Alexander B. Sideridis
Charalampos Z. Patrikakis (Eds.)

LNICST

26

LNICST

Next Generation Society

Technological and Legal Issues

Third International Conference, e-Democracy 2009
Athens, Greece, September 2009
Revised Selected Papers

ICST

Springer

Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 26

Alexander B. Sideridis
Charalampos Z. Patrikakis (Eds.)

Next Generation Society

Technological and Legal Issues

Third International Conference, e-Democracy 2009
Athens, Greece, September 23-25, 2009
Revised Selected Papers

Springer

Volume Editors

Alexander B. Sideridis
Agricultural University of Athens, Informatics Laboratory
75, Iera Odos Street, Botanikos, 11855, Athens, Greece
E-mail: as@aua.gr

Charalampos Z. Patrikakis
Agricultural University of Athens, Informatics Laboratory
75, Iera Odos Street, Botanikos, 11855, Athens, Greece
E-mail: bpatr@aua.gr

Library of Congress Control Number: 2009943163

CR Subject Classification (1998): J.1, J.4, J.7, K.4, K.5, K.6

ISSN 1867-8211
ISBN-10 3-642-11629-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-11629-2 Springer Berlin Heidelberg New York

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12841752 06/3180 5 4 3 2 1 0

Preface

Recent developments in information and communication technology (ICT) have paved the way for a world of advanced communication, intelligent information processing and ubiquitous access to information and services. The ability to work, communicate, interact, conduct business, and enjoy digital entertainment virtually anywhere is rapidly becoming commonplace due to a multitude of small devices, ranging from mobile phones and PDAs to RFID tags and wearable computers. The increasing number of connected devices and the proliferation of networks provide no indication of a slowdown in this tendency. On the negative side, misuse of this same technology entails serious risks in various aspects, such as privacy violations, advanced electronic crime, cyber terrorism, and even enlargement of the digital divide. In extreme cases it may even threaten basic principles and human rights. The aforementioned issues raise an important question: Is our society ready to adopt the technological advances in ubiquitous networking, next-generation Internet, and pervasive computing? To what extent will it manage to evolve promptly and efficiently to a next-generation society, adopting the forthcoming ICT challenges?

The Third International ICST Conference on e-Democracy held in Athens, Greece during September 23–25, 2009 focused on the above issues. Through a comprehensive list of thematic areas under the title "Next-Generation Society: Technological and Legal issues," the 2009 conference provided comprehensive reports and stimulated discussions on the technological, ethical, legal, and political challenges ahead of us.

As regards the technical program, the conference consisted of 54 oral presentations constituting 10 sessions, and two invited speeches, covered in two days. The conference ended with a round table, summarizing and stimulating discussion. Two invited speakers from the legal and the technical section of the conference's twofold topic led each day's presentations.

The first day, invited speaker Spyros Simitis presented recent developments in ICT technology and their repercussions in the field of data protection. Two parallel sessions followed addressing both legal and technical topics. Regarding the legal issues, the first day included two special sessions on politics, legislation, and regulatory framework, in which papers addressing surveys, studies, and discussions regarding the regulatory issues, enforcement of data protection acts, and data protection laws, impact of Web technologies to e-Democracy, and e-services, digital forensics, biometric data, as well as protection of privacy were discussed among others. Regarding technical issues, e-government and e-procurement services, as well as the use of ICT for supporting e-participation and e-voting, were discussed, with the parallel presentation of applications, services, and project results. Finally, security and privacy issues, covering also the topics related to crime and attacks, were discussed with presentations on trust and security over the Web, security management, and computer virology.

The second day, invited speaker Andrew Tanenbaum had opened the technical program with a plenary speech on the way the Internet has affected politics and elections. Following the pattern of the first day, parallel sessions—focusing mostly on technical issues—concluded the presentations of the conference. The areas of interest of the researchers included e-Government, educational, collaboration, and social networking, as well as pervasive mobile and ubiquitous computing issues. Presentations on e-Government applications and frameworks in European countries such as Greece and Austria, but also non-European such as Zambia—even fictional (as the case of Balmeda)—were given providing a comprehensive coverage of the status and state of the art in e-Government and local e-Government. In the same context, the critical issue of the digital divide as regards ICT use and penetration was also addressed. As regards education, the corresponding session focused on the access to knowledge, copyright issues, and future of e-learning, while the results of projects regarding training on ICT and Internet safety were presented. Moving to the next session, issues related to social networking and blogs were addressed through presentations on online communities and collaboration, social networking and interacting covering up to state-of-the-art communication and collaboration tools such as virtual worlds. Concrete paradigms such as that of social networking among youth in South Africa complemented the coverage of the topic. The final session was devoted to pervasive, ubiquitous, and intelligent computing, including issues covering ad-hoc and mobile networks, vehicular communications, and pervasive applications. During this session an extensive coverage of the corresponding application fields was obtained.

The conference concluded with a discussion panel consisting of four academics (the conference Chair Alexander B. Sideridis, the invited speakers Spyros Simitis and Andrew Tanenbaum and Elias Pimenidis) and an eminent practitioner (the Federal Commissioner for Data Protection and Freedom of Information in Germany, Peter Schaar). During this session, conclusions drawn from the conference sessions were presented enriched with questions raised by the conference Chair and the audience. Answers and stimulating comments were offered by the panel mainly focused on the future of e-Democracy, as this is foreseen through the technological breakthroughs, the evolution of legislation and the need for personal freedom, access to added value services, and preservation of personality and privacy.

Alexander B. Sideridis
Charalampos Patrikakis

Organization

Conference Chair

A.B. Sideridis	President of the Scientific Council for the Information Society, Greece

Conference Co-chairs

Ch. Patrikakis	National Technical University of Athens, Greece
S. Voulgaris	Vrije University, The Netherlands

Tutorials Co-chairs

V. Zorkadis	Hellenic Data Protection Authority, Greece
Z. Kardasiadou	Hellenic Data Protection Authority, Greece

Travel and Fees Grants Chair

K. Gialouris	Agricultural University of Athens, Greece

Workshops Chair

C. Costopoulou	Agricultural University of Athens, Greece

Demos Co-chairs

J. Soldatos	Athens Information Technology Center, Greece
O. Pyrovolakis	General Secretariat of Information Systems of Greece

Invited Papers Chair

N. Manouselis	Greek Research & Technology Network (GRNET S.A.)

Technical Program Chair

M. Anagnostou	National Technical University of Athens, Greece

Local Arrangements Co-chairs

S. Karetsos	Agricultural University of Athens, Greece
M. Drougka	Agricultural University of Athens, Greece

Financial Chair

G. Loukeris	Lawyer

Web Co-chairs

A. Makrandreou	Agricultural University of Athens, Greece
M. Koukouli	Agricultural University of Athens, Greece

Sponsorship and Affiliations Chair

E. Vasilaki	Scientific Council for the Information Society, Greece

Publications Co-chairs

M. Anagnostou	National Technical University of Athens, Greece
E. Pimenidis	University of East London, UK
Ch. Patrikakis	National Technical University of Athens, Greece
S. Voulgaris	Vrije University, The Netherlands

Publicity Co-chairs

E. Boubouka	Journalist "Eleftherotipia", Greece
M. Tsimitakis	Journalist, Greece

International Committee Co-chairs

E. Vasilaki	Scientific Council for the Information Society, Greece
H.C. Chao	National Ilan University, Taiwan
E. Pimenidis	University of East London, UK

Program Committee

N. Alexandris	University of Piraeus, Greece
E. Alexandropoulou	University of Macedonia, Greece
M. Anagnostou	National Technical University of Athens, Greece
G. Anastassopoulos	Democritus University of Thrace, Greece
T. Banyan	Statewatch
Ch. Bouras	University of Patras, Greece
H.C. Chao	National Ilan University, Taiwan
V. Chrisikopoulos	Ionian University, Greece
C. Costopoulou	Agricultural University of Athens, Greece
L. Crearie	University of the West of Scotland, UK
G. Doukidis	Athens University of Economics and Business, Greece
Ch. Douligeris	University of Piraeus, Greece

Ch. Georgiadis	University of Macedonia, Greece
P. Georgiadis	National and Kapodistrian University of Athens, Greece
K. Gialouris	Agricultural University of Athens, Greece
D. Gritzalis	Athens University of Economics and Business, Greece
S. Gritzalis	University of the Aegean, Greece
M.P. Gupta	Indian Institute of Technology Delhi, India
G. Haramis	University of Macedonia, Greece
L. Iliadis	Democritus University of Thrace, Greece
G. Iliopoulos	University of the West of Scotland, UK
H. Jahankhani	University of East London, UK
D. Kaklamani	National Technical University of Athens, Greece
Z. Kardasiadou	Hellenic Data Protection Authority, Greece
G. Karetsos	Technological Educational Institute of Larissa, Greece
S. Katsikas	University of Piraeus, Greece
E. Keravnou-Papailiou	University of Cyprus, Cyprus
S. Kokolakis	University of the Aegean, Greece
M. Lambrou	University of the Aegean, Greece
Sp. Likothanassis	University of Patras, Greece
D. Livingston	University of the West of Scotland, UK
E. Loukis	University of the Aegean, Greece
F. Makedon	University of Texas Arlington, USA
N. Manouselis	Greek Research and Technology Network (GRNET S.A.)
V. Manthou	University of Macedonia, Greece
L. Merakos	National and Kapodistrian University of Athens, Greece
E. Mitrou	University of the Aegean, Greece
J. Najjar	Synergetics NV, Belgium
G. Nouskalis	Aristotelean University of Thessaloniki, Greece
M. Nunes	Inesc Inovacalo, Portugal
X. Ochoa	Escuela Superior Politécnica del Litoral, Ecuddor
G. Pangalos	Aristotelean University of Thessaloniki, Greece
A. Pateli	Ionian University, Greece
Ch. Patrikakis	National Technical University of Athens, Greece
F. Paulsson	Umeå University, Sweden
J. Pawlowski	University of Jyväskylä, Finland
E. Pimenidis	University of East London, UK
N. Polemi	University of Piraeus, Greece
A. Pouloudi	Athens University of Economics and Business, Greece
N. Prasad	Aalborg University, Denmark
R. Prasad	Aalborg University, Denmark
A. Pucihar	University of Maribor, Slovenia
O. Pyrovolakis	General Secretariat of Information Systems of Greece
M.A. Sicilia	University of Alcalá, Spain
A.B. Sideridis	President of the Scientific Council for the Information Society (SCIS), Greece
Th. Simos	University of the Peloponnese, Greece
S. Sioutas	Ionian University, Greece

P. Spyrakis	University of Patras, Greece
C. Stracke	University of Duissburg-Essen, Germany
E. Sykas	National Technical University of Athens, Greece
A. Tatnall	Victoria University, Australia
M. Tentzeris	Georgia Institute of Technology, USA
A. Tsakalidis	University of Patras, Greece
P. Tsanakas	Greek Research and Technology Network (GRNET S.A.)
N. Tselikas	University of the Peloponnese, Greece
Th. Tsiligiridis	Agricultural University of Athens, Greece
I. Venieris	National Technical University of Athens, Greece
G. Vassilakopoulos	University of Piraeus, Greece
M. Vlachopoulou	University of Macedonia, Greece
S. Voulgaris	Vrije University, The Netherlands
M. Yannakoudakis	Athens University of Economics and Business, Greece
V. Zorkadis	Hellenic Data Protection Authority, Greece

National Ambassadors

Australia	A. Tatnall
Belgium	J. Najjar
Canada	L.T. Yang
Equador	X. Ochoa
Finland	J. Pawlowski
France	A.M. Kermarrec
Germany	C. Stracke
Greece	M. Anagnostou
India	M.P. Gupta
The Netherlands	S. Voulgaris
Portugal	M. Nunes
Rep. of Korea	J. H. Park
Slovenia	A. Pucihar
Spain	M.A. Sicilia
Sweden	F. Paulsson
Taiwan	H.C. Chao
UK	E. Pimenidis
USA	F. Makedon

Table of Contents

Session 1: Politics – Legislation – Regulatory Framework I

Session 2: Enhancing Quality of Life through e-Services

Session 3: Politics – Legislation – Regulatory Framework II

Session 4: Supporting Democracy through e-Services

Session 5: Identity Management, Privacy and Trust

Session 6: Security, Attacks and Crime

Session 7: e-Government and Local e-Government

Session 8: Education and Training

Session 9: Collaboration, Social Networking, Blogs

Session 10: Pervasive, Ubiquitous, and Intelligent Computing

Session 1

Politics – Legislation – Regulatory Framework I

A Study on the Lack of Enforcement of Data Protection Acts

Thorben Burghardt[1], Klemens Böhm[1], Erik Buchmann[1],
Jürgen Kühling[2], and Anastasios Sivridis[2]

[1] Universität Karlsruhe (TH), 76131 Karlsruhe, Germany
{burgthor,boehm,buchmann}@ipd.uni-karlsruhe.de
[2] Universität Regensburg, 93040 Regensburg, Germany
{Juergen.Kuehling,Anastasios.Sivridis}@jura.uni-regensburg.de

Abstract. Data privacy is a fundamental human right, not only according to the EU perspective. Each EU state implements sophisticated data protection acts. Nevertheless, there are frequent media reports on data privacy violations. The scientific and the political community assume that data protection acts suffer from a lack of enforcement. This paper is an interdisciplinary study that examines this hypothesis by means of empirical facts on juridical assessment criteria – and validates it. We have inspected 100 service providers, from social online platforms to web shops. Our study considers legal requirements of the privacy policy and how providers ask for consent and react to requests for information or deletion of personal data. Our study is based on articles of German law that have a counterpart in the EU Directive 95/46/EC. Thus, our study is relevant for all EU states and all countries with similar regulations.

Keywords: Privacy, study, lack of enforcement, data protection acts.

1 Introduction

In the last years, data protection acts have not kept pace with new developments, with unpredictable consequences for society. Data protection directives like 95/46/EC [5] establish data privacy as a human right and require each EU state to implement privacy regulations. However, global organisations have established various links to internal and external subsidiaries, service providers, etc. It has become difficult to keep track of the whereabouts of personal data, to identify the company responsible and to enforce those privacy rights. Many of the data privacy scandals of the last years might not have happened if existing data protection acts would have been enforced. Thus, the scientific and political communities tend to assume that data privacy acts suffer from a lack of enforcement. However, to our knowledge there is no empirical study that supports this hypothesis by collecting facts on juridical assessment criteria.

In this work, we present an interdisciplinary study of the lack of enforcement of data protection acts. Since it is impossible to analyze company-internal violations of data privacy laws, we focus on privacy violations from an external perspective. We analyze if an individual concerned would be able to assert

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 3–12, 2010.

her privacy rights against a broad range of service providers. Therefore we consider legal requirements of the privacy policy, and how providers ask for consent and react to requests for information or deletion of personal data. We focus on German law and representative German providers. As the EU directives, e.g., 95/46/EC [5], have harmonized data protection laws throughout the EU, and most of the providers investigated are supra-national companies that operate in many other states as well, we deem our results representative for all EU members and all states with similar privacy legislation.

2 Background

2.1 Related Work

We are first to confirm a lack of enforcement based on juridical assessment criteria. There are some studies that indicate an enforcement problem, but do not implement juridical expertise. [8] uses a web crawler to automatically identify conflicts in machine-readable privacy policies (P3P). However, most privacy violations tend to be more complex than matching P3P policies with the use of cookies or web bugs. [9] is a study of 655.000 German Web pages of 14.000 providers. They study if a provider uses a statistics service like Google Analytics and declares this properly. Another study [10] has browsed 815.000 web sites for contact forms, data requested and how much effort is required to find the privacy policy. As a result, 35% of all providers requesting personal information do not display a privacy policy. However, without juridical expertise such studies cannot detect many typical privacy violations, e.g., if the provider has to specify the purpose of data acquisition, or if it is obvious.

2.2 Legal Background

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [6] introduce principles in order to unify privacy regulations in the OECD countries. The guidelines are intended to establish common privacy standards, and to ease transborder data flow between countries with similar regulations. The principles include openness, collection limitation, data quality, purpose specification, use limitation, security safeguards, and individual participation in data protection. The OECD principles are part of many data protection acts like the Asia-Pacific Economic Cooperation Privacy Framework [7]. While the OECD provides recommendations only, all EU member states must transpose directives of the European Community (EC) to national law. Directive 95/46/EC [5] implements the OECD principles to harmonize data protection legislation throughout Europe. Beyond that, the directive specifies privacy as a human right [4], as laid down in Art.6 p.2 European Union Treaty referring to the European Convention on Human Rights.

In Germany, Directive 95/46/EC has been cast into national laws, such as the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG [1]) and acts for specific application areas. The German Telemedia Act (Telemediengesetz, TMG [2]) is one of the core Internet regulations in Germany. It includes a number of articles that implement Directive 95/46/EC, thus consider the OECD Guidelines. The scope of the TMG includes all providers that operate under German law and offer services via the Internet, but exclude telecommunication or related services.

Our goal is to investigate the lack of enforcement of Internet data protection acts throughout the EU. Since legal issues cannot be investigated based on a directive, we rely on the TMG [2] and on the BDSG [1]. In the following, we will enumerate regulations relevant for our study, and we will name corresponding articles of Directive 95/46/EC. The regulations will be described in Section 4. Relevant privacy regulations fall into two categories:

Data Acquisition and Usage. According to 95/46/EC, data protection follows the principles of (1) purpose specification and (2) prohibition with the option of authorization. §12 p.1 and 2 TMG (Art. 6 and 7 of 95/46/EC) implement these principles. The articles require the provider to request a consent from the user if data acquisition and usage goes beyond what is necessary for service delivery or what is allowed by the legislator.

Information Duties. §13 p.1 s.1 TMG (Art.10 of 95/46/EC) obliges the provider to inform the individuals concerned on the kind of data acquired, the purpose of the data acquisition and the storage period, and if data is processed in countries not addressed by 95/46/EC. According to §13 p.1 s.2 TMG (Art.5 p.3 of 2002/58/EC), each provider has to inform about automated processes that manage personal data. §13 p.2 TMG specifies the electronic declaration of consent. §13 p.1 s.1 TMG requires to inform the user on forwarding data to other companies. In particular, §4 p.3 BDSG (Art.10 of 95/46/EC) requires to categorize the receivers, e.g., dispatcher or credit agency. According to §13 p.7 TMG and §34 BDSG (Art.12 of 95/46/EC), each provider has to answer requests for information from an individual concerned about her personally identifiable data. The request has to be answered precisely to allow to assert subsequent rights, e.g., to block, correct or delete data as outlined in §35 BDSG (Art.12 of 95/46/EC).

This set of regulations is not exhaustive. However, all of these regulations have a counterpart in the Directive 95/46/EC, i.e., a study based on these articles is relevant for other countries with similar privacy regulations. Furthermore, those regulations are important for almost all service providers on the Web.

3 Study Setup

Provider Sample. We have examined 100 providers on the Internet (first row of Table 1). Our complementary website[1] lists all providers and details of the study data. Our sample is based on usage statistics on teenagers [12] and young adults [11], and considers statistics from an online marketer group [3] and similar sources. We have chosen a representative sample of providers according to their *Impact*, *Relevance* and *Comparability*.

[1] http://privacy.ipd.uka.de

Table 1. Provider Sample

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of providers investigated	*100*	21	48	8	6	10	7
Number of registrations	*89*	21	38	8	6	9	7

Impact. The number of customers and customer interactions defines the impact. Our sample contains providers with a high market share. Further, we take into account that individuals of different age and from different social groups might prefer different providers.

Relevance. We have selected a provider mix from various categories, i.e., news portals, web shops, auction platforms, messaging services and social community platforms. These categories are relevant for a wide range of society. Note that we do not investigate the same number of providers from each category, because in some categories a few providers dominate the market.

Comparability. Providers are comparable only as long as they follow the same regulations. Thus, we have decided to focus on providers that fall under German law. Our selection still includes international providers, but we have verified that they operate under German law.

Study Procedure. We cannot expect meaningful results if providers realize that they are subject of a study. Thus, we have constructed an artificial identity including name, day of birth, post office box, address, phone, fax and cellphone number, email and a pseudonym. Our study consists of four phases:

1. **First Visit.** Before registering, we investigate if the privacy policy is visible, and if it contains all mandatory information.
2. **Registration.** We register our artificial person at the web site of the providers (cf. Table 1, second row) and analyze the registration process. Only 11 providers did not require a registration before it was necessary, e.g., to pay products bought in a web shop.
3. **Request for Information.** We send an email in the name of our artificial person to each provider where the person is registered. The email asks for all information (1) stored and (2) forwarded to other companies.
4. **Right of Deletion.** We let our artificial person assert her right of deletion, i.e., we send an email to each provider that asks for all personal data to be deleted.

4 Study Results

4.1 The Privacy Policy

We have analyzed the privacy policies of our 100 providers regarding (1) availability, the obligation to inform about (2) data acquisition and handling, (3) data forwarding and (4) automated processing.

Table 2. Anytime Availability

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Directly accessible	*9*0	16	45	8	6	8	7
Can be found	*9*	5	2	0	0	2	0
Undiscoverable	*1*	0	1	0	0	0	0
Based on outdated laws	*1*0	2	6	0	0	2	0

Anytime Availability. §13 p.1 s.3 TMG: *Each customer must be able to obtain the privacy policy easily and at any time. The provider should offer links on each page which direct the user to a valid privacy policy.* □

Table 2 shows that 90 providers offer privacy polices directly reachable via highlighted links from every web page. The policies are either part of the general terms and conditions or are presented on a standalone web page. 9 providers require their users to follow a sequence of links. It depends on the concrete design of the web site if this procedure would be considered acceptable by court. We did not find the privacy policy of one provider, i.e., the provider is in conflict with law. Finally, 10 providers refer to outdated laws that are invalid by now.

Information on Data Acquisition and Handling. §13 p.1 s.1 TMG: *A provider has to inform on (i) the kind of data, i.e., which attributes are acquired, (ii) the storage period and (iii) the purpose of data acquisition and usage. The purpose specification can be omitted when obvious.* □

Table 3. Information on Data Acquisition and Handling

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Kind of data							
Detailed specification	*4*7	12	18	2	4	5	6
Coarse categories	*2*1	5	10	2	1	2	1
Unspecific terms	*3*1	4	19	4	1	3	0
Storage period							
Data stored for a specified period of time	*6*8	15	26	8	5	8	6
No information	*3*1	6	21	0	1	2	1
Purpose of acquisition							
Specific information	78	10	42	7	5	7	7
Unspecific terms	*2*1	11	5	1	1	3	0

Kind of data. The 99 providers with a privacy policy specify the data acquired in different ways. As the first part of Table 3 shows, 47 providers explicitly specify each single attribute they store, and 21 of them name coarse but intuitive categories of data, e.g., 'shipping address'. 31 providers use unspecific terms like 'information necessary for order processing'. 6 providers do not specify the kind of data they acquire, i.e., they are in conflict with law.

Storage period. 68 providers (second part of Table 3) state that data is stored for a specific period of time, namely until the user revokes her account; after that the data will be locked for legal obligations. 31 providers do not address storage time, thus conflict with the regulations.

Purpose of acquisition. 78 providers (third part of Table 3) explicitly state the purpose of the data acquisition. 21 providers use unspecific statements, e.g., 'for service provision'. Legislation accepts this only if the purpose is obvious. However, this holds only for 6 of the 21 providers, which operate common web shops. The other 15 providers run information portals or email services and integrate additional services, i.e., that purpose is not obvious.

Information on Data Forwarding. §13 p.1 s.1 TMG: *Each provider has to inform about personal data being forwarded. The privacy policy should explain which data is transferred to whom.* □

As shown in Table 4, 64 providers state in their privacy policy to forward personal data. While 23 providers state to forward data in order to execute the contract, 27 providers give an unspecific reason, e.g., to provide better services.

Table 4. Information on Data Forwarding

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Provider forwards data	*64*	13	30	5	6	7	3
Reason							
To execute the contract	*23*	2	18	2	0	1	0
Unspecific reason	*27*	9	5	0	6	5	2
Receivers							
Logistics services or credit agencies	*26*	0	24	1	0	1	0
Associated companies	*27*	7	6	2	5	6	1
. . . Receiving companies are named	*7*	5	0	2	0	0	0
Unspecific partners	*22*	4	9	0	3	4	2
. . . Partners are named	*1*	0	0	0	0	0	1
Receiving countries							
Outside of the EU	*12*	0	4	1	3	3	1
. . . Receiving countries are named	*8*	0	2	1	3	1	1

26 providers declare to forward data to logistics services or credit agencies, and 27 forward to associated companies, but only 7 name them explicitly. When the receivers are clearly described, the individual concerned can guess why data is forwarded. On the other hand, 22 providers forward data to vaguely defined business partners, and only one provider names them. Finally, 12 providers declare to transfer data to locations outside the EU, but only 8 explicitly list these locations. If unspecific statements prevent a person from asserting her privacy rights, e.g., request the deletion of personal data from an unnamed partner or a company outside the EU, such privacy policies conflict with law.

Information on Automated Processing. §13 p.1 s.2 TMG: *Each provider has to inform about automated data processing if those processes facilitate or give way to the identification of an individual. The obligation to inform includes the (i) kind of data, (ii) storage period and (iii) purpose of processing.* □

Table 5. Information on Automated Processing

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Providers using cookies	*96*	21	46	7	6	9	7
Information on automated data processing							
Cookie usage is specified	*72*	16	35	2	6	7	6
Purpose of the cookie is specified	*65*	14	33	1	5	6	6
Storage time of the cookie is specified	*28*	5	18	0	1	2	2
Legal aspects							
Usage of cookies without information	*24*	5	11	5	0	2	1
No information about storage time	*41*	11	14	2	5	5	4
Wrong information on storage time	*9*	3	3	0	1	1	1

A well-known example of these processes are cookies. Cookies can be used to track the movement of users on a web portal over long periods of time, i.e., they allow to map users to IDs which might be used to build comprehensive user profiles. We have investigated if and how our providers use cookies, and if they declare the use of cookies properly. While 96 of 100 providers use cookies (first row of Table 5), only 72 of them refer to automated processes in the privacy policy. Furthermore, only 65 providers name the purpose of the cookie, and only 28 specify the storage time (second part of Table 5). We found that 24 providers do not inform about the use of cookies at all, 41 providers do not declare the storage time of the cookie, and 9 of them report a wrong storage time[2] (third part of Table 5). Only 19 providers implement the law properly.

[2] Since cookies are stored at the client site, we can observe the storage period.

Table 6. Request for Consent

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Consent required	*72*	16	27	8	5	9	7
. . . but no request for consent	*12*	0	10	1	0	1	0
Consent requested on privacy policy/terms and conditions	*47*	13	8	6	5	8	7
Information on consent revocation	*54*	16	16	5	4	6	7
Consent to personalized user profiles							
Consent required for user profiles	*27*	5	6	2	3	6	5
Consent requested on privacy policy/terms and conditions	*23*	5	2	2	3	6	5
No request for consent	4	0	4	0	0	0	0
Consent to data acquisition							
Consent required for data acquisition	*26*	2	9	6	1	1	7
Consent requested on privacy policy/terms and conditions	*18*	2	3	5	1	0	7
No request for consent	*8*	0	6	1	0	1	0

4.2 Request for Consent

§12 p.1, §13 p.2 TMG: *Acquisition and usage of personal data are allowed only if permitted by law, if required for obvious reasons, or if the user gives her consent. The user must be informed that the consent can be revoked at any time.* □

Following our analysis, 72 providers would have to ask the user for consent (Table 6). 12 of these 72 providers do not ask for consent at all. 47 expect the user to give her consent to the privacy policy or the general terms and conditions as a whole. It depends on the specifics if this would be accepted by court. For example, a consent is invalid if important information is hidden in a voluminous policy. Only 54 inform on the right to revoke the consent. The other providers conflict with law. The second and third part of Table 6 list our findings in detail. 27 providers build personalized user profiles, but 4 do not ask for consent. 23 ask for consent on a lengthy document. Similarly, 26 providers want to acquire data not needed for the service, but require consent on a large document (18) or do not ask for consent (8).

A valid consent requires that the user can check what she has given her consent to. If a provider has modified its conditions, the user might have consented to a declaration different from the current one. Only a few providers (e.g., Amazon) have previous versions of the privacy policy or of the declaration of consent available. No provider let the user identify the version she has consented to.

4.3 Request for Information

§13 p.7 TMG, §34 BDSG: *Each customer can ask a provider to inform her on her personal data. The provider has to list all data stored or forwarded to support the subsequent exertion of rights, e.g., the right of deletion.* □

Table 7. Request for Information

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of responses	56	14	27	4	2	4	5
Average response time	2.05	1.38	2.67	2.5	0.5	3,25	2
No information, but reference to privacy policy	8	4	1	1	1	1	0
No information, but reference to user profile page	7	3	2	0	1	0	1
Useless answer	6	2	3	0	0	0	1
States not to have forwarded data	25	6	11	3	1	0	4
Wrong information about forwarding	2	2	0	0	0	0	0
No information about forwarding	16	5	8	0	1	1	1

We let our artificial person ask 87 providers to list all information they (1) store and (2) have forwarded to other companies. As Table 7 shows, we have obtained responses from 56 providers, i.e., 33 have ignored our request outright. The others have answered within two days on average.

Some providers have not responded with the data required, but have told us to only store information listed in the privacy policy (8 providers) or shown at the user profile page on their web site (7 providers). 6 providers replied with canned text that had nothing to do with our request. 25 provider stated not to forward data. In 2 cases the answer was sent from a different company within the company group, i.e., the advice was obviously wrong. 16 providers ignored our request for information on the data forwarded.

4.4 The Right of Deletion

§35 p.2 BDSG, §12 p.1 and p.2, §14 p.1 and §15 TMG: *A provider has to delete all personal data if the person concerned asserts her right of deletion. Exceptions include legal obligations or data required for accounting.* □

Table 8. The Right of Deletion

	Total	News Portals	Shops	Auction Platforms	Shops	Messaging	Social Platforms
Number of responses	59	14	31	4	3	2	5
Average response time	1.15	1.07	1.96	1.5	1	1	0.40
Immediate deletion	35	5	17	4	2	3	4
Self deletion	5	1	2	1	0	0	1
Deletion refused	2	1	1	0	0	0	0
Not registered	5	1	4	0	0	0	0

We let our artificial person send a request for deletion to all 87 providers where the person has been registered. As shown in Table 8, 59 providers answered the request. 35 of them deleted all account information directly or after a confirmation and acknowledged the deletion. 5 providers stated not to store any information beyond the one the user can delete after logging in. 2 providers refused the deletion due to technical reasons, and 5 providers told us that our artificial person is not registered, or the data cannot be found. In total, 35 providers are in conflict with law.

5 Conclusions

This paper is an interdisciplinary study on the lack of enforcement of data protection acts on the Internet. We have compared the practices of 100 service providers to requirements from German law that have a counterpart in EU Directive 95/46/EC. Our analyses show that the vast majority of privacy policies use unspecific terms and/or do not display all information required by law. A significant share of the providers does not ask users for consent, as requested by law. Though many providers respond quickly to requests for information or deletion of personal data, such responses often lack mandatory information.

Acknowledgments. This work was partly funded by DFG BO2129/8-1. We thank Mathis Schwuchow and Timo Wankmüller for their intensive support.

References

1. Bundesdatenschutzgesetz (BDSG). Bundesgesetzblatt I 2003 S.66 (2003)
2. Telemediengesetz (TMG). Bundesgesetzblatt I 2007 S. 179 (2007)
3. Arbeitsgemeinschaft Online-Forschung e.V. AGOF Internet Facts 2008-IV (2008), http://www.agof.de
4. Council of Europe. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), http://www.echr.coe.int
5. European Parliament and the Council of the European Union. Directive 95/46/EC. Official Journal L 281, 11/23/1995, p. 31 (1995)
6. Organization for Economic Cooperation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
7. Privacy Framework. Asia-Pacific Economic Cooperation, APEC (2004)
8. Jensen, C., et al.: Tracking Website Data-Collection and Privacy Practices with the iWatch Web Crawler. In: Proceedings of the SOUPS 2007 (2007)
9. Lepperhoff, N., Petersdorf, B.: Datenschutz bei Webstatistiken. Datenschutz und Datensicherheit - DuD 32, 266–269 (2008)
10. Lepperhoff, N., Petersdorf, B.: Wie Unternehmen im Internet bei Konsumenten Misstrauen sähen. In: XAMIT (2008)
11. Media Pedagogy Research Assisiation South-West. JIM-Studie - Youth, Information, Multi-Media (German) (2006)
12. Media Pedagogy Research Assisiation South-West. KIM-Studie - Children and Media, Computer and Internet (German) (2006)

The Impact of the Web and Political Balance to e-Democracy

Christos Manolopoulos[1], Rozina Efstathiadou[1], and Paul Spirakis[1,2]

[1] Research Academic Computer Technology Institute
{manolop,efroz,spirakis}@cti.gr
[2] University of Patras
spirakis@cti.gr

Abstract. In this paper we explore the relations between the Web, governance individual and collective action.

We set three questions which arise in relation to the interaction between the Internet and socio-political dynamics.

1. How do we delineate democracy in these new conditions?
2. Does the Internet create a new crisis of political balance or does it intensify an imbalance of a whole political cycle?
3. How can we explore new forms of political balance based on the reality of the Internet?

We explore these complex dynamics from a theoretical perspective proposing a model which combines the theory of minorities with a catnet framework. We run simulation experiments and analyze experimental outcomes. We conclude that the complex relation between the Web, governance models and collective action produces non predictable outcomes and a possible crisis .Only a substantial shift in the stance of the state and the authority, bearing the meaning of acceptance of a widen democracy, will create a new balance that will reflect the new conditions. This shift could occur either cooperatively or through a social conflict.

Keywords: Web, e-Democracy.

1 Introduction

It is accepted that the need for a strong governance perspective where citizens and businesses seek empowerment becomes a challenge for the public sector and state entities. In recent years both e-participation and e –government had made significant advances and have set in motion certain social interactions, as well as opinion and public service distribution procedures accordingly. On the one hand ICT advances in the fields of information diffusion and social networks, caused a critical mass of coherent e- communities and groups which grow at certain rates either at the level of population size or at the level of dense collaboration and information flow.

According to D. Broster [10] next stage is probably “the need to include a strong governance perspective where citizens and businesses seek empowerment and where

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 13–28, 2010.

both geographic boundaries and the role of administrations, the private and civil sectors, are all blurring". This situation entails profound challenges and opportunities for governance. A new governance model where government is seen as just one form of collectivity alongside other forms which are emerging as ICT is taken up, could meet these new challenges. People are becoming increasingly educated and connected and therefore seek to be involved. On the other hand they demand this involvement to guarantee transparency, collaboration, accountability in information flow through an increased intelligent use of the technology.

In principle this demand could be based on the interlink of e- participation and e-government dynamics and practices. Each one could provide advantages to such a process. For instance e-participation could mobilize citizens in order to provide arenas for deep conversations and opinion exchanges and operate as providers of crucial innovative ideas and concepts concerning governance. But at the same time e- participation practices are not themselves mature to guarantee misuse of the participation processes as well as threats to sensitive data and identity protection. Besides e-government practices, while matured to a more or less degree seem to be developed and run with no significant relevance to proposals expressed directly by citizens. Therefore the concept of e-government itself should be reoriented towards a) interrelations with citizens, b) overcoming border, racial, etc barriers c) incorporating direct on line collaboration, communication between government agencies and citizens.

ICT growth could provide these opportunities. As is shown by European e-Participation study [27] 258 e-Participation cases were identified and collected which entail weak e-Participation culture diffusion and lack of a dense citizen – government networking model while private social networking grows at significant and accelerated rates. Concerning e-Participation areas a vast majority of these 258 reported cases enable information provision (113 cases) and deliberation (78 cases), followed by consultation and discourse.

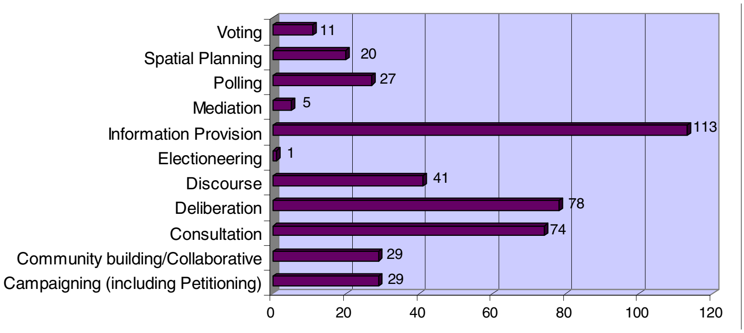


Fig. 1. e-Participation Areas -Source European e-Participation Study

Regarding the participation level, cases were identified in all different levels but the majority of pf the results refer to the local level confirming that participation is usually higher at the local level and consequently indicating that governments are seldom being willing to communicate governmental plans, legislature proposals and several issues of great importance to citizens.

The results also show that EU's policy encourages e-Participation practices which is indicated by the percentage of e-Participation projects funding. National Governments seem to be unwilling to financially support e-Participation practices.

2 Web, State and Political Movements

2.1 Web and the Democratic Deficit Condition

The Web interacts with the population through a wide range of procedures and primarily regards them as consumers. Thus, it sets into motion an interaction between the market and the consumer. Although this type of interaction is market oriented, has the property of diffusing information in a manner where the customer is not passive receiver.

E-Governance interacts with the citizen, through a network of services, which not only offers, but also accommodates conventional government functions. However, the fact that the services offered to citizens do indeed improve their lives, does not compensate for their dissatisfaction in light of other distinct government practices. To illustrate, the fact that the citizens of a country, as Web users enjoy the benefit of services allowing straightforward transactions with the state and averting bureaucracy, does not imply that this will compensate for their malcontent in the likely event that their country becomes embroiled in a war or in practices which destroy the environment, etc. Yet, it is exactly this empowerment of the consumers and the citizens, granted by the possibilities offered through the Web and ICT that prompts them to become more demanding consumers of both the state and of the market provided services. Web, therefore, entails user's empowerment while e-Government does not yet target citizen's empowerment.

In interpreting such a setting, Castells [12] proceeds with an analysis of the relationship that holds between the Internet and democracy and he discovers that for the time being Internet use, rather than reinforcing democracy by enhancing knowledge and citizen participation, tends to exacerbate the crisis regarding political justification. He goes on to say that in the contemporary world, there is a widespread crisis vis a vis political justification and the dissatisfaction of citizens with their representatives. However, beyond the citizen-state relation, intense crises and discontent arise in relation to the nature of the economic globalization system and the inequality and imbalances it produces, the global environmental problems, the violation of human rights by many states, events and conditions that generalize, globalize and aggravate the crisis environment. Indeed, it is the Internet itself that acts as the platform for the swift diffusion of these feelings of discontent, thus breeding rapid destabilization.

In venturing to express the aforementioned in a loose formalism, we could describe the citizen-state relation as multi-dimensional and we could grade satisfaction according to how the citizen-consumer perceives the level of satisfaction that each governmental act generates. Thus, we could define as {U+} and {-u} the levels of satisfaction and dissatisfaction accordingly which consumer is able to compare with a value Ui. Furthermore, provided that the Web provides an organizational framework that empowers the Internet user through communication and information, Ui, constantly increases, putting pressure on {U+} and {-u}.This process does not necessarily enable consumer to suggest a policy that will bring about the result she/he anticipates. Therefore, we must define the justification crisis not as a number of propositions put forward by the citizens, but as a rising wave of increasing malcontent that within the Web finds suitable conditions to gain speed and force.

Having defined the process which concerns the decreasing political justification of governments and the empowerment of the citizen as an ICT consumer, we can build a model that describes the dynamic development of this form of social change. Aberg [5] has shown population dynamics and the expected values of two alternative strategies of a population (in fact, in the standard Aberg model the alternatives are: being or not being a member of a trade union). She specified a differential equation model with a reasonable micro foundation. Generalizing as referring to the decisions between doing I (accept a particular policy) and doing S (don't accept it), if the actor's opportunity sets consist of these two alternative actions, if the value of doing one thing rather than another depends upon what others do and if the speed at which individuals change actions depends on how desirable each alternative is perceived to be, then the social outcomes the actors are likely to bring about can be approximated by a set of differential equations. When applying the Aberg's model, it is evident that only a small percentage of a population is required to take on a strategy or an action to dismiss a particular policy or to reject the political justification of a government or the representatives of the citizens in general (political parties – the government, etc.), so that eventually the whole population supports this strategy.

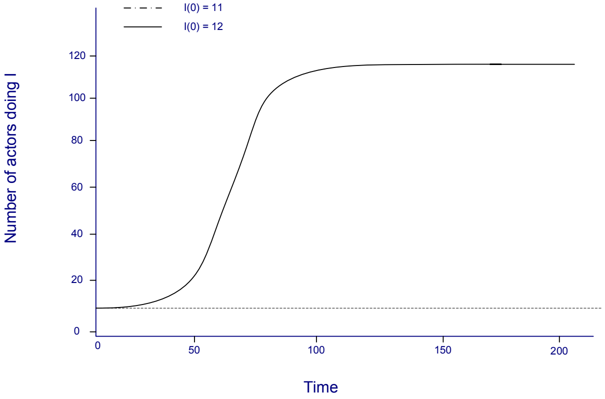


Fig. 2. Social outcomes expected in a structurally undifferentiated setting – Source P. Hedstrom [16]

The trend described above could depict the process by which the citizens empowered by ICT technologies would call political justification into question and demand their involvement in the decision making process. Yet this trend would not inform us about the specific political counter-propositions, nor can this model provide information on the dynamics in the development of such policy producing processes. This process requires collective action and collective action must be precisely specified.

2.2 Web and Collective Action

In a careful study of the current bibliography referring to the relation between the Internet and society, the state and democracy, it appears that this relation is classified in four discrete levels: the relation of the citizen and the state (institutions, policies, governmental procedures), the empowerment of the citizen – Internet user (user empowerment), the rising, dynamic presence of collective movements that flourish on the Internet and the reinforcement of the citizen through state initiatives (e-government, e-learning, etc.). It is usually the case that collective movements are cited, but their dynamic is not included in the procedures for the improvement in the quality of democracy. On the contrary, the results of the actions of collective movements are considered on the one hand, as processes that are derived and justified according to the vested rights of the citizens within the contemporary interpretation of democracy and on the other, they are considered as expressions of protest, although not capable to impose forms and aims of governance.

The history of social movements, as is commonly acknowledged, is traced back to the time that the capitalist system emerged. As Ch. Tilly [30] demonstrates in his research, structural change (economic transformation, urbanization and state expansion) has shaped collective action, not only directly, but also indirectly through the transitions in the form of collective expression in everyday life. Moreover, the reorganization of daily life transformed the nature of conflict and the forms of solidarity (that had been established in the Middle Ages), which after all, bear the most important impact on the structural change of political conflict.

Castells confirms Tilly's position (albeit without any reference to the latter) and develops a similar line of reasoning, stressing that the Internet is not just a useful tool that is used simply because it exists. It fits in with the underlying attributes that distinguish the emerging social movements in the Information Age. These movements found in the Internet the appropriate organizational means with which to build the highways to social change. According to Castells, the Internet has always been the organizational framework of such movements and it therefore cannot be separated from these, just as the industrial plant and the local inn became the organization frameworks for the formation of the labour movement. According to Cohen and Rai [13] the distinction between old and new movements is misleading. Movements such as the labour movement of the industrial age, still exist in our day, redefining themselves according to the social values whose connotations they extend, for example by demanding social justice for all, as opposed to the defense of the interests of a specific class. Cohen and Rai indicate six important social movements that have developed a form of coordination and action on an international scale. These include the movements concerned with human rights, women's rights, the environment, the labour movement, the religious movement and the peace movement. Social movements in the age of the Internet are mobilized essentially in reference to cultural values, so that the efforts to change the codes of meaning in the institutions and the practices of society become the real battle in the process of social change within the new historical context [11].

What needs to be noted is that the discontent of individuals described above, is not automatically transformed into a collective action that proposes policies and raises political demands, but on the contrary it leads to simple abstinence from democratic participation that invalidates political justification and conduces to the political crisis. It virtually reproduces a form of behaviour in citizens that corresponds to their behaviour as consumers that is consumer's usual reaction.

At the same time, the state, as the authority, favours individualistic behavior since it usually does not subvert the state authority. State authority is undermined only when the citizens collectively articulate specific positions regarding the forms and strategies of governance that will yield specific and desirable results. Such positions are generated only by collective movements and collective action. In our day, it stands that the crisis of political justification bears direct impact upon political parties and the bureaucratic syndicate organizations. Castells refers to political parties as empty shells that become active only every four years in view of elections, inevitably becoming increasingly alienated from society. Syndicate organizations are organized according to the old-fashioned model of a vertical hierarchy and for this reason they are falling from grace with society.

The Web however, with the organizational possibilities it provides for communication, information and coordination is gradually replacing these forms, creating the conditions for collective action, which most often springs from the spontaneous coordination of the users and from their initial malcontent. L and C. Tilly [30] defines collective action as the situation where people act together in order to achieve common interests. Olson [25] maintains a similar view. These definitions, although seemingly extremely simple, require complex concepts to understand them, for example the concept of interest. Connolly [14] names these compound concepts "cluster concepts".

In order to comprehend collective action, it needs to be determined in relation to individual action. As is referred by Alexandropoulos [1], very collective action builds upon the existence of an opposite to a separate and clearly defined sphere of individuality, within a discernable field of individual interests that exist independently of collective interests. This position does not coincide with the common idea that the term individual refers to someone who acts alone as an individual, while the term collective refers to someone who cooperates with others to achieve a common goal [1]. The criterion of the common goal does not suffice to define collective action. The space separating individual and collective action, contains the common or combined actions (joint actions), a term coined by Blumer [6,7,8], which refers to common collaborations in daily life (e.g. support of a sports team, a wedding, a company venture, etc.), whose nature and substance are discriminate from collective action. Collective action, on the other hand, refers to particular characteristics, the most important being that it causes a shift in the social structure to which it incurs change.

Today, when technological advances and especially the Web have instigated and set into motion a large number of combined actions by virtue of the communication potential ICT offers (e.g. FACEBOOK, YAHOO, etc.), collective action appears as a derivative of the combination of the new possibilities ICT provides to the individual and the crisis in political justification. Developments progressing at an ever increasing pace, but perceived at a much slower rate, prove that in fact the Internet actually does interact with progressively greater intensity with the socio-political dynamics, so that it is not yet clear, if it is simply a tool for political interaction or on the contrary, it is the reason for transforming the rules of the political game, by transforming the aims and the forms of intervention and action of the politically active. The Internet simultaneously displays conflict and management, the liberty of new movements and supervision, citizen networks and networked individuality, which all reflect on the political level. The perception of democracy as the situation, in which the cooperation of the state and the citizens is only possible exclusively through state initiatives and in the forms of e-government services, tends to ignore this type of dynamic. Social movements with an intense political character are present on the Internet. These movements set political goals, to a greater or to a lesser extent, or in any case, they set goals that oftentimes take on an intense political hue.

Also on the Internet there coexist state supervision, the introversion of the state and the effort to increase its effectiveness in the form of services provided to the citizens and a strong trend in networking among states, either to reinforce their supervision or to deal with universal problems; a dynamic that circumvents older stereotypes in relation to the texture, the mandate and the tendencies of the state. From the above, what should we include and what should we exclude from the concept of democracy in the age of the Internet, as we have perceived it thus far?

The Internet, according to Castells changes the rules of the game, conflict changes societies and politics manages societies.

From this viewpoint three interesting questions arise in relation to the interaction between the Internet and socio-political dynamics.

4. How do we delineate democracy in these new conditions?
5. Does the Internet create a new crisis of political balance or does it intensify an imbalance of a whole political cycle?
6. How can we explore new forms of political balance based on the reality of the Internet?

3 The Limits of Democracy

Recent literature points at the mass changes occurred by the interaction of empowerment dynamics caused by ICT and the changing role of citizen which demands control over his life and improved and efficient governance

European Commission points at the role of e-Government as an enabler for better government, an intrinsic political objective encompassing a series of democratic, economic, social, environmental and governance objectives, which are could be articulated around two major axes namely cost effectiveness and efficiency as well as the creation of public value (European Commission, 2004).

J. Millard (2007) has proposed that these axes should not be seen as independent and equal pillars, but rather as means and ends with the interrelationships that this implies. Therefore public value is the ultimate goal while effectiveness and efficiency are only means to this higher end. According to Millard (2007) public value can be provided by governments. He has identified four overarching ends to which public sector can contribute.

1. Liberal values covering constitutional and subsidiarity structures
2. Democratic values covering citizenship democratic participation through a) representation b) direct engagement
3. Social values covering needs for and responses to socio economic support are determined

4. empowerment values covering how citizens, communities, groups and interests in society can be empowered to further their own as well as collective benefits.

Seang Tae KIM [28] proposes two theoretical models of development and convergence of e- Government and e- democracy.

This process is shown in the following Figures

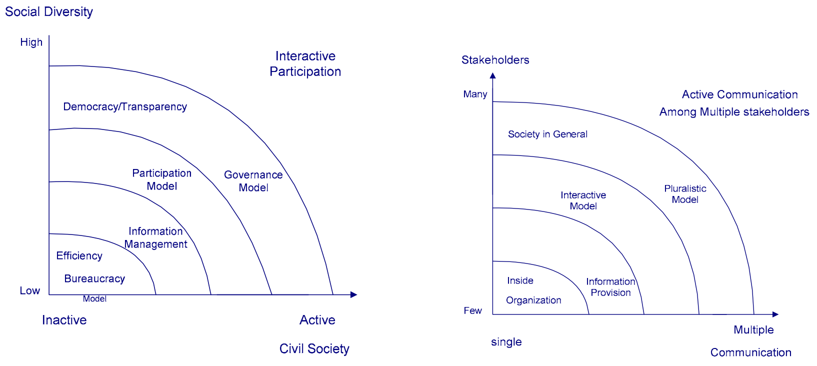


Fig. 3 and 4. Source Seang Tae KIM (2008)

According to Seang Tae KIM the concept and function of e –government has been changed because of advanced technology and social needs. The emergence of citizens as policy decision makers and as the focal point of democracy has brought about the emergence of e- democracy. Current discussions concerning e- government have some limitations in addressing possibility and current change, because they ignore developments of civil society and democracy.

J. Millard remarks the necessity of a widely defined public domain which incorporates public interests, public space, public culture and public sanctuaries, i.e. beyond the existing formalised public sector.

“The public domain is thus seen more and more as wider (possibly much wider) than the public sector, as it also includes and empowers civil society. The old narrow idea of government in which citizens passively receive services and vote every four or five years, and where the state acts on their behalf (government for the people but not by the people) is being challenged by the responsible parent, the informed patient, the active citizen, the dedicated teacher, nurse or local public servant, and by outsourcing to individual volunteers or private companies. Each of these could, with an extension of choice and voice, both individual and collective, be enabled to take greater control over their own lives and the lives of their communities, with or without direct support from the formal democratic and government institutions. We need to decide the extent to which we wish to see such developments take place” [22].

We have entered in a phase where old state practices are strongly challenged and citizens demand direct involvement to social collective and political issues. Accordingly problems are becoming global and complex while Web is transformed from a mean of political facilitation to a context of challenging state’s dominance. In such a context it becomes problematic a prediction of the character and impact of social outcomes to be brought about by social actors.

4 Crisis or Reinforcement of Balance

In the pages of this paper, but also in the bibliography, the significance of the crisis concept is repeatedly revisited. The concept, according to Morin E. [3] refers to a twofold gap: in our knowledge and in the social reality. Morin has processed the significance of crisis in a systemic approach according to which the concept of crisis consists of a constellation of interrelated concepts.

The first suggestive situation and evidence of a crisis is the occurrence of disorder. Usually, the sources of disorder are external but the most interesting cases are those that derive from ostensibly non-disruptive, routes. Often, these processes are revealed as a rapid increase of a variable against other variables. "When we consider, from a systemic point of view those types of processes, we can observe that the boost causes an overcharge phenomenon: the system cannot resolve the problems that used to, under specific limits. It should be able to be reshaped. But, the system cannot comprehend or realize such a reshaping. Or the crisis does originates from a double blind situation, that is double stagnancy where the system is stagnant between two conflicting demands and it is disrupted and finally goes out of control" [3].

Morin argues that under crisis emergence, the systemic operation will be mutated to irregularity, the functionality to a glitch, the continuity to a rupture, the complementarity to a collision. This Morin's version seems to be verified by the aforementioned events. In the following we will focus on two possible disorder signs which may indicate crisis caused by the Web era.

The first sign refers to a latent disruptive process which appears in the Web evolution itself. The Web is considered, until nowadays, an endless innovation process which joins a huge and accelerated amount on information which flows among large populations worldwide. In the current debate about Web, is stated the question if its rapid expansion can be continued smoothly or it will lead to a disorder affecting its functionality. It is argued that considering that the storage of the largest amount of information in the history of human nation, in the context of the biggest computational capacity ever existed, it will be jeopardized from the lack of more intelligent and faster ways of retrieval of information, which can lead to an inflation not supported from its underlying technologies.

A specialization of this argument is the skepticism developed concerning the new intended directives for the semantic Web [29]. It is pointed out that the continuous uploading of content to the Web, begins to create problems in the selection of the desirable content, shifting to the user the uncertainty of selection. "The power of the Web will increase dramatically if the data can be defined and linked in such a way that the machines will overcome the representation layer and will include the combination data beyond the limits of specific applications, organizational and social structures" [29]. For this purpose, an argument of ontology application has been suggested, which retortion argues that liberty and decentralization are better than centrally defined and controlled ontologies. The retortion also mentions as arguments the increase of cost which is implied from the decision of ontology use and the risk of top down absolutist structures, which may the ontologies imply.

The specific example of Web evolution:

a) Confirms Morin's statement that the excessive system expansion incurs disruptive appearances which derive from non-disruptive routes.
b) That every (social) system contains irregularity which, in some degree, is reduced, controlled and managed. But, beyond a specific limit the crisis that, initially, emerges as a disorder incurs a reduction of the capability to apply determinism, which emerges with uncertainty, bottleneck in the reorganization mechanisms and irregularity.

If we transfer this view in the social-political field of the Web, we have to wonder whether the Web simply revealed the crisis of political legalization or, on the contrary, the expansion of Web interactions and the consequent social networking in fact have set in motion this process through the facilitation and empowerment of the user. In this case Web liberated disorder. Since social dynamic is very complex this disorder could be transformed into trend through the gradual formation of social movements which directly challenge policy making. In this case the system has to increase complexity in order to manage error.

5 New Forms of Political Balance

Under the new circumstances, a large number of empirical observations and studies report the strengthening of the mash-users. Furthermore, the citizen's strengthening is becoming more globalized thanks to the Internet, and it is often observed that users originating from different cultures and countries, or even speaking different languages join each other seeking for certain practices to be applied or demanding others to be stopped. For example, a newspaper article [2] reports that: *"… comments and posts on digital walls often go as far as the contents of a meal, teasing among friends, inside jokes among colleagues or the aftermath of a wild night out. Of course there is another side, which is evident in the various actions and initiatives that have sprung from the "book", with causes varying from the Gaza horror and the American Elections to the assassination of Grigoropoulos and last December events in Athens. The massive nature and the momentum of the reactions in these initiatives is so strong, that certain regimes (Syria, Myanmar, Bhutan, and Iran are some of them) choose to lock their citizens out of the electronic home of Facebook*".

Despite the fact that raw suppression does not characterize democratic governments of the modern world, monitoring and suppression is rising in an international level. Also, it is often accompanied by ideological interventions, such as the necessity of increased security against global terror.

The aforementioned Aberg model captures the dynamics of the emergence of behavioural patterns of the user population, but it is not equipped with tools that can be used to record the evolution structure of these events. Societies (modern societies even more) do not feature just persons and a state authority, but are characterized by the dynamics of forming and reforming of groups, according to the notions of the combined actions of Blumer. In a sense, even authority is reflected as such a group, although it is divided in clusters and layers following the actions and the dynamics of the dominant trend, of pressure subgroups or the various political parties e.t.c. A more complicated dynamics determines the diffusion of action from group to group, and the result is always dynamic and constitutes an emergence.

Depending on whether there are consensus circumstances or not, the existence of a stable or unstable equilibrium points, a society of beliefs or deviant beliefs, in other words, whether the society is hot, using Morin (Μωρέν) definition, social interaction takes several forms and directions that sometimes lead to collisions or conflicts (?), and when this happens, group behaviour emerges.

To understand this complex dynamics, we refer to the theory of minorities [4, 23, 24], according to which the notion of "population" does not have a real meaning. The population we usually refer to as a "silent majority" must be considered as a complex mesh (grid?) of social subgroups or other social sub-categories, whose bonds with authority, connecting or opposing, may be more or less powerful, rendering it more or less sensitive to the changes proposed by various sources, and especially minorities.

It is exactly this pattern of social interaction which is captured by an extended version of Aberg's model proposed by Hedstrom [16]. According to Hedstrom the potentially relevant actor to actor network will be difficult to define ex ante and furthermore the causally efficacious network will vary considerably from one time point to another. In situations such as these where the relevant actor to actor networks are unstable and difficult to pin down, it may be better to focus on a type of network that White (1965) referred to as a catnet that is, a network connecting the social categories to which individuals belong. A catnet then describes the relations that exist between such categories.

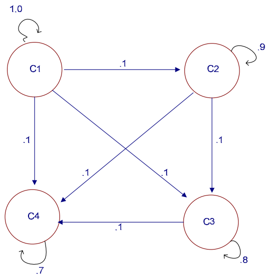


Fig. 5. A catnet – Source P. Hedstrom [16]

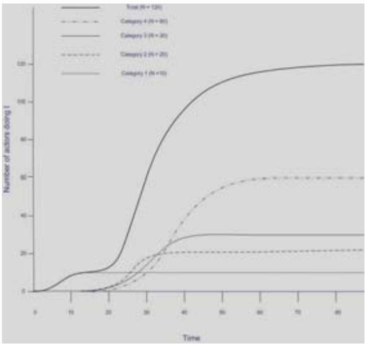


Fig. 6. Social outcomes in a structurally differentiated setting Source P. Hedstrom [16]

The likely influence exerted by members of one category on members of another can be seen as a joint function of

1. how aware members of one category are of what those in other categories do, which partly, but only partly, depends upon the frequency of contacts between the categories
2. The probability that such awareness results in an individual in one category adopting the beliefs, desires and actions of an actor in the other category.

Hedstrom argues that by embedding the Aberg's model into a catnet concept we get a handle on how the group structure is likely to influence the social outcomes actors bring about.

According to the above Figure provided by Hedstron, contrary to Aberg' s structurally undifferentiated setting where an initial proportion of actors was required in order to be observed a coordination of actor's actions, in a differentiated setting no coordination is required. It is sufficient for a single actor in Category 1 to do I for everyone else to end up doing the same.

In order to explore social dynamics under circumstances such as those described above we extended Hedstrom' s model in order to be combined with the model of influence of minorities [23, 24, 26]. In this setting a dominant collective actor (the state) has been modeled as just one form of collectivity which is consistent in that proposes a particular strategy. Besides a minority has been modeled representing a collective actor which tries to propagate an opposed strategy. Both collectivities affect population.

For simplicity we assume four groups (C1 the authority propagating strategy {I}, C2 a minority propagating strategy {S}, C4 a subgroup of the general population which is capable of being informed of both available strategies and is also assumed as more sensitive towards strategy {S} and finally a subgroup C3 which is assumed not perfectly informed about the competitive strategy {S} and therefore traditionally accept both the dominant group (C1) and the suggested dominant strategy {I}. All these groups consist a catnet. We executed a series of simulation experiments where influence rates between groups vary considerably from one case to another. Therefore, influence of groups and the diffusion of strategies from one group to another entail complex social dynamics.

We have summarized the experimental results into three distinct outcomes.

Case 1

1. In this case the particular parameterization concerning influence rates is as follows:

   (a) The dominant group (C1) influences subgroup C3 while the minority (C2) influences subgroup C4.

   (b) C3 influences weakly C1 and C4 influences weakly C2 accordingly.

   (c) There is an influence transmission between C3 and C4. In the first experiment C3 influences C4 while in the second experiment C4 influences C3.

The outcomes are as follows:

1st experiment

The outcomes of experiment 1 show that in this case C3 and C4 groups perceive strategy {I} and there is no ability to the minority group C2 to diffuse its strategy. This outcome derives from the indirect influence of strategy {I} from C3 to C4 group. Outcomes show the gradual domination of strategy {I} and are presented in Figure 7.

2nd experiment

On the contrary in this case influence is assumed to be indirect but it is also assumed to flow the opposite direction, that is, C4 influences C3 and not vice versa. The assumption of a direct influence (C1 influences C3 and C2 influences C4) remain the same as this in experiment 1. In this case the outcomes that social actors bring about are shown in Figure8. Outcomes of this particular setting show that in this case the minority's strategy propagates through population subgroup's indirect influence and becomes the dominant strategy.

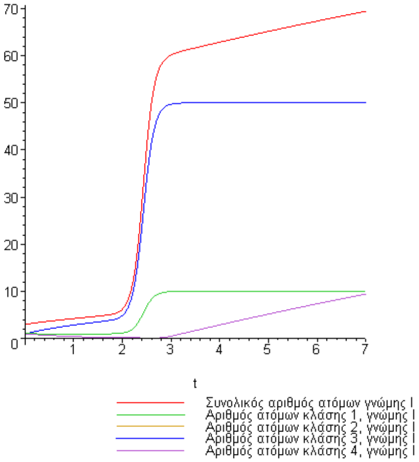


Fig. 7. 1st Experiment indirect influence

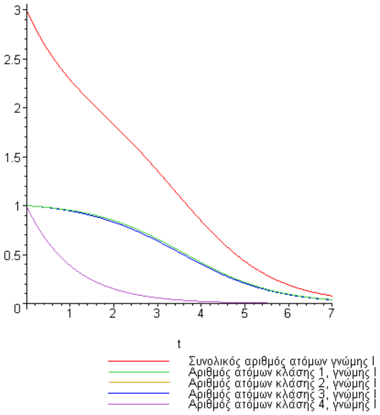


Fig. 8. 2nd experiment indirect influence

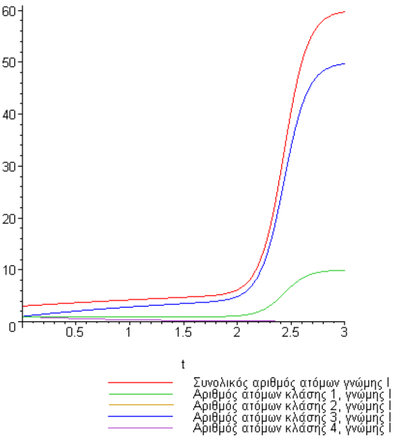


Fig. 9. Emergence of conflict

Case 2

In this case parameterization supports the assumption that social influence is distinguished into two different paths so that C1 influences C3 and C2 influences C4 but no influence dynamics exist between C3 and C4 groups. In this case results show that there is a possibility for locking to a condition of social conflict. Outcomes however, depend upon the tension of influence. In an extreme case two clusters emerge which adopt opposite strategies.

Case 3

In this case we have extend the assumption setting in order to permit influence exchange between groups C1 and C4 while influence rates between groups C3 and C4 hold.

This setting is more consistent to social conditions where groups debate but also coordinate and therefore influence each other. The outcomes of this particular setting shows that both strategies are possible to become dominant depending on the particular values of influence rates. Those outcomes, however, are qualitatively different from those shown in cases 1 and 2 in that, social influence propagates directly between conflicting groups C1 and C2. This influence transmission is more likely to occur through direct bargaining and could therefore entail social consensus.

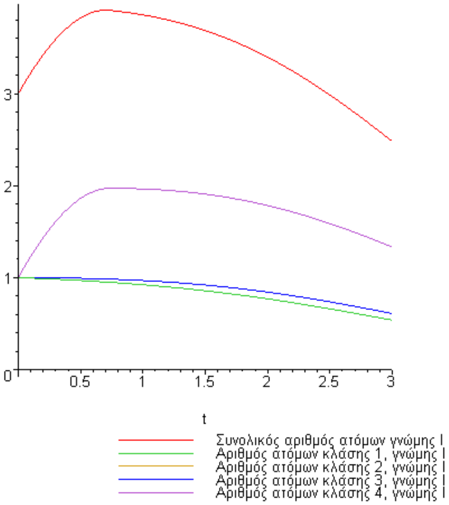


Fig. 10. Influence exchange between conflicting groups

6 Conclusions

Nowadays, Internet is a reality that offers no guarantees by its self that a new political and democratic balance will replace political practices that undergo a legitimation crisis. Therefore, everything is possible.

Only a substantial shift in the stance of the state and the authority, bearing the meaning of acceptance of a widen democracy, will create a new balance that will reflect the new conditions. This shift can occur either cooperatively or through a conflict. In the past, this dreadful dynamics has appeared in the form of conflicts of dynamic movements and destabilization. With each appearance, it caused a generalized crisis leading to the emergence of a new political balance. The struggle that lead to the welfare state is an example of such a dramatic event. Today, the political, social and economic system are put to the test, and on top of that, ICT and the Internet create a new user profile, more educated, up to date and insisting on new values

It is very odd how things seem to repeat, using analogies. J. St. Mill [18, 19, 20, 21], although a supporter of a utilitarian individualist tradition approached group action by dealing with the relationship between the person and the state. This lead to the formation of arguments explaining the reasoning behind the participation of people in groups, collective actions and democratic processes. According to Mill, a rationalist person is motivated to participate in collective actions, in order to protect its own rights by the representatives, the leaders, and others. At the same time, participating in a collective actions acts as an educational process. Mill's position was that citizen participation in the state functions is a necessity. This participation is what ensures that their interests will be served by those appointed to represent them. On the contrary, the presence of passive individuals that abstain from political functions favours the natural tendency of the representatives to represent their own self interests instead of the interests of the people who appointed them. The Web may bring this issue back to our societies.

References

1. Αλεξανδρόπουλος Σγέλις, Θεωρίες για συλλογική δράσηκ αι τα κοινωνικά κινήματα Τόμος Α' Κλασσικές Θεωρίες, Αθήνα Εκδόσεις ΚΡΙΤΙΚΗ (2001)
2. Εφημερίδα το «ΒΗΜagazino» 15/2/2009 σελ, pp. 36–39 (2009)
3. Edgar, M.: Κοινωνιολογία, Αθήνα Εκδόσεις του ΕΙΚΟΣΤΟΥ ΠΡΩΤΟΥ (1998)
4. Παπαστάμον Σ. και. Γκ. Μιούνν, Μειονότητες και Εξονσία: Μιακοινωνιοψνχολογική κι πειραματική προσέγγιση της κοινωνικής επιρροής καισνμπεριΦοράς των μειονοτήτων Αθηνα (1983)
5. Aberg, Y.: Individula Social Action and Macro Level Dynamics: A Formal Theoretical Model. Acta Sociologica 43, 193–205 (2000)
6. Herbert, B.: Theory of Social Revolutions, M.A. thesis Missuri University (1922) (unpublished)
7. Herbert, B.: Social Disorganization and Individual Disorganization. American Journal of Sociology 42, 871–877 (1936-1937)
8. Herbert, B.: Collective behavior. In: Park, R.E. (ed.) An Outline of the Principles of Sociology, N.Y. Barnes and Noble, pp. 219–280 (1939)
9. Buedieu, P.: L'opinion publique n' existe pas. Temps modernes 29(318), 1292–1309 (1973)
10. David, B.: WP 2009-2010: Objectives of the consultation and state of play in "ICT for Governance and Policy Modelling Consultation Workshop (draft report) (2008)
11. Manuel, C.: The Power of Identity. Blackwell, Oxford (1997)

12. Castels, M.: The Internet Galaxy (Reflections on the Internet, Business and Society). Oxford University Press, Oxford (2001)
13. Cohen, R., Rai, S.M.: Global Social Movements. The Athlone Press, London (2000)
14. Connoly, W.E.: The Terms of Political Discourse. Martin Robertson, Oxford (1983)
15. Centeno, C., van Bavel, R., Burgelman, J.B.: European Commission: e-Government in the EU in the next decade: vision and key challenges, Final draft version, DG JRC, Institute for Prospective Technological Studies, Sevilla Spain (August 2004)
16. Peter, H.: Dissecting the Social: On the principles of Analytical Sociology. Cambridge University Press, Cambridge (2005)
17. Rose, J. (2006), `http://www.egov.aau.dk/`
18. Stuart, M.J.: Utilitarianism, Liberty and Repressive Government. J. M. Dent, London (1950)
19. Stuart, M.J.: “On Liberty”. In: Robson, J. (ed.) Collected Works of John Stuart Mill, Toronto, vol. 18, pp. 203–310 (1977a)
20. Stuart, M.J.: Considerations on Representative Government. In: Collected Works, Essays on Politics and Society. University of Toronto Press, Routledge & Kegan Paul, Toronto – London (1977b)
21. Stuart, M.J.: Chapters on Socialism. In: Collini, S. (ed.) On Liberty and other writings. Cambridge University Press, Cambridge (1989)
22. Jeremy, M.: Danish Technological Institute, e-Governance and e-Participation: lessons from Europe in promoting inclusion and empowerment (2007)
23. Mocovici, S., Lage, E., Naffrechoux, M.: Influence of a consistent minority on the responses of a majority in a color perception task. Sociometry 32, 365–379 (1969)
24. Mocovici, S., Personnaz, B.: Studies in social influence, V. Minority influence and conversion behavior in a perceprual ask. Journal of experimental social psychology 16, 270–282 (1980)
25. Mancur, O.: The Logic of Collective Action, Public Goods and the Theory of Groups. Harvard University Press, Cambridge (1965)
26. Papastamou, S.: Strategies d’ influence minoritaires et majoritaires. These de doctorat, roneo (1979)
27. Panopoulou, E., Tambouris, E., Tarabanis, K.: European e-Participation —Study and supply of sevices on the development of e-Participation in the EU, eParticipation good practice cases Deliverable D4.2b second version (2008)
28. Kim, S.-T.: Converging E-Democracy and E-Government Model toward an Evolutionary Model of E-Governance: The Case of South Korea (2008)
29. Lee, T.B., et al.: «το πλαίσιο της επιστήμης του Web: Η νέα επιστήμη από τον εφευρέτη του www», Αθήνα εκδόσεις hyperconsult (2007)
30. Charles, T.: From Mobilization to Revolution. Addison-Wesley, Chicago (1978)
31. Louise, T., Charles, T.: Class Conflict and Collective Action. Sage, London (1981)

Using Structured e-Forum to Support the Legislation Formation Process

Alexandros Xenakis[1] and Euripides Loukis[2]

[1] Panteion University, Athens
Department of Psychology
a.xenakis@panteion.gr
[2] University of the Aegean, Samos
Department of Information and Communication Systems Engineering
eloukis@aegean.gr

Abstract. Many public policy problems are 'wicked', being characterised by high complexity, many heterogeneous views and conflicts among various stakeholders, and also lack of mathematically 'optimal' solutions and pre-defined algorithms for calculating them. The best approach for addressing such problems is through consultation and argumentation among stakeholders. The e-participation research has investigated and suggested several ICT tools for this purpose, such as e-forum, e-petition and e-community tools. This paper investigates the use of an advanced ICT tool, the structured e-forum, for addressing such wicked problems associated with the legislation formation. For this purpose we designed, implemented and evaluated two pilot e-consultations on legislation under formation in the Parliaments of Austria and Greece using a structured e-forum tool based on the Issue Based Information Systems (IBIS) framework. The conclusions drawn reveal the advantages offered by the structured e-forum, but also its difficulties as well.

Keywords: e-participation, e-consultation, public policy, structured e-forum, Issue Based Information Systems (IBIS).

1 Introduction

The high diffusion of ICT, and particularly the Internet, which offer new interactive, cheap, inclusive and unconstrained by time and distance environments for public political communication, and at the same time the trend towards more participation of citizens in the processes of public decision-making and policy-making, have been the main drivers of the emergence and development of e-participation [1], [2], [3], [4]. Electronic participation (or e-participation) is defined as the extension and transformation of participation in societal democratic and consultative processes mediated by information and communication technologies (ICT) [2], [3], [4]. As local, regional and national governments of many OECD member countries try to extend citizens participation with the provision of additional effective channels of communication with civil society based on innovative usage of ICT, several different tools have been

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 29–40, 2010.

researched, deployed and tested for this purpose, such as e-forum, e-petition and e-community tools [3] - [7].

However, limited research and use has been made of more structured ICT tools for this purpose, such as the structured discussion e-forum. The structured e-forum tool allows participants to enter in an electronic discussion semantically annotated postings, or postings on other participants' postings, based on a predefined discussion ontology [8], [9]. This paper investigates the use of an advanced ICT tool, the structured e-forum, for addressing such wicked problems associated with the legislation formation process. For this purpose we designed, implemented and evaluated two pilot e-consultations on legislation under formation in the Parliaments of Austria and Greece using a structured e-forum tool based on the Issue Based Information Systems (IBIS) framework [10] – [12]. The research presented in this paper has been part of the LEX-IS project ('Enabling Participation of the Youth in the Public Debate of Legislation among Parliaments, Citizens and Businesses in the European Union') (www.lex-is.eu) of the 'eParticipation' Preparatory Action of the European Commission [13].

This paper consists of six sections. In section 2 the background is briefly described, while in section 3 we present the research methodology we adopted. Then in sections 4 and 5 we presented the evaluation results for the abovementioned two pilots we implemented. Finally in section 6 we suggest a set of combined conclusions drawn from the collective experience of the two cases presented.

2 Background

Rittel & Weber [14] proposed a classification of problems into 'wicked' and 'tame' ones. The wicked problems are the most difficult to address, since they are characterised by many stakeholders with different and heterogeneous problem views, values and concerns, and also lack mathematically 'optimal' solutions and pre-defined algorithms for calculating them, having only 'better' and 'worse' solutions, the former having more positive arguments in favour them than the latter. Kunz and Rittel [10] suggest that wicked problems are most effectively addressed through consultation and argumentation among stakeholders, and propose for this purpose the use of 'Issue Based Information Systems' (IBIS), which aim to '*stimulate a more scrutinized style of reasoning which more explicitly reveals the arguments. It should help identify the proper questions, to develop the scope of positions in response to them, and assist in generating dispute'*. They are based on a simple but powerful discussion ontology, whose main elements are 'questions' (issues-problems to be addressed), 'ideas' (possible answers-solutions to questions-problems) and 'arguments' (evidence or viewpoints that support or object to ideas) [10] - [12].

Many public policy problems belong to the class of wicked problems, being characterised by high complexity, many heterogeneous views and conflicts among various stakeholders. Therefore the best approach for addressing them is through consultation and argumentation among the stakeholders, using ICT to the largest possible extent. Based on the relevant literature [10] – [12], [14], the most appropriate kind of ICT tools for this purpose would be structured ones according to the abovementioned IBIS framework. However, the tools which have been researched and used for this purpose, such as e-forum, e-petition and e-community tools, are characterised by low structure.

For, instance most of the political e-consultations on public policy problems are conducted in e-forum environments, which allow participants to enter postings, or postings on other participants' postings, without any semantic annotation or structure. This might reduce the quality, discipline, focus and effectiveness of the e-consultations.

On the contrary, a structured e-forum tool based on the IBIS framework and require from the participants to make semantic annotations of their postings in an electronic discussion. The type of allowed semantic notations are predefined, based on the adopted discussion ontology, e.g. in case of adopting IBIS allowing the entry of a new 'issue', the suggestion of an 'alternative' or simply a 'comment' on an existing issue, or the entry of a 'pro' or a 'contra' argument on a previously suggested alternative. Therefore the participants themselves have to annotate their postings with a semantic that properly represents the content of their text entries the forum. Also they have to associate their postings to other participants' postings according to rules defined in the adopted discussion ontology, e.g. in case of having adopted IBIS we can associate an 'alternative' only to an 'issue', but not to a 'pro' or a 'contra' argument. This sequence of semantically annotated postings creates threads of in depth discussions which are more convenient to be tracked, analysed in a formal manner and subsequently evaluated in order to draw useful conclusions. The above characteristics of the structured e-forum tool might have a positive impact on the quality, discipline, focus and effectiveness of the e-consultations. For this reasons it is important to examine its suitability, advantages and disadvantages as an e-participation tool for supporting e-consultations on wicked public policy problems. However, to this date there has been conducted very little research work in this area [8], [9]. Our research aims to contribute to filling this research gap.

3 Research Methodology

In order to investigate the use of structured e-forum for addressing wicked problems associated with the legislation formation process, through structured e-consultations among stakeholders, we adopted the following methodology:

I. Initially we analyzed the process of legislation formulation in the Parliaments of Austria and Greece, which were participating in the LEX-IS project.

II. Based on this analysis, we designed two pilot e-consultations on legislation under formation in these two Parliaments using structured e-forum. This included definitions of the bills to be discussed, the participants, the discussion ontology, the timing of the discussion and also the informative material to be provided to the participants). Concerning the discussion ontology it was decided in most of the threads to use the one of IBIS: issue-alternative (or comments) – pro or contra argument (termed 'structured forum I'); also, in some threads to use a simpler one for comparison purposes: question – answer – comment (termed 'structured forum II').

III. As a next step we proceeded to the implementation of the pilot e-consultations.

IV. Finally we evaluated the two pilots using both quantitative and qualitative methods. In particular, the evaluation of each pilot included four stages:

i) Analysis of the discussion trees that had been formed by the postings of the participants. This analysis included the calculation of the following metrics:

- number of postings entered by the participants per thread,
- number of postings per type, for each the allowed types (i.e. for 'structure forum I' e-discussions: key issues, comments, alternatives, pro-arguments, contra-arguments, while for 'structure forum II' e-discussions: Questions, answers, comments),
- number of postings per level of the discussion trees
- percentage of the postings assigned a mistaken type

ii) Quantitative Evaluation, based on the statistical processing of participants' responses to an evaluation questionnaire we formulated and distributed electronically to them, which allows the assessments of:

- the perceived ease of use
- and the usefulness of the structured e-forum,
  adopting a 'Technology Acceptance Model' (TAM) approach [15].

iii) Qualitative Evaluation, based on semi-structured focus-group discussions with participants and representatives of the Parliaments, which allows as well assessments and in-depth understanding of the perceived ease of use and usefulness of the structured e-forum, and the corresponding.

iv) Synthesis of the conclusions from the above three stages and final conclusions.

4 The Austrian Parliament Pilot

The Austrian pilot concerned a ministerial draft bill titled "Child and Youth Welfare Law"; it reached a high number of participants (120 registered users – mainly high school pupils), who entered 253 postings, and made 12618 visits in the e-participation platform. This draft bill has been discussed in ten threads.

Analysis of the discussion trees. In six threads the IBIS discussion ontology was used, while in the remaining ones was used the abovementioned simpler one. Table 1 shows the numbers of postings per type and in total for each discussion thread. We can see that the forums of type I, though the a more complicated discussion ontology, were used more intensively than the forums of type II. However, we remark that the difficulty of assigning to each comment the correct type lead to the large number of "comments", i.e. many participants decided to choose the "comment" instead of pro- and contra-arguments or questions and answers (overall 55% of all postings were comments, 40% from forum type I and 15% from forum type II); we can see that in the threads "Eingriff in die privaten Lebensbereiche", "Junge Erwachsene", and "Rechtsansprüche" participants used almost only comments to express their opinion. This indicates that while the structured e-forum tool imposes more structure in the e-discussion, these young participants (mainly high school pupils) tend to less structure.

Table 1. Postings per type for each forum thread

	Forum type 1					Forum type 2			
forum/entry	Issue	Alternative	Pro argument	Contra argument	Comment	Question	Answer	Comment	Total
Verwandtenpflege §21	3	5	40	29	18	0	0	0	95
Recht auf Erziehung §1	1	3	3	2	28	0	0	0	37
Rechtsansprüche	0	0	0	0	0	2	1	13	16
Datenverwendung §40	0	0	0	0	0	2	2	8	12
Eingriff in die privaten Lebensbereiche	2	1	0	0	49	0	0	0	52
Junge Erwachsene §29	0	0	0	0	0	2	0	11	13
§35(2)4	0	0	0	0	0	2	2	4	8
Aufgaben der Kinder und- Jugendhilfe §3	0	0	0	0	0	1	0	1	2
Kündigung von Pflegeverhältnissen §19(6)	0	0	0	0	0	0	0	0	0
Stellungnahmen	7	3	1	0	7	0	0	0	18
Total	13	12	44	31	102	9	5	37	253
Total %	5%	5%	17%	12%	40%	4%	2%	15%	100%

In Table 2 we can see for each thread the percentage of total postings and pupils' postings which have been assigned a mistaken type; we remark that in some threads this percentage is very high. The main reason for this is that, as explained above, many participants have simply chosen the entry type 'comment' instead of 'answer' (in forum type II) or 'alternative' (in forum type I); in some other cases type 'comment' was used instead of 'pro' or 'contra argument'. These mistakes appeared mainly in discussion threads with a bigger depth. One reason for these mistakes can be the complexity and bad readability of the threads, which increases with depth. We estimated that 16 of the 'comments' entered should have been 'answers', 65 should have been 'pro' or 'contra arguments' and 7 should have been 'alternatives'. Another reason can be that when there is a sequence of 'pro' and 'contra arguments', the participants finally do not know whether to use a 'pro' or a 'contra argument' to make their statement clear. We estimate about 11 mistakes of choosing 'pro' instead of 'contra argument' or the opposite.

Table 2. Percentage of postings assigned a mistaken type for each forum thread

forum/entry	total entries	user entries	mistakenly chosen entry types	mistakenly chosen entry types out of total entries	mistakenly chosen entry types out of user entries
Verwandtenpflege §21	95	93	21	22,1%	22,6%
Recht auf Erziehung §1	37	36	22	59,5%	61,1%
Rechtsansprüche	16	14	5	31,3%	35,7%
Datenverwendung §40	12	9	2	16,7%	22,2%
Eingriff in die privaten Lebensbereiche	52	51	40	76,9%	78,4%
Junge Erwachsene §29	13	11	9	69,2%	81,8%
§35(2)4	8	6	1	12,5%	16,7%
Aufgaben der Kinder und- Jugendhilfe §3	2	1	0	0,0%	0,0%
Kündigung von Pflegeverhältnissen §19(6)	0	0	0	-	-
Stellungnahmen	18	9	2	11,1%	22,2%

Finally we examined and compared the depths of the discussion threads. In general a discussion with a higher depth means higher interaction among the participants. Table 3 shows for all threads the number of entries per level. We remark that discussions in the threads of forum type I (e.g. the first, second and fifth ones) reached a higher depth than the ones of type II. This can be explained taking into account the bigger interaction that the usage of 'pro' and 'contra arguments' creates. However, on the one hand these argument types improve the interactive discussions among the participants, but on the other hand this results in a number of simplistic posts containing only "I agree" or "I disagree" (mainly in forum type I threads). This problem may be reduced through the provision to the user of a 'rating' capability, enabling him/her to state 'agree' or 'disagree' on a previous entry, without having to enter one more entry for this.

Table 3. Number of postings per level for each forum thread

forum/entry	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8
Verwandtenpflege §21	3	13	25	14	17	13	7	3
Recht auf Erziehung §1	1	7	14	12	3	0	0	0
Rechtsansprüche	2	3	4	5	1	1	0	0
Datenverwendung §40	2	4	5	1	0	0	0	0
Eingriff in die privaten Lebensbereiche	1	4	14	22	8	3	0	0
Junge Erwachsene §29	2	9	2	0	0	0	0	0
§35(2)4	2	3	1	1	1	0	0	0
Aufgaben der Kinder und- Jugendhilfe §3	1	1	0	0	0	0	0	0
Kündigung von Pflegeverhältnissen §19(6)	0	0	0	0	0	0	0	0
Stellungnahmen	7	9	2	0	0	0	0	0

Quantitative analysis. A quantitative evaluation questionnaire was returned by 37 out of the 120 registered participants in this e-participation pilot (31% response rate). In Table 4 are shown the average ratings for the structured e-forum evaluation questions. The participants of the Austrian pilot found the structured forum on average between difficult to medium and medium to easy (nearer to the latter - AvR: 2.69) and similarly they evaluated the easiness to access, read and understand the posting of other participants (AvR: 2.76). The structured forum proved is perceived by them on average between slightly worse and slightly better than the normal forum tools (nearer to the latter - AvR: 2.68). Overall most of the participants found that the platform provides proper participation tools and structuring mechanisms to engage in online discussions on such topics (AvR: 1.89), and that the quality of contributions of other participants was on average between low to medium and medium to high (nearer to the latter - AvR: 2.63).

Qualitative analysis. In semi-structured focus-group discussions with participants and representatives of the Austrian Parliament one of the topics was whether it was easy to use the structured e-forum, which are the main difficulties of using it and which are the main advantages it offers. They mentioned that it was not too difficult to assign the right type in a new posting, since all predefined posting types were clear, but this requires additional mental effort; the same happens with finding the right

Table 4. Average ratings of the Austrian pilot respondents in the structured e-forum evaluation questions

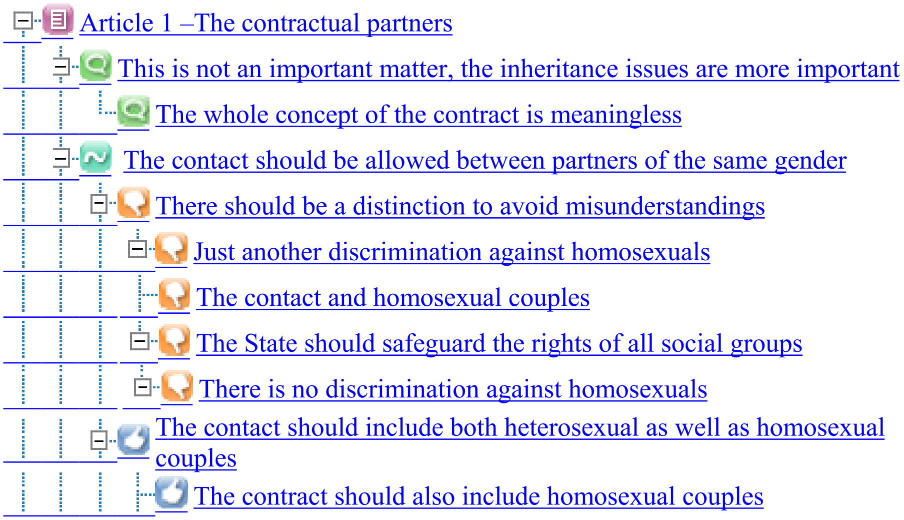
QUESTION	AVERAGE RATING
How easy it was to use the structured forum (i.e. to correctly characterize your idea as an issue, an alternative, a pro-argument, a contra-argument, or a comment, and then correctly enter it in the structured forum)? 1=difficult, 2= difficult to medium, 3= medium to easy, 4=easy	2.69
How easy it was to access, read and understand the postings of the other participants and the connections among them in the structured forum? 1=difficult, 2=medium to difficult, 3=easy to medium, 4=easy	2.76
What is your general assessment of the structured forum as a tool for important e-consultations in comparison to the normal forum tools (where you do not have to characterize your posting as an issue, an alternative, a pro-argument, a contra-argument, or a comment, and then enter it correctly)? 1=much worse, 2= slightly worse, 3=slightly better, 4=much better	2.68
Does the platform provide proper participation tools and structuring mechanisms to engage in the online discussion of the topics? 1=no, 2=yes	1.89
How do you assess the quality of the contributions (postings) entered by the participants in this e-consultation? 1=low, 2= low to medium, 3= medium to high, 4=high	2.63

place to add the new posting. Young participants are more ‘spontaneous’ and do not think much about their statement before entering it; they just choose one possible and reasonable posting type (e.g. ‘comment’) and start writing it, and do not mind if it can be a ‘pro’ or ‘contra statement’, an ‘alternative’ or an ‘answer’. Also, participants could be afraid of writing an ‘alternative’ or ‘answer’, finding then as more ‘high profile’ types and thinking that the text they need to write should be of very good quality and grammatically correct; the fear of too much ‘attention’ is a reason for avoiding to use alternatives and answers. The main advantage mentioned was the better overview provided on the meanings of participants’ postings through the icons in front of each. In general the usage of the structured forum was satisfactory, but some participants found it hard to follow a discussion in threads with a higher depth.

Synthetic Conclusions. From the above three evaluation stages it is concluded that the structured e-forum seems to be ‘medium’ as to its ease of use to these young and non-sophisticated participants, because it creates to them some difficulties, e.g. in finding the right place to add a new posting and selecting its type, since they require additional mental effort. These difficulties, in combination to the ‘spontaneity’ of this age and the fear of too much ‘attention’, results in the mistaken selection of ‘lower profile’ types (e.g. ‘comments’) instead of ‘higher profile’ ones (e.g. ‘alternatives’ or answers’). Concerning its usefulness these young and non-sophisticated participants find that the structured e-forum, in comparison with the simple forum, offers some advantages, but they do not perceive them as very high and important.

5 The Greek Parliament Pilot

The Greek pilot concerned the law on ‘Contracts of Voluntary Cohabitation’; it reached a number of 79 registered users, which contributed 131 postings on this highly debated topic in Greece, and made 4192 visits in the platform. A partial length image of the discussion tree of the Greek pilot is provided hereafter in Figure 1, which shows some of the postings entered by the participants (in Greek).



- Article 1 –The contractual partners
  - This is not an important matter, the inheritance issues are more important
    - The whole concept of the contract is meaningless
  - The contact should be allowed between partners of the same gender
    - There should be a distinction to avoid misunderstandings
      - Just another discrimination against homosexuals
        - The contact and homosexual couples
      - The State should safeguard the rights of all social groups
      - There is no discrimination against homosexuals
    - The contact should include both heterosexual as well as homosexual couples
      - The contract should also include homosexual couples

Fig. 1. Greek Forum Overview

Analysis of the discussion tree. In total 131 postings have been entered by the participants in the Greek pilot. Initially we calculated the number of postings per type and found that we had 8 ‘issues’, 13 ‘comments’, 15 suggested ‘alternatives’, 35 ‘pro-arguments’, and 60 ‘con-arguments’; we did not have the excessive use of ‘comments’ we saw in the Austrian pilot. We remarked that a good and balanced discussion tree has been formed, with the expected structure from a well-developed electronic discussion: with several new issues (8) entered by the participants on the root topic (=the law on the ‘Contract of Voluntary Co-habitation’), a higher number of alternatives (suggestions) (15) and a similar number of comments (13) on these issues, and also a much higher number of pro-arguments (35) and con-arguments (60). These results indicate that a structurally well-developed electronic discussion. Next we calculated the percentages of the simplistic postings (=not adding value/new information), and found only 8, which make a 6% of the total number of postings. As a next step we calculated the number of postings with mistaken type, and found 13 such postings, which makes a 10% of the total number of postings, much lower than in the Austrian pilot. Finally, in order to assess the level of depth of this electronic discussion, we calculated the number of postings per level, and found 8 first level postings, 24 second level postings, 38 third level postings, 27 fourth level postings, 20 postings of fifth level, 13 sixth level postings and finally one 1 seventh level posting. Therefore it can be concluded that the electronic discussion of the Greek pilot was characterized by considerable depth and interaction among the participants.

Quantitative Analysis. A quantitative evaluation questionnaire was returned by 27 out of the 79 registered participants in this e-participation pilot (34% response rate). In Table 5 we can see the average ratings for the structured e-forum evaluation questions. The participants of the Greek pilot on average found the structured forum as medium to easy (AvR: 2.92), and also believe that it is between difficult to medium and medium to easy (nearer to the latter - AvR: 2.76) to access, read and understand the posting of other participants. The structured forum proved is perceived by them on average between slightly better and much better than the normal forum tools (nearer to the latter - AvR: 3.56). Overall most of the participants found that the platform provides proper participation tools and structuring mechanisms to engage in online discussions on such topics (AvR: 1.88), and that the quality of contributions of other participants was high to medium (AvR: 3.08).

Table 5. Average ratings of the respondents in quantitative evaluation questions for the Greek pilot

QUESTION	AVERAGE RATING
How easy it was to use the structured forum (i.e. to correctly characterize your idea as an issue, an alternative, a pro-argument, a contra-argument, or a comment, and then correctly enter it in the structured forum)? 1=difficult, 2= difficult to medium, 3= medium to easy, 4=easy	2.92
How easy it was to access, read and understand the postings of the other participants and the connections among them in the structured forum? 1=difficult, 2= difficult to medium, 3= medium to easy, 4=easy	2.76
What is your general assessment of the structured forum as a tool for important e-consultations in comparison to the normal forum tools (where you do not have to characterize your posting as an issue, an alternative, a pro-argument, a contra-argument, or a comment, and then enter it correctly)? 1=much worse, 2= slightly worse, 3=slightly better, 4=much better	3.56
Does the platform provide proper participation tools and structuring mechanisms to engage in the online discussion of the topics? 1=no, 2=yes	1.88
How do you assess the quality of the contributions (postings) entered by the participants in this e-consultation? 1=low, 2= low to medium, 3= medium to high, 4=high	3.08

Qualitative Analysis. In a semi-structured focus-group discussion we conducted with participants and representatives of the Greek Parliament one of the topics was whether it was easy to use the structured e-forum, and also its main advantages and disadvantages. They mentioned that overall the use of the structured e-forum was considered a strength of the pilot, since it enables a more focused and effective e-discussion. Also, the semantic capability it offers allows users to quickly form an opinion as to the progress of the discussion on a particular key issue of interest. Most of the difficulties mentioned during this discussion had more to do with the design implementation of the structured e-forum rather than the concept of the structured forum itself. One of them was the difficulty of correct assignment of type to the postings; this is confirmed by the percentage of mistakes in this pilot, which was about 10% as mentioned in the analysis of the discussion tree, being lower than in the Austrian pilot, due to the relatively higher educational level of the participants in the Greek pilot, but not negligible. Another difficulty in using the structured e-forum was wording the title of each posting, which is directly shown in the discussion tree of the structured forum box (while the full description of the posting is shown in another box only by clicking its title in the tree), so that it reflects the content of the posting. In several cases the title was not representative of the explanation of the full argument presented in this separate fill-in description box provided, so the other participants could not understand from the title the content of the posting. Another problem mentioned was due to the moderation of the postings: from the time one posting was entered by a user it usually took 5-6 hours until the moderator approved it and the posting became visible; so it was not possible for this user to see it immediately, and possibly enter more postings associated with it, while the other users could see it with such a long delay. Also, it was mentioned that the platform provides a very small space (box) for the structured e-forum, so the users have to use much scrolling up and down when trying to access previous participants' postings. Another design weakness mentioned is that the structured forum was placed four levels below the homepage of the platform, and this created difficulties for the users to access it.

Synthetic Conclusions. From the above three evaluation stages encouraging conclusions are drawn concerning the potential of using structured e-forum in the legislation process. The participants in the Greek pilot regard the structured e-forum platform as medium to easy to use, though they mention some difficulties they had in using it, and some design weaknesses that have to be addressed. Concerning its usefulness, these more educated and non-sophisticated participants, in comparison to the ones of the Austrian pilot, find that the structured e-forum, is better than the simple forum, enabling a more focused and effective electronic discussion.

6 Conclusions

In the previous sections of this paper has been investigated the use of structured e-forum for e-consultations on 'wicked' public policy problems associated with the legislation formation. It has been concluded that for the older, more educated and sophisticated participants of the Greek pilot the structured e-forum is better than the simple forum, offering important advantages and enabling a more focused and effective electronic discussion. Different are the perceptions of the younger and less educated and sophisticated participants of the Austrian pilot, who find that it offers some advantages in comparison with the simple forum, but they do not perceive them as very high and important. The participants in the Greek pilot regard the structured e-forum as medium to easy to use, while the ones of the Austrian pilot seem to perceive higher level of difficulties, regarding it 'medium' as to its ease of use. However, both groups find that it requires some additional mental effort from the users than the simple forum. In both pilots the extent of use of the platform by the participants (visits and postings) was satisfactory, and the majority of the participants were rather satisfied by their co-participants and their contributions. Therefore we can conclude that the structured e-forum is a better solution for more sophisticated and knowledgeable discussion groups, while larger and less sophisticated and coherent groups could be best served by the traditional forum tools. So Parliaments could organize e-consultations with the wider public using simple forum, and also with the more sophisticated experts on the laws under discussion using structured e-forum.

References

1. Coleman, S., Gotze, J.: Bowling together: Online public engagement in policy delibaration (2002), http://bowlingtogether.net
2. Saebo, O., Rose, J., Flak, L.S.: The shape of eParticipation: Characterizing an emerging research area. Government Information Quarterly 25, 400–428 (2008)
3. Organization for Economic Co-operation & Development – OECD, Engaging Citizens Online for Better Policy-making, Policy Brief. OECD, Paris (2003)
4. Organization for Economic Co-operation & Development – OECD, Promise and Problems of e-Democracy: Challenges of Online Citizen Engagement. OECD, Paris (2004)
5. Whyte, A., Macintosh, A.: Analysis and Evaluation of E-Consultations. e-Service Journal 2(1), 9–34 (2003)
6. Macintosh, A., Malina, A., Whyte, A.: Designing E-Participation in Scotland. Communications 27, 261–278 (2002)
7. Macintosh, A.: Characterizing E-Participation in Policy Making. In: Proceedings of the 37th Hawaii International Conference on System Sciences (2004)
8. Karacapilidis, N., Papadias, D.: Computer Supported Argumentation and Collaborative Decision Making: The HERMES system. Information Systems 26(4), 259–277 (2001)
9. Karacapilidis, N., Loukis, E., Dimopoulos, S.: Computer-supported G2G collaboration for public policy and decision making. Journal of Enterprise Information Management 18(5), 602–624 (2005)
10. Kunz, W., Rittel, H.: Issues as Elements of Information Systems, Working Paper No. 131, California, Berkley (1979)
11. Conklin, J., Begeman, M.: gIBIS: A tool for all reasons. Journal of the American Society for Information Science 40(3), 200–213 (1989)

12. Conklin, J.: Dialog Mapping: Reflections on an Industrial Strength Case Study. In: Kirschner, P., Buckingham Shum, S., Carr, C. (eds.) Visualizing Argumentation: Software Tools for Collaborative and Educational Sense-Making. Springer, London (2003)
13. Loukis, E., Wimmer, M., Triantafillou, A., Gatautis, R., Charalabidis, Y.: Electronic support of participation in the development of legislation: the LEX-IS project. In: 5th Eastern European eGov Days 2007, Prague, Czech Republic, April 11-13 (2007)
14. Rittel, H.W.J., Weber, M.M.: Dilemmas in a general theory of planning. Policy Sciences 4, 155–169 (1973)
15. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly 13(3), 319–340 (1989)

Session 2

Enhancing Quality of Life through e-Services

From the Digital Divide to Digital Inequality: A Secondary Research in the European Union

Emmanouil Stiakakis, Pavlos Kariotellis, and Maria Vlachopoulou

University of Macedonia
{Stiakakis,mavla}@uom.gr, kariotellisp@gmail.com

Abstract. The digital divide is nowadays evolving to digital inequality, i.e., the socio-economic disparities inside the 'online population'. This paper examines two main dimensions of the digital inequality, namely 'skills' and 'autonomy' of Internet users. The level of formal education was selected as a representative variable of the skill dimension, as well as the density of population in different geographical areas as a representative variable of the autonomy dimension. The research was focused on the member states of the European Union (EU). The data, provided by Eurostat, included the daily use of computers for the last three months and the average use of the Internet at least once per week. The findings state that the EU already faces the problem of digital inequality to an extended rate, since there are significant disparities among the European countries with regard to the aforementioned variables.

Keywords: Digital divide, digital inequality, digital disparity, ICT.

1 Introduction

During the last decades the use of Information and Communication Technologies (ICTs) has become the key factor for the social and economic development of every country. The advent of World Wide Web has significantly contributed to the diffusion of ICTs, mostly due to the rapid information exchange. Everyday life changes occur in terms of communication, entertainment, learning, shopping, etc. People join into processes that alter not only many aspects of their lives but themselves, too. Moreover, the diffusion of ICTs among firms is widely considered to be one of the primary factors behind their economic growth. E-marketing activities, online sales, as well as work flow automation and resource planning have been fostered considerably. Even though a widespread technology boom is being witnessed, with innovative services and applications able to be rapidly spread through the Internet, the adoption of ICTs is distributed unevenly. It is a fact that, different groups of people are more or less privileged in accessing and using technology. This technological gap is called digital divide. As information revolution spreads rapidly the notion of digital divide becomes even more substantial and therefore gains an increased interest for observation from researchers and policy makers. Moreover, a discussion and debate about the definition and the empirical analysis of its components is on the way.

According to the literature, many attempts to accurately define the notion of the digital divide have been made. The definition, given by the Organization for Economic

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 43–54, 2010.

Co-operation and Development (OECD), refers to the digital divide as the '*gap between individuals, households, businesses, and geographical areas at different socioeconomic levels with regard both to their opportunities to access ICTs and their use of the Internet for a wide variety of activities*' [1]. In the same direction, Novak and Hoffman [2], as well as Wilhelm and Thierer [3] also illustrate this ICT gap as a binary classification of ICT '*haves*' and '*have-nots*', pointing to those who have access to new technologies and those who do not. However, this perspective is not dominant. In the last decade, the substantial magnitude of the Internet use penetration brought to surface significant differences among the Internet users' profiles. It has been shown that digital divide is more a complex and multidimensional phenomenon than just a matter of ICT access. Since the digital divide is directly associated with users' characteristics, the potential ICT adoption depends on and embodies to some extent the society's disparities. Cuervo and Menendez [4] describe it as the '*consequence of the economic and social disparities*'. Furthermore, DiMaggio and Hargittai [5] disassociated the inequality of access from digital inequality, while Attewell [6] refers to this distinction as the *first-level* and *second-level* digital divide.

The digital divide occurs in workplaces, home, among countries, groups of people, etc. This technological gap is mainly examined at individual, household, business or geographical area level. According to the level of analysis the factors that contribute to the digital divide widening differ. Furthermore, inequalities in ICT diffusion become more substantial where a great demand for a high degree of information processing and efficient communication procedures exists.

2 Determinant Factors of the Digital Divide

This section consists of a brief review of the available literature so far, divided into two subsections. In the first subsection, the focus is set on studies which explore and analyze the factors that affect ICT adoption regarding the individual, household and geographical area level. At this point it must be declared that, depending on each approach, literature often categorizes certain factors in order to provide a comprehensive framework of research. Examples of frameworks are those proposed by Barzilai-Nahon [7], Selhofer and Hüsing [8], Barclay and Duggan [9]. The current subsection presents these factors due to their importance given by the literature and not based on a specific framework. In the second subsection, an overview of the available literature on the adoption of ICTs by businesses is presented.

As it was mentioned earlier, the notion of the digital divide is so complicated mainly because it mirrors the society's inequalities, at least to some extent. Due to this fact, it is more difficult for researchers and policy makers to develop a concrete research framework. Consequently, the factors proposed and the variables used in the literature vary, depending on the perspective and the methodological approach of each study. The factors, on which literature emphasizes more, are: network infrastructure, ICT cost, education, income, age, gender, and use of ICT, while support, accessibility, language, location, and ethnicity are also gaining increased attention.

Network infrastructure is obviously the most determinant factor of ICT diffusion. The limitations on physical lines, communication channels, ISPs, secure servers, etc. dramatically decrease the diffusion process of the technological innovations especially regarding to the Internet. The variables mostly used to reflect the development degree of the network infrastructure are: number of Internet hosts, secure servers' density, and access lines. Menkova states that, there is a generic convergence across countries on a worldwide basis regarding the number of Internet hosts [10]. However, Cuervo and Menendez [11] underline the important differences among countries of the EU, in terms of secure servers per million inhabitants (e.g. Greece: 17, Luxembourg: 155). The same result derives from OECD, where the number of Internet hosts per million inhabitants in the United States of America is far greater (more than 250 hosts) than OECD average (88 hosts) and EU average (42 hosts).

The cost of equipment and/or Internet access is highly correlated with ICT penetration [12]. While it is true that ICT access costs decline over time, the higher cost of ICT use negatively affects ICT adoption and is referred as the main reason for people not having Internet at home in fourteen European countries [13]. Additionally, according to OECD [14] the cost of ICTs tends to be higher in rural areas. The data analyzed by Cuervo and Menendez show that Greece has the highest prices for Internet dial up access costs for a residential user among the members of the EU.

Indisputably, the higher the level of education, the more likely it is for a person to have access and use ICTs. Moreover, among individuals with the same income level, those with higher educational background have higher rates of access. The same conclusion was reached by Selhofer and Hüsing [15], who underlined that it is more difficult for low educated people to catch up with those with average education. More specifically, the analysis of the data from a survey conducted in the EU-15 in 2002 revealed that people with university education are 5.1 times more likely to use the Internet than people with primary school education [16]. Finally, the Observatory for the Information Society [17] reports that Greece follows the same rates of ICT adoption by education level with EU-27 average, with the exception that low educated people are notably below the EU-27 average.

Another factor that definitely affects the degree of ICT use and access is income, as it illustrates the extent to which a user can afford the cost of Internet access, PCs, peripherals, etc. Studies mainly focus on individual or household income expressed as the Gross Domestic Product (GDP) per capita or per household, respectively. OECD [18] underlines that household and/or individual income is a key determinant of the presence of a personal computer (PC) at home. Undeniably, higher income positively affects ICT adoption.

The age and gender of the potential ICT users also have a considerable impact on accessing and using ICTs. In general, Internet access and PC use tend to be higher for younger people than for older people. According to data from the OECD, the age group with the most ICT users was the 35 to 45 years old group. A more recent study, in which data of EU-25 were analyzed, indicates that the age group of 16 to 24 leads, having a three times higher proportion of computer or Internet use than the age group of 55 to 74 [19]. The same outcome arises from the report of the Observatory for the Information Society [20], when examining ICT adoption by groups of age in Greece. Consequently, the presence of children in a household significantly increases the potential of having a PC and accessing the Internet. Specifically, the use of PCs at home in Greece for households with dependent children is two times the percentage of households without children [21]. The role of gender in accessing and using ICTs is often examined in parallel with age. However, most studies show that contrary to what happens with age, gender contributes less to the digital divide widening. The differences in ICT use, regarding gender, are mainly illustrated between older men (over 50) and younger women (up to 45). Men over 50 years old are more likely to use the Internet than women of the same age, while women up to 40s make a greater use when compared with men of the same age [22].

The use of ICTs has been fostered enormously during the last years. Specifically, the number of PCs was raised from 2.5 to 9 per one hundred inhabitants between 1990 and 2001, while in the same period the Internet use was raised from almost zero to 8 percent of world's population [23]. Although there is an increasing use of ICTs worldwide, there are still significant disparities among countries regarding their adoption degree. Cuervo and Menendez [24] underline the major differences existing between countries of the EU, in terms of the number of computers per one hundred inhabitants giving the example of Greece, which is far below Sweden (Greece: 8, Sweden: 56). Moreover, according to Demunter [25] the degree of the Internet and computers' use for Greece is among the lowest when referring to EU of 25 and the lowest among the EU of 15. The same results stand either for household or individual level.

It is obvious that the analysis of the factors presented above can not explain in total the inequalities in ICT adoption because they can not depict the society's disparities in a comprehensive way. Many other factors have been proposed and found to be correlated with the use and access of ICTs. Some of the most important are: support, profession, language, skill, location, ethnicity, etc. Based on Barzilai-Nahon [26], the notion of support involves governmental and social acts and is relevant to policy adopted by the government regarding the promotion of technology use (through investment and funding). It seems that in those cases where the user's profession involves the use of a PC there is a positive effect on ICT uses at home [27]. Undeniably, given that English is the language of the Internet, people who cannot understand English have a great difficulty in using the Internet. The skills of the ICT user also have proved to be very important. The Observatory for the Information Society [28] reports that, 14 percent of those who do not use or have access to the Internet, indicate as main reason the lack of appropriate skills. Moreover, Hargittai [29] found a great variance in people's ability to locate content online. The location of residence within a country and/or the location of a country within a geographical region also affect ICT adoption. Urban areas tend to have better infrastructure and lower prices in contrast with rural ones. Billón *et al.* [30] state that adjacent regions of EU tend to have similar rates of Internet adoption. Finally, ethnicity can prevent groups of people from accessing and using ICTs [31].

As far as the examination focuses on groups of people and countries a brief overview of the major factors which contribute in the widening of the digital divide has been presented. Another field of research, in which the digital divide is apparent, is business. It is true that, the use of ICTs in business has fostered firms' productivity dramatically. Nevertheless, the use of ICTs differs a lot among industries and firms. The literature indicates as factors with greater importance firm size, firm's location, type of industry, external environment, and IT investment. Variables mostly used to examine the diffusion of ICTs among firms are: Internet access, existence of a Web site, number of computers per employee, employee's skills, use of e-mail, browsing, use of ERP, online sales, online purchases, etc.

The size of a firm seems to be the most determinant factor for its performance in using and accessing ICTs. The variable used in order to categorize the firms by size is the total number of employees [32]. Firm size plays a major role not only in accessing and using ICTs, but in IT investment too. Bigger firms are more likely to invest in new technologies. Moreover, the size of a firm in correlation with the external environment shows that small firms expand their use and access to ICTs due to the external pressure of larger enterprises [33]. Since the Internet provides firms the advantage to target not only the local but the national and the global market as well, the competition in terms of ICT uses significantly increases. The external environment pushes firms to invest more on IT and innovation in order to maintain their competitive position [34]. Another factor that significantly affects the diffusion of ICTs among firms is their established location. Similarly to the individuals whose location influences the adoption of ICTs, the location of enterprises affects the extent to which they access and use ICTs. A classification of a firm's location within a country may be rural or urban. There is not a specific definition to accurately describe and distinct the rural from the urban areas. This mostly happens due to the major socio-economic disparities among countries. A convenient variable which is used to classify these areas is the population density. Undoubtedly, enterprises located in urban areas are more likely to confront lower costs of access [35]. Geographical dispersion, as Forman [36] underlines, has less impact on the use of applications than on the use of the Internet. Finally, the type of industry plays a major role in the use and access of ICTs. Moreover, industries that provide information-intensive services such as communication and finance usually have higher penetration rates.

According to the Observatory for the Information Society [37] the location and the size of a firm definitely affect the access and use of ICTs. An example from the tourism industry is given below. Researchers from the Observatory for the Information Society analyzed a sample consisting of 250 hotels and 250 smaller firms ('rooms to let') divided into three groups according to their size (large, medium, and small). It was found that large hotels have a double Internet access rate than smaller ones, while large 'rooms to let' firms have four times higher access rate than smaller ones. The process of selling online is mainly adopted by hotels. The rate of selling online for hotels ranges between 62 to 67 percent, in contrary to 'rooms to let' firms where rates vary a lot (20 to 57 percent) depending on the firm's size. Finally, the possibility for the firms which lack of Internet access, computers, etc. to invest on ICTs seems rather low. While the majority of the firms states their satisfaction from the adoption of ICTs and believes that online sales benefit their business, only a very small percentage of them (10 percent at most) hires an IT expert.

An overall conclusion of this brief literature review could be that the widening of digital divide is mainly influenced by users' characteristics and behaviors, while physical infrastructure and policies also play a major role. Moreover, it should be noted that generally there is a lack of sufficient data, since the available data mostly apply on a national level. Due to this, the process of examining and measuring the digital divide becomes even more difficult.

3 Forms of Digital Inequality

Researchers have recently started to discuss the term 'digital inequality'. This term refers to socio-economic disparities inside the 'online population', such as the quality and the cost of the connection to the Internet, the skills and the knowledge to find the required information, etc. The primary issue nowadays is not whether there is an Internet access but what people are able to do when they have access to the Internet [38]. There are five broad forms of digital inequality [39]:

- Inequality with regard to technical means
  Internet users, who have no access to powerful and usually expensive means, can not exploit the full range of Internet content.
- Inequality with regard to autonomy of use
  The autonomy of Internet users may be restricted by the constraints of the geographical area or the exact location where the access is feasible. Such constraints might concern the access time (e.g. public libraries), the content itself (e.g. workplaces), the quality of the Internet connection (e.g. urban versus rural areas), etc.
- Inequality with regard to skills
  Internet users differ regarding the level of their expertise, education, and technical skills. The more the knowledge about the medium, the better the exploitation of it.
- Inequality with regard to social support
  The people, whose friends and/or families are more familiar with new technologies, are usually more motivated to adopt and use ICTs too.
- Inequality with regard to purpose of use

The higher the purpose of use of the Internet, the more the knowledge required for it. This means that, if the medium is used only for entertainment then the user usually has limited knowledge; but if the medium is used for the accomplishment of complicated tasks, the user should have extended knowledge.

4 Methodological Approach

In our research, the basic tendencies of some critical parameters of the digital inequality in the EU were examined. We focused our analysis upon the level of formal education, which is a representative variable of the ‘skill’ dimension, and the density of population in different geographical areas, as a representative variable of the ‘autonomy of use’ dimension. The level of formal education was considered as a three-scaled ordinal variable: (i) high: university level, (ii) medium: high school level, and (iii) low: lower than high school education. The density of population was also considered as a three-scaled ordinal variable: (i) high: $\geq$ 500 inhabitants per squared kilometer, (ii) medium: 100-499 inhabitants per squared kilometer, and (iii) low: $\leq$ 99 inhabitants per squared kilometer.

The measurements we actually used were the daily use of computers for the last three months (every day or almost every day) and the average use of the Internet at least once per week. Our intention was to avoid the random use of new technologies, which would probably be the result of a longer time period selection. Examining the level of education, we dealt with the user group of people between 25 and 54 years old. This is due to the fact that, these ages have mostly experienced the transition from the traditional means to ICTs. The most recent data at the time of writing were employed, published by Eurostat [40]. The purpose of this secondary research is to demonstrate the differences among the member states of the EU with regard to the aforementioned variables, thus giving evidence of the existence of the digital inequality.

5 Findings

The findings of the secondary research, described in the previous section, are presented in the Figs. 1, 2, 3, 4, 5, and 6. As it can be seen in Fig. 1, the percentages of the daily use of computers, with regard to the individuals with high formal education, are particularly high for all the European countries. Denmark and Slovenia have the leading positions with the highest percentage (91%), while Greece, having the lowest percentage (63%), is far behind the mean value of EU-27 (81%). The average use of the Internet at least once per week, as regards the individuals with a high education level, also receives high values, a little higher than the previously mentioned variable in most cases. The Netherlands and Finland have the highest percentage (97%), while Greece has again the lowest (66%). The mean value of EU-27 is 86%.

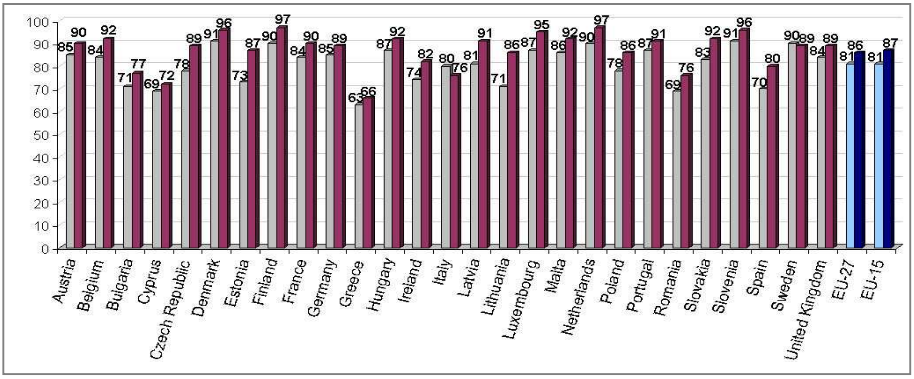


Fig. 1. Percentage of individuals aged 25 to 54 with high formal education, who used a computer every day (first column) and the Internet at least once per week (second column)

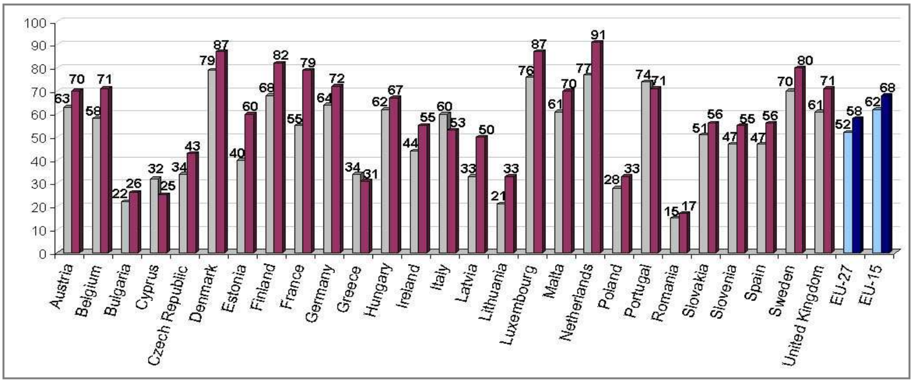


Fig. 2. Percentage of individuals aged 25 to 54 with medium formal education, who used a computer every day (first column) and the Internet at least once per week (second column)

The findings for the sample of individuals with a medium education level are completely different (Fig. 2). The mean values in the EU-27 and the EU-15 are 52% and 62% respectively. Denmark has the highest percentage (79%), while Romania the lowest (15%). Greece (34%) occupies a better position compared to the results in the previous case of highly educated people. Concerning the average use of the Internet by individuals with a medium education level, there are many fluctuations among the European countries. The highest percentage is 91% (the Netherlands) and the lowest only 17% (Romania). The percentage of Greece is one of the lowest (31%). The difference between the mean values of the EU-27 (58%) and the EU-15 (68%) is exactly the same with the respective difference for the daily use of computers.

As it was expected, the low educated individuals use computers, as well as the Internet, at a minimum level (Fig. 3). The Netherlands have the highest percentage, both in computers (61%) and the Internet (76%). On the other hand, Bulgaria has tremendously low percentages, both in computers (1%) and the Internet (lower than 1%). Unfortunately, the percentages of Greece are only slightly better (6% for the daily use of computers and 4% for the average use of the Internet at least once per week).

According to the findings, the density of population has an impact on the daily use of computers and the average use of the Internet. The 79% of Swedish, living in densely populated areas, use a computer every day or almost every day, i.e., the highest percentage, while only 27% of Romanians do the same thing, i.e., the lowest percentage (Fig. 4). The percentage of Greeks is 36%, i.e., the second lowest. This percentage is repeated for Greece, when the average use of the Internet is examined. In that case, the highest percentage is related to Finland (85%) and the lowest to Romania (34%).

In the areas with a medium population density, there were not significant differences compared to the previously mentioned areas, with regard to the daily use of a computer (Fig. 5). The Netherlands have the highest percentage (72%), while Greece and Bulgaria the lowest (22%). Taking into consideration the average use of the Internet, the Netherlands occupy again the first position in the ranking order (84%) and Greece the last position (24%).

In the sparsely populated areas, the daily use of computers seems to be quite limited (Fig. 6). This can be seen by the much lower percentage of EU-27 (37%) compared to 51% (high density) and 48% (medium density). The Netherlands have the highest percentage (65%) and Romania the lowest (6%). The data for the Internet are in correspondence with the data for computers. The average use of the Internet in the EU-27 is only 42%, while it comes to 58% for densely populated areas and 52% for areas with a medium density. Once again the Netherlands have the highest percentage (78%) and Romania the lowest (6%).

Trying to interpret these results we need to make the following comments: northern European countries demonstrate a much more intense use of ICTs than the southern part of Europe. We believe that the most significant factors to this kind of digital divide, which is actually a form of digital inequality, are: (i) the higher family income in northern European countries, (ii) the faster acquaintance of younger people with ICTs at school, (iii) the more effective and efficient education and training systems, and particularly (iv) the much greater development of network infrastructure. It is also a matter of mentality since people in north Europe are more used to sophisticated equipment, and therefore they know how to fully exploit the tremendous possibilities of new technologies. Further analysis of these factors is a prerequisite to making suggestions on how to bridge the digital inequality among the countries of the EU.

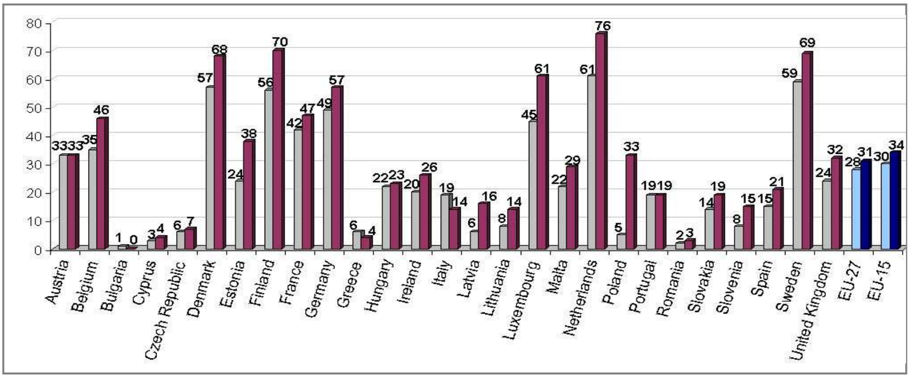


Fig. 3. Percentage of individuals aged 25 to 54 with low formal education, who used a computer every day (first column) and the Internet at least once per week (second column)

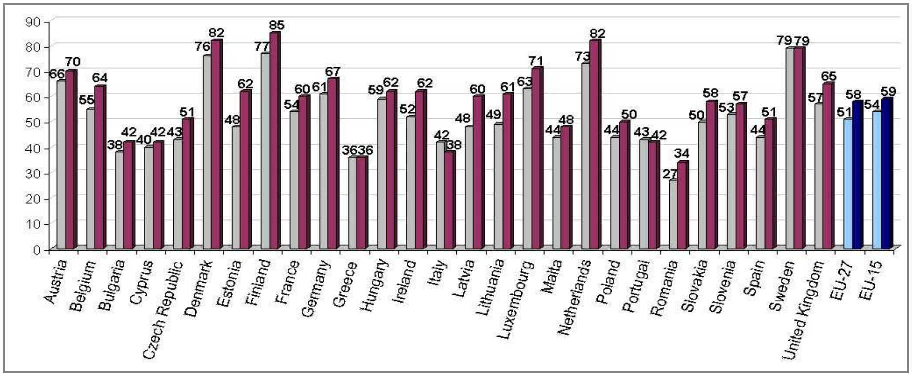


Fig. 4. Percentage of individuals, living in densely populated areas, who used a computer every day (first column) and the Internet at least once per week (second column)

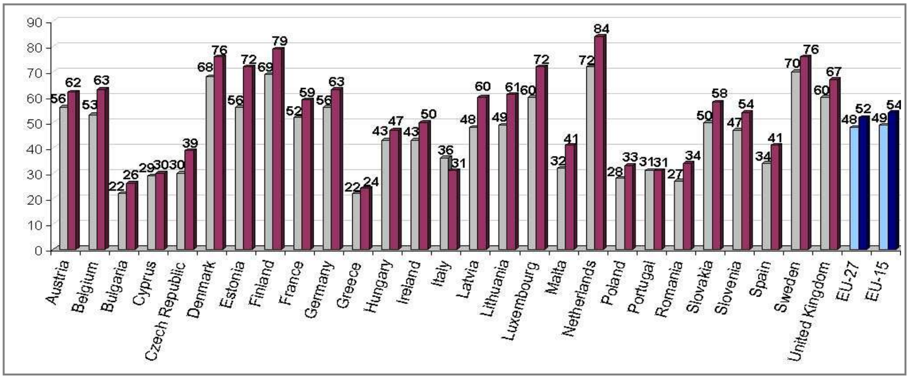


Fig. 5. Percentage of individuals, living in areas with a medium population density, who used a computer every day (first column) and the Internet at least once per week (second column)

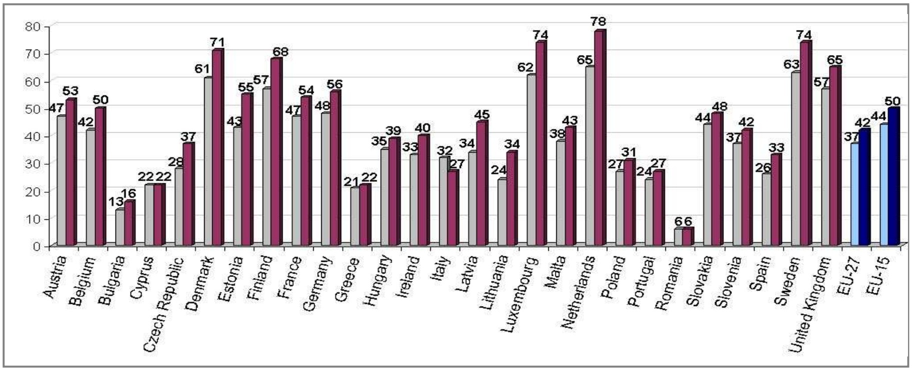


Fig. 6. Percentage of individuals, living in sparsely populated areas, who used a computer every day (first column) and the Internet at least once per week (second column)

6 Conclusion

Analyzing the secondary data provided by Eurostat, we found that there are significant disparities among the member states of the EU. The disparities, which our analysis focuses on, are related with the level of formal education and the density of population in different geographical areas. These disparities are characteristic of the digital inequality among individuals who have access to the Internet. More specifically, the differences in terms of the formal education are connected with the 'skill' dimension of the digital inequality. Moreover, the differences in terms of the density of population are connected with the 'autonomy' of Internet users, i.e., another dimension of the digital inequality. Even if the bridging of the digital divide becomes a reality, the digital inequality is evolving to a crucial problem, which should be confronted with essential and immediate measures by the European leaders.

We also found that, Greece seems to have very low percentages in terms of the daily use of computers and the average use of the Internet. For instance, highly educated Greeks use a computer and the Internet at the lowest rate in the EU. Additionally, Greeks, who live in areas with a medium population density (100-499 inhabitants / km^2), also use a computer and the Internet at the lowest rate among the member states of the EU. These findings are clear indications of the size of the digital inequality in Greece.

It is true that network infrastructure is still under development in many areas of Greece, mostly including rural areas, as well as a few large cities. Consequently the cost for having a broadband Internet connection at home is still quite high. Moreover, in an attempt to explore more the reasons why Greek people are not so familiarized with technology, we can focus on the education system which is not adequately modernized. It must be underlined that the telecommunication companies in Greece started investing on high speed network infrastructure just a few years ago. Nevertheless, Greek authorities and telecommunication companies make efforts to motivate people to increasingly access the broadband Internet.

Finally, we should mention as a limitation of this research the fact that, it focuses only on two dimensions of the digital inequality; further research should be extended to the other three dimensions of the digital inequality, namely technical means, social support, and purpose of use.

References

1. OECD, Understanding the Digital Divide (2001), `http://www.oecd.org/dataoecd/38/57/1888451.pdf`
2. Novak, T.P., Hoffman, D.L.: Bridging the Digital Divide: The Internet of Race on Computer Access and Internet Use (2000), `http://www2000.ogsm.vanderbilt.edu/digital.divide.html`
3. Wilhelm, A.G., Thierer, A.D.: Should Americans be Concerned about the Digital Divide? Insight on the News 16(33) (September 4, 2000)
4. Cuervo, M.R.V., Menendez, A.J.L.: A Multivariate Framework for the Analysis of the Digital Divide: Evidence for the European Union-15. Information & Management 43, 756–766 (2006)
5. DiMaggio, P., Hargittai, E.: From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases. Center for Arts and Cultural Policy Studies, Princeton University, Working Paper #15 (2001)
6. Attewell, P.A.: The First and Second Digital Divides. Sociology of Education 74, 252–259 (2001)
7. Barzilai-Nahon, K.: Gaps and Bits: Conceptualizing Measurements for Digital Divide/s. The Information Society 22(5), 269–278 (2006)
8. Selhofer, H., Hüsing, T.: The Digital Divide Index – A Measure of Social Inequalities in the Adoption of ICT. In: IST Conference, Copenhagen (2002)
9. Barclay, C., Duggan, E.W.: Rethinking the Digital Divide: Towards a Path of Digital Effectiveness. In: 41st International Conference on System Sciences, Hawaii (2008)
10. Menkova, V.: Digital Divide and Cross Country Diffusion of the Internet. Thesis of Master of Arts in Economics, National University 'Kyin-Mohyla Academy' (2004), `http://kse.org.ua/library/matheses/2004/Menkova_Viktoriya/body.pdf`
11. Cuervo, M.R.V., Menendez, A.J.L.: A Multivariate Framework for the Analysis of the Digital Divide: Evidence for the European Union-15. Information & Management 43, 756–766 (2006)
12. Ganley, D., Dewan, S., Kraemer, K.L.: The Co-Diffusion of Successive Information Technologies: Implications for the Global Digital Divide. Center for Research on Information Technology and Organizations and the Paul Merage School of Business, University of California, Working Paper (2005)
13. Demunter, C.: The Digital Divide in Europe. Statistics in focus, Eurostat (2005)
14. OECD, The Development of Broadband Access in Rural and Remote Areas. Working Party on Telecommunication and Information Services Policies (2004)
15. Selhofer, H., Hüsing, T.: The Digital Divide Index – A Measure of Social Inequalities in the Adoption of ICT. In: IST Conference, Copenhagen (2002)
16. Cuervo, M.R.V., López, J.: Patterns of ICT Diffusion across the European Union. Economics Letters 93, 45–51 (2006)
17. Observatory for the Information Society, The Profile of Internet Users in Greece (2008B), `http://www.observe.gr/files/press_releases/080604_DT_InternetUsers07.pdf`
18. OECD, Understanding the Digital Divide (2001), `http://www.oecd.org/dataoecd/38/57/1888451.pdf`
19. Demunter, C.: The Digital Divide in Europe. Statistics in focus, Eurostat (2005)

20. OECD, Understanding the Digital Divide (2001), http://www.oecd.org/dataoecd/38/57/1888451.pdf
21. Demunter, C.: The Digital Divide in Europe. Statistics in focus, Eurostat (2005)
22. National Telecommunication and Information Administration, A Nation Online: How Americans are Expanding their Use of the Internet. U.S. Department of Commerce, Washington, D.C. (2002)
23. Chinn, M.D., Fairlie, R.W.: The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration. IZA Discussion Paper No. 1305 (2004)
24. Cuervo, M.R.V., Menendez, A.J.L.: A Multivariate Framework for the Analysis of the Digital Divide: Evidence for the European Union-15. Information & Management 43, 756–766 (2006)
25. Demunter, C.: The Digital Divide in Europe. Statistics in focus, Eurostat (2005)
26. Barzilai-Nahon, K.: Gaps and Bits: Conceptualizing Measurements for Digital Divide/s. The Information Society 22(5), 269–278 (2006)
27. National Telecommunication and Information Administration, A Nation Online: How Americans are Expanding their Use of the Internet. U.S. Department of Commerce, Washington, D.C. (2002)
28. Observatory for the Information Society, The Profile of Internet Users in Greece (2008B), http://www.observe.gr/files/press_releases/080604_DT_InternetUsers07.pdf
29. Hargittai, E.: Second Level Digital Divide: Differences in People's Online Skills. First Monday 7(4) (2002), http://www.eszter.com/research/pubs/hargittai-secondleveldd.pdf
30. Billón, M., Ezcurra, R., Lera-López, F.: The Spatial Distribution of the Internet in the European Union: Does Geographical Proximity Matter? European Planning Studies 16(1), 119–142 (2008)
31. Korupp, S.E., Szydlik, M.: Causes and Trends of the Digital Divide. European Sociological Review 21(4), 409–422 (2005)
32. Forman, C.: The Corporate Digital Divide: Determinants of Internet Adoption. Management Science 51(4), 641–654 (2005)
33. Dewan, S., Riggins, F.J.: The Digital Divide: Current and Future Research Directions. Journal of the Association for Information Systems 6(12) (2005)
34. Iacovou, C., Benbasat, I., Dexter, A.: Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. MIS Quart. 19(4), 465–485 (1995)
35. Labrianidis, L., Kalogeressis, T.: The Digital Divide in Europe's Rural Enterprises. European Planning Studies 14(1), 23–39 (2006)
36. Forman, C.: The Corporate Digital Divide: Determinants of Internet Adoption. Management Science 51(4), 641–654 (2005)
37. Observatory for the Information Society, A Study on the ICT Penetration on Tourism Sector in Greece: Strategies and Perspectives (2008A), http://www.observe.gr/files/meletes/Tourism_Presentation_FINAL_web.pdf
38. Alvarez, A.: Behavioral and Environmental Correlates of Digital Inequality (2003), http://www.stanford.edu/group/siqss/itandsociety/v01i05/v01i05a06.pdf
39. DiMaggio, P., Hargittai, E.: From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases. Center for Arts and Cultural Policy Studies, Princeton University, Working Paper #15 (2001)
40. Eurostat, Individuals – Frequency of Computer Use (2007), http://nui.epp.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_cfp_fu&lang=en

Inkjet-Printed Paper-Based RFID and Nanotechnology-Based Ultrasensitive Sensors: The "Green" Ultimate Solution for an Ever Improving Life Quality and Safety?

Manos Tentzeris and Li Yang

Georgia Electronic Design Center, School of ECE, Georgia Tech, Atlanta,
GA 30332-250, U.S.A.
{etentze,liyang}@ece.gatech.edu

Abstract. The paper introduces the integration of conformal paper-based RFID's with a Single Walled Carbon Nanotube (SW-CNT) composite for the development of a chipless RFID-enabled wireless sensor node for toxic gas detection and breathing-gas-content estimation. The electrical performance of the inkjet-printed SWCNT-based ultra-sensitive sensor if reported up to 1GHz. The whole module is realized by inkjet-printing on a low-cost "green" paper-based substrate designed to operate in the European UHF RFID band. The electrical conductivity of the SWCNT film changes in the presence of ultra-small quantities of gases like ammonia and nitrogen dioxide, resulting in the variation of the backscattered power level which can be easily detected by the RFID reader to realize reliable early-warning toxic gas detection or breathing monitoring with potentially profound effects on ubiquitous low-cost "green" quality-of-life applications.

Keywords: Nanotechnology, RFID, carbon nanotube composites, green technologies, gas sensing, conformal/wearable sensors, inkjet printing, wireless sensor, quality-of-life, gas detection, biomonitoring.

1 Introduction

The steadily growing Radio Frequency Identification (RFID) industry requires an ever improving performance of the RFID systems, including reduced size and cost, and higher levels of integration. Also, the tag flexibility is becoming a must for almost all applications, including body area networks for medical systems, tracking for pharmaceutical and food industries, supply chain, space and many more. This demand is further enhanced by the need for lightweight, reliable and durable wireless RFID-enabled sensor nodes [1]. Hence, the two major challenges for such applications are the choice of the material and the advanced integration capabilities. The choice of paper as the substrate material presents multiple advantages and has established paper as one of the most promising materials for UHF RFID applications: it is widely available, and the high demand and the mass "reel-to-reel" production make it the cheapest material ever made. Plus, its environmentally friendly features make it extremely

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 55–63, 2010.

suitable for “green” electronic applications. Previous work has demonstrated the successful development of a fully inkjet-printed RFID module on paper [2]. The next challenge is to integrate the sensor on the paper substrate as well. The application of interest for this work is wireless sensing of toxic gas. Carbon Nanotubes (CNT) composites were found to have electrical conductance highly sensitive to extremely small quantities of gases, such as ammonia (NH_3) and nitrogen oxide (NO_x), etc. at room temperatures with a very fast response time [3]. The conductance change can be explained by the charge transfer of reactive gas molecules with semiconducting CNTs [4]. Previous efforts have shown the successful utilization of CNT-based sensors employing the change in resistance [5]. However, due to the insufficient molecular network formation among the inkjet-printed CNT particles at micro-scale, instabilities were observed in both the resistance and, especially, the reactance dependence on frequency above several MHz, which limits the CNT application in only DC or LF band [6]. To enable the CNT-enabled sensor to be integrated with RFID antenna at UHF band, a special recipe needs to be developed.

This paper presents, for the first time, a conformal CNT-based RFID-enable sensor node for gas sensing applications, fully printed directly on paper substrate. Specifically, in this study one benchmarking RFID tag was designed for the European UHF RFID band centering at 868 MHz. The printed CNT particles were Single-Walled Carbon Nanotubes (SWCNT) from Carbon Solutions, which were dispersed in dimethylformamide (DMF) solution and sonicated to meet the viscosity requirement for the inkjet printer. The SWCNT composite is printed directly on the same paper as the antenna, for a low cost, flexible, highly integrated module. The impedance of the SWCNT film forms the sensor part. The antenna was printed first, followed by the 25 layers of the dispersed SWCNT as a load with “gas-controlled” value. When 4% consistency ammonia was imported into the gas chamber, the SWCNT impedance changed from 51.6-j6.1Ω to 97.1-j18.8Ω at 868MHz, resulting in a 10.8dBi variation in the backscattered power from the RFID antenna, that can be easily detected by the RFID reader to realize the “real-time” gas detection.

2 Inkjet-Printed SW-CNT

As a direct-write technology, inkjet printing transfers the pattern directly to the substrate. Due to its capability of jetting one single ink droplet in the amount as low as 1 pl, it has widely drawn attention from the industrial world as a more accurate and economic fabrication method than the traditional lithography method.

To enable the SWCNT to be inkjet printed, a SWCNT ink solution was developed as the first step. Two types of SWCNT, namely, P2-SWCNT and P3-SWCNT were tested. P2-SWCNT is developed from purified AP-SWNT by air oxidation and catalyst removing. P3-SWCNT is developed from AP-SWNT purified with nitric acid. Compared with P2-SWCNT, P3-SWCNT has much higher functionality and is easier to disperse in the solvent. In experiments, P2-SWCNT started to aggregate at the concentration lower than 0.1mg/ml, while P3-SWCNT can go up to 0.4mg/ml and still show good dispersion. Therefore, P3-SWCNT was selected for the latter steps.

The sample SWCNT powder was dispersed in DMF, a polar aprotic solvent. The concentration of the ink was 0.4mg/ml. This high concentration helped the nano particle network formation after printing; otherwise there would be instability in the impedance response versus frequency of the SWCNT film due to insufficient network formation, such as a sharp dropping of resistance value after 10 MHz [7]. The diluted solution was purified by sonicated for 12 hours to prevent aggregations of large particle residues. This is important to avoid the nozzle clogging by SWCNT flocculation during the printing process. One Materials Printer was used to eject the SWCNT ink droplet onto a flexible substrate.

Silver electrodes were patterned with the nano-practical ink from Cabot before depositing the SWCNT film, followed by a 140°C sintering. The electrode finger is 2mm by 10mm with a gap of 0.8mm. Then, the 3mm by 2mm SWCNT film was deposited. The 0.6mm overlapping zone is to ensure the good contact between the SWCNT film and the electrodes. Four devices with 10, 15, 20 and 25 SWCNT layers with an approximate thickness of 0.75um/layer were fabricated to investigate the electrical properties. Fig. 1 shows the fabricated samples.

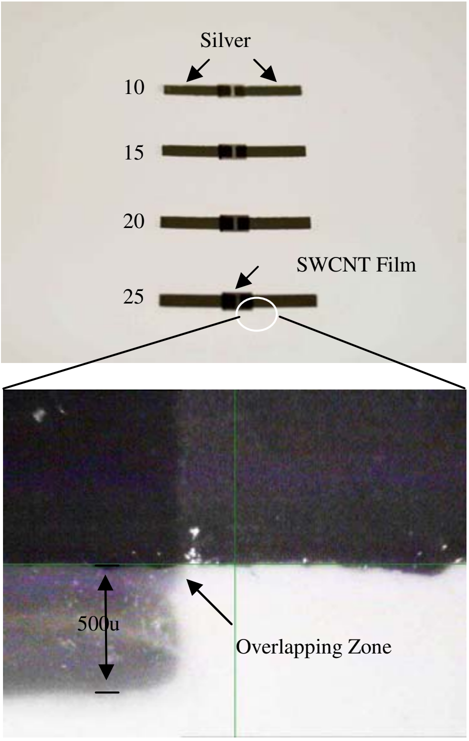


Fig. 1. Photograph of the inkjet-printed SWCNT films with silver electrodes. The SWCNT layers of the samples from up to down are 10, 15, 20 and 25, respectively. The dark region in the magnified picture shows the overlapping zone between the SWCNT and the silver electrodes.

CNT composites have been found to have a very unique resistance performance that can enable the realization of the next generation of sensors with a very high sensitivity up to 1ppb (part per billion), an improvement of 2-3 orders to traditional sensors. The electrical resistance of the fabricated device was measured by probing the end tips of the two electrodes. The DC results in air are shown in Fig. 2. The resistance goes down from when the number of SWCNT layers increases. Since a high number of SWCNT overwritten layers will also help the nano particle network formation, 25-layer film is expected to have the most stable impedance-frequency response and selected for the gas measurement. In the experiment, 4% consistency ammonia was guided into the gas flowing chamber, which includes gas inlet, outlet and exhaust hood. The test setup is shown in Fig. 3. The SWCNT film was kept in the chamber for 30 minutes. A network vector analyzer (Rohde&Schwarz ZVA8) was used to characterize the SWCNT film electrical performance at UHF band before and after the gas flowing. In Fig. 4, the gas sensor of SWCNT composite shows a very stable impedance response up to 1GHz, which verifies the effectiveness of the developed SWCNT solvent recipe. At 868MHz, the sensor exhibits a resistance of 51.6Ω and a reactance of -6.1Ω in air. After meeting ammonia, the resistance was increased to 97.1Ω and reactance was shifted to -18.8Ω.

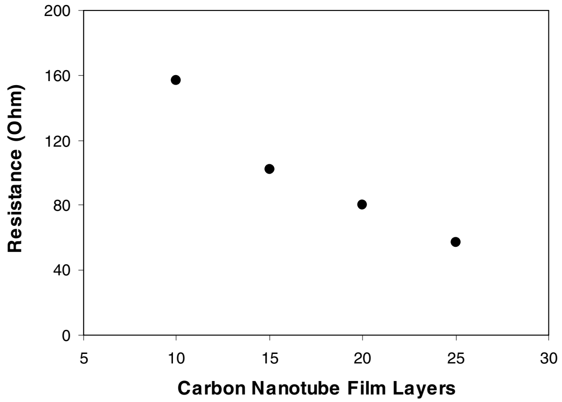


Fig. 2. Measured electrical resistance of SWCNT gas sensor

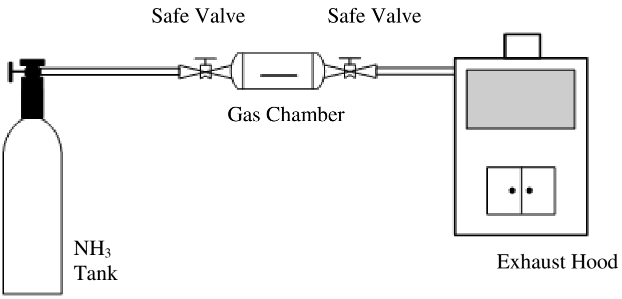


Fig. 3. Schematic of NH_3 gas detection measurement

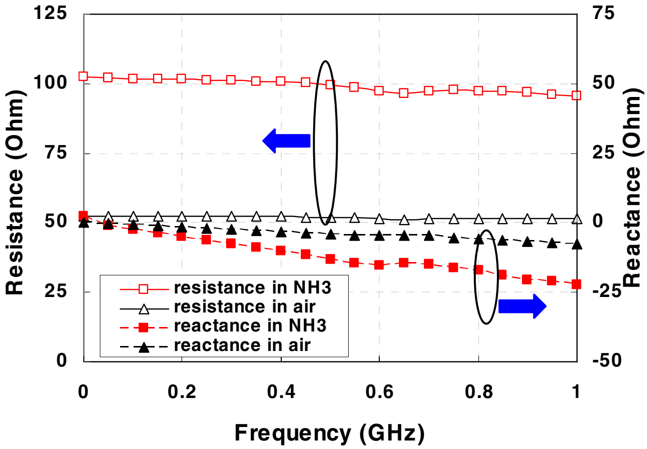


Fig. 4. Measured impedance characteristics of SWCNT film with 25 layers

3 RFID-Enabled "Green" Wireless Sensor Node Module

A passive RFID system operates in the following way: the RFID reader sends an interrogating RF signal to the RFID tag consisting of an antenna and an IC chip as a load. The IC responds to the reader by varying its input impedance, thus modulating the backscattered signal. The modulation scheme often used in RFID applications is amplitude shift keying (ASK) in which the IC impedance switches between the matched state and the mismatched state [8]. The power reflection coefficient of the RFID antenna can be calculated as a measure to evaluate the reflected wave strength.

$$\eta = \left| \frac{Z_{load} - Z_{ANT}{}^{*}}{Z_{load} + Z_{ANT}} \right|^2 \tag{1}$$

where Z_{Load} represents the impedance of the load and Z_{ANT} represents the impedance of the antenna terminals with Z_{ANT}* being its complex conjugate. The same mechanism can be used to realize sensor-enabled RFIDs. The inkjet-printed SWCNT film functions as a tunable resistor Z_{Load} with a value determined by the existence of the target gas. The RFID reader monitors the backscattered power level. When the power level changes, it means that there is variation in the load resistance, therefore the sensor detects the existence of the gas, as illustrated in Fig. 5.

The expected power levels of the received signal at the load of the RFID antenna can be calculated using Friis free-space formula, as

$$P_{tag} = P_t G_t G_r \left(\frac{\lambda}{4\pi d} \right)^2 \tag{2}$$

where P_t is the power fed into the reader antenna, G_t and G_r is the gain of the reader antenna and tag antenna, respectively, and d is the distance between the reader and the tag.

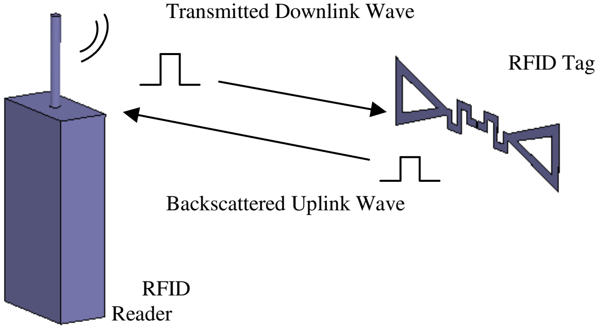
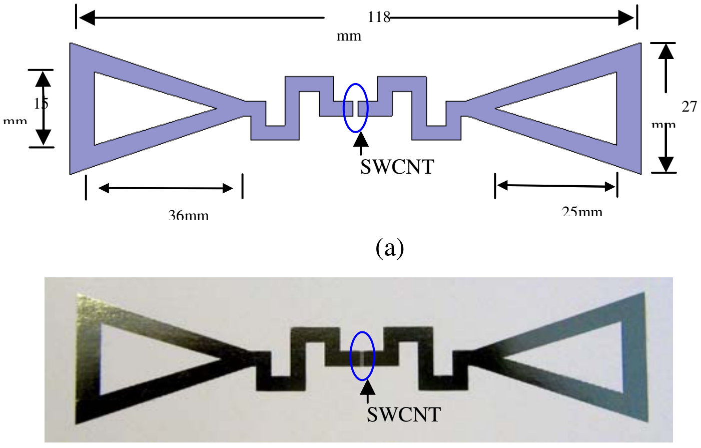


Fig. 5. Conceptual diagram of the proposed RFID-enable sensor



(a)

(b)

Fig. 6. The RFID tag module design on flexible substrate: (a) configuration (b) photograph of the tag with inkjet-printed SWCNT film as a load in the middle

Due to the mismatch between the SWCNT sensor and tag antenna, a portion of the received power would be reflected back, as

$$P_{ref} = P_{tag}\eta \tag{3}$$

where η is the power reflection coefficient in (1). Hence the backscattered power received by the RFID reader is defined as

$$P_r = P_{ref} G_t G_r \eta \left(\frac{\lambda}{4\pi d}\right)^2 = P_t G_t^2 G_r^2 \eta \left(\frac{\lambda}{4\pi d}\right)^4 \tag{4}$$

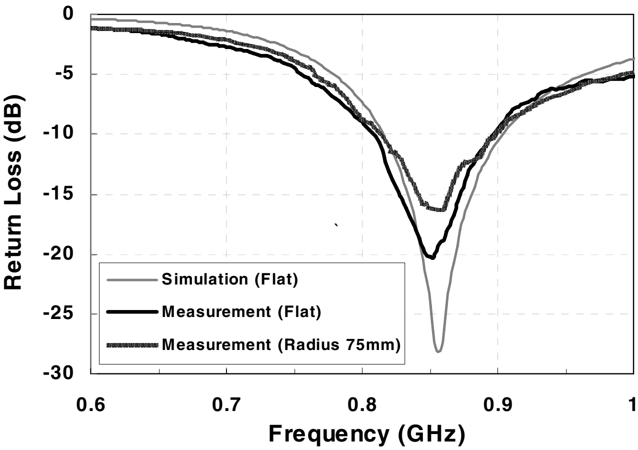
or written in a decibel form, as

$$P_r = P_t + 2G_t + 2G_r - 40\log_{10}\left(\frac{4\pi}{\lambda}\right) - 40\log_{10}(d) + \eta \tag{5}$$

where except the term of η, all the other values remain constant before and after the RFID tag meets gas. Therefore the variation of the backscattered power level solely depends on η, which is determined by the impedance of the SWCNT film.

A bow-tie meander line dipole antenna was designed and fabricated on a 100um thickness flexible paper substrate with dielectric constant 3.2. The RFID prototype structure is shown in Fig. 6 along with dimensions, with the SWCNT film inkjet printed in the center. The nature of the bow-tie shape offers a more broadband operation for the dipole antenna.

A GS 1000μm pitch probe and a dielectric probe station were used for the impedance measurements. The calibration method used was short-open-load-thru (SOLT). The measured Z_{ANT} at 868MHz is 42.6+j11.4Ω. The simulation and measurement results of the return loss of the proposed antenna are shown in Fig. 7, showing a good agreement. The tag bandwidth extends from 810MHz to 890MHz, covering the whole European RFID band. It has to be noted that the flexible property of the paper substrate enables the RFID-enabled module's application in diverse areas, such as in the applications of wireless health monitoring and wearable sensing electronics. In order to verify the performance of the conformal antenna, measurements were performed as well by sticking the same tag on a 75mm radius foam cylinder. As shown in Fig. 7, there is almost no frequency shifting observed, with a bandwidth extending from 814MHz to 891MHz. Overall a good performance is still remained with the interested band covered. Fig. 8 shows the photograph of the designed conformal tag. The radiation pattern is plotted in Fig. 9, which is almost omnidirectional at 868MHz with directivity around 2.01dBi and 94.2% radiation efficiency.



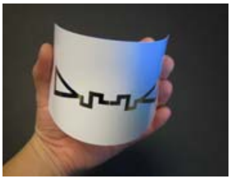


Fig. 7. Simulated and measured return loss of the RFID tag antenna

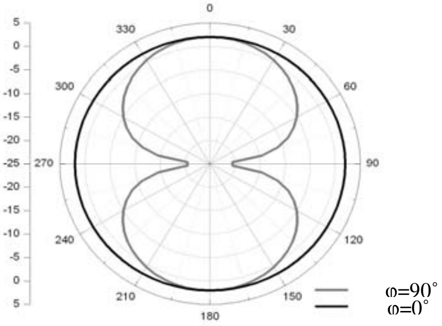


Fig. 8. Far-field radiation pattern plots

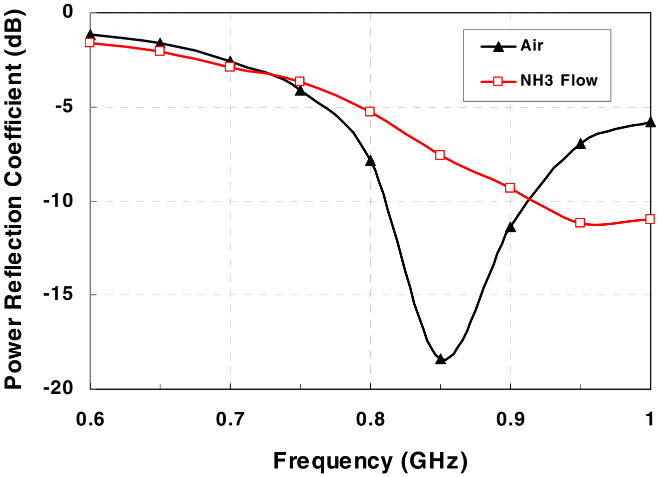


Fig. 9. The power reflection coefficient of the RFID tag antenna with a SWCNT film before and after the gas flow

In the air, the SWCNT film exhibited an impedance of 51.6-j6.1Ω, which results in a low power reflection at -18.4dB. When NH_3 is present, SWCNT film's impedance was shifted to 97.1-j18.8Ω. The mismatch at the antenna port increased the power reflection to -7.6dB. From (5), there would be 10.8dBi increase at the received backscattered power level, as shown in Fig. 9. By detecting this backscattered signal difference on the reader's side, the sensing function can be fulfilled.

4 Conclusions

The inkjet printing method has been utilized to deposit SWCNT film on a fully-printed UHF RFID module on paper to form a "green" flexible ultra-low-cost wireless gas sensor node. To ensure reliable printing, an SWCNT ink solution has been developed. The resistance of the SWCNT film was also characterized up to 1GHz for the first time. The design demonstrated the great applicability of inkjet-printed CNT for the realization of ultrasensitive, fully-integrated "green" wireless RFID-enabled flexible sensor nodes based on the ultrasensitive variabiliity of the resistive properties of the CNT materials with numerous applications in quality-of-life, structural health monitoring, industrial safety and patients' status biomonitoring.

References

[1] Mishima, T., Abe, N., Tanaka, K., Taki, H.: Toward construction of a mobile system with long-range RFID sensors. In: IEEE conference on Cybernetics and Intelligent Systems, vol. 2, pp. 960–965 (2004)

[2] Yang, L., Rida, A., Vyas, R., Tentzeris, M.M.: RFID tag and RF structures on a paper substrate using inkjet-printing technology. IEEE Transaction on Microwave Theory and Techniques 55, 2894–2901 (2007)

[3] Ong, K.G., Zeng, K., Grimes, C.A.: A wireless, passive carbon nanotube-based gas sensor. IEEE Sens. Journal 2, 82–88 (2002)

[4] Cantalinia, C., Valentini, L., Lozzic, L., Armentano, I., Kenny, J.M., Lozzi, L., Santucci, S.: Carbon nanotubes as new materials for gas sensing applications. J. Eur. Ceram. Soc. 24, 1405–1408 (2004)

[5] Yun, J.-H., Chang-Soo, H., Kim, J., Song, J.-W., Shin, D.-H., Park, Y.-G.: Fabrication of Carbon Nanotube Sensor Device by Inkjet Printing. In: 2008 Proc. of IEEE Nano/Micro Engineered and Molecular Systems, January 2008, pp. 506–509 (2008)

[6] Song, J., Kim, J., Yoon, Y., Choi, B., Kim, J., Han, C.: Inkjet printing of singe-walled carbon nanotubes and electrical characterization of the line pattern. Nanotechnology 19 (2008)

[7] Dragoman, M., Flahaut, E., Dragoman, D., Ahmad, M., Plana, R.: Writing electronic devices on paper with carbon nanotube ink (January 2009), ArXiv-0901.0362

[8] Nikitin, P.V., Rao, K.V.S.: Performance limitations of passive UHF RFID systems. In: IEEE Symposium on Antennas and Propagation 2006, July 2006, pp. 1011–1014 (2006)

Examining Adoption of e-Procurement in Public Sector Using the Perceived Characteristics of Innovating: Indonesian Perspective

Fathul Wahid

Department of Informatics, Faculty of Industrial Technology,
Islamic University of Indonesia, Yogyakarta, Indonesia
fathulwahid@fti.uii.ac.id

Abstract. This study aims to examine factors affecting adoption of e-procurement in public sector with special reference to Indonesian context. The Perceived Characteristics of Innovating defined by Moore and Benbasat [1] used as the framework. Based on a survey to 87 contractors/suppliers in the city of Yogyakarta, the study finds that only trialability that affects use intention of e-procurement among the contractors/suppliers. The survey conducted in the early stage of e-procurement implementation is of the possible explanations. Government policy that forces the contractors/suppliers to use the e-procurement also partakes in this context. Practical implication of the findings are also discussed in the paper.

Keywords: e-procurement, e-government, adoption, Indonesia, the Perceived Characteristics of Innovating.

1 Introduction

During the last decade, governments from all over the world have tried to take advantage of information technology (IT) to improve their business processes. IT offers the opportunity for the government to better deliver its information and services and to interact with all its citizens, businesses, and other government partners in a more effective manner [2].

Adoption of e-government has increased in most countries but at the same time the rate of adoption varies from country to country. Generally, developing countries, including Indonesia, are lagging behind in e-government adoption compared to developed countries [3, 4].

In the context of Indonesia, where transparency in public sector is still facing a great burden, the advent of e-government gives a hope on a one side and at the same time a challenge in another. It is hoped that e-government will improve transparency of governmental-related processes, such as public procurement, but the existing challenges are not easy to deal with. One of key challenges is combating widespread corruption in the public procurement.

In order to cope with such a problem, in 2007 the Indonesian government started using e-procurement as an advancement of e-government features. National Planning Board took the lead in this initiative. In the national level, the e-procurement can be

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 64–75, 2010.

assessed at http://www.pengadaannasional-bappenas.go.id. In addition to the use of such system in the national level, the central government has also instructed local governments to adopt the same e-procurement systems gradually taken the readiness of the local government into account [5].

In many developing countries, including Indonesia, often a system that is already developed is underutilized, which in turn the optimal benefits cannot be harvested. Dooley and Purchase [6] found that one of factors influencing e-procurement usage is contractors'/suppliers' participation and intentions. Most previous studies focused on advantages of using e-procurement from the perspective of the users (in this case, the local government) and not from contractors/suppliers' point of view (e.g. [7, 8]). Against this backdrop, the current study aims to address the following research questions: what factors affecting intention to adopt the e-procurement in public sector among the contractors/suppliers?

The extended Perceived Characteristics of Innovating (PCI) proposed by Compeau et al. [9] will be used as a framework. The PCI originally was developed Moore and Benbasat [1] and has received a significant attention through repetition and validation in a variety of contexts (e.g. [9, 10]).

The rest of paper will be organized as follows. In the next section, theoretical basis of e-procurement will be presented along with theory on diffusion of innovation and the PCI. Research design will be explained in third section, followed by section presenting and discussing results of the study. Section of conclusion brings this paper to an end.

2 Theoretical Framework

In this section, issues related to e-procurement is briefly discussed, followed by giving theoretical basis for diffusion of innovation, and more specifically, the perceived characteristics of innovating that is used in the study.

2.1 e-Procurement

According to Croom and Brandon-Jones [8], e-procurement refers to "the use of integrated (commonly web-based) communication systems for the conduct of part or all of the purchasing process; a process that may incorporate stages from the initial need identification by users, through search, sourcing, negotiation, ordering, receipt and post-purchase review." There are several kinds of implementation of e-procurement. Some e-procurement systems in place provide information only, while other facilitate transaction [11].

E-procurement offers benefits to the organization through purchase process efficiency gains and price reductions, enhanced collaborative relationships, and significant opportunity for improving the internal service and status of the purchasing function [12]. In addition, more specifically in public sector, e-procurement also offer other benefits such as enhanced transparency, better access for non-local bidders, better access for Small and Medium-Sized Enterprises (SMEs), and corruption avoidance [11].

Previous studies (e.g. [6, 13]) found several critical success factors (CSFs) in implementing e-procurement. Some of the factors are end-users uptake and training, supplier adoption, system integration, re-engineering the process, top management support, performance measurement, and implementation strategy. In line with the CFSs, there are also several barriers take cope with in implementing e-procurement systems, include expensive implementation cost, limited resources, technology barriers, governing body resistance, and supplier resistance [7].

2.2 Diffusion of Innovation

According to Taylor and Todd [14], the problem of innovation diffusion can be approached from several levels. Some researchers have approached from a macro-view within a societal context or at country level (e.g. [15, 16]). Other researchers have examined this issue at an organizational level (e.g. [10, 17]) and still other researchers have approached this issue by investigating the determinants of adoption and usage by an individual (e.g. [18]).

The adoption and use of IT at organizational and individual levels have received a great deal of attention in recent information systems literature. Rogers [19] also discussed the diffusion of innovation at these two levels. Our study of e-procurement adoption falls into the organizational level.

Taylor and Todd [14], further distinguish the research on the determinants of IT usage into two streams: those based on intention-based models, exemplified by such theories as Technology Acceptance Model (TAM), and diffusion of innovation, exemplified by Roger's diffusion of innovation theory and the PCI model proposed by Moore and Benbasat [1]. In this study, e-procurement is both an innovation and a technology.

Rogers' [1] classical work on the area of diffusion of innovation has been widely used in the study of technology adoption. He defined diffusion of innovation as "the process by which an innovation is communicated through certain channels over time among the members of a social system" [19].

An innovation is characterized as "an idea, practice, or object that is perceived as novel by an individual or other unit of adoption" [19]. Rogers' review of a large number of studies of adoption and diffusion of innovation unearthed five general characteristics of innovations that regularly affect adoption, namely: relative advantage, compatibility, complexity, observability, and trialability.

Relative advantage refers to "the degree to which an innovation is perceived as better than the idea it supersedes" [19]. This characteristic may be measured in economic terms, social prestige, convenience, and satisfaction. The more advantageous an innovation, the faster the rate of adoption will be.

Compatibility is "the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters" [19]. An innovation's incompatibility with cultural values can hinder its adoption. Compatibility of an innovation with a prior idea can speed up its rate of adoption. Complexity represents "the degree to which an innovation is perceived as relatively difficult to understand and use" [19]. The simpler or less complicated an innovation, the higher the speed of adoption will be.

Trialability refers to "the degree to which an innovation may be experienced with on a limited basis" [19]. Some innovations are difficult or even impossible to be tried before adoption, while some are not. When an innovation is possible to be tried out before adoption, it will be easier to decide either to adopt or to reject the innovation.

Further, Rogers [19] defines observability as "the degree to which an innovation is visible to others". The results, either benefits or detriments, of some innovations are easy to measure, observe and communicate to others, while it is difficult for some other innovations. The easier it is for potential adopters to see the positive results of an innovation, the more likely they are to adopt it, and vice versa.

2.3 The Perceived Characteristics of Innovating

The Perceived Characteristics of Innovating (PCI) developed by Moore and Benbasat [1] consists of eight antecedent constructs to predict intention of technology adoption. The PCI model is based on Rogers' [19] model of diffusion of innovation. It may be recalled that Roger's model incorporates five innovation characteristics as antecedents to any adoption decision: relative advantage, compatibility, complexity, trialability, and observability as aforementioned.

The PCI model incorporates three of those constructs – relative advantage, compatibility, and trialability – as in their original definitions. Moore and Benbasat replaced the complexity construct of Rogers' model with ease-of-use construct from Plouffe et al. [10]. Ease-of-use represents "the degree to which [an innovation] is easy to learn and use" [1]. Visibility and result demonstrability constructs replace the observability construct in Rogers' model [1].

Visibility "is the degree to which an innovation is visible during its diffusion through a user community" as defined by Plouffe et al. [10]. Moore and Benbasat [10] define result demonstrability as "the degree to which the benefits and utility of an innovation are readily apparent to the potential adopter". Image represents "the degree to which the use of [an innovation] enhances one's image or status within the organization" [1].

Finally, voluntariness reflects "the degree to which the use of [an innovation] is perceived as being voluntary" [1]. Altogether, the PCI incorporates eight constructs: relative advantage, ease-of-use, compatibility, trialability, visibility, image, result demonstrability, and voluntariness.

The PCI has been used in IS research to predict intention to adopt of a variety technology (e.g. [10, 20, 21]). In a study on smart-card adoption among Canadian government employees, Gagliardi and Compeau [22] found that out of the eight antecedent constructs in the PCI model, seven were significant predictors to adoption intent. Only compatibility was not significant.

A study conducted by Agarwal and Prasad [20] used three constructs from the PCI model (usefulness, compatibility, and ease-of-use) along with additional constructs. They found that only compatibility predicted intention to adopt World Wide Web. In another study, Agarwal and Prasad [23] found that compatibility, trialability, visibility, and voluntariness had direct and significant effects on Internet usage, whereas the effects of relative advantage and ease-of-use were not significant. In another study on adoption of expert system application, Agarwal and Prasad [21] discovered that relative advantage affected intention to adopt significantly, while ease-of- use and compatibility did not.

Plouffe et al. [10] study found that among the PCI antecedent constructs, six – relative advantage, compatibility, trialability, visibility, image, and voluntariness – had significant effect on intention to adopt smart card-based payment systems. In that study, they used both the PCI model and the TAM and compared them. They found that the PCI model was superior over the TAM as it explained 45% of total variance compared to 32.7% for the TAM.

Compeau et al. [9] extended the PCI with three additional constructs. Compatibility was separated into three construct as proposed by Karahanna et al. [24]. These three reflect compatibility with preferred work style, values, and previous experience. Compeau et al. [9] defined the compatibility with preferred work style as “the degree to which the innovation is perceived as being consistent with the way the potential adopter would like to work, even if that is not the way they work now”, while compatibility with prior experience reflects “the degree to which the innovation is perceived as being consistent with the prior experience of potential adopters”. Compatibility with values is defined as “the degree to which the innovation is perceived as being consistent with the existing values of potential adopters” [9].

In addition, result demonstrability in the PCI was divided into two constructs, namely communicability and measurability. Communicability is defined as “the degree to which the result of using the innovation can be easily communicated to others”, while measurability represents “the degree to which the impact of the innovation can be assessed” [9].

Moreover, Compeau et al. [9] also re-conceptualized visibility in the original PCI termed as other’s use and defined as “the degree to which potential adopters are aware of the people using the innovation.” Using the extended PCI, Compeau et al. [9] examined the adoption of comprehensive hospital computer systems by non-physician employees. They found that several constructs significantly linked to each other, while relative advantage, voluntariness, and communicability were found to have a significant relationship to use intensity. However, other constructs (e.g. measurability, others’ use, image, compatibility with values) were revealed to have a significant indirect impact on use intensity. In the final model, Compeau et al. [9] dropped compatibility with preferred work style since the lack of validity of the construct. This made the extended PCI proposed by Compeau et al. [9] consists of 10 construct, namely: (1) relative advantage; (2) compatibility with prior experiences; (3) compatibility with values; (4) ease of use; (5) image; (6) communicability; (7) measurability; (8) trialability; (9) voluntariness, and (10) others’ use.

3 Research Design

3.1 Research Setting

e-Procurement has been formally adopted by the Indonesian government since April 2007 following up the Ministrial Decree of National Development Planning No. 002/MPPN/04/2007. Since that time, e-procurement has been implemented in the central government level, and gradually in the local government level. However, before the decree issued, several government agencies has used e-procurement in some extents.

In Indonesia, public expenditures account for 30% to 40% of total national spending. Even, in some government departments, public procurement expenditures may reach 70% of total annual budgets. Public procurement expenditure, therefore, is important, as are the sound processes and proper management that must accompany measures must be thoroughly implemented to reduce and minimize the potential for irregularities and misconduct [11].

According to Transparency International [11], in 2008, Corruption Perception Index of Indonesia is 2.6 (out of 10, 10 = no corruption, 0 = maximum corruption) which reflects perceptions of rampant corruption, but represents an improvement over its score of 2.3 in the 2007. Corruption that affects public procurement in Indonesia, involves a wide spectrum of individuals and organizations, including political leaders, judicial figures, senior administrators, and officials in procurement roles, as well as suppliers and contractors [25]. Several sources of figures indicate that between 10% to 50% of the procurement budget had been misappropriated (e.g. [26, 27]).

In Indonesia, the use of e-procurement has saved between 20% and 40% of the procurement budget of the central government from 2004 until 2006 [26]. Experience from the city of Surabaya (East Java) proved that e-procurement gave 50% savings for small contract and 23% for big ones [11].

The city of Yogyakarta, the study site, is known as student city and cultural city, with more than a half million population, where a rich blend of cultures from all corners of Indonesia meets. The government of Yogyakarta started to implement e-procurement system since March 2008. Since March until December 2008, 160 contractors/suppliers have been registered. Training for using the procurement systems have been held in December 2008 until January 2009. In the beginning of 2009, Yogyakarta was awarded by the Transparency International Indonesia as the cleanest city from corruption in Indonesia

3.2 Research Instrument

This recent study is considered as quantitative in nature. A questionnaire was developed as the main research instrument. Items in the questionnaire were based on those developed by Compeau et al. [9], as an extension of the PCI defined by Moore and Benbasat [1]. The 47 items was used to measure nine constructs, namely relative advantage (8 items), compatibility with prior experiences (4), compatibility with values (4), ease of use (6), image (4), communicability (4), measurability (3), trialability (6), and voluntariness (5). Other's use construct was excluded as when the survey conducted, e-procurement was in the early implementation stage. Use intention was operationalized using three items developed in this study. Each item was measured using 5-point Likert scale anchored by strongly disagree (score = 1) and strongly agree (score = 5).

As the questionnaire was already tested [9], we did confirmatory factor analysis to examine the validity of the questionnaire. The reliability of the questionnaire was measured using Cronbach's alpha. All analyses were done with help of statistical software SPSS. The confirmatory factor analysis unveiled that not all items were valid. Items with factor loadings less than 0.3 were dropped. Factor analysis was done using principal component extraction method and varimax rotation method.

Subsequently, using only valid items, reliability test was conducted. As the result, from 47 items represented nine constructs, only 24 items were valid and represented five constructs, namely relative advantage (8 items), compatibility with values (4), ease of use (5), measurability (3), and trialability (4). Compatibility with prior experiences, image, and voluntariness were dropped because the items used to measured respective constructs were unreliable as indicated by Cronbach's alpha less than 0.6 [28]. Descriptive statistics of the constructs and result of reliability test is summarized in Table 1.

Table 1. Descriptive statistics of the constructs

Construct	No. of items	Mean*	Standard deviation	Cronbach's alpha
Relative advantage	8	3.74	0.27	0.73
Compatibility with values	4	2.52	0.29	0.84
Ease of use	5	3.59	0.31	0.79
Measurability	3	3.20	0.35	0.77
Trialability	4	3.98	0.40	0.73
Use intention	3	4.12	0.49	0.81

Notes: Measured using 5-point Likert scale (1 = strongly disagree, 5 = strongly agree).

3.3 Sample and Data Collection

Respondents of the study were contractors/suppliers of the public procurement carried out by the city of Yogyakarta. The questionnaire was distributed to 130 contractors/supplier in the list who has attended e-procurement training, but only 90 who were willing to fill in the questionnaire, where 87 of them were valid for further analysis. The data collection was conducted in February and March 2009, both through face-to-face meeting and e-mail communication. However, several unstructured interviews with some procurement officials were also carried out to get a more complete picture of grand design on e-procurement implementation in the city of Yogyakarta. In addition, several unstructured interviews were also done to the contractors/suppliers.

Out of 87 respondents, 90.8% are male. Average age of the respondents is 30.6 years, with the vast majority (52.9%) of them age 25-30 years. The respondents with university level education account for 75.9%, while other has senior high school education level. As much as 62.1% of them are contractors, while the rest serve as suppliers.

The positions of 26.4% of the respondents are managers/directors, while other are staffs dealing with procurement in their firms. At average, the firms' age is 8.4 years, with 8 employees at average. The respondents have been being contractors/suppliers for government procurement for 7.1 years at average, ranging from 3 to 11 years. At average, they have used the Internet in supporting business for 6.7 years with online time 19 hours per week. Out of the respondents, 73.6% has used in e-procurement to participate in public procurement, while the rest have attended the training, but have never used it.

4 Results and Discussion

As can be seen in Table 1, with exception of use intention, scores for all construct are considered to be moderate. Even, the score of compatibility with values is less than

3.0, meaning that the respondents perceive that e-procurement does not fit with values they believe in. In the context of this study, the values might be manifest as permissive values to unethical business practices or even illegal ones, such as involving “the insider”, as procurement officials called, in giving uneven information or opportunity for all the contractors/suppliers, or making unethical deal between the contractors/suppliers that violates the level of the playing field.

In general, we might conclude that the respondents score the e-procurement somewhat positive as regards its relative advantage, ease of use, measurability, and trialability. However, intention of the respondents to adopt/use e-procurement systems provided is high as indicated by score of 4.12. Then, what factors affecting this use intention?

Table 2. Results of regression analysis

Construct	**Beta**	***t***
Relative advantage	-0.09	-0.70
Compatibility with values	-0.10	-0.78
Ease of use	0.13	1.04
Measurability	0.13	1.25
Trialability	0.41	3.12 *
Summary:		
F (9,77) = 5.40*	R square = 0.29	Adj R square = 0.23

Notes: * *p*<0.01

Table 2 shows the result of regression analysis. From five constructs, only trialability that affects use intention significantly in positive direction, while other four do not have direct significant effect on use intention. Since the implementation is in its early stage, relative advantage of using e-procurement is not persistent from the eyes of the contractors/suppliers. As stated earlier, despite the fact that 73.6% respondents has used in e-procurement to participate in public procurement, but they have participated only in one to three tenders.

Ease of use might not an issue in the adoption process, since the respondents have been using the Internet for several years. This is the fact that so far the e-procurement systems introduced is automation of conventional public procurement processes without any substantial business process changes. It is not surprising that the respondents that have got used with such the processes in the public procurement as they have been in the business longer than seven years at average will not find any significant difficulties in using the e-procurement systems.

Again, since the respondents have been acquainted with the e-procurement systems for a short time, the impact of it is still difficult to measure. This is might be of explanation why measurability is found to have no significant impact on use intention.

The only determining factor of use intention in this study is trialability. This might be associated with uncertainty inherent in the e-procurement systems because they have never used or have been used it in a short time. A cross-country study conducted by Hofstede [29] found that Indonesia is of countries with high score on uncertainty avoidance. He defines uncertainty avoidance as ‘‘the degree to which members of a society feel uncomfortable with uncertainty and ambiguity''. Adoption of a new technology involves risk and uncertainty. People in countries with a high score on uncertainty avoidance are more risk-averse and do not approve of making changes [30] and hence has a lower adoption rate to new technology/innovation [31].

Training conducted by the local government for the contractors/suppliers, then, could be considered as very influential in making them adopt the systems since they have opportunity to try the systems, and thus reduce the degree of uncertainty. Implementation strategy chosen that takes readiness of both the local government and the contractors/supplier into consideration should be appreciated.

However, trialability only explains 23% of total variance of use intention, meaning that there are other factors affecting the use intention in a larger power. Government's policy that forces to use the e-procurement systems gives the contractors/suppliers no choice. This factor might be the reason why the degree of use intention among the contractors/suppliers is very high as indicated in the interviews. However, since not all contractors/suppliers come with various internal capabilities, initiatives to leveling the playing field, such as ensuring equal information access and training should be well designed.

Table 3. Results of mean comparisons

Demographic variable	**Use intention**		*t*
	Low	**High**	
Age of firm	4.14	4.09	0.38
Procurement experience	4.20	4.01	1.76*
Size of firm	4.11	4.12	-0.11
Internet experience	4.15	4.09	0.60

Notes: * p<0.1

In searching of additional explanation of e-procurement use intention among the contractors/suppliers, several demographic variables believed to have impact on the degree of use intention are analyzed. The variables are age of firm, procurement experiences, size of firm, and Internet experience of the contractors/suppliers. Procurement experience is measured in years since a firm has participated in public procurement in the first time, while size of firm is measured using number of permanent employees. Internet experience represents how long a firm has been using the Internet, and is measured in years. Due to small variances in the data, all variables are converted into nominal scale with two categories (labeled as 'low' and 'high') using the mean as cut-off point. Table 3 summarizes the results of mean comparisons using independent-sample t-test.

As can be seen in Table 3, e-procurement use intention does not differ between younger and older firms, between smaller and larger firms, and between those with less and more Internet experience. But, we find that e-procurement use intention between the firms with a longer experience in public procurement is significantly less than those with a shorter experience. Resistance to changes among "the older players" might be higher than those "the new coming players" in public procurement. The change from conventional to e-procurement in some extent might be seen as a threat for the firms that have a longer experience as contractors/suppliers in public procurement. However, their use intention is still considered high as indicated by score greater 4.00. Condition where the policy of the government gives contractors/suppliers no choices other than adopting e-procurement might have a great impact.

5 Concluding Remarks

The recent study has examined the factors affecting the use intention to e-procurement among contractors/supplier of public procurement with special reference to Indonesian context. The study found that only trialability that has significant impact on use intention. The recent study conducted in the early stage of e-procurement implementation might of the explanations of the finding. The study also found that adoption rate among the new coming contractors/supplier is significantly higher than among the older players. This finding leads to an implication that the government should provide the contractors/suppliers a chance to try the e-procurement before they use it. Training on and giving comprehensive information about the e-procurement are among the initiatives might be carried to reduce uncertainty perceived by the contractors/suppliers.

Despite the fact that the government's policy has forced the contractors/suppliers to use the e-procurement systems, gradual implementation strategy that the contractors'/suppliers' readiness into consideration is of possible best option. However, it is possible that similar study that might be conducted in future when the contractors'/suppliers' e-procurement experience is more mature, will give different results and hence different ways will be required to deal with the situation.

Acknowledgement

The author would like to thank Tito Erza Laksana for his precious help during data collection process.

References

1. Moore, G.C., Benbasat, I.: Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research 2, 192–222 (1991)
2. Chen, H.: Digital Government: Technologies and Practices. Decision Support Systems 34, 223–227 (2002)
3. West, D.M.: Global E-Government 2006. Center for Public Policy, Brown University, Rhode Island (2006)
4. United Nations: Global E-Government Readiness Report 2005: From E-Government to E-Inclusion. United Nations, New York (2005)
5. Ministry of National Development Planning: Peraturan Menteri Tentang Pedoman Pelaksanaan Pengadaan Barang/Jasa Secara Elektronik. Ministry of National Development Planning, Jakarta (2007)

6. Dooley, K., Purchase, S.: Factors Influencing E-Procurement Usage. Journal of Public Procurement 6, 28–45 (2006)
7. Prier, E., McCue, C.P.: E-Procurement Adoption in Local Governments of the United States. Government Procurement, pp. 12–31 (2007)
8. Croom, S., Brandon-Jones, A.: Impact of E-Procurement: Experiences from Implementation in the Uk Public Sector. Journal of Purchasing & Supply Management 13, 294–303 (2007)
9. Compeau, D.R., Meister, D.B., Higgins, C.A.: From Prediction to Explanation: Reconceptualizing and Extending the Perceived Characteristics of Innovating. Journal of the Association for Information Systems 8, 409–439 (2007)
10. Plouffe, C.R., Hulland, J.S., Vandenbosch, M.: Richness Versus Parsimony in Modeling Technology Adoption Decisions - Understanding Merchant Adoption of a Smart Card-Based Payment System. Information Systems Research 12, 208–222 (2001)
11. Transparency International: Handbook for Curbing Corruption in Public Procurement, Berlin (2008)
12. Croom, S.R., Brandon-Jones, A.: Key Issues in E-Procurement: Procurement Implementation and Operation in the Public Sector. Journal of Public Procurement 5, 367–387 (2005)
13. Vaidya, K., Sajeev, A.S.M., Callender, G.: Critical Factors That Influence E-Procurement Implementation Success in the Public Sector. Journal of Public Procurement 6, 70–90 (2006)
14. Taylor, S., Todd, P.: Understanding Information Technology Usage: A Test of Competing Model. Information Systems Research 6, 144–176 (1995)
15. Kiiski, S., Pohjola, M.: Cross-Country Diffusion of the Internet. Information Economics and Policy 14, 297–310 (2002)
16. La Ferle, C., Edwards, S.M., Mizuno, Y.: Internet Diffusion in Japan: Cultural Considerations. Journal of Advertising Research, 65–79 (March-April 2002)
17. Harrison, D.A., Mykytyn Jr., P.P., Riemenschneider, C.K.: Executive Decisions About Adoption of Information Technology in Small Business: Theory and Empirical Tests. Information System Research 8, 171–195 (1997)
18. Mathieson, K.: Predicting User Intention: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research 2, 173–191 (1991)
19. Rogers, E.M.: Diffusion of Innovations, 4th edn. The Free Press, New York (1995)
20. Agarwal, R., Prasad, J.: A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology. Information Systems Research 9, 204–301 (1998)
21. Agarwal, R., Prasad, J.: The Antecedents and Consequences of User Perceptions in Information Technology Adoption. Decision Support Systems, 15–29 (1998)
22. Gagliardi, P., Compeau, D.: The Effects of Group Presentations on Intentions to Adopt Smart Card Technology: A Diffusion of Innovations Approach. In: Proceedings of the ASAC. Administrative Sciences Association of Canada, Windsor (1995)
23. Agarwal, R., Prasad, J.: The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies. Decision Science 28, 557–582 (1997)
24. Karahanna, E., Agarwal, R., Angst, C.: Reconceptualizing Compatibility Beliefs in Technology Acceptance Research. MIS Quarterly 30, 781–804 (2006)

25. Jones, D.S.: Public Procurement in Southeast Asia: Challenge and Reform. Journal of Public Procurement 7, 3–33 (2007)
26. Haswidi, A.: E-Tendering Will Improve Transparency, Official Says. The Jakarta Post (2007)
27. Anonymous: Corruption Ingrained in Procurement Processes. The Jakarta Post (2009)
28. Nunally, J.C.: Psychometric Theory. McGraw-Hill, New York (1978)
29. Hofstede, G.: Cultures and Organizations: Software of the Mind. McGraw-Hill, New York (1997)
30. Erumban, A.A., de Jong, S.B.: Cross-Country Differences in Ict Adoption: A Consequence of Culture? Journal of World Business 41, 302–314 (2006)
31. Batenburg, R.: E-Procurement Adoption by European Firms: A Quantitative Analysis. Journal of Purchasing & Supply Management 13, 182–192 (2007)

Session 3

Politics – Legislation – Regulatory Framework II

Studying the Interaction of the Epistemology in e-Government, Organization Studies and Information Systems

Vassilis Meneklis and Christos Douligeris

University of Piraeus, Department of Infomatics,
Karaoli & Dimitriou Str. 80, 18534 Piraeus, Greece
{bmenekl,cdoulig}@unipi.gr

Abstract. Although there are significant differences between Organization Studies, Information Systems and e-Government, certain boundaries between them have started to dissolve in the light of recent developments. Even though influences can be traced among all three concerning research results, epistemological interaction could produce interesting outcomes. In this paper we propose such an interaction in epistemology, and particularly in methods following the interpretive tradition, which has been notably underused. We present a brief review of literature in e-Government and after sketching its route, we propose ways to integrate in it perceptions and methods from Organization Studies and Information Systems.

Keywords: e-Government, epistemology, integrative approach, interpretivism, positivism.

1 Introduction

The last decades have introduced the discipline of e-Government as a central area of concern in matters of innovative public administration. E-Government's focus is strategically placed on both the fields of governmental organizations and of information systems technologies, without attributing primacy of one over the other. After almost three decades of evolution we feel that e-Government has mainly acknowledged the importance of the results of research in organization studies (OS) and information systems (IS), but it has not yet fully incorporated the epistemological insights of these two fields, whether they were developed independently or in conjunction to each other.

Although there are significant differences, in both scope and method, between OS and IS on the one hand and e-Government on the other, certain boundaries between them have started to dissolve in the light of recent developments in the three disciplines. These three disciplines form a triangle of interaction with each one affecting the other two. The interaction of OS and IS, and the influence between them has already been adequately studied [34]. According to Orlikowski and Barley, the fields of OS and IS have many points of intersection and the researcher who enmeshes himself in hybrid research in these points faces a great potential for the discovery of interesting and thought-provoking results. Nevertheless, they argue that the cross-fertilization of ideas

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 79–86, 2010.

in the two fields has not been symmetrical, with the field of OS being more influential to IS than the reverse [34 p. 146]. In this work we focus mainly on the interaction between OS and e-Government and IS and e-Government. We posit that e-Government research has mainly been influenced by research either from OS or from IS, but not simultaneously from both. We feel that the consideration of insights simultaneously from both OS and IS will enable e-Government scholars to be mindful of organizational as well as of technological particularities in their research, without favoring the former over the latter. Moreover, e-Government scholars seem to favor positivistic methods of research while a slim minority of them employs interpretive tools.

In this paper, we provide an account of our conceptualization of how e-Government researchers could benefit from adopting the epistemological positions that have driven the research efforts of their colleagues in OS and IS, and especially the ones that belong to the interpretive school of thought. By incorporating a more integrative approach (both epistemologically and methodologically) we feel that e-Government stakeholders will be able to explore interesting fields of knowledge that until now have been either underdeveloped or unexplored. The consequences of this endeavor will reflect on both researchers and practitioners. The first having access to more analytical tools and the second being provided with more inclusive implementation tools for e-Government information systems.

Employing more inclusive analysis and implementing more integrative information systems, that take into consideration apart from technical, social issues (such as citizen participation and knowledge diffusion) too, is expected to lead to the support of more direct, efficient and practically applicable implementations of e-Democracy.

The rest of the paper is structured as follows: Chapter 2 presents an integrative approach on the debate of positivism versus interpretivism and ties it with the concern of cross-fertilization of methods and ideas between OS, IS and e-Government; Chapter 3 provides a brief analysis of the literature in e-Government and explicates the main implications that can be drawn for the epistemologically integrative approach that is suggested in this work; Chapter 4 presents the conclusions of this paper.

2 Positivism and Interpretivism

The rhetoric of positivism versus interpretivism has been studied extensively in other works and in greater detail than this paper can afford. Scholars have devoted time and effort to explicate the significances of each approach and highlight the shortcomings of the other. In this work we do not opt for a detailed description of such a debate, but rather for an integrative approach on the matter, an approach that seems to be shared by other researchers as well [24], [42], [46]. Supporters of this thesis posit that the differences between positivism and interpretivism can be overcome by acknowledging their deeper ontological points of conformance, such as the quest for insightful results of situated cases and individually unbiased research.

In a similar vein, we suggest that positivist and interpretivist modes of research instead of being addressed as opposing each other can be addressed as supplementing each other. Where positivism can uncover causal relationships, interpretivism can highlight causal mechanisms [25]. In other words, positivism can help the researcher discover causal relationships between phenomena while interpretivism can help the researcher deeply probe into the dynamics of these relationships and uncover their mode of operation, their causal mechanisms. In this respect, the two approaches can supplement each other in any research that strives for completeness. As we will suggest shortly, e-Government and IS have been dominated by the positivist perspective, and thus, the application of interpretivist methods can greatly enhance research in these fields.

3 Analysis of e-Government Literature and Implications

To conduct this study of epistemology in e-Government literature we decided to focus on journals that were specifically involved in e-Government and public administration research and especially on papers that were tackling problems of e-Government implementations and initiatives. Even though a small amount of theoretical approaches has been included, this was done because of their clear exemplifying of the main trends in e-Government research, as we construed them. Leading journals on IS and OS were used as sources for works concerning the study of information systems and organizations in general, but they were not used as primary sources for research specifically in e-Government. Moreover, the thorough epistemological investigation of the IS and OS disciplines falls out of the scope of this work since extensive research on both fields has already been carried out.

The literature in e-Government has mainly evolved upon two axes: one based on technologies and services [2], [7], [13], [16], [26], [27], [30], [45], [48] and the other based on social and organizational considerations [1], [4], [9], [10], [11], [14], [17], [18], [19], [20], [31], [32], [39], [40], [41], [47], [49]. The contributions of these papers can be divided in three general strands; frameworks for evaluation, theoretical models for studying and understanding, and empirical studies with insights or guidelines for initiatives of e-Government. However, their methodological choices evidence a favor to positivistic methods of analysis. The majority of the reviewed papers that are based specifically on data analysis employ statistical tools and hypothesis testing for their studies [4], [10], [14], [16], [27], [30], [39], [45], [47], [48], with only two papers following a different method; one of them employs a survey based on workshops [17] and the other carries out an interpretive analysis [18].

This seems to follow the pattern of evolution of the IS discipline, when in its first phases IS scholars regarded positivistic methods as the only reliable tools to capture useful results [35]. As the discipline evolved, however, attention started being paid to interpretive methods as well [5], [6], [21], [43], [44] and eventually their role was acknowledged not as better than positivistic methods, but as providing different, equally interesting, insights to research. In its current stage, e-Government follows a similar route with the discipline of IS in its first phases. However, e-Government scholars can benefit from the experiences of their colleagues in IS and “skip” some steps of evolution, coming to acknowledge from these early stages the usefulness of interpretivism as an epistemological tradition.

Moreover, e-Government has borrowed from IS considerations for the technologies’ materiality. The structural features of technologies as they were created by the designers and developers provide influential drivers for the way that these technologies will be applied [8] in the everyday practice of the governmental organizations. IS research is particularly focused on technological particularities and the way technologies can influence business processes in organizations and in society in general. A major theme for e-Government research is the technological theme. In that light, research in e-Government can sufficiently benefit from advances in methodologies and tools in the IS field. Paradigms for development, architectures for information systems and models for evaluation and assessment are all of value to e-Government researchers, who have been drawing on such tools as they are being developed in the IS field.

However, e-Government IS are different, both in their scope and in the surrounding environment, from business IS and, thus, e-Government researchers have to modify the IS frameworks and models to satisfy the peculiarities of the public administration domain. At this stage though, it seems that e-Government is drawing on results from IS research while the reverse is not true. Publications in e-Government can be found to cite numerous papers from the IS field, but IS papers seem to bear little acknowledgement of the advances in e-Government. On a first thought, this is all too natural since, as far as e-Government IS is concerned, the field of IS is more general. Yet, the design and development of e-Government IS which must specifically take into consideration, apart from the usual, legal and policy parameters can provide novel ways to study IS in practice, based on situated data that are relevant to politics and particular to the field of public sector. These ways could extend the knowledge in the field of IS with factors which until now have not received so much attention or with new conceptual insights [15].

For instance, the works of Irani et al. [18] and Gil-Garcia and Pardo [12] although departing from different standpoints, rest on the same theme: how to implement in practice workable e-government information systems. Irani et al. [18] employ an interpretivist study of the process of e-Government evaluation. They highlight the importance of implementing such systems in order to provide practical gains that extend "outwards towards citizen groups – not merely doing so for the sake of technology change" [18 p. 162], thus bringing the user involvement and evaluation factor at the forefront of information systems implementation. This is an especially persistent requirement in the public sector where the implemented information systems are expected to render services to the major part of the population.

Gil-Garcia and Pardo [12] carry out a study of the relevance between practical tools and theoretical foundations that underpin the e-Government discipline. Their stated purpose is to enable more close relationships between research results and practitioner practices. The long-term goal of their work being the enabling of more theoretically informed implementations and, therefore, increased chances for workable e-Government information systems.

Both of these works can be used as exemplars for the incorporation and development of methods for investigating the theme of workable systems in the IS discipline. The omnipresent requirement of efficiency and practicality of initiatives in the e-Government discipline has sparked works that address these requirements. Hence, these works from the e-Government literature can provide the ground for further conceptual and methodological developments in the same vein in the IS discipline.

On the other hand, concerning the influence from OS, e-Government can benefit from institutional approaches [38] and, generally, theoretical perspectives on organizing [3], [36], [37], to adequately capture social and organizational diversities. Institutional perspectives can explain how institutions, norms and power asymmetries can affect technologies and their use; an account of these processes is often lost in analyses of e-Government initiatives who have been influenced by IS concepts, and thus, unfold at levels closer to the hardware. Institutional perspectives can help e-Government in departing from the technologically deterministic account of the relationship between governmental organizations and IS that the one-sided focus on technologies can bring.

The work by Gil-Garcia and Martinez-Moyano [11] unfolds an institutional study based on the concepts of systems of rules to rethink the politics and administration dilemmas. In their analysis they tackle the conceptualization of rules as mechanisms of behavior constrain, solution guiding and bi-dimensional nature to conclude that the designer of a system of rules "is a single actor who can unilaterally decide the components of the system of rules and its overall orientation" [11 p. 279]. The authors continue to suggest that this particular requirement must be relaxed in the specific environment of e-Government implementations where the solution to a problem is a conceptual construct generated by groups of public managers. Their work, hence, is an example of how conceptual constructs (such as the institutional perspective of ICT in organizations) from OS can be adopted by e-Government scholars and be reframed by the peculiarities of their research.

Furthermore, both diachronic and cross-sectional studies aimed at unraveling the relationship between ICT and governmental organizations can provide useful results. Particular to the e-Government discipline, studies have investigated the readiness of governmental organizations prior to developing e-Government information systems in order to provide fully integrated electronic services [22], [23]. These studies have developed a cross-sectional prism across the themes of strategy, technology and e-Government initiatives.

On a different level, the structurational perspective of technologies in organizations that has been proposed [8], [28], [29], [33] supports both diachronic and synchronic analyses and accords for the study of the reciprocal interaction between social structures in governmental organizations, technological features and everyday practices of the organizations' employees. Such topics of focus are essential for e-Government research when the concern is not limited to technological artifacts, but also on the enabling and constraining effect of institutions and the unfolding of social interactions in organizational settings.

4 Conclusions

In this paper we have developed the position that the cross-fertilization between OS, IS and e-Government can produce fruitful results to all three disciplines, but especially so in e-Government. Currently there seem to be streams of influence running in one direction mainly from IS and OS to e-Government, but not the other way around. Moreover, e-Government research is practically dominated by a positivistic epistemology as was experienced in the early stages of evolution of both OS and IS. However, these two fields have developed interesting interpretive schools, too, and our belief is that e-Government researchers can benefit from these schools by adopting them to the particularities of the research in their field.

If we are living through the transformation, both in form and in function, that many e-Government analysts identify, then researchers will need new tools to study advances in this process. We feel that the research results in more mature fields like OS and IS can provide such tools. However, we do not only support the application of ideas from OS and IS to e-Government, but also the reverse. Governmental particularities are invaluable sources of practical knowledge for the analysis of either organizational or technological phenomena.

References

1. Akther, M.S., Onishi, T., Kidokoro, T.: E-government in a developing country: citizen-centric approach for success. International Journal of Electronic Governance 1(1), 38–51 (2007)
2. Anttiroiko, A.: Building Strong E-Democracy – The Role of Technology in Developing Democracy for the information Age. Communications of the ACM 46(9), 121–128 (2003)
3. Blau, P.M.: A Formal Theory of Differentiation in Organizations. American Sociological Review 35(2), 201–218 (1970)
4. Burroughs, J.M.: What users want: Assessing government information preferences to drive information services. Government Information Quarterly 26, 203–218 (2009)
5. Checkland, P.: Systems Thinking, Systems Practice. Wiley, Chichester (1981)
6. Checkland, P., Holwell, S.: Information, Systems and Information Systems. Wiley, Chichester (1998)
7. Chen, Y., Gant, J.: Transforming local e-government services: the use of application service providers. Government Information Quarterly 18, 343–355 (2001)
8. DeSanctis, G., Poole, M.S.: Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. Organization Science 5(2), 121–147 (1994)
9. Dunleavy, P., Margetts, H., Bastow, S., Tinkler, J.: New Public Management Is Dead – Long Live Digital-Era Governance. Journal of Public Administration Research and Theory 16, 467–494 (2005)
10. Ghapanchi, A., Albadvi, A., Zarei, B.: A framework for e-government planning and implementation. Electronic Government, An International Journal 5(1), 71–90 (2008)
11. Gil-Garcia, J.R., Martinez-Moyano, I.J.: Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. Government Information Quarterly 24, 266–290 (2007)
12. Gil-Garcia, J.R., Pardo, T.A.: E-government success factors: Mapping practical tools to theoretical foundations. Government Information Quarterly 22, 187–216 (2005)
13. Guijarro, L.: Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States. Government Information Quarterly 24, 89–101 (2007)
14. Hammer, M., Al-Qahtani, F.: Enhancing the case for Electronic Government in developing nations: A people-centric study focused in Saudi Arabia. Government Information Quarterly 26, 137–143 (2009)
15. Heeks, R., Bailur, S.: Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. Government Information Quarterly 24, 243–265 (2007)
16. Ho, A.T.: Reinventing Local Governments and the E-Government Initiative. Public Administration Review 62(4), 434–444 (2002)
17. Irani, Z., Elliman, T., Jackson, P.: Electronic transformation of governance in the U.K.: a research agenda. European Journal of Information Systems 16, 327–335 (2007)

18. Irani, Z., Love, P.E.D., Jones, S.: Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government. Journal of Strategic Information Systems 17, 155–164 (2008)
19. Jaeger, P.T.: Deliberative democracy and the conceptual foundations of electronic government. Government Information Quarterly 22, 702–719 (2005)
20. Jefferson, T.I., Harrald, J.R.: Collaborative technology: providing agility n response to extreme events. International Journal of Electronic Governance 1(1), 79–93 (2007)
21. Klein, H.K., Myers, M.D.: A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. Management Information Systems Quarterly 23(1), 67–93 (1999)
22. Koh, C.E., Prybutok, V.R., Ryan, S., Ibragimova, B.: The Importance of Strategic Readiness in an Emerging e-Government Environment. Business Process Management 12(1), 22–33 (2006)
23. Koh, C.E., Prybutok, V.R., Zhang, X.: Measuring e-Government Readiness. Information & Management 45, 540–546 (2008)
24. Lee, A.S.: Positivist and Interpretive Approaches to Organizational Research. Organization Science 2(4), 342–365 (1991)
25. Lin, A.C.: Bridging Positivist and Interpretivist Approaches to Qualitative Methods. Policy Studies Journal 26(1), 162–180 (1998)
26. Mahler, J., Regan, P.M.: Developing Intranets for Agency Management. Public Performance & Management Review 26(4), 422–432 (2003)
27. Meijer, A.J.: E-mail in government: Not post-bureaucratic but late-bureaucratic organizations. Government Information Quarterly 25, 429–447 (2008)
28. Meneklis, V., Douligeris, C.: Enhancing the Design of e-Government: Identifying Structures and Modelling Concepts in Contemporary Platforms. In: Proceedings of the First International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), pp. 108–116 (2007)
29. Meneklis, V., Douligeris, C.: Technological Integration: Evidence of Processes of Structuring in Governmental Organizations. In: Proceedings of the Second International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008), pp. 16–23 (2008)
30. Moon, M.J.: The Evolution of E-Government among Municipalities: Rhetoric or Reality? Public Administration Review 62(4), 424–433 (2002)
31. Navarra, D.D., Cornford, T.: Globalization, networks, and governance: researching global ICT programs. Government Information Quarterly 26, 35–41 (2009)
32. Nour, M.A., AbdelRahman, A.A., Fadlalla, A.: A context-based integrative framework for e-government initiatives. Government Information Quarterly 25, 448–461 (2008)
33. Orlikowski, W.: Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. Organization Science 11(4), 404–428 (2000)
34. Orlikowski, W.J., Barley, S.R.: Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn From Each Other? Management Information Systems Quarterly 25(2), 145–165 (2001)
35. Orlikowski, W.J., Baroudi, J.J.: Studying Information Technology in Organizations: Research Approaches and Assumptions. Information Systems Research 2(1), 1–28 (1991)
36. Orlikowski, W.J., Gash, D.C.: Technological Frames: Making Sense of Information Technology in Organizations. ACM Transactions on Information Systems 12(2), 174–207 (1994)
37. Perrow, C.: A Framework for the Comparative Analysis of Organizations. American Sociological Review 32(2), 194–208 (1967)

38. Powell, W.W., DiMaggio, P.J. (eds.): The New Institutionalism in Organizational Analysis. University of Chicago Press, Chicago (1991)
39. Reddick, C.G.: Citizen interaction with e-government: From the streets to the servers? Government Information Quarterly 22, 38–57 (2005)
40. Silcock, R.: What is e-Government? Parliamentary Affairs 54, 88–101 (2001)
41. Strickland, L.S.: The information gulag: Rethinking openness in times of national danger. Government Information Quarterly 22, 546–572 (2005)
42. Trauth, E.M., Jessup, L.M.: Understanding Computer-Mediated Discussions: Positivist and Interpretive Analyses of Group Support System Use. Management Information Systems Quarterly 24(1), 43–79 (2000)
43. Walsham, G.: Interpretive case studies in IS research: nature and method. European Journal of Information Systems 4, 74–81 (1995)
44. Walsham, G.: Cross-Cultural Software Production and Use: A Structurational Analysis. MIS Quarterly 26(4), 359–380 (2002)
45. Wang, Y., Liao, Y.: Assessing eGovernment systems success: A validation of the DeLone and McLean model of information systems success. Government Information Quarterly 25, 717–733 (2008)
46. Weber, R.: The Rhetoric of Positivism Versus Interpretivism: A Personal View. Editorial Management Information Systems Quarterly 28(1), iii-xii (2004)
47. Welch, E.W., Hinnant, C.C., Moon, M.J.: Linking Citizen Satisfaction with E-Government and Trust in Government. Journal of Public Administration Research and Theory 15(3), 371–391 (2004)
48. West, D.M.: E-Government and the Transformation of Service Delivery and Citizen Attitudes. Public Administration Review 64(1), 15–27 (2004)
49. Wright, S.: Electrifying Democracy? 10 Years of Policy and Practice. Parliamentary Affairs 59(2), 236–249 (2006)

Session 4

Supporting Democracy through e-Services

e-Campaigning: The Present and Future

Sonali Batra

Georgia Institute of Technology
batra.sonali@gmail.com

Abstract. The practices of E-Campaigning are gradually gaining momentum in the world. This paper discusses the Democratic campaign of the 2008 American Presidential Election. It contends that the effective use of E-Campaigning techniques was the key to their success. It also deliberates upon the tremendous increase in public involvement over the Internet during the campaigning period. Also, it predicts the future of E-Campaigning and gives an in depth analysis of what the world can expect to see in future elections. Lastly, it examines the relation between E-Campaigning and E-Democracy in the context of the aftermath of the election.

Keywords: Election, Campaign, Internet, Barack Obama, John Mc Cain, YouTube, Facebook, Web Accessibility, E-Voting, Representative, Interaction, Web 2.0.

1 Introduction

The year 2008 brought with it a multitude of surprises for the American citizens. It will definitely be marked as one of the most volatile periods in American history. Apart from the stock market crash, for the very first time in American history an African American candidate- Mr. Barack Obama was elected president of the United States.

The 2008 Presidential Election was in itself very different from previous elections. For the first time since 1952, there was no president or vice president running for re-election [7]. Also, the Obama campaign was conducted in an unprecedented manner that reflects the true maverick nature of our newly elected president. The campaign unleashed the power of the Internet, making it the primary medium of campaigning. Traditional mediums like the television and radio were completely overshadowed. The Obama campaign was able to gather together an enormous supporter base using the Internet and was able to collect 500 million dollars in online donations from more than 3 million people [11].

There has been a tremendous rise in Internet use over the past decade. When George Bush was running for president in 2000, the use of the Internet was not so widespread. Dial up connections were still being used and broadband was almost unknown [7]. The situation is drastically different today. The Internet is the lifeline of most individuals and organizations. The Obama campaign was smart to notice this change and incorporate it wisely in their campaigning strategy. ‘Micro targeting’, i.e. reaching out to the voters individually, was made much more effective through the use of the Internet [7]. Another

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 89–98, 2010.

motivation behind Obama campaign's strategy was the nature of their target audience. The campaign primarily targeted the 'Youth Vote' – a factor which had been overlooked in previous elections. They correctly gathered that in order to get support from the youth, they had to speak to the youth in the language they understood the best, i.e. the language of blogs, forums and social networking sites. This move on the part of the Democratic campaign reaped enormous benefits. Given the tendency of the youth to get hugely influenced by their peers, an enormous supporter base was accumulated for Obama. Those who were a part of the campaign personally advocated Obama to their friends and family. The youth movement became the heart of the campaign and it was undeniably the reason for the Democrats' success.

Another factor that contributes to the 2008 Presidential Election being 'distinct' from previous elections was the tremendous involvement of the public in the democratic process. It is said that this was the election of 'public generated context' [7]. Through the use of blogs, forums, social networking sites and YouTube videos, the public shared their opinions and made their voices heard. Never before was it so easy to get involved in the democratic process. A person just had to make a video expressing her views and upload it on YouTube in order to be heard by millions of people. And the only cost involved was the video production cost [1], which is hardly anything. However, one downside to using this cost effective measure of being 'heard' was that the YouTube videos did not distribute themselves. Instead, they needed to be distributed through email or by links on blogs, forums and personal web sites [1].

In this paper we shall see how the recent American Presidential election of 2008 was a great example of E-campaigning. We shall also see what the world might expect from future elections. Sections 2 to 4 discuss the election whereas sections 5 to 10 discuss possible future trends in E-Campaigning. Lastly, Section 11 discusses the relation between E-Campaigning and E-Democracy in the context of the aftermath of the election.

2 The McCain Campaign

The 'YouTube Effect' was clearly manifest in McCain's campaign. The best example that illustrates this manifestation is the 'Celebrity' series of advertisements. The first 'Celebrity' advertisement made by John McCain's campaign appeared on television. It referred to Barack Obama as a celebrity and compared him to Britney Spears and Paris Hilton. The advertisement further questioned Obama's leadership ability. This advertisement was later pushed to YouTube and a series of accompanying advertisements, all ridiculing Obama's celebrity status and questioning his skills as a leader, appeared on YouTube as well. This 'Celebrity' series triggered the 'YouTube' effect and throughout the campaign, both campaigns were seen to respond to television and radio advertisements via YouTube [1].

3 The Obama Campaign

As mentioned earlier, the Obama campaign completely unleashed the power of the Internet. It started with Barack Obama announcing his candidacy online[7]. It ended with Obama being ‘Everywhere’ in the words of his own website. Facebook, MySpace, Twitter, Digg, Flickr, LinkedIn, Eventful, BlackPlanet, Eons, Glee, DNCPartybuilder, Asian Ave : Obama was ‘Everywhere’ [2].

3.1 Obama on Facebook

Barack Obama has an elaborate profile on Facebook and has 3,377,496 supporters. There are Obama pictures, videos, albums, personal notes and messages. His profile information adds the personal touch. It has information about Obama’s favorite movies, songs, hobbies etc.

3.2 Generation Obama

Generation Obama (GO) was the name of the nationally coordinated grassroots movement led by young activists with a simple goal of electing Barack Obama the next President of the United States of America [2]. It operated as follows. Obama supporters logged in to myBO (my Barack Obama) and created their profile. Following this they could enter their zip code and search for support groups near their location. Each group had an activity tracker. Members would receive email updates on the activities of the group. It was a great way to get locally involved in the campaign.

Another way to get locally involved was for the supporters to try and convince the voters living near their location to vote for Obama. Through the website, the supporters could get access to a list of 80 voters near their location. They would also be provided with a script i.e. what they would say when they tried to influence their votes. The supporters would ‘knock on doors’, say their scripts and report feedback to the website. When the election was approaching very close, the supporters also got the option to ‘make calls’ to voters on their candidate’s behalf. In the final 4 days of the campaign, volunteers on myBO made 3 million calls to voters mainly to ensure that people who favored Obama actually got out of the house and voted [11].

Other aspects of GO that were very enterprising were ‘Invite Your Friends’ and ‘Personal Fund raising’. Supporters would write a personal note to friends and family on why they were supporting Obama. They would load contacts from their personal address book asking them to join the campaign and to donate generously for the cause. Each supporter had a fund raising thermometer on their personal web page that depicted how much money they had raised and what was remaining. MyBO supporters' self directed fund raising efforts resulted in a donation of 30 million dollars from 70000 people [11]. This can be compared to Howard Dean’s 2004 campaign in which a large sum of money was collected using similar means [7].

The GO website also helped voters find their early vote or polling location online. The convenience provided effectively increased voter turnout.

3.3 Obama Mobile

The Obama campaign gave supporters the option to join the movement through their personal mobile phones. Supporters could sign up to receive text messages on their phone. Those who had signed up got periodic updates from the campaign as well as advance notices about local Obama events and important updates about Obama’s public appearances [2].

The campaign also provided a set of 12 Obama ringtones that the supporters could download into their mobile phones.

3.4 Obama on Twitter

Twitter is a free social messaging utility for staying connected in real-time. Through Twitter, people can frequently broadcast 140 character updates to everyone on their contact list. This is called ‘Micro Blogging’. The updates can be sent to the contacts’ computers, IM programs or cell phones.

Barack Obama sent regular Twitter updates to all his supporters who signed up for it. The updates reflected what he was doing or thinking.

3.5 Advertising in Video Games

As a part of their plan to target the youth vote, the Obama campaign took out advertisements in online video games. These advertisements were made on Electronic Arts (EA) XBOX 360 games like Burnout Paradise, Skate, Madden NFL 09, and 15 other games [1]. The advertisements were a cheap alternative to the traditional media and provided the ability to target the specific group of males in the 18-34 age groups. They focused mainly on voter registration and early voting.

4 Public Involvement

The 2008 Presidential Election saw an unusual increase in public involvement in the democratic process. Through email, blogs, forums, personal web sites and YouTube videos, people exchanged information, shared their views and made their voices heard. In particular, the campaigning period was marked by a plethora of citizen initiated campaign videos.

4.1 Vote Different

The ‘Vote Different’ video was put up on YouTube by an activist who wanted to influence people to vote for Barack Obama instead of Hilary Clinton. It became one of the most ‘viral’ videos of the campaign and was viewed by an estimated number of 5 million people [10].

4.2 Obama Girl

The ‘Obama Girl’ videos on YouTube were a huge sensation and had an estimated number of 12 million views worldwide [10]. In the initial video ‘Obama Girl’, wearing hot pants, danced and sang in public streets while proclaiming her undeniable infatuation with Obama and extolling his virtues. This was followed by more than 30 accompanying videos during the course of the campaign[10]. It is needless to say that the videos did wonders for Obama’ campaign.

5 The Future of e-Campaigning

It is quite probable that novel and breakthrough technology would be invented that would define E-Campaigning in the future. However, it is more probable that existing technology would be put to more innovative uses. This is exactly what the Obama campaign did. They did not reinvent Facebook. Instead they completely unleashed the power of the web as it exists today and used it as the primary force behind their campaign. The future harbingers a complete migration of election campaigning to the World Wide Web. However, before this complete shift can take place, a few accessibility issues need to be taken care of. We need to ensure that each and every person has access to the Internet. Further, we also need to ensure that everyone has access to web content. As we shall see in further sections, Internet access does not automatically imply Web Accessibility.

6 World Internet Usage Statistics

The following statistics have been taken from internetworldstats.com [3]. The statistics are for June 30, 2008. The Internet penetration rate of North America is 73.6%. This is good but not enough to ensure a complete migration to the Internet. However, according to the same source, North America's usage growth has been 129.6% from 2000-2008.On interpolating this, we see that the prospects are good. Internet Usage shall rise further in the coming years and this shall largely increase the scope of E-Campaigning in the United States.

As far as developing countries like India and China are concerned, the future of E-Campaigning is not so bright. Even though the largest number of Internet users are in the continent of Asia, Asia lags far behind North America, Australia and Europe when we look at Internet penetration rates. Usage Growth from 2000-2008 has been 406.1% which is excellent, however there is a lot of catching up to do and people in these countries shall have to wait for years before they experience fully unleashed E-Campaigning.

Meanwhile, they should use the same tactics discussed in this paper for enhancing campaigning but in an offline environment, if possible. For example, many of the myBO methods like 'Personal Fundraising' and 'Invite Your Friends' can be implemented by making use of the cellular network.

7 Providing Web Accessibility for Everyone

The main goal of Web Accessibility is to make it possible for everyone to use, understand and communicate using Web based resources, despite any disabilities or technological restrictions [4]. There are a vast number of web users that have special needs that need to be addressed by developers while making web sites eg. people having motor disabilities and visual or auditory impairments. Older readers are a very fast growing group of such web users. They have to use assistive technology like screen readers and alternative devices in order to comprehend web content. The web sites need to be developed in such a manner that they are compatible with these devices.

In general there is a lack of knowledge among developers about existing techniques for supporting development of accessible web applications. The W3C (World Wide Web Consortium) promotes the development of guidelines for accessible web content. The WCAG (Web Content Accessibility Guidelines) document contains some such guidelines [9]. However, by and large developers are not aware of them.

A screen reader is a software application that attempts to identify and interpret what is being sent to standard output irrespective of whether a video monitor is used or not [4]. This interpretation is then re-presented to users with text to speech, sound icons or a Braille output device. It is of tremendous use to the blind, visually impaired, illiterate or learning disabled people. But if web pages are not designed properly, they are interpreted wrongly and thus become inaccessible. For example, if a web pages consists of images but the images do not have alternative text supporting them to describe what the image depicts. The screen reader cannot read the images, it can only read alternative text. In such a scenario, a lot of information is lost. A screen magnifier used by older readers to magnify the text on their computer screen is another example of assistive technology that does not work with badly designed web page.

Another way of enhancing web accessibility is to provide instructions within a web application for non techno-savvy users [8].

8 e-Voting

E- Voting is the process by which voters can vote via the Internet while sitting in their own homes. If this were legalized, it would be a huge stimulus for people to cast their votes. This process may be advocated by future campaigns in order to maximize voter turnout. However, there are many issues with Evoting that need to be fixed before it can legally be adopted. Some of these are authentication problems, secret ballot support, database security and the prevention of Denial of Service attacks on the Internet [5]. There might come a day when all these issues are effectively addressed and then the world would finally experience the convenience of E-Voting.

9 Representative Interaction Websites

Obama's campaign made effective use of existing web technologies to accumulate a large supporter base and collect millions of dollars from online donors. However, what it lacked was an effective method by which supporters could interact with their chosen representative. No such feature exists on the GO website. There is a website called 'community counts' that has been collecting text and video questions for the presidential candidate. People have access to these questions and they can vote these questions 'up' or 'down'. This shall ensure that the most popular questions be answered by the candidate in due time. The idea is good but there are lots of drawbacks to this websites. Firstly, it seems like a black hole where questions keep getting posted and voted upon but there is no feedback from the candidate. The 'Questions' tab has over 600 pages. The 'Answers' tab is blank. Secondly, the formatting and layout of the website is very confusing. It appears congested and is complex to comprehend.

A website that shows more promise in this area is 'change.gov' which is Obama's transition web site. It is a part of Obama's team's effort to create an online platform that provides a measure of interactivity. Along with many other features, it has a tool called ' Open for Questions'. It allows users to submit questions and vote on the ones they want answered the most. It is promised that the most popular questions would be answered on a regular basis. 'Open for Questions' is not taking any more questions as of now,i.e.13th Dec 2008. Also, 'Voting for Questions' closed on 12:00 am on 12th December and will reopen next week. Though this website seems much more reliable than the previous one, it still does not provide a high measure of interactivity. Although it is certain that questions will be answered on a regular basis, there is no guarantee that `all` the popular questions will be addressed. The questions are not there on the site any more with their user votes. When Obama's team releases a list of answered questions, they will have a hard time proving that they have answered all popular questions. Also, the time gap between question submission and answer provision is a bad idea and it gives citizens an impression of unresponsiveness. A better idea would be for the future President to regularly answer one or two questions that he feels are the most important. He could avoid answering the ones that are repeated.

However, whatever its shortcomings are, this tool at least sends the message across that the new government is trying to be interactive and is aiming for transparency. No such tool was present during the campaigning period. It can be that the team recently came up with the idea. However, had the tool been there for the campaigning period as well, it would had definitely added a lot to the force of the campaign.

A better idea of creating an online interactive platform would be to use a forum. An Internet forum is an online discussion site. It is like a message board where users post their messages. Citizens could post their questions for Obama on different threads of the forum. Other people could comment on the question as well and in due course, the question would be answered on that thread itself. It is definitely a much more interactive solution than just putting all questions into a black hole and awaiting replies.

However, there are many maintenance problems in an Internet forum. In 'Open for Questions' the only thing Obama's team had to worry about was the scalability issue, i.e., would the tool be able to handle such a huge number of questions. If they decide to use a public forum, they will have a lot more to worry about. There can be a number of antagonists trying to create mischief on a forum eg. Trolling, spamming, double posting etc. This shall need to be taken care of on a regular basis.

A recent graduate project at Georgia Institute of Technology addresses this problem of creating an effective, self maintaining representative interaction website. The website is called 'SoapBox'. In this website, the notion of self maintenance is achieved by having members vote on the messages as well as on the following comments. The idea is that messages that receive the highest votes automatically trickle to the top thus it achieves auto filtering of irrelevant content. Also, there is a concept of 'User Karma'. Users that receive more votes have higher karma than the ones who receive less. In fact, each user has a profile page that contains various information about the user including his karma. This way, if someone asks a question and user A comments on it, the person can know how reputable user A is by looking at his karma. Future work on this site is to add functionality that gives the users with highest karma administrative powers i.e., they can periodically delete irrelevant messages and comments from the site. Thus the site shall become fully self maintaining.

Another feature of this site that is very innovative is submission to the site via an in browser button, apart from the traditional mode of submission that is logging in to the site and submitting a message eg. If a user comes across some news item in a website that she wants to discuss with a candidate, she selects the text that she wants displayed in her message and clicks on an in browser button. She is redirected to the 'SoapBox' submission page in which the message title and message body is already filled in for her. The message title is the title of the previous page she was at and the message body is the text she selected on that page. All she has to do now is submit. Auto login is done for her so that she might submit. More future work is to enable the user to enter her zip code. This way users will be able to get categorized into their respective constituencies automatically. This will make it easy for the representative to address the questions of people from her own constituency. More future work in this area is to add support for a 'Representative' page where each representative's profile shall be displayed along with the most popular questions directed towards her and her answers to them.

Even though this site is meant for interaction with the 'elected' representative, it can be used for campaigning as well. As we see, the process is completely transparent and it provides an extremely high measure of interactivity.

10 Web 2.0 Technologies

Web 2.0 describes the changing technology of the World Wide Web. The term does not refer to an update to any technical specifications but rather to changes in the ways software developers and end users utilize the web [4]. Earlier, web site users could just view the websites. Now using web 2.0 technologies they can add value to a site as they use it. Web 2.0 technologies refer to the web as a 'participation' platform [4]. We shall see a lot of Web 2.0 technology being used for campaigning and governance in the future. Some Web 2.0 technologies that show a very high promise of featuring in future campaigns are as follows.

10.1 Web Feeds

A web feed is also called a news feed. It is a data format used for providing users with frequently updated content [4]. Web feeds are very useful as they provide users with a summary of the website's latest added content eg. Latest news or forum posts. This shows great promise of being used in future campaigns to keep users updated of the latest campaign activities.

10.2 Wikis

A wiki is a page or a collection of web pages that allows anyone who accesses it to contribute or modify content using a simple markup language [4]. It is used to create collaborative websites and to power community websites. A potential use of this in campaigning can be during fund raising. All the fund raisers can have a shared Excel page among them to which they regularly put their updates. The document shall automatically total the total sum of money raised and maybe it could notify them and other users of updates through RSS feeds. It would be a great way of keeping track of money raised.

10.3 Mashups

A mashup is a web application that combines data from more than one source into a single integrated tool. e.g. the use of cartographic data from Google Maps to add location information to real estate data, thereby creating a new and distinct web application that was not originally provided by either source [4]. Mashups provide a tremendous scope for making very innovative web applications. We may see some mashups in future elections for representative interaction or other such applications.

10.4 Folksonomies

Folksonomy refers to collaboratively creating and managing tags to annotate and categorize content [4]. An example is the very popular website 'Delicious' [6]. Folksonomies are an alternative to searching the web via traditional search engines. The argument in favour of them is that instead of viewing a list of url's that the search engine's algorithm pulls up, one can see the most popular url's matching one's search criteria. It greatly improves how people discover, remember and share on the Internet. A website like delicious that caters solely to political content would be a great addition to the World Wide Web and also to the world of E-Campaigning.

11 e-Campaigning and e-Democracy

Obama's team is continuing its E-strategy for governance as well. Our new President Barack Obama is very technosavvy and firmly believes in the power of technology. It is rumored that he wants to have a laptop in his Oval Office, and if it is true, he shall be the first president to do so. People have already started talking about 'White House 2.0' and what changes and innovations it shall bring.

As mentioned in section 9, before Obama was elected as President there was a website called 'community counts' that was collecting questions for the presidential candidate. The day after he won the election, Obama's transition team launched a new interactive website -'change.gov'. This website was taken down on Inauguration Day, i.e. 20th January and was replaced by a new website- 'whitehouse.gov'. This site does a good job of ensuring transparency of the functioning of the government. Some of its features are as follows. It contains a weekly video address that President Obama intends to publish every Saturday morning. It has a list of legislations signed by the government that is continuously being updated. There is also text and video information about the new legislations. There is a section 'Presidential Actions' that contains the official actions by the President that do not require legislation or congressional approval [12].There is a list of nominations and appointments made by the president ever since he started his presidency. There is a blog through which ordinary people can express their views and concerns. There is a media center that has videos and slideshows about Obama events and public meetings. Lastly, all Obama speeches, remarks and press briefing are there on the website.

There is another community website-'serve.gov'. It is an online resource by which people can find as well as create volunteer opportunities in their community. It aims to meet growing social needs resulting from the economic downturn [13].

Thus we can see that the E-Campaigning tactics used in the 2008 American Presidential Election have definitely led to the enhancement of E-Democracy in the United States. And this is not the end. Thanks to the efforts of the supporters of myBO, Obama's team has now accumulated a huge database on US voters [11]. This information can be used to involve citizens in the governing process in many ways.

12 Conclusion

Thus we have seen how the Internet played a major role in the 2008 American Presidential Elections. Future campaigns are expected to use this as an example of effective campaigning. Many more innovative E-Campaigning techniques are expected in the future. An in depth analysis has been made of what trends might be manifest in future E-Campaigns. Lastly, the relation between E-Campaigning and E-Democracy has been examined in the context of the aftermath of the election.

Acknowledgment

I am very grateful to Professor Mike Hunter for the excellent guidance given by him, without which this paper would not have been possible.

References

1. How the Internet Changed Campaigning by Eric Sembrat featured in The Georgia Tech FIREWALL, November 21 (2008)
2. Generation Obama website, `http://www.go.barackobama.com`
3. Internet World stats website, `http://www.internetworldstats.com`
4. Wikipedia website, `http://www.wikipedia.com`
5. Paul, N., Evans, D., Rubin, A., Wallach, D.: Authentication for Remote Voting, `http://www.cs.rice.edu/~dwallach/pub/remote-voting2003.pdf`
6. Delicious website, `http://www.delicious.com`
7. Graff, G.M.: Blog Entry on Washingtonian.com website: Smile You’re on YouTube, `http://www.washingtonian.com/blogarticles/people/capitalcomment/5840.html`
8. Blog Entry in Brian Swartzfager’s Blog: Techniques for Providing Instructions within Web Applications, `http://www.swartzfager.org/blog/index.cfm/2008/1/22/Techniques-For-Providing-Instructions-Within-A-Web-Application`
9. Mankoff, J., Fait, H., Tran, T.: Is Your Web Page Accessible – A Comparative Study of Methods for Assessing Web Page Accessibility for the Blind. ACM Digital Library
10. YouTube, `http://www.youtube.com`
11. The E-Campaign:Rallying Volunteers and Voters by David Talbot featured in ejournal USA, Nonviolent Paths to Social Change (March 2009)
12. The Presidential Website, `http://www.whitehouse.gov`
13. `http://www.serve.gov`

e-Democracy: The Political Culture of Tomorrow's Citizens

Triantafillou Vasilis and Kalogeras Dimitris

Telecommunications Systems & Networks Department,
Technological Educational Institute of Messolonghi, Nafpaktos Branch,
Nafpaktos, Greece
triantaf@teimes.gr, dkaloger@teimes.gr

Abstract. The aim of this study is to investigate how Internet influences the political-social behavior of the members of the School Community. In order to do so we questioned students (tomorrow's citizens) and teachers of secondary schools and analyzed their understanding about e-democracy issues. The research is held by the department of Telecommunication Systems & Networks, Nafpaktos Branch of the Technological Educational Institute of Messolonghi with the participation of students and teachers from the Region of Western Greece. It was observed that Internet offers new possibilities for people's participation in the political process. The results show that students feel more confident against technology and Democracy in contrast to their teachers.

Keywords: e-democracy, e-voting, e-participation.

1 Introduction

Democracy has proven to be an exceptionally adaptive form of government through time. Its form has changed, from the homogeneous city-state in its direct form to multinational big-state in its representative form. The role of participants and the way of participation has been altered, from a small number of men, relatively old, to a big number of free citizens including men and women. All this period, democracy is still founded on several basic rules: equality of citizens, participation in common affairs, freedom of speech, the right of assembly and the responsibility of governors.

The effect of Information and Communication Technologies (ICTs) in politics and democracy and the role of students (tomorrow's-citizen), is highly relevant to the ability of offering catholic access to the Internet [10]. However, catholic access on its own is not enough. "If citizenship means catholic access, democracy needs reliable channels of information and public dialogue (deliberation) if is to flourish" [4]. Human's interaction is more important than the technological infrastructures.

What characterizes human communities in a globalised society today is their common interests and concerns. Virtual communities, blogs, digital cities form new social structures that function with the use of network technology. Their organisation and

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 99–107, 2010.

their way of operation herald e- democracy. Due to the growth of communities, digital cities of the future will not have only geographic characteristics but also space-time ones. Consequently a new form of "redeployment of" the population of earth emerges, and one of the main issues will be how current representative democracy corresponds to new digital social structures. Democracy will we forced to redefine who can participate, the form of participation and how this will be utilised.

The definition of the term “e-Democracy” depends on the political culture of societies and the application scale (locally, nationally or globally). It is likely that nations will learn from each other while developing new practices towards this direction, international comparisons and standardised methods of evaluation. We can define e-Democracy as "Direct Operation of Democracy" [1].

"E-Democracy, aims to define the system components that will support increased participation of citizens, in the political process". It can not only be seen as a substitute of traditional democracy but as the communication, presentation and support of public interest and the decision-making through public dialogue and voting. Decentralization - a condition essential for the realization of direct participation that affects positively the political process - can be minimized strengthening the role of individuals, democratic control, transparency of processes and plurality [7].

The basis of democracy is an informed and active citizen. Many governments are positively activated towards developing the digital means for distributing information to the citizens. There is a lot of space to cover in order to "engage actively" citizens to influence world politics though the use of digital means. These facts include the most ignored side of e-Democracy, the strategic side.

1.1 Aim

The main aims of our study were to investigate: a) How Internet influences the political and social behaviour of students of secondary schools and b) How tomorrow's citizens realize the concept of e-Democracy. At the same time we conducted a comparative study based on the answers of students against those of their teachers.

2 Method

The utilization of our questionnaire was based on the use of open source software in order to implement a web based application to facilitate access independent from location of the users and immediate storage of the results. We developed a client server application, through the use of PHP and MYSQL.: http://noc.tesyd.teimes.gr/erotimatologia.

The home page includes information material about the methodology approach followed and the questionnaire used both for teachers and students. The users were granted access through a username, password mechanism. Passwords were issued, independently, upon request and registration for each school.

Our sample constituted of 722 of High school and Lyceum students and 102 public and private teachers from public and private schools of Western Greece. Data were stored in a mySQL database and SQL queries were used to analyse the results.

2.1 Data Collection

The questionnaires for students and teachers consisted of four parts. The first part was comprised of a set of personal data and data about the usage of Internet. The second includes questions about how students and teachers conceptualize e-democracy, e-government and the use of Internet in the political and social process. In the third part our aim is to obtain results of how the users react against means of participation similar to applications of e-Democracy. Finally, the fourth part includes questions about the challenges of e-Democracy, and generally Information and Communications Technologies in the new digital and social structures.

2.2 Data Analysis

In order to analyze how Internet affects the political and social behavior of students we investigated: a) the percentage of students which have access to Internet b) the relationship between accessibility of Internet and the educational level of their parents and the region they live, c) how many students have utilized Internet to participate in an e-voting process or use any means of communication with public delegates of services or visit a public institutions web site and obtaining information.

In order to analyze how today's students and tomorrow's citizens conceive e-Democracy we investigated: what in their opinion are the positive and negative issues, what are the possible challenges e-Democracy applications will face in the future.

Our comparative study of how students understand and realize the different issues against those of their teachers, we investigated: a) the use of e-democracy applications: e-voting, participation in forums, information retrieval from governmental web pages e.t.c.. b) The use of services that is related with subjects of e-Democracy and the factors that influences them. c) The different perspective of students and teachers.

3 Results

In the following section we present the analytical results of our study:

3.1 The Effect of Internet on Students and the Factors That Influence It

We present here the effect of Internet on students based on their availability to access Internet, the factors that govern it and the tendency of students to use e- Democracy services.

3.1.1 Student Access of the Internet

The 72% of the students have access to the Internet. From the above percent the 54% have access from home, the 22% from school and the 18% from an Internet cafe. The reasons reported which probably that are responsible for not having Internet access are the failure of purchasing a computer (43%), the absence of interest (16%), the limited or no knowledge of using the Internet (14%) and the cost (10%).

It is obvious that the percentage of students with Internet access is by far bigger than what is reported in the total population. This familiarization of students with

Internet produces a positive prospect for tomorrow's citizens/users and emerges an increasing tendency for the use of Internet services.

3.1.2 Factors That Influence the Access of Students to the Internet

The educational level of parents plays an important role on the percentage of students that access Internet. 44% of the students that their parents are graduates of Primary school have Internet access, (the 23% of them from home), 68% of those whom their parents are graduates of Secondary school, (the 29% of them from home) the 87% of those whom their parents are holding an University Degree (the 44% from home) and the 97% from those whom their parents have completed postgraduate studies (the 62% from home).

The place of residence also influences Internet access of students. From those that live in a city (up to 3.000 residents) access have the 48%, (the 24% from home), the 73% from those that live in a town (from 3.000 up to 15.000) (33% from home) and the 81% in cities above 25.000 residents (the 40% from home).

Summarising, students which their parents have obtained a Higher education degree seem to have a greater percentage of Internet access and mainly from their home. The students that are residents of cities appear also to have increased accessibility to Internet. School seems to be able to help in covering these differences through computer laboratories and information technology courses since they are available for all students.

3.1.3 The Tendency of Students to Use e-Democracy Services

Participation of students in e-voting applications, use e-mail in order to express their opinion and visit governmental web pages to retrieve information are the main e-democracy applications reported.

In diagrams 1 and 2, we present the percentage of students that participated in e-voting applications, sent an e-mail to express their opinion or visited a governmental web page. In diagram 1 the applications are derived based on the educational level of their parents and diagram 2 based on the place of residence.

These diagrams suggest that the use of e-dem services, from tomorrow’s citizens, is relevant to the educational level of their parents and their region. It is clear that these students are favourable candidates to easily become familiarized and actively participate in future e- Democracy services and systems. However strong doubts arise from the possibility of exclusion of social groups with low level of education or citizens of remote regions thus failing to support one of the main objectives of e-Democracy which is the increase of active participation of citizens in the political decision-making process.

3.2 Students Opinions for e-Democracy

In this section we focused on the answers of students about what are considered to be the positive and the negative consequences of the application of e-Democracy and how they realise the challenges of e- Democracy.

3.2.1 Positive Repercussions of e-Democracy

In the question "In which of the following questions the exploitation of technologies of e-Democracy can have positive results", the choices of students were categorized as follows: a) More rapid and reliable benefit of services and information from government owned institutions (29%). b) More direct and bigger participation of citizens in the process of decision-making (27%). c) Enforcement of democratic processes and consequently Democracy (21%). d) Continuous feedback of government with the opinions of citizens 16%.

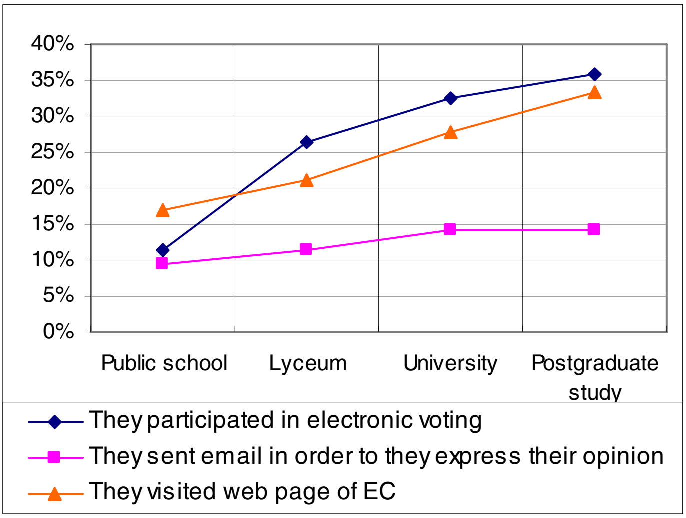


Diagram 1. E-dem applications used based on the educational level of parents

3.2.2 Negative Consequences of e-Democracy

Students were called to answer to the following questions: "In which of the following questions the exploitation of technologies of e-Democracy can have negative consequences". a) The creation of an impersonal e-citizen and e-state (36%), b) The division of citizens in "digital" and "traditional (25%), c) The use of technology from the government in order to reform politics (20%), d) The weakness of the government to correspond and due to that the minimization of participation. (The problem of scale) (17%).

3.2.3 Realisation of the Challenges of e-Democracy

The students realise the possible challenges that can rise from the growth of e-Democracy through answering the following question: "What do you believe that they will be the bigger challenge for the e-Democracy" and they rated their answers as follows: a) The growth of technology thus being accessible by all (29%). b) The electronic activation of citizens (28%). c) The familiarization of citizens with the new ways of participation in decision-making (24%). d) The adaptation of governments in forming politics(14%).

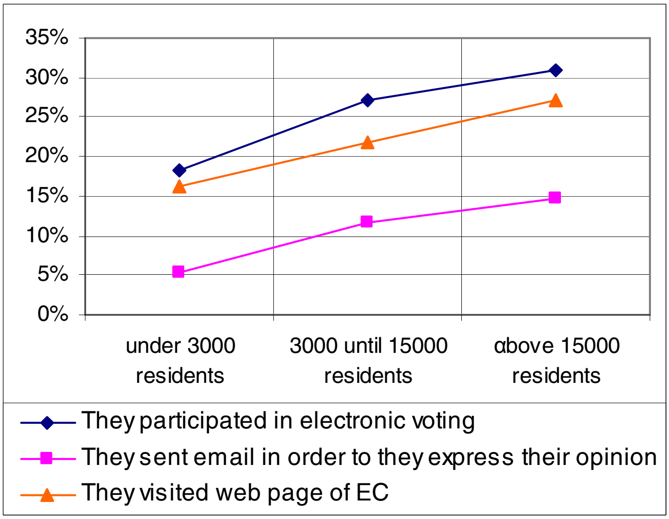


Diagram 2. E-dem applications used based on the place of residence

3.3 The Opinions of Students Opposed to Those of Their Teachers

The comparative analysis of opinions of teachers against the opinions of students where deducted on subjects that concern the use of Internet in daily life, their participation in e-voting, and their opinions about e-Democracy from those who have Internet access and those who do not .

3.3.1 The Familiarization of Use of Services of Internet in the School Community on Issues e-Democracy

The students use the Internet mainly for recreational reasons, but show big interest for e-voting. On the contrary, they don't use it for economic transactions and for purchase of products, as their teachers to mostly. Both students and teachers use the Internet for searching information and communicating by email. In the question concerning participation in Internet e-voting students appear to have participated more than their teachers.

Table 1. Answers of students and teachers, which have access in the internet, in the question: What are the reasons you use the internet

	Students	**Teachers**
Participation in forum discussions	29%	52%
Entertainment	79%	43%
Communication with e-mail	52%	89%
Economic transactions	1%	58%
Purchase of products	2%	59%
Search for information	57%	84%
Have you participated in voting via the internet?	46%	20%

3.3.2 How Do You Believe or Intend to Use e-Democracy in the School Community

The tendency of students and teachers to use services related with e-Democracy and the factors that influence their answers justify their perspective for an age of digital politics and democracy.

Table 2. Answers of students and teachers which have access to internet, in the question: Do you believe that our society is mature enough to accept e- Democracy applications

	Students	Teachers
YES	39%	29%

Students but also teachers that do not have access to Internet, consider in a high percentage that our society is not mature to accept e- Democracy applications.

3.3.3 The Perception of Students and Teachers for e-Democracy

Students and teachers that have access to Internet (Table 3) conceive the dynamics of new means of communication and intervention and they believe that e-Democracy will strengthen the role of citizens and government. On the contrary students and teachers that do not have access to Internet (Table 4), realise in e- Democracy the parts that are more familiar to them.

Table 3. Answers of students and teachers, which have access to internet, in the question: What do you believe is e- Democracy

	Students	Teachers
The strengthening of Democratic processes through the use of new technologies	29%	26%
The strengthening of the role of citizens and government with the use of ICT	33%	42%
Electronic deliberation of citizens with government organizations (delegates, public services and organisations)	26%	23%
e-voting and e-polls	9%	7%

Table 4. Answers of students and teachers, which do not have access to internet, in the question: What do you believe that e-Democracy is

	Students	Teachers
The strengthening of Democratic processes through the use of new technologies	10,81%	0%
The intensification of role of citizens and government with the use of ICT	17%	5%
Electronic deliberation of citizens with government owned institutions (delegates, public services and organisations)	6,49%	10%
e-voting and e-polls	54%	75%

The results of the research confirmed the existence of the “digital gap”. The answers between those having Internet access and those not having Internet access have a distinct difference. A challenge for those that have Internet access is to assure that students - tomorrow's citizens - will participate actively in a new Digital Democracy. The design and development of actions to enforce knowledge acquisition about e-participation is a very important issue in order to engage young people in a democratic decision-making process. Young people are familiarized with the use of technology, vote on line, chat rooms and potentially in the electronic expression of their opinions.

The challenge is the design and implementation of advanced services in such a way to support the exchange of opinions and to produce logical arguments and political thesis. Success of e-Democracy, according to the answers of the persons familiar with Internet, will be based strongly on the preparation of ICTs in order to encourage and familiarize citizens with public subjects, to hear and to participate in a number of forums. The need for acceptable and reasonable information will provide the spark for dialogue and solid opinions.

Education can help in enhancing public reason, and consequently in the intensification of participation. Such educational tools would offer the ability of young citizens to experience and understand the process of democratic decision making [8]

4 Conclusions

ICTs are part of the current culture of students and the school can be the place where participative democracy and electronic applications can be used. The familiarization of students on issues e-Democracy can begin through the school. This will contribute decisively in their tomorrow's active participation in the e-environment for democratic processes.

The use of Internet services can familiarize the students with e-Democracy issues and applications. Technology however cannot alone educate the students for the importance of participation. The education of students in order to define and understand important democratic issues should precede the use of technology.

The research’s results show that, in order to achieve a sustainable growth of the Information Society, the adoption and diffusion of new means should not enforce existing inequalities neither fragment society to those who are able to access information and those not.

There is also, a number of participants in electronic participation such as the elected representatives, governmental persons in charge for the formulation of policies and citizens which need to be introduced in the world of new technologies. Many of the challenges of future are not strictly technological but more socio-economic. Structures should be developed for the support of e-democracy systems, in order to overcome organisational and cultural obstacles which are related with the adaptation of a new principle of Democracy.

References

1. Bellamy, C., Taylor, J.: Governing in the Information Age. Open University Press (1998)
2. Bouras, C., Katris, N., Triantafillou, V.: An e- voting service to support decision-making in local government. Telematics and Informatics 20, 255–274 (2003)

3. Clift, S.: E-Democracy E-Book: Democracy is Online 2.0 (2002), `http://www.publicus.net/ebook/`
4. Coleman, S.: The transformation of citizenship? In: Axford, B., Huggins, R. (eds.) New Media and Politics. Sage Publications, London (2001)
5. Coleman, S.: Connecting Parliament to the Public via the Internet: Two Case Studies of Online Consultation, Information, Communication & Society, March 2004, pp. 1–17 (2004)
6. Coleman, S.: New Mediation and Direct Representation: Reconceptualising Representation in the digital age. New Media & Society (2004)
7. Hagel, J., Armstron, A.: Net Gain: Expanding Markets Through Virtual Communities. Harvard Business School Press, Boston (1997)
8. Kalogeras, D., Triantafillou, V., Sklabos, N.: e-Democracy: The Internet Effect to the Citizens of Tomorrow. In: Proceedings of IADIS International Conference www/Internet 2006, Murcia, Spain, October 5-8 (2006)
9. Macintosh, A.: Ζώντας στην εποχή της ηλεκτρονικής δημοκρατίας. Νέος πολιτικός μετασχηματισμός (2002), `http://www.gsrt.gr/default.asp`
10. Kennard, W.E.: Building New Crossroads for the Information Age. In: Remarks of the US FCC Chairman before the Budapest Business Journal Conference, Budapest, Hungary, December 4 (2000)
11. `http://www.fcc.gov/Speeches/Kennard/2000/spwek027.html`
12. Triantafillou, V., Kalogeras, D.: e-Democracy: The Internet effect at the students. Magazine Education and New Technologies, Copy 4, Athens. Publications Kaleidoscope (2006)
13. Triantafillou, V., Kalogeras, D.: e-Democracy: The opinion of tomorrow citizens. Kathimerini Athens (2006)
14. Triantafillou, V.: Electronic democracy: Democracy over time and space. The Economist, Athens (2008)
15. Triantafillou, V., Kalogeras, D.: The future of Democracy is digital (to be published, 2009)
16. Triantafillou, V.: E-Democracy, MsC, Virtual Communities, Panteion University (2004)
17. Webster, Fr. (ed.): Culture and Politics in the Information Age. Routledge, London (2001)

Parademo: e-Democracy Based on a Delegated Expert Selection Process in a Small-World Network

Ronny Siebes

VU University Amsterdam, De Boelelaan 1081a, 1081HV,
Amsterdam, The Netherlands
RM.Siebes@few.vu.nl

Abstract. Many countries have a representative democracy where their governments consist of a relatively small group of politicians that represent the values and beliefs of the majority of the voters. Unfortunately, many citizens are un- satisfied with their rather limited influence on politics especially regarding governments on national level or even higher like the EU or the UN. On the other side, referenda or direct democracies seem to be a too risky way of letting un- knowledgeable or uninterested individuals decide over complex issues. We mainly have these extreme opposites in our democracies due to the limitations of our manually maintained ballot system. Initiatives like Vivarto propose an alternative, called 'Delegated voting' where parts of a vote can be delegated to people with more knowledge on a certain topic. This leads to a convenient position in the middle between both mentioned extremes. We want to use the vast amount of expertise of many online citizens in our societies in selecting the right politicians and solutions. In this paper we propose the design of system called Parademo, that enables a fine-grained e-democracy. Next to this we briefly describe how we can achieve more transparency and third-party functionality by allowing listeners to subscribe to specific information-streams within communities that are formalized in a Semantic-Web language.

Keywords: E-democracy, Small-world expertise, Tokens, Fine-grained voting delegation, Semantic Web, Voting Cafés.

1 Introduction

Our democracies are mostly representative democracies, where in regular periods (often four years), people go to vote for their favorite party to represent their wishes and beliefs. The advantage of a representative democracy is that the average citizen often does not have the time or the right expertise to solve national problems. The problem remains however that the voter still has the burden to figure out which representative has the right knowledge and is trustworthy enough. This almost requires that the voter needs some expertise on the topic him/herself and should almost know the person to determine its trustworthiness.

The famous Milgram experiment [6] showed that the average 'acquaintance distance' between any two randomly selected persons is very small (around 6 hops). This means also that for any "Joe the plumber", the acquaintance distance to the president

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 108–117, 2010.

of the United States is as small. Similarly, this holds between any voter and the best expert(s) for any topic. This means that everybody should have somebody in their acquaintance group who knows somebody closer to the best expert for a given problem. This leads to an important assumption in our paper:

We assume that most people are capable in identifying from their friends and colleagues the person(s) closer to the best experts and that during this selection process, members along the selection route have an increased expertise themselves to make valuable contributions in the decision making processes.

Analysis of massive online social networks show that also the graph of the relations between the members adhere the properties of a small-world network [7]. Therefore we make an even stronger assumption in this paper:

We assume that most members of an online social network are capable in identifying from their friends and colleagues (within the online network) those person(s) who are closer to the best online experts and that during this selection process, members along the selection route have an increased expertise themselves to make valuable contributions in the decision making processes.

The enormous amount of high-quality content on Wikipedia shows that there are many people who are 1) online, 2) are experts and 3) have an incentive of sharing it with the community for free.

Assuming that a large amount of these experts also participate in online social networks we perhaps can conclude that the time is ready to investigate if we can reform our representative democracy to an e-democracy.

The ballot systems in most mature representative democracies did not radically change in the last centuries. When we compare this with other important organizations in our societies, like the banking system, defense, the stock market, secret agencies, social security and health-care, it is surprising that computers play only a minor role in the way the core of our democracy is managed. The only digitalization that we currently see is that electronic alternatives are used for the paper ballots, but that the course-grained structure stays the same. A possible explanation for this slow pace is that most people do not trust the management of the democracy in hands of computers, especially when voting can be done at home behind a computer with an Internet connection.

In other words, ICT is often simplistically coupled to direct democracy, ignoring the need to be more specific on democracy [11]. Advances in computer science resulted in technology dealing with security and anonymity of online voting [3], although there are also serious concerns [8, 9].

There are already some promising examples of country-wide binding Internet Voting systems in Sweden [1], Estonia [5], Austria [4] and Brazil [8]. Although more fine- grained, these systems still are very similar to the 'classical' representative democracies with digital ways to vote.

In this paper we propose the design of a system, called Parademo[1] where the representative selection process is smoother by making the selecting process of the final representatives via the acquaintance chain within an online social network.

[1] For latest information on Parademo, please visit http://www.parademo.org

Currently, there are already some approaches similar to the one we propose in this paper. For example, The World Parliament Experiment[2] is an Internet platform for political discussions. Besides elections, the forum allows people to debate in a structured way, discuss and share views. The focus of this system is more on the discussion process than selecting delegates for vote-distribution. This however gives us valuable lessons to create that part of the user interface taking for the ”debate” phase (discussed later) of our Parademo system.

Vivarto[3] comes close to Parademo in the sense that they also focus on implementing a decision-making system based on delegating votes to more knowledgeable members in an organization. Unfortunately, the activity on development seems to be halted.

The MetaGovernment project[4] is most similar to the work presented in this paper. Like Parademo, the project is in a preliminary state and therefore there are still many things unknown, like the software design. Content-wise, there is at least one big difference: MetaGovernment is a direct democracy, where it (currently) is not possible to identify a group or person to delegate some of the voting decisions for specified topics. The core of Parademo is to allow members to delegate parts of the decision making process in order to relief most of the members of being ’mini-politicians’ and to allow more knowledgeable members to get more influence.

Recently the European commission funded more than 21 projects by the ”eParticipation” program[5]. The objectives of the program are to demonstrate how using modern ICT tools and applications can make it easier for people to participate in decision-making and can contribute to better legislation. Most of these projects focus on facilitating a platform to debate political issues or try to make the legislation more simple for the average citizen.

We hope by developing Parademo, we enable a fine grained delegation mechanism of expertise selection and hope to achieve that:

1. A reduction of the complexity may be expected in identifying the best candidates to govern an organization due to the delegated responsibility of the members who participate in an online social network.
2. An increase of usable expertise in the government may be expected due the increased number of available knowledge of the online community and allowing the most knowledgeable members to participate in the decision making process.
3. An increase of trust in the political system, resulting in an increased voting participation can be expected due to the smaller social distance between the voter and the delegates.

The remainder of this paper is ordered as follows: first we elaborate on the concept of e-voting and its relation to an e-democracy. After that we introduce the idea that votes are the currency of a democracy resulting in splitting votes into Tokens. After that we introduce Parademo, by defining the main concepts and member roles. Section 4 outlines the initial ideas behind the main algorithms to manage the Tokens and to calculate reputation of the members. In Section 5 we briefly describe an important implementation aspect of the Parademo software. We conclude with a summary and future work.

[2] http://www.tgde.org/

[3] http://www.vivarto.com

[4] http://www.metagovernment.org

[5] http://www.eu-participation.eu/

2 Electronic Voting

Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting technology can include punch cards, optical scan voting systems and specialized voting kiosks (including self-contained Direct-recording electronic (DRE) voting systems). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet ... Internet voting can use remote locations (voting from any Internet capable computer) or can use traditional polling locations with voting booths consisting of Internet connected voting systems.

[Wikipedia]

In this paper we focus on the most advanced and controversial e-voting system, namely voting via the Internet. Voters have a 'budget' of Tokens that represent their 'voting power' in the communities where they are member of. Due to very limited possibilities for human control and guidance over the circumstances of the voter at home, we have to focus on technical and organizational solutions to guarantee the security, authentication of the voters, their privacy and the clarity and simplicity of the user- interface(s).

As we will discuss later, the members of the communities in Parademo can monitor and manage their Token placements from any computer with an Internet connection. The risks of this can be categorized in two parts:

1. Unauthorized observations and manipulations by unknown individuals. By this we mean somebody 'hacking' the computer. Payment systems of banks are currently considered a secure way to prevent this. We plan to use similar approaches for Parademo to prevent unauthorized tracking and manipulation of voting behavior. More on this in the section on the design of the Parademo system.
2. Unauthorized observations and manipulations of known individuals. In some families there might be a dominant individual that wants to control the voting behavior of the other family members. Due to the lack of control on privacy when voting at home, this is a serious problem. This problem holds for any decision- making process where there is no authority that controls the privacy of the decision makers. A solution for this problem has to be found in an organizational sense rather then technical. For example, a government could organize voting-cafés several locations in the country where citizens after identifying themselves can login on secure computers in a protected environment and spend time to participate in the e-democracy process. This also solves the previous problem where computers at home are more vulnerable to security problems.

The idea of Voting cafě́s is of course a rather costly solution, but probably the only possibility to make sure a voter can trust the computer (s)he is working on and participate in a private environment. Perhaps we have to accept that, next to roads and fire-brigades, Voting cafés should belong to the public infrastructure of future democracies and are paid by community funds (e.g. tax).

Next to security and privacy, we also have to deal with the different capabilities of the voters in working with computers. In other words, computer systems can be easy for the one, but intimidating for the other. Luckily we see that the improvement of the user-friendliness of interfaces, the increasing education on IT and increasing knowledge of friends and family to help out. We assume that this leads to an increasing acceptance of doing things digitally. Splitting the ballots into Tokens, placing them, monitoring them etc. does not make life easier. Therefore, as a design requirement, Parademo will have different user-interfaces, where the simplest one is a one-to-one mapping to the traditional system: as a default an automatically subscribed member of a community can place once in four years a vote (the whole Token budget) on one of the parties within the subscribed community. Also all effort needs to be taken to keep the algorithms and monitoring system transparent and well documented. Next to this, when Voting cafés are organized, authorized instructors can help people in demonstrating the possibilities of the system (of course taking the privacy constraints in account).

3 Parademo as a Large-Scale Decision Making System for Communities

Any government is a kind of large dynamic decision making and execution system with a layered internal feedback loop. Similarly, also Parademo can be seen as such.

A decision making process involves participants, definitions, a mix of formal rules and protocols and conventions on behavior. The participants involved with the process can play several roles with different degrees of influence and responsibilities. Often, the larger the organizational complexity the more formal and explicit the protocols, audits and definitions are needed. We plan to use popular description logic language 'OWL' [2] to write down most stable parts of the model which has several advantages and also to use is as the language of the messages in the information-streams between the software components.

Given the ambitions of Parademo of facilitating also large governmental organizations, we focus on making most procedures and definitions as explicit as possible. Next to this, given the nature of the system, a computer system, it also needs to have a formal definition in order to translate parts to a programming language.

We first start with giving an overview of the basic concepts in Parademo. After that we list the different roles the participants can play. Finally, we describe the possibilities for members to form groups that can fulfill the role of the traditional notion of political parties.

3.1 Basic Concepts of Parademo

Communities. Our aspiration is that one Parademo 'system' can support many communities. For example, one community could be the national government 'community' of the Netherlands, and another community the 'Amsterdam' community. Every community has their own rules like the membership policies, token distribution policies etc. These are all written down in the community constitutions, partially in a formal language when automated support is desired.

Tokens. Every person allowed to vote within a community has a fixed budget of Tokens. These Tokens are the elements to express the agreement or disagreement with the different types of proposals, representatives, advisors or groups in Parademo. Later we describe what all these entail. The Tokens are uniquely bound to an owner, meaning that an owner normally never looses ownership. The owners always have the right to see where their Tokens are placed at any moment. Based on the return policy described in the constitutions of the communities in Parademo, it can retract is immediately to its own account or has to wait for a determined period. Next to an owner, a Token has two date-pairs: the return-period and the place- period. The return-period indicates when the Token is to be returned to the local ac- count of the owner. The place-period indicates when the desired purpose of the placement should be executed. Both periods are based on the constitutions and the voter preferences in the respective communities.

Tokens also have a current-account, which is the account of a representative, a representative group, an advisor, an advisor group, who we generalize to delegates or a proposal account. The amount of Tokens in an account indicates the influence of the respective account in the system.

Tokens have a polarity indicating if it should have a positive or negative effect on the total influence of the current account. In this way, it counts as a vote in favor or against the 'owner' of the account. The owner and delegates can change the polarity of the Tokens that they have.

Categories can be seen as the different ministries that governments have. For example: Education, Immigration, Defense, Finance, Health-care. These categories are used to specify the topics of the proposals made in communities. Also they function to bind the Tokens. For example, you may trust your brother who is a medical doctor to delegate votes on the category 'health-care'.

Proposals are the initiators of any kind of change within the organization. This can be a proposition of a solution, a constitutional change or a management up- grade etc. Proposals have a proposal-type which is explained next. Proposals have a duration-request where members can place Tokens to lengthen or shorten the duration of the proposal-stage of the proposal. The constitution determines the maximum duration extension or reduction a proposal phase has.

Proposal types indicate the nature of the proposal. It can be the introduction or adaptation of a category, constitution change, proposing a member for a Role, an issue, a solution, a consensus-solution, a bid to plan, a plan, relevant external source, facts to live with and a critique. The constitution of each community determines for each proposal type the duration for the several stages and other procedures.

Hidden author option. Some proposals may be controversial. The member that makes such a proposal may think that revealing his/her identity can bias the decision making process, or even endanger his or her position. Therefore, it can be that a proposal has an anonymous author. The constitution determines the types of proposals that are allowed to be anonymous and also the changed statutorily value of it.

Proposal stages indicate the current stage of a proposal, which can be ”candidate”, ”debate”, ”vote”, ”formal check”, ”formal check result”, ”accepted”, ”rejected”, ”retracted”. Each phase has an agreed duration time, but as said can be subject to change within constitutionally determined margins.

Constitution. The constitution can be seen as the meta-rules of Parademo. Some examples are the rights and obligation of the member types, the distribution key of the different Tokens, the duration of phases etc. The members can submit proposals to make changes to the constitution.

Facts-to-live-with. Every government or other organization has to deal with some facts that constrain the possible decisions. For example, the national planning bureau can predict the available budget for the next year. In Parademo there is a list of these facts- to-live-with, public to its members and perhaps even to the visitors. These facts can then be used as formal material to legitimate proposals. Every 'fact-to-live-with' has a validity-period and references to 'proof' agreed as valid by a significant relevant part of the community.

3.2 Roles

The members of Parademo can have multiple roles. Each role comes with formally defined responsibilities, rights, behaviors and ethics. These are described in the constitution and therefore subject to change.

- **Members** are those who are being accepted as participant within one or more communities. They are at least allowed to vote within the subscribed communities. Membership can be achieved when the person successfully passes his or her membership-proposal.
- **Representatives** are members that agreed to make their voting behavior for some Categories public. By doing this, they gain the right to maintain a Token account for that topic, where other members can donate their Tokens. Representatives express their "categories constraints" in their public profile, in order not to receive any Tokens categories for which they don't want responsibility. Representatives can always decide to change these constraints with the result that Tokens which are not fulfilling the new constraints are returned to the previous placer, however with a built-in 'rethink' period (determined by the constitution).
- **Advisors** are representatives that also think to have expertise on the topics they are representatives about. Next to their obligation to make voting behavior on the categories public, also some of the types of the proposals falling under that category, will be enforced to be non-anonymous.
- **Planners** are voters that write concrete execution plans for accepted solutions. In Parademo this is considered to be a job, and planners can bid via an auction on Parademo to write executing plans. Planners cannot fulfill any other role than being a voter, this is to keep independence. Of course this is determined by the constitution and subject to change.
- **Ministers** are members who are responsible to execute accepted plans. To become a minister, the voter has to submit a proposal. This is also a 'rewarded job' where the minister, as part of the proposal, proposes the reward (s)he wants to have.
- **Administrators** are also rewarded members without the right to vote and are responsible for keeping the system running, blocking accounts (when allowed) etc. They have special privileges and obligations on observing behavioral patterns of the system and report to the community.
- **Developers** are members without the right to vote and are responsible for adapting features of the system according to agreed execution plans governed by ministers. Also this is considered a rewarded job.
- **Controllers** are members that have special rights to request for checking if things go well. It is a rewarded job. There are several types of controllers. For example those who can check the administration of ministers. Or controllers that audit the workings of the software. Controllers are obliged to report to the community in a periodical fashion.

3.3 Groups

Members can 1) create groups, 2) apply for membership and 3) place Tokens on groups.

The reason to have groups in Parademo is for convenience of the voters. Groups can function as conventional political parties, but also any other item relevant to Parademo, like a controllers group, administrators group etc. A group is treated by Parademo in the same way as a normal member however with some additional constraints, mainly on accountability. Parademo does not enforce any internal procedures, like the organizational structure and they creation of proposals etc. Membership can be private or public, ac- cording to the decision made by the group creator. Voters (not necessarily members of the group) may choose to place Tokens on the group for being advisor and/or representative. The group determines which group-members are allowed to place Tokens and make proposals via the collective group accounts. For convenience, we call the collection of representatives, representative groups, advisors and advisory groups: delegates. The placement behavior of these delegates are public. This allows other members to see if they are reliable and knowledgeable, and also automated reputation algorithms can analyze the behavior and summarize that for the members of the community. The proposals have the group name as the identifier of the author. The group announces in the group description the category constraints for which they accept Tokens.

4 Algorithms

4.1 Algorithm to Calculate the Weight of Proposals

As previously mentioned, all proposals in Parademo go through different stages. One of the stages is the ”vote” stage. In that stage, voters, delegates, groups, and advisors can place their Tokens together with the polarities. Given our choice of Tokens as a currency instead of weight influence graph like Google’s PageRank algorithm, the calculations can be fairly simple. Namely, the system counts the number of tokens in favor and against the proposals to detect if the proposal is controversial and compares it to the total number of Tokens in that Category to see if the proposal has a significant support within the effected community. If not, an extra round to request Consensus proposals. The ratios to determine if some proposal is controversial and has enough support is defined in the constitution.

4.2 Algorithm for Automated Reputation Feedback

As previously mentioned, a voter can anonymously place its Tokens on delegates. In contrast to this, the placements of delegates are public. This means that the placement routes in a community from delegate to delegate and from delegate to the advisor delegate that places the tokens can be monitored. When the owner of the Tokens checks the placements of the proposals that are in the ”Vote” stage, (s)he can decide to retract it. When this happens, the whole route between delegates leading to the placement should be ’punished’ because they are as a whole responsible for a placement on which the owner in the end did not agree with. How much ’punishment’ each delegate in the route should get is up to the designer of the algorithms and the parameters that are part of the constitutions. In the prototype we will have a simple counter for each hop. More advanced algorithms can be found in literature [10].

5 Listeners on Information Streams within Communities

A bit more technical is the concept of having listeners on information streams within communities. Listeners are software components that have authorized subscriptions on information-flows between the software components of Parademo that facilitate the particular communities. In this way these 'external components' can offer useful services for these communities. For example, every time a member-ship proposal is accepted, a Web-service can be informed about this in order to analyze trends. Listeners are only added after it passes a 'listener-proposal' for which community members have to vote.

These feeds also will be used by processes of the Parademo system itself, for example to monitor the behavior of critical components. Although we did not decide yet on the format of the information streams between the software components of Parademo, it is very likely that we will use RDF[6], because it is a very popular language to describe structured linked data and can be used by Semantic web reasoning tools and Semantic Web Mash-ups.

6 Summary and Future Work

In this paper we presented the design of a fine-grained electronic voting system to run a complex organization governed via a democratic process. The delegated democracy can be seen as a convenient position between a direct democracy and a representative democracy where the citizens can choose by themselves the amount of participation and accountability. Parademo tries to make use of the vast amount of available expertise currently unused in the official decision-making process of representative democracies. Next to this we try to increase the trust and participation of the citizens in their democracies, based on having a chain of delegates to smoothen and improve the decision making process. By using Semantic Web technology for standardizing and formalizing information-streams between the software components of Parademo, we hope to create a radical transparent system which can be monitored and extended by third parties. We plan to evaluate the algorithms and different settings of the initial constitution rule-set via large-scale simulations on the Distributed ASCI Supercomputer 3 (DAS-3), a five-cluster grid system in the Netherlands[7].

Acknowledgements. Much gratitude goes to the colleagues and friends, participating in the necessary tough discussions that lead to the design decisions in this paper. Special thanks to Ajit Skanda and Thrasyvoulos Nerantzis for deciding to start doing their masters thesis on Parademo.

[6] http://www.w3.org/RDF

[7] http://www.cs.vu.nl/das3/

References

1. Nordfors, M., et al.: The demoex portal (2006), `http://demoex.net/en/`
2. Horrocks, I., Patel-Schneider, P., van Harmelen, F.: From shiq and rdf to owl: the making of a web ontology language. Web Semantics 1, 7–26 (2003)
3. Jefferson, D., Rubin, A.D., Simons, B., Wagner, D.: Analyzing internet voting security. Commun. ACM 47(10), 59–64 (2004)
4. Krimmer, R. (ed.): Electronic Voting 2006: 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting. CC, August 2- 4, 2006 in Castle Hofen, Bregenz, Austria. LNI, vol. 86. GI (2006)
5. Madise, Ü., Martens, T.: E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. In: Krimmer [4], pp. 15–26 (2005)
6. Milgram, S.: The small world problem. Psychology Today 31(2), 60–67 (1967)
7. Nazir, A., Raza, S., Chuah, C.N.: Unveiling facebook: a measurement study of social network based applications. In: IMC 2008: Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, pp. 43–56. ACM, New York (2008)
8. Rodriges-Filho, J., Alexander, C., Batista, L.: E-voting in Brazil - the risks to democracy. In: Electronic Voting 2006. GI Lecture Notes in Informatics, pp. 85–94 (2006)
9. Rubin, A.D.: Security considerations for remote electronic voting. Commun. ACM 45(12), 39–44 (2002)
10. Sabater, J., Sierra, C.: Regret: reputation in gregarious societies. In: AGENTS 2001: Proceedings of the fifth international conference on Autonomous agents, pp. 194–195. ACM, New York (2001)
11. Saebo, O., Pivrinta, T.: Defining the ”e” in e-democracy: a genre lens on it artifacts. In: 29th Information Systems Research Seminar in Scandinavia (2006)

Telep@b Project: Towards a Model for eParticipation and a Case Study in Participatory Budgeting

Federica Paganelli and Dino Giuli

National Interuniversity Consortium for Telecommunications,
Dept. of Electronics and Telecommunications, Univ. of Firenze
federica.paganelli@unifi.it,
dino.giuli@unifi.it

Abstract. eParticipation concerns the use of ICT tools for facilitating the two-way communication between governments and citizens. Designing eParticipation activities is a complex task. Challenges include the need of interdisciplinary expertise and knowledge (for example, political, sociology, usability and technology domains) and the lack of widely accepted models and standards. This paper attempts to provide a model for eParticipation, aiming at providing guidelines for the design, implementation and management of eParticipation applications. This model has been put into practice for the design of an eParticipation portal in the framework of the Telep@b project. We also report on the experimental use of the portal services in a group of Tuscany municipalities for supporting participatory budget activities and future activities in a follow-on project (PAAS_Telep@b project).

Keywords: eParticipation, ICT tools, participatory budget.

1 Introduction

Many governments around the world are promoting several initiatives in the e-Government domain, thus massively investing on information and communication technologies to ground public sector innovation.

Among several e-Government application domains, eParticipation is one which is recently emerging. As defined in [1]: "*Public participation is the process by which public concerns, needs, and values are incorporated into governmental and corporate decision making. It is two-way communication and interaction, with the overall goal of better decisions that are supported by the public*".

Typically, public participation processes include actions for informing, involving and consulting citizens to provide an input to a specific stage of the democratic process.

eParticipation concerns the use of ICT tools for facilitating the two-way communication between governments and citizens. Designing eParticipation activities is a complex task. Challenges include the need of interdisciplinary expertise and knowledge (for example, political, sociology, usability and technology domains) and the lack of widely accepted models and standards.

The objective of this paper is to provide a model for eParticipation, aiming at providing guidelines for the design, implementation and management of eParticipation

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 118–127, 2010.

applications. This model has been put into practice for the design of a eParticipation portal in the framework of the Telep@b project. We also report on the experimental use of the portal services in a group of Tuscany municipalities for supporting participatory budget activities.

2 Related Work

eParticipation is an emerging research field. In the last decade several research and innovation projects have been promoted by governments in order to experiment and put eParticipation into practice.

Conceptual modeling efforts have been done in order to provide guidelines and framework aiming at driving the design of eParticipation services.

Phang et al. in [2] provide a framework to support eParticipation designers in choosing appropriate ICT tools for participation initiatives to be supported during a policy-making process. eParticipation objectives are distinguished in: Information exchange, education and support-building, decision-making and input probing.

In [3] the authors propose a conceptual model of the eParticipation domain aiming at formalizing the relationships among organizational and social aspects of the participation process with ICT tools. The study includes the specification of three subdomains and related interrelationships. The sub-domains are: main stakeholders and related roles, participation levels (e-informing, e-consulting, e-involving, e-collaborating and e-empowerment) and related ICT tools.

While the framework proposed by [2] aims at supporting the implementation of eParticipation initiatives, the contribution in [3] models more granular aspects (such as the stakeholders) but seems targeted for analyzing existing eParticipation projects rather than designing new ones.

For what regards eParticipation initiatives, several projects have been promoted at local, national and international level. For instance, at European level, European Citizen's Consultations (http://www.european-citizens-consultations.eu/) uses web tools to create a pan-european discussion space for debating about the future of the European Union, while “Your Voice in Europe” (http://ec.europa.eu/yourvoice/) is the European Commission's portal providing tools for consultation and discussion targeted to civil society representatives. At local level some relevant examples are AskBristol (http://www.askbristol.com), which is a web site promoted by the Bristol City Council to make citizens influence the municipality decision-making by means of e-petitions, forums and webcasting services. In Spain, Consensus (http://www.consensus.cat) is a citizens’ e-Participation platform used by 73 Catalan municipalities with the aim of informing, consulting and allowing citizens’ participation in decision-making processes.

A more exhaustive list of relevant eParticipation projects is presented in [4],[5],[2].

3 Model for eParticipation Application Design

The design of ICT services aiming at supporting the activation and management of eParticipation processes is a complex and interdisciplinary activity. As a matter of fact, an eParticipation process may be considered as the result of the interweaving of two processes, the policy process and the participation process, exploiting both off-line and on-line participation activities.

A typical policy-making process can be distinguished into the following phases: agenda setting, policy formulation, policy adoption and implementation, and policy evaluation [6]. A participation process can be made of different activities:

- Information/education: institutional communication and education/training activities needed to inform citizens about the subjects of participation process.
- Discussion: citizens debate and exchange opinions on the subjects of the participation process or share ideas and concerns on open themes.
- Consultation: citizens are asked to express their opinions on a set of issues.
- Memory: citizens are made aware of how participation process results have been taken into account in the policy-making process and are made capable of monitoring the implementation of the participation process results. Moreover, memory of completed participation processes should be conserved. For instance, a report documenting the most relevant intermediary and final results of completed participation processes might be produced and made available to citizens in order to encourage their involvement in future participation initiatives.

These activities are not necessarily related with this sequential order, even if some patterns may be defined for common use (e.g. information and discussion activities should be performed before a consultation).

A participation model defines the relationships between policy-making process stages and participation activities to be activated and supported during such stages. At present, several participation models have been studied and experimented in local, national and international eParticipation initiatives. In [7] the authors analyse several contributions in theories and implementation of eParticipation and propose a framework made of four basic “idealised” models of eDemocracy: the Liberal, the Deliberative, the Partisan, and the Direct. The framework is based on two main dimensions: agenda setting and decision making. The four models are obtained as different combinations of explicit/implicit roles assigned to citizens in these dimensions.

The model depicted in Fig. 1 extends this approach by providing a more granular classification of such dimensions.

The above mentioned participation activities may be effectively supported by means of ICT tools. Several studies on the definition of ICT tools for e-democracy have been performed. The DEMO-net project have provided a non-exhaustive framework for classifying eParticipation tools and projects [4]. These categories include ePetitions, eVoting, eConsultation systems, ePolling, community systems, GIS and Map-based tools.

Thus, a general method for designing eParticipation processes includes the following steps:

a) identifying the objective and stages of a policy-making process which should be the target of the participation process
b) associating the participation activities to the policy stages in order to define the participation model
c) choose the ICT tools to be used to support participation activities in the different policy making stages.

These steps can be assigned to different actors. The first phase is usually performed by political representatives. Also the second one may be performed by political representatives, supported by domain experts, e.g. persons with expertise in the participation domain and/or persons which will tutor the participation process by mediating the citizens' access to the participation process (a "tutor" of the participation process). The third step could be profitably performed by the "tutor" or by an ICT designer.

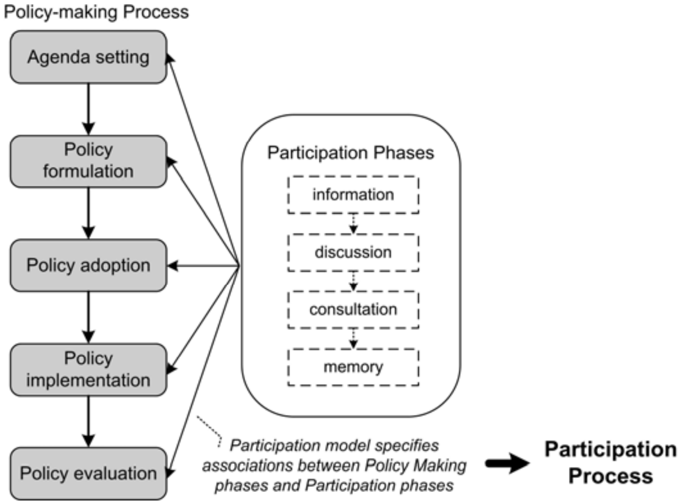


Fig. 1. Participation process

At present, most eParticipation service platforms are designed on top of existing or web-based Content Management Systems to specifically support a participation model but are hardly reconfigurable in order to support new participation processes.

In the followings we report on the activities of the Telep@b project for the design of a web-based framework aiming at facilitating the model-based design of eParticipation processes and its experimental use in a group of Tuscany municipalities for participatory budgeting.

4 Telep@b Project

The Telep@p (Electronic Technologies for the Participatory Budget) project is a 2-year project funded by the Italian Minister for innovation in public administration.

The project, concluded in July 2008. has been participated by 29 towns in different mountain areas of Tuscany, for approximately 200.000 inhabitants.

The aim of the project has been the development and experimentation of a technological platform facilitating the involvement of citizens in the process of budget formulation. The project results include a first release of a web-based portal for participatory process design and management. The portal services have been experimented for the activation of a 6-month participatory process for municipal budget formulation. Based on the results of Telep@b, a follow-on project has started in October 2008

(PAAS-Telep@b project). The aim of PAAS-Telep@b is to re-design and extend the existing portal by taking into account the results of the experimentation activities and integrating further access and dissemination means for promoting inclusion and participation.

Hereafter we describe the Telep@b portal's main features and the experimentation activities. Then, we introduce current research and development activities in the ongoing PAAS-Telep@p project.

4.1 Telep@b Portal

The Telep@b portal is a web-based framework integrating ICT modules to design and activate eParticipation processes according to the above mentioned model.

The project aims at promoting participation in the policy-making process related to budget formulation. The roles identified for this participation scenario are:

- citizens, as individuals or member of associations;
- representatives of the public administration (technical and/or political profile);
- tutor of the participation process;
- designer of the participation process.

The portal provides different views, according to user's roles:

- *administration view*: this view provides tutors and/or designers with basic administration services, including users' profiles and access roles management.
- *design view*: this view provides designers with services for modeling the participation process and its relation with policy-making stages, as depicted in Fig 1. Each participation activity is also associated with web-based services.
- *participation process view*: this view provides services enabling users (citizens and public administration representatives) to perform activities planned in the participation process.

More specifically, the designer view offers a drag&drop menu which guides the design of the participating process according to the following steps:

a) select the policy-making stages which are the target of the participation process
b) For each selected stage, assign the participation activities to be performed (i.e. information, discussion, consultation and memory)
c) For each instantiated combination of policy-making stage and participation activity, select the services to be activated (e.g. agenda, news, forum, online polls) and information resources to be put in evidence to citizens. These information resources mainly include budgetary documents, i.e. documents which are used according to law and practice for the definition of the municipal annual budget.

Table 1 shows the list of services offered by the Telep@b framework. The design view associates participation activities with most appropriate services, according to the relations marked in Table 1.

Table 1. Telep@b services and participation activities

		PARTICIPATION ACTIVITIES				
		Information/ Institutional Communication (government to citizens)	Information/ Non-institutional communication (citizens to government)	Discussion	Consultation	Memory
Telep@b services	Web content publishing and management	X				
	News	X				
	Calendar	X				
	Newsletter	X				
	Document Management	X				
	Knowledge Management for Budgetary Documents	X				
	Mail to local administration representatives	X	X			
	Forum			X		
	On-line polls				X	
	Report generation tool	X				X
	Integration with social networking tools[1]	X	X			X

The participation process view instantiates the flow of activities specified in the design phase. At present the transition from an active stage to the following one is configured manually by the participation tutor.

4.1.1 Information Resources for the Budgetary Process

In order to support communication and information activities related to the budgetary process, the portal provides also services for budgetary document presentation, indexing, and retrieval.

Information resources which are considered relevant for the budget formulation process, according to the Italian legislation and practice, have been analysed in [8]. These information resources include:

A) Documents for strategic planning: general plan; triennial budget; provisional and programmatic report; the public works triennial plan.
B) Documents for operational planning: provisional and programmatic report for the 1st year; upcoming annual budget; annual public works list.
C) Documents for executive planning: executive management plan.

Telep@b services for budgetary documents management are based on XML models which have been recognized as standard specification by Regione Toscana (see project SIFAL "Informative System On the Finance of Local Autonomies). These models for budgetary documents help identifying the main relevant formal-functional entries

[1] Feature to be developed in the PAAS_Telep@b Project.

in terms of “income” and “expenditure” and related areas of intervention (e.g. functions and services for expenditures). Functions and Services, which are defined as child elements of functions, help describing the town investment domain and have been selected as possible themes for structuring and guiding the participation process.

Based on the structured information models of budgetary documents, the Telep@p portal offers the following functions:

- uploading and browsing budgetary documents;
- help for navigation across budgetary documents based on semantic similarities and syntactic links among documents structured content;
- searching for single entries;
- for each entry, generating reports which aggregates information related to that entry and extracted from a set of budgetary documents.

More details on the Knowledge Management services provided by the Telep@b portal for the participation process and the implementation of the overall Telep@b portal (based on Joomla Content Management System) are provided in [8].

5 Experimentation Activities in Telep@b and Future Activities in the PAAS-Telep@b Project

The Telep@b portal is active since December 2007. At present, 24 municipalities have a participation web area in the Telep@b portal[2]. These municipalities represent small towns with less than 15,000 inhabitants, located in disadvantaged geographical mountain areas of Tuscany.

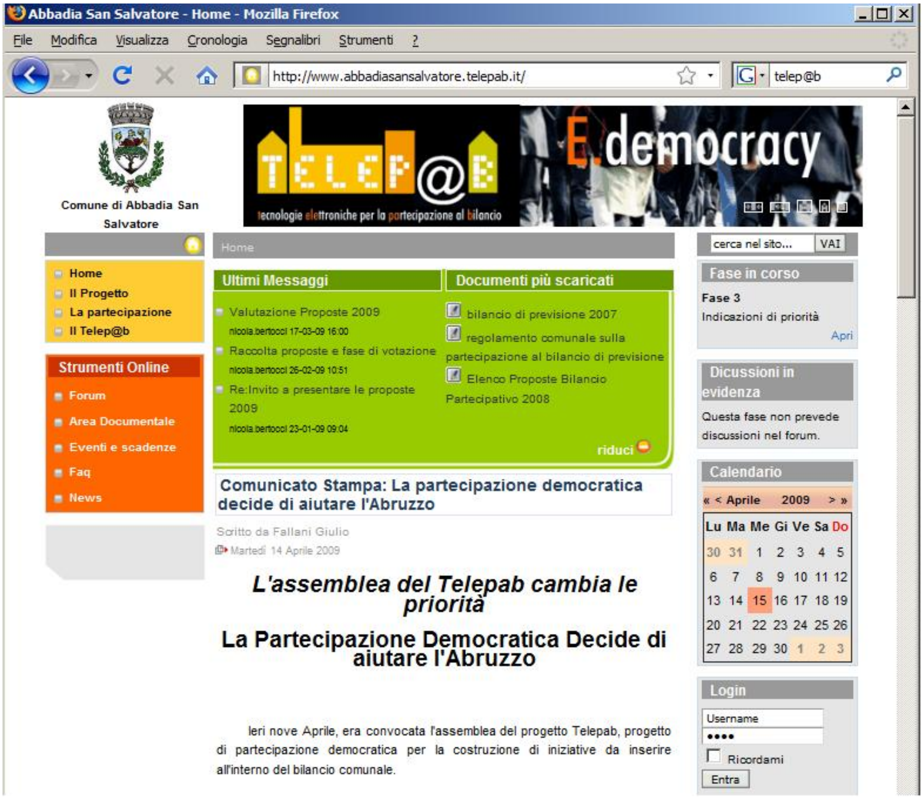
Two towns have initiated and completed a participative process by using Telep@b services. Figure 2 is a snapshot of the Telep@b area dedicated to a municipality.

In each municipality the participation process is regulated by a participation policy. The policy is a document defining scope, thematic areas and subjects allowed to participate. It also defines the stages of the participation processes, resources to be spent for the activation and management of the participation process, initiatives and channels for dissemination and involvement of the population.

In the first phase of experimentation, concluded in July 2008, the users which have accessed the Telep@b portal services was approximately 1,7% of the municipality population. The percentage of population which actively used the portal for discussion was less than 0,5% of population in one town, while in the second municipality the discussion has moved in external online communities already used by citizens.

The tutors of participatory process used the portal design view to configure the participation web area, according to the model in Fig.1. They found this portal view useful but they complained the lack of pre-defined configuration patterns to be used and adapted in order to speed-up the configuration process and minimize mistakes.

[2] Public Administrations which at present have a Telep@b site are listed at the following web link: http://www.telepab.it/index.php?option=com_telepab&task=viewComuni&Itemid=49


Abbadia San Salvatore - Home - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
http://www.abbadiasansalvatore.telepab.it/
telep@b
Comune di Abbadia San Salvatore
TELEP@B
tecnologie elettroniche per la partecipazione al bilancio
E.democracy
Home
Home
Il Progetto
La partecipazione
Il Telep@b
Strumenti Online
Forum
Area Documentale
Eventi e scadenze
Faq
News
cerca nel sito...
VAI
Fase in corso
Dicussioni in evidenza
Calendario
Login
Username
••••
Ricordami
Entra
riduci

Ultimi Messaggi

- Valutazione Proposte 2009
  nicola.bertocci 17-03-09 16:00
- Raccolta proposte e fase di votazione
  nicola.bertocci 26-02-09 10:51
- Re:Invito a presentare le proposte 2009
  nicola.bertocci 23-01-09 09:04

Documenti più scaricati

- bilancio di previsione 2007
- regolamento comunale sulla partecipazione al bilancio di previsione
- Elenco Proposte Bilancio Partecipativo 2008

Fase 3
Indicazioni di priorità
Apri

Questa fase non prevede discussioni nel forum.

« < Aprile 2009 > »

Lu	Ma	Me	Gi	Ve	Sa	Do
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Comunicato Stampa: La partecipazione democratica decide di aiutare l'Abruzzo

Scritto da Fallani Giulio
Martedì 14 Aprile 2009

L'assemblea del Telepab cambia le priorità

La Partecipazione Democratica Decide di aiutare l'Abruzzo

Ieri nove Aprile, era convocata l'assemblea del progetto Telepab, progetto di partecipazione democratica per la costruzione di iniziative da inserire all'interno del bilancio comunale.

Fig. 2. Telep@b Portal for a Tuscany Public Administration

These elements have been considered in order to define the objectives of a follow-on project, named PAAS_Telep@b, started in October 2008. More specifically the objectives of PAAS_Telep@b are:

- to activate the Telep@b areas in further 35 Tuscan municipalities.
- to improve existing features of the Telep@b portal. More specifically, in order to match remarks emerged during the use of the system, one specific aim will be to make the design of the participation process more intuitive. This will be done by improving the presentation of the design view and by offering a set of predefined process templates which could represent some relevant examples of participation.
- to promote the involvement of a larger percentage of population, especially young and elder people.

The latter point is the most critical one. As a matter of fact, it has been widely recognized that government bodies find it difficult to make citizens access and discuss on political issues in their web sites [9]. More in general, participation to civic and politic activities in local communities is perceived as declining, due also to recent social and economic transformations (i.e. many people work and live in different places) [10].

Even if ICT technologies have proved to encourage and increase the amount of communication between people separated by physical distances, it is not yet clear how ICT and social network tools can increase citizens' involvement in the participation process.

Leveraging on the experiences of the participation processes activated in the Telep@b process and the remark that citizens tend to discuss issues in digital places that they are familiar with [11], the PAAS-Tele-p@b project will experiment the use of two complementary strategies to facilitate the involvement of population with different ages and attitudes towards ICT tools in the participation process.

First, the activation of the Telep@b areas in new municipalities will go with the activation of access nodes, named "Assisted Access Point to Services and Internet" (PAAS), across the territory of interested municipalities. PAAS is a community service initiative promoted and funded by Regione Toscana to facilitate the use of online government services. A PAAS is a sort of enhanced Internet Point which are free of charge and are run by qualified personnel assisting users in accessing e-services.

Second, the project will investigate the use of social networking tools. The aim is to leverage existing communities and/or ICT tools for community building in order to disseminate participation activities by sharing events notification and links to resources published on the Telep@b portal. The aim is thus to develop an application for linking the Telep@b portal to Facebook (via Facebook API) with the following objectives: on one side, to exploit municipality's Facebook accounts in order to disseminate participation events and activities across municipality's network members; on the other side, to enable Facebook users interested in the public sphere to receive and personalize the notification of participation events as well as to post and share comments on these notifications by using the social network services.

We chose Facebook because of its wide diffusion (at the end of 2008 there were 4 millions active accounts in Italy, which has a total of 60 millions of inhabitants).

An aspect to be carefully evaluated in designing the application for integrating Telep@b with existing social networks will consist in finding the appropriate compromise between activities to be performed in external social networks and those to be performed in the Telep@b portal. The objective is thus to exploit existing social network communities for boosting involvement in participation, but without compromising the role of the Telep@b site (or in any case, the institutional site) as the digital place for participation processes. Otherwise, the risk of bridging external social networks is to disperse citizens' participation effort in different digital places.

6 Conclusions

This paper described a model for designing eParticipation processes as a result of weaving participation activities with policy-making stages and activating appropriate ICT tools and services. The model has been adopted for the design of a web-based portal, named Telep@b portal. The portal helps eParticipation designers in configuring and activating web-based services in relation with the appropriate participation activity, thus focusing on the participation model rather than on implementation details of the underlying web-based Content Management System.

The Portal services have been experimented in two Tuscany towns for budget-related participation activities. The design model for eParticipation have been experimented by participation tutors by using the Telep@b configuration services (design view). The approach has been positively evaluated, even if some remarks have been done on the design view ease-of-use. The low percentage of population actively involved in the eParticipation is the most critical aspect of such experimentation. Future activities planned in the PAAS_Telep@b project aims at offering a better support to the design model support by refining the configuration services and at increasing citizens participation by disseminating Assisted Access Points to Services and Internet (PAAS) in the local territory and by integrating the portal services with existing social networking tools.

References

1. Creighton, J.L.: The Public Participation Handbook: Making Better Decisions Through Citizen Involvement. Jossey-Bass, San Francisco (2005)
2. Phang, C.W., Kankanhalli, A.: A framework of ICT exploitation for e-participation initiatives. Communications of the ACM 51, 128–132 (2008)
3. Kalampokis, E., Tambouris, E., Tarabanis, K.: A Domain Model for eParticipation. In: The Proc. of ICIW 2008. Third International Conference on Internet and Web Applications and Services, 25-30, pp. 8–13 (2008)
4. Tambouris, E., Kalampokis, E., Tarabanis, K.: A survey of e-participation research projects in the European Union. International Journal of Electronic Business 6(6) (2008)
5. Chrysos, C., Kercic, D., Porquier, E., Todorovski, L.: State of the Art in e-Participation, Deliverable D2.1, IDEAL-EU Project, http://www.ideal-eu.net/images/Documents/IDEAL_EU_D2.1_State_of_the_Art_in_e_participation.pdf
6. Anderson, J.E.: Public Policy Making. An Introduction, 6th edn. Houghton Mifflin, Boston (2006)
7. Päivärinta, T., Øystein, S.: Models of E-Democracy. Communication of AIS 17, 818–840 (2006)
8. Mercatali, P., Romano, F., Fabrizi, R., Becchi, G.: Digital budgets for town administrations: participation, transparency and reverse process engineering. In: Proc. of the 1st international Conference on theory and Practice of Electronic Governance ICEGOV 2007, vol. 232, pp. 196–204. ACM, New York (2007)
9. Meijer, A., Burger, N., Ebbers, W.: Citizens4Citizens: Mapping Participatory Practices on the Internet. Electronic Journal of e-Government 7(1), 99–112 (2009), http://www.ejeg.com
10. Komito, L.: Community and inclusion: the impact of new communications technologies. Irish Journal of Sociology 16(2), 77–96 (2007)
11. Calenda, D., Meijer, A.: Young people, the Internet and Political Participation: Findings of a web survey in Italy, Spain and The Netherlands' Information, Communication and Society (to be published, 2009)

Stakeholder e-Participation in Local Planning: The Camargue Park Case

Nicolas Desquinabo, Nils Ferrand, and Julie Marlier

Cemagref, UMR G-Eau, 361 rue Jean-François Breton,
BP5095, 34196 Montpellier Cdx 05, France
nicodeski@yahoo.fr, {nils.ferrand, julie.marlier}@cemgref.fr

Abstract. The goal of this study is to evaluate several features and outcomes of the e-consultation organized by the Camargue Natural Park on its management plan. To estimate the benefits of the selected Internet devices, we have compared our assessment of this e-consultation with other face-to-face participative events organized on the same management plan. Following "computer-mediated communication" and deliberative theories, we expected that the tested e-tools would increase the deliberative features of the stakeholder participation. Several economic and organisational benefits were also expected. Our first results confirm the organisational benefits of this e-consultation (information gain, cost of the process, etc.). Several "deliberative" benefits have also been observed (more opinion and thematic diversity without an increase of "flames"). Nevertheless, speech is apparently more concentrated than in face-to-face events, even if many "non-posters" visited the consultation site but did not post because they had "all their comments already included".

Keywords: e-participation, e-deliberation, stakeholder, local government, planning, influence on decision, speech equality, inclusion.

1 Introduction

As descriptive research on public participation grows, so does the question of the impact of institutional and interface designs on public participation quality and impact. This question has already guided various researches comparing different types of face-to-face debates [1], [4], [16], different online devices [5], [19], [21] or face-to-face vs. online debate designs [10], [13], [14]. The variations observed can be related to the actual process of debates or their outcomes. The quality of the process is often measured by the representativeness of the participants, the equality of expression or the cost of the participative event. Outcomes or "impact" variables go from political knowledge to social trust gains and from argument repertoire to influence on actual policy decision. In the case of local planning processes, public participation is encouraged by laws and treaties at National and International scale (e.g. Aarhus convention). But participation is usually limited to selected professional stakeholders and experts in a few thematic meetings, [1], [8], [11]. Even when sponsors and managers

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 128–137, 2010.

want to widen the participation, they have to overcome many barriers (long procedures, complex documents, important organizational costs, etc.). In this context, which electronic tools can facilitate a wider, more "deliberative" and less expensive participation in such planning processes?

To answer this question, the Intermed project (2008-2011, funded by the French National Research Agency) aims at designing Internet tools and testing their potential benefits for local planning debate. These tests use case-study, comparative and experimental designs. In this paper we will present a study of the e-consultation organized by the Camargue Park on its management plan. The goal of this study is to evaluate several features and outcomes of this e-consultation. To estimate the benefits of the selected Internet device, we will compare our assessment of this e-consultation with other face-to-face participative events organized on the same management plan. More deliberative debates (inclusive, equal, diverse, etc.), a more equal influence on decision and several economic benefits for organizers are expected.

After a short discussion on Internet potential benefits for this type of debate (2), we will describe the context and the tools used for this e-consultation (3). Then we will precise the evaluation design of our study (4) and present the first results of our assessment (5). In the conclusion the limits and further directions of our research are discussed.

2 Internet Potential for Participation in Local Planning

Local planning processes evaluations are not frequent, but general features and challenges can be described (2.1.). For this type of public participation, Internet devices could have many potential benefits and less pitfalls than in general (2.2).

2.1 Public Participation in Local Planning

Compared to "deliberative events" like deliberative polls or consensus conferences [7], local planning debates have generally several institutional features that don't facilitate public participation. The procedures are long (3 to 6 years form diagnosis to policy plan), the texts are over 100 pages, the themes are complex, uncertainty is high and sponsors and organizers have limited resources. Thus, small group moderated and informed deliberation between "lay" participants is difficult to organize, except with large findings [9].

Given these "institutional features" and political routines, only a few "expert" stakeholders generally participate to planning processes in thematic meetings in France [11], in other EU countries [8], or in the USA [1]. The participation of most of stakeholders and citizens is then limited to meeting attendance or uninformed answers to polls [1], [6]. If "lay citizen" participation faces numerous barriers, the participation of a large part of the stakeholders is still problematic for many local governments. The main challenges for this type of policy making processes are generally:

- The implication of the maximum of stakeholders in the process in order to avoid potential conflicts and further contestations during the implementation phase
- A facilitated information gathering on the different issues faced by the diverse groups of inhabitants, workers and businesses of the district

- An increased awareness and knowledge of the urban and environmental issues of the district by their inhabitants
- Limited organisational and financial costs linked to the participation process and its synthesis at each step of the decision

In this context, what is the potential of e-participation to planning process? More precisely, which electronic tools can facilitate a wider, more "deliberative" and less expensive stakeholder participation to these planning processes?

2.2 Internet Potential for Local Planning Participation

The main potential benefit of Internet for public participation in general is its impact on organisational and financial costs. If managers and participants can save time and money, participation events are expected to be more frequent, interactive and representative [10]. More generally, if information and expression on public issues takes less time for participants, they should probably participate more, especially if they are not "professional stakeholders" [6].

Beyond "cost" factors, some Internet interface features may facilitate more inclusive, interactive and equal debates. According to many experiments in "Computer-Mediated Communication studies", usual features of online interfaces (lack of status indication, asynchronous and written communication, physical distance, etc.) enhance the equality and diversity of expression in group discussions [12], [18]. Some large experiments or observations have since confirmed these results [2], [14], [15]. Thus, in stakeholder consultations, Internet tools could facilitate the expression of the less "experts" in the topics discussed (and more generally in oral expression) and then lead to more informed, legitimated and accepted decisions.

One of the most frequent pitfalls of online debates is the high proportion of flames generally observed in online political discussion [3]. Moderation devices and practices can reduce this problem [2], [21] but their cost is high when the targeted level of participation is high. Moreover, these tools can also decrease participation rates or the level of perceived fairness of a public debate when confidence between citizens and government is low or when the moderation rules are vague [19], [20]. In stakeholder consultations moderation problems could be less important: the participants are not anonymous and they also meet in face-to-face meetings. Indeed, the potential benefits of e-tools for a class of public debate vary according to its institutional features and specific goals [17].

3 Context and Tools of Camargue e-Consultation

The studied e-consultation is one of the last "participative event" in a long process run by the Camargue "Regional natural park" on its management plan (3.1) Given the institutional features of this participative event and its context, a specific electronic design has been proposed to the Camargue Park government (3.2)

3.1 Institutional and Social Context of the Camargue e-Consultation

Camargue County is a coastal Regional natural park located in the south of France. Like every park it legally has to adopt a management plan. This plan must define the main goals and policies for the protection and the sustainable development of the concerned area. More limitations are possible, especially about business or infrastructures allowed in the Park area. These plans are legally superior and directly influence most of the policy choices made at the local scale. For instance, every urban planning document must be conformed to the park management plan. Like most of the local planning processes, the Camargue process is very long: it began in 2005 and it is supposed to end in 2010. At each step of the planning process, different types of public participation have been organized, generally with the same group of stakeholders. At the end of each step, an outline of the "public" proposals is produced by the managers of the park and then given to the park representatives for an "official validation". At the end of the process, local representatives and national government will finally adopt (or do not adopt) the co-written document (Cf. Table 1).

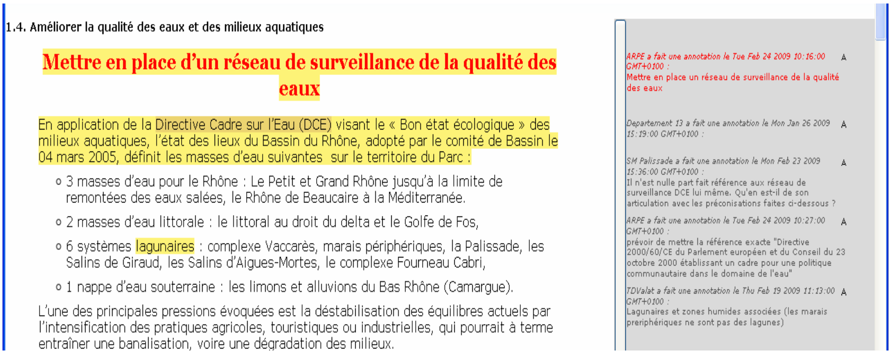
Table 1. Camargue Park management plan process

Steps	Participation
Area diagnosis (05-06/2006)	A few national and local governments experts and selected stakeholders
General goals (09/2006-06/2007)	A phone poll (250 participants) and 20 public meetings (300 participants)
Management plan "elaboration" (12/2006-07/2007)	40 thematic workshops (5 themes x 8 meetings) with approximately 100 stakeholders invited
Management plan "precision" (10/2008-03/2009)	16 thematic workshops and one global meeting with approximately the same stakeholders **E-consultation of around 90 stakeholders**
Management plan "validation" (Summer 2009-End of 2010)	"Public consultation" Local and National governments vote

The step of the process mainly concerned by our evaluation is the e-consultation of around 90 stakeholders (that began on 22 January 2009 and ended on 28 February 2009) who have been invited by mail and email to give their opinion and debate on the management plan project before the beginning of the "validation phase".

3.2 e-Tools for Costless and More Deliberative Planning Debate

Given the main institutional features and goals of planning debate between stakeholders, the Internet device tested was a website with an annotation tool, a controlled login and a "slight" moderation. The invited participants could read the management plan (one page for each of the 20 chapters), select any part of the text and comment it with no expression or size restriction. All the invited participants were able to read all the annotations and know who wrote it and when. They could also visualize to which part of the text the annotation were referring (Cf. Figure 1). The debates were not moderated; the participants were just warned that different type of "illegal" messages could be suppressed by a moderator.



1.4. Améliorer la qualité des eaux et des milieux aquatiques

Mettre en place d'un réseau de surveillance de la qualité des eaux

En application de la Directive Cadre sur l'Eau (DCE) visant le « Bon état écologique » des milieux aquatiques, l'état des lieux du Bassin du Rhône, adopté par le comité de Bassin le 04 mars 2005, définit les masses d'eau suivantes sur le territoire du Parc :

- 3 masses d'eau pour le Rhône : Le Petit et Grand Rhône jusqu'à la limite de remontées des eaux salées, le Rhône de Beaucaire à la Méditerranée.
- 2 masses d'eau littorale : le littoral au droit du delta et le Golfe de Fos,
- 6 systèmes lagunaires : complexe Vaccarès, marais périphériques, la Palissade, les Salins de Giraud, les Salins d'Aigues-Mortes, le complexe Fourneau Cabri,
- 1 nappe d'eau souterraine : les limons et alluvions du Bas Rhône (Camargue).

L'une des principales pressions évoquées est la déstabilisation des équilibres actuels par l'intensification des pratiques agricoles, touristiques ou industrielles, qui pourrait à terme entraîner une banalisation, voire une dégradation des milieux.

ARPE a fait une annotation le Tue Feb 24 2009 10:16:00 GMT+0100 :
Mettre en place un réseau de surveillance de la qualité des eaux

Departement 13 a fait une annotation le Mon Jan 26 2009 15:19:00 GMT+0100 :

SM Palissade a fait une annotation le Mon Feb 23 2009 15:36:00 GMT+0100 :
Il n'est nulle part fait référence aux réseau de surveillance DCE lui même. Qu'en est-il de son articulation avec les préconisations faites ci-dessous ?

ARPE a fait une annotation le Tue Feb 24 2009 10:27:00 GMT+0100 :
prévoir de mettre la référence exacte "Directive 2000/60/CE du Parlement européen et du Conseil du 23 octobre 2000 établissant un cadre pour une politique communautaire dans le domaine de l'eau"

TDValat a fait une annotation le Thu Feb 19 2009 11:13:00 GMT+0100 :
Lagunaires et zones humides associées (les marais preriphériques ne sont pas des lagunes)

Fig. 1. E-consultation tool screenshot

This type of annotation tool was supposed to entice the participants to read the different parts of the planning document and select the sections or proposals they wanted to comment. This possibility is particularly important for local planning processes in which the documents discussed are generally over 100 pages long. To collect complex information and evaluations of stakeholders, free flow text has been preferred to poll, although a form of pre-structured expression has been suggested: participants were asked to precise if their message was a comment or a modification proposal.

The controlled and identifying type of login (e.g. "Asso_camarguais" for "Association des camarguais") has been chosen to create accountability and limit the need for moderation. A systematic pre or post-moderation is too expensive for this type of local government, especially if the level of participation becomes high. Moreover, censorship could have a negative impact on trust and dissuade some stakeholders to continue their participation to these long and complex planning processes.

4 Evaluation Design of the e-Consultation Features and Outcomes

In order to test several hypotheses about the benefits of e-tools for stakeholder participation (4.1) we have analyzed several process features and outcomes of the Camargue e-consultation and compared them to similar face-to-face participation processes (4.2).

4.1 Hypotheses

We expected that this stakeholder e-consultation should have several benefits compared to the usual features of the Camargue Park workshops. The definition of these "process" and "outcome" benefits refers to previous research on public participation [1], [2], [15], [16].

First, given the limited cost of moderation, economic and organisational benefits of this Internet tool for this type of consultation will be confirmed:

- if its cost (preparation, moderation, processing) is inferior to the usual cost of a comparable face-to-face consultation

- if the organizers are satisfied with the participation rate and with the type and quantity of information and opinions gathered
- and if the proportion of "flames" [3] is not very different from the moderated face-to-face workshops

Second, according to many results in "Computer-mediated Communication" studies [12], [18], this e-consultation event is expected to:

- decrease the concentration of speech vs. comparable face-to-face debates (% of speech time for each participant and type of participant)
- increase the expression of disagreement and the diversity of speech acts produced
- decrease the "thematic specialization" of the participants (% of questions and part of the plan discussed by each participant and type of participant)

Finally, if these process features are observed (with a low level of flaming), deliberative theories [5] predict

- an increased perception of satisfaction and competence gain by the participants
- and more influence on decision by "weak" stakeholders (who participate and speak less than the "expert" or "professional" stakeholders in face-to-face workshops).

4.2 Evaluation Design

To test our hypotheses, we have used several methodological tools (face-to-face interviews, phone poll, workshops proceedings analysis) to collect data on two set of face-to-face workshops that could be compared to the e-consultation (the 40 thematic meetings organized between December 2006 and July 2007 and the 16 thematic meetings organized between October and December 2008). During these workshops, approximately the same stakeholders were invited to debate about the main policies to adopt in the management plan. First, we interviewed the organizers and main "moderators" of the process in order to collect:

- their estimation of the 3 processes general "cost" (preparation, moderation, outline)
- their assessment of the workshops main features (concentration of speech, proportion of disagreements and "flames", themes discussed)
- their level of satisfaction with the type and quantity of the information and opinions gathered (in the three processes)
- and their estimation of the different stakeholders' influence on decision

We also analyzed the workshops proceedings to assess more precisely the participation rate of each type of participants (National or local government agency expert, local government representative, business lobby, local association) in each thematic meeting.

The e-consultation process features (concentration of speech, proportion of flames, etc.) have been analyzed "directly" on the participation data collected online (text of the annotation, text annotated, author, etc.)

Finally, we interviewed a large part of the invited stakeholders in order to collect data on their practices (previous participations, use of Internet) on their assessment of the e-consultation and on the reasons why they did or did not post messages.

5 First Results

Given the limited cost of this non-moderated e-consultation, economic and organisational benefits of this "basic" Internet tool are confirmed, at least for this type of consultation. As shown in table 2, many additional comments, proposals and form corrections have been collected (630 posts, 20 450 words) with a limited cost and without a flame increase. Moreover, the organizers of the process emphasized that the annotation system induced the posters to "locate" their comment in the text and thus allowed an easier "integration process" (i.e. the political discussion of what proposal should be integrated in the plan with which wording).

Table 2. Face-to-face vs online consultations "organisational costs and benefits"

	Face-to-Face workshops		E-consultation of February 2009
	2007	2008	
Participation	51 participants M=14 part./ meeting	52 participants M=7 part./ meeting	90 invited-52 visitors 20 posters-630 posts
Information and opinions gathered	List of goals and possible policies (very vague)	More precisions and commitments by lobbies (hunters, etc.)	Additional policy proposals and form corrections
Proportion of flames	Very few (?)	Very few (?)	Very few (2) by the main Park opponent
Estimated cost of the process	30 000 euros	15 000 euros	5 000 euros

Concerning the deliberative features, three hypotheses have been tested only approximately: distribution of speech, level of disagreement and diversity of speech. Indeed, the data collected on face-to-face events were mainly based on managers' memories. Nevertheless, it seems clear that the e-consultation did not facilitate speech equality: only 20 stakeholders have posted at least one annotation and the 10 most active posted 88% of the messages (Cf. table 3). On the contrary, more disagreements have been expressed online and the thematic specialization has significantly been reduced. As expected, participants widely used the possibility they had to comment the different parts of the management plan (although only local government representatives and a few "professional" stakeholders managed to participate to several thematic workshops during the face-to-face processes).

Although not complete yet, the interviews of the invited stakeholders (90) give already some interesting results. Almost all the interviewed (41) have visited the consultation site at least one time, even the "non-posters" (28). Concerning the interviewed stakeholders who read at least several posts (17), 65% found the debate interesting and diverse and a majority claim that they have learned about the management plan (59%) and about the other participants' opinions (53%). The main reason for non-posting is the "lack of time" (43%). More interestingly, some stakeholders did not post because their opinion was "already included in the plan" (21%). Seven stakeholders printed the plan to annotate it in an "internal meeting" and sent it by mail (mostly "big" agencies and lobbies). Only 11% of the non-posters claimed that their Internet access or the web site usability were a barrier. But at least 4 posters apparently lost a few messages and found the web site not enough usable.

Table 3. Face-to-face vs online consultations "deliberative features"

	Face-to-Face workshops		E-consultation of February 2009
	2007	2008	
Who attended?	18 Agency Experts 7 Local Gov. 14 Lobbies 12 Associations (at least 1 meeting/40)	16 Agency Experts 7 Local Gov. 18 Lobbies 7 Associations (at least 1 meeting/16)	5 Agency Experts 6 Local Gov 3 Lobbies 6 Associations (at least 1 post)
Distribution of speech?	Relatively equal (?)	Dominance of a few (?)	Dominance of a few (88% of posts by 10 most active)
Thematic specialization	Most of participants confined to one theme	Most of participants confined to one theme	90% of posters talk about most of the themes
Disagreements	Very rare (except on one "bridge or not bridge" issue)	Rare (One workshop per type of activity)	25% of messages disagree on content

6 Conclusion

To estimate the benefits of the "Camargue management plan" e-consultation, we have compared our assessment of this e-governance process with other face-to-face participative processes organized on the same plan. Following "computer-mediated communication" and deliberative theories, we expected that the tested e-tools would increase the deliberative features of stakeholder participation with several economic and organizational benefits. Our first results confirm most of the expected organizational benefits: many additional policy proposals and form corrections have been collected with a limited cost and without an increase of flames. Several "deliberative" benefits have also been observed (more diverse opinions without an increase of flames and knowledge gains for participants). Inversely, speech is apparently more concentrated than in face-to-face events, even if many "non-posters" did not post because they had "all their comments already included".

Concerning the influence on decision, it is too soon to analyze the impact of this e-consultation. Yet, according to the process managers, almost all the proposals precisely formulated have been included in the new draft of the management plan. These proposals were generally about "personal" commitment that a given stakeholder made previously and then wanted to modify. But “common” goals and policy proposals have also been included if any explicit disagreement was expressed by other participants (except if the disagreements were expressed by the two main opponents of the park: a local government and an inhabitant association). Further “textual” comparisons between drafts of the plan and posts of the participants have to be done to check these claims.

Although our assessment is not complete, it seems likely that the “basic” Internet tool proposed had several benefits. For this type of consultation a moderation tool is not useful and polls would have decrease the information gain for organizers. Still, several improvements of the e-tool usability are possible and have been asked by participants. Moreover, cartographic or multi-criteria decision supports could probably enhance participation and deliberative features. Nevertheless, the main barriers to a wider and more deliberative participative e-governance are clearly “institutional”. For instance, the length, complexity and vagueness of the management plan were probably the main barrier for most of the non-participants.

In further assessments of this type of participative e-governance process, several methodological barriers should be overcome. First, direct observation of similar face-to-face events could improve the comparison of speech concentration and disagreement expression. Second, consultation processes in which face-to-face meetings are organized in parallel with online consultations on the same topic, though rare would be more interesting to study. Finally, our knowledge of e-tools effectiveness for public participation processes would above all be improved by comparative studies between processes using different e-tools in similar institutional and social contexts.

References

1. Chess, C., Purcell, K.: Public Participation and the Environment: Do We Know What Works? Environmental Science & Technology 33(16), 2685–2692 (1999)
2. Coleman, S.: Connecting Parliament to the Public via the Internet: Two Case Studies of Online Consultations. Information, Communication & Society 7(1), 3–22 (2006)
3. Davis, R.: Politics Online. Routledge, New York (2005)
4. Delli Carpini, M.X., Lomax, C.F., Jacobs, L.R.: Public Deliberation, Discursive Participation, and Citizen Engagement: A Review of the Empirical Literature. Annual Review of Political Science 7, 315–344 (2004)
5. Desquinabo, N.: Webforum design and debate practices during the 2007 French presidential campaign. In: Politics: Web 2.0 Conference, Royal Holloway, University of London (2008), http://newpolcom.rhul.ac.uk/politics-web-20-paper-download/
6. Fung, A.: Varieties of Participation in Complex Governance. Public Administration Review, Special Issue, 66–75 (2006)
7. Gastil, J., Levine, P. (eds.): The Deliberative Democracy Handbook. Jossey-Bass, San Francisco (2005)
8. Hatzilacou, D., Kallis, G., Mexa, A., Coccosis, H., Svoronou, E.: Scenario workshops: A useful method for participatory water resources planning? Water Resources Research 43 (2007)
9. Hartz-Karp, J.: A Case Study in Deliberative Democracy: Dialogue with the City. Journal of Public Deliberation 1(1) (2005), http://services.bepress.com/

10. Iyengar, S., Luskin, R., Fishkin, J.: Facilitating Informed Public Opinion: Evidence from face-to-face and on-line Deliberative Polls. Presented at Annual Meeting of American Political Science Association, Philadelphia (2003)
11. Le Bourhis, J.P.: De la délibération à la décision: l'expérience des commissions locales de l'eau. In: Billé, R., Mermet, L., Berlan-Darqué, M. (eds.) Concertation, décision et environnement. Regards croisés, vol. 4. La Documentation Française, Paris (2006)
12. Lemus, D.R., Seibold, D.R., Flanagin, A.J., Metzger, M.J.: Argument and Decision Making in Computer-Mediated Groups. Journal of Communication 54, 302–320 (2004)
13. Min, S.: Online vs. Face-to-face deliberation: Effects on civic engagement. Journal of Computer-Mediated Communication 12(4) (2007), http://jcmc.indiana.edu/vol12/issue4/min.html
14. Monnoyer-Smith, L.: Citizen's deliberation on the Internet: a french case. In: Norris, D. (ed.) E-Government Research: Policy and Management. IGI Publishing, New York (2007)
15. Price, V.: Citizens Deliberating Online: Theory and Some Evidence. In: Davies, T., Noveck, B.S. (eds.) Online Deliberation: Design, Research and Practice. University of Chicago Press, Chicago (2006)
16. Rowe, G., Frewer, L.J.: Evaluating Public-Participation Exercises: A Research Agenda. Science, Technology, & Human Values 29(4), 512–556 (2004)
17. Smith, S., Macintosh, A., Millard, J.: Major factors shaping the development of eParticipation. European eParticipation Deliverable, 1.1a (2008), http://www.european-eparticipation.eu
18. Witschge, T.: Online Deliberation: Possibilities of the Internet for Deliberative Democracy. In: Shane, P.M. (ed.) Democracy Online. Routledge, London (2004)
19. Wojcik, S.: How does eDeliberation work? A Study of French Local Electronic Forums. In: Avdic, et al. (eds.) Understanding eParticipation – Contemporary PhD eParticipation Studies in Europe, DEMO-net, Örebro University Library, Sweden (2005)
20. Wright, S.: Government-run Online Discussion Forums: Moderation, Censorship and the Shadow of Control. British Journal of Politics and Intern. Relations 8(4), 555–568 (2006)
21. Wright, S., Street, J.: Democracy, deliberation and design: the case of online discussion forums. New Media & Society 9(5), 849–869 (2007)

Session 5

Identity Management, Privacy and Trust

Core Structure Elements Architectures to Facilitate Construction and Secure Interconnection of Mobile Services Frameworks and Advanced IAM Systems

Athanasios Karantjias and Nineta Polemi

University of Pireaus, Informatics Department
80 Karaoli & Dimitriou Str,
185 34 Pireaus, Greece
karant@unipi.gr, dpolemi@unipi.gr

Abstract. The impressing penetration rates of *electronic and mobile* networks provide the unique opportunity to organizations to provide advanced e/m-services, accelerating their entrance in the digital society, and strengthening their fundamental structure. *Service Oriented Architectures (SOAs)* is an acknowledged promising technology to overcome the complexity inherent to the communication among multiple e-business actors across organizational domains. Nevertheless, the need for more privacy-aware transactions raises specific challenges that SOAs need to address, including the problems of managing identities and ensuring privacy in the e/m-environment. This article presents a targeted, user-centric scalable and federated *Identity Management System (IAM),* called *SecIdAM,* and a mobile framework for building privacy-aware, interoperable, and secure mobile applications with respect to the way that the trust relationship among the involved entities, users and SOAs, is established. Finally, it analyzes a user-transparent m-process for obtaining an authentication and authorization token, issued from the *SecIdAM* as integrated in the IST European programme SWEB for the public sector.

Keywords: e/m-Federation, Identity and Access Management, Privacy, Security, Cryptography.

1 Introduction

Until now, XML technologies and *Web Services (WSs)* have been considered as the most appropriate approach for achieving interoperability, facilitating the communication among multiple e/m-business actors, across organizational domains. However, till recently these solutions faced many problems due to:

- The impediments to the delivery of bundled, context-sensitive services to end-users couldn't satisfy the desire of *Service Providers (SPs)* to develop and deliver user-centric, strong and secure identity services 1.
- The increasing regulatory compliance and audit requirements 2, which force SPs to consider a higher assurance level for user identity in e/m-provision of services, imposing the implementation of proprietary *Identity and Access*

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 141–150, 2010.

Management (IAM) mechanisms with questionable levels of usability, manageability, and scalability.
- The fact that the mobile aspect is partially covered in these solutions.

Service Oriented Architectures (SOAs) encompass services that essentially implement business processes involving various actors. A major concern of these actors is related with the accomplishment of secure interactions. The satisfaction of the main dimensions of security (authentication, confidentiality, integrity, and non-reputation) has always been a vital issue when integrating large-scale enterprise solutions. The adoption of world-wide accepted standards such as XML Cryptography, *Public Key Infrastructure (PKI)* and *WS-Security (WS-S)* already provide viable solutions to create secure e/m-environments 3.

However, the need for privacy aware transactions raises specific problems that SOAs need to solve including the management of users' identities both in the electronic environment and the mobile one. The common practice is the adoption of privacy policies 45 as a means to imprint the capabilities and requirements of the entities participating in a SOA enterprise system. Nevertheless, privacy policies do not constitute a full identity handling solution on their own, since they do not implement or guarantee all the required identity management processes. Even if the research and industry communities have identified several identity management solutions that implement complete e-identity handling frameworks 46 nowadays a SOA designer has to identify the appropriate e/m framework that better suites the needs of his system, without introducing additional complexity to the design or leaving out important aspects of privacy management.

This article proposes a targeted, user-centric and federated IAM system, called *SecIdAM,* and a mobile development framework for building advanced m-services, with respect to the way that the trust relationship among the involved entities, users and SOA enterprise systems, is established enabling the user to e/m-access advanced business services. The proposed system *SecIdAM* has been implemented in the IST European programme SWEB 7. The rest of the paper is organized as follows: Section 2 presents existing IAM-solutions, models, and related work performed. Section 3 presents the *SecIdAM* and Section 4 presents an advanced mobile framework for building synchronous, privacy-aware m-applications. Section 5 presents the usage scenario, while Section 6 contains acknowledgements and Section 7 draws conclusions.

2 Existing Implementations and Related Work

Several solutions for managing and controlling end-user's access, permissions, and allowed actions to e-resources are already proposed by many projects and initiatives. According to their results, three main types of IAM-solutions were proposed. The first refers to account management and implements an *Authentication, Authorization, and Accounting (AAA)* infrastructure. Representative designs of this type are the *Liberty Alliance (LA)* 48 and the WS-Federation 69. LA creates a set of specifications (*ID-FF, ID-WSF, and ID-SIS*) for identity federation in network environments, ensuring interoperability, supporting advanced privacy, and promoting the adoption of its guidelines and best practices. WS-Federation, on the other hand, is a component of the WS- Security model, defines mechanisms for enabling different security domains to federate by allowing and brokering trust of identities, attributes, and authentication between the WSs implemented.

The second type refers to user data profiling process, such as the detailed log files or data warehouses, which support personalised services and analyse user's behaviour. Finally, the third type is based on solutions for user-controlled, context-dependent role and pseudonym management.

Other projects and research initiatives 1011 propose and implement system architectures that reconcile privacy and accountability of users' e-interactions, distinguishing mainly two IAM-solutions:

- The *enterprise IAM-solutions*, in which data-control is exercised by the enterprise instead of the individual user.
- The *user-centric IAM-solutions*, in which the administration and control of identity information is placed directly into the hands of individuals, allowing users themselves to have full control of their personal information and preferences.

All these attempts aim to cover all possible cases, and therefore remain in a generic level. The facts that privacy and identity management, at the time that many of these solutions were deployed, were very innovative assets when building advanced e/m-enterprise systems, and the primitive status of core WSs standards, led to ineffective and rather closed IAM solutions 12.

In addition these solutions provide automated systems to SPs for managing identities, authentication and authorization, whereas do not adopt the user perspective, who needs to simplify his entrance in a large scale enterprise framework. Last but not least, the fact that the mobile aspect is partially covered imposes the replacement of these solutions with more synchronous ones.

3 Federated Identity Management System

Privacy in massively inter-connected environments and its social acceptance from end-users requires totally novel approaches to identity and privacy management 13, through trustworthy interfaces, taking into account multiple requirements such as anonymity, pseudonimity, linkability / unlinkability 14, and data protection regulations 1516 in place.

Our approach recognizes the need for broader e/m-business solutions, in which the notion of federation is expanded, and the relationship of each user with the overall framework is established, guaranteed and monitored by a trusted third entity. The user-centric *SecIdAM,* the architecture of which is depicted in Figure 1, undertakes the management of the partial identities and pseudonyms of all kind of users, as well as for the provision of proper asserted claims for accessing business services deployed in SOA oriented enterprise systems.

The *SecIdAM* consists of four different and district tiers, the *Interaction Tier*, the *Main Enterprise Tier*, the *Secondary Enterprise Tier*, and the *Middleware* one.

The *Interaction Tier* undertakes the establishment of communication with all external entities such as the e/m-users, and the enterprise systems of the SPs. This communication is based on WSs, processed from the *Web Service Manager.* The quality of protection through message integrity, message confidentiality, and single message authentication, is provided through the use of WS-S mechanisms, the implementation and validation of which are undertaken from the *Message Security Manager*.

The *Main Enterprise Tier* implements the core authorization mechanisms. The *Service Handling* component handles all service calls into the enterprise and assigns specific events to other internal handlers and components. The XACML-based *Policy Enforcement* 5 module specifies and enforces fine-grained, system-readable privacy policies, used to control access to WSs, digital objects and services, enclosing users' preferences and *SecIdAM's* requirements.

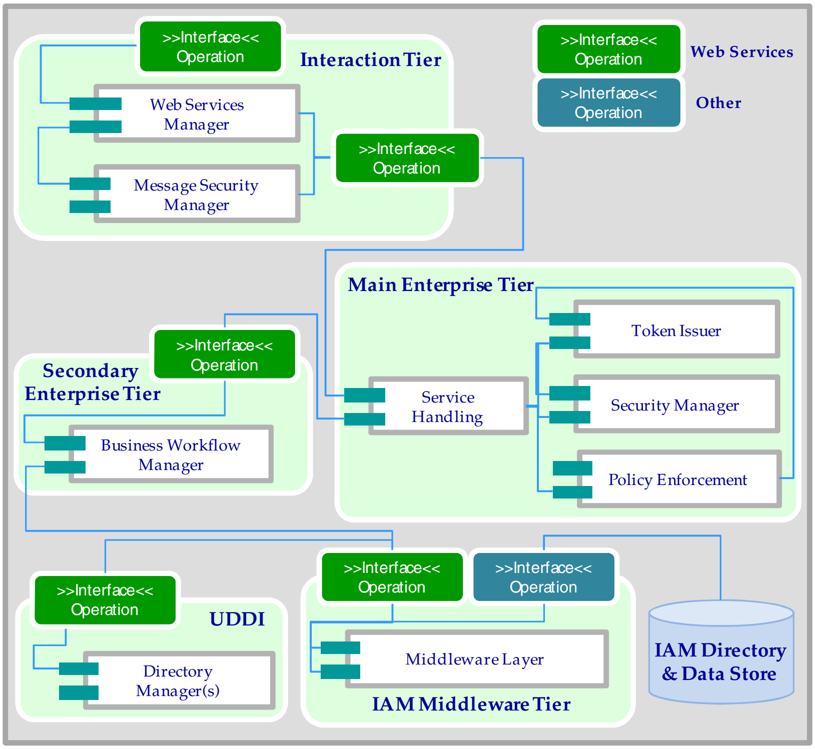


Fig. 1. Architectural overview of *SecIdAM*

Therefore, within this component an initial policy matching of the SPs' requirements with the users' preferences and capabilities and vice versa is achieved. The *Security Manager* module handles all security cryptographic credentials provided from a PKI, while it implements all the advanced security mechanisms on the *SecIdAM* such as the creation/validation of XML digital signatures and XML encryption and decryption.

The *Token Issuer* module issues XML-based security tokens, integrating the WS-Trust standard 21, providing authorization, and advanced auditing mechanisms. To maximize interoperability with clients and systems from multiple vendors, the *SecIdAM* supports the WS-Federation and SAML 2.0 protocols 17. For higher administrative efficiency, it automates federation trust configuration and management, using the harmonized federation metadata format 18. This automation enables the *SecIdAM* and SPs to publish their federation metadata in a standard format, which can be exchanged between potential partners. Consequently, using a single specification that can support both passive web application and active WS requestors is a key advantage for effectively using this system in multiple and heterogeneous environments.

The *Secondary Enterprise Tier* manages the choreography of the core IAM system's services, implementing their business logic, defining and mixing human based actions, and creating business rules based on workflow data, through the use of *Business Process Management Notation (BPMN)* systems. It actually places a significant emphasis on all processes within the secondary enterprise tier of the system, both in terms of streamlining process logic to improve efficiency, and also to establish processes that are adaptable and extensible so that they can be augmented in response to business change 19. Our primary goal was to establish a highly agile automation environment, fully capable of adapting to change, which is realized by abstracting the business process logic into its own tier.

The *Middleware Tier* integrates all required interoperable mechanisms through the integration of an *Enterprise Service Bus - ESB* framework 20. This tier is actually a light weight messaging layer that uses disparate technologies, transports and protocols. Specifically this tier undertakes to communicate with a UDDI server or any other directory server, or even a single database server, which provides a set of services supporting the description and discovery of all businesses, and SPs, as well as the predefined policies, agreed between the *SecIdAM* and each SP separately. An optimum federated IAM system must give the capability to adopt and manage data structures from multiple and heterogeneous environments while not changing the implemented services. Therefore, the middleware tier operates as a transformation layer for every possible data that have to be inserted or exported from the *SecIdAM.*

4 Privacy-Aware Mobile Framework

A shrinking workforce, combined with the need to deliver higher levels of service to key constituents is contributing to a requirement for federal organizations workers to use wireless networks and devices to perform mission-critical business functions at anytime, anywhere. A set of fundamental design principles, strategies and guidelines has to be clearly specified, addressed, built, and maintained in order catch common goals and benefits. The goals behind these principles are tied directly to some of the most strategic objectives of service-oriented computing:

- Allow for service logic to be repeatedly leveraged over time so as to achieve an increasingly high return on the initial investment of delivering the m-service.
- Increase business agility by enabling the rapid fulfillment of future business automation requirements through wide-scale m-service composition.
- Successfully address advanced m-privacy and m-security mechanisms.

Rather than embedding functionality that should be deployed across every specific m-service, the distributed m-architecture, depicted in Figure 2, offers secure, interoperable, extensible and reusable WSs interfaces to application developers in order to easily expand the m-functionality and build upon it.

Our main focus, when designing and implementing this innovative mobile framework in SWEB project for the public sector, was to integrate essential functions that can be easily reused, configured and customized for every m-service offered through four core modules.

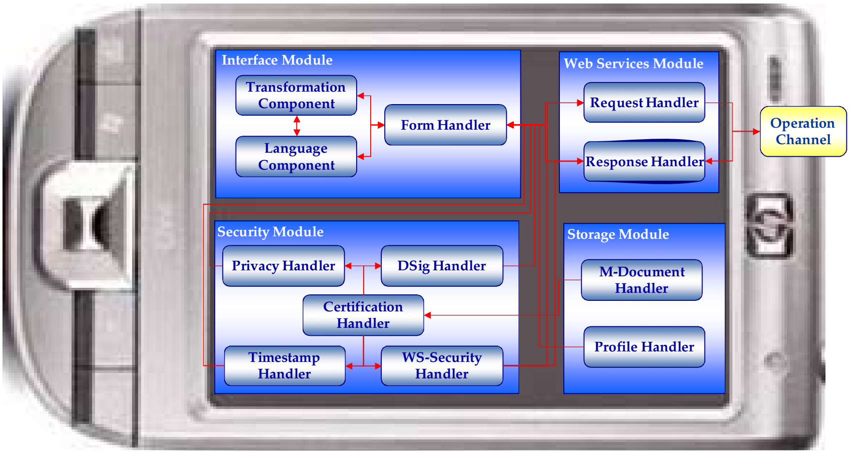


Fig. 2. Mobile Client Tier Architecture

The *Web Services Module* implements all formulation and handling mechanisms of the transmitted messages to external communicating entities through the *Request Handler*. It actually encloses all clusters of data into WSs, integrating as well the reception and extraction of the main body mechanisms, though the *Response Handler*, on every other end of communication.

The *Interface Module* implements the transition between m-forms, through the *Form Manager* during the process of user interaction, the selection and automated adjustment of language and character set on these forms through the *Language Manager*, and the transformation of the given data into a format compliant with the adopted XML schemas through the *Transformation Manager*.

The *Security Module* integrates strong security mechanisms on the mobile device, providing essential interfaces for achieving multilayer security (transmission, processing and storage). It creates and verifies XML digital signatures on the m-documents through the use of the *XML Security Manager*, which are automatically structured from the *Form Manager*, as well as the hash values of the signed m-documents and requests for valid timestamps (if needed) through the *Timestamp Manager*. All SOAP messages are digitally signed and encrypted from the *WS-Security Manager* using strong cryptographic credentials which are stored and handled by the *Certificate Manager*. Furthermore, it creates the appropriate requests for obtaining valid authorization tokens from the *SecIdAM* through the *Privacy Handler*, receives and handles them by automatically embedding them into messages to be sent to SOA oriented platforms.

Finally, the *Storage Module* stores and handles the created and received m-documents, through the use of the *m-Document Manager*, and the various profiles of users on the mobile device, activating the *Profile Manager*. Depending on each authenticated user on the application, many required fields (ex. name, surname, V.A.T. number, etc), are automatically filled on the m-forms.

The logic encapsulated in this m-framework by each service is associated with a context that is sufficiently generic and agnostic to all usage scenarios, so as to be considered reusable.

5 Usage Scenario of *SecIdAM*

There are several prerequisites for using the *SecIdAM* in a large scale framework for both end-users and SPs that operate one or more SOA oriented enterprise systems. First of all, the SP has to communicate with it and register all the e/m-services provided from its systems. This procedure requires the names of the services and the policies for e/m-accessing them as well as to build the profile of the SP. Consequently, each SP must define the roles for all kind of end-users, (e.g. “simple user”, “admin”, “employee”, etc) for each service and the required information provided from the end-user for obtaining these roles.

Moreover, the SP has to specify the exact URL in which the WSs for each business e/m-service listen. This URL is kept in the UDDI registry, with the name of the service and the WSDL description of the corresponding WS. The *SecIdAM* handles only information, which is required for assigning authorization roles to end-users. The UDDI registry undertakes the better organization of a large-scale enterprise framework, managing e-records for each e/m-service that the core IAM system doesn’t need to be aware of. In addition all WSDL descriptions of the integrated WSs are stored in this registry.

On the other hand, each end-user has to create one or multiple profiles, providing his/her preferences that concern the information he/she wants to disclose in his/her transactions. Optionally, the user may provide a subset or all the required information, creating multiple profiles, which correspond to different roles. Specific authentication information and a pseudonym are bound to each of the above profiles. In addition to these, the user has to be registered at the PKI in order to obtain the required cryptographic credentials. These credentials have to be successfully installed in the mobile device, in which the mobile application operates.

The satisfaction of these prerequisites makes the user able to access the e/m-services offered from the SOA oriented enterprise platforms, following the sequence of steps depicted in Figure 3. These steps are totally transparent to the end-user, who doesn’t need to be aware of all the advanced security mechanisms that run on every m-transaction.

The mobile application receives a request from the user, who has already specified the profile he/she wishes to use, to proceed with the authorization process. It creates a Request Security Token Request 22, embedding the preferred profile, the e/m-service that the user wishes to access and the name of the SP where this service is available. This request is embedded in a SOAP message and the application applies WS-S features on the message, ensuring that this request can only be processed from the SecIdAM.

The latter receives the request, and performs decryption on the message and validation on the XML digital signature. This process requires the communication with the PKI, which performs validation on the cryptographic credentials used. Under a successful validation the user is authenticated.

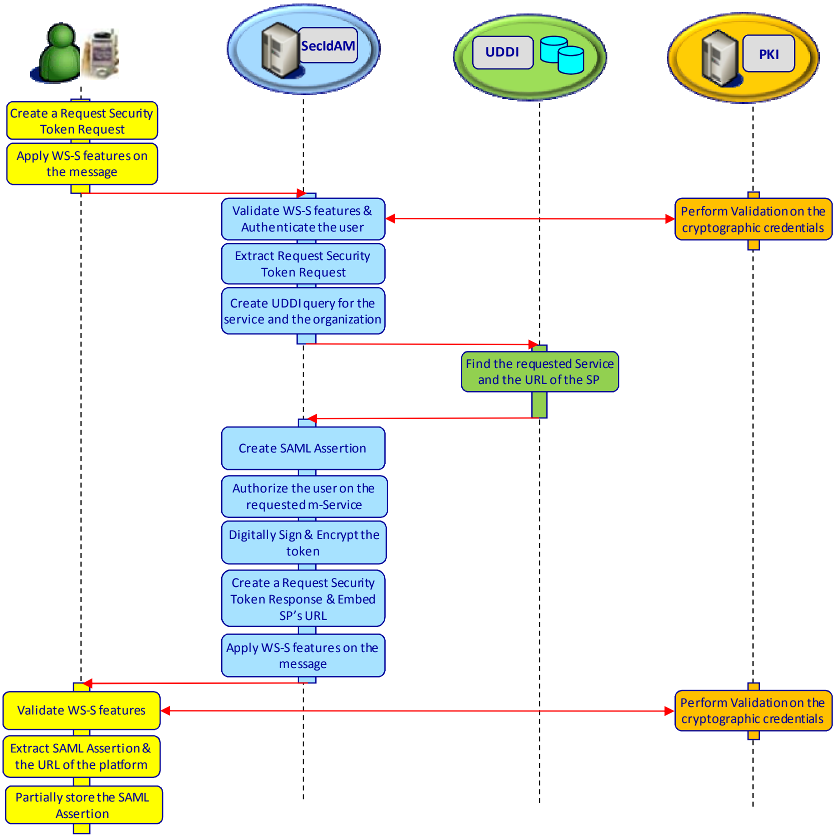

SecIdAM
UDDI
PKI
Create a Request Security Token Request
Apply WS-S features on the message
Validate WS-S features & Authenticate the user
Perform Validation on the cryptographic credentials
Extract Request Security Token Request
Create UDDI query for the service and the organization
Find the requested Service and the URL of the SP
Create SAML Assertion
Authorize the user on the requested m-Service
Digitally Sign & Encrypt the token
Create a Request Security Token Response & Embed SP's URL
Apply WS-S features on the message
Validate WS-S features
Perform Validation on the cryptographic credentials
Extract SAML Assertion & the URL of the platform
Partially store the SAML Assertion

Fig. 3. Usage Scenario for obtaining a valid m-token from SecIdAM

The *SecIdAM* extracts the actual request and retrieves the name of the requested m-service, and the name of the SP. It then structures a query and submits it to the UDDI registry in order to get the appropriate record of the requested service on the given SP. Upon successful retrieval of this record, the UDDI returns the appropriate URL, in which the mobile application has to communicate and request the actual m-service, to the *SecIdAM*.

It receives the results and authorizes the user according the preferred profile, selected form the user, and the policies specified from the SP. After successful authorization, the *SecIdAM* creates a SAML assertion. This assertion has a specific validity period, which is actually specified from the SP, embeds the role of the end-user and a new pseudonym for him/her, ensuring his/her anonymity. The role assigned to the user results from the information that he/she intends to release, and has been defined during the profile creation.

The *SecIdAM* digitally signs the assertion with its private key and encrypts it with the public key of the SP. Consequently, only this organization will be able to decrypt and further process this SAML assertion, which is required for the accomplishment of the authorization process on its SOA oriented enterprise system.

The next step requires the creation of *Request Security Token Request* 22 in which the URL is embedded. The *SecIdAM* structures a SOAP message which includes the above response, applies WS-S features on it, and responds to the m-application.

The latter receives this SOAP message, performs decryption on it and validation on the digital signature. As previously this procedure requires communication with the PKI in order to ensure the validity of the credentials used. Under successful validation the mobile application extracts the encrypted SAML assertion and partially stores it in the mobile device, in order to embed it on the headers of the actual m-service request that will be submitted on the SOA platform. It also extracts the required URL in which the platform that provides the actual m-service operates.

6 Conclusions

Advanced SOAs are considered the most promising way to achieve complex communication among multiple e/m-business actors across organizational domain. However, the lack of strong security and privacy mechanisms, and the adoption of inefficient, insecure, and expensive enterprise identity management systems necessitate a large-scale innovation, across organizational boundaries and between public and private institutions, in which privacy and identity management will not be treated as generic problems.

Essentially, this paper intends to provide practical and comprehensive coverage of a synchronous enterprise, user-centric and federated IAM system, and a mobile development framework for building advanced privacy aware m-applications that can be implemented on a modular basis, designed and implemented in the IST European programme SWEB 7. These solutions encompass fundamental design principles such as interoperability, scalability & extensibility, privacy, security, and reusability, in order for large-scale frameworks to successfully solve problems arising from identity management, ensuring privacy awareness for each managed identity.

Acknowledgements

The authors would like to thank the E.C. for its support in funding the SWEB project [7], and all the project partners.

References

1. Bertino, E., Martino, L.D.: A Service-oriented Approach to Security - Concepts and Issues. In: Eighth International Symposium on Autonomous Decentralized Systems, ISADS 2007, Sedona USA, pp. 7–16 (2007)
2. Peyton, L., Doshi, C., Seguin, P.: An audit trail service to enhance privacy compliance in federated identity management. In: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research, CASCON 2007, pp. 175–187. ACM, Ontario (2007)

3. Kaliontzoglou, A., Sklavos, P., Karantjias, T., Polemi, D.: A secure e-Government platform architecture for small to medium sized public organizations. Electronic Commerce Research & Applications 4(2), 174–186 (2005)
4. Liberty Alliance. Liberty ID-WSF Web Services Framework Overview, version 2.0 specifications, `http://www.projectliberty.org`
5. Papastergiou, S., Karantjias, A., Polemi, D.: A Federated Privacy-Enhancing Identity Management System (FPE-IMS). In: Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Athens (2007)
6. Lockhart, H., et al.: Web Services Federation Language (WS-Federation). Version 1.1 (December 2007)
7. SWEB IST project, Secure, interoperable, cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries, Sixth Framework Programme, IST-2006-2.6.5, `http://www.sweb-project.org`
8. Liberty Alliance Project, Liberty Alliance & WS-Federation: A Comparative Overview (2003), `http://www.projectliberty.org/resources%20/whitepapers/`
9. Goodner, M., et al.: Understanding WS-Federation, version 1.0 (2007)
10. PRIME Project, Privacy and Identity Management for Europe, European R&D Integrated Project under the FP6/IST Programme (2005), `http://www.prime-project.eu.org`
11. Meints, M., et al.: D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems (2005), `http://www.fidis.net/fileadmin/fidis/deliverables%20/fidis-wp3-del3.1.overview_on_IMS.final.pdf`
12. Rieger, S., Neumair, B.: Towards usable and reasonable Identity Management in hererogeneous IT infrastructures. In: 10th IFIP/IEEE International Symposium on Integrated Network Management – IM 2007, Munich, pp. 560–574 (2007)
13. Corradini, F., et al.: The e-Government digital credentials. International Journal of Electronic Governance (IJEG) 1(1), 17–37 (2007), `http://www.inderscience.com/filter.php?aid=14341`
14. Haddad, W.: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. Network Working Group, IETF Trust (2008)
15. Directive, Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Official Journal L L 024, 0001– 0008 (1997)
16. Directive, Directive 01/45/EC of the European Parliament and the Council of Ministers on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Official Journal L 008, 0001– 0022 (2001)
17. SAML, Security Assertion Markup Language v.2.0 – Technical Overview. Working Draft 1.0 (2006), `http://www.oasis-open.org`
18. OASIS WSFED Technical Committee, Web Services Federation Language Version 1.2, OASIS, Working Draft (2008)
19. Pasley, J.: How BPEL and SOA Are Changing Web Services Development. IEEE Internet Computing 9(3), 60–67 (2005)
20. Mule Technical Committee, "Mule 2.0", Release Candidate 2 (2008), `http://mule.mulesource.org`
21. OASIS Web Service Secure Exchange Technical Committee, OASIS WS-Trust 1.3, OASIS Standard (2007)
22. SWEB consortium, D4.1: SWEB platform development report, European Commission, Belgium (2008)

Economics of Personal Data Management: Fair Personal Information Trades

A. Tasidou, P.S. Efraimidis, and V. Katos

Department of Electrical and Computer Engineering,
Democritus University of Thrace,
Vas. Sophias 12, 67100 Xanthi, Greece
{atasidou,pefraimi,vkatos}@ee.duth.gr

Abstract. Individuals today have no control over the way their personal information is being used even though they are the ones to suffer the consequences of any unwanted uses of their information. We propose addressing this externality through the creation of a market for personal information, where licenses to access individuals' personal information will be voluntarily traded. Through this market, satisfactory compensation to the information owner is provided, whilst personal information remains under the owner's control. Using cryptographic tools and micropayments we propose and develop a prototype for personal information trades where the above principles are implemented and tested.

Keywords: Economics of Privacy, Information Markets, Privacy Enhancing Technologies.

1 Introduction

The protection of personal privacy and the negative externalities that arise from the exploitation of personal information have become growing concerns for Internet users, as pointed out in [1] and [12]. Individuals provide their personal information to companies during online transactions. This information lies at the company's disposal and can be used uncontrollably, violating data protection-relevant policies [3]. Such violations include secondary uses inside a company or even disclosing the information to third parties. Additionally, incidents of (un)intentional data loss are an almost daily occurrence [8]. This situation can bring great profits to the parties who exploit the information and significant costs to the information owners, both financial and security related.

On the other hand, by processing personal information important benefits are brought to the marketplace for both companies and customers. Therefore, a fair, effective and legitimate way to acquire individuals' personal information for processing should exist. Besides, the aspiration of privacy protection technology is not to lock all personal information away from any possible access or use, but to allow access to personal information in a controlled manner. Moreover, it is possible that individuals would be willing to provide access to (some of) their personal information in exchange for some profit, provided they could be assured of the safety of their information.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 151–160, 2010.

To this end, we consider the use of the Personal Information Market (PIM) concept, where access to personal information can be legitimately exchanged, providing at the same time mutual benefits to companies and individuals. In order for a PIM to be effective many challenges need to be addressed. First, it is important that personal information is exchanged in a way that misuse attempts are prevented or deterred. In this paper we address this challenge by using data licenses, which are based on cryptographic primitives. These licenses provide access to individuals' personal information under well specified conditions and therefore ensure that information owners do not lose control over their information.

We believe that an interesting analogy can be drawn between modern Internet users' privacy rights and developing countries producers' rights. Just like producers in such countries are vulnerable to work exploitation and suffer the consequences that arise from it, Internet users today suffer the exploitation of their personal information and the infringement of their privacy rights. Following this analogy, we propose an architecture named "*Fair Personal Information Trades*" (FPIT), that follows the principles of the Fair Trade movement, which offers better trading conditions to, and secures the rights of, marginalized producers and workers [20]. Just like Fair Trade, FPIT can support fair trades of personal information between information owners and information consumers, while protecting their information owners' privacy.

In our view, the necessary technology exists today for better personal information management to be realized. The ideas and principles have been developed earlier and now the enabling technologies are present, both in information science and telecommunications, for them to be put into practice. In order for this to happen, there is a need for public demand for privacy protection which will in turn motivate companies to change today's situation. Apart from that, the necessary tools that use the recent technological advancements to create better privacy preserving conditions for well meaning companies and individuals need to be developed.

The rest of this paper is structured as follows: In the following section we present some interesting related work. In Section 2 the FPIT concepts, architecture and components are described. In Section 3 the FPIT prototype is presented along with snapshots of test-runs. Finally, in Section 4 the contribution of this work is discussed, along with some open problems and some possible extensions and applications of FPIT.

Related Work

One of the first proposed markets for personal information was Laudon's National Information Markets [16], where personal information can be traded through a National Information Exchange. There are two major differences between Laudon's NIM and FPIT. First, in this work we follow a distributed approach, where no third parties are involved for the information exchange. Second, in FPIT the personal information itself is never sold. Temporary access to personal information is sold, by means of appropriate licenses. Information users have to acquire information from their owners each time they need to use it, paying a small fee every time.

A decentralized approach for information markets is Information Crystals [2]. This model aims at creating large groups of personal information, to be used aggregated for data mining, while protecting the owner's privacy.

An interesting work that implements the idea of Personal Information Market (PIM) is [9]. In that approach, only preference and behavioral information is for sale and therefore privacy protection is achieved by keeping Personal Identifiable Information (PII) undisclosed. PII is defined as any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. In our work, both PII and preference/behavioral information can be exchanged. We argue that companies should be able to acquire individuals' contact information, with their consent, for marketing purposes. We address the problem of privacy protection by using data licenses and the convention that no information is allowed to be stored at the company's side. Another important differentiator is that our platform does not rely on the existence of trusted third parties for transferring personal information.

Contemporary privacy enhancing technologies are presented in [8]. An interesting analysis on the economic aspects of personal privacy and how market mechanisms might solve privacy problems is presented in [19]. The economics of privacy are also discussed in [4,13,15,14,11].

An insightful analysis of the different approaches to personal information protection, including market-based approaches is presented in [10]. In that work the conclusion is drawn that it is very difficult to protect from unauthorized information copying and distribution. This is especially important for personal information, because there is no way of preventing a person allowed to see the information once, from writing it down on a piece of paper. This problem could be addressed by requiring information users to exhibit licenses from the information owners, entitling them to use this piece of information for this particular purpose. The benefits from the use of data licenses are discussed in [5].

2 Fair Personal Information Trades

In the following sections we provide a description of the FPIT concepts and its proposed architecture.

2.1 Concepts and Architecture

The basic principle of FPIT is that the control of personal information should be maintained by its owner. Therefore, companies are not allowed to store individuals' personal information and use it without their consent. The main players in FPIT are the following:

– *Individuals* who voluntarily participate in FPIT, selling access to their personal information.
– *Companies* interested in collecting and processing personal information.

These players are represented in the FPIT architecture by the *entity* component. Both individuals and companies can be called *FPIT-users*, or just *users*.

The resources traded in FPIT are licenses to access personal information of individuals. This renders the task of storing, managing and retrieving personal data a very critical operation in FPIT.

2.2 Personal Data Management in FPIT

In order for FPIT to work efficiently, it must contain a privacy enhanced subsystem for the storage of the individuals' personal data. We call this subsystem the "Personal Data Management System" (PDMS). Due to the nature of FPIT, the management of personal data has to meet the following requirements:

- Personal data can only be stored at the owner's side.
- Personal data must always be accessible for licensed use.
- Information security must be ensured and information leaks should be prevented.

A system that satisfies the above requirements for the management of personal information is the Polis platform described in [6]. In Polis, for every individual there is a personal agent, which is constantly accessible over the Internet. The agent contains the personal information, the policies and the contracts of the individual. Each company also has its own agent, which contacts individuals' agents in order to retrieve (some of) their personal information. The functionality and services of the agents in Polis can be extended by implementing appropriate (cryptographic) protocols. We use this feature in the implementation of the FPIT prototype.

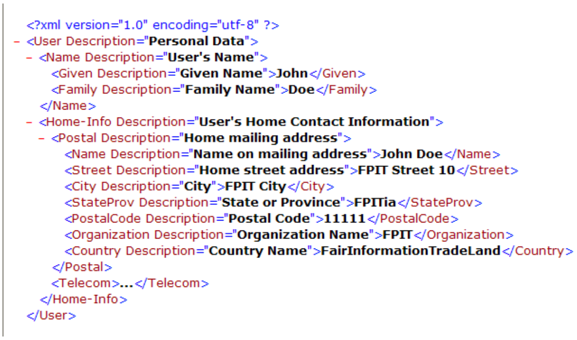
2.3 FPIT-Users

Each FPIT-individual entity is characterized by its personal information and its policies. This architecture can be expanded to contain more sophisticated components, like a transaction logging service or a negotiation mechanism.

In order for FPIT to work efficiently, its agents need to have reliable Internet connectivity. This requirement is straightforward for companies. As far as individuals are concerned, constant connectivity is quite common today and is soon expected to become a given. Nevertheless, the protocol for personal information exchange described below could be implemented in such a way, that even if the agent of an information provider loses connectivity, there will be no monetary loss for the companies this user interacted with.

Personal Information Representation

Personal Information traded in FPIT can be Personal Identifiable Information (PII), like the name, phone number, address, birth date etc, as well as preference and behavioral information of a person. However, as this is work in progress, we decided to first examine the market for trading PII. It is straightforward, though, to expand FPIT to deal with preference and behavioral information as well.



```
  <?xml version="1.0" encoding="utf-8" ?>
- <User Description="Personal Data">
  - <Name Description="User's Name">
      <Given Description="Given Name">John</Given>
      <Family Description="Family Name">Doe</Family>
    </Name>
  - <Home-Info Description="User's Home Contact Information">
    - <Postal Description="Home mailing address">
        <Name Description="Name on mailing address">John Doe</Name>
        <Street Description="Home street address">FPIT Street 10</Street>
        <City Description="City">FPIT City</City>
        <StateProv Description="State or Province">FPITia</StateProv>
        <PostalCode Description="Postal Code">11111</PostalCode>
        <Organization Description="Organization Name">FPIT</Organization>
        <Country Description="Country Name">FairInformationTradeLand</Country>
      </Postal>
      <Telecom>...</Telecom>
    </Home-Info>
  </User>
```

Fig. 1. Personal Information in FPIT

Personal Information can be represented in an XML schema like the one shown in Figure 1. This representation is simple and efficient enough to suit the needs of FPIT. Personal information is organized hierarchically in a number of categories, each of which can contain appropriate subcategories. This scheme can be expanded according to the implementation and usage needs of FPIT.

Policies and Licenses

Policies are integral components of FPIT trades. Agent policies define whether the agent will accept or reject a transaction request. A policy, represented in an XML schema, contains the following fields:

- *Principals*: The FPIT-entities.
- *Info-item*: Every distinct item of an information provider's personal information.
- *Purposes*: The set of purposes that entitle principals to retrieve data. Some indicative purposes are promotion and statistics. Further additions could be made according to specific transaction needs.
- *Usage restrictions*: Additional restrictions may exist that limit access rights to a specific number of accesses or a specific time interval, or both.
- *Charge*: Value and unit of payment and conditions for charging.

Another important component/concept of this architecture is the license. A license is used to set the rules under which a company is entitled to have access to an individual's personal information. Licenses play a key role in this work, since they are the mechanism that controls personal information use and distribution.

The architecture overview of FPIT is presented in Figure 2.

2.4 Payments in FPIT

The payment scheme within FPIT needs to be efficient enough to facilitate large numbers of small amount payments, without entailing substantial transaction costs. Therefore, we consider that micropayments as proposed in [17], suit the aforementioned needs.

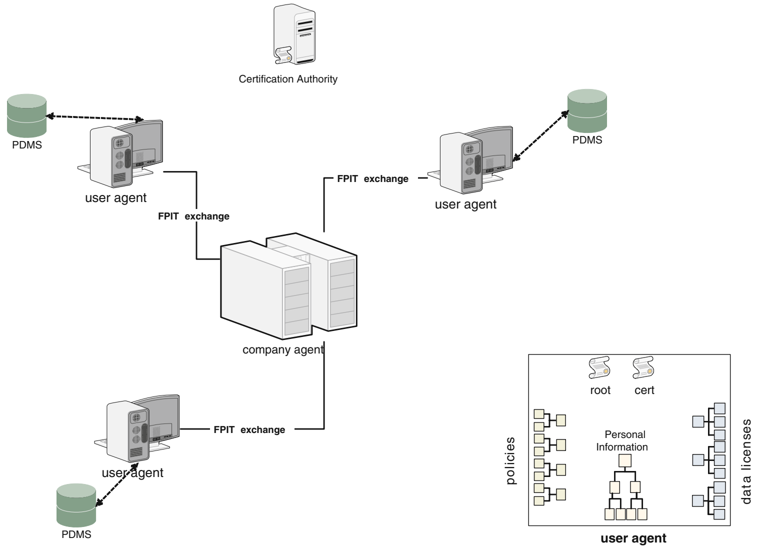


Fig. 2. The FPIT architecture overview

The main actors in micropayment schemes are Brokers, Vendors and Users. A User becomes authorized to make micropayments by the Broker. A Vendor receives micropayments from authorized users and redeems them through the Broker. Relationships of Users and Vendors with the Broker are long term. The micropayment scheme we use in FPIT is Payword, presented in [17]. Payword is a credit-based scheme, based on chains of hash values (Paywords). Due to lack of space, the Payword protocol is not presented. For more information you can go to [17] or the long version of this paper [18].

2.5 Trading Process in FPIT

Locating potential personal information providers can be achieved in several ways. The first and simplest solution is for companies to use their own clientèle database which would contain the agents' contact information of the clients that were interested in participating in personal information trades. Apart from that, other possibilities exist, like the creation of whitepages for participating individuals, or even participating agents' contact information exchanges between companies. In this work, we consider the act of locating the information provider already accomplished and propose a protocol for the actual exchange of the personal information.

As far as pricing is concerned, i.e., the price per personal information item access, this is set to a fixed price of one Payword coin (usually representing the value of one cent). A pricing policy could be used in order to allow individuals to set different prices on their information items. For example, a person's phone number could be more expensive than their age. Prices could also vary depending on the time of day or the season of the year. For example, acquiring one's phone number to call them during the evening or holidays could be more expensive. Pricing rules or even negotiation mechanisms could be introduced in future versions of FPIT.

Informal Description of Protocols

Once a company (information buyer) finds the contact information of an information provider's agent, the trading process can begin. The information trading process in FPIT consists of two phases: The Initial Agreement phase and the Purchase phase. These phases are described below:

During the Initial Agreement phase the following actions occur:

1. The information buyer contacts the information owner, sending a message about the kind(s) of personal information they are interested in, the period of time for which they are requesting access to the information and the price they are willing to pay for it. For example, an online shop might be interested in a person's e-mail for one year in order to send them promotional e-mails with offers and be willing to pay one coin for each e-mail.
2. The information owner's agent receives the request, checks whether it complies with its policies and responds accordingly.
3. If the request is accepted, the information buyer agent sends the commitment M, according to the Payword protocol.
4. The information owner verifies the buyer's certificate according to the Payword protocol.
5. If the verification is successful, a license is sent to the buyer, entitling them to the requested access to the owner's personal information.

After having established the initial agreement with the data owner, the data buyer can make several purchases, according to the agreed upon license. During a Purchase phase, the following actions take place:

1. The data buyer requests a specific item of personal information.
2. The owner's agent receives the request and verifies the accompanying license.
3. If the license is valid, an ACCEPT message is sent to the buyer's agent (verifying at the same time that the owner's agent is up).
4. The buyer sends the payment for the requested items according to the Payword protocol.
5. The owner's agent sends the requested information.

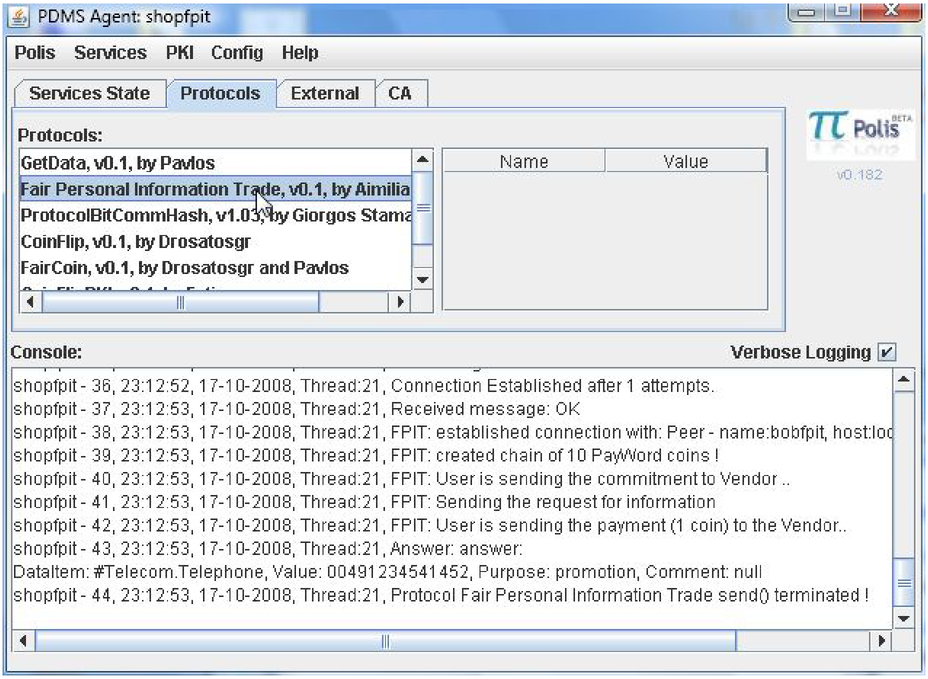
Using this protocol companies are protected from potential malicious information providers. The access to the personal information is not prepaid at the Initial Agreement phase and thus, information providers cannot receive their payment and disappear. Payment occurs each time an information item is requested. Therefore, the company can confirm that the information provider's agent is up before making any payments. The only way for an information provider to cheat is to receive the coin for the particular information item requested and then disappear. Even then, the gain for the information provider as well as the loss for the company will be minuscule. Besides, the company can always revoke the stolen Payword coin at the Broker.

3 The FPIT Prototype

We implemented an FPIT prototype and performed proof-of-concept experiments. The main objective was to become acquainted with the practical difficulties intrinsic to a platform like FPIT. The prototype is implemented in *Java*. We use the *Bouncycastle* library for the cryptographic primitives. The management of the personal data is done with the Polis platform developed in [6]. The Payword micropayments used in the prototype are an adaptation of the Payword implementation in [7].

The development of the prototype proved to be straightforward. We used the following components for the experiment: An FPIT-shop, two FPIT-individuals and a Broker. The scenario of the experiment was that a shop named *shopfpit* buys and retrieves personal information from two FPIT-individuals, *alicefpit* and *bobfpit*. A snapshot of an agent used in FPIT is given in Figure 3.

In the FPIT prototype, we employ some security measures: the communication is performed over SSL sockets with both server and client authentication enabled. Contracts are digitally signed by both parties. However, at this stage we did not address malicious behavior or general fault tolerance issues. We are mainly interested in verifying the basic operations involved in the FPIT transactions and their efficiency. The main outcome of the experiments is that all the building blocks of the FPIT-platform work well. This confirms that the basic functionality of FPIT is attainable.



Protocols:

- GetData, v0.1, by Pavlos
- Fair Personal Information Trade, v0.1, by Aimilia
- ProtocolBitCommHash, v1.03, by Giorgos Stama
- CoinFlip, v0.1, by Drosatosgr
- FairCoin, v0.1, by Drosatosgr and Pavlos

```
shopfpit - 36, 23:12:52, 17-10-2008, Thread:21, Connection Established after 1 attempts.
shopfpit - 37, 23:12:53, 17-10-2008, Thread:21, Received message: OK
shopfpit - 38, 23:12:53, 17-10-2008, Thread:21, FPIT: established connection with: Peer - name:bobfpit, host:loc
shopfpit - 39, 23:12:53, 17-10-2008, Thread:21, FPIT: created chain of 10 PayWord coins !
shopfpit - 40, 23:12:53, 17-10-2008, Thread:21, FPIT: User is sending the commitment to Vendor ..
shopfpit - 41, 23:12:53, 17-10-2008, Thread:21, FPIT: Sending the request for information
shopfpit - 42, 23:12:53, 17-10-2008, Thread:21, FPIT: User is sending the payment (1 coin) to the Vendor..
shopfpit - 43, 23:12:53, 17-10-2008, Thread:21, Answer: answer:
DataItem: #Telecom.Telephone, Value: 00491234541452, Purpose: promotion, Comment: null
shopfpit - 44, 23:12:53, 17-10-2008, Thread:21, Protocol Fair Personal Information Trade send() terminated !
```

Fig. 3. FPIT agent snapshot

4 Discussion

We believe that Fair Personal Information Trades provides a straightforward proposal that could constitute a regulatory solution to the large scale privacy invasion that is currently perpetrated. In particular, FPIT sets well-defined, clear rules for the proper utilization of personal information, giving the ability to individuals to control and decide upon how information about themselves is used. Additionally, it provides a legitimate and fair, yet efficient enough, way for companies to acquire dynamic, up-to-date information, relevant to the purpose of their intended use. Hence, FPIT attempts to reduce information collecting companies' unrestrained personal information exploitation and motivates them to behave more responsibly. In general, FPIT puts the idea of compensating the information owner into practice. It ensures that individuals who provide information are compensated for their service, while their personal information is being protected, at least as much as it is protected currently, but most possibly even more. Finally, it successfully combines the use of data licenses with the ideas of information markets and micropayments to propose a broader solution for trading personal information.

Open Problems and Future Work

The underlying issues related to FPIT have a wide and transdisciplinar scope, as there are social, economical and technical challenges which need to be addressed. The following issues and problems have been identified, which mainly lie in the technical domain, as the main volume of our research is technically focused:

- Cryptography is sought to be the main technical enabler of the proposed infrastructure. As such, all (cryptographic) goals should be defined in order to evaluate the soundness of the underlying cryptographic protocols.
- Currently there is no distinguisher that can deterministically separate personal identifiable information from personal information. This leads to considering by default all personal information as identifiable, which forces the application of legislative protective controls to the whole data set, which in turn reduces efficiency of the proposed infrastructure.
- The proposed framework needs to revisit the business partnering model, as this constitutes well accepted business practices and excluding this from the framework is not a realistic assumption.

References

1. Acquisti, A.: Privacy and security of personal information: Technological solutions and economic incentives. In: Camp, J., Lewis, R. (eds.) The Economics of Information Security, pp. 165–178. Kluwer, Dordrecht (2004)
2. Adar, E., Huberman, B.A.: A market for secrets. First Monday 6, 200–201 (2001)
3. Anderson, R.: U.k. government loses personal data on 25 million citizens. EDRI-gram 5.22 (November 21, 2007)
4. Anderson, R., Moore, T.: The economics of information security. Science 314(5799)

5. Cha, S.-C., Joung, Y.-J.: From p3p to data licenses. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 205–222. Springer, Heidelberg (2003)
6. Efraimidis, P.S., Drosatos, G., Nalbadis, F., Tasidou, A.: Towards privacy in personal data management. Accepted for publication in Information Management and Computer Security, Emerald
7. Georgakopoulos, G.: Privacy enhancing technologies for personal data management. Master's thesis, Dept. Electr.& Comp. Eng., DUTH, Greece (October 2008)
8. Goldberg, I.: Privacy-enancing technologies for the internet iii: Ten years later. In: Acquisti, A., Gritzalis, S., Lambrinoudakis, C., di Vimercati, S. (eds.) Digital Privacy: Theory, Technologies, and Practices, December 2007, ch. 1 (2007)
9. Gopal, R., Garfinkel, R., Nunez, M., Rice, D.: Electronic markets for private information: Economic and security considerations. In: HICSS 2006: Proceedings of the 39th Annual Hawaii International Conference on System Sciences, Washington, DC, USA. IEEE Computer Society, Los Alamitos (2006)
10. Greenstadt, R., Smith, M.D.: Protecting personal information: Obstacles and directions. In: WEIS 2005 (2005)
11. Gritzalis, S.: Enhancing web privacy and anonymity in the digital era. Information Management and Computer Security 12(3), 255–287 (2004)
12. Bernardo, A.H., Adar, E., Fine, L.R.: Valuating privacy. IEEE Security and Privacy 3(5), 22–25 (2005)
13. Katos, V., Patel, A.: A partial equilibrium view on security and privacy. Information Management & Computer Security 16, 74–83 (2008)
14. Katsikas, S.K., Lopez, J., Pernul, G.: Trust, privacy and security in e-business: Requirements and solutions. In: Bozanis, P., Houstis, E.N. (eds.) PCI 2005. LNCS, vol. 3746, pp. 548–558. Springer, Heidelberg (2005)
15. Kleinberg, J., Papadimitriou, C., Raghavan, P.: On the value of private information. TARK: Theoretical Aspects of Reasoning about Knowledge 8 (2001)
16. Laudon, K.C.: Markets and privacy. Commun. ACM 39(9), 92–104 (1996)
17. Rivest, R.L., Shamir, A.: Payword and micromint: two simple micropayment schemes. In: CryptoBytes, vol. 2, pp. 69–87 (1996)
18. Tasidou, A., Efraimidis, P.S., Katos, V.: Economics of personal data management: Fair personal information trades. Technical Report LPDP-2009-01, Dept. Electr.& Comp. Eng., DUTH, Greece (2009)
19. Varian, H.: Economic aspects of personal privacy. U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age (1996)
20. Wikipedia. Fair trade, http://en.wikipedia.org/wiki/Fair_trade

Evaluating Common Privacy Vulnerabilities in Internet Service Providers

Panayiotis Kotzanikolaou, Sotirios Maniatis, Eugenia Nikolouzou, and Vassilios Stathopoulos

Hellenic Authority for Communications Privacy (ADAE)
{p.kotzanikolaou,s.maniatis,e.nikolouzou,v.stathopoulos}@adae.gr

Abstract. Privacy in electronic communications receives increased attention in both research and industry forums, stemming from both the users' needs and from legal and regulatory requirements in national or international context. Privacy in internet-based communications heavily relies on the level of security of the Internet Service Providers (ISPs), as well as on the security awareness of the end users. This paper discusses the role of the ISP in the privacy of the communications. Based on real security audits performed in national-wide ISPs, we illustrate privacy-specific threats and vulnerabilities that many providers fail to address when implementing their security policies. We subsequently provide and discuss specific security measures that the ISPs can implement, in order to fine-tune their security policies in the context of privacy protection.

Keywords: Internet Service Provider, Privacy, Vulnerabilities, Security Measures.

1 Introduction

Due to the social impact of privacy [1,2], the legislation in many countries explicitly recognizes privacy in electronic communications as a fundamental human right. In this context, the European Union has issued Directives concerning the privacy in electronic communications [3], while the EU member states are responsible to harmonize their legislation with the related Directives. Moreover, in several countries Independent Authorities are responsible to regulate and audit the proper implementation of privacy protection in electronic communications, see for example the Hellenic Authority for Communications Privacy (ADAE) [4].

Privacy in electronic communications refers to the right to communicate in private with others through a publicly available communication network or service. An electronic communications network may be a fixed line telephone network (such as PSTN or ISDN), a mobile network (such as GSM or UMTS), a wireless network (such as WiFi, Wimax, or Satellite), or a packet-based communication network such as the Internet or an add-on service, such as e-mail and voice over the Internet protocol (VOIP) services. Communication privacy involves the protection of all the communication data that are processed, stored and traversed through a public communication network or during the provision of an electronic communications service. Communications data can be distinguished in two broad categories [5]:

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 161–170, 2010.

- *Content data*, which comprise the actual content of the communication, and
- *Context data*, which are the external data of a communication, used for the establishment and provision of a communication.

The disclosure of the context data will in most cases affect the anonymity of the communicating parties. In some cases it may also affect the privacy of the actual content. For example, the context data during a web-surfing will also leak information concerning the actual content of a communication, since the IP address of the destination can easily be resolved to the related URL, which in turn can be accessed in order to describe, at least partially, the content of the communication.

Although privacy assurance requires the active involvement of both the user and the ISP, in this paper, we only focus on the role of the provider. Assuring the privacy from the ISP side requires a combination of technical, procedural and regulatory measures, based on ISP-specific security risks and security standards, either generic (e.g. ISO 27001:2005 [6]) or telecommunication specific (e.g. ITU-T X.1051 and ISO/IEC 27011 [7]). However, our experience has shown that although the vast majority of the ISPs have implemented security management programs, several common vulnerabilities exist, which can be exploited in order to violate the privacy of communications.

In this paper, we describe common security vulnerabilities of the Internet Service Providers (ISPs), which may lead to breach of communication privacy for their users. The results presented in this paper have emerged from a preliminary round of external security audits performed in a number of Internet Service Providers, operating in Greece. Moreover, we describe possible security measures to thwart these vulnerabilities. The rest of the paper is structured as follows. Section 2 describes the basic systems within the ISP environment, which are critical for the assurance of privacy in communications. Then it describes privacy-specific security threats that can endanger communications privacy. Section 3 points out common vulnerabilities that have been identified within the ISP environment and which may be exploited by privacy-specific threats in order to reveal communication data of the users. Also, it describes possible security measures that should be applied, in order to minimize the identified vulnerabilities and prevent privacy breaches. Finally, Section 4 concludes this paper.

2 Privacy Related Critical Systems and Threats

Most of the systems that are within the ISP's responsibility, handle communication data. For example, network elements such as routers and switches are used to enable the connectivity of a communication, and IT systems such as mediation devices and billing systems process communication data.

To start with, active network elements, such as wired or wireless access (layer-2) devices, switches, soft-switches, and routers, among others, are the primary systems that have to be protected, since they handle both user communication data (both content and context data), as well as signaling data, which still can reveal a lot of information about the user. If such a system is compromised, then a simple traffic analysis will reveal the actual communication, e.g. by extracting the contents of an email out of the TCP packets captured.

Table 1. Critical systems in relation to privacy

Category of System	Specific system	Criticality level in relation to privacy
Active Network Elements	Layer-2 access devices	Medium to High
	Routers	High
	Switches	Medium to High
	Soft-switches	High
IT Systems	E-mail servers	Very High
	Media gateways	High to Very high
	VoIP servers	High
	Web proxies	High
	P2P proxies	High
Passive Network Elements	Monitoring devices	Medium to High
	Management Devices	Medium to High
	Software tools & computers	High
	Data storage devices	High
Specialized Systems	Call Data Record systems	Very High
	Lawful Interception systems	Very High
	Data Retention systems	Very High
	Call Center systems	Very High

Apart from active network elements, IT systems that are related to specific communication services, like email servers, media gateways, Voice over IP (VoIP) servers, web proxies, peer-to-peer (P2P) proxies, etc., comprise an even more significant factor, since they contain the actual content and context of a user's communication (emails, visited web pages, voice sessions, etc).

Another type of critical systems from a privacy perspective is the passive network elements, such as monitoring and management devices, software tools and computers, and communication data storage devices. Such systems are important not only because they may allow direct access to communication data, but also because they can reveal accountability-related information, such as logical access to systems, administrative actions, and security-related incidents, among others.

Last but not least, there are specialized systems that may provide direct access to communication data due to operational or law enforcement requirements. The most imperative systems of this kind are systems that handle Call Data Records (CDRs), Lawful Interception systems and Data Retention systems.

2.1 Privacy-Specific Threats

Based on audit results performed on ISPs in Greece, we have identified the most commonly found privacy threats and we have mapped these threats to specific systems that are subject to these threats.

To ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible.

If screenshots are necessary, please make sure that you are happy with the print quality before you send the files.

1. **Masquerading by internal users.** This involves an internal user accessing a system by using an existing identity belonging to another internal user. In the environment of ISPs it has been found that it is common practice to use loose authentication and authorization policies for the internal users, despite the fact they are very strong for the external users. For example, the administrators of network elements or IT systems may share common usernames and passwords.
2. **Unauthorized use of data/systems/applications.** In addition to the above, it is quite common to find internal users with access privileges to sensitive applications and systems, although these users do not have official authorization, according to the security policy of the organization. This may involve systems managing CDR files and Call Center calls, which usually give access to sensitive communication data. Unauthorized use can be intentional or unintentional e.g. by misconfiguring access procedures and access rights.
3. **Embedding of malicious software.** Embedding of malicious software in systems like email servers or proxy servers may lead to loss of privacy for hundreds of users, if this is not noticed in time. A simple example is the installation of a passive interception tool which may monitor all the traffic in promiscuous mode.
4. **Communication infiltration/manipulation.** These threats mainly concern active network elements. Communication infiltration/manipulation may be the result of unauthorized use or of malicious software installed in an active network element. This will then put at risk the privacy of all the communications routed through the compromised network element.

3 Common Privacy Related Vulnerabilities and Possible Measures

Most of the systems that are within the ISP's responsibility, handle communication data. For example, network elements such as routers and switches are used to enable the connectivity of a communication, and IT systems such as mediation devices and billing systems process communication data.

3.1 User Account Management

User account management is a common area of user-related vulnerabilities in many systems with a large number of users. Concerning user account management, the following vulnerabilities have been identified:

1. ***Lack of personalized access and lack of accountability.*** The results from our security audits in various ISPs showed that within the ISP environment, it is quite common that the administrators share the same username/password, especially for systems such as edge routers in PoPs, proxy servers and WCS. This is also the case in remote management through dial-up. The modem is usually configured only with a single username/password shared among different administrators. Obviously this makes hard to ensure the accountability of the users and makes

the internal systems vulnerable to masquerading attacks by insiders, despite the fact that administrators are usually highly skilled and trusted users. Although the use of unique, personalized passwords introduces increased password management costs, these costs should be accepted by the providers it order to minimize possible impersonation attacks and lack of accountability.

2. ***Authorization control.*** Although the security policies of the ISPs involve periodic audits of user authorization privileges, this is rarely the case in the real environment. In several providers, accounts belonging to former employees have been found active, even in critical systems which are expected to be audited in short periods, such as the CRM. The lack of periodic audits has also lead to the existence of accounts with more privileges than the authorized ones. Such inconsistencies can be minimized if the security officer centrally maintains the personnel privilege management, by maintaining lists with the personnel access privileges as well as the possible changes to those privileges. On the other hand, the internal auditor should perform internal audits in critical systems, by matching the authorized user privilege lists against the actual user accounts.
3. ***Separation of duties.*** Most critical systems do not support the separation of duties between different kinds of users. For example, the system root/administrator can perform both the administrative and auditing action. This separation can be enforced by applying role-based access control (RBAC) systems. However, most versions of the widely used operating systems cannot support RBAC. This enables the system administrator to have access to the system logs, even if he may not formally be authorized to act as the system auditor.
4. ***Password management.*** Password management weaknesses have been identified in several systems within the ISPs. A commonly found security weakness is the use of unencrypted passwords for the initialization of user email accounts. Although these passwords are only used for the initialization of the account and this should not be considered as an important weakness, in some providers there is no automated policy in place to enforce password change after the first user connection to the e-mail service. The lack of password change enforcement policy is more common in web-based e-mail services. Another weakness found in the ISP environment related with password management is the use of admin accounts for ordinary purposes, despite the fact that the system administrators usually have different accounts for administrative purposes and for common purposes.

3.2 Logging and Auditing

System logging and auditing are the most valuable controls for the detection of security breaches, policy mis-configurations and system vulnerabilities.

1. ***Secure logging mechanisms.*** In most cases the ISPs maintain logging information that concerns system miss-configurations, erroneous operations or system performance evaluation, such as syslog information. In terms of security, user access logs are the most valuable log traces that are used by them. This information is not enough for guarantying the acceptable level of information privacy within the ISP premises. Indeed, system (network or IT) configuration files, application configuration files and executed commands (accounting) all consist of useful

security resources for preventing security breaches. More specifically regarding the network systems logging should also include the administrators' commands, as well as events retrieved from the AAA server including authorization, authentication and accounting logging. Regarding the IT systems, the transactions involving critical systems such as the Billing system, the CDRs and the e-mail servers should also be logged. A log file storing architecture should be also considered as an important security requirement. Experience shows that a centralized storage architecture with supportive distributed storing points is the most security effective method, since it provides a centralized control to the logging information, while the distributed storing points may support communication failures or achieve load balancing of log data when that is necessary. For information that is usually stored temporary in local memory (e.g. command history in IT systems) it should be transferred to permanent files at the earliest convenience. Also, the distributed storage points may be used in order to verify the integrity of the centralized log files. Since the logged events may contain context communication data of end-users, the confidentiality and the integrity of the logged data should be protected. Secure logging can be based on well-defined architectures and cryptographic techniques (e.g. [8,9]). The integrity of the log files can also be supported by applying immutable storage devices, such as WORM (Write Once Read Many) media.

2. ***Internal auditing controls.*** In most of the examined ISPs the already maintained log files can provide useful information for the identification and correction of possible security flaws and system mis-configurations. This however requires effective internal auditing procedures to be in place, in order to process and correlate the existing logging information. An ISP that uses secure logging for preventing security breaches should combine logging with effective auditing procedures. Auditing techniques can be continuous or periodic. Its aim is to identify the cause of a security incident and sometimes it gives evidences for identifying a security incident.

3.3 Contractors and Third Parties

A significant set of vulnerabilities discovered during our preliminary audits is related with the implicit trust assumptions between the ISP and its subcontractors or collaborating third-parties.

1. ***Trust Relationship between ISP and manufacturer.*** There is a substantial relation of dependence between the ISP and the various manufacturers of the systems used within the ISP. A manufacturer usually participates in all phases of a system's lifecycle within an ISP: from installation and configuration to support and maintenance. Thus, the manufacturers may gain knowledge of the network architecture and/or the configuration of various systems within the ISP. Moreover, in several cases the system/software manufacturers may have access to internal systems for maintenance reasons, which may lead to intended or unintended actions against users' privacy. Providers usually use state of the art technical and procedural measures to protect themselves from the potential harm of unauthorized use by the manufacturers, such as access controls, logging of operations performed

by the manufacturer, and control of components or patches to be installed through e.g. digital signatures, among others. We observed however that not all ISPs had similar levels of protection. Moreover, we observed that sometimes even ISPs with the strictest measures, in case of an emergency, could neglect formal access control procedures. Nevertheless, these measures are not a panacea. A manufacturer's expert, taking advantage of his explicit knowledge of the system, is potentially able to perform some actions that could pass over all the technical measures set by the ISP and therefore threaten communications privacy without being perceived. Unfortunately trust cannot be based on technical measures only. Trust is built over time and is further related with non-technical issues such as organizational reputation. It can also be based on strict bilateral agreements. However, the accurate enforcement of state of the art measures, frequent control of the system and reporting to technical managers, and frequent and in depth training of ISP's employees to gain good knowledge of the system, can eliminate the risks, although they demand additional resources (manpower, time, money).

2. ***Interconnection through other providers.*** The networks of the ISPs need to be inter-connected, in order ot provide world-wide connectivity to their subscribers. For example the communication data from a tier-3 ISP is forwarded between two regions through a tier-2 ISP interconnection. Data is usually not encrypted during transmission, so there is no technical guarantee that the interconnecting provider will maintain the same levels of protection. In case of a privacy incident, it is not always easy to technically discriminate the responsibility in case of interconnected providers. Trust comes into play again. Organizational reputation and bilateral agreements are the common measures followed by providers. For relatively low bandwidth interconnections, encryption or some kind of a VPN tunnel could provide a technical mean to overcome this vulnerability. For high bandwidth interconnections, the risk to analyze transmitted communication data is low because of the intrinsic difficulty to accomplish that and therefore current business models based on trust seem adequate. Regulatory controls can also provide a level of protection, by legally enforcing a common level of security for all the providers.
3. ***Provision of value-added services through third parties.*** The ISPs usually rely on third parties to provide some individual services. This is very common with billing services and value-added services (e.g. email). Of course such a provisioning increases the privacy related risks for the processed communication data. As in the case of interconnections, regulatory controls may legally enforce a common level of security controls for all the involved third parties, under the supervision and responsibility of the ISP. Enforcement of this rule however is not always straightforward, especially in the case of a third party organization residing in a foreign country where regulations may impose different security and privacy levels. Additionally, the ISP or the home regulator is difficult (or even impossible) to control the security level of the third party.
4. ***Co-location of systems.*** It is quite common that systems of various providers are physically co-located in the (shared) premises of a third provider. This makes easy for the administrators of one provider to physically access the systems of another provider. Moreover, in several cases it has been found that contractors of

providers or other third parties gain unattended physical access to the systems. In these cases, physical access control must be strengthened and vigorously enforced, in addition to existing logical access control measures, which may protect the systems from unauthorized use.

3.4 Perimeter and Network Security

This part of the auditing procedure was focused on the perimeter security of the provider's network, and specifically with well known-entities: firewall, intrusion detection and/or prevention systems, anti-virus/anti-spam software. The basic outcome is that providers are well-informed of the importance of those systems; however the actual implementation and proper monitoring reveals many weak points. A common practice found was the operation of network security systems under the initial default settings, without examining their suitability to the providers needs and without regular inspection of the produced results (e.g. log files).

Another major report was the inadequate antivirus/anti-spamming protection of internal networks. In some cases it has been found that the internal network of the ISPs is not adequately protected against virus and malware. Although in all cases anti-virus programs are used, in some cases no central antivirus administration is used, which may lead to outdated antivirus. Moreover, solutions that eliminate spam, phishing attacks, spyware are rudimentary operating without adequately protecting the internal users.

It is also worth reporting some issues concerning remote management of the network elements. It would be advisable to generally deny remote management and exceptionally allow under specific security restrictions; for certain cases and for certain users. For example, router management in many cases is performed using telnet over the insecure Internet. SHH2 is a secure replacement of telnet and the r-utilities, which provides strong authentication and encrypted communication over the Internet.

In case of a line-down event, modems are reported to be used for remote connection to routers, where the username/password pair is the only security measure. It would be advisable to restrict remote access from specific remote locations (e.g. IP addresses) using access lists and additionally to lock users after a certain number of unsuccessful login attempts.

3.5 System and Network Maintenance

The main report was the lack of systematic recording of the maintenance/installation/repair actions planned or performed on systems/networks, e.g. in a powerful ticketing system. This should be also coupled with a well maintained inventory of systems/networks, e.g. to allow for searching all actions performed in a certain device for a certain period of time. The above would be beneficial also in an auditing procedure.

Usually, installation, maintenance, and repair actions are performed either on site or remotely without a predefined procedure and recording of the specific actions. This would stimulate malicious users to install malicious code as part of the official software in order to gain access to internal resources.

The above example attains significant weight if one considers the same situation with critical systems, like Lawful Interception and Data Retention System. The installation of an unwanted software module, e.g. passive monitoring tool may lead to the disclosure of sensitive information of thousands of subscribers.

The providers could ensure the authenticity and integrity of the system software, as well as its updates and patches by enforcing that each piece of software installed in the system is signed by means of a recognized electronic signature by its manufacturer. Moreover, key splitting could be used for any software changes together with electronic signatures. In this case, more than one authorized persons could cooperate to initiate the procedure of new or updated software installation.

4 Conclusion

The ISPs play a significant role in the protection of communications privacy. Even though most of the ISPs already employ a number of technical security measures to protect users communications privacy, the results from our external security audits report that a more effective and thorough application of technical, procedural and regulatory measures is required.

The importance of communications privacy mandates a thorough analysis and design of security policies to detect and prevent unauthorized and malicious actions by both insiders and outsiders. As it is shown by our preliminary auditing results, most ISPs do not always adequately apply the security measures set by their security policies in specific areas, such as user account management, logging and auditing, third party agreements, perimeter and network security, and system and network maintenance. Complementing an ISP’s security policy with the proper handling of the aforementioned issues can provide a good level of guarantees on the protection of the communications privacy. We are going to further extend those preliminary security results and provide a framework, which will guide ISPs to perform self-audits and strengthen their network defense in support of communications privacy.

References

1. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review IV(5), 193–220 (1890)
2. The European Opinion Research Group: European Union citizens’ views about privacy, Special Eurobarometer 196 (December 2003)
3. Directive 2002/58/EC of the European Parliament and of the Council: On Privacy and Electronic Communications, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Official J. European Union, July 12 (2002)
4. The Hellenic Authority for Communications Privacy (ADAE), `http://www.adae.gr/adae/index.html?langid=en`
5. Zugenmaier, A., Claessens, J.: Privacy in Electronic Communications. In: Douligeris, C., Serpanos, D.N. (eds.) Network Security: Current Status and Future Directions, pp. 419–440. IEEE-Wiley (2007)
6. ISO/IEC 27001:2005 Information technology – Security techniques – Specification for an Information Security Management System (2005)

7. ISO/IEC 27011 Information technology – Security techniques – Information security management guidelines for telecommunications (draft), will be published jointly as ITU-T X.1051 and ISO/IEC 27011
8. Stathopoulos, V., Kotzanikolaou, P., Magkos, E.: A Framework for Secure and Verifiable Logging in Public Communication Networks. In: López, J. (ed.) CRITIS 2006. LNCS, vol. 4347, pp. 273–284. Springer, Heidelberg (2006)
9. Stathopoulos, V., Kotzanikolaou, P., Magkos, E.: Secure Log Management for Privacy Assurance in Electronic Communications. Elsevier Computers & Security 27(7-8), 298–308 (2008)

Intellectual Property Rights Protection in Peer to Peer Networks

Georgios Stylios[1] and Dimitrios Tsolis[2]

[1] Department of Applications of Informatics in Management and Economy,
TEI of Ionion, Greece
stylios@teiion.gr
http://epdo.teiion.gr

[2] Computer Engineering and Informatics Department, University of Patras, Greece
dtsolis@upatras.gr
http://www.ceid.upatras.gr

Abstract. Peer to Peer Networks are oftenly used by internet users to share and distribute digital content (images, audio and video) which is in most of cases protected by the Intellectual Property Rights (IPR) legislation. This fact threatens e-inclusion and Internet democracy as a whole as it forces organizations to block access to valuable content. This paper claims that IPR protection and P2P can be complementary. Specifically, a P2P infrastructure is presented which allows broad digital content exchange while on the same time supports data and copyright protection through watermarking technologies.

Keywords: Computer networks, copyright protection, peer to peer networks, digital image processing, watermarking.

1 Introduction

Peer to peer networking is supported by suitable software which enables a computer to locate a content file (text, image, video, sound, software etc.) on another networked device and copy the encoded data to its own hard drive. P2P technology often is used to reproduce and distribute copyrighted content without authorization of rights owners. Except for digital music and video the P2P infrastructure is also used to make and distribute illegal copies of digital content which lies under the protection of the Intellectual Property Rights (IPR) legislation. For this reason the short history of P2P technology and software has been one of constant controversy by many in the content industry. The content owners are feeling even more threatened by the broad and unregulated exchange of digital content in P2P environments [2].

Proposed solutions for the organizations to the problem of IPR protection in the internet include simple business models and marketing strategies for organizations and corporations which are the digital content owner and application of complex technologies and systems [3]. These solutions tend to lock valuable educational and cultural content which is accessed only from private and restricted numbers of users threatening e-inclusion and the Internet democracy as a whole.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 171–178, 2010.

As a general protection measure for copyright violations through digital technologies including P2P, copyright owners often uses digital watermarking techniques to encrypt and watermark content or otherwise Digital Rights Management technologies to restrict access, totally blocking digital content to be accessed through the Internet and the P2P software infrastructure.

This paper claims that watermarking, Digital Rights Management (DRM) and P2P can be quite complementary. Specifically, a P2P network infrastructure is presented which allows broad digital content exchange while on the same time supports data protection and copyright protection through watermarking technologies. In brief, the platform is functioning mainly for digital images and is tracking all the watermarked image files which are distributed and copied through the P2P network. The challenge is the algorithmic complexity of detecting multiple watermarking keys in the P2P network effectively and quickly, especially when thousands of image files are concerned. This is managed by an optimization detection algorithm which allows effective watermarking key detection in optimal P2P hops.

Equivalent systems, which combine watermarking, DRM and P2P technologies do not yet exist in practice but only in theory. Certain methodologies and strategies have been proposed for exploiting P2P technologies in DRM and vice versa [9]. The proposed system is setting a new basis for the close cooperation of the two different scientific areas of DRM and P2P aiming at exploiting the distributed computing nature of P2P networks for efficient digital rights protection and management.

2 IPR Protection – Watermarking and Keys

In this section the copyright protection part of the P2P infrastructure is presented which is mainly based on a watermarking algorithm for digital images which produces the correspondent watermarking keys distributed within the P2P environment.

2.1 Copyright Protection through Watermarking

The copyright protection systems main objectives are to provide an appropriate information infrastructure which supports rights management for the digital content and for the transactions taking place and on the same time protects the digital images and their copyright though robust watermarking techniques.

The watermarking techniques are playing a very important role in such systems mainly because they provide the protection means for proving the identification of the copyright owner and detecting unauthorized use of digital content [4]. Towards this functionality, watermarking algorithms are casting keys to the digital content (in most of cases invisible keys) which when detected prove the copyright ownership of the digital content [5].

In case of digital content transactions a very large number of digital images are being exchanged through networks and the Internet for which the legality of their future use is highly improbable. The situation is even more difficult in P2P network infrastructures through which digital content is being exchanged based on specialized stand alone applications which exchange digital files of all kinds (and not only images).

A proposed solution is to apply a watermarking algorithm which produces sufficient information which is distributed to the P2P nodes. This information consists mainly of the watermarking key and other data relating to the digital image itself.

2.2 Generating Keys with the Watermarking Algorithm

Generally, a watermark is a narrow band signal, which is embedded to the wide band signal of a digital image [1]. In our case spread Spectrum techniques are being used and are methods by which energy generated at one or more discrete frequencies is deliberately spread or distributed in time or frequency domains.

In particular, this technique employs pseudorandom number sequences (noise signals) to determine and control the spreading pattern of the signal across the allotted bandwidth. The noise signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence: this process, known as ”de-spreading”, mathematically constitutes a correlation of the transmitted pseudorandom number sequence with the receivers assumed sequence [10]. Thus, if the signal is distorted by some process that damages only a fraction of the frequencies, such as a band-pass filter or addition of band limited noise, the encrypted information will still be identifiable [11]. Furthermore, high frequencies are appropriate for rendering the watermarked message invisible but are inefficient in terms of robustness, whereas low frequencies are appropriate with regards to robustness but are useless because of the unacceptable visual impact.

In our case, the embedding of a robust multibit watermark is accomplished through casting several zero-bit watermarks onto specified coefficients. The image watermark, a random sequence of Gaussian distribution in our case, is casted multiple times onto the selected coefficients preserving the same sequence length but shifting the start point of casting by one place.

Actually the final watermark that is embedded into the image is not a single sequence but many different sequences generated with different seeds. These sequences are casted, one after the other, on the mid coefficients of the image, using the additive rule mentioned above and begging from successive starting points. If all sequences where to be casted, beginning from the same starting point, then, besides the severe robustness reduction resulting from the weak correlation, the possibility of false positive detector response would dramatically increase, since every number that has participated as a seed during the sequence generation procedure, will be estimated by the detector as a valid watermark key. Shifting the starting point by one degree for every sequence casting ensures that the false positive rate will remain in very small level due to the artificial desynchronisation introduced. Every single random sequence of Gaussian distribution is generated using a different number as the seed for the Gaussian sequence generator. It is

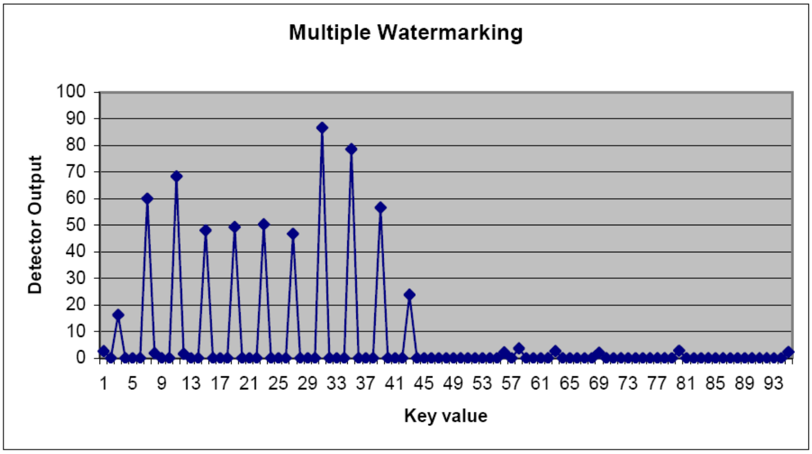


Fig. 1. Multiple Watermarking Keys per Image

important to differentiate the sequences in order not to mislead the detection mechanism, since it is based on the correlation between the extracted sequence and the sequence produced with the watermark key.

The watermark key is responsible both for the generation of the first sequence and the construction of a vector, containing the rest of the numbers that will serve as the corresponding seeds. The placement of several Gaussian sequences into the image content can model, under specific conventions, a multi-bit watermark. The detection of a zero-bit watermark is interpreted as if the bit value of the specified bit is set to one. On the contrary, failure of the detector to detect the zero-bit watermark leads to the conclusion of a zero bit value. Thus, in order for a message to be casted into the image content, it is initially encoded using the binary system and applied afterwards in the sense of zero-bit watermarks using the embedding mechanism and according to the derived bit sequence.

2.3 Watermarking Keys and the P2P Network

In this section a watermarking algorithm has been presented which is robust enough to facilitate data and copyright protection for the digital images while at the same time produces sufficient information which is distributed and stored to the P2P nodes. This information consists mainly of the watermarking key.

Taking into consideration that for each digital image a set of watermarking keys are being used for copyright protection, the next step towards an efficient P2P environment which supports digital rights management is to use these keys as an information for retrieving the copyright status of each image transacted through the P2P network. For this reason, the watermarking keys are being stored in the independent network Peers. The copyright owner can use the watermarking key as query information to track down its digital images and their use. The issue is how quickly and efficiently the Peer that contains the under inspection key is being located taking into account that thousands of digital images could exist in the P2P network and multiple watermarking keys could exist in a digital image. The solution proposed is a scalable and robust data indexing structure based on a Nested Balanced Distributed Tree (NBDT). The next section presents the NBDT P2P Network.

3 NBDT P2P Network

NBDT provides a tree-like structure for the P2P network upon which watermarking key-based searching can be performed. In terms of bandwidth usage, searching scales very well since no broadcasting or other bandwidth consuming activities take place during searches. Since all searches are key based there are two possibilities: either (a) each host implements the same algorithm, that translates a keyword to a binary key or (b) another service provides the binary key. This service accepts keyword based queries and can respond with the corresponding key. The second approach is more precise. It is also possible to use a more centralized implementation for such a service. From now on we assume that the key is available. This section describes an algorithm for the first case.

The structure was built by repeating the same tree-structure in each group of nodes having the same ancestor, and doing this recursively [6]. This structure may be imposed through another set of pointers. The innermost level of nesting will be characterized by having a tree-structure, in which no more than two nodes share the same direct ancestor. The figure 2 illustrates a simple example (for the sake of clarity we have omitted from the picture the links between nodes with the same ancestor). Thus, multiple independent tree structures are imposed on the collection of nodes inserted. Each element inserted contains pointers to its representatives in each of the trees it belongs to.

Let an initial given sequence of w-bit keys belonging in universe K=[0,2w-1], where an unknown density. At initialization step we choose as peer representatives the 1st key, the lnKst key, the 2lnKst key and so on, meaning that each node with label i (1<i<N) stores ordered keys that belong in range [(i-1)lnK,..ilnK-1], where N=K/lnK the number of peers. Note that during update operations; it is not at all obvious how to bound the load of the N peers, since new w-bit keys with w¿w may be appeared in the system and K must exceed. For this purpose we will model the insertions/deletions as the combinatorial game of bins and balls presented in [10]: Modeling the insertions/deletions of keys in this way, the load of each peer becomes Q(polygonN) in expected case with high probability. Obviously, peers representatives early described have also been chosen according to this game. We also assume that each key is distinct and as a result the probability of collisions is zero. Each key is stored atmost in O(loglogN) levels. We also equip each peer with the table LSI (Left Spine Index). This table stores pointers to the peers of the left-most spine (for example in figure 2 the peers 1, 2, 4 and 8 are pointed by the LSI table of peer 5) and as a consequence its maximum length is O(loglogN). Furthermore, each peer of the left-most spine is equipped with the table CI (Collection Index). CI stores pointers to the collections of peers presented at the same

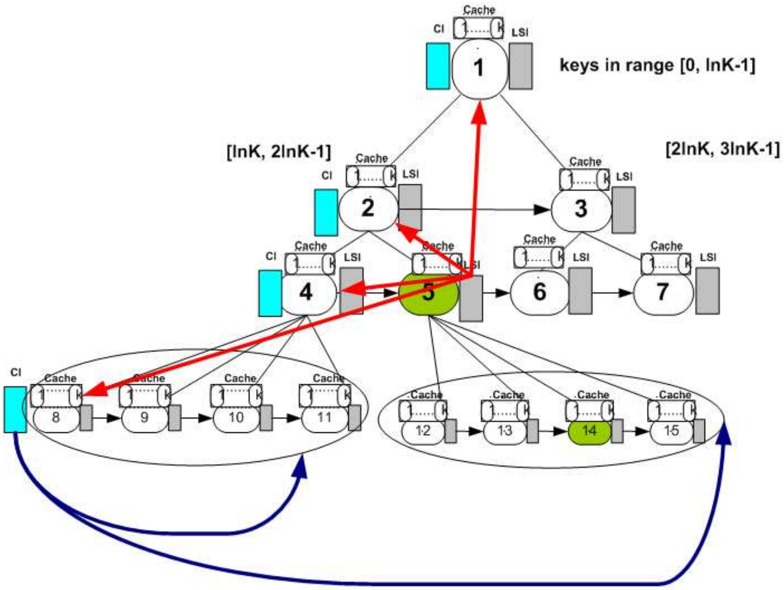


Fig. 2. The NBDT P2P System

level (see in figure 2 the CI table of peer 8). Peers having same father belong to the same collection. For example in the figure 2, peers 8, 9, 10, and 11 constitute a collection of peers. Its obvious that the maximum length of CI table is OpN. For example in figure 2 we are located at (green) node 5 and we are looking for a key k in [13lnn, 14lnn-1]. In other words we are looking for (green) node 14. As shown in [12], the whole searching process requires an optimal number of O(loglogN) hops or lookup messages for detecting the watermarking key and that is also validated using the proposed simulator.

When we want to insert/delete a key/node from the structure, we initially search for the node that is responsible for it (using a number of O(loglogN) hops in worst-case) and then we simply insert/delete it from the appropriate node.

If new w-bit watermarking keys, with w¿w, request to be inserted into the system, then we have to insert new peers on the network infrastructure and as a result we have to re-organize the whole p2p structure. In practice, such an expensive reorganization is very sparse. The new peers of NBDT are inserted at the end of the whole infrastructure consuming O(1) hops in worst-case. In particular, when a node receives a joining node request it has to forward the join request to the last node. The last node of NBDT infrastructure can be found in O(1) hops in worst-case by using the appropriate LSI and CI indexes.

If the load of some peer becomes zero, we mark as deleted the aforementioned peer. If the number of marked peers is not constant any more then we have to re-organize the whole p2p structure. Based on the basic theorem of [7], if we generate the keys according to smooth distributions, which is a superset of regular, normal, uniform as well as of real world skew distributions like zipfian, binomial or power law (for details see [8]), we can assure with high probability that the load of each peer never exceeds polylogn size and never becomes zero. The latter means that with high probability split or delete operations will never occur. In other words, the re-organization of the whole P2P structure with high probability will never occur which means that only the O(loglogN) hops are necessary to detect the appropriate watermarking key and no further time is being consumed for structure re-organization.

4 Conclusions

In this paper we focused on a P2P network infrastructure which allows broad digital content exchange while on the same time supports data protection and copyright protection through watermarking technologies.

In brief, a watermarking algorithm casts watermarking keys to the digital images and the same time the watermarking keys are being stored in the independent network Peers. The watermarking algorithm is robust enough to facilitate data and copyright protection for the digital images while at the same time produces sufficient information which is distributed and stored to the P2P nodes (the watermarking key).

The P2P environment which supports digital rights management is achieved through the use of these keys as an information for retrieving the copyright status of each image transacted through the P2P network. The copyright owner can use the watermarking key as query information to track down its digital images and their use. The tracking down solution used is a scalable and robust data indexing structure based on a Nested Balanced Distributed Tree (NBDT). Based in the NBDT system, in the steady state, in a N-node network, each node resolves all lookups via O(loglogN) messages to other nodes. Key updates require only O(loglogN) number of messages in worst-case. Node updates require O(1) number of messages in expected-case with high probability.

The watermarking key detection process withih the P2P framework is very efficient and outperforms the most popular infrastructures used directly for many solutions for P2P information discovery. The key detection process is very important for the copyright owner because when successful the copyright status of each digital image can be retrieved and evaluated.

The future applicability of the proposed infrastructure is strong as it could be used for the creation of P2P environments, supported by GUIs, with which a user could exchange digital files while copyright protection occurs at the same time.

References

1. Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. Morgan Kaufmann Publishers, San Francisco (2002)
2. Computer Science and Telecommunications Board, National Research Council. The Digital Dilemma: Intellectual Property in the Information Age, pp. 2–3. National Academy Press, Washington (1999)

3. House of Representatives. Digital Millennium Copyright Act (October 1998)
4. Davis, R.: The Digital Dilemma. Communications of the ACM 44, 80 (2001)
5. Wayner, P.: Disappearing Cryptography - Information Hiding: Steganography and Watermarking, 2nd edn., pp. 291–318. Morgan Kaufmann, San Francisco (2002)
6. Sioutas, S.: NBDT:An efficient P2P indexing scheme for Web Service Discovery. International Journal of Web Engineering and Technologies 4(1), 95–113
7. Kaporis, A., et al.: Improved Bounds for Finger Search on a RAM. In: Di Battista, G., Zwick, U. (eds.) ESA 2003. LNCS, vol. 2832, pp. 325–336. Springer, Heidelberg (2003)
8. Kaporis, A., et al.: Dynamic Interpolation Search Revisited. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4051, pp. 382–394. Springer, Heidelberg (2006)
9. Einhorn, M., Rosenblatt, B.: Peer to Peer Networking and Digital Rights Management - How Market Tools Can Solve Copyright Problems. Policy Analysis Journal 534 (2005)
10. Fotopoulos, V., Skodras, A.N.: A Subband DCT Approach to Image Watermarking. In: Proc. X European Signal Processing Conference (EUSIPCO 2000), Tampere, Finland, September 5-8 (2000)
11. Fotopoulos, V., Skodras, A.N.: Image Watermarking for Quality Control Based on Modified Key-Dependent DCT Basis Functions. In: 15th Int. Conf. on Digital Signal Processing (DSP 2007), Cardiff, Wales, UK, July 1-4 (2007)

Session 6

Security, Attacks and Crime

Information Assurance and Forensic Readiness

Georgios Pangalos[1] and Vasilios Katos[2]

[1] Aristotle University of Thessaloniki, Greece
pangalos@auth.gr
[2] Democritus University of Thrace, Greece
vkatos@ee.duth.gr

Abstract. Egalitarianism and justice are amongst the core attributes of a democratic regime and should be also secured in an e-democratic setting. As such, the rise of computer related offenses pose a threat to the fundamental aspects of e-democracy and e-governance. Digital forensics are a key component for protecting and enabling the underlying (e-)democratic values and therefore forensic readiness should be considered in an e-democratic setting. This position paper commences from the observation that the density of compliance and potential litigation activities is monotonically increasing in modern organizations, as rules, legislative regulations and policies are being constantly added to the corporate environment. Forensic practices seem to be departing from the niche of law enforcement and are becoming a business function and infrastructural component, posing new challenges to the security professionals. Having no a priori knowledge on whether a security related event or corporate policy violation will lead to litigation, we advocate that computer forensics need to be applied to all investigatory, monitoring and auditing activities. This would result into an inflation of the responsibilities of the Information Security Officer. After exploring some commonalities and differences between IS audit and computer forensics, we present a list of strategic challenges the organization and, in effect, the IS security and audit practitioner will face.

Keywords: Computer forensics, e-discovery, IS audit, compliance.

1 Introduction

Information Systems auditing (IS auditing) is a cornerstone function of Information Assurance. IS auditing is performed on all facets of the corporate IS, to ensure that the security controls placed within the system support IT governance which will allow the company to align its IT strategy with its enterprise objectives. The enterprise objectives in turn are reflected in the security policies which are the main means for communicating the *acceptable* behavior of all parties involved.

Recently the extroversion of the companies has been amplified with the facilitation of the Information and Communication Technologies. The speed of collecting, processing and disseminating information warranted a closer coupling between a company and its third parties and customers. However this setting posed additional challenges with respect to the protection of the data which in many cases involves third party personal information and as such regulatory compliance was mandated.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 181–188, 2010.

In addition, the overwhelming presence of ICT and the fact that the corporate IS has become the main instrument for conducting business, computer crime has enjoyed a proliferation in the recent years [1, 2]. As a result computer forensics not only have become the fastest growing market in information security [3], but also have become a centerpiece of the ICT infrastructure.

Currently the overlap between digital forensics and information security is acknowledged [4] and this is represented in Fig. 1a. It is advocated in this paper that the scope of forensics needs to be expanded in order to encompass the whole IS security domain as shown in Fig. 1b. This all-inclusive paradigm is primarily due to the expanding use of ICT and the substantial increase of user acceptance which is in line with the directions toward e-Governance in an Information Society. As such, it is anticipated that the term *user* will become synonymous to the term *citizen*. Consequently, strict corporate security policies will be challenged and could potentially conflict with the wider societal trends. A typical example is the policies prohibiting the use of corporate communication resources such as email for personal use, which could be viewed as an attempt to socially exclude the user who is already accustomed to using the email for accessing State services. This would create an environment where practices to detect security policy violations would need to be investigated in a legally acceptable way, regardless whether there is a civil or criminal offense committed or suspected. Naturally, this could lead to the need to incorporate digital forensics and incident response practices in the IS auditor's activities. Absence of formal forensic investigation processes could jeopardize the privacy and rights of the user as well as elevate the risk of the company facing lawsuits.

This paper is structured as follows. In Section 2 the audit process is outlined for the benefit of the reader who is unfamiliar with the area. Section 3 highlights the main aspects of digital forensics and forensic readiness. The material presented in Sections 2 and 3 is leveraged in Section 4 in order to highlight the challenges of the contemporary IS operating in a highly networked company placed in the information society. Finally the conclusions are presented in Section 5.

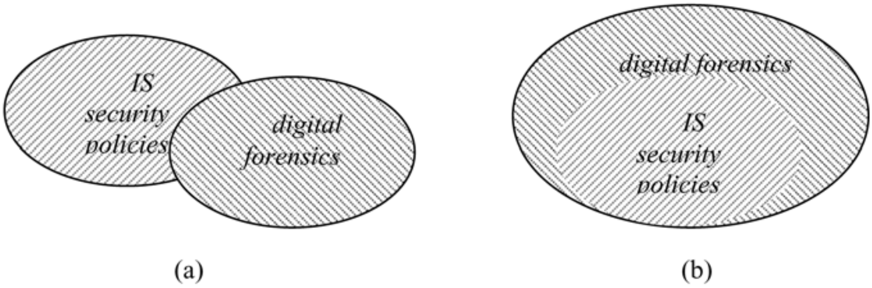


Fig. 1. The overlapping scopes between IS security and forensics

2 The Audit Process

IS audit is performed in order to assess the correctness of installation of the security controls aiming to reduce the risks to acceptable levels. Such exercise would imply that a security assessment has been performed and the business owner and stakeholders together with the security consultant or security architect have agreed upon a number of security controls, but most important the business owner has agreed on accepting the residual risk. The Information Systems Audit and Control Association (ISACA) specifies the following five distinct tasks within the IS audit area [5]:

1. Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.
2. Plan specific audits to ensure that IT and business systems are protected and controlled.
3. Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
4. Communicate emerging issues, potential risks and audit results to key stakeholders.
5. Advise on the implementation of risk management and control practices within the organization while maintaining independence.

The above tasks can be viewed as primitives for building an audit framework. An audit framework can be build upon a plethora of published standards, guidelines and procedures. Table 1 summarizes a small portion of known standards guidelines and procedures which are available to the IS auditor.

Table 1. Representative standards, guidelines and procedures

Short name	Title	Type
ISO 27002 (ISO/IEC 17799)	Code of practice for information security management	Standard
ISO 27005	Information security risk management	Standard
BS25999	Standard for Business Continuity Management	Standard
ISACA-S9	Irregularities and Illegal Acts	Standard
ISACA-S10	IT Governance	Standard
ISACA-G28	Computer Forensics	Guidelines
ISACA-G31	Privacy	Guidelines
ISACA-P3	Intrusion Detection	Procedures
ISACA-P8	Security Assessment – Penetration Testing and Vulnerability Analysis	Procedures

Of particular importance in this paper is the guideline G28, which relates to computer forensics. This guideline is further studied later on in Section 4.

Perhaps the most representative source of information is the material pertaining to the Certified Information Systems Auditor qualification. The CISA material consists of the following six domains [5]:

- The IS audit process, which encompasses the entire IS auditing process.
- IT Governance, which sets the context in which the controls are placed.
- Systems and Infrastructure Life Cycle Management, which relates to the key processes and methodologies adopted by organisations when creating and maintaining IS.

– IT service delivery and support, which is about service level expectations as derived from the organisation's business objectives.
– Protection of information assets, where the controls implemented are evaluated against the three security criteria of confidentiality, integrity and availability.
– Business continuity and disaster recovery, focusing on the controls that are responsible for ensuring the availability of the critical IS processes.

Other paradigms such as ISO and BS have a slightly different mix and definition of domains, but they all consent to the protection of the IS assets against confidentiality, integrity and availability threats.

3 Forensic Readiness and the Digital Forensics Process

Digital forensics is the examination of computer systems and digital storage media by the use of investigative and scientific techniques for the preservation, identification, acquisition, analysis, interpretation and documentation of the (digitally stored or encoded) information for evidentiary and/or root cause analysis and presentation of digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal [4,6,7,8,9]. Forensic readiness is the state of the organisation where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorised actions shown to be disruptive to planned operations.

From the above definitions it should be evident that effective forensics cannot exist without security controls. Preservation for example is demonstrated with the use of cryptographic hashes [10], in the case of dead forensics [11]. The concept of preservation is also found in disaster recovery and business continuity practices. Analysis and interpretation of the findings highly depends on the ability to distinguish the malicious from benign activities, which is an area well studied in the domain of intrusion detection, whereas accountability and identification of a user/suspect suggests that acceptable user authentication is in place.

In modern organizations the vast majority of documents are in a digital form. The term Electronically Stored Information, ESI refers primarily to storage and retention of electronically generated documents. As such, the digital forensics process when invoked must deal with the acquisition of documents from a variety of sources and states and the forensic analyst is burdened with the task to identify and correlate the digital evidence. The term which encompasses the above forensic tasks is referred to as e-discovery. Consequently, the effectiveness as well as cost of e-discovery would depend on the capability and maturity of the attained forensic readiness. In addition when there is a litigation involved, there may be compliance and other legislative issues. This is already reflected in the US with the enactment of the new amendments to the US court system's Federal Rules of Civil Procedure, FRCP [12], which emphasizes on the timeliness of serving electronic documents in court. A representative example is the case of General Motors being fined $700,000 by the Alabama Circuit Court of Appeals for delaying a discovery process by 98 days [13].

The attribute which differentiates forensic investigations from other type of investigations such as network monitoring, is due diligence and the ability to demonstrate this.

The investigator needs to take care in order not to harm or offend the interests of all parties involved as well as their properties, and the forensics procedures are built around these considerations. As an example, due diligence is shown in the case of a suspect hard disk acquisition, if reasonable effort is invested to preserve the state of a hard disk, and the cryptographic hashes are calculated against the whole disk at the earliest possible stage of the e-discovery process. As we will present below, due diligence is not necessarily one of the objectives in information security led investigations.

4 Analysis and Discussion

ISACA's G28 guideline on computer forensics [14] aims to introduce the forensics process to the IS auditor practitioner and also provides a list of audit considerations. The very fact that the reference to forensics is in a form of a guideline, shows a weak coupling between the IS audit practice and the domain of computer forensics. Provided that the need for compliance is gaining ground, digital forensics will become a core and established practice in the corporate. Thus, integration between the two disciplines must be targeted on an epistemological level.

Against the above, a number of issues are becoming apparent which are detailed below.

4.1 The Security Auditor Needs to Revisit the Risk Analysis Paradigm

Typically on a risk assessment exercise the auditor and the stakeholders agree on the company's risk exposure. More analytically, the auditor assesses the risk and if this is found to be acceptably high, then security controls are introduced in order to lower the risk to an acceptable level. The acceptable risk is the so called residual risk and the auditor is not normally concerned with this quantity. We subscribe to the view that the presence of the residual risk is the very reason for the need and existence of forensics. By accepting the residual risk, we also accept that the security controls will at some point fail. Security breaches, no matter how low risk may be, must be treated as potentially criminal activities due to the lack of the *a priory* knowledge of the nature of the security event. The tunnel vision of risk analysis which focuses primarily on financial losses does not provide information on the long term impact of an event which may exhibit low losses during its genesis.

Risk assessment seems to be the common denominator between IS auditing and forensics, as it is emphasized in [7] that the need for forensic readiness can be established via a risk assessment. However, if the scope of forensics is to be expanded to include all aspects of information security, the auditors need to adapt there practices to the forensics paradigm.

4.2 Redress

The limited dimensions of risk assessment can also be understood if one examines the goals of the security controls. More analytically, information security controls serve three goals, namely prevention, detection and recovery. Detection in security does not necessarily include the goal of identifying the perpetrator, or as colorfully mentioned in forensics to "put fingers on keyboards". In [15] the synonyms of resistance, recognition, recovery are used to describe the components of what the authors equivalently call a survivable system (that is an IS with security controls). In the same paper the authors recognize the need for a fourth goal, redress [15]:

> *Redress is the ability to hold intruders accountable in a court of law and the ability to retaliate.*

It can be seen that accountability is a subset of redress. Again, due to the need for compliance and risks of litigation, the traditional accountability solutions may not be sufficient in the modern organization, but should be enriched with computer forensics techniques and processes for legal remedies and active defense. It should be highlighted that the traditional accountability processes should not become obsolete, but be enriched instead with the above aspects.

4.3 Business Continuity and Forensic Readiness

The domain of business continuity and disaster recovery can be a valuable source of information to support forensic readiness and incident response respectively. Business continuity includes processes for data backup and recovery. These processes can form the specification documents for developing forensic readiness processes. Disaster recovery may in turn benefit from incident response practices which can run in parallel in the event of a security breach.

4.4 Well Established Roles in Forensics

Roles such as Chief Information Security Officer, Security Architect and Security Administrator are well established in many organizations. The expanding scope of security and forensics though necessitates a dedicated role relating to forensics. A Security Architect for example is not responsible and does not maintain the key skills for conducting forensics and setting forensic readiness requirements. Depending on the organization, its size and the industry it is in, a Forensic Consultant type of role will most likely be required. At the time of writing there is no established body of knowledge in digital forensics and there is a plethora of professional certifications. It is expected that the computer forensics discipline will undergo a lifecycle similar to that of information security.

4.5 Forensics on the Security Policies

The security policies can be found to be exposed and the need for applying computer forensics practices. For example, firewall and intrusion detection policies do not usually include forensic considerations within their incident response processes. Since one would not know *a priori* if a suspected action (e.g. obtained by detecting abnormal network activity) will result to a criminal offense being committed, monitoring should incorporate live forensics practices in order to secure the potential evidence from spoliation. On the other hand, forensic acquisition of evidence normally includes safeguards to protect the privacy of the users on the corporate network.

Consequently, the security policies would also need to be assessed for their forensic readiness status. A deliverable for this exercise could be a metric for forensic readiness.

5 Conclusions

The challenges faced by the corporations and the auditors with respect to compliance and forensic readiness need to be addressed in a systematic way. Although a corporate policy violation will not necessarily lead to court (in fact about a third of the violations do lead up in court [16]), the actual severity and legal implications of a security event cannot be established beforehand. Consequently, forensic practices seem to be departing from the niche of law enforcement and are becoming a business function and infrastructural component. This migration will pose challenges to the security professionals and may require the establishment of the role of a computer forensics analyst.

It is argued that the two main components of information assurance is security auditing and forensics. The former is a mature discipline in IS and can provide some of the primitives to both incorporate and facilitate the computer forensics processes within the organization. The need for synergy between forensics and IS auditing can be justified with the compliance restrictions which are regularly introduced in the corporate environment. This synergy in turn would trigger further integration practices between the two disciplines and in this paper we exposed some of the reasons that the integration may lead to research intensive directions, as well as the challenges an audit practitioner will face.

The issues raised in the discussion section essentially require a methodology for integrating the disciplines. This is an ongoing area of research.

References

1. Antiphishing Working Group. Phishing Activity Trends Report Q2, 2008 (2008), `http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf`
2. Parliamentary Office of Science and Technology. Computer Crime. POSTNOTE, 271 (2006)
3. Harris, S.: To Catch A Thief: Bringing Forensics In-House And The Necessary Tools To Succeed. Amazines (2008)
4. Grobler, T., Louwrens, B.: Digital Forensic Readiness as a Component of Information Security Best Practice. In: Venter, H., Eloff, M., Labuschanc, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 13–24. Springer, Boston (2007)
5. Information Systems Audit and Control Association: CISA Review Manual 2008 (2007)
6. Kruse II, W., Heiser, J.: Computer Forensics: Incident Response Essentials. Addison Wesley, Reading (2004)
7. Rowlingson, R.: A Ten Step Process for Forensic Readiness. Int. Journal of Digital Evidence 2(3) (2004)
8. Sinangin, D.: Computer Forensics Investigations in a Corporate Environment. Computer Fraud & Security 8, 11–14 (2002)

9. EDRM, The E-Discovery Reference Model, http://edrm.net
10. Chen, L., Wang, G.: An Efficient Piecewise Hashing Method for Computer Forensics. In: 2008 Workshop on Knowledge Discovery and Data Mining, pp. 635–638 (2008)
11. Kotze, D., Olivier, M.: Patlet for Digital Forensics First Responders. In: 18th International Workshop on Database and Expert Systems Applications, pp. 770–774 (2007)
12. US Court, Amendments to the Federal Rules of Civil Procedure (2006), http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf
13. Marcella, A.: Electronically Stored Information and Cyberforensics. Information Systems Control Journal 5, 44–48 (2008)
14. Information Systems Audit and Control Association, Guidline G28: Computer Forensics (2000)
15. Endicott-Popovsky, B., Frinke, D.: Adding the 4th R: A Systems Approach to Solving the Hackers Arms Race. In: Proc. of the 2006 Symposium 39th Hawaii International Conference on System Sciences (2006)
16. Computer Security Institute CSI Survey 2007 (2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

An Ontology-Driven antiSPIT Architecture

Stelios Dritsas and Dimitris Gritzalis

Information Security and Critical Infrastructure Protection Research Group
Dept. of Informatics, Athens University of Economics & Business (AUEB)
76 Patission Ave., Athens, GR-10434 Greece
{sdritsas,dgrit}@aueb.gr

Abstract. Over the last years Voice-over-IP (VoIP) is getting widespread adoption from business and residential customers.The preference towards VoIP services stems from the fact that VoIP provides many ways to communicate, with a lower cost than traditional telephony. However, VoIP in its present form may allow malicious users to exploit a number of vulnerabilities, make bulk unsolicited telephony calls and send bulk unsolicited instant messages. This exploitation is referred to as Spam over Internet Telephony (SPIT). In this paper we introduce an antiSPIT management architecture, by using ontologies, which allow domain administrators to detect and handle SPIT automatically, based on predefined requirements and preferences.

Keywords: Security, Availability, VoIP, SPIT, Ontology.

1 Introduction

The explosive growth of the Internet has introduced a wide array of new technological advances and more sophisticated end-user services. One of them is Voice-over-IP (VoIP), which offers telephony and other multimedia services over existing data networks. Some of the basic reasons that make Voice-over-IP (VoIP) increasingly appealing are: (a) VoIP's seamless integration with the existing IP networks and the Internet, (b) lower costs compared to PSTN telephony, (c) use of computer-based soft-phones, (d) existence and implementation of sophisticated end-user services in terms of portability, accessibility and convergence of telephone networks.

Currently, the majority of VoIP implementations are based on the Session Initiation Protocol (SIP), which tends to be the dominant protocol in VoIP environments [7]. Despite its benefits, SIP has a number of vulnerabilities which can negatively impact the use of VoIP services [1]. One introduced threat is the capability of malicious users to make bulk unsolicited telephony calls and/or send bulk unsolicited instant messages. This situation is a new form of spam, which - in the case of VoIP environments - is called Spam over Internet Telephony (SPIT) [2,3]. Although several anti-SPIT approaches have been proposed, their effectiveness has been characterized as inadequate due to their ad-hoc nature, their strong dependence to the used context, and to their inability to fully take into account the real-time nature of VoIP services [4,5]. This situation necessitates the development and deployment of specific anti-SPIT mechanisms and techniques in an effort to thwart SPIT phenomenon and enhance VoIP further pervasiveness.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 189–198, 2010.

The effective management of SPIT phenomenon depends on many factors and on the specific characteristics that are introduced in a VoIP environment. Hence, in this paper we propose a SPIT management architecture that takes into consideration all the requirements posed so as to manage SPIT. The proposed architecture is based on: (a) the anti-SPIT policies that might be adopted in any SIP-based environment and (b) our ontology model (ontoSPIT), which operates as a policy enforcement tool.

The paper is organized as follows: First, we present some generic issues regarding SPIT phenomenon and the SPIT management procedure. In the sequel, we present our proposed SPIT management architecture in conjunction with its basic building blocks. Furthermore, in section 4 we demonstrate how our approach could be integrated in a SIP-based VoIP environment as well an example of an anti-SPIT policy rule and how this could be included in our ontoSPIT model. In section, 5 we evaluate our proposal in terms of (a) how they respond to some SPIT attacks. Finally, we conclude by providing the reader with some noteworthy remarks.

2 Spam over Internet Telephony (SPIT)

VoIP is an advancing technology that provides several benefits to its users. These benefits have been acknowledged, and VoIP users are continuously increasing over time. However as with any technological advancement, the rapid adoption of VoIP technologies will introduce new types of threats and will attract malicious users. Such a threat is SPIT, which is defined as the sending of a set of bulk unsolicited voice calls or instant messages [1].

Currently, three different types of VoIP spam forms have been recognized [2]: (a) Call SPIT, which is defined as bulk, unsolicited session initiation attempts in order to establish a multimedia session, (b) Instant Message SPIT, which is defined as bulk, unsolicited instant messages and it is well known as SPIM, and (c) Presence SPIT, which is defined as bulk, unsolicited presence requests so as the malicious user to become a member of the address book of a user or potentially of multiples users.

SPIT starts getting recognized as a possible serious problem in VoIP networks. The research community foresees that it will be very attractive for spammers and telemarketers (spitters) in the near future; a situation that may cause major annoyance to end-users. This interest of researchers for SPIT can be observed by the proposal of many anti-SPIT mechanisms and techniques. These mechanisms rely on well researched solutions and approaches for the email spam. However such approaches might not be satisfactory for VoIP, and some issues with these mechanisms have already been identified [4,5]. Hence, one can conclude that the SPIT management process (i.e. detection and handling of SPIT calls/messages) is not a simple one. It requires actions that take into account not only the specific characteristics of the VoIP technology but, also, the requirements posed by the administrators of each SIP-based VoIP domain. In Fig. 1 we provide a macroscopic view of the SPIT management. It is obvious that the prevention, detection and reaction of SPIT incidents, should be considered very carefully in an effort to manage SPIT phenomenon efficiently and effectively.

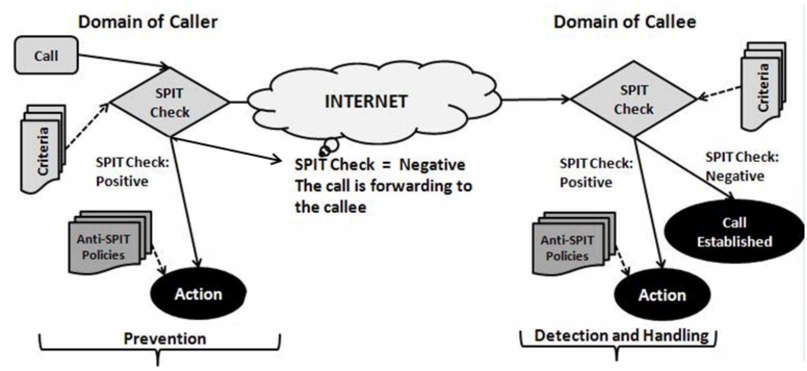


Fig. 1. SPIT management

3 A Proposed Anti-SPIT Architecture

In this section we present a SPIT management architecture. The architecture is based on two major components: a) anti-SPIT policies and b) the ontoSPIT model. We will first describe these two components, and then we will show how these components blend together in our architecture in order to manage SPIT.

3.1 Anti-SPIT Policies

Security policies can play a significant role in the enforcement of the basic security properties, namely: confidentiality, availability and integrity [8]. In this context, and with an eye towards to SPIT phenomenon handling, we define an anti-SPIT policy as the set of rules that should be adopted in an effort to detect and counter possible SPIT attacks and incidents.

In general, an anti-SPIT policy should include a set of rules that describe the actions to be taken for handling SPIT (i.e. actions that should be considered whenever a SPIT call/message is detected). The rules are consisted of two major components:

a) The underlying *conditions*, in charge of detecting possible SPIT voice calls and/or instant messages. The conditions are based on specific SPIT detection criteria that have been identified in [9], as well as on SPIT attack scenarios [10].
b) The appropriate *actions*, which represent the actions that should be adopted so as to handle an identified SPIT call and/or message. The actions that we have defined in the context of our proposed architecture are the following:

- *Allow:* In this case, the SIP message is forwarded to the next proxy or to the end-user.
- *Block:* This case denotes the rejection of a SIP message. The action is enforced when we are sure that specific conditions are satisfied, therefore the message has been recognized as SPIT.
- *Check Further*: This action is referred to the activation of further checks (e.g. CAPTCHA tests) so as to make more absolute conclusions regarding the nature of a SIP message (if it is SPIT or not).

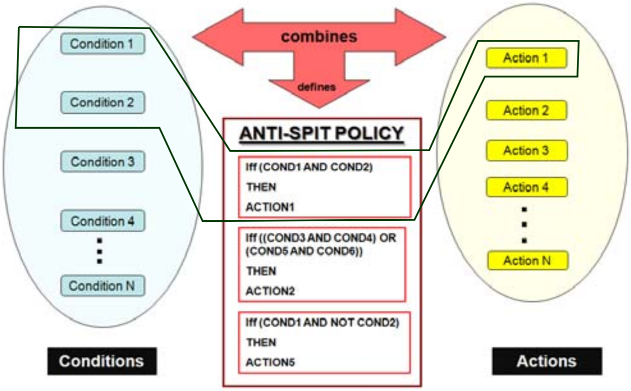


Fig. 2. Anti-SPIT policies representation

Fig. 2 depicts how each policy is represented by its underlying rules (i.e. the combination of conditions and actions).

3.2 The OntoSPIT Model

An ontology is an explicit specification of a conceptualization, which can be used to describe structurally heterogeneous information sources, helping both people and machines to communicate in a concise manner by supporting knowledge sharing and reuse [11,12]. The reusability approach is based on the following assumption: if a modeling scheme is explicitly specified and mutually agreed by the parties involved, then it is possible to share, reuse, and extend knowledge.

In this paper we adopt a SPIT management ontology model (ontoSPIT) that provides a SPIT-oriented knowledge base and enhances the sharing of its information and components [13]. By using ontologies, we can use their advantages in an effort to help stakeholders of SPIT domain (i.e. administrators and end-users) make decisions regarding the efficient SPIT management. These decisions should be based on pre-defined assumptions or on tacit knowledge entailed by the amount of SPIT related information generated by different sources, such as anti-SPIT systems, VoIP domains, SPIT related SIP vulnerabilities, SPIT attack patterns and scenarios, etc.

3.3 SPIT Management Architecture

Our proposed SPIT management architecture tries to handle SPIT by incorporating a series of SPIT-related information including the SPIT related vulnerabilities of the SIP protocol [14], SPIT-related attack patterns and scenarios [10], and specific SPIT incident detection criteria [9]. This is essential information that provides a satisfactory starting point for countering SPIT phenomenon at its early stages. The following picture depicts our proposed architecture, while in the next paragraphs we describe the steps needed to adopt our architecture in a VoIP domain.

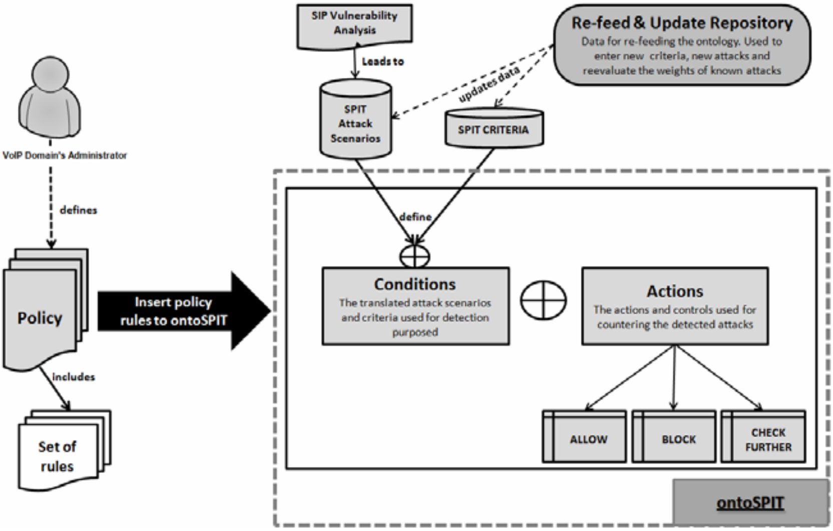

SIP Vulnerability Analysis
Leads to
SPIT Attack Scenarios
updates data
SPIT CRITERIA
Re-feed & Update Repository
Data for re-feeding the ontology. Used to enter new criteria, new attacks and reevaluate the weights of known attacks
VoIP Domain's Administrator
defines
Policy
Insert policy rules to ontoSPIT
includes
Set of rules
define
Conditions
The translated attack scenarios and criteria used for detection purposed
Actions
The actions and controls used for countering the detected attacks
ALLOW
BLOCK
CHECK FURTHER
ontoSPIT

Fig. 3. The proposed anti-SPIT architecture

Step 1: *Anti-SPIT Policy Definition:* The first step is to define the anti-SPIT policies that will be adopted in the SIP-based VoIP domain. The administrator of the domain defines the rules of the policy, i.e. the conditions under which a SIP message is checked and the desired actions that will be taken if a SPIT suspicious message has been identified.

Step 2: *Anti-SPIT Policy Adoption:* After the definition of the policy, it is important to translate it into a format that is compatible with the ontoSPIT model; that is the administrator of the VoIP domain needs to express the policy rules into the desired conditions and actions that will be included into the ontology in a language that will be recognizable from the ontoSPIT model. One such language is the OWL language [15,16,17], which was also used in the original OntoSPIT model [13].

Step 3: *Anti-SPIT Policy Enforcement:* The final step is to enforce the defined anti-SPIT policy. This is taken care by the implementation and execution of the ontoSPIT model. When a SIP message is received the ontology is instantiated and its basic concepts and classes take specific values. Based on these values every SIP message is handled according to the conditions and actions that were defined by the policy. Therefore, the ontoSPIT model is responsible to draw conclusions about the nature of each SIP message (i.e. whether it is a SPIT message or not) by fulfilling the requirements posed by the underlying anti-SPIT policy.

4 Use of the Architecture

In this section we show how the proposed architecture could be integrated in a SIP-based VoIP environment, which is based on the SIP Express Server (SER), an open source software product that provides the basic SIP services [19,20]. A macroscopic view of our approach is presented in Fig. 4.

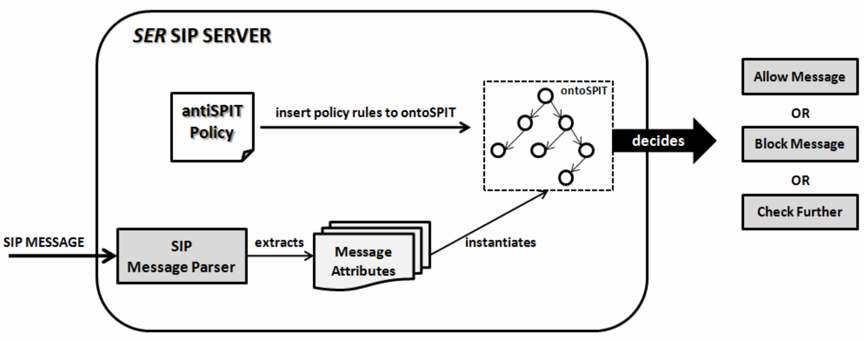


Fig. 4. Use of the proposed anti-SPIT Architecture

The basic elements of our approach are the following:

a) *SIP Message Parser:* This module is an automated process, integrated to the SER server and is used to support the routing of the incoming SIP messages. The SIP parser can scan SIP messages and extract the message attributes that will be used to check whether the messages are SPIT or not.
b) *antiSPIT Policy:* This element refers to the antiSPIT policy that is adopted by the specific SIP-based VoIP domain, which is expressed using the SWRL language [18], so as to be incorporated into the ontoSPIT model.
c) *ontoSPIT:* This module is the implemented ontoSPIT model which is responsible for enforcing the above-mentioned antiSPIT policy. The ontoSPIT model has been implemented using the well-known Protégé tool [21].

Having in mind the aforementioned approach we now present an example of a policy rule and how this rule is incorporated into ontoSPIT model using the SWRL language. The rule is responsible for checking the PRIORITY header of a SIP INVITE message and if specific conditions are met, then the message is characterized as SPIT and hence is blocked.

The condition of the rule checks if the SIP message has the PRIORITY field set as urgent and at the same time if the FROM header includes a sender that is not trusted (i.e. not presented in the white list of the domain and/or receiver of the message). The action of the rule defines that if the abovementioned condition is true, then the message is blocked. The overall rule, as well as how it is written using SWRL language, is depicted in Table 1.

5 Architecture Evaluation

In section 1 we mentioned that the current proposed anti-SPIT techniques and mechanisms are influenced by the methods used for countering spam. Therefore, they fail to take into account the SPIT vulnerabilities that are introduced by the use of SIP protocol, even when some of the mechanisms focus on SIP to handle SPIT.

Having in mind the list of SPIT oriented SIP vulnerabilities as presented in [14], we provide an evaluation of the proposed architecture using as criteria the SPIT related attacks that could be conducted in a SIP-based VoIP domain [5].

Table 1. Incorporating a policy rule into the ontoSPIT model

Rule for checking the PRIORITY header of a SIP Message	
IF (*SIP Message arrived*) **AND** ((<SIP Header=*PRIORITY*>) **AND** **IF** (< *PRIORITY* field = urgent>)) **AND** (**IF** (<*FROM* field != ID presented in WhiteList>))) **THEN** **BLOCK**	**Rule written in SWRL language:** SIPMessage(?m) ∧ ((has_header(?m,?h) ∧ has_field(?h,?f) ∧ Priority(?f) ∧ swrlb:equal (?f,"Urgent")) ∧ (has_field(?h,?f2) ∧ From(?f2)) ∧ Whitelist(?wl) ∧ contains(?wl,?x) ∧ differentFrom(?f2,?x)) ∧ (checking_of(?c,?m) ∧ previous_to_decision_1(?d,?c)))→ Block(?d)
Detailed SWRL Code	**Comments – Description**
SIPMessage(?m) ∧ (	**Whenever** a message m is received,
(has_header(?m,?h) ∧ has_field(?h,?f1) ∧ Priority(?f1) ∧ swrlb:equal (?f1,"Urgent")) ∧	**and** this message has a priority field with value "Urgent" (which means that the message m has a header h **and** this header h has a header-field f1 **and** this field f1 is of type Priority equal to "Urgent")
(has_field(?h,?f2) ∧ From(?f2)) ∧	**and** this header h has another field f2 of type From
(Whitelist(?wl) ∧ contains(?wl,?x) ∧ differentFrom(?f2,?x)) ∧	**and** there is a whitelist wl that contains the values x **and** the from field f2 is different from the values x
(checking_of(?c,?m) ∧ previous_to_decision_1(?d, ?c)))	**and** the checking c of this message m is previous to the decision d based on this checking c
→ Block(?d)	**then** the decision d must be of type Block

Moreover, we compare our approach with the current anti-SPIT mechanisms, so as to better illustrate its advantages in terms of a holistic SPIT management process. Table 2 presents our findings.

Table 2. Evaluation of the proposed architecture

Anti-SPIT frameworks **SPIT attacks**	SPIT Prevention using Anonymous Verifying Authorities	SPIT Mitigation through a Network Layer Anti-SPIT Entity	SPIT Detection based on Reputation and Charging techniques	DAPES	Progressive Multi Gray-Leveling	Biometric Framework for SPIT Prevention	RFC4474	SIP SAML	DSIP	Voice SPAM Detector	Hidden Turing Tests	VoIP SEAL	**Proposed architecture**
Address harvesting													√
Multiple Account Instantiation													√
Open relays and proxies		√	√	√	√				√	√		√	√
Anonymity Services		√	√	√	√				√	√		√	√
Obfuscating message content													√
Support services		√	√	√	√				√	√	√	√	√
Sending messages to multicast addresses													√
Exploitation of forking proxies													√
Exploitation of registrars servers						√	√	√					√
Exploitation of re-INVITE request messages													√
Exploitation of the record-route header field													√
Exploitation of messages and header fields structure													√

6 Conclusions and Further Research

VoIP technology is gaining a recognizable market share. For this reason, significant concerns are raised regarding the possibility of an explosion for SPIT attacks to the extent of email SPAM. Recently some anti-SPIT mechanisms were proposed, but they neither took into account any SPIT-related threat or vulnerability analysis, nor any attack schemes that spitters may use.

In this paper, we proposed a SPIT management architecture based on specific anti-SPIT policies that might be adopted in any SIP-based VoIP domain. The enforcement of the policies is guaranteed through the use of a SPIT oriented ontology model (onto-SPIT). Our approach takes into consideration the SPIT-related SIP vulnerabilities and threats with an eye towards providing a holistic SPIT management framework.

Regarding future work, we aim to enhance our architecture, so as to take into consideration specific statistics data, regarding SPIT traffic, and to handle this traffic in a dynamic manner. Furthermore, we are looking to incorporate the ontology in general security ontologies, so as to enhance the existing models and thus also incorporate SPAM/SPIT management processes.

Acknowledgements. We would like to thank our colleagues Yannis Mallios (Carnegie Mellon University, USA) and Marianthi Theoharidou (Athens University of Economics & Business, Greece) for their helpful comments and suggestions.

References

1. VOIPSA, VoIP Security and Privacy Threat Taxonomy (October 2005), `http://www.voipsa.org/Activities/taxonomy.php`
2. Rosenberg, J., Jennings, C.: The Session Initiation Protocol (SIP) and Spam, draft-ietf-sipping-SPAM-03 (October 2006)
3. Dritsas, S., Mallios, J., Theoharidou, M., Marias, G., Gritzalis, D.: Threat analysis of the Session Initiation Protocol regarding spam. In: Proc. of the 3rdIEEE International Workshop on Information Assurance (WIA 2007), April 2007, pp. 426–433. IEEE Press, USA (2007)
4. Marias, G., Dritsas, S., Theoharidou, M., Mallios, J., Gritzalis, D.: SIP vulnerabilities and anti-SPIT mechanisms assessment. In: Proc. of the 16th IEEE International Conference on Computer Communications and Networks (ICCCN 2007), August 2007, pp. 597–604. IEEE Press, Los Alamitos (2007)
5. Gritzalis, D., Mallios, Y.: A SIP-based SPIT management framework. Computers & Security 27(5-6), 136–153 (2008)
6. Rosenberg, J., et al.: SIP: Session Initiation Protocol, RFC 3261 (June 2002)
7. Johnston, A.: SIP: Understanding the Session Initiation Protocol. Artech House (2004)
8. Sloman, M., Lupu, E.: Security and management policy specification. IEEE Network, Special Issue on Policy-Based Networking 16(2), 10–19 (2002)
9. Dritsas, S., Soupionis, J., Theoharidou, M., Mallios, J., Gritzalis, D.: SPIT Identification Criteria Implementations: Effectiveness and Lessons Learned. In: Samarati, P., et al. (eds.) Proc. of the 23rd International Information Security Conference (SEC 2008), September 2008, pp. 381–395. Springer, Milan (2008)

10. Mallios, J., Dritsas, S., Tsoumas, B., Gritzalis, D.: Attack modeling of SIP-oriented SPIT. In: Lopez, J., Hämmerli, B.M. (eds.) CRITIS 2007. LNCS, vol. 5141. Springer, Heidelberg (2008)
11. Gruber, T.: Toward principles for the design of ontologies used for knowledge sharing. In: Formal Ontology in Conceptual Analysis and Knowledge Representation, March 1993. Kluwer Academic Publishers, Dordrecht (1993)
12. Guarino, N.: Understanding, Building, and Using Ontologies: A commentary to "Using explicit ontologies in KBS development. International Journal of Human and Computer Studies 46(3/4), 293–310 (1997)
13. Dritsas, S., Dritsou, V., Tsoumas, B., Constantopoulos, P., Gritzalis, D.: OntoSPIT: SPIT management through ontologies. Computer Communications (April 2008) (in press)
14. Dritsas, S., Mallios, J., Theoharidou, M., Marias, G., Gritzalis, D.: Threat analysis of the Session Initiation Protocol, regarding spam. In: Proc. of the 3rd IEEE International Workshop on Information Assurance, April 2007, pp. 426–433. IEEE Press, New Orleans (2007)
15. W3C Recommendation, The Ontology Web Language
16. OWL. W3C Recommendation. The Ontology Web Language (2004)
17. W3C. W3C Recommendation (10-02-2004), OWL Guide (2004)
18. Horrocks, I., Patel-Schneider, P., Boley, H., Tabet, S., Grosof, B., Dean, M.: SWRL: A Semantic Web Rule Language Combining OWL and RuleML, The DARPA Agent Markup Language Homepage
19. SIP Express Router (SER), Iptel.org.
20. Example SER deployments,
    `http://mit.edu/sip/sip.edu/deployments.shtml`
21. Protégé, Ontology development environment (2005),
    `http://protege.stanford.edu/`

Can Formalism Alone Provide an Answer to the Quest of a Viable Definition of Trust in the WWW Society?*

V. Liagkou[1,3], P. Spirakis[1,3], and Y.C. Stamatiou[2,3]

[1] University of Patras, Department of computer Engineering, 26500,
Rio, Patras, Greece
[2] Mathematics Department, 451 10, Ioannina, Greece
[3] Research and Academic Computer Technology Institute, N. Kazantzaki,
University of Patras, 26500, Rio, Patras, Greece
{liagkou,spirakis}@cti.gr, istamat@cc.uoi.gr

Abstract. Ever since the creation of the first human society, people have understood that the only way of sustaining and improving their societies is to rely on each other for exchanging services. This reliance have traditionally built on developing, among them, *trust*, a vague, intuitive to a large extend and hard to define concept that brought together people who worked towards the progress we all witness around us today. Today's society is, however, becoming increasingly massive, collective, and complex and includes not only people, but huge numbers of machines as well. Thus, trust, being already a difficult concept to define and measure when applied to a few people that form a cooperating group or a set of acquaintances, it is far more difficult to pinpoint when applied to large communities whose members may hardly know each other in person or to interconnected machines employed by these communities. In this paper we attempt to take a pragmatic position with regard to trust definition and measurement. We employ several formalisms, into each of which we define a reasonable notion of trust, and show that inherent weaknesses of these formalisms result in an inability to have a concrete and fully measurable trust concept. We then argue that trust in the modern intertwined WWW society must, necessarily, incorporate to some degree non-formalizable elements, such as common sense and intuition.

Keywords: Trust, formalism, logic.

1 Introduction

Although it is rather straightforward to say that I trust someone with whom I have been long together stating, also, the reason behind my belief (e.g. good previous collaboration, absence of hostile moves etc.), it seems very difficult to come to a

* This work has been partially supported by the ICT Programme of the European Union under contract number ICT-2008-215270 (FRONTS) and by the Open University of Cyprus within the Programme (DYSAT).

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 199–208, 2010.

conclusion as to whether to trust or not when I ``meet'' someone on the WWW or when I encounter a machine which I should use to meet my goals (e.g. a server to make an online transaction or a remote sensor that monitors a critical distant infrastructure). Although in a sufficiently large interconnection pattern like the WWW, all pairs of entities, people and machines, are only a few hops apart and, thus, massiveness of the WWW should not pose a trust problem in principle (e.g. If I do not know you, I most probably know someone else that knows you and may provide a well justified opinion of whether I should trust you or not), there are two major obstacles to the success of this approach: i) trust seems not to possess nice logical properties that aid formal deduction processes like, for instance, the transitivity property, and ii) decisions as to whether I should trust a human or a machine have to take place in an infinitesimal time instance (for instance, when an electronic transaction is pending and needs to be completed soon) and, thus, automation in trust manipulation is a highly desirable property of any formalization of the trust concept.

There is much ongoing research on the development and analysis of new trust management models for complex and dependable computer systems. Blaze *et al.* in [3] proposed the application of automated trust mechanisms in distributed systems. Josang [11] focus on the strong relationship between the notions of trust and security. Moreover a number of schemes for the design of secure information systems have been proposed (see, for example, [5, 10]) which are based on automated trust management protocols. The composition and propagation of trust information between elements of information systems is also of pivotal concern and a number of research works are devoted to them (see [21, 13, 23, 7]). Grandison and Sloman try to see the trust as a belief [17]. Based on a brief analysis they formulate the trust as *a firm belief in the competence of an entity to act dependably, securely and reliably within a specified context.* Moreover they establish the trust as a composition of several different attributes - such as reliability, dependability, honesty, truthfulness, security, competence, and timeliness - which may have to be considered depending on the environment in which trust is being specified. Here we take a different direction, we follow Dimitrakos' (see [15, 16]) definition of trust. We believe that *the trust of a party* A *in a party* B *is the measurable belief of* A *in* B *behaving dependably for a specified period within a specified context in relation to* X . Here we define the trust for a service X as a service requestor A to a service provider B for a service X . Thus, A and B are interlinked with a trust relationship, directed from A to B .

The goal of our paper is not, principally, to propose a certain formalism that allows to express and handle, algorithmically, trust. We rather have a look of several formal frameworks and explore their limitations with regard to their expressive and deductive power in defining and manipulating trust. The main principle behind this approach, is that that unpredictably dynamic, global societies encompassing huge number of elements (either people or machines) are not likely to be amenable to a static viewpoint of trust, no matter how this concept is formalized. The main reason behind this belief is exactly the dynamic nature and massiveness of the modern WWW society. We, thus, believe that trust should be a statistical, asymptotic concept to be studied as a complex relationship *emerging* in the limit as the target system of entities expands and evolves. Thus, our main goal is to study trust within formal frameworks and see how facets of it *emerge* when the involved entities, as well as the interrelationships among them, change in time in unpredictable ways. We present the limitations of these formal approach and discuss possible alternatives.

2 Random Graphs

As we discussed above, the departure point of our work is that dynamic, massive systems like the WWW society of people and machines, are not amenable to a static viewpoint of the trust concept, no matter how this concept is formalized. Thus, our main goal is to define trust as an emerging relationship among entities of the system, that ``appears" when a set of properties hold, asymptotically, almost certainly in random communication structures that model computing systems and the interaction between constituent devices. And one of the most well studied and most intuitively appealing formalism for studying *emergent properties* is the *graph*. This trust metric model can be used to evaluate trust assertions in a distributed information system. Generally, directed graphs can be used to represent and answer the following questions: A trusts B, A trusts C, B trusts D, C trusts D, when trust is assumed to be a binary, directed relationship. In order to evaluate trust between two or more entities, we can assign weights (or believe estimates) to the degree of trust given on the trust relationship. the trust as a numerical value, weighted edges can be introduced in the Strust graph model T. These weights can provide primary data for acquiring a trust value. As long as trust values are just complete definable (e.g. A trusts B and C, no trust statement is expressed to all the other entities), it is quite easy to represent a trust metric in a weighted directed graph and make suitable deductions using, for instance, belief propagation techniques or Bayesian reasoning.

However, things may get complicated if very large community graphs are involved, that evolve in an unpredictable way, such as the WWW society (see [2] for a thorough treatment of threshold phenomena in relation to random graph properties).

3 First and Second Order Logic and Relationships

3.1 First Order Language of Graphs

We are interested in discovering conditions under which a random graph model displays threshold behavior for certain properties that can also be relevant to trust or security issues. In this subsection we will be focused on properties expressible in the *first order language* of graphs. This language can be used to describe some useful (and naturally occurring in applications) properties of random graphs under a certain random graph model using elements of the first order logic.

The alphabet of the first order language of graphs consists of the following (see, e.g., [22]):

- Infinite number of variable symbols, e.g. $z, w, y \ldots$ which represent graph vertices.
- The binary relations ``==" (equality between graph vertices) and ``$\sim$" (adjacency of graph vertices) which can relate only variable symbols, e.g. ``$x \sim y$" means that the graph vertices represented by the variable symbols x, y are adjacent.

- Universal, $\exists$, and existential, $\forall$, quantifiers (applied only to *singletons* of variable symbols).
- The Boolean connectives used in propositional logic, i.e. $\vee, \wedge, \neg, \Rightarrow$.

An example of graph property expressible in the first order language of graphs is the existence of a triangle: $\exists x \exists y \exists w (x : y) \wedge (y : w) \wedge (w : x)$. Another property is that the diameter of the graph is at most 2 (can be easily written for any fixed value k instead of 2): $\forall x \forall y [x = y \vee x : y \vee \exists w (x : w \wedge w : y)]$. However, other equally important graph properties, like connectivity, cannot be expressed in this language.

We will now define the important *extension statement* in natural language, although it clearly can be written using the first order language of graphs (see [22] for the details):

Definition 1 (Extension statement $A_{s,t}$). *The extension statement $A_{s,t}$, for given values of s, t, states that for all distinct $x_1, x_2, \ldots, x_s$ and $y_1, y_2, \ldots, y_t$ there exists distinct z adjacent to all x_i s but no y_j.*

The importance of the extension statement $A_{s,t}$ lies in the following Theorem. When applied to the first order language of graphs.

Theorem 1. Let G to be a random graph with n nodes and $A_{s,t}$ to be an extension statement, then if $A_{s,t}$ for all s, t $\lim_{n \to \infty} Pr[G\ has\ A_{s,t}] = 1$, then for every statement A written in the first order language of graphs either $\lim_{n \to \infty} Pr[G\ has\ A] = 0$ or $\lim_{n \to \infty} Pr[G\ has\ A] = 1$.

The connection between threshold properties and first order logic was first noted by Fagin in the seminal paper [6].

3.2 Second Order Language of Graphs

Although the extension statement can be used in order to settle the existence of thresholds for all properties expressible in the first order language of graphs in any random graph model, things change dramatically when properties are considered that are expressed in the *second* order language of graphs. The second order language of graphs is defined exactly as the first order language (see Section 3.1) except that it allows quantification over subsets of graph vertices (predicates) instead of single vertices. An example of such a property follows (see, e.g., [12]).

Definition 2 (Separator). *Let $F = \{F_1, F_2, \ldots, F_m\}$ be a family of subsets of some set X. A separator for F is a pair (S, T) of disjoint subsets of X such that each member of F is disjoint from either S or from T. The size of the separator is* $\min(|S|, |T|)$

In the context of trust, this property may be interpreted as follows. Let us assume that $|F_i| = 2$, modeling an edge of a graph. Thus, the sets F_i model a graph's links between pairs of nodes. With this constraint, the separator property says that in a graph there exist two disjoint sets of nodes S and T such that any set of two adjacent (i.e. communicating) nodes is disjoint from either S or T. In other words, it is not possible to have one node belonging to one of the two disjoint sets S and T and the other node belonging to the other. This might mean that no two communicating nodes are authenticated by two different authentication bodies (the two disjoint sets of nodes). Thus, the two nodes can trust each other more since they are not authenticated by two disjoint (i.e. unrelated) authentication bodies. Each of the two disjoint sets may form, for instance, Certification Authority (CA) providing authentication services.

In order to cast the separator property into the language of graphs, we set X to be a set of vertices and the subsets F_i to be of cardinality 2 so as to represent graph edges. Then the separator property can be written in the framework of the second order language of graphs as follows

$$\exists S \exists T \forall x \forall y [\neg (Sx \wedge Tx) \wedge (Axy \to \neg (Sx \wedge Ty \vee Sy \wedge Tx)]. \qquad (1)$$

Let us define another property:

Definition 3 (Trusted representatives). *A graph G has the trusted representatives property if there exists a set of vertices such that any vertex in the graph is an adjacent with at least one of these vertices.*

A formal definition using second order logic is the following

$$\exists S \forall x \exists y [Axy \wedge Sy]. \qquad (2)$$

The extension statement, cannot, unfortunately, be used in order to examine whether (and under which conditions on the random graph model parameters) the separator property or the trusted representatives property is a threshold property since these properties cannot be written in the first order language of graphs.

However, in 1987 Kolaitis and Vardi initiated in [18] a research project in order to characterize fragments of the second order logic that display threshold behavior (i.e. they have a 0-1 law). The interested reader may consult the review paper [19] by the same authors. Without delving into the details, one of the important conclusions reached at by this project is that there are second order fragments that do not have a threshold behavior while other second order fragments do.

Let Σ_1^1 denote the existential second order logic (i.e. formulas contain only existential quantification over second order variables, that is sets). Let FO denote the first order logic formalism and L be any fragment of FO. Then a $\Sigma_1^1(L)$ sentence over a vocabulary R is an expression of the form $\exists S \phi(R, S)$, where S is a set of relation variables and $\phi(R, S)$ is a first order sentence on vocabulary (R, S). In general threshold behavior is not displayed by Σ_1^1 (see [19]). Thus, in order to discover fragments of Σ_1^1 that do have such a behavior, a restriction is imposed on the first order part (i.e. the sentence ϕ written in L) of the sentences considered. This restriction refers to the pattern of quantifiers that appear in the first order sentence ϕ. Some restricted first order logics that have been studied in connection to Σ_1^1 are the following:

1. The *Bernays-Schönfinkel class*, which is the set of all first order sentences with quantifier prefixes of the form $\exists^*\forall^*$ (that is, the existential quantifiers precede the universal quantifiers).
2. The *Ackermann class*, which is defined as the collection of first order sentences of the form $\exists^*\forall\exists^*$ (that is the quantification prefix contains only one universal quantifier.
3. The *Gödel class*, which is defined as the collection of first order sentences of the form $\exists^*\forall\forall\exists^*$ (that is, the prefix contains two consecutive universal quantifiers).

The separator property defined by (1) belongs to the second order fragment Σ_1^1(Gödel) since it contains (in the first order part) two consecutive universal quantifiers. On the other hand, the trusted representatives property defined by (2) belongs to the second order fragment $\Sigma_1^1(Ackermann)$ since it contains a single universal quantifier.

The trusted representatives property can be proved to be a threshold property since the second order logic fragment $\Sigma_1^1(Ackermann)$ has a threshold behavior in general (see [19]). This means that, asymptotically, it holds with either probability 0 or 1 depending on the random graph model parameters. On the other hand, the separator property is not guaranteed to be a threshold property since the Σ_1^1 (Gödel) second order logic fragment does not display a threshold behavior in general (see [19]).

Thus, sentences (properties) that can be written in fragments of second order logic that have a threshold behavior (e.g. $\Sigma_1^1(Ackermann)$) are threshold properties. However, some second order logic fragments allow the construction of sentences that have no limiting probability and, thus, are not 0/1 properties, limiting our ability to assert their long-term validity.

It should be stressed that we do not know (perhaps it is not possible to know) whether all possible trust-related properties can be cast either within the framework of first order logic or second order logic.

4 Probability Theory – Undecidable Probabilities

Theorem 2 [Trachtenbrot-Vaught Theorem [24]]. *There is no decision procedure that separates those first order statements S that hold for some finite graph from those S that hold for no finite graph.*

With regard to random graphs now which, as we show, in conjunction with the first and second order language of graphs, can be used to express, formally, complex relationships that can be related to trust, we have the following result (see [4]):

Theorem 3. *There is no decision procedure that separates those first order statements S that hold almost always for the random graph $G_{n,p}$ from those for which $\neg S$ holds almost always.*

This theorem is targeted to $G_{n,p}$ random graphs, with $p = n^{\alpha}$, α being a rational number between 0 and 1. In summary, for any first order statement A about a finite graph, a first order statement A^* is given that holds almost always in $G_{n,p}$, *if* A holds for some finite graph, while it never holds, if A holds for *no* finite graph. Now, if a formal procedure (algorithm) existed for deciding such statements for the $G_{n,p}$ model, then relationship between A and A^* would allow using the procedure to separate those first order statements A that hold for some finite graph from the statements that hold for no finite graph, contradicting the Trachtenbrot-Vaught Theorem.

More specifically, let us consider the following statement S: There is no isolated vertex in the graph, which can be written as $\forall y \exists z (y : z)$. Let S^* be the corresponding statement, for the random graph $G_{n,p}$ with $p = n^{-2/5}$ (see [4]): $\exists x_1 \exists x_2 \exists x_3 \exists x_4 [\forall y MEM(y; x_1, x_2, x_3, x_4) \Rightarrow \exists z MEM(z; x_1, x_2, x_3, x_4) \wedge ADJ(y, z)]$ with MEM and ADJ the following first order language predicates:

$$MEM(y; x_1, x_2, x_3, x_4) \Leftrightarrow \exists z [(z : x_1) \wedge (z : x_2) \wedge (z : x_3) \wedge (z : x_4) \wedge (z : y)]$$

$$\begin{gathered} ADJ(u, v) \Leftrightarrow MEM(u; x_1, x_2, x_3, x_4) \wedge \\ MEM(v; x_1, x_2, x_3, x_4) \wedge \exists t MEM(t; x_1, x_2, u, v). \end{gathered}$$

$$\lim_{n \to \infty} Pr[G_{n,p} \ has \ S^*] = \begin{cases} 0 \ if \ S \ holds \ for \ no \ finite \ graph, \\ 1 \ if \ S \ holds \ for \ some \ finite \ graph. \end{cases} \tag{3}$$

Then a decision procedure that could differentiate between statements that hold almost always in $G_{n,p}$ and the statements whose negation holds almost always, would provide a decision procedure to differentiate between those statements S that hold for *some* finite graph and those that hold for no finite graph, contradicting the Trachtenbrot-Vaught Theorem.

The morale of this discussion is that it may not even possible to mechanically analyze whether a given state of affairs (e.g. trust assertion) or its negative, within the world of discourse (WWW society), is expected to almost certainly appear. Thus, it may be the case that one may have to observe the target world for sufficiently much time in order to be able to make a safe prediction about the state of affairs that will finally prevail in the limit.

5 The Self-referential Nature of Trust

Finally, in this section, we discuss an important weakness that arises in any formalism, when it is sufficiently powerful to be able to ``talk about itself", i.e. to contain statements about its expressive and deductive power (i.e. derivable statements).

According to the famous incompleteness theorem of Gödel, any formal system powerful enough to encompass the Peano axioms, contains statements for which neither the statement or its negation can be proved using the axioms and deductive rules of the formal system. In other words, there are truths and valid statements that cannot be asserted, using the formalism and its derivation rules alone. Another expression of this ``self-reference" phenomenon, from the point of view of computability theory this time, was given by Alan Turing in 1936 who described a universal computation machine model. In his famous work *On computable numbers, with an application to the Entscheidungsproblem* Turing defined a mathematical model for a device that performs mechanical calculations, later named *Turing machine* after its inventor. This suprisingly minimal, yet maximally powerful, model consisted simply of a infinite tape divided into cells each holding a particular symbol (say 0 or 1), a tape head that can move about the tape reading or writing symbols and, most important, a finite control able to decide on the next thing to do based on the current machine state and the symbol currently under the tape head. The first success of this simple model of algorithmic computation came immediately: Turing proved that no Turing machine and, hence, no algorithm according to *Church's Thesis* exists to decide whether another Turing machine halts when it starts computing with a specified input putting an end to Hilbert's grand program of mechanizing mathematics. The proof, actually, is a computational version of the proof of Gödel, which was cast within the logic calculus formalism. (We would like to urge the interested reader to consult [8] for an excellent account of the developments that paved the way to the rich theories of Computation and Complexity and [9] for a most comprehensive presentation of Computation and Complexity theory as it stands today.)

We can modify the main argument of the two historic results by Gödel and Turing, so as to give a glimpse of the inherent limitations of formalisms with respect to trust definition and manipulation as follows. We recall, that for our purposes trust is a property, a predicate more precisely, that dictates that the involved entities are in a certain state with regard to each other, i.e. the predicate holds.

Let us assume that we have defined a set of trust axioms that we believe are applicable in the situation at hand. For instance, these axioms may include the fact that in our world of discourse trust has the transitivity property, i.e. from $T(x, y)$ and $T(y, z)$ we may deduce $T(x, z)$. We would like to be able to test whether the trust property holds among some other set of entities, by exploiting the axioms and the deduction mechanisms of our formalism. We may recursively enumerate the possible axioms (given trust assertions) of our world of discourse (assumed to be finite) into strings, $w1, w_2, \ldots$. We may also enumerate the possible deduction mechanisms (algorithms) that start from the axioms, apply a set of derivation rules, and then reach a decision with respect to whether a certain trust assertion among entities of our world of discourse is true or not. Then, using an argument similar to Turing's, we may show that no universal trust derivation process may exist that starts from a description of the world of discourse (axioms plus derivation rules) and decides whether a trust assertion follows or not.

6 Discussion

Trust has been one of the cornerstones of the success of modern society in building well-organized groups of people working towards their own wealth as well as that of theirs peers. This traditional notion of trust, however, has two basic characteristics: i) it is based on personal contact, and ii) frequently, it cannot be explained.

Today, it is impossible to have personal information about any entity (either human or a machine offering a service) of the huge and ever expanding WWW society, with which we may want to communicate or perform a transaction. Thus, we would like to rely on rules as well as automated deductive procedures as to whether we should trust an WWW entity or not.

In this paper we have reviewed a number of formalisms with respect to their expressive and deductive power when describing large combinatorial structures, where the structure consists of a number of entities as well as trust assertion among them. We saw that each of the formalisms has some weaknesses in handling trust in complex, large environments containing a huge number of entities that interact unpredictable (almost randomly). Our position is that these observations seem to hint that reliance on formalism alone is not the answer to the problem of defining and manipulating trust. Rather, WWW entities should better focus on including fast heuristics as well as approximations to reality (even accepting trust in some cases axiomatically, e.g. to avoid the incompleteness pitfalls of powerful formal deductive systems). Moreover, it seems that trust will rely, for some time (until we manage to define it alternatively) on what it relied traditionally for the past few centuries: personal experience, public guidance from organizations and governments, creation of awareness groups, and avoiding trusting a WWW entity whenever one is not totally sure about trusting it (educated decisions). Otherwise, formal trust may either be unattainable (e.g. incompleteness results about formalisms) or hard to verify (NP-completeness results from computational complexity).

References

1. Bars, J.-M.L.: Fragments of existential second-order logic without 0-1 laws. In: 13th IEEE Symp. on Logic in Computer Science, pp. 525–536 (1998)
2. Bollobás, B.: Random Graphs, 2nd edn. Cambridge University Press, Cambridge (2001)
3. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 164–173 (1996)
4. Dolan, P.: Undecidable statements and random graphs. Annals of Mathematics and Artificial Intelligence 6, 17–26 (1992)
5. Trachtenbrot, B.: Impossibility of an algorithm for the decision problem on finite classes. Doklady Akad. Nauk. S.S.R. 70, 569–572 (1950)

6. Eschenauer, L., Gligor, V., Baras, J.: On trust establishment in mobile ad-hoc networks. In: Security Protocols Workshop, Cambridge, UK, pp. 47–66 (2002)
7. Fagin, R.: Probabilities on finite models. Symbolic Logic 41, 50–58 (1976)
8. Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust. In: International Conference on World Wide Web, pp. 403–412 (2004)
9. van Heijenoort, J.: From Frege to Gödel: A Source Book in Mathematical Logic. Harvard University Press, Cambridge (1967)
10. Herken, R. (ed.): The Universal Turing Machine: A Half-Century Survey. Springer, Heidelberg (1995)
11. Hubaux, J.-P., Buttyan, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: ACM International Symposium on Mobile ad-hoc networking and computing, pp. 146–155 (2001)
12. Josang, A.: The right type of trust for distributed systems. In: New Security Paradigms Workshop, pp. 119–131 (1996)
13. Jukna, S.: Extremal Combinatorics - with Applications in Computer Science. Springer, Heidelberg (2001)
14. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: International Conference on World Wide Web, pp. 640–651 (2003)
15. Cheeseman, P., Kanefsky, B., Taylor, W.M.: Where the really hard problems are. In: Proc. of the International Joint Conference on Artificial Intelligence, pp. 331–337 (1991)
16. Dimitrakos, T., Bicarregui, J.C.: Towards A Framework for Managing Trust in e-Services. In: Proceedings of the 4th International Conference on Electronic Commerce Research, ATSMA, IFIP (November 2001) ISBN 0-9716253-0-1
17. Dimitrakos, T.: System Models, e-Risk and e-Trust. Towards bridging the gap? In: Towards the E-Society: E-Business, E-Commerce, and E-Government (2001)
18. Grandison, T., Sloman, M.: A Survey of Trust in Internet Applications. In: IEEE Communications Surveys and Tutorials (2000)
19. Kolaitis, P., Vardi, M.: The decision problem for the probabilities of higher-order properties. In: 19th ACM Symp. on Theory of Computing, New York, pp. 425–435 (1987)
20. Kolaitis, P., Vardi, M.: 0-1 laws for fragments ofexistential second-order logic: A survey. In: Nielsen, M., Rovan, B. (eds.) MFCS 2000. LNCS, vol. 1893, pp. 84–98. Springer, Heidelberg (2000)
21. Nikoletseas, S., Raptopoulos, C., Spirakis, P.: The existence and efficient construction of large independent sets in general random intersection graphs. In: Díaz, J., Karhumäki, J., Lepistö, A., Sannella, D. (eds.) ICALP 2004. LNCS, vol. 3142, pp. 1029–1040. Springer, Heidelberg (2004)
22. Richardson, M., Agrawal, R., Domingos, P.: Trust management for the semantic web. In: International Semantic Web Conference, pp. 351–368 (2003)
23. Spencer, J.: The strange logic of Random Graphs. Springer, Heidelberg (2001)
24. Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: ACM Workshop on Wireless security, pp. 1–10 (2004)
25. Trachtenbrot, B.: Impossibility of an algorithm for the decision problem on finite classes. Doklady Akad. Nauk. S.S.R. 70, 569–572 (1950)

Biological Aspects of Computer Virology

Vasileios Vlachos[1], Diomidis Spinellis[2], and Stefanos Androutsellis-Theotokis[2]

[1] Department of Computer Science and Telecommunications
Technological Educational Institute of Larissa
vsvlachos@gmail.com

[2] Department of Management Science and Technology
Athens University of Economic Business
{dds,stheotok}@aueb.gr

Abstract. Recent malware epidemics proved beyond any doubt that frightful predictions of fast-spreading worms have been well founded. While we can identify and neutralize many types of malicious code, often we are not able to do that in a timely enough manner to suppress its uncontrolled propagation. In this paper we discuss the decisive factors that affect the propagation of a worm and evaluate their effectiveness.

Keywords: Malware, Computer Epidemiology, Artificial Immune Systems.

1 Introduction

Computer viruses and worms are definitely not a new threat as they exist for several decades. The striking difference between the "ancient" viruses and the modern ones lies in the time-frame in which they operate. Ancient viruses needed weeks or even months to propagate and reach a noticeable level of prevalence because of the completely different means of infection, such as diskettes, on which they relied. On the contrary, modern viruses and worms utilize the Internet and other high-speed networks achieving sizable infection rates. Theoretical studies [44,51,52], but also empirical evidence [32] suggests that last generation worms are perfectly capable of infecting a susceptible population in about 15 minutes. The construction of rapid malcode is by no means an easy task. While thousands of worms exist, only a small fraction managed to prevail in an observable level and only a handful of them to create epidemic outbreaks. Similarly, though thousands biological pathogens survive, just a small percentage of them is able to cause major health threat. Therefore it would be useful to stand on the experience of practical epidemiologists, so as to identify the major factors that dominate the propagation of a biological pathogen and thereafter to try to correlate these factors with components that may affect the virulence of computer malware. The rest of the paper is organized as follows. Section 2 surveys the existing literature on biologically inspired computer security research. In Section 3 we discuss the effective parameters that can lead to infectious diseases epidemics and draw the first analogies between biological and computer virulence.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 209–219, 2010.

In Sections 4 and 5 we present and analyze these factors, while in Section 6 we fit these findings in the concept of Computer Epidemiology. Section 7 concludes this paper.

2 Related Work

The similarities between biological pathogens and computer malware are semantically evident, as the most popular description of malcode suggests. Computer virus is the term that F. Cohen with his supervisor L. Adleman coined to describe the earliest and simplest forms of malicious software [9,10]. Even before the formalism that was developed from Adleman's term and Cohen's work, an other category of misbehaving programs was described with another biological analogy as *rabbits* [45]. The similitude of computer malcode and live pathogens was not overlooked by the research community. In particular, researchers [28] looked in great detail characteristics of computer worms and well known biological diseases and tried to compare specific types of pathogens with prominent species of malware and examine their most important properties in regard to their propagation success. Other efforts [54] concentrated on public health policies that are in place against major epidemics (Acquired Immune Deficiency Syndrome – AIDS) and proposed equivalent public policies for computer malware. An extensive review of the literature reveals that two basic strategies are available to tackle the malware problem: A microscopic approach that extends the analogies between the biological viruses and computer malware and tries to develop artificial systems with similar functionality to the human immune system and a macroscopic methodology that employs epidemiological tools to gain insights in the propagation dynamics of rapid malcode as happens with the infectious diseases.

Many efforts focused on the application of the basic mechanisms of the immune system to computer security. Forrest et al. [14,15,43] implement some immunological functions paying attention to the mechanism that distinguishes self to non-self elements of the human body so as to embed a similar technique to computer systems that is capable of recognizing legitimate use from abuse. A large part of their work has found application to the 'pH' patch for the Linux kernel [42] with promising results, while some other efforts that also use immunological concepts are in early stages [34]. Aickeling & Greensmith claim that the insufficiency of various artificial immune systems to address the problem of computer security could be due to use of older immunological models. In their work they employ the most recent immunological theories. In collaboration with practical immunologists they implement two algorithms, the Dendritic Cell Algorithm (DCA) [21] and the Toll-Like Receptor Algorithm (TLR) [1]. These algorithms are part of the Danger Theory Project [11], which adapts the recent theories of immunologists. According to the Danger Theory, a complex signaling mechanism is responsible for the activation of the immune system, rather the simplistic 'non-self' versus 'self' principle [29]. The fact that the Danger Theory is not unanimously accepted in the medical world [31], raises some questions about its effectiveness as viable model for Artificial Immune Systems.

Burgess [8] dealt with the most basic foundations of biology such as health and sickness and tried to express them as security policies. Many of his ideas have been realized in the *cfengine* project [7]. Of particular interest are his remarks about redundancy, which he founds of limited use in computer security. On the other hand, others base their work on this concept and accept as unavoidable the loss of some computer systems. Though this loss is not pleasant at larger scale can act as an alarm for the majority of the networked components [48]. According to previous research [49,50] principles of Computer Hygiene could slow down the spread of malicious agents. Another biological inspired approach focuses on models that try to mimic the functionality of genomics and protomics. Goel and Bush [19] propose a system that is able to create new virus - signatures by mutation of the existing signatures. Shafi and Abbass [40] present in their work a more holistic approach as they consider several Complex Adaptive Systems with foundations in the physical world. They examine paradigms of security systems that utilize Genetics Based Machine Learning, Swarm Intelligence and Coevolution.

Most of the conducted research tackles specific aspects of computer virulence in order to find appropriate means to minimize the risk of a malware epidemic. This paper investigates the joint effects of the factors that dominate the propagation of malicious agents. Three major components seem to dominate the propagation of a worm, the *Infection Propagator*, the *Target Locator* and the *Worms Virulence*.

3 Infection Propagator

The type of the attacked vulnerability is one of the most critical factors that heavily affect the virulence of a worm. Generally what influences the outcome of that choice, could be best described by the prevalence of the exploited vulnerability, the age of the vulnerability at time of exploitation and the exploitation difficulty of the attacked vulnerability.

3.1 Vulnerability Prevalence

Worm writers normally prefer to infect the largest possible number of susceptible systems. To maximise the number of the contaminated systems it is necessary for a worm to exploit a popular vulnerability. As [18,17,20] showed, the homogeneity of operating systems and applications is perfectly suited for worm writers. The fact that up to 95 percent [35] of all the computer systems in the world use some version of Microsoft's Windows operating system and the majority of them have also a version of Microsoft's Office installed make them attractive targets for any kind of attack. Given that Microsoft's operating systems and applications exhibit a large number of vulnerabilities renders the situation even worse. The OpenBSD operating system on the other hand, which according to its authors, suffered 'only two remote holes in the default install, in more than 10 years' and occupies less than 1 percent share is obviously less attractive as a target. This asymmetry leads directly to a constantly increasing number of attacks against the popular operating systems and applications making their use even more insecure. The monocultures have also significant impact on other aspects of the worm's development process. The possibility of contaminating up to 95 percent of the susceptible population using only a single infection vector lowers the bar regarding the required skills of a worm writer. Complicated malcode, such as the Slapper worm [3] necessitate extra work to utilize multiple attack vectors in order to infect a number of different distributions of the Linux operating system thus requiring much more effort from a worm writer to achieve similar effects with a worm that operates in a homogeneous environment. It has yet to be decided whether we prefer to have highly homogeneous environments so as to avoid the cost of portability and to further enhance the standardization of software development, or we should pay more attention to the security disadvantages of that approach and start building more heterogeneous systems. Even if we stick to the current monoculture, whether we have other means to diminish these effects and whether it is possible to obtain software diversity as a countermeasure, are nevertheless open questions.

3.2 Age of the Vulnerability at Time of Exploitation

The cycle from discovering a vulnerability till the development of a patch is a lengthy process that requires a number of intermediate steps. Obviously, recently discovered vulnerabilities are much more promising from a worms' writer perspective, because most users need several days, if not weeks or longer, to update their systems. If a vulnerability is recent enough it is highly probable that a significant number of systems will be unpatched and hence unprotected. Recent evidence indicates that modern malcode tends to minimise the time interval between the disclosure of a vulnerability and its exploitation. The Witty worm [41] took advantage of a vulnerability that was announced only the day before, however the great fear is for worms that will exploit an unknown or *zero-day* vulnerability. To protect better against known threats the standard methodology followed by vendors, researchers and system administrators involves: *vulnerability discovery, patch development and testing* and *vulnerability announcement and patch deployment.*

This procedure showed positive results, but also highlighted a number of downsides. When a vulnerability is announced, both the legitimate users and the malicious crackers become aware of it. Thus, adversaries start actively seeking susceptible non-patched systems in order to exploit them. It is important to note that the technical skills required to discover a vulnerability are quite different and much higher than to exploit a public announced one. Furthermore, the reverse-engineering of a patch offers valuable information to an adversary allowing him to develop in a lesser time an exploit for the specific vulnerability. Recent research [39] provides provocative but also sound arguments to keep some discovered vulnerabilities secret, questioning the way we handled the vulnerabilities disclosure procedure till now. We are confident that this and other related studies [4] will initiate some very interesting debates in the near future regarding whether, when and who should publicly announce vulnerabilities.

3.3 Exploitation Difficulty

As security becomes a major factor during the software development lifecycle not only the number of vulnerabilities diminishes, but also they become much more difficult to be exploited. Hence we can observe a switch from the traditional and easy to implement *stack smashing* techniques to much more sophisticated *arc injections, pointer subterfuge* and *heap smashing* attacks [38]. While these developments are overall positive, they lead to a new breed of malicious crackers with exceptional skills. Unfortunately these crackers don't limit their operations only to breaking systems but also write highly advanced worms such as the Slapper worm. These advancements seem to conclude the shift of successful worm writers from disgruntled teenagers with limited abilities (also known as *script kiddies*, because they tend to use already available tools and code instead of developing their own) to highly skilled malevolent programmers. It remains to be seen what other measures or designs should be embedded in the future programming languages in order to further limit the space in which the malicious crackers operate.

4 Target Locator

A worm, in order to propagate successfully, should have an efficient target locator. Staniford et al showed the great importance of the propagation strategy of a worm as different propagation dynamics can cause completely different outcomes in the spread of a worm. In their seminal work [44] they presented a short-list of the most eminent target locators namely *Random Scanning*, *Localized Scanning*, *Hit-list Scanning*, *Permutation Scanning*, *Topological Scanning* and argued for or against their efficiency. They also coined the terms *Warhol Worm* and *Flash Worm*.

5 Worm Virulence

Pathogens, microbes and parasites share a common behavior with artificial viruses regarding their propagation, because of their virulence. The virulence of a microorganism (such as a bacterium or virus) is defined as a measure of the severity of the disease it is capable of causing [30]. Ebola hemorrhagic fever has one of the highest mortality and fatality rates and therefore is able to eradicate small villages, but because of the severe symptoms and the short incubation time is almost never spread over large geographic areas [37]. On the contrary the influenza virus has usually mild symptoms and therefore the patients neglect to search for cure during the early phases of the infections, which turns them to a carriers of the disease to a large number of the population. During the 20th century the influenza A is responsible for deaths of 20 to 40 million persons [47], while the *Spanish flu* [6] is still considered as one of the worst pandemics ever. The biological analogy between the destructiveness of the malware, measured by the rate of worm-induced host mortality, and the parasite virulence has brought to general attention the underestimated, but nonetheless critical factor of the effectiveness of worm virulence. Most of the successful worms did not carry an explicitly destructive payload [16]. Undoubtedly the more harmful a worm is, the more attention it attracts. Therefore, it is highly probable that if a worm has been developed just for fun or for surveillance purposes without damaging properties, it will not be easily noticed.

On the other hand, Hofmeyr [22] argues that the virulence of malware is a far more complicated issue and poses interesting questions regarding the interaction between different types of malware coexisting in the same host. Though these interactions have been studied in biology [53], they are still neglected in the case of malware. The consequences of this omission may become evident in the feature as it is quite common for different types of malware to compete for the same resources. Malware writers started to use to their benefit the spread of the other types of malcode as it can be seen from the infection techniques of the Nimda worm which took advantage of the Code Red II and Sadmind backdoors. Often worm writers tend to act antagonistically as was with the heavily noticed Netsky – MyDoom wars, but most of the times malcode works synergistically. An arguable [33] solution to slowdown most of the existing worms proposes the release of ‘good’ worms that will search and eliminate both the malicious worms by deleting them and simultaneously reduce the number of the susceptible hosts by upgrading specific vulnerabilities making them immune to future attacks that target the specific vulnerabilities [26,46].

6 Computer Epidemiology

As showed in the previous sections many factors contribute to the success or the failure of a worm. To which extent each one of them affects their overall performance and consequently where we should concentrate our efforts to suppress their spread are still open questions which we will have to focus on in the near future. Numerous renowned scientists, including Daniel Bernoulli, Ronald Ross, Lowell Reed and Wade Hampton Frost, combined epidemiology with mathematical models to establish Mathematical Epidemiology. William Ogilvy Kermack and Anderson Gray McKendrick [25] however, were responsible for the most widely accepted mathematical model to describe the progress of an epidemic, the *General Epidemic Model*. Based on that model and by using the following three differential equations, where N is the fixed population size, S is the number of the susceptible hosts, I is the number of the infected hosts, R is the number of the recovered, quarantined or deceased individuals, β is the *pairwise rate of infection*, γ is the removal rate and under certain assumptions such as the homogeneous mixing of the population, it is possible to depict accurately the circulation of a disease.

$$\frac{dS}{dt} = -\beta SI \tag{1}$$

$$\frac{dI}{dt} = \beta SI - \gamma I \tag{2}$$

$$\frac{dR}{dt} = \gamma I \tag{3}$$

given that the population size is constant

$$N = S(t) + I(t) + R(t) \tag{4}$$

In our effort to correlate the variables of this model, which is also known as S-I-R (Susceptible-Infective-Recovered) model, with the physical quantities of an epidemic, we will find striking similarities between the spread of biological viruses and the propagation of computer worms. Kephart was the first, who in his seminal work introduced McKendrick's epidemiological models to describe the spread of computer viruses [23,24]. While he is the founder of computer epidemiology at that time the propagation speed of malicious code did not constitute a major threat. It was only shortly after the malware epidemics of Code Red, Code Red II and Nimda that it was made clear that traditional approaches to protect against malicious code, were no longer sufficient. Hence, Staniford et al [44] started to investigate worms' propagation dynamics under the prism of epidemiology with remarkable success. Since then, a lot of effort has been put into the improvement and finetuning of these models [55].

The following interpretation of biological epidemiology in a computer network context is our own and may only slightly differ from other established approaches, but we believe that are closely related and can sufficiently explain the three essential ingredients of worms' effectiveness, which we presented in the first part of the paper.

- N: the fixed population size. In computer epidemiology, it is usually the total number of hosts connected to the Internet, if the spread of a given worm is to be examined.
- S: the number of the susceptible hosts. In our context this means computers running the application or operating system that the virus targets. As discussed in the third section of this paper, the more prevalent an operating system or an application is, the more likely to get exploited in case of an vulnerability and the sooner the susceptible population will become infected. Therefore, the diversity in our digital infrastructure is not an unnecessary luxury, but an essential precaution.
- I: the number of the infected hosts. Our collective efforts should focus on minimizing that set.
- R: the number of the recovered, quarantined or deceased individuals. In a malware epidemic R represents patched or well hardened systems, resilient to the exploited vulnerabilities. It is clearly to our best interest to convince users to keep their systems secured and updated and thus to have R maximized. As the age of an vulnerability decreases, is more difficult to have the majority of systems updated. Moreover, if a worm utilizes a *zero day* exploit, the only way to increase R is to rely on external security mechanisms, such

as firewalls, in the hope that way a malcode attack can be intercepted. Of course, there is also another aspect of R. In a similar way to the biological death of some part of the population due to a pathogen, also some computer systems can be damaged from a destructive worm. Therefore a super virulent worm might face significant challenges to its further propagation.

- β: the *pairwise rate of infection*. The larger β this is, the more rapidly a worm spreads. In order to increase β malcode writers employ, usually intuitively, various techniques. Characteristic examples are the spawning of multiple threads of the target locator as in the case of the Code Red Worm or fitting the whole worm code in a single UDP packet to eliminate TCP connection latency [32].
- γ: the removal rate, either via disinfection, isolation or death in the physical world. During a malware epidemic a large γ would obviously help the containment of a worm. This can be attributed to either an effective mechanism to timely provide patches to vulnerable systems or to a very destructive payload. Contrary to the common belief, a very harmful worm could hinder its further propagation leading to its extinction.

Another important parameter that does not appear directly to the aforementioned equations is ρ the *relative removal rate* which is defined as

$$\rho \equiv \frac{\gamma}{\beta} \tag{5}$$

An epidemic outbreak is possible only when the number of initial susceptible population $S_0 > \rho$.

Of course that depends also on the underlying network topology, as useful theoretical studies have indicated [27] with implicit implications for scale-free graphs [36], which represent the majority of most technical and technosocial networks [2,5,13,12]. The developments in computer epidemiology allow us to understand, model and accurately predict the spread of malicious software, which is necessary for the implementation of effective network defenses and automatic containment mechanisms capable to suppress its propagation in the available time frame.

7 Conclusion

Given the dependency of modern societies on digital infrastructures the rapid malcode is a serious problem. The most advanced nations strive to implement effective cyber-defences against the new generation of malware-based threats. The development of malcode detection algorithms that are applicable to anti-virus programs or host-based intrusion detection systems have proven useful, but inadequate to contain rapidly spreading malware epidemics. The microscopic analysis is nonetheless essential to disinfect or protect a system, once a worm has gained access to it. On the other hand to secure the operational availability of critical information, communications, and control systems a strategic approach is required. In medicine, microbiologists and epidemiologists act complementary to ensure timely identification of new threats and provide the best possible protection of the susceptible population. In our domain a similar methodology should be applied to fight efficiently digital threats.

References

1. Aickelin, U., Greensmith, J.: Sensing danger: Innate immunology for intrusion detection. Information Security Technical Report 12, 218–227 (2007)
2. Albert, R., Barabási, A.: Statistical mechanics of complex networks. Reviews of Modern Physics 74(1), 47–97 (2002)
3. Arce, I., Levy, E.: An analysis of the slapper worm. IEEE Security & Privacy 1(3), 82–87 (2003)
4. Arora, A., Telang, R.: Economics of software vulnerability disclosure. IEEE Security & Privacy 3(1), 20–25 (2005)
5. Barabási, A., Albert, R., Jeong, H.: Scale-free characteristics of random networks: the topology of the world-wide web. Physica A 281, 69–77 (1999)
6. Barry, J.: The Great Influenza. Penguin Group, New York (2005)
7. Burgess, M.: Probabilistic anomaly detection in distributed computer networks. Science of Computer Programming 1, 1–26 (2006)
8. Burgess, M.: Biology, immunology and information security. Information Security Technical Reports 12, 192–199 (2007)
9. Cohen, F.: Computer viruses – theory and experiments. Computers and Security 6, 22–35 (1987)
10. Cohen, F.: A Short Course on Computer Viruses. Wiley Professional Computing. Wiley, Canada (1994)
11. DangerProject. The danger project (September 2008), http://www.dangertheory.com/
12. Ebel, H., Mielsch, L., Bornloldt, S.: Scale-free topology of e-mail networks. Physical Review E 66(035103(R)) (September 2002)
13. Faloutsos, M., Faloutsos, P., Faloutsos, C.: On power-law relationships of the internet topology. In: Proceedings of ACM SIGCOMM, Cambridge, MA, USA, pp. 251–262 (1999)
14. Forrest, S., Hofmeyr, S., Somayaji, A.: Computer immunology. Communications of the ACM 40(10), 88–96 (1997)
15. Forrest, S., Somayaji, A., Ackley, D.: Building diverse computer systems. In: IEEE 6th Workshop on Hot Topics in Operating Systems (1997)
16. Furnell, S., Ward, J.: The true computer parasite (June 2005), http://securityfocus.com/infocus/1838
17. Geer, D.: Monopoly considered harmful. IEEE Security & Privacy 1(6), 14–16 (2003)
18. Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C.P., Quarterman, J.S., Schneier, B.: Cyber insecurity: The cost of monopoly. Technical report, Computer & Communications Industry Association (2003)
19. Goel, S., Bush, S.: Biological models of security for virus propagation in computer networks. Login 29(6) (December 2004)
20. Goth, G.: Addressing the monoculture. IEEE Security & Privacy 1(6), 8–10 (2003)
21. Greensmith, J., Aickelin, U.: The deterministic dendritic cell algorithm. In: Bentley, P.J., Lee, D., Jung, S. (eds.) ICARIS 2008. LNCS, vol. 5132, pp. 291–302. Springer, Heidelberg (2008)

22. Hofmeyr, S.: On the virulence of malware (June 2007), http://www.nthworld.org/archives/malware/index.htm
23. Kephart, J.: How topology affects population dynamics. In: Proceedings of Artificial Life 3, New, Mexico, USA (June 1992)
24. Kephart, J., White, S.: Directed-graph epidemiological models of computer viruses. In: Proceedings of the 1991 Computer Society Symposium on Research in Security and Privacy, California, USA, pp. 343–361 (1991)
25. Kermack, W.O., McKendrick, A.G.: A contribution to the mathematical theory of epidemics. In: Proceedings of the Royal Society of London. Series A, vol. 115, pp. 700–721 (1927)
26. Kim, H., Kang, I.: On the functional validity of the worm-killing worm. In: Proceedings of the 2004 IEEE International Conference on Communications, June 2004, vol. 4, pp. 1902–1906 (2004)
27. Leveille, J.: Epidemic spreading in technological networks. Hpl-2002-287, School of Cognitive and Computing Sciences, University of Sussex at Brighton, Bristol (October 2002)
28. Li, J., Knickerbocker, P.: Functional similarities between computer worms and bilogical pathogens. Computers & Security 26, 338–347 (2007)
29. Matzinger, P.: The danger model: A renewed sense of self. Science 296, 301–305 (2002)
30. MedicineNet. Definition of virulence (2008), http://www.medterms.com/script/main/art.asp?articlekey=6911 (December 2008)
31. Medzhitov, R., Janeway, C.: Decoding the patterns of self and nonself by the innate immune system. Science 296, 298–300 (2002)
32. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N.: Inside the slammer worm. IEEE Security & Privacy, 33–39 (July 2003)
33. Weaver, N., Ellis, D.: White worms don't work. Login 31, 33–38 (2006)
34. Okamoto, T., Ishida, Y.: A distributed approach against computer viruses inspired by the immune system. IEICE Transaction on Communications E83-B, 908–915 (2000)
35. OneStat. Microsoft's windows os global market share is more than 97 to onestat.com (2008), http://www.onestat.com/html/press-release-microsoft-windows-vista-global-usage-share-december-2008.html (May 2005)
36. Pastor-Satorras, R., Vespignani, A.: Epidemic spreading in scale-free networks. Physical Review Letters 86, 3200–3203 (2001)
37. Pattyn, S. (ed.): Ebola Virus Haemorrhagic Fever. Elsevier/North-Holland, Amsterdam (1977)
38. Pincus, J., Baker, B.: Beyond stack smashing: Recent advances in exploiting buffer overruns. IEEE Security & Privacy 2(4), 20–27 (2004)
39. Rescorla, E.: Is finding security holes a good idea? IEEE Security & Privacy 3(1), 14–19 (2005)
40. Shafi, K., Abbass, H.: Biologically-inspired complex adatpive systems approaches to network intrusion detection. Information Security Technical Report 12, 209–217 (2007)
41. Shannon, C., Moore, D.: The spread of the witty worm. IEEE Security & Privacy 2(4), 46–50 (2004)
42. Somayaji, A., Forrest, S.: Automated response using system-call delay. In: Nith USENIX security symposium (2000)

43. Somayaji, A., Hofmeyr, S., Forrest, S.: Principles of a computer immune system. In: Meeting on New Security Paradigms, Langdale, UK, September 23-26, 1997, pp. 75–82. ACM, New York (1998)
44. Staniford, S., Paxson, V., Weaver, N.: How to 0wn the internet in your spare time. In: Proceedings of the 11th USENIX Security Symposium, August 2002, pp. 149–167 (2002)
45. Szor, P.: The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River (2005)
46. Tanachaiwiwat, S., Helmy, A.: Modeling and analysis of worm interactions (war of the worms). In: Fourth International Conference on Broadband Communications, Networks and Systems, 2007. BROADNETS 2007, pp. 649–658 (2007)
47. Sabelis, M., Dieckmann, U., Metz, J., Sigmund, K. (eds.): Adatpive Studies in Dynamics of Infectious Diseases. Cambridge University Press, Cambridge (2002)
48. Vlachos, V., Androutsellis-Theotokis, S., Spinellis, D.: Security applications of peer-to-peer networks. Comput. Networks 45(2), 195–205 (2004)
49. Vlachos, V., Raptis, A., Spinellis, D.: PROMISing steps towards computer hygiene. In: Furnel, S. (ed.) International Network Conference (INC2006), Plymouth, UK, July 2006, pp. 229–236 (2006)
50. Vlachos, V., Spinellis, D.: A PRoactive malware identification system based on the computer hygiene principles. Information Management and Computer Security 15(4), 295–312 (2007)
51. Weaver, N., Paxson, V., Staniford, S.: A worst-case worm. In: Proceedings of the Third Annual Workshop on Economics and Information Security (WEIS 2004) (May 2004)
52. Weaver, N., Paxson, V., Staniford, S., Cunningham, R.: Large scale malicious code: A research agenda (May 2003), http://www.cs.berkeley.edu/~nweaver/largescalemaliciouscode.pdf (June 2005)
53. Williams, P.D., Day, T.: Interactions between mortality sources and the evolution of parasite virulence. In: Proceedings of the Royal Society of London B, vol. 268, pp. 2331–2337 (2001)
54. Zelonis, K.: Avoiding the cyber pandemic: A public health approach to preventing malware propagation. Master's thesis, Carnegie Mellon University (December 2004)
55. Zou, C., Gong, W., Towsley, D.: Code red worm propagation modeling and analysis. In: Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS), Washington DC, USA (November 2002)

Information Systems Security Management: A Review and a Classification of the ISO Standards

Aggeliki Tsohou, Spyros Kokolakis, Costas Lambrinoudakis, and Stefanos Gritzalis

Dept. of Information and Communication Systems Engineering,
University of the Aegean, Samos GR-83200, Greece
{agt,sak,clam,sgritz}@aegean.gr

Abstract. The need for common understanding and agreement of functional and non-functional requirements is well known and understood by information system designers. This is necessary for both: designing the "correct" system and achieving interoperability with other systems. Security is maybe the best example of this need. If the understanding of the security requirements is not the same for all involved parties and the security mechanisms that will be implemented do not comply with some globally accepted rules and practices, then the system that will be designed will not necessarily achieve the desired security level and it will be very difficult to securely interoperate with other systems. It is therefore clear that the role and contribution of international standards to the design and implementation of security mechanisms is dominant. In this paper we provide a state of the art review on information security management standards published by the International Organization for Standardization and the International Electrotechnical Commission. Such an analysis is meaningful to security practitioners for an efficient management of information security. Moreover, the classification of the standards in the clauses of ISO/IEC 27001:2005 that results from our analysis is expected to provide assistance in dealing with the plethora of security standards.

Keywords: Information security management systems, standardization.

1 Introduction

Standardization is the process of developing and agreeing upon technical standards. A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes, or practices [1]. Standards may fall into one of the following categories: International standard (a standard adopted by an international standards organization and made available to the general public), European standard (a standard adopted by a European standards organization and made available to the general public), and National standard (a standard adopted by a national standards organization and made available to the general public) [2]. The International Organization for Standardization's (ISO) [3] standards and guides for conformity assessment represent an international consensus on best practices. Their use contributes to the consistency of conformity assessment worldwide and so facilitates trade. Joint ISO/IEC International Standards and guides for conformity assessment, encourage best practice and consistency when products, services, systems, processes and materials need to be evaluated against standards, regulations or other specifications.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 220–235, 2010.

In this paper we provide a state of the art review of standards that guide information security management and its sub-areas. Such an enlisting of information security management standards would be useful to security practitioners in order to have a clear picture of current security standardization. Also in this paper, we reduce the complexity of the plethora of security standards by revealing the interrelation among them.

The paper is organized in five sections. The following two sections are dedicated to information security management systems and information security risk management standards and the information security management specific areas' standards respectively. Section 4 presents a classification of the standards according to the ISO/IEC 27001:2005 [4] security clauses. Finally, in section 5 we highlight the limitations of this work and we provide suggestions for future work.

2 Information Security Management Systems Standards

A series of security standards define and guide the procedures of implementing information security management. Information security management is the process by which an organization aims to achieve effective confidentiality, integrity and availability of its information and services. An information security management system (ISMS) refers to that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources (ISO/IEC 27001:2005 [4]).

2.1 Concepts and Models for Information and Communications Technology (ICT) Security Management

The ISO/IEC 13335-1:2004 [5] standard is dedicated in providing government and commercial organizations' managers a high-level management overview of an overall security program for ICT systems. It focuses on concepts and models for managing the planning, implementation and operations of ICT security. The series ISO/IEC 13335 also included ISO/IEC TR 13335-2:1997 [6] that has been withdrawn and revised by the ISO/IEC 13335-1:2004 [5]. It also included the ISO/IEC 13335-3:1998 [7] and ISO/IEC 13335-4:2000 [8] that have been withdrawn and revised by ISO/IEC 27005:2008 [9] (Section 2.3). Finally, it included ISO/IEC 13335-5:2001 [10] that has been revised by ISO/IEC 18028-1:2006 [11] (see Section 3.1).

2.2 Information Security Management Systems

Overview and Vocabulary

ISO/IEC 27000:2009 [12] provides an overview of information security management systems and defines terms which are related to the overall ISMS family of standards.

Code of Practice

ISO/IEC 27002:2005 [13] is highly interrelated to ISO/IEC 27001:2005 [4], and establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It provides general guidance on the commonly accepted goals of information security management. The control objectives and controls that it proposes are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 [13] revises the well-known ISO/IEC 17799:2005 [14] standard. The structure of the best practices includes 11 control clauses that contain 39 objectives aimed by 133 controls. The 11 clauses are:

✓ Security Policy
✓ Organizing Information Security
✓ Asset Management
✓ Human Resources Security
✓ Physical and Environmental Security
✓ Communications and Operations Management
✓ Access Control
✓ Information Systems Acquisition, Development and Maintenance
✓ Information Security Incident Management
✓ Business Continuity Management
✓ Compliance

Each main clause includes one (or more) control objectives stating what is to be achieved and one or more controls that can be applied to achieve the related control objective.

Requirements

ISO/IEC 27001:2005 [4] applies to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations), regardless of type, size and nature. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. ISO/IEC 27001:2005 [4] specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. The proposed requirements are structured in a classification of 11 clauses that include 39 objectives aimed by 133 controls, as further described in the ISO/IEC 27002:2005 [13].

The standard proposes the application of a system of processes within an organization, together with the identification and interactions of these processes, and their management. Such a system is further referred to as a "*process approach*", which is structured in the circular "Plan-Do-Check-Act" (PDCA) model. The processes of "Planning" an ISMS, begin with the definition of its scope, boundaries and an ISMS policy. Continuing, a systematic approach to information security risk management is necessary (see section 2.3). Such a risk management approach is described in the standard, but specified in detail in ISO/IEC 27005:2008 [9]. In sequence, the processes of obtaining management authorization to implement and operate the ISMS and preparing a Statement of Applicability (SOA[1]) are suggested. The processes of "Doing" include the

[1] SOA is a documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

implementation of risk treatment plan (described within the ISO/IEC 27005:2008 [9]), the definition of the way the effectiveness of the selected controls will be measured, the implementation of security awareness and training programs, and also managing the operation and resources of the ISMS and implementing procedures for prompt detection of response to security events. The third phase of the PDCA model includes continual monitoring and reviewing of risks (described in ISO/IEC 27005:2008 [9]), monitoring and reviewing procedures that promptly identify attempted and successful security breaches and incidents, and errors, undertaking regular reviews of the effectiveness of the ISMS, and measure the effectiveness of controls. The final “Act” phase refers to maintaining and improving the risk management process (described in the ISO/IEC 27005:2008 [9]), and also taking the appropriate corrective and preventive actions, communicating the actions and improvements to all interested parties and ensuring that the improvements achieve their intended objectives.

Implementation Guidance

Complementary advice on ISMS implementation will be provided by the ISO/IEC FCD 27003 [15], which is under development.

Guidelines for Telecommunications Organizations Based on ISO/IEC 27002

ISO/IEC 27011:2008 [16] provides guidelines for supporting the implementation of information security management in telecommunications organizations. The adoption of these guidelines will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security properties.

Auditing

Similarly, auditing guidance for ISMSs will be provided by the ISO/IEC WD 27007 [17], which is under development.

Certification

ISO/IEC 27006:2007 [18] specifies requirements and provides guidance for bodies providing audit and certification of ISMSs. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. ISO/IEC 27006:2007 [18] strongly correlates to ISO/IEC 17021:2006 [19] which sets out criteria for bodies operating audit and certification of organizations' management systems. ISO/IEC 27006:2007 [18] is required because additional requirements and guidance to ISO/IEC 17021:2006 [19] are required for the auditing and certification of ISMSs according to ISO/IEC 27001:2005 [4].

2.3 Information Security Risk Management Standard

ISO/IEC 27005:2008 [9] provides guidelines for information security risk management and revises the former ISO/IEC 13335-3:1998 [7] and ISO/IEC 13335-4:2000 [8]. It supports the general concepts specified in ISO/IEC 27001:2005 [4] and describes a risk management approach to assist the implementation of information security. The concepts, models, processes and terminologies described in ISO/IEC 27001:2005 [4] and ISO/IEC 27002:2005 [13] are essential for the understanding of

ISO/IEC 27005:2008 [9]. ISO/IEC 27005:2008 is also applicable to all types of organizations.

Risk management process is described to include the activities of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review. Context establishment involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the information security risk management. Risk assessment involves the identification, description of risks (quantitatively or qualitatively), and prioritization of risks against risk evaluation criteria and objectives. Risk treatment contains the selection of controls to reduce, retain, avoid, or transfer the risks and the definition of a risk treatment plan. Risk acceptance includes the decision to accept the risks and the recording of accepted risks with justification for those that do not meet the organization's normal risk acceptance criteria (e.g. because the cost of risk reduction is too high). Risk communication refers to the exchange and sharing of information about risk between the decision-maker and other stakeholders. Finally, risk monitoring and review includes the monitoring of risks and their factors (i.e. value of assets, impacts) and their reviewing in case of any changes in the context of the organization.

3 Information Security Management Specific Areas' Standards

3.1 Network Security Management

ISO/IEC 18028 series include five standards that provide guidance for network security management. The series ISO/IEC 18028 will be revised by the upcoming ISO/IEC 27033. ISO/IEC 18028-1:2006 [11] provides detailed guidance on the security aspects of the management, operation and use of Information Technology (IT) networks, and their interconnections. To do so, it defines and describes the concepts associated with, and provides management guidance on, network security. Its audience includes anyone who owns, operates or uses a network. The standard will be revised by the upcoming ISO/IEC FCD 27033-1 [20]. ISO/IEC 18028-2:2006 [21], serves as a foundation for developing the detailed recommendations for end-to-end network security. The standard will be revised by ISO/IEC WD 27033-2 [22]. ISO/IEC 18028-3:2005 [23] outlines the techniques for security gateways to analyze network traffic. The techniques discussed are packet filtering, stateful packet inspection, application proxy, network address translation, content analyzing and filtering. Also, provides guidelines for the selection and configuration of security gateways. It will be revised by ISO/IEC NP 27033-4 [24]. The fourth part provides guidance for securely using remote access and its implication for IT security. It introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely. ISO/IEC 18028-4:2005 [25] will be revised by ISO/IEC NP 27033-5 [26]. The final part provides detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. It defines techniques for securing inter-network connections that are established using virtual private networks (VPNs). ISO/IEC 18028-5:2006 [27] will be revised by the ISO/IEC NP 27033-6 [28]. Additionally, the series ISO/IEC 27033 will include ISO/IEC WD 27033-3 [29].

Intrusion Detection Systems

ISO/IEC 18043:2006 [30] provides guidance for including an intrusion detection capability within an organizations' IT infrastructure. ISO/IEC 18043:2006 [30] provides a brief overview of the intrusion detection process, discusses the benefits and limitations of an intrusion detection system, and provides a checklist that helps identify the best features for a specific IT environment, describes various deployment strategies, provides guidance on managing alerts and discusses management and legal considerations.

3.2 Auditing

Guidelines

As already mentioned in section 2.2, auditing guidelines for ISMSs will be provided ISO/IEC WD 27007.

Time-Stamping Services

ISO/IEC 18014 series specify time-stamping techniques. It consists of three parts, which include the general notion, models for a time-stamping service, data structures, and protocols. ISO/IEC 18014-1:2008 [31] describes a framework and defines the basic notion, the data structures, and protocols which are used for any time-stamping technique. It identifies the objective of a time-stamping authority, describes a general model on which time-stamping services are based, describes a process of generating and verifying time-stamp, defines the data structures of time-stamp token, defines the basic protocols of time-stamping and specifies the protocols between the involved entities. ISO/IEC 18014-2:2002 [32] describes time-stamping services producing independent tokens, time-stamps using digital signatures, message authentication codes and archiving. ISO/IEC 18014-3:2004 [33] describes time-stamping services producing linked tokens, that is, tokens that are cryptographically bound to other tokens produced by these time-stamping services.

3.3 Trusted Third Parties (TTPs)

ISO/IEC TR 14516:2002 [34] provides guidance for the use and management of TTPs, a clear definition of the basic duties and services provided their description and their purpose, and the roles and liabilities of TTPs and entities using their services. ISO/IEC TR 14516:2002 [34] identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public. The guidance for TTP services to support the application of digital signatures is provided by ISO/IEC 15945:2002 [35].

3.4 Incident Management

ISO/IEC TR 18044:2004 [65] does not possess the status of an International Standard, but rather it is published as a Technical Report. Technical reports can either be transformed into International Standards after being reviewed within three years of publication or are normally published as an International Standard until the data they provide are considered to be no longer valid or useful. The report is interrelated with the ISO/IEC 13335-1:2004 [5] and ISO/IEC 27002:2005 [13].

ISO/IEC TR 18044:2004 [65] provides advice and guidance on information security incident management for information security managers, and information system, service and network managers. After security controls and policies have been implemented, residual weaknesses are likely to remain. Residual weaknesses, together with the occurrence of new previously unidentified threats, make information security incidents possible. Information security incident management proposed by the technical report consists of processes structured in a model of four phases: Plan and Prepare, Use, Review, and Improve. "Plan and Prepare" includes the actions of developing, documenting and communicating an information security incident management policy, developing and documenting an information security incident management scheme (forms, procedures and support tools, for the detection, reporting, assessment and response to incidents), establishing an appropriate information security incident management organizational structure, and performing personnel training. "Use" refers to detecting, reporting the occurrence of information security events and evaluate their significance, making responses to the information security incidents. The "Review" step includes forensic analysis, identifying the lessons learnt from information security incidents, and identifying improvements. Finally, in the "Improve" phase improvements are realized and the organization's existing information security risk analysis and management review results are revised.

3.5 Business Continuity

Guidelines for Information and Communications Technology Disaster Recovery Services

ISO/IEC 24762:2008 [66] guides the provision of information and communications technology disaster recovery services as part of business continuity management. Business continuity management is an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand and value. It includes activities which identify potential threats that may cause adverse impacts on an organization's business operations, and associated risks, providing a framework for building resilience for business operations, providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures. The standard is interrelated with the ISO/IEC 27001:2005 [4] and ISO/IEC 27002:2005 [13].

ISO/IEC 24762:2008 [66] provides guidelines for both in-house and outsourced disaster recovery services. The guidelines are divides into two areas: disaster recovery guidelines and disaster recovery facilities. Disaster recovery guidelines include issues of environmental stability, asset management and protection, proximity of sites, vendor management, contractual agreements, activation and deactivation of disaster recovery plan, training and education etc. Disaster recovery facilities refer to the basic requirements that need to be fulfilled by disaster recovery service providers so that they can provide secure physical operating environments to facilitate organization recovery efforts. These include location of recovery sites (taking into account accessibility, natural hazards, weather changes etc.) physical access controls, physical facility security, environmental controls, telecommunications, power supply, fire protection etc.

3.6 Non-repudiation

ISO/IEC 13888-1:2004 [67] serves as a general model for subsequent parts of the series ISO/IEC 13888 by specifying non-repudiation mechanisms using cryptographic techniques. The goal of the non-repudiation service is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. There are two main types of evidence, the nature of which depends on cryptographic techniques employed: a) the secure envelopes generated by an evidence-generating authority using symmetric cryptographic techniques, and b) the digital signatures generated by an evidence generator or an evidence generating authority using asymmetric cryptographic techniques. ISO/IEC 13888-2:1998 [68] and ISO/IEC 13888-3:1997 [69] provide non-repudiation mechanisms for the following phases of non-repudiation: evidence generation, transfer, storage, retrieval and verification. The non-repudiation mechanisms are then applied to a selection of specific non-repudiation services such as non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport.

3.7 Digital Signatures

Two types of digital signature mechanisms exist: a) signature mechanism with appendix and b) signature mechanism giving message recovery. In the first case the verification process needs the message as part of the input. A hash-function is used in the calculation of the appendix. In the second case the verification process reveals all or part of the message. A hash-function is also used in the generation and verification of these signatures.

ISO/IEC 14888 series specify digital signatures with appendix. ISO/IEC 14888-1:2008 [36] specifies general principles and requirements for digital signatures with appendix. ISO/IEC 14888-2:2008 [37] addresses digital signatures based on integer factoring, and ISO/IEC 14888-3:2006 [38] addresses digital signatures based on discrete logarithm. ISO/IEC 9796-2:2002 [39] specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. Also specifies a method for key production for the three signature schemes. A complementary Annex has been provided by the ISO/IEC 9796-2:2002/Amd 1:2008 that provides an additional ASN.1 module. Finally, ISO/IEC 9796-3:2006 [40] gives the general model for digital signatures giving partial or total message recovery aiming at reducing storage and transmission overhead. It also, defines types of redundancy: natural redundancy, added redundancy, or both. ISO/IEC 9796-1:1991 [41] has been withdrawn.

3.8 Access Control

ISO/IEC 15816:2002 [42] defines guidelines for specifying the abstract syntax of generic and specific Security Information Objects (SIOs) for Access Control, specifying generic SIOs for Access Control and defining specific SIOs for Access Control.

Entity Authentication

ISO/IEC 9798-1:1997 [43] specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a TTP. The subsequent five parts ISO/IEC 9798-2:2008 [44], ISO/IEC 9798-3:1998 [45], ISO/IEC 9798-4:1999 [46], ISO/IEC 9798-5:2004 [47] and ISO/IEC 9798-6:2005 [48] provide details of the mechanisms and the contents of the authentication exchanges.

3.9 Cryptographic Controls

Encryption Algorithms

ISO/IEC 18033 series specify encryption systems (ciphers). ISO/IEC 18033-1:2005 [49] specifies terms and definitions used throughout all parts of ISO/IEC 18033, the purpose of encryption, the differences between symmetric and asymmetric ciphers, and the key management problems associated with the use of ciphers, the uses and properties of encryption, and criteria for the inclusion of encryption algorithms in ISO/IEC 18033. ISO/IEC 18033-2:2006 [50] specifies the functional interface of an asymmetric (i.e. public-key) encryption scheme, and a number of particular schemes considered to be secure against chosen ciphertext attack. ISO/IEC 18033-3:2005 [51], along with its amendments ISO/IEC 18033-3:2005/Cor 1:2006, ISO/IEC 18033-3:2005/Cor 2:2007 and ISO/IEC 18033-3:2005/Cor 3:2008, specify block ciphers. Finally, ISO/IEC 18033-4:2005 [52] specifies stream cipher algorithms.

Key Management

The series ISO/IEC 11770 consists of three parts dedicated to key management of cryptographic controls. ISO/IEC 11770-1:1996 [53] defines a general model of key management that is independent of the use of any particular cryptographic algorithm. It identifies the objective of key management, basic concepts and key management services. It will be soon revised by a homonym standard (ISO/IEC CD 11770-1 [54]). ISO/IEC 11770-2:2008 [55] specifies a series of 13 mechanisms for establishing shared secret keys using symmetric cryptography. These mechanisms address three different environments for the establishment of shared secret keys: point-to-point key establishment schemes, mechanisms using a Key Distribution Centre (KDC), and techniques that use a Key Translation Centre (KTC). ISO/IEC 11770-3:2008 [56] defines key management mechanisms based on asymmetric cryptographic techniques. ISO/IEC 11770-4:2006 [57] defines key establishment mechanisms based on weak secrets. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing off-line brute-force attacks associated with the weak secret.

Message Authentication Codes (MACs)

ISO/IEC 9797-1:1999 [58] specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC. ISO/IEC 9797-2:2002 [59] specifies three MAC algorithms that use a secret key and a hash-function (or its round-function) with an n-bit result to calculate an m-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The standards will be soon revised by homonym standards (ISO/IEC FCD 9797-1, ISO/IEC FCD 9797-2).

Hash Functions

ISO/IEC 10118 series specify hash-functions that are applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map arbitrary strings of bits to a fixed-length string of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, and for committing the user to a given string of bits without revealing this string. ISO/IEC 10118-1:2000 [60] contains definitions, symbols, abbreviations and requirements, which are common to all the other parts of ISO/IEC 10118. ISO/IEC 10118-2:2000 [61], along with its amendment ISO/IEC 10118-2:2000/Cor 2:2007, specifies hash-functions which make use of an n-bit block cipher algorithm; therefore they are suitable for an environment in which such an algorithm is already implemented. This standard is also under revision (ISO/IEC CD 10118-2). ISO/IEC 10118-3:2004 [62] specifies seven dedicated hash-functions, e.g. RIPEMD-160 that provides hash-codes of lengths up to 160 bits. Finally, ISO/IEC 10118-4:1998 [63] specifies two hash-functions which make use of modular arithmetic.

3.10 Systems Security Engineering

ISO/IEC 21827:2008 [64] specifies the Systems Security Engineering - Capability Maturity Model, which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.

3.11 Assurance and Evaluation

Evaluation Criteria for IT Security

This multipart standard ISO/IEC 15408 defines criteria, which are known as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. The CC is applicable to IT security measures implemented in hardware, firmware or software.

ISO/IEC FCD 15408-1.3 [71] is under development and will revise the ISO/IEC 15408-1:2005 [72]. That part of the ISO/IEC 15408 defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. ISO/IEC 15408-2:2008 [73] defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products. ISO/IEC 15408-3:2008 [74] defines the assurance requirements of the standard. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).

ISO/IEC TR 19791:2006 [75] provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation.

Methodology for IT Security Evaluation

ISO/IEC 18045:2008 [70] is a companion document to the evaluation criteria for IT security defined in ISO/IEC 15408. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation. The proposed evaluation process consists of the roles and responsibilities of the parties involved and the general evaluation model. The general roles involved are the sponsor, the developer, the evaluator and the evaluation authority. The general evaluation model consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities. The evaluation input task ensures that the evaluator has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. The evaluation output task refers to the documentation of the Observation Report[2] and the Evaluation Technical Report[3]. The evaluation sub-activities vary depending whether it is a Protection Profile (PP) or a Target of Evaluation (TOE) evaluation.

Assurance

ISO/IEC TR 15443 is also a technical report to guide the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel. ISO/IEC TR 15443-1:2005 [76] describes the fundamentals of security assurance and its relation to other security concepts. It is under revision (ISO/IEC NP TR 15443-1). ISO/IEC TR 15443-2:2005 [77] describes a variety of IT security assurance methods and approaches and relates them to the IT security assurance framework in ISO/IEC TR 15443-1 [76]. It is under revision (ISO/IEC NP TR 15443-2). ISO/IEC TR 15443-3:2007 [77] provides general guidance to an assurance authority in the choice of the appropriate type of international communications technology assurance methods and to lay the framework for the analysis of specific assurance methods for specific environments. It will be revised by ISO/IEC NP TR 15443-3.

4 Classification of Information Security Management Standards

In this section we classify the various information security management specific areas standards, described in the previous sections, according to the clauses of ISO/IEC

[2] A report written by the evaluator requesting a clarification or identifying a problem during the evaluation.

[3] A report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority.

27001:2005 [4]. Such a categorization would enhance the application of information security management code of practice and would facilitate security managers aiming at conformance assessment.

Table 1. Information Security Management standards' classification

Areas of concern (based on ISO 27002: 2005)	**Published standards or series of standards**	**Standards under development**	**Will be revised by**
ISMSs	Series ISO/IEC 27000 ISO/IEC 13335-1:2004	ISO/IEC CD 27003 ISO/IEC WD 27007	
Security Policy	ISO 27002: 2005		
Organizing Information Security	ISO 27002: 2005 ISO/IEC TR 14516:2002 ISO/IEC 15945:2002		
Asset Management	ISO 27002: 2005		
Human Resources Security	ISO 27002: 2005		
Physical and Environmental Security	ISO 27002: 2005		
Communications and Operations Management	Series ISO/IEC 18028	ISO/IEC WD 27007	Series ISO/IEC 27033
	Series ISO/IEC 18014		
	ISO/IEC 18043:2006		
	ISO/IEC TR 14516:2002		
	ISO/IEC 15945:2002		
Access Control	ISO/IEC 15816:2002		
	Series ISO/IEC 9798		
Information Systems Acquisition, Development and Maintenance	Series ISO/IEC 11770		ISO/IEC CD 11770-1
	Series ISO/IEC 14888		
	Series ISO/IEC 9796		
	Series ISO/IEC 18033		
	Series ISO/IEC 9797		ISO/IEC FCD 9797-1 ISO/IEC FCD 9797-2
	Series ISO/IEC 10118		ISO/IEC CD 10118-2
	ISO/IEC 21827:2008		
	Series ISO/IEC 13888		
Information Security Incident Management	ISO/IEC TR 18044:2004		
Business Continuity Management	ISO/IEC 24762:2008		
	ISO/IEC 18045:2008		
	Series ISO/IEC 15408		ISO/IEC FCD 15408-1.3
	ISO/IEC TR 19791:2006		
	Series ISO/IEC TR 15443		ISO/IEC NP TR 15443-1 ISO/IEC NP TR 15443-2 ISO/IEC NP TR 15443-3
Compliance		ISO/IEC WD 27007	

5 Limitations and Further Research

In this paper we provided a state of the art review of exclusively ISO/IEC information security management published standards. The accuracy of the information provided in the paper is connected to the pace of standards' publications. However, this paper gives a structure of the international standards that shall guide managers in their attempt to follow the standards' advancements. In addition, we have included in our description several fore coming revisions and publications in order to assist security practitioners to keep pace with standards' validity. Finally, we should mention that other sub-areas of information security management are guided by national standardization organizations, such as NIST. The next step would be to extend our analysis, including such publications.

References

1. Standardization definition, `http://en.wikipedia.org/wiki/Standardization`
2. Guijarro, L.: ICT standardisation and public procurement in the United States and in the European Union: Influence on egovernment deployment. Telecommunications Policy 33(5-6), 285–295 (2009)
3. International Organization for Standardization, `http://www.iso.org/iso/home.htm`
4. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements (2005)
5. ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (2004)
6. ISO/IEC TR 13335-2:1997. Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security (1997)
7. ISO/IEC TR 13335-3:1998. Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security (1998)
8. ISO/IEC TR 13335-4:2000. Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards (2000)
9. ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management (2008)
10. ISO/IEC TR 13335-5:2001. Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security (2001)
11. ISO/IEC 18028-1:2006. Information technology – Security techniques – IT network security – Part 1: Network security management (2006)
12. ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary (2009)
13. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management (2005)
14. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management (2005)
15. ISO/IEC FCD 27003. Information technology – Security techniques – Information security management system implementation guidance

16. ISO/IEC 27011:2008. Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (2008)
17. ISO/IEC WD 27007. Information technology – Security techniques – Guidelines for information security management systems auditing
18. ISO/IEC 27006:2007. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems (2007)
19. ISO/IEC 17021:2006. Conformity assessment – Requirements for bodies providing audit and certification of management systems (2006)
20. ISO/IEC FCD 27033-1. Information technology – Security techniques – IT network security – Part 1: Guidelines for network security
21. ISO/IEC 18028-2:2006. Information technology – Security techniques – IT network security – Part 2: Network security architecture (2006)
22. ISO/IEC WD 27033-2. Information technology – Security techniques – IT network security – Part 2: Guidelines for the design and implementation of network security
23. ISO/IEC 18028-3:2005. Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways (2005)
24. ISO/IEC NP 27033-4. Information technology – Security techniques – IT network security – Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues
25. ISO/IEC 18028-4:2005. Information technology – Security techniques – IT network security – Part 4: Securing remote access (2005)
26. ISO/IEC NP 27033-5. Information technology – Security techniques – IT network security – Part 5: Securing Remote Access - Risks, design techniques and control issues
27. ISO/IEC 18028-5:2006. Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks (2006)
28. ISO/IEC NP 27033-6. Information technology – Security techniques – IT network security – Part 6: Securing communications across networks using Virtual Private Networks (VPNs) – Risks, design techniques and control issues
29. ISO/IEC WD 27033-3. Information technology – Security techniques – IT network security – Part 3: Reference networking scenarios – Risks, design techniques and control issues
30. ISO/IEC 18043:2006. Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (2006)
31. ISO/IEC 18014-1:2008. Information technology – Security techniques – Time-stamping services – Part 1: Framework (2008)
32. ISO/IEC 18014-2:2002. Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens (2002)
33. ISO/IEC 18014-3:2004. Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens (2004)
34. ISO/IEC TR 14516:2002. Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services (2002)
35. ISO/IEC 15945:2002. Information technology – Security techniques – Specification of TTP services to support the application of digital signatures (2002)
36. ISO/IEC 14888-1:2008. Information technology – Security techniques – Digital signatures with appendix – Part 1: General (2008)
37. ISO/IEC 14888-2:2008. Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms (2008)

38. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms (2006)
39. ISO/IEC 9796-2:2002. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms (2002)
40. ISO/IEC 9796-3:2006. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms (2006)
41. ISO/IEC 9796-1:1991, Information technology–Security techniques–Digital signature scheme giving message recovery –Part 1: Mechanisms using redundancy (1991)
42. ISO/IEC 15816:2002. Information technology – Security techniques – Security information objects for access control (2002)
43. ISO/IEC 9798-1:1997. Information technology – Security techniques – Entity authentication – Part 1: General (1997)
44. ISO/IEC 9798-2:2008. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms (2008)
45. ISO/IEC 9798-3:1998. Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques (1998)
46. ISO/IEC 9798-4:1999. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function (1999)
47. ISO/IEC 9798-5:2004. Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques (2004)
48. ISO/IEC 9798-6:2005. Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer (2005)
49. ISO/IEC 18033-1:2005. Information technology – Security techniques – Encryption algorithms – Part 1: General (2005)
50. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers (2006)
51. ISO/IEC 18033-3:2005. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers (2005)
52. ISO/IEC 18033-4:2005. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers (2005)
53. ISO/IEC 11770-1:1996. Information technology – Security techniques – Key management – Part 1: Framework (1996)
54. ISO/IEC CD 11770-1.Information technology – Security techniques – Key management – Part 1: Framework
55. ISO/IEC 11770-2:2008. Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques (2008)
56. ISO/IEC 11770-3:2008. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques (2008)
57. ISO/IEC 11770-4:2006. Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets (2006)
58. ISO/IEC 9797-1:1999. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher (1999)
59. ISO/IEC 9797-2:2002. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function (2002)
60. ISO/IEC 10118-1:2000. Information technology – Security techniques – Hash-functions – Part 1: General (2000)
61. ISO/IEC 10118-2:2000. Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher (2000)

62. ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions (2004)
63. ISO/IEC 10118-4:1998. Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic (1998)
64. ISO/IEC 21827:2008. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®) (2008)
65. ISO/IEC TR 18044:2004. Information technology – Security techniques – Information security incident management (2004)
66. ISO/IEC 24762:2008. Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services (2008)
67. ISO/IEC 13888-1:2004. IT security techniques – Non-repudiation – Part 1: General (2004)
68. ISO/IEC 13888-2:1998. Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques (1998)
69. ISO/IEC 13888-3:1997. Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques (1997)
70. ISO/IEC 18045:2008. Information technology – Security techniques – Methodology for IT security evaluation (2008)
71. ISO/IEC FCD 15408-1.3. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
72. ISO/IEC 15408-1:2005. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (2005)
73. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components (2008)
74. ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components (2008)
75. ISO/IEC TR 19791:2006. Information technology – Security techniques – Security assessment of operational systems (2006)
76. ISO/IEC TR 15443-1:2005. Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework (2005)
77. ISO/IEC TR 15443-2:2005. Information technology – Security techniques – A framework for IT security assurance – Part 2: Assurance methods (2005)
78. ISO/IEC TR 15443-3:2007. Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods (2007)

Web Server Security on Open Source Environments

Dimitrios X. Gkoutzelis[1] and Manolis S. Sardis[2]

[1] University of the Aegean, Samos, Greece
icsd04126@icsd.aegean.gr
[2] National Technical University of Athens - NTUA, Athens, Greece
sardis@telecom.ntua.gr

Abstract. Administering critical resources has never been more difficult that it is today. In a changing world of software innovation where major changes occur on a daily basis, it is crucial for the webmasters and server administrators to shield their data against an unknown arsenal of attacks in the hands of their attackers. Up until now this kind of defense was a privilege of the few, out-budgeted and low cost solutions let the defender vulnerable to the uprising of innovating attacking methods. Luckily, the digital revolution of the past decade left its mark, changing the way we face security forever: open source infrastructure today covers all the prerequisites for a secure web environment in a way we could never imagine fifteen years ago. Online security of large corporations, military and government bodies is more and more handled by open source application thus driving the technological trend of the 21st century in adopting open solutions to E-Commerce and privacy issues. This paper describes substantial security precautions in facing privacy and authentication issues in a totally open source web environment. Our goal is to state and face the most known problems in data handling and consequently propose the most appealing techniques to face these challenges through an open solution.

Keywords: Open Source, Security Practices, Authentication Management.

1 Introduction

In today's electronic world thousands of application layer software is being designed and shared throughout the Open Source (OS) communities. Utilized solely by volunteering work which produces pioneering outcome when combined with world wide projects sharing resources and human personnel, projects in this area often win the trust of the vast majorities of website developers and website owners with its easy-to-use and free of charge benefits [1], [2], [38]. But do those solutions come with a security-cost or not [3], [36]?

This work examines the ways in which the new trend in global programming produces solutions from non commercial products in an absolutely secure and safe way - compared to close source. It is common logic to assume that when it comes to data security and handling sensitive transactions it is not always a clever idea to have your code open, or even worse, shared with millions of people. Today, people are able to get educated, trained and specialized in certain programming areas of their likes without the

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 236–247, 2010.

need to pay for extra education fees or joining a closed group of professionals. Writing open source software has enabled thousands of people to look closely at professionally-written code, learn the ropes of advanced software engineering methods and in that way excel the way we read, write and understand code to our own advantage. It would certainly not be an exaggeration to state that the open source movement has influenced the security of modern networks and large computing compounds. One of the most well known examples is the LAMP (Linux, Apache, MySQL and PHP) architecture used to minimize security risks and provide a totally open source solution to handling security on your web server [4]. LAMP software consists of the main tools security professionals most commonly use for business systems.

A recent survey [5] performed by Netcraft, a data collection and analysis of hosting companies organization, showed that 46,35% of the servers on the market use Apache as their web server software leaving the second position to Microsoft with 29,47%. What is more worth mentioning is that on the survey on the 1 million busiest servers in the world that percentage reaches 66,6% leaving IIS (Internet Information Server) with a 18,6% (Fig. 1).

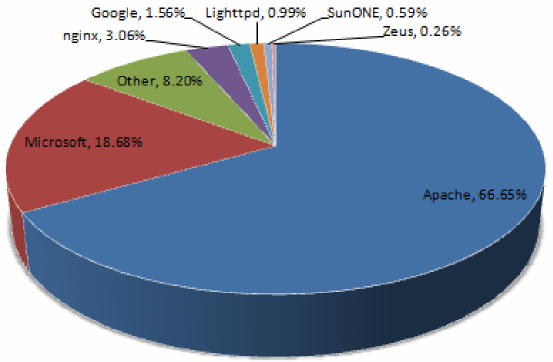


Fig. 1. Server Share amongst the Million Busiest Sites (March 2009)

This paper analyzes separately each of the main problems a server administrator has to address, when facing security issues and special care will be given on the meaning of open source tools to aid that goal. The paper is composed of three parts. In the first we present the basic ground of server security measures that every administrator should start with. The second part contains a new approach in how we face security with some advanced practices that have begun to gain administrators trust around the world. In the third and final part, the future work in the field of security is described and the limits that still need to be crossed in order to maximize efficiency.

2 Facing Security Issues on the Front Line

When talking about security over the Internet, from an administrator's point of view, there are really a lot to talk about. In this section we analyze the most crucial techniques to be established by a web server administrator to protect the box from the most common and popular attacks.

2.1 File Permissions

Every folder or directory our website contains has its own permissions. Those permissions are defining who is allowed to do what on our files. On Unix-based operating systems there are three kind of permissions: read-write-execute and three kind of owners: owner-group=other. Permissions are set by using a three-digit number: for example with 000 being the most restricting as it takes away all rights on the file and with 777 being the most liberal as it provides all permissions to all groups. The first digit represents what is allowed to be done by the owner of the file, the second represents what the rest authorized users can do and the third everybody else's permissions on it. The command with which we change or set the permissions of a file is chmod. To keep balance between usability and security all directories should be set to 755 and all files to 644 unless a certain file has specific configuration that demand otherwise [7].

It is a spread and good practice to keep the files and directories non-writable in the extent that it is possible for the normal function and to make them writable only in the need of significant content-changing such as configuration files or where manual editing is the only choice available. What should drive our actions is the Least Privilege Approach: if someone has no reason to have access to a specific resource or to able to perform a certain action on it then he should be banned from doing, or in a more polite rephrase "one should only be able to do what he is needed to do and nothing else". All the typical recommendations, to set any files on status 777, are given by people who have no concern about security or at least it is not their first priority and should be avoided at all costs. One other thing to be considered is to avoid setting as server-writable files under the document root. A large percentage of the attacks occurring in small websites are caused because the web server could write under the document root, so all an attacker had to do was to upload a php script which he called through his/her browser.

2.2 Shielding Your Server with SSL

First and foremost when talking about building something secure is to keep the administrator's keys to a safe place. If fallen to the wrong hands then all efforts about security go down the gutter. All user data should be handled exclusively through SSL (TLS) [8], a technology that is used to encrypt the data over the channel you sent it on Internet to avoid eavesdropping, tampering or message forging and your user's data to end up on the wrong hands. TLS runs on many layers below protocol layer such as:

- HTTP (Hypertext Transfer Protocol): which could be used for application users' login through HTTPS (http secure).
- FTP (File Transfer Protocol): in order to secure file transfer procedures through SFTP mechanisms.
- SMTP (Simple Mail Transfer Protocol): for your email accounts protection.

Today all the algorithms and libraries required for those cryptographic protocols to work are open and unified under the OpenSSL [6] project which is an open source implementation of the SSL and TLS protocols. The core library implements the basic cryptographic functions and provides various utility functions.

2.2.1 How It Works

The client and the server to be contacted negotiate a connection by using a handshaking procedure (Fig. 2). In the meaning of handshaking we mean the agreement on using certain parameters as common in order to establish the connection's security.

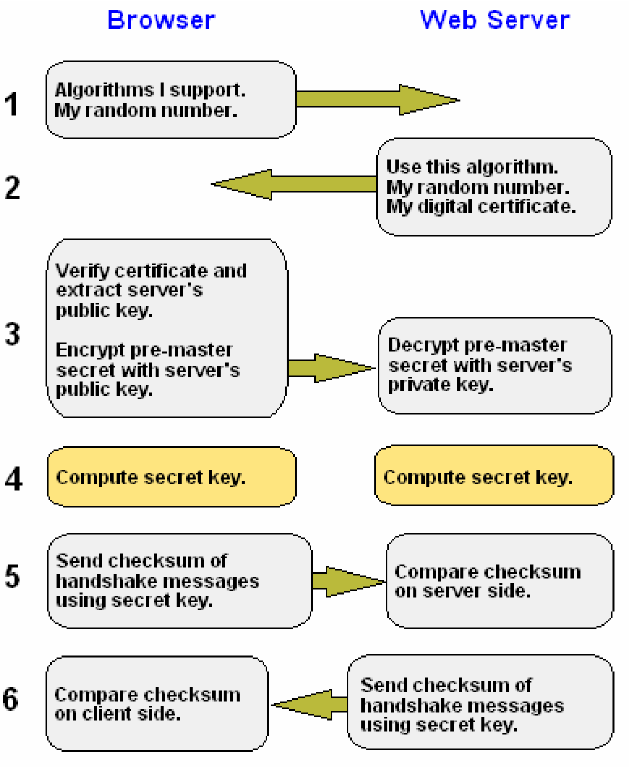

Browser
Web Server
1
Algorithms I support. My random number.
2
Use this algorithm. My random number. My digital certificate.
3
Verify certificate and extract server's public key.
Encrypt pre-master secret with server's public key.
Decrypt pre-master secret with server's private key.
4
Compute secret key.
Compute secret key.
5
Send checksum of handshake messages using secret key.
Compare checksum on server side.
6
Compare checksum on client side.
Send checksum of handshake messages using secret key.

Fig. 2. Description of the TLS handshaking

The procedure is initiated by the client's request to connect to a TLS-enabled web server after it presents it to a list of supported ciphers and hash functions. In turn, the server picks the strongest ones that it also supports and sends a message to the client about his decisions in the form of a digital certificate which usually holds valuable information such as the server's name, trusted certificate authority, and the server's public key.

In cases of strict security measures, the client will contact that authority to verify the validity of the server's before it establishes a connection. After the validation, the client encrypts a random number with the server's public key and sends it to the server to be decrypted with its private key.

2.2.2 Advantages of Using SSL

The success of SSL in e-commerce is a testament to the advantages of the technology. Using the common web browser as the primary client software, simplifies support requirements by eliminating the need for additional software applications. Authentication of the target SSL Web server is transparent to the end user and is fairly reliable.

Encryption algorithms have evolved with the technology to provide a high level of security with the availability of 256-bit and higher keys. Authentication with SSL is achieved with the identification of the server by the client via a Digital Certificate that is issued and signed by a Certificate Authority (CA) and stored on the server. Identification and authentication of the client accessing the server, although possible, is not practical for the purposes of e-commerce since the vast percentage of clients do not have Digital Certificates that are signed by a registered CA. Without a certificate signed by a CA, reliable identification of the client to the server is not possible. This can lead to a situation where an anonymous client on the Internet can connect to the SSL server, establish an encrypted session and then use this session as a secure channel for attacking the specific Web server associated with the session. The encrypted SSL connection has traditionally prohibited network security, or management personnel from inspecting the contents of the session prior to its termination at the SSL concentrator, or the Web Server that terminates the SSL session.

2.3 Logging Critical Information

If the server is unrecoverable, remote logs allow to see what happened prior to the crash, even without the system running. If the crash is related to an intrusion, any information that can describe how the system was compromised can help determine the cause of the problem. Because of the importance of the log files to the administrator's duties, the location of those files should not be adjacent to the logged system. A very common approach is to use a remote logging server with tight security, where the logs can be kept safe from crashes or attacks to our system.

One of the main logging tools on every Linux distribution is *syslogd*, which is very easy to configure and use. Different software stores its logs to different places, for example with Apache [9] you set where you store your logs through *httpd.conf* and if we use Red Hat [10] the *httpd.conf* is usually stored in */etc/httpd/conf/httpd.conf*.

There are countless tools and applications out there today that enable detailed and user-defined logging [11] of all actions and data that are characterized as important for the system. A good system is one that keeps track of all actions performed so as to revive in case of a disaster [12].

2.4 Password Management and Backups

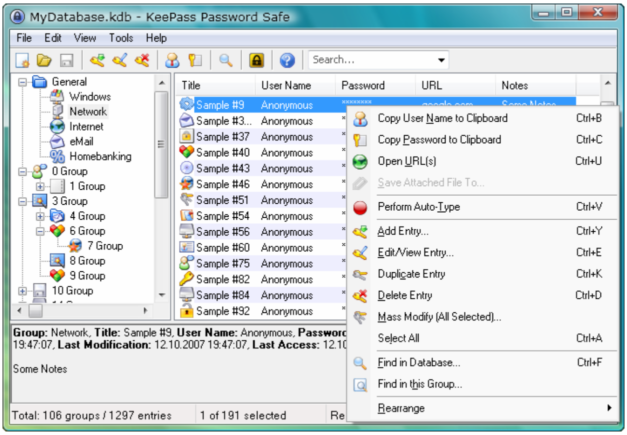
2.4.1 Passwords

Due to cost and compatibility with legacy systems, the most popular form of user authentication continues to be a secret password. Passwords are simply secret words, or at best secret phrases. They can be compromised in many ways:

- Users may write them down or share them, so that they are no longer really secret.
- Passwords can be guessed, either by a person or a program designed to quickly try many possibilities.
- Passwords may be transmitted over a network either in plaintext, or encoded in a way which can be readily converted back to plaintext.
- Passwords may be stored on a workstation, server or backup media in plaintext, or encoded in a way which can be readily converted back to plaintext.

Users in a large organization frequently have many passwords, each protecting their access to a different computer system. Users have some basic limitations, which limit what can be done in the context of secure password management. One of the primary weaknesses of passwords is that they may be guessed. While a human may give up after trying guessing ten or a hundred possible passwords, software will happily try millions of combinations. To combat password guessing attack, users should pick hard-to-guess passwords. One way to do this is to ensure that the set of all possible passwords is too large to search thoroughly, and then to eliminate probably guesses.

To limit the usefulness of passwords that have been compromised, a best practice is to change them regularly.



Title	User Name	Password	URL	Notes
Sample #9	Anonymous	********	google.com	Some Notes
Sample #3...	Anonymous	*		
Sample #37	Anonymous	*		
Sample #40	Anonymous	*		
Sample #43	Anonymous	*		
Sample #46	Anonymous	*		
Sample #51	Anonymous	*		
Sample #54	Anonymous	*		
Sample #56	Anonymous	*		
Sample #60	Anonymous	*		
Sample #75	Anonymous	*		
Sample #82	Anonymous	*		
Sample #84	Anonymous	*		
Sample #92	Anonymous	*		

Group: Network, **Title:** Sample #9, **User Name:** Anonymous, **Passworc**
19:47:07, **Last Modification:** 12.10.2007 19:47:07, **Last Access:** 12.10

Some Notes

Total: 106 groups / 1297 entries 1 of 191 selected Re

Fig. 3. Open Source Password Manager for multi user environments (KeePass [39])

A common rule on many systems is to force users to change their passwords when they log in, if they have not been changed for an extended period (e.g., 60 or 90 days). In general, users should be required to change their passwords regularly, at most every 90 days, and preferably more frequently. For the same reasons, users should not reuse old passwords, as they may already have been compromised. Many systems support this (Fig. 3) by recording some representation of old passwords, and ensuring that users cannot change their password back to a previously used value.

2.4.2 Backups

In an information environment, an organization's success is tightly coupled to its ability to store and manage information. Storage systems provide a critical part of an organization's network infrastructure. With the amount of data growing at an incredible rate, your storage strategy must keep pace. In designing a storage strategy for your organization, you must select the right technology for your primary storage system, implement solid backup procedures and ensure ongoing management of the system.

When you start thinking of backing up the data, first thing comes to be considered is what data to backup and how much storage is available for the backup to take place. This depends on what data is important. So before backing up your data, the capacity of your data places an important role, identifying the capacity of the backup medium to the quantity of data you propose to backup is very important. An optimized solution is to maintain storage devices able to store a mirror copy of your server's data so as not to make any cutbacks on the amount to be rescued in case of a disaster.

2.5 VPN Usage for Extra Security

A Virtual Private network (VPN) is a network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. A well-designed VPN uses several methods for keeping your connection and data secure (Fig. 4):

- Firewalls
- Encryption
- IPSec
- AAA Server

A firewall provides a strong barrier between a private network and the Internet. We can set firewalls to restrict the number of open ports, what type of packets are passing through and which protocols are allowed through. We should already have a good firewall in place before we implement a VPN, but a firewall can also be used to terminate the VPN sessions.

Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption [14] each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer.
- Public-key encryption [15] uses a combination of a private key and a public key. The private key is known only to our computer, while the public key is given by our computer to any computer that wants to communicate securely.

Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication. IPSec has two encryption modes: tunnel and transport. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload.

AAA (authentication, authorization and accounting) servers are used for more secure access in a remote-access VPN environment. When a request to establish a session comes in from a dial-up client, the request is proxied to the AAA server. AAA then checks the authentication, the authorization and the accounting. By effectively administering the server through a VPN network and granting access to the users only through it, we maximize security precautions. As it adds an extra layer of protection on the server and the data, a VPN installation deters hackers from performing an assault on the network. It is today a very well known practice to use VPN as an extra layer of security in many large corporations [35].

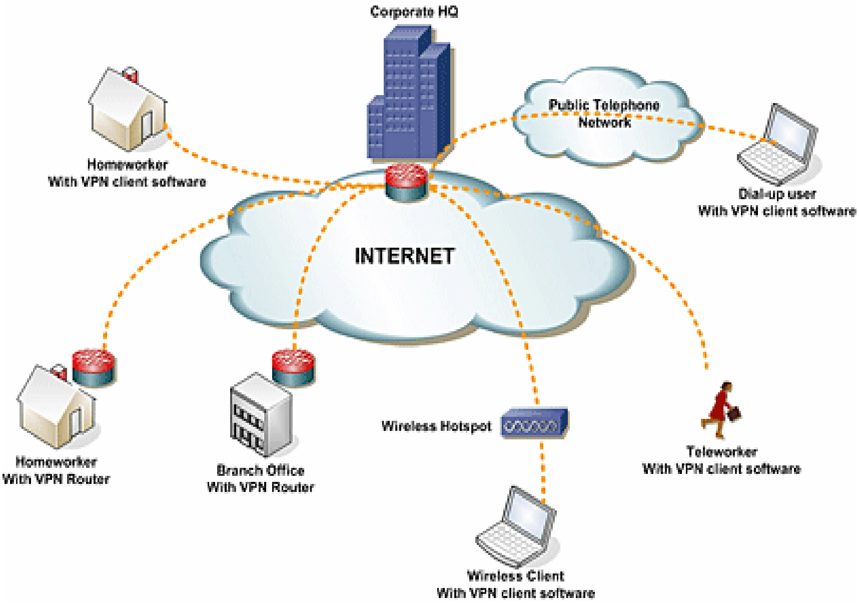


Fig. 4. Representation of a VPN network [13]

3 Pioneering Security Mechanisms

3.1 Building Your Own Honey Pots

Sophisticated hackers that have the means and knowledge to hack into your system will eventually succeed in their task. That is the reason why preventing unauthorized access is not adequate any more. Defenders have to be as smart and pioneering as their intruders in order to successfully face a serious hacking attempt. Honeypots [16] can help prevent attacks in several ways. The first is against automated attacks, such as worms or auto-rooters. These attacks are based on tools that randomly scan entire networks looking for vulnerable systems. If vulnerable systems are found, these automated tools will then attack and take over the system (with worms self-replicating, copying themselves to the victim). One way that honeypots can help defend against such attacks is slowing their scanning down, potentially even stopping them. Called sticky honeypots, these solutions monitor unused IP space. When probed by such scanning activity, these honeypots interact with and slow the attacker down.

Honey pots [17] appeared on the security scene as the means to cover the hole in creating an "ambush" to the attacking parties. It is a very complex security mechanism designed to act as a trap for the intruders luring them to exploit a resource intentionally kept unprotected giving time to the defender to collect information on his attackers. Its diversity in usage is what makes it unique in its purpose: a honey pot can either act as distraction from more valuable machines on a network, serve as an early warning mechanism about unauthorized access into the server or as a research mechanism that observes the intruder and collects valuable information about his steps and system information. There are two types of Honeypots:

- *Production Honeypots* are easy to use, capture only limited information, and are used primarily by companies or corporations; Production honeypots are placed inside the production network with other production servers by organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots which are easier to deploy. They give less information about the attacks or attackers than research honeypots do. The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value [18] to the security measures of an organization.
- *Research Honeypots* are run by a volunteer, non-profit research organization or an educational institution to gather information about the motives and tactics of the Blackhat [19] community targeting different networks. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

3.2 Password-Less Login Using RSA Keys

There eventually comes a point in technologies where current mechanisms are outdated and surpassed. In the presence of such needs new ideas emerge? Password orientated authentication has been for ages the most popular of all login procedures but the number of hacking tools for intercepting or cracking those passwords have multiplied as well [20]. The new trend in authentication processes is password less logins to the system using public key cryptography.

With the use of OpenSSH [21] which fully supports the RSA [22] algorithm, remote users can authenticate themselves to the server using its public key to encrypt data and their own private key to decrypt it. With the use of a secret master password to protect our private key we maximize the security measures of loss or interception of our data. Even if our master password gets stolen the intruder will still not have our private key and same reasons hold if he has only our private key without the master password. SSH clients like Putty [23] need the master password to authenticate that we are the owner of the private key. So in effect, combining the two technologies leads to the best results.

3.3 Port-Knocking

Port scanning [25] is one of the main tools in the hands of the attacker that troubles the security community trying to find a permanent solution. Such a solution is known as *port knocking*, [26] a very sophisticated mechanism to prevent attackers from discovering the open ports of your server.

The procedure is a very simple yet quite intelligent packet sending sequence which imitates the known “Open Sesame” story from the fairy tales. In order for the remote host to be able to connect to a specific port he must first send packets to pre-specified closed ports in a predefined sequence so as to inform the Firewall that it must open the port. Unless the correct closed ports have been “pinged” the wanted port will not appear open. That way even ports that are really open will appear closed to potential port scanning attacks wishing to exploit services of the web server [37]. This method is used to isolate critical resources from the Internet and grant access and awareness of existence only to those really intended to. The best way to keep a door locked is if people do not know how to find the door at the first place, except of course the owners.

3.4 File System Encryption

Sometimes there is really nothing we can do and even the best administrator of the world can not save a violated private property that had its hard drives stolen from their server. Physical security is a big chapter in the Security community but one popular and widespread technique is *file system encryption* [27]. By encrypting the data kept on the web server’s hard drivers we prevent unauthorized access in case of theft from the datacenter. Documents of great corporate, military or financial importance often worry enterprise and government officials about their fate should they fall on the wrong hands. There are a variety of tools for open source usage in Linux file system encryption [28] that fit the needs of every IT professional.

4 Conclusions and Future Work

Undoubtedly, open source ideology has contributed to the growth and evolution of computer software security [29] in every aspect. Its ability to reach inside thousands of programmer’s eyes before hitting the market makes the product solid against a series of attacks the developers couldn’t humanly have noticed themselves. Vincent Rijmen [30], one of the inventors of the known AES algorithm, which today is the basis of Internet security claims that the open source (OS) culture will gradually improve security and make vulnerabilities easier to spot:

“*Not only because more people can look at it, but, more importantly, because the model forces people to write more clear code, and to adhere to standards. This in turn facilitates security review*” [40].

Although making your code transparent certainly improves your readiness to respond to programmer’s suggestions and bug fixes this alone is not enough as it can “*lull people into a false sense of security*” [31]. Among the biggest opponents of open source ideology there is the argument that the construction process of code is absent in large open source projects [32] whereas proven in practice those projects are lead by one or few version with owners with reputation at stake.

Security professionals agree that sharing a code and exposing it to the eyes of possible attackers actually makes it safer. Safer to spot, track and fix. When the question of who might spend hours to figure out bugs in someone else's code the answer is simple: people who use it often, people in the enterprise business that depend their data and money on it and also volunteers from anywhere simply wanting to help. Closed Source software that keeps the code secret away from the eyes of the attacker does not guarantee that is safer by no means [33]. *Security through transparency* is the new trend to substitute *Security through obscurity*.

There are dozens of security techniques pending exploration; new mechanisms introduced by OS communities and IT professionals every day and all part of volunteering open source code writing from the people for the people. The importance and magnitude of this trend can be measured in the scale that governments and large organizations turn their back on the unaffordable, expensive and badly maintained closed source applications and adopt open source platforms and infrastructures [34] for their critical data handling operations. The global community is now mature enough to proceed to a new model of Systems and Information Security based on open procedures and no one can foresee what can be achieved in the future of computer software. Business, E-Commerce, Education, Defense, Science and all important aspects of our everyday encounters will evolve around the ability to share and improve each other's life through open and participatory procedures.

References

1. Lawton, G.: Open source security: opportunity or oxymoron? Computer 35(3), 18–21 (2002)
2. Spinellis, D., Szyperski, C.: How is open source affecting software development? IEEE Software 21(1), 28–33 (2004)
3. Witten, B., Landwehr, C., Caloyannides, M.: Does open source improve system security? IEEE Software 18(5), 57–61 (2001)
4. Shankar, K.S.D., Kurth, H.: Certifying open source - the Linux experience. IEEE Security & Privacy 2(6), 28–33 (2004)
5. Net Craft Secure Server Survey -, Web Server Survey (March 2009), `http://news.netcraft.com/archives/2009/03/15/march_2009_web_server_survey.html`
6. OpenSSL Project, `http://www.openssl.org/`
7. World writable/tmp, `http://seclists.org/bugtraq/1998/Jul/0119.html`
8. Transport Layer security, `http://en.wikipedia.org/wiki/Transport_Layer_Security`
9. Apache Software Foundation, `http://www.apache.org/`
10. Red Hat Entreprise, `http://www.redhat.com/`
11. Linux log Analyzers, `http://www.linux.org/apps/all/Administration/Log_Analyzers.html`
12. Schroder, C.: Enhance Security with a Linux Logging Server, `http://www.enterprisenetworkingplanet.com/netos/article.php/3521481`
13. VPN Image, `http://www.lanos.co.uk/main/images/stories/diagram/vpn.gif%20`
14. Toolbox for Information Technology, Symmetric key Encryption, `http://it.toolbox.com/wiki/index.php/Symmetric_Key_Encryption`

15. Online Encyclopedia: Wikipedia, Public-key cryptography, http://en.wikipedia.org/wiki/Public-key_cryptography
16. Tian, Z.-H., Fang, B.-X., Yun, X.-C.: An architecture for intrusion detection using honey pot, November 2-5, vol. 4, pp. 2096–2100 (2003), doi:10.1109/ICMLC.2003.1259851
17. Honey pots Intrusion Detection, http://www.honeypots.net/
18. Spitzner, L.: Honey pots: Definitions and Value of Honey pots (May 2003), http://www.tracking-hackers.com/papers/honeypots.html
19. Black Hat Homepage, http://www.blackhat.com/
20. Online Encyclopedia: Wikipedia, Password Cracking, http://en.wikipedia.org/wiki/Password_cracking
21. OpenSSH Project, http://www.openssh.com/
22. RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2146
23. Putty Homepage, http://www.chiark.greenend.org.uk/~sgtatham/putty/
24. OpenSSH Passwordless Connections, http://wiki.e-shell.org/OpenSSHPasswordlessConnectionsTheQuickWay#rsa
25. Introduction to Port Scanning, http://netsecurity.about.com/cs/hackertools/a/aa121303.htm
26. Linux Journal, Port Knocking, http://www.linuxjournal.com/article/6811
27. Linux journal, Encrypt your file system, http://www.linuxjournal.com/article/7743
28. Linux.com, Enhance Security with file encryption tools, http://www.linux.com/feature/59932
29. Secure Programming for Linux and Unix, 'Is Open Source Good for Security? http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html
30. Biography of Vincent Rijmen, http://www.nist.gov/public_affairs/releases/biovince.htm
31. Viega, J.: The Myth of Open Source Security, http://it.slashdot.org/article.pl?sid=02/02/15/1846214
32. Schneider, F.B.: Open Source in Security: Visiting the Bizarre, May 14-17, pp. 126–127. IEEE CNF (2000)
33. The Risks of Closed Source security, http://www.ibiblio.org/oswg/oswg-nightly/oswg/en_US.ISO_8859-1/articles/alan-cox/risks/risks-closed-source/risks.html
34. Linux Adoption worldwide, Online Encyclopedia: Wikipedia, http://en.wikipedia.org/wiki/Linux_adoption#Government
35. Khanvilkar, S., Khokhar, A.: Virtual private networks: an overview with performance evaluation. IEEE Communications Magazine 42(10), 146–154 (2004)
36. Hissam, S.A., Plakosh, D., Weinstock, C.: Trust and vulnerability in open source software. IEE Proceedings Software 149(1), 47–51 (2002)
37. Ohmaki, K.: Open source software research activities in AIST towards secure open systems. In: Ohmaki, K. (ed.) Proceedings of 7th IEEE International Symposium on High Assurance Systems Engineering, 2002 High Assurance Systems Engineering, 2002, pp. 37–41 (2002)
38. Sarkinen, J.: An open source(d) controller. In: Telecommunications Energy Conference, 2007. INTELEC 2007, September 30-October 4, pp. 761–768 (2007)
39. KeePass password Safe, http://keepass.info/
40. Rijmen, V.: http://www.linuxsecurity.com/content/view/117552/49/

Session 7

e-Government and Local e-Government

e-Government Readiness, Strategy and Two Different User Groups - in Austria

Noella Edelmann[1], Johann Hoechtl[2], and Peter Parycek[3]

[1] Center for E-Government, Danube University Krems
noella.edelmann@donau-uni.ac.at
[2] Center for E-Government, Danube University Krems
johann.hoechtl@donau-uni.ac.at
[3] BKA - Austrian Chancellery
peter.parycek@bka.gv.at

Abstract. This paper offers a description of the e-Government Strategy in Austria and its e-Government readiness, and looks at how two different user groups are experiencing e-Government in Austria. Studies conducted show that adolescent citizens are more optimistic and enthusiastic about the possibilities offered whilst the municipalities are more skeptical. The Austrian e-Government strategy, the decisionmakers and IT solution providers must understand the needs of all stakeholders and provide viable solutions accordingly.

Keywords: e-Government, e-Participation, municipalities, adolescents, e-Government readiness, e-Government Strategy, Austria.

Introduction

1 The Austrian e-Government Strategy

The Austrian e-Government Strategy[1] states that: “All policy making of public administration has to be carried out by electronic means and to be simple and quick, without requiring in-depth technological knowledge. Thus, public administration has to utilize modern electronic media for communication”. While this clearly marks a strategic viewpoint, one question inevitably arouses: Where does “All policy making [...]” start and where does it end? Should each and every “conventional” process of public administration be made available electronically or should a more careful approach be taken?

Only the most basic and fundamental principles of what comprises the Austrian e-Government strategy are anchored by law. The federal structure of Austria, with its layers state, province, town and municipality and their respective sovereign rights, do not really allow for a centralised e-Government strategy. Defining technical terms and standards in law is impractical, as terms and standards are subject to frequent changes. Thus the states, provinces, towns and municipalities have agreed to set up a “vertical

[1] http://www.digitales.oesterreich.gv.at/site/5237/Default.aspx

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 251–258, 2010.

layer" to ensure a common understanding, mutually accepted conventions and methods as to how the e-Government strategy should be implemented. The conventions on the Austrian reference server[2] are the authoritative resource for data formats, interface descriptions, procedure models and good practices of e-Government in Austria. By defining and agreeing to the decision making process, it is possible to achieve normative conventions, although these do not have legal status.

2 e-Government Readiness

In 2001, the Austrian province Salzburg applied an all-or-nothing strategy with the goal that by the end of 2004 all public administrative processes should be electronic. In 2006, the provincial accounting office (Landesrechnungshof) reported a defeating result: 83 pages described how the project was 30% over the set budget, behind schedule, missing implementations, and that during the period 2001 - 2005 only a total of 577 electronic applications had been received [1]. Further major concerns were the missing measurement of frequency (how often a procedure is actually used) and that stakeholders had not been involved, leading to poor and unpractical solutions.

Project management is a key factor for the successful implementation of e-Government services. It is important to identify the relevant processes for electronic implementation and to take into consideration factors such as frequency, cost and benefit, risk and utility and impact. Answers to some of these factors can easily be obtained by asking the stakeholders, for example, by using a survey. Then, on the basis of the data received, a decision should be taken.

The report on e-Government implementation in Salzburg focused on the failures in project management. However, another important aspect was quietly ignored: the ex-ante readiness for e-Government. Readiness must be present in the following areas [2]:

- Leadership and governance readiness assessment: the leaders must agree upon and recognize e-Government as an important part of the governmental strategy which supplements public services and enables faster, more flexible and friction-free service delivery for business and citizens.
- Legal readiness: does the state have a legal framework which allows electronic application and communication with the governmental agencies?
- Organizational readiness: digital communication flows are very different to the traditional information flow in governmental institutions. Traditionally, these are organized in a strict top-down, bureaucratic manner. An "e"-ready state has to design a process model showing how to deal with digital information flows, and then legally anchor them.
- Competency readiness: both government and administrative personnel must have the knowledge to deal with electronic communication facilities, not merely on a technological basis but on the conceptual side too. An indicator

[2] http://reference.e-government.gv.at

for competency readiness is whether internal trainee programs focusing on ICT knowledge mediation are available.

- Technology readiness: this encompasses all the ICT facilities necessary for electronic information brokerage, communication and service delivery such as hardware, software and network infrastructure. In underdeveloped countries, even a stable source of electricity may be an issue that needs to be taken into consideration.
- Customer readiness: despite the availability of the technical infrastructure, it is impossible to expect an even distribution of e-Service acceptance. “E-” acceptance is influenced by literacy rate, rural / urban residence, cultural factors and accessibility. For example, some people strongly prefer face-to-face communication over electronic communication.

3 Two Different e-Government User Groups in Austria

3.1 User Group 1: The Municipalities

In 2008, the Danube University Krems invited all 2357 Austrian municipalities to participate in an online survey hosted by the Austrian Federal Bureau of Statistics. The project was to look at the Austrian municipalities’ availability of e-Services, participatory facilities and e-Government readiness. The survey could be accessed on the web platform 10th July – 22nd August 2008.

2357 Austrian municipalities were invited to participate, 1249 completed the questionnaire, which represents an excellent return rate of almost 53%. Some of the interesting results obtained were:

- 93% of the municipalities have a website;
- 49.14% of the municipality websites have the domain name “gv.at” (governmental domain);
- 79.76% of the municipalities believe that the website adds value to the way the municipality is perceived;
- 1.6% of the municipality employees are assigned to ICT-related work;
- 87.9% of the municipalities have a network structure;
- 94.9% of the municipalities have antivirus;
- 87.7% of the municipalities have a firewall;
- 54.8% of the municipalities back up their data;
- 68.3% of the municipalities believe that the adoption of IT processes will lead to increased efficiency and simplify daily work.

The IT infrastructure available per employee (PC, laptop, internet connection) and the type of network connection are further important indicators for e-Government progress. The correlation between the number of employees and the number of available PC's or laptops is 0.57, or a mean of 1.33 employees per computer. This number makes sense as it takes into consideration operative personnel too, which may not be equipped with computers at all.

Awareness of IT security is generally very good: employees know about the risks of viruses and malware, and computer systems are secured – but they often lack backup strategies. Since an ever increasing dependency on working computer appliances is to be expected, a working day (or even longer) lost due to defective hardware can be catastrophic. Training programs for public administration need to address this issue.

3.2 User Group 2: Adolescent Citizens

The other side of the coin is highlighted by the projects "Mitmachen.at –Move Your Future" and "Jugend2help" led by the Danube University Krems. These projects investigated the attitudes and expectations of those citizens assumed to be most technically adept and "savvy": adolescents. Adolescents, also known as the „online generation", digital participation is a key success factor for involvement and integration into the evolving e-State. They must be recognised as a significant target group of e-Government and e-Participation users; their interests include further education, obtaining a driving license, starting a family, housing and re-location. These are services which can be facilitated by online information, communication and transaction.

In Austria, 95% of the 14–18-year-olds use the internet [3] so online-based participation projects are possible (as long as they are made accessible to everyone). A common prejudice is that young citizens are not interested in politics at all, yet a survey [4] reveals that 86.7% of all adolescents do want to be involved in political decisions, and 92.5% believe that political engagement is beneficial to their personal development, although only 50.9% are actually willing to contribute towards such activities. Whilst 25.4% of the adolescents asked know about any youth programmes, only 15% participate. This shows that there is a big discrepancy between the value given to participation and the actual level of engagement, particularly in traditional or party politics. These young users are important for the further development of e-Skills and online integration as they act as disseminators and teachers of digital skills and knowledge in their families and communities, a role which is particularly important in marginalised groups. Digital inclusion is based on technical resources; for that reason in Austria accessibility is legally anchored in the E-Government Act[3].

In 2007, "mitmachen.at" was the first Austrian youth e-Participation project to look at adolescent users and their interaction with e-Government and views on e-Participation. The Jugend2help web portal project followed in 2008, and the adolescent citizens were invited to participate in the creation of the content and take decisions concerning their own space ("youth") on the Austrian e-Government webportal www.help.gv.at.

The name of the project " Mitmachen.at – move your future" reveals the objective: in German, the verb 'mitmachen' means 'to participate', and the project provided young citizens aged 15–25 living in Austria the opportunity to use the internet to present and voice their concerns about the future. It was one of the biggest e-Participation projects, and involved a number of organisations, including youth institutions, software companies, various Think Tanks and the relevant public authorities so as to develop a democratic participation process.

The focus of the study was online participation, participant involvement, the relationships that developed between participants and, at a meta-level, how participants

[3] http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=31191

felt about online participation. The project results were analysed as a case study, with the aim to analyse the project and its results as a whole, to show the opportunities and limitations of online deliberation as a means of increasing citizen engagement and reducing the problem of citizen apathy,(see [5] [6]). The project investigated and tested the general electronic participation processes, and the technical implementation and the (technical) framework which make such participation processes possible. Portals are important for simplifying the vertical and horizontal integration of e-Government [7] and the virtual portals used for this project included both the necessary instruments for participation as well as two different user levels (administrative and end-user).

The discussion process was governed by the pre-set eight topics, but the participants had the opportunity to voice their opinions about anything else they considered to be important. The highest number of comments were made in the category 'political system', and revealed the participants' frustration with politics and politicians. A few wanted to know more about the Austrian political system and politics but, in general, the comments were derisive and very superficial. A small number of participants displayed interest in the project itself, the results to be obtained from the project and how opinions and results would be used. A participant declared: "The politicians should read this …"[4].

The results show that a web portal can be a method of participation and communication which is accepted and will be used by young people. The ideas generated provide a "mini-governmental program determined by young Austrians" (as described by a member of the expert panel involved in the project).

In 2008, the follow-up project "Jugend2help" (www.jugend2help.gv.at) was conducted. It was largely influenced by valuable information gained from the project "mitmachen.at" ([8][9]). Therefore, the central aim was to collect new e-Participation and collaboration experiences and data, to examine the way a public Web 2.0 project works and to find out to what extent young citizens can be engaged in public decision-making processes. The cooperation between civic society, public administration and various partners (from schools to unemployment agencies) was to lead to a better, user-friendly provision of public services.

Besides obtaining correlations between the users and their e-Government needs, the researchers also investigated the adolescents' understanding of e-Participation, e-Government and public administration. Asked what they knew about e-Government, the adolescents' answers included "something to do with the government"[5], and "an opportunity to look into the state's finances and expenditure"[6]. Although they know little about e-Government and the digitalisation processes occurring at state level they responded positively to it and adolescents seem to want the opportunity to participate (physically and digitally) in the participation process, as they strongly believe in the value of communicating and sharing. They were also particularly enthusiastic about participating in this e-Government portal project - they recognised the project as an opportunity to participate in government and public administration, and to have their say on issues which are relevant and important to them. The adolescents liked the idea of

[4] Comment made on www.mitmachen.at

[5] Comment made by a participant.

[6] Ibid.

finding all the information they need electronically; they belong to the generation that is growing up expecting to find everything on the internet [10] and to integrate their e-Participation and e-Government needs seamlessly into their work and personal lives.

4 Lessons Learned

The results obtained from the "mitmachen.at" and "Jugend2help" projects were positive, and show that citizens do have an interest in online deliberation and interaction, and that the internet certainly offers a new possibility of involving citizens in political discussions and e-Government.

An important issue that needs to be considered is age: the age bracket of the intended users is a determining issue for such projects. A strategy for youth e-Participation and e-Government therefore requires a specific definition of the category "young people" or "adolescents" that may vary in different countries – the Austrian Census Office, for example, defines a youth as a person up to 19 years of age. The means and channels of participation must be adapted to the target group characteristics, age will determine the appropriate topics and the choice of language to be used. The (marketing) strategy will also be determined by the age of the citizens, so that it can reach and encourage those citizens to participate. It should carefully consider the choice of communication channels (i.e. the ones users really like and use) and what institutions (e.g. schools) can help to reach out to those citizens.

Citizens and political/public actors now do have a wide range of media and ICT tools to assist them with complex processes such as participation and public administration, but they must be able to "enhance representative democracy, whilst creating a vibrant, inclusive, transparent and responsive Knowledge-based Democratic Society and not just be a new form of political communication." [11]. Digital networks can support all forms and stages of public involvement and empowerment, ranging from simply providing information to actual decision-making [12]. New electronic media provides a way to enhance deliberation (rather than replace existing democratic mechanisms) by providing transparency, encouraging broad discussions and supporting opinion-building. The collaboration between public administration and all sectors of civic society includes integration in policy-making and the co-development of public services, and in the long run, participation can contribute to the process of democratisation in both state and society by breaking down social barriers and structural inequalities.

The results obtained from the e-Government survey show that by 2010 97% of the municipalities in Austria aim to have websites and 92% plan to provide online forms. Many municipalities already offer such services, but a closer cooperation with the Austrian Help.gv (which also offers the national e-Government webportal www.help.g.v.at) would be beneficial for all stakeholders. Such a co-operation could start to meet citizen needs and requirements, and so increase citizen satisfaction.

At the beginning of 2007, the Austrian parliament reformed the voting laws: beside the new possibility of postal voting and e-voting, the voting age was reduced to 16 years. This means that political education is more important than ever before, and adolescents must be well informed in order to be able to take good decisions. It is well known that political education needs to include a practical approach; so, beside the right to vote, youth participation programmes should encourage young people to engage in politics. Public administration too needs a policy and guidelines for online citizen participation – such a policy should have standardised e-Participation methods, including the four-phase model tested in “mitmachen.at” and “Jugend2help”, as it can then be used for a wide range of future e-Participation and e-Government projects ranging from local, neighbourhood projects to nation-wide involvement. The aim of developing a policy is not to regulate participation, but to provide an overview and a documentation of tested methods, as well as allowing further innovation.

Some cornerstones of the Austrian eGovernment strategy require better marketing and information policies or a change in general conditions: 49.6% of municipal employees did not know about e-Delivery and 52.6% cannot e-Sign any documents. Better cooperation of software providers, public management consultants, and a strategic brochure such as “5 Steps towards e-Delivery” would improve the situation.

More Austrian projects will be launched in the coming years, and will show the extent to which citizens want to become politically involved and make use of the new technologies for this purpose. All in all, we will soon know if technology can actually change democracy. In general, the results from “mitmachen.at” and “Jugend2help” show that most young Austrians have a positive attitude towards online deliberation, new methods and opportunities to participate. Municipality officers tend to have a somewhat negative attitude as to whether eGovernment and eParticipation can increase work efficiency and simplify processes. E-Government is viewed as a tool geared more towards the citizens than to the officers, and usability seems to address citizen issues rather than the employees.

An important indicator for e-Government readiness is a project plan for IT-projects and the results show that 87% of the Austrian municipalities do not plan their IT projects! The tendency of smaller communities to provide fewer online services and their negative attitude towards IT applications and projects is partially an infrastructure problem. Today’s public administration still operates in structures set after World War II: a federal reorganisation is long overdue, at least at the operative layer. Inter-community collaboration with service orientation and an option for higher specification may be a solution. Virtual communities, e-Villages in terms of their proper meaning, will make rural areas more attractive for citizens and business. Both IT solution providers and decision makers try to address both the citizens’ and municipalities’ needs, by understanding what their issues are and then by finding viable solutions.

References

1. Landesrechnungshof Salzburg, Bericht des Landesrechnungshofes über die Projekte E-Government und ELISA, Land Salzburg (2006)
2. Al-Omari, A., Al-Omari, H.: E-Government Readiness Assessment Model. Journal of Computer Science 2, 841–845 (2006)
3. GFK AUSTRIA, Online Monitor 3. Quartal, GfK Austria (2007)
4. Serloth, A., Maerki, O.M.: Partizipation und Information – Ergebnisse einer Jugendbefragung, Study conducted for the Austrian Ministry of Social Security Generations and Consumer Protection, das Fernlicht, Vienna (2004)
5. Blumler, J.G., Coleman, S.: Realizing Democracy Online: A Civic Commons in Cyberspace, IPPR, London (2001)

6. Klein, H.: Tocqueville in cyberspace: using the internet for citizen asssociations. Information Society 15(4), 213–220 (1999)
7. Moon, M.J.: The evolution of e-government among municipalities: rhetoric or reality? Public Administration Review 62(4), 424–433 (2002)
8. Edelmann, N., Krimmer, R., Parycek, P.: Engaging youth through deliberative e-participation: a case study. Int. J. Electronic Governance 1(4), 385–399 (2008)
9. Krimmer, R., Makolm, J., Parycek, P., Steininger, I., Kripp, M.: Politik zum Mitmachen, Jugenddeliberation im Internet, Arbeitspapiere zu elektronischen Wahlen und Partizipation, pp. 69–78 (2007)
10. Codrington, G., Grant-Marshall, S.: Mind the gap! Penguin South Africa (2005)
11. van Lerberghe, D.: Are we moving towards a more participatory representative democracy? In: Proceedings of the Eastern European e|Gov Days 2007: Best Practice and Innovation, OCG Band 222, Vienna, pp. 197–204 (2007)
12. Parcyek, P., et al.: EDEM. Positionspapier zu E-Democracy und E-Participation in Österreich (2008)

On e-Government Project Development in Balmeda

Miltiades E. Anagnostou[1] and Maria A. Lambrou[2]

[1] National Technical University of Athens, School of Electrical and Computer Engineering, Athens 15780, Greece
miltos@central.ntua.gr
http://www.ece.ntua.gr

[2] University of the Aegean, Department of Shipping, Trade and Transport, Chios, 82100, Greece
mlambrou@aegean.gr
http://www.stt.aegean.gr

Abstract. An e-government project management and development scenario in a fictional country is described. Emphasis is given on how local culture undermines project quality. A detailed fictional project development scenario is presented. The interplay between different players, i.e. project developers, reviewers, and public services, is illustrated. While the rules of technology are the same everywhere, local adaptation due to socio-economic factors can bend them to the degree of making them ineffective.

Keywords: e-government, project management, life-cycle, requirements, implementation.

1 Introduction

Is ICT project management in less developed countries performed in the same way as in top of the GDP list countries? Are the project development rules equally effective everywhere? How do the characteristics of local societies affect this process and the final quality? Can formal specification methods be applied with equal success everywhere? Is the outcome of the project of the same quality everywhere? How do differences influence the ICT infrastructure, which is offered to the citizen and to the business sector? These are some of the questions, which are addressed in this paper by giving a condensed scenario of project management and development.

Information Systems in Developing Countries (ISDC) research cites ICT development as a process of technology and knowledge transfer and adaptation to local social conditions [1]. The important theme of ICT failure is often discussed in connection with ICT systems design and implementation research issues, emphasizing on the complex interplay of action and local context and the gap between the professional knowledge and practice of systems development and the actual conditions of organizational practice in developing countries. Within

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 259–269, 2010.

current e-government research, significant recognition of human and other contextual factors that influence or mediate the impacts of e-government has been achieved [2]. Considerable research efforts have been made towards improving the understanding of the interaction among technology, organizations, and environments in e-government initiatives [3], and the primary challenges are categorized according to their core aspect into: (1) information and data, (2) information technology, (3) organizational and managerial, (4) legal and regulatory, and (5) institutional and environmental.

While M. Ayyad thinks that "all nations face the same problems" w.r.t. e-government [4], M. Yildiz supports the view that e-government research suffers from oversimplification of the e-government development processes within complex political and institutional environments [5]. According to the technology enactment view of e-government, adoption and implementation processes transform the objective form of ICT to its enacted form, in other words, technology is customized to the needs and the environment of a specific organization through the process of enacting. The context of the existing institutional arrangements, organizational forms and the involved stakeholders interacting, determine e-government initiatives as complex socio-technological systems [5], rather than deterministically approached technological ventures. In a few words, e-government quality can be poor and e-government projects can fail for complex reasons.

Spectacular project failures are not rare in history. A recently popular story is the history of Vasa. Vasa was a warship, which was built between 1625 and 1628 for the royal Swedish navy. It sank in the bay of Stockholm only half an hour after it was launched, thereby causing a huge waste of resources and a plunge in national prestige. The documentation of the trial, which followed the spectacular failure, has allowed today's researchers to partially assess the underlying reasons. In the literature of software technology and project management Vasa [6] serves as an example of patterns, which can also be found in these areas and should be avoided.

In modern times another spectacular failure has been documented by H. Goldstein in [8]. He explains how 700,000 lines of code in a $170 million project were scrapped together with the project itself. The Virtual Case File (VCF) "was supposed to automate the FBIs paper-based work environment, allow agents and intelligence analysts to share vital investigative information, and replace the obsolete Automated Case Support (ACS) system."

In a broad sense both failures can be regarded as a (lack of) know-how problem, not only in their specific technology areas (ship-building and software engineering respectively), but also in project management and formal specification. Swedish shipbuilders of 1620's had never before constructed a ship with two rows of canons. They did not know how to prepare and use a detailed plan before moving to actual construction. Management was chaotic, and the broader management group included non-experts, including the king himself. Requirements were not clear from the beginning and they were changing even within advanced phases of development. Finally, pre-launch testing was inadequate. The

VCF was more of a complexity problem, which could be confronted by modern formal specification and description technology.

Such failures are treated in the literature as examples of breaking the "rules." Rules consist of mainly two sets: (a) Project management rules (which, in the area of software development, usually embody a clear life-cycle model), and (b) formal specification. The second set is optional, but it is strongly recommended in the design of complex systems or systems with intense reliability requirements. Note also that we are speaking of today's rules and technologies, which were largely unknown in the age of Vasa.

On the contrary, in this paper we present a scenario, which involves persons who usually are aware of the rules, but they consciously decide to bend them. We show that local culture can have a profound effect on project execution and on final product quality. The scenario is not real in the sense that it consists of a mixture of elements that (a) may belong to different occasions or (b) may be fictional, but, to the best judgement of the authors, could possibly happen.

2 The Environment

The aforementioned scenario is presented in the context of a fictitious country, which is called *Balmeda*. Balmeda is a typical country of the European South. Its inhabitants exhibit a mixture of Mediterranean and Balkan mentality. European South is less industrial and less well organized than North. The lack of organization is partly balanced by the warmer climate. Eventually this gives a subjective feeling of happiness and well being, which gives high values to life quality indices. GDP in the South is typically lower than the GDP in the North, but it is underestimated since it does not include black market, which is again typically stronger in the South.

Balkan mentality has inherited reactions from an era, in which Balkans belonged to the Ottoman Empire. This era is for some regions less than a hundred years distant. Around 1900 the organization of the Ottoman Empire was substantially different than European organization. The latter was mainly industrial and offered a large collection of public services including public order, healthcare, transportation and communication infrastructure. The Ottoman Empire was forced by the Great Powers to adopt most of these services in an effort towards modernization, i.e. incorporation in a global production scheme. Brailsford, an English journalist, gives a detailed account [9] of the results in 1906: "In a vague way the bureaucracy has learned that certain institutions utterly foreign to its own civilisation exist among the greater Powers, and for ends of its own it has attempted to imitate them ... This comical anxiety to ape Europe has no other result than to confuse the minds of the official class, to burden the treasury, and to distract the Government from humbler work less hopelessly beyond its competence ... Its inhabitants are not citizens but subjects. No sense of a commonwealth has grown up in their minds to bridge this isolation, or to cement warring races in a care for their common country ... Before the superficial and insincere aping of Western peoples during the last generation, there was no place even for civil law, not to speak of such comparatively modern functions of the State as the care of education ... The military proper and the gendarmerie were concerned not so much with the preservation of order as with the maintenance of the system of ascendancy ... There are no terms in our language in which this system can be adequately described." In other words, the Ottoman State was a system optimized for conquest and occupation, not for industrialization.

However, Balmeda is not an underdeveloped country. It is an EU member and, therefore, it satisfies the EU economic and political criteria, albeit some of them marginally. A detailed analysis of the country would entail a description of its educational and economic structure, but for the sake of brevity casual references will be made only when necessary.

3 The General Projects Office

A few years ago Balmeda decided to set up a General Projects Office (GPO). All projects of almost any nature must be submitted to the GPO in order to get a license (and pay a fee). GPO has more than 100 local offices, which deal with local project submissions. If they are within the competence of the local office, the proposal is reviewed locally, otherwise it is forwarded to the closest competent office. A central office in the capital city of Balmeda can deal with any kind of proposal, therefore it ensures that all proposals can finally be accommodated.

GPO ensures that the proposal is sound, useful, financially and technically feasible, manageable, and well documented. Projects fall into a number of categories. For each category a set of concrete review steps has been determined. The rules are the same for both private and public projects. GPO claims that its reviews are unbiased and purely technocratic Some general policy criteria (for example, environmental protection, respect to local tradition etc.) apply in its decisions, but the criteria are open, well known and have been set by the parliament. Occasionally criticisms regarding the influence of local financial, political and personal relationships on GPO's decisions find their way to the press. Also, some cases of bribery have been uncovered, and GPO decisively lowers Balmeda's CPI (the subjective Corruption Perceptions Index of Transparency International), which is close to the CPI averages of Mediterranean countries and Balkan countries, but very far from the average CPI of Nordic countries. The government has considered a random re-distribution of the reviews among GPO's offices, but this solution was found impractical, as most of the proposal reviews require a series of local inspections.

In Balmeda e-government is rapidly gaining momentum for a number of reasons: (a) It is recommended and partially funded by the EU, (b) it relies on automation of decisions, which can possibly reduce favoritism, (c) it brings cost reduction and it increases efficiency, (d) it improves the quality of services, which are offered to citizens, and (e) it gives an incentive to citizens and businesses to buy computers and fast Internet connections; this improves the country's ICT infrastructure. Such conceptualizations of the e-government are common [5,7].

4 The Main Story

4.1 Call for Tender Phase

A few years it was decided that GPO should enter the electronic era. An open tender for proposal was launched. Some of the terms of the tender have been:

- All local offices of GPO and all of their procedures should join e-government.
- Any existing electronic infrastructure should be incorporated into the new system, unless it is definitely obsolete.
- The final set of requirements should be formulated by consulting all GPO's offices. The development phase would be able to start only after a thorough review of the requirements and only if they were found complete.
- Testing should include a pilot phase, in which the system would run in selected offices for a few months.

The project of modernizing the GPO was found sound and was summarily approved. Immediately after the approval the tender was publicly announced. The contestants were three well known companies of the software sector. The contract was awarded to the Balmedan Advanced Software Technologies (BAST) on the basis of a combination of low cost and past experience in developing and installing e-government systems.

Although the GPO was the usual external reviewer of all projects, it was the client in this particular project. Therefore it was deemed inappropriate to play both roles. Of course GPO employees would participate at least in the requirements collection phase, and in the testing phase, but an additional tender for the supervision of the project was launched. Valid contestants would be consulting companies. *Way Forward Consulting* (WFC), a small Balmedan consulting company, was given the inspection and quality control project. Some large international consulting firms operate in Balmeda, and they immediately filed a protest against this decision saying that the WFC offer was too low. They backed their statement by pointing at the large number of local offices, which should be visited by the inspectors at least on a statistical sampling basis in both the requirements collection phase and in the testing phase. Their plea was rejected on the ground that the inspection could be based mainly on paper and software deliverables.

There was a more serious reason, which could have excluded WFC. The technical expertise to inspect a project of that scale did not exist within WFC, since the permanent personnel of WFC mainly consists of experts in finance and general project management. Having foreseen this obstacle, WFC had asked for the cooperation of three university professors, A.B., C.D. and E.F. who did have the required technical expertise. Their CVs had been included in WFC's response to the tender. It is a usual Balmedan practice to include professors in review, inspection and audit committees. When a GPO or other public sector committee is about to officially accept the results of a project (or a tender), it sets up a secondary "committee of experts," who accept the responsibility to review the results (in a tender, to confirm that the chosen contestant was the right one). After all they are experts, aren't they? Professors who are badly paid or belong to the ruling political party usually accept this risk. The role and effect of external advisors has been recognized in the literature [11].

4.2 Requirements Collection

The first deliverable involved a presentation of the existing situation in local offices, in terms of both infrastructure and procedures. The term "requirement collection" is rather weak in describing the real task, which consists of the following steps:

1. Write down all existing processes and procedures, including alternative actions towards the same end,
2. describe them in terms of concrete and discrete simple steps,
3. redesign processes in order to make them simpler, if possible, and more amenable to mechanization.

Step 3 requires a through understanding of all processes and objectives and its importance and required effort cannot be overestimated.

BAST visited a small number (less than 10) offices and contacted a few more by phone. The BAST emissaries met sufficient resistance from local office employees, who were unwilling or too busy to provide them with suitable input, or they could simply not understand the exact purpose of the visit. Of course the latter carried a letter, which assured the office head that they were entitled to ask for information. Moreover, the office employees often followed less than clear procedures, they had multiple responsibilities, and the forms they finally filled was the only uniform element in all offices.

A BAST employee, who was fairly experienced in writing deliverables was commissioned to prepare the requirements deliverable. Despite the small number of offices that were visited, all existing infrastructure was deemed obsolete. All data found in older systems were considered either unimportant or impossible to port. Effectively this meant that (a) no data migration was needed, (b) no interface or other interworking mechanism with older systems was needed, and (c) new equipment was necessary. A few weeks later the deliverable was presented at a joint meeting of the BAST project team, representatives of the GPO, and WFC members, which included the three professors. After the slide presentation of the main results, which actually were very poor, prof. A.B. made the following observation: "This deliverable describes the process of collecting requirements, and the difficulties in achieving this purpose. However, it does not deliver the promised results, namely the requirements per se. In this sense the deliverable must be clearly rejected". A GPO representative, who probably was offended by the negative colors, in which GPO's response was presented, asked for the addition of a phone number list of all GPO offices in the deliverable. He implied that perhaps most offices had not been contacted. If this were true, the contract would have clearly been violated.

The BAST employee, who served as a project manager, promised that a second version of the deliverable would present the requirements. He asked however for a deadline extension, which effectively meant that it would appear together with the next deliverable on system architecture. The obvious interpretation of this statement was that requirements would appear as a byproduct of the first version of the real system.

4.3 Development

In the following few months BAST presented a first version of the system, which mainly consisted of the user interface, but the actual behavior behind the curtains of the interface was largely absent. Nevertheless there was substantial progress, which showed that the development team had acquired significant knowledge of the GPO internal organization, even though this was not achieved from the requirements phase. BAST had hired two GPO employees, who in their spare time provided consulting services to the BAST team and remained invisible throughout the project. The requirements deliverable was also updated. Its bulk consisted of printouts of different instances of the user interface. The person who presented it argued that the requirements were obvious from the interface, since all important functions and their sequencing were represented by the "buttons" and fields of the interface. A long list of comments was written by the review committee and the deliverable was marked as "pending acceptance."

The next meeting of the joint review committee took place prior to testing. In the meantime a new project manager was appointed by BAST. He immediately asked for the extension of some deadlines, in order to find the time to get acquainted with the project. In the meeting version 2.0 of the system was presented, which was ready for final testing before targeting (i.e. before installation at real offices). A test description deliverable was also presented. Prof. A.B. made the following observations:

1. Version 2.0 of the system showed significant improvement over version 1.0, but he was hardly convinced that it was ready for testing.
2. Test descriptions were fuzzy, as they did not describe concrete tests, but they rather indicated possible areas of testing in broad terms.
3. A test plan was absent from the deliverable.

Finally, A.B. asked for direct access to the system pilot, which was installed on a BAST server, for testing purposes.

Prof. C.D. offered a few other angles of view:

1. He said that what actually was done by the system was a duplication of the work of the GPO employees. GPO's main objective was the technical approval of submitted projects. Every project proposal was reviewed and approved step by step. He said that while the system did nothing to really help with the technical review of a specific proposal, it asked the public servant, who was responsible for the review, to write the equivalent of a short status report in each step.
2. Effectively, this system helped the local and global GPO management be in control of the progress of GPO works, but it did nothing to improve the core business.

3. Project proposers, i.e. GPO's actual "clients," were asked to fill and file the same application form, albeit electronically. This might save them one or two visits at GPO's offices, but they were asked to collect and bring any supporting documents by themselves. Moreover, documentation could not be submitted electronically. Therefore personal visits to the offices were not eliminated. He also said that ideally the citizen should not be bothered for documents, which were produced by other public services; they should be collected by using direct electronic communication between the GPO and these services. Effectively, GPO should serve as an *one stop shopping* point for the citizen (or the business).
4. He added that this latter point made the GPO e-government project hardly legal, because there were explicit EU rules saying that the main objective of e-services was to simplify the life of citizens. On the contrary, this project mainly aimed at improving the internal function of the GPO (which also was questionable according to observation 1).

Then a GPO employee stood up and said that he had discovered another annoying problem in the presentation of the system. According to internal GPO rules concerning the review of any project, project steps were approved sequentially (i.e. a waterfall model approach [10] was applied). In system version 2.0 when a step was approved it was marked as "closed." This meant that this step could not be revisited. He was interrupted by a BAST programmer (originally a chemical engineer), who was responsible for the implementation: He said that irreversibly closing a step conformed to an anti-corruption requirement, which protected the citizen from drawbacks in the proposal approval process. The GPO employee offered one or two practical examples, which definitely proved that the waterfall model could not be applied strictrly, i.e. without going back to previous steps. The programmer said that he would consider an appropriate solution without sacrificing the guarantees against corruption.

After the meeting a private discussion between A.B., C.D., and the new project manager took place. Both reviewers criticized the situation of the project and they said that the quality of the software was unacceptable. The manager said that the performance of his company was not below average. He added that this was typical Balmedan software quality. He boldly declared that he was not be willing to spend more than average resources, because if he did so, his company would loose its position in the internal market. Later in the day both A.B. and C.D. received a phone call from their colleague E.F. He said that one of the managers of WFC had called him and asked for the patience and tolerance of the reviewers w.r.t the project.

4.4 Testing

A week later A.B. and C.D. were granted remote access to the system, as they had required. They started a kind of unofficial testing and spent 2-3 days in trying to make an exhaustive search in the different menus and branches of the system. Since they were not real experts in GPO operations they were unable to find any major logical errors (similar to the one mentioned by the GPO employee in the last meeting). However, they found that safeguards to prevent erroneous and double data entries were largely missing. They also found several input sequences, which made the system crash. Then they produced a detailed report with all their findings, including the error conditions.

A few days later the first "public" tests took place. It involved actual GPO employees as testers according to the contract. The tests were conducted in the premises of BAST. A sample of 20 GPO employees from five different offices were seated in front of an equal number of terminals. A BAST representative distributed around 50 test sheets of paper. Each sheet described a single test. Then he instructed them to perform each test step-by-step at the same time. At the end of a test they signed the corresponding sheet and wrote a "pass" verdict. The testers were not allowed to conduct their own tests, but even if they were allowed to, most of them would not know what to do. Their experience with computers was limited and they were not aware of the capabilities of the system, which they actually saw for the first time.

Load and stress testing were among the last tests to be conducted before pilot installation in selected GPO offices. Although these tests were mandatory according to the contract, they were insufficiently described in the testing deliverable. One test for each kind test type was performed by using an automated tool. In the next deliverable, which gave an account of all tests (save the tests which were independently conducted by A. B, and C.D.), the results of the load test were astonishing. The more the system was loaded, the better it seemed to perform.

A month later a system beta version was installed in selected GPO offices. A few more errors were located and some last corrections were made. BAST was awarded an education (of GPO employees) and maintenance contract, which assured that unexpected user behavior would be minimized and future problems would be solved. The normal operation of the system started right after the pilot phase.

A few months later a citizen's project was approved by the GPO and he received a notice to pay €1000 for the license. He was assured by the system that a discount of 10% was applicable on immediate payments. He duly transfered €900 from his bank account to the GPO. A month later he received a notice to pay €400 more. He paid a visit to the GPO in trying to find an explanation. He was informed that he had paid only €900 of the total €1100 he originally owed and that the rest €200 was a fine because the payment was overdue. Two hours later a local office employee eventually understood and admitted the mistake. The discount was added to the original sum instead of being subtracted. He said, "alright, this is no big deal. Pay the €400 now, so that you are not fined again by the computer, and within six month time we shall manually correct the mistake and reimburse the money."

5 Analysis and Conclusions

It could be easily argued that, as in the case of Vasa [6], every single rule of good software production was broken. Requirements were incomplete, they were definitely not fixed before proceeding with development, process re-engineering was omitted, development was done in a rather ad hoc manner, and testing was minimal and erratic. However, and in contrast with the Vasa story, (a) we have a better knowledge of both the story and the environment, and (b) the architects of the system cannot plead ignorance. While Vasa was an innovative ship (in the Swedish environment at least) the GPO system was a rather common e-government system. Among other arguments, which allowed BAST to be awarded the contract, was its extensive experience with e-government projects.

Not only general software development rules were broken, but also specific requirements of the contract. However it is fair to say that Balmedan calls for bids often involve too strict and grandiose requirements, which give an air of impartiality and seriousness to the call. Such requirements also repel some contestants, who think that they are impossible to satisfy. In short, the collection of information of all local offices was rather far fetched. On the contrary, an inspection of a representative sample of offices would be both sufficient and necessary.

Why did the project manager object putting enough human resources into the project? Was the funding insufficient? In fact the funding of Balmedan projects is rarely insufficient. However, rumors exist that the budget is not always consumed for the project per se.

Does the inclusion of strict reviewers improve the final outcome? In as much as their suggestions concern minor details, which can be patched easily, there is some improvement. However, suggestions with serious consequences (e.g. the one stop shopping approach, or the restructuring of processes, or the suggestion for detailed testing) are set aside. Actually in a corrupt environment strict reviews, even if they are sincere, can further reinforce corruption. They can be used as an argument to increase protection money. Effectively this decreases the actual funding of the project.

Is there a lack of education in Balmeda? Each year some thousands of software engineers and computer experts are produced by its higher education. Why do they not apply the principles they have learnt? Obviously for two reasons at least: (a) Because they have a limited resources (time and money) to produce an outcome, and (b) low quality personnel is often hired.

What is the the role and negotiation power of private IT vendor firms and policy networks, and what is the way these actors influence the government policy-making processes, in the case of e-government projects [5]?

Finally, why does the Balmedan society tolerate an e-government quality that degrades public services and the quality of life in general? First of all the bulk of the population has never seen a better quality, with which to establish a measure of comparison. Second, as it was said in the beginning of the paper, the average Balmedan citizen keeps in himself an image of a rather hostile state, which provides minimum care and bad services. Not only are his expectations low, but he also thinks that his interests are best protected when a faulty e-government system exists. In such an incomplete environment there are ways to hide himself and opportunities to negotiate with representatives of the state face to face. Of course, since everything must be built on a thin infrastructure, making business in Balmeda is more expensive than elsewhere and life quality is only supported by the mild climate.

References

1. Avgerou, C.: Information Systems in Developing Countries: a Critical research Review. LSE Working Paper Series, No. 165 (2007)
2. Heeks, R., Bailur, S.: Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. Government Information Quarterly 24(2), 243–265 (2007)
3. Gil-Garcia, J.R., Pardo, T.A.: E-government success factors: Mapping practical tools to theoretical foundations. Government Information Quarterly 22(2), 187–216 (2005)
4. Ayyad, M.: E-government informatics. In: Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance, pp. 31–38 (2008)
5. Yildiz, M.: E-government research: Reviewing the literature,limitations, and ways forward. Government Information Quarterly 24(3), 646–665 (2007)
6. Fairley, R.E., Willshire, M.J.: Why the Vasa Sank - 10 Problems and Some Anecdotes for Software Projects. IEEE Software 20(2), 18–25 (2003)
7. Garson, G.D.: Information systems, politics, and government: Leading theoretical perspectives. In: Garson, G.D. (ed.) Handbook of public information systems, pp. 591–605. Marcel Dekker, New York (1999)
8. Goldstein, H.: Who killed the virtual case file? [case management software]. IEEE Spectrum 42(9), 24–35 (2005)
9. Brailsford, H.N.: Macedonia. Methuen & Co., London (1906)
10. Laplante, P.A., Neill, C.J.: The Demise of the Waterfall Model Is Imminent and Other Urban Myths. IEEE Queue 1(10), 10–15 (2004)
11. Wilson, C., Harsha, P.: Advising Policymakers is more than just Providing Advice. Communications of the ACM 51(12), 24–28 (2008)

A Prototype System for Electronic Data Interchange among Registrar's Offices of Different States

Igor Metz[1], Adrian Blöchlinger[2], and Alexandros Varveris[3]

[1] GLUE Software Engineering AG, Zieglerstrasse 34, CH-3007 Bern, Switzerland
[2] Federal Office of Justice, Bundesrain 20, CH-3003 Bern, Switzerland
[3] University of Athens, Asklipiou 9 Street, 10679 Athens, Greece

Abstract. This work presents a prototype system that enables electronic integration of civil status records of the International Commission on Civil Status (ICCS) member states; the pursued issues are involving civil status matters for citizens of member states through their respective Registrars' Offices organization. Phase 1 of the prototype system is presented together with the technical feasibility securely to exchange messages among civil status offices as well as to assure message integrity, authenticity, confidentiality and non-repudiation.

Keywords: Civil Status, ICCS, CIEC, Electronic Data Interchange, Registrars' Office, e-government, e-participation, Civil Status certificates.

1 Introduction

Governmental initiatives on electronic information require a high-level set of standards in order to cover a large spectrum of services. It is also necessary to produce design parameters that will ensure data security, privacy, reduction of paperwork and free data access [1, 2].

Currently, messages between civil status offices have been exchanged on front and a back side paper forms, where the front side holds the labeled fields written in several languages, usually in the language of the sending country and in French, the latter being the official diplomatic language. The fields are numbered on the front of the message, having the translations and some explanatory articles of conventions [3] on the back side in order to facilitate the reader. Such a form is referred to as "formule plurilingue" by the International Commission on Civil Status (ICCS or Commission Internationale de l'État Civil) [4], an intergovernmental organization since 1948, aspiring the promotion of international cooperation on civil status matters while improving national authorities collaboration on the subject. The Commission concluded to address the arising needs with a computer system designed for the exchange of information on civil status matters in the various ICCS member countries and to resolve the resulting problems.

To date, each of the participating countries has designed individual forms. These forms differ in the language used on the front page, whereas some may include supplementary fields. Currently, the ICCS is working on a system of label codes, which allows searching the individual translations of a label within a multilingual dictionary

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 270–278, 2010.

which will render the translations on the back side useless. Also, it endeavours to limit the language of the system to French in addition to the language used by the sender.

In the present work, the term 'civil status' contains all the attributes assigned to an individual in accordance to civil law, namely citizenship, marriage, paternity, relations, name, residence, legal endowment, and sex. Consequently, the term 'civil status' includes the administrative mechanism for registering authentic personal records. Additionally, ICCS aims at establishing a platform for a world-wide secure electronic interchange of civil status messages in-between participating civil status offices. The following figure shows an overview of the final target architecture of the ICCS platform (Fig. 1).

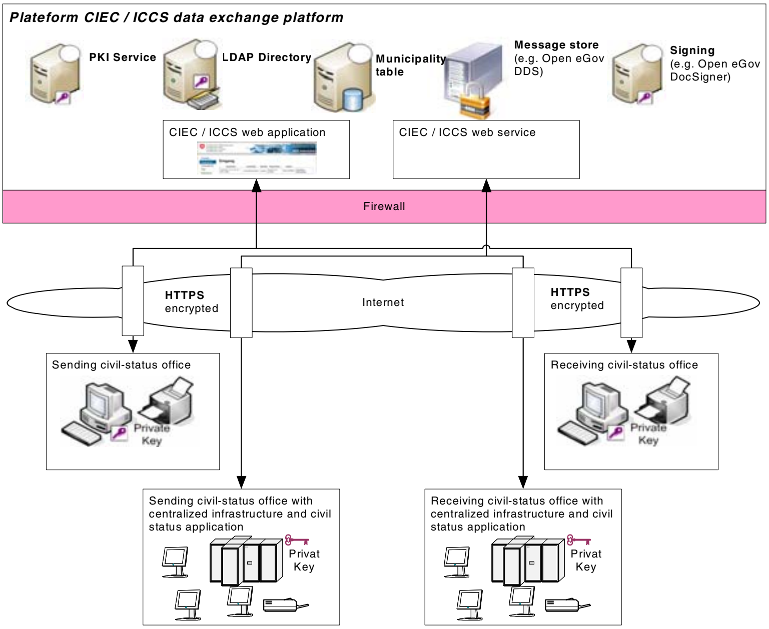

Plateform CIEC / ICCS data exchange platform
PKI Service
LDAP Directory
Municipality table
Message store (e.g. Open eGov DDS)
Signing (e.g. Open eGov DocSigner)
CIEC / ICCS web application
CIEC / ICCS web service
Firewall
HTTPS encrypted
Internet
HTTPS encrypted
Sending civil-status office
Private Key
Receiving civil-status office
Private Key
Sending civil-status office with centralized infrastructure and civil status application
Privat Key
Receiving civil-status office with centralized infrastructure and civil status application
Privat Key

Fig. 1. Overview of the ICCS Platform Target Architecture

The proposed platform is planned to be realised in several phases which are:

Phase 1: A prototype [5], supporting Death and Free Text messages. The goal of this phase is to display the secure electronic interchange of messages, giving a special attention to the feature of authentication of users using digital certificates, and the signing and en-/decrypting of messages.

Phase 2: Introduction of the LDAP (Lightweight Directory Access Protocol) directory [6], municipality table, PKI (Public Key Infrastructure) [7]. Also, support of three to five additional ICCS forms and one or two additional languages.

Phase 3: Introduction of an online registration process and application. Also, support of five to seven additional ICCS forms and three or four additional languages.

Phase 4: Support of remaining ICCS forms and languages, optimisations, and transfer to operational environment.

This paper intends briefly to describe the system as already built in the context Phase 1. It employs a service-oriented architecture and emphasises on the reuse of pre-existing components provided by the Swiss Federal Administration [8].

2 Overview

Figure 2 presents an overall view of the ICCS Phase 1 platform. As envisaged, the final platform will be using a centralized architecture, where all the messages are exchanged via one central hub system, supported only by human users. In regard to the civil status applications worldwide, these will be integrated in later phases.

The ICCS platform is designed to be secure. Message authenticity, integrity, confidentiality and non-repudiation are technically enabled by the signing and encrypting all messages. However, the quality of the used certificates is crucial, and only certificates with sufficient quality can guarantee the above security requirements.

The ICCS Phase 1 platform uses its private OpenSSL installation to create the necessary public/private key pairs and certificates [9]. This is considered sufficient for the purpose of a prototype. For the succeeding phases a fully fledged PKI is foreseen.

The said system can be accessed by authorised users through personal digital certificates. The ICCS platform, in particular the ICCS web application, has to support all languages of the participating countries, and it is possible to extend the platform for additional languages just by providing the relevant textual resources.

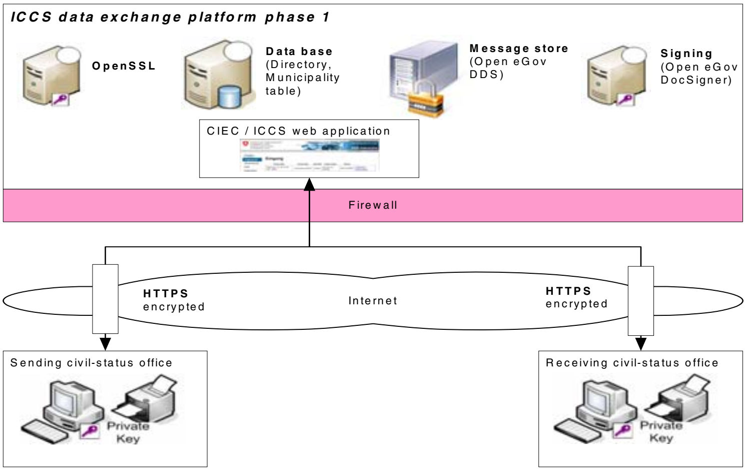

ICCS data exchange platform phase 1
OpenSSL
Data base (Directory, Municipality table)
Message store (Open eGov DDS)
Signing (Open eGov DocSigner)
CIEC / ICCS web application
Firewall
HTTPS encrypted
Internet
HTTPS encrypted
Sending civil-status office
Private Key
Receiving civil-status office
Private Key

Fig. 2. Overview of the ICCS Phase1 platform

3 System Architecture

This section gives a more detailed view of the building part of the system architecture of the ICCS Phase 1 platform. Some of the components have been built to provide a minimal functionality as needed for this phase, while others are already fully functional. The components of the systems are based in Java enterprise applications, which run in a Java EE container.

The *ICCS Web Application*: This provides the user interface for human platform users, which are the clerks of the civil status offices. It is accessed via HTTPS using mutual authentication, i.e. both the server and the client are identified using digital certificates. For this purpose, the user certificates are stored on the server-side.

The *ICCS Core*: This contains the business logic of the ICCS platform. The core functionality has been isolated in a separate component in order to allow an easy integration with an ICCS Web Service in later phases.

The *Database:* The ICCS Phase 1 platform uses a central database for the following purposes:

- Storing user and office information as well as the certificates. Here, the users and offices are organised in the form of a tree having the following structure: ICCS/<country>/<office>/<user>, where the ICCS is the root node (Fig. 3). It has a sub-node for each participating country, the country nodes containing office nodes, which in turn contain the user nodes.
- Storing of process cards, inbox, sent and read box per office.
- Storing of the ICCS label codes and the label texts in all necessary languages. In Phase 1 we support four languages, namely, English, French, German, and Greek.
- Access to the database is always performed through abstract interfaces.
- The interface IDirectory provides the look-up interface for user and office certificates, in addition contact information, such as e-mail addresses of users and offices, etc.
- The interface IMunicipality provides the look-up interfaces for the civil status offices and the type of messages an office may send or receive. In Phase 1 this is simply another interface to the directory.
- The interface IFormTexts provides the label codes and the texts used within the PDF message documents in the necessary languages.

The *Document Delivery Service (DDS), Message Store*: This is used to store the messages in a secure manner. All messages are encrypted and may be decrypted and read only by the intended recipient. The DDS provides interfaces to supply and deliver messages and to notify the ICCS Core about any events concerning the stored messages (download, expiration, deletion).

Finally, the DDS notifies the recipient civil status office by e-mail, if there are new messages to be downloaded.

DDS is a generic service of the Open eGov platform [10] and is available as an open source component under GPL (General Public License).

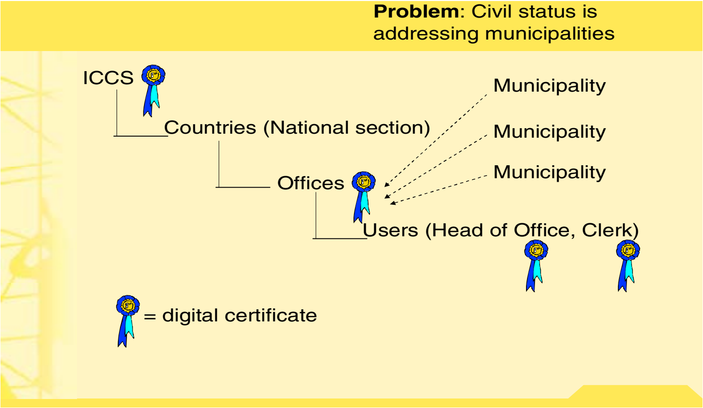

Problem: Civil status is addressing municipalities
ICCS
Countries (National section)
Offices
Users (Head of Office, Clerk)
Municipality
Municipality
Municipality
= digital certificate

Fig. 3. Organisational structure of the ICCS Platform

The *Doc Signer*: This component provides the functionality to sign the PDF messages locally. For this purpose, a signed Java applet is downloaded to the clerk's local browser. The applet loads the document to be signed by the ICCS Web Application server to the local machine, searches the clerks to locally install the certificate and performs the signing process, including the query for the clerk's certificate PIN (Personal Identification Number).

The Doc Signer [11] is a generic component of the Open eGov platform. It is available as an open source component under GPL.

The *Content Management System (CMS)*: The ICCS Web Application is using a CMS from where all static pages, labels, texts, images, etc. are retrieved. In Phase 1 this integration has been kept very simple.

The *Application Container*: The Glassfish [12] open source application server is used as the runtime environment for the platform**.**

The *OpenSSL Public Key Infrastructure (PKI)*: The ICCS platform is using certificates for user and office authentication and authorisation, as well as for message encryption and message signing. The certificates are issued by a dedicated PKI. In Phase 1 this PKI is realised using an OpenSSL installation on the platform.

The ICCS platform uses PKCS#11 (Public Key Cryptography Standards) [13] hard and PKCS#12 [14] soft certificates for its purposes. Soft certificates are issued by the ICCS (ICCS Certification Authority)

Each clerk has a personal certificate for authentication. This can be a soft certificate provided by the ICCS CA (Certification Authority) or an already existing hard certificate, which is accepted by the ICCS platform.

Each participating civil status office has a soft certificate for addressing.

The ICCS platform itself uses a soft certificate to sign the messages in the XML (Extensible Markup Language) form.

4 Message Structure and Signing

Messages, whose, authenticity and integrity is ensured through several signatures, are transmitted as zip files. Fig. 4 shows the structure of such a zip file and how it is assembled.

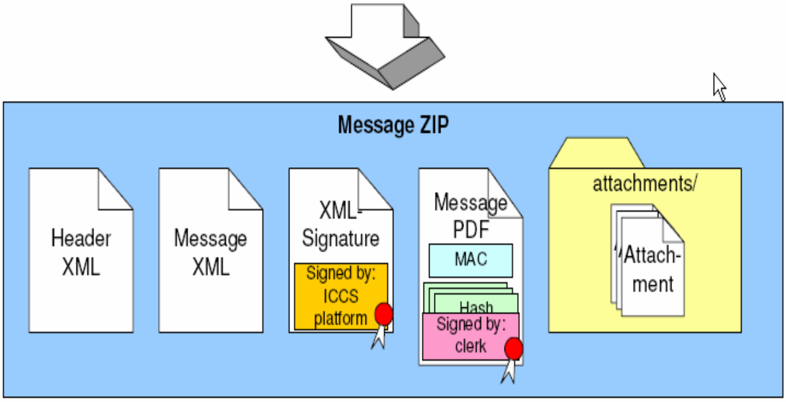
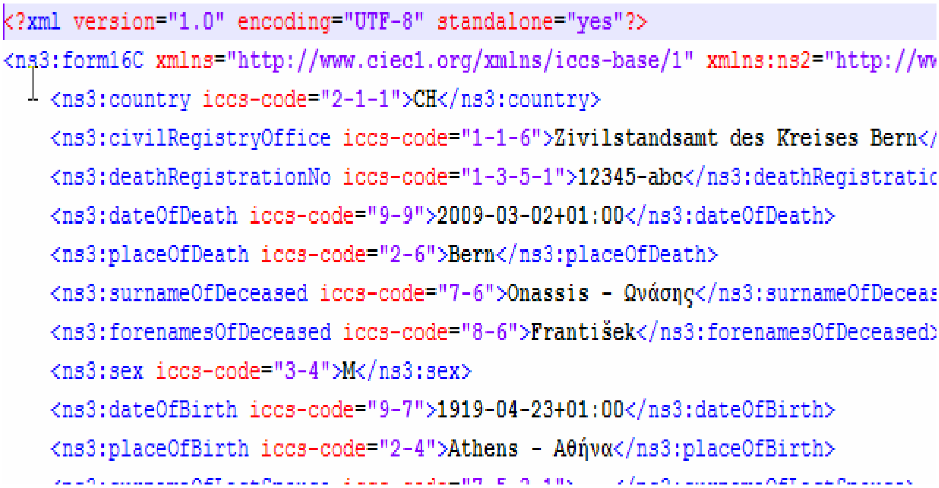


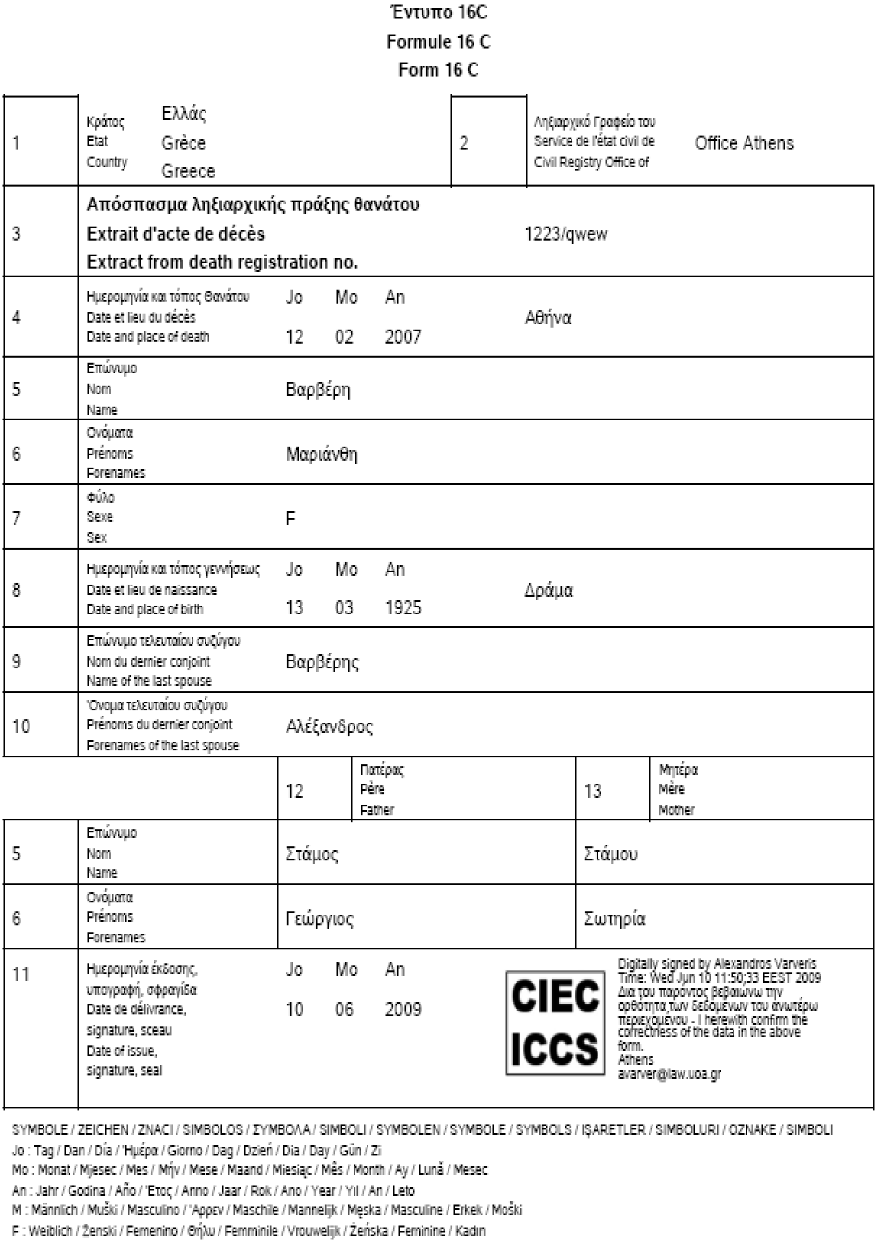
Fig. 4. ZIP Message structure

The base of a message is an XML document containing all the business case specific data entered by the clerk during data capturing (e.g. Fig. 5). Additionally, the clerk may also provide a set of attachment documents. The list of attachments and an optional comment per attachment is also part of the XML document.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns3:form16C xmlns="http://www.ciec1.org/xmlns/iccs-base/1" xmlns:ns2="http://ww
    <ns3:country iccs-code="2-1-1">CH</ns3:country>
    <ns3:civilRegistryOffice iccs-code="1-1-6">Zivilstandsamt des Kreises Bern</
    <ns3:deathRegistrationNo iccs-code="1-3-5-1">12345-abc</ns3:deathRegistratic
    <ns3:dateOfDeath iccs-code="9-9">2009-03-02+01:00</ns3:dateOfDeath>
    <ns3:placeOfDeath iccs-code="2-6">Bern</ns3:placeOfDeath>
    <ns3:surnameOfDeceased iccs-code="7-6">Onassis - Ωνάσης</ns3:surnameOfDeceas
    <ns3:forenamesOfDeceased iccs-code="8-6">František</ns3:forenamesOfDeceased>
    <ns3:sex iccs-code="3-4">M</ns3:sex>
    <ns3:dateOfBirth iccs-code="9-7">1919-04-23+01:00</ns3:dateOfBirth>
    <ns3:placeOfBirth iccs-code="2-4">Athens - Αθήνα</ns3:placeOfBirth>
```

Fig. 5. XML Message structure



Έντυπο 16C
Formule 16 C
Form 16 C

1	Κράτος Etat Country	Ελλάς Grèce Greece	2	Ληξιαρχικό Γραφείο του Service de l'état civil de Civil Registry Office of	Office Athens
3	**Απόσπασμα ληξιαρχικής πράξης θανάτου** **Extrait d'acte de décès** **Extract from death registration no.**		1223/qwew		
4	Ημερομηνία και τόπος θανάτου Date et lieu du décès Date and place of death	Jo Mo An 12 02 2007	Αθήνα		
5	Επώνυμο Nom Name	Βαρβέρη			
6	Ονόματα Prénoms Forenames	Μαριάνθη			
7	Φύλο Sexe Sex	F			
8	Ημερομηνία και τόπος γεννήσεως Date et lieu de naissance Date and place of birth	Jo Mo An 13 03 1925	Δράμα		
9	Επώνυμο τελευταίου συζύγου Nom du dernier conjoint Name of the last spouse	Βαρβέρης			
10	Όνομα τελευταίου συζύγου Prénoms du dernier conjoint Forenames of the last spouse	Αλέξανδρος			
		12	Πατέρας Père Father	13	Μητέρα Mère Mother
5	Επώνυμο Nom Name	Στάμος		Στάμου	
6	Ονόματα Prénoms Forenames	Γεώργιος		Σωτηρία	
11	Ημερομηνία έκδοσης, υπογραφή, σφραγίδα Date de délivrance, signature, sceau Date of issue, signature, seal	Jo Mo An 10 06 2009	CIEC ICCS	Digitally signed by Alexandros Varveris Time: Wed Jun 10 11:50:33 EEST 2009 Δια του παρόντος βεβαιώνω την ορθότητα των δεδομένων του ανωτέρω περιεχομένου - I herewith confirm the correctness of the data in the above form. Athens avarver@law.uoa.gr	

SYMBOLE / ZEICHEN / ZNACI / SIMBOLOS / ΣΥΜΒΟΛΑ / SIMBOLI / SYMBOLEN / SYMBOLE / SYMBOLS / IŞARETLER / SIMBOLURI / OZNAKE / SIMBOLI
Jo : Tag / Dan / Día / 'Ημέρα / Giorno / Dag / Dzień / Dia / Day / Gün / Zi
Mo : Monat / Mjesec / Mes / Μήν / Mese / Maand / Miesiąc / Mês / Month / Ay / Lună / Mesec
An : Jahr / Godina / Año / 'Έτος / Anno / Jaar / Rok / Ano / Year / Yıl / An / Leto
M : Männlich / Muški / Masculino / 'Άρρεν / Maschile / Mannelijk / Męska / Masculine / Erkek / Moški
F : Weiblich / Ženski / Femenino / Θήλυ / Femminile / Vrouwelijk / Żeńska / Feminine / Kadın

Fig. 6. A signed PDF Message

For transmission, the ICCS platform generates an individual platform XML signature [15] for the XML message document using the platform certificate, and also calculates an individual hash value for each of the attachments. As for the next step, the platform transforms the original XML document, the platform signature value and the attachment hash values into an equivalent PDF document. This document is presented to the clerk for validation. Once accepted by the clerk, the PDF document is signed with the clerk's personal certificate (Fig. 6).

In such described way, the PDF document can always be traced to the original XML document and to the clerk, who sent the message.

The XML document, the platform signature, the signed PDF document and the attachment documents are packed into a ZIP file. The attachments and their respective signatures are put into a subfolder named "attachments".

Finally, an XML header document is added. This document contains the following transport information:

Sender Id: ICCS participant identifier of the sending office.

Recipient Id: ICCS participant identifier of the recipient office.

Message type: The business case type, i.e. 1603 for death message, or 0 for free text.

Message identifier: ICCS platform Referenced message identifier for replies only.

Date of sending.

Unique identifier of the message (UUID).

Subject: e.g. the business case type and some kind of case id, such as the name of the person involved.

The header document is not signed; however, it is transmitted in an encrypted form, as the whole ZIP container is transmitted in an encrypted form.

5 Conclusion

The International Commission on Civil Status (ICCS) platform Phase 1 discussed above has successfully created a fully operational prototype system enabling electronic integration of civil status records in-between four member states. The next phases will include additional member states inporting supplementary civil status forms that will serve the community. The above mentioned work intends to provide easily accessible information and to lessen bureaucracy for the benefit of citizens.

Acknowledgment

The authors wish to express their appreciation to the Swiss Open eGov project team for their assistance.

References

1. Varveris, A.G.: Electronic data interchange among the Registrar's Offices of different countries. In: Proceedings of 2nd Conference entitled Electronic democracy - challenge of digital era, Scientific Council for the Information Society, Athens, pp. 191–204 (2006)

2. Varveris, A.G., Tsouca, Ch., Papatheodorou, Ch.: Electronic data interchange among the Registrar's Offices of different states: Technical standards and administrative consequences, Revue Hellenique de Droit International, Sakkoulas Editions, pp. 283–311 (2005)
3. Commission Internationale de l'Etat Civil (C.I.E.C.), http://web.lerelaisinternet.com/CIECSITE/ListeConventions.htm
4. International Commission on Civil Status (ICCS), http://www.ciec1.org/
5. CIEC Platforme - ICCS Platform Wiki, http://www.ciec-plateforme.org/wiki/display/platformpublic/Home
6. The OpenLDAP Project, http://www.openldap.org/
7. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W.: RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008), http://www.ietf.org/rfc/rfc5280.txt
8. Swiss Federal Administration, http://www.admin.ch/ch/index.en.html
9. The OpenSSL project, http://www.openssl.org/
10. The Open eGov Project, http://www.e-service.admin.ch/wiki/display/openegov/Home
11. Open eGov DocSignerService, http://www.e-service.admin.ch/wiki/display/suispublic/Open+eGov+DocSignerService
12. The GlassFish Community open source software, https://glassfish.dev.java.net/
13. RSA Laboratories Inc., PKCS #11 v2.20 Amendment 3 Revision 1 Additional PKCS#11 Mechanisms (2007), ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20a3.pdf
14. RSA Laboratories Inc., PKCS 12 v1.0: Personal Information Exchange Syntax (1999), ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
15. XML Signature Syntax and Processing (Second Edition) (2008), http://www.w3.org/TR/xmldsig-core/

e-Government for Development Information Exchange (DIE): Zambia

Bwalya Kelvin Joseph

University of Botswana, Corner Mobutu / Notwane Road, Gaborone,
Private Bag UB0073, Gaborone, Botswana
Tel.: +267 355 4109; Fax: + 267 318 5098,
kelvin.bwalya@mopipi.ub.bw

Abstract. In most parts of the world, political systems which utilize authoritative rule and mostly employ top-down decision-making processes are slowly transcending towards democratic norms. Information Technology Systems have been identified and adopted as one of the most efficient vehicles for appropriate, transparent and inclusive / participatory decision making. Zambia has shown a higher propensity to indigenous knowledge systems which are full of inefficiencies, a lot of red tape in public service delivery, and prone to corrupt practices. Despite that being the case, it is slowly trying to implement e-government. The adoption of e-government promises a sharp paradigm shift where public institutions will be more responsive and transparent, promote efficient PPP (Public Private Partnerships), and empower citizens by making knowledge and other resources more directly accessible. This paper examines three cases from Zambia where ICT in support of e-government has been implemented for Development Information Exchange (DIE) – knowledge-based decision making. The paper also assesses the challenges, opportunities, and issues together with e-government adoption criteria regarding successful encapsulation of e-government into the Zambian contextual environment. I propose a conceptual model which offers balanced e-government adoption criteria involving a combination of electronic and participatory services. This conceptual e-government adoption model can later be replicated to be used at the Southern African Development Community (SADC) level given the similarity in the contextual environment.

Keywords: E-Government, DIE, e-participation, Zambia, policy-making, ICT, decentralization.

1 Introduction

Throughout the whole world, there has been a paradigm shift where governments and other independent policy/law makers have realised the importance of e-government as a strong tool for responsive governance. Traditionally, many governments have been using paper-and-file approaches in running their day-to-day businesses and this has proved disadvantageous in as far as resource accountability is concerned. With the changing landscape where the majority of government's transactions with citizens,

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 279–292, 2010.

businesses and private partners take place at the local level, it is imperative that much effort be devoted towards putting in place mechanisms which allow maximum collaboration and participatory governing. The paradigm shift in way of governance has been brought about also partly by the rapid growth in Information and Communications Technologies (ICT) which has potential to transform the generation and delivery of public services by public institutions.

Along with other countries throughout the world, African governments have understood and appreciated the contribution of e-government to the government agenda. At the moment, strategic plans have been initiated in Egypt, Senegal, Mozambique, South Africa and Kenya. Although, a claim cannot be made that all of African leaders have understood the importance of e-government, a handful of them have accepted the notion of e-government and have recognised that this concept has come to stay if Africa were to compete favourably in global economic value chains. The African continent as a whole cannot be excluded from this paradigm shift of e-government. This can be substantiated by the communiqué which was released by the 4th African Development Forum (Addis Ababa, October 2004) and reads in part:

> *'E-governance ..... is an important innovation for enhancing good governance and strengthening the democratic process and can also facilitate access to information, freedom of expression, greater equity, efficiency, productivity, growth and social inclusion. Successful e-government initiatives can have demonstrable and tangible impact on improving citizen participation and quality of life as a result of effective multi-stakeholder partnerships.........'*

This consensus statement further proves that policy makers in Africa do understand the need for massive engagement of ICT in their governance paradigms in order to be competitive enough in as far as nations' resource accountability is concerned.

Thus, it is right to state that e-government has the potential to improve public service delivery by public institutions towards transparency, accountability and responsiveness, promote collaborative and joint-up administrations in which other stakeholders in the government business can access services through portals or 'one-stop-shops. E-Government also has the potential to enhance the decentralization reforms by bringing decision making closer to the doorsteps of ordinary citizens by collaborative reasoning made possible with the use of ICT.

ICT in the context of e-government is looked at as a portal for information exchange or a platform through which decisions can be made. The growth of the internet has had a transformational effect on the global society making information and services accessible in ways that were not conceived, let alone imagined, just some 30 years ago. Further, the use of the internet and web tools for supporting participatory actions in legislative processes, political or societal decision-making in governmental or communities' context, but also user friendly electronic government services is becoming a common practice, described by the general term *e-Participation*. With regards to e-Participation, many tangible issues suffice; such as are the e-government platforms trusted? What are the security levels in these platforms? Are they user-friendly? What are the issues of privacy? How to organize and present the content to the user? The other issue of great concern is the issue of ICT infrastructure: is the infrastructure advanced enough to handle advanced applications that are evident in government departments? e-Participation discusses the Critical Success Factors

(CSFs) of e-government. The CSFs considered in this paper are tailored according to the local context (Zambia). These are identified after having identified the challenges that have been met in implementing e-government programs such as e-Voting, traffic on government's websites if there are any, government knowledge and information portals, etc.

It is assumed that governments lie at the centre of driving the development agenda of any one country. In this regard, e-government facilitates a fast track development highway by facilitating information exchange between/amongst the different stakeholders. This brings us to look at e-government as a medium for Development Information Exchange (DIE) where information is freely and largely available for informed decision/policy-making. This paper highlights the important challenges, issues and opportunities that determine the adoption of e-government in Zambia. As aforementioned, three case studies are visited to acquaint the leaders with the current status of the e-government readiness environment in Zambia.

The rest of the paper is organized as follows: section 2 covers the literature review from recent studies that have been covered in the content of e-government implementation and adoption; section 3 looks at the challenges, issues and opportunities that avail themselves for Zambia's e-government initiatives. Three cases are identified: the ZAMLII information portal, the Integrated HMIS, and the Zambia Health Management Information System. After these cases have been looked at, the paper discusses several e-government adoption criteria with much emphasis on the context (Zambia). The conclusion is given at the end of the paper detailing the lessons learnt from the case studies as well as the set of recommendations to make e-government a reality in Zambia.

2 Literature Review

Many studies have defined e-government in different ways: the Bertelsmann Foundation defines e-government as the combination of electronic information-based services (e-administration) with the reinforcement of participatory elements (e-democracy) to achieve the objective of "balanced e-government" [21]. [13] define e-government as the delivery of government information and services online through the internet or other digital means. It is also defined as the delivery of improved services to citizens, businesses, and other members of the society through drastically changing the way governments manage information [17]. Full utilization of e-government will bring a lot of benefits to the management philosophy of many democratic governments and is going to bridge the gap between ordinary citizens and the government. This entails that participatory decision making is going to be achieved and that citizens can collaboratively participate in decision/policy making. This is the case because governments have been viewed as complex, mammoth bureaucratic establishments with a set of information silos that erect barriers to information access and make the provision of services cumbersome and frustrating [10]. E-Government can also result in huge cost savings to governments and citizens alike, increase transparency and reduce corrupt activities in public service delivery. Previous studies have categorized public service delivery in three groups: publishing, interacting, and transacting.

During the past decade, many governments all over the world have embraced the digital revolution to improve domestic and foreign government operations. Having realized the benefits that e-government brings along, many governments the world over have adopted e-government as an effective tool for reaching to its citizens and the other different stakeholders. In general, it is to be mentioned that the growth and development of the internet to what it is today was mainly due to interests by the private sector to conduct businesses on the cyber space. However, nowadays there has been a paradigm shift because even governments are equally interested in using the internet in carrying its day-to-day activities [26].

Despite the huge determination of many governments the world over in implementing e-government, previous studies present mixed cases (failure or success) of implementing and adopting e-government into the socio-economic setup. According to different countries' case studies, there are many challenges and issues that need to be addressed for successful implementation of e-government. E-Governance has shown a lot of maturity in Canada which currently is considered the most developed country in as far as employing of e-government is concerned. This is so because the Canadian government has committed to shaping itself as the government mostly connected to its citizens. Some of the commitments done by the Canadian government have been allocating of a handsome CAD$880 million to support the development of e-government initiatives in Canada [10]. The only bigger challenge that Canada faces is citizen's usage of the available e-government portals, web sites etc. The issues of trust and usability have come in as a barrier to wide-adoption of the e-government in Canada. Previous studies have emphasized website navigability and aesthetics [8], personalization and customization [19] and loyalty programs [17] as key strategies to attracting individuals to visit a website, which, in the context of this discussion are the e-government portals.

In proposing adoption criteria for e-government, [25] proposed a conceptual model with citizen trust as the underlying catalyst for e-government adoption. [4] proposed and tested a model that combines altitude-based and service quality-based approaches. From the literature, it is clear that a number of frameworks founded on the Theory of Reasoned Action and Technology Acceptance model have been utilized to explain the consumer adoption of the internet. The study by [25] proposes perceived risk, perceived behavioral control, usefulness, and perceived ease of use. It defines perceived risk as a fear of losing personal information and fear of being monitored on the internet. The conceptual model proposed ascertains that if an individual had control over how personal information is going to be used, and the control of how and when information can be acquired, then adoption of e-government could be possible. In this model, there was also the power distance which is the distance between the upper and lower castes of the society which states that citizens in higher power distance countries are more likely to adopt e-government that those in lower power distance countries. The other model by [4] brings attitude-based and service-quality-based approaches together. The model outlines the willingness to use e-government services incorporating perceived (confidentiality, ease of use, safety, reliability, visual appeal and enjoyment) and perceived relative benefits. There are three aspects to this model: first, the diffusion of innovation theory which seeks to understand the process through which innovations such as the internet are disseminated in the society; second, the Technology Acceptance Model (TAM) which has roots in Information Systems theory showing how users accept and use a new technology e.g., the Internet; and the Service-Quality-Based (SQB) approach which seeks to understand the antecedents that affect user behavior. It is desired that a novel eModel be composed of four main components: Application architecture, Channels/interfaces, Info-structure, and Regulation [20]. The following diagram shows the architectural components of a novel eModel scenario which e-governments the world over have been using.

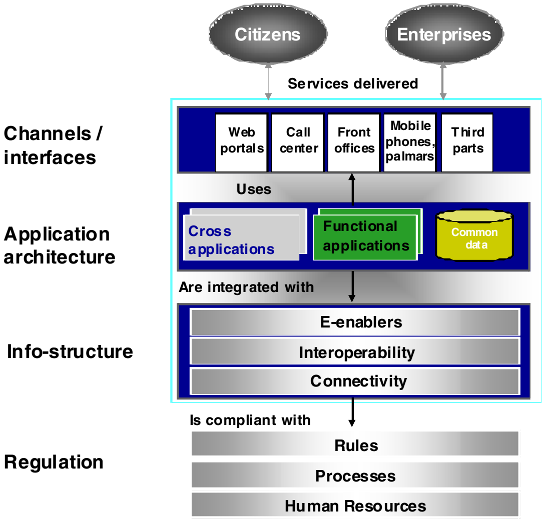


Fig. 1. Basic eModel architectural components (UN e-government report 2002)

An across-the-board analysis of different countries worldwide on the capacity to adopt e-government as a major governing tool depends on a set of factors [15]. The key factors are the country's political will, the availability and strength of their human capital, the ICT (telecommunications) infrastructure, and the presence of administrative priorities. Based on these factors, [20] presents a synthetic 'e-government index' that reflects the 'requisite conditions' that contribute to establishing an enabling environment for e-government. [20] classifies the countries in 4 different groups: High eGov capacity (index = 2.00 – 3.25), Medium eGov capacity (1.60 – 1.99), Minimal eGov capacity (1.00 – 1.59) and Deficient eGov capacity (below 1.00). Zambia is categorized as having deficient eGov capacity with an index of 0.76 below Zimbabwe, Congo, South Africa and Burkina Faso in the Africa category [21]. 2008's E-Government Readiness Index shows Zambia occupying 158th position out of 182 countries surveyed with an e-readiness Index of 0.22 out of 1 [21]. Zambia has just introduced itself in the world of e-government. It is known that in 2005, the country's government literally had no online presence [21]. An excerpt from the table showing E-readiness data for 2008 shows Zambia pitted against the leading nation as follows:

Table 1. E-Government readiness Index and Metrics (2008) – [UN e-government Report - 2008]

Rank	**Country**	**Web Measure Index**	**Infrastructure Index**	**Human Capital Index**	**E-government Readiness Index**
`1	Sweden	0.9833	0.7842	0.9776	0.9157
`2	Denmark	1.0000	0.7441	0.9933	0.9134
	⬇				⬇
`157	Djibouti	0.1137	0.0202	0.5531	0.2279
`158	Zambia	0.0000	0.0316	0.6569	0.2266

According to the same survey [21], the United States of America scored a complete 1.0 on the e-participation index, closely followed by South Korea with 0.9773. This was primarily due to its strength in e-information and e-consultation. Zambia's neighbor, Mozambique, came out as the top African country on e-participation out of all the countries surveyed at position 16 with e-participation index of 0.43178.

Out of this scenario in the standing of Zambia in the world with regards to e-participation and e-government, and the different studies which have shown that different models can be applied to different environments with different specifications, we need to design a tailor-made conceptual model specifically for Zambia and similar environments (e.g. SADC countries). This paper proposes a conceptual model that is going to weigh the pros and cons out of the models reviewed, get the best approaches and build a model taking into consideration the local context. But before we develop the model, let's review the current e-government status in Zambia by taking a closer look at three e-government projects that were taken in the recent past.

3 Zambia's e-Government Environment: Challenges, Issues and Opportunities

Zambia's government has had the desire to implement e-government as a way to reach to its people with a view of promoting e-participation and e-consultation in the policy/decision-making process with its citizens. Projects have been initiated but have met serious challenges to being adopted by the ordinary citizens. In Zambia's context, usability, trust and ICT infrastructure have acted as the main impediments to e-government adoption. This paper's aim is to suggest a conceptual model that is more accustomed to the e-government uptake status in Zambia at the moment. This model combines the Warkentin et al. and Gilbert and Balestrini models described above. But before we do just that, let us look at three ICT projects (in the context of e-government) that have been implemented in Zambia.

a) Zambia Health Management Information System (ZHMIS)

As a strategic plan towards reaching out to its citizens, the Zambian government through the Ministry of Health contracted Health Partners International (HPI) to set up modern, integrated health management information systems (HMIS) database that would be flexible, user-friendly and able to handle all necessary data sources. This was done in the context of e-government – reaching out to citizens and improving the effectiveness of health care delivery system through the strengthening of HMIS. The HMIS software was acquired to specifically improve health data management. The HMIS software was developed from the manual system and was developed in Access 97. The system had the same screens as the manual HMIS input and output forms and reports. This greatly eased the understanding of the automated system. Automation software also included Microsoft Office 97 Professional edition, Windows 95 operating system, Eudora software for e-mail and Mcafee antivirus software. Computer hardware included Compaq Deskpro 4000 computers, with the following minimum specs, 166mhz pentium processor, 32MB Ram, 1.2gig hard disk capacity, 28.8 kps external modem, 15 inch colour monitor, APC UPS and HP 690c Deskjet printers.

In the pipeline, there is an implementation of the Hospital Information System (at major hospitals countrywide) and Financial and Administrative Management System (FAMS). The HMIS will integrate with the HMIS to provide an online and active information system for the health system.

As in the previous cases, e-government even in HMIS is being looked at as the sole provision of better service to the citizens. The HMIS is being used particularly to help the medical staff in addressing illnesses in a more convenient and appropriate manner. The citizens do not have access to this system. Because of lack of developed ICT infrastructure, health centers that are located in remote places of Zambia do not have chance to benefit from this initiative. The full potential of this system could not be tapped because, in some places which had some ICT infrastructure, the human resources do not have the necessary skills to operate the HMIS. In some districts, there may be even 1 person to manage all the HMIS systems installed at different health centers (Simenda 2009).

b) Zambia Online Legal Information Portal (Zamlii)

Zamlii which is the online Zambian legal information portal is a comprehensive online collection of documents and research relating to Zambian legal and constitutional issues, intended as a legal network for lawyers, judges, academics, students and citizens http://www.zamlii.ac.zm/ . Through this portal, citizens can download documents to their convenience. This site contains up-to-date legal information about Zambia and is highly friendly to even people with limited computer skills.

c) Zambia Immigration Management System (ZIMS)

ZIMS has been implemented by the Zambia Immigration Authority as part of its agenda to provide its services efficiently and therefore contribute a substantial amount of tax returns to Zambia. The need for the authority to introduce this computer-based application was specifically to improve immigration service delivery; reduce the time it takes for the department to issue Permits and Visas and Clearing of persons at the ports of entry by about 50% ultimately reducing the cost of doing business for the applicants in

Table 2. Zambia's e-government initiatives: strengths and weaknesses

	Strengths	**Weaknesses / challenges**
ZIMLII	- Contains up-date legal information - Highly friendly to ordinary citizens (good usability)	- Access restricted to people with internet connectivity
Integrated HMIS (2007 to ...)	- full backing of the Zambian Government and cooperating partners - decentralized platforms - on time responsiveness - used local people during its design phase of the HMIS	- Difficult to mobilize funds for full-scale implementation - Rampant costs in training of local population in the use of the software - Lack of political continuity and commitment from the co-operating partners - Poor-grade procurement of IT equipment - Limited ICT infrastructures at local health centers - Exorbitant fees charged by local ISPs for internet connectivity - Unreliable and no guaranteed donor support for project sustainability.
ZIMS	- Faster processes of applications for VISAs, PERMITs, etc. - Convenient and easy method of accessing s ervices - Anytime, anywhere	- Lack of synergy between ZIMS and the immigration website - Unwillingness of the staff to adopt ZIMS - Limited ICT infrastructure - Shaky sustainability framework of the new system

ZIMS – Zambia Immigration Management System
HMIS – Health Management Information System
MOH – Ministry of Health

the country [18]. In line with this, and with a quest to reach more citizens with this improved service, the authority has opened a website where various services offered by the co-operation can be accessed (http://www.zambiaimmigration.gov.zm). ZIMS is an electronic integrated visa and permit approval system which also has a component of border management within itself just the website. This means the processing of applications for permits and visas is done through ZIMS.

Some of the challenges faced in the full-scale implementation of this project have been the following: a) it was not easy to bring all the staff on board due to education limitations (computer illiteracy), mind set (attitude problems towards computers); b) lack of linkage between the Zambia Immigration Website and ZIMS. This would have created an atmosphere where clients file in queries and monitor the status of their queries; c) there is generally inadequate physical ICT infrastructure at various Immigration Offices and Border Controls in the country to facilitate speedy processing of applications and the efficient handling of travelers (Citizens, tourists and other visitors) at all Borders; d) limitation in the confidence levels of the staff in the new system as it is a IT based system, and how to revamp that confidence; e) lack of trust in the new system by most people, rendering the newly introduced ZIMS platform unreliable; and f) sustainability of the institutional capacity building in ICTs at various departments countrywide.

In summary, the following table outlines the characteristics of the initiatives for e-government taken by the Zambian Government.

The other major setback of these systems is that they concentrate on, and give accessibility to the workers in different departments that have implemented e-government systems. Despite having websites, these websites are used as online information stores rather than as interaction bridges between the government and the people. E-Government in Zambia is much more centered on improving public service delivery, with almost neglecting the collaboration nature (between citizens and the government) of e-government. Put in other words, the e-participation component of e-government is almost completely ignored for the case of Zambia.

4 e-Government Adoption Criteria

Before we understand fully the adoption criteria according to the local context in Zambia, let's consider the following hypothesis which can be either rejected or accepted given a set of conditions (Kumar et al. 2007):

a) *The characteristic feature of "correct" e-government shall be a balanced combination of electronic services and forms of electronic participation. Many decision-makers still concentrate one-sidedly on the provision of electronic services (The case of Zambia).*
b) *E-democracy in the form of specific possibilities for participation must be anchored as a central element in all e-government strategies from the very start. If the modernization of the public sector initially concentrates exclusively on the implementation of electronic services, it will make the subsequent introduction of participatory elements more difficult.*
c) *The implementation of participation-promoting e-government initially increases the complexity of institutional control, inter alia, as a result of the increasing in-*

> *fluence of the citizens and the demands on the service providers in the form of a mix of technical and business management elements.*

These hypotheses are intertwined with the fact that e-participation shall not only contain the provision of services to the citizen (what I call a damp-and-take scenario) but will comprise feedback from the citizens to the government (e-participation). Thus, we can state succinctly that the profound objective of the e-government initiative ought to be the frequent and recurring use of online services by citizens not only for obtaining information but also for interacting with the government in the form of e-participation. [25] described adoption as the intention of citizens to engage in e-government to receive information and request services from the government. [4] measure it as the willingness to use e-government services while Carter and Belanger (2005) measure it as the intent to use e-government services. The model proposed in this paper aims to make an extension of the conceptual model proposed in [10]. In that paper, the model was premised on the belief that e-government adoption is largely shaped by the extent to which the government can provide a rich, engaging, and hassle-free experience that is reliable and can provide higher levels of satisfaction. The model in [10] says for effective e-government adoption, the different attributes to be satisfied are the following: a) User characteristics (perceived risk, perceived control, internet …); b) Website design (perceived usefulness, perceived ease of use (usability); c) service quality; and d) client satisfaction.

As distinct to earlier models which were only unidimensional in nature, [10] looked at e-government adoption as a multi-dimensional construct. However, a careful look at the model presented by [10] reviews that, despite it being multi-dimensional in nature, it

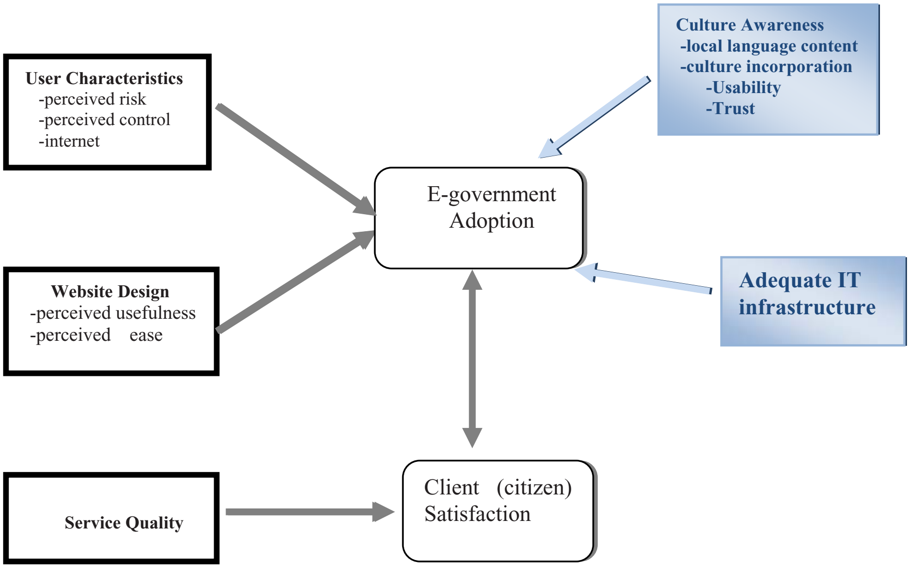


Fig. 2. Proposed e-adoption model

lacks certain attributes thus rendering it not very suitable to be applied for the Zambian case. The figure below represents the different attributes that may be needed for a normal to be suitable for the case of Zambia. Note that some of the explanations of the attributes can be found in [10, 17, 28]. The blue attributes are proposed.

From the case studies outlined in this paper, it is clear that limited ICT **infrastructure is** limiting the number of people accessing digital content presented online on websites. Computers, especially ones connected to the internet, are still hard to come by. The relatively few computers that are found especially in business areas of major cities of Zambia are very expensive to access. This is attributed to the exorbitant rates charged for the internet service by Internet Service Providers (ISPs). Another impediment has also been attributed to the content being presented only in English. Although English is the official language in Zambia, we cannot claim that it is the mostly spoken. The case studies have shown that people continue shunning away from e-government services (mostly the website) because they cannot understand the content presented in them. Simple, properly designed websites to meet the local specifications should be put in place. It is also desired that culture of the local people should be incorporated into the design of these information systems.

Thus, the complete conceptual model this paper is proposing incorporates all the attributes found in the earlier model with the extension of the culture awareness and the need to improve on the ICT infrastructure for the content to be easily accessible. Once the culture content is incorporated into the conceptual model, this will mean that the implementation of the e-government initiative will not only depend on the 'damp-and-take scenario' but will also have e-participation of the citizens as a feedback mechanism for policy/decision making.

5 Conclusions

E-Government is a channel through which the ruling class interacts with its citizens. This creates a win-win relationship where the work of the government is made easier by providing a public service at the disposal of a citizen. Also, time is saved, corruption is reduced and hence transparency and accountability of different resources is promoted. E-Government can also allow the government to timely collect more tax from different sectors of the economy. The citizen benefits by having a say in the policy/decision-making on different issues affecting the country. Efficient service delivery to citizens is also achieved by the employing of e-government.

This paper has looked at different e-government initiatives and conceptual adoption models that have been employed to achieve appropriate e-government. The cases presented from different government (Zambia's) departments employing different e-government strategies suggest that Zambia may not be completely ready to fully implement or replicate the implementation of e-government. There is need to involve the e-participation component of e-government adoption which is to be looked at as e-government for development information exchange (DIE). It is desired that there is a flow of information between the government and different stakeholders involved in the development process. In order to achieve the same, the following recommendations are in order:

1) The government should create an enabling environment for the adoption of ICT in everyday lives of its citizens as this is the start-point of e-government. For the case of Zambia, the government's commitment has been shown by the ICT policy that has been put in place. The only attribute lacking in this case is the follow-up to implementation of the same. It seems all the nice policies are just on paper and implementation is lacking.
2) The government should play a leading role in developing the ICT infrastructure. This can be making sure that the nation's internet backbone and the International Gateway are managed responsibly. Further, the government should encourage developing of fiber-optic network for efficient broadband communication, reducing the rates for internet access through ISPs, and subsidizing the prices for getting Personal Computers (Desktops and Laptops). This can be done indirectly by reducing import duty on internet accessories, computers and computer gadgetry.
3) The government should take full advantage of various initiatives taken by the international community to assist African governments in their bid towards adoption of e-government models such as the Information Technology Center for Africa (ITCA); and the CAFRAD which is Center for Research in Administration and Government. These initiatives basically offer technical support and training (to address HR concerns who are competent enough for change management from paper to electronic form of governing) to different African governments. ZIMS above has shown that even employees in the government department trying to implement e-government can actually reject it.
4) There should be a lot of awareness campaigns sensitizing the ordinary citizens on the benefits of e-government for them to fully adopt it and incorporate it as part of their culture.
5) The development of e-government systems should be funded locally. Over-dependence on foreign (donor) support has its own repercussions (The case of HMIS outlined above). The local people should be part and parcel of developing the system to instill sense of ownership in them.

Zambia presents a case where the transition from pre-colonial practices to contemporary practices has been very slow. There is need to change the pre-colonial administrative culture and mentality which was characteristic for under-resourced and unaccountable bureaucracies. Having outlined Zambia's ignorance of e-participation, it is worth noting that the whole 'package' of e-government is not attained, and if this continues to be the case, the much talked –about benefits of e-government will not be attained. The notion of e-government brings along e-participation which reconfigures relationships between government and citizens (G2C), Government and Businesses (G2B) as well as between governments (G2G). Such kinds of interactions provide a framework where important inputs even in the line of decision-making can be tapped.

There is need to develop appropriate ICT infrastructure and adequately inform the citizens before e-government can be promoted. Zambia has not done enough on the basics and has overridden over necessary steps towards full-scale implementation of e-government. For e-government to thrive in Zambia, there is need that the conceptual model presented here is taken into consideration, and the necessary ICT infrastructure together with appropriate awareness campaigns be put in place.

This paper has further looked at three cases of implementing e-government by different public institutions in Zambia. The cases have shown that there is a lot of discrepancy in the quest to implement e-government systems in Zambia. A conceptual model based on the findings of the three cases, and reference to other models developed thus far, is being suggested. Future works for this study are analyzing more e-government cases for Zambia and comparing them with cases from other countries in the SADC (Southern African Development Community) region. This will bring us to understand the major issues and challenges that are faced in this region in as far as e-government is concerned and how we can overcome these. At the end of such a study, a general conceptual model for the entire region of Southern Africa can be designed. The usefulness of such a model would be to create checks and balances against the implementation of e-government in the SADC region and ascertain whether the SADC strategic framework for the development of e-government is working or not.

References

1. ADF IV, Fourth African Development Forum, Governance for a Progressing Africa, October 11-15, 2004, Addis Ababa, Ethiopia (2004), `http://www.uneca.org/adf/adfiv/adf_4_report_final_sml.pdf` (Accessed 11/03/2009)
2. Joseph, B.K., Angelina, P.: Trust and Confidence for E/M-Commerce Transactions in African States: A Paradigm Shift. In: IST Africa conference proceedings, Maputo, Mozambique, pp. 63–73 (2007)
3. Carter, L., Belanger, F.: The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal 15(1), 5–25 (2005)
4. Gilbert, D., Balestrini, P.: Barriers and benefits in the adoption of e-government. The International Journal of Public Sector Management 17(4), 286–301 (2004)
5. Stephen, C.: African e-Governance – Opportunities and Challenges. University of Oxford, Univ. Press, Oxford (2006)
6. Choudrie, J., Weerakkody, V., Jones, S.: Realising e-government in the UK: rural and urban challenges. The Journal of Enterprise Information Management 18(5), 568–585 (2005)
7. Curtin, G.G., Sommer, M.H., VisSommer, V.: Introduction. In: Curtin, G.G., Sommers, M.H., VisSommer, V. (eds.) The world of e-government, pp. 1–16. The Haworth Political Press, New York (2003)
8. Heeks, R.: Achieving Success/Avoiding Failure in e-government Projects, IDPM, Univ. of Manchester (2003), `http://www.egov4dev.org/success/sfdefinitions.shtml` (Accessed 06/06/2009)
9. Kitiyadisai, K.: The implementation of IT in reengineering the Thai Revenue Department. In: Information Flows, Local Improvisations and Work Practices, Proceedings of the IFIP WG9.4 Conference 2000, Cape Town (2000)
10. Vinod, K., Bhasker, M., Butt, I., Persaud, A.: Factors for successful e-Government adoption: a Conceptual Framework. The Electronic Journal of e-Government 5(1), 63–77 (2007)
11. Mehrtens, J., Cragg, P.B., Mills, A.M.: A Model of Internet Adoption by SMEs. Information and Management 39, 165–176 (2001)
12. MOH Report, Assessment of the Health Information System in Zambia (2007), `http://www.who.int/entity/healthmetrics/library/countries/hmn_zmb_hisassessment.pdf` (Accessed 13/02/2009)

13. Muir, A., Oppenheim, C.: National Information Policy Developments Worldwide in Electronic Government. Journal of Information Science 28(3), 173–186 (2002)
14. Napoli, J., Ewing, M.T., Pitt, L.F.: Factors Affecting the Adoption of the Internet in the Public Sector. Journal of Nonprofit and Public Sector Marketing 7($), 77–88 (2000)
15. Reichheld, F.F., Markey Jr., R.G.: E-customer loyalty – applying the traditional rules of business for online success. European Business Journal 12(4), 173–179 (2000)
16. Shih, H.P.: An empirical study on predicting user acceptance of e-shopping on the web. Information and Management 41, 351–368 (2004)
17. Stiftung, B.: Balanced E-government: E-government – Connecting Efficient Administration and Responsive Democracy. A study by the Bertelsmann Foundation (2002), http://www-it.fmi.uni-sofia.bg/eg/res/balancede-gov.pdf (Accessed 23/04/2009)
18. Rana, T., Tony, E.: Generating Citizen Trust in e-government using a Trust Verification Agent: A Research Note. European and Mediterranean Conference on Information Systems (EMCTS) (2006), http://www.iseing.org/emcis/EMCIS2006/Proceedings/Contributions/EGISE/eGISE4.pdf (Accessed 18/05/2009)
19. Thorbjornsen, H., Supphellen, M., Nysveen, H., Pedersen, P.E.: Building brand relationship online: a comparison of two interactive Applications. Journal of interactive marketing 16(3), 17–34 (2002)
20. United Nations Report, Benchmarking E-Government: a Global Perspective, United Nations Division for Public Economics and Public Administration (2002), http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN021547.pdf (Accessed 22/06/2009)
21. United Nations Report, UN E-Government Survey 2008: From E-Government to Connected Governance, ISBN 978 -92-1-123174-8, UN White paper (2008), http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf (Accessed 22/06/2009)
22. Kennedy, S.: Electronic/Mobile Government in Africa: Progress Made and Challenges Ahead, Addis Ababa, Ethiopia (2009), http://www.unpan.org/emgkr_africa (Accessed 08/04/2009)
23. Venkatesh, V., Morris, M., Davis, G., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Quarterly 27(3), 425–478 (2003)
24. Wangpipatwong, S., Chutimaskul, W., Papasratorn, B.: A Pilot Study of Factors Affecting the Adoption of Thai e-government Websites. In: Proceedings of the International Workshop on Applied Information Technology 2005, Bangkok, Thailand, November 25-26, pp. 15–21 (2005)
25. Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M.: Encouraging citizen adoption of e-Government by building trust. Electronic markets 12(3), 157–162 (2002)
26. White Paper, Hillwatch E-Impact Benchmark and Visitor Pattern Analytics Alignment with Government Web Asset Performance Measurement. Hillwatch Inc. – E-Services, No. 334 Maclaren Street, Ottawa, Ontario, Canada (2006)
27. Wu, G.: Conceptualizing and Measuring the perceived Interactivity of Websites. Journal of Current Issues and Research in Advertising 28(1), 87–104 (2006)
28. Zhu, J.J.H., He, Z.: Perceived Characterisitcs, Perceived Needs,a nd Perceived Popularity: Adoption and Use of the Internet in China. Communication Research 29(4), 466–495 (2002)

Session 8

Education and Training

Semantic e-Learning: Next Generation of e-Learning?

Markellos Konstantinos[1], Markellou Penelope[1], Koutsonikos Giannis[2], and Liopa-Tsakalidi Aglaia[3]

[1] Department of Computer Engineering & Informatics,
University of Patras, 26504 Patras, Greece
kmarkel@cti.gr, markel@ceid.upatras.gr
[2] Department of Business Planning and Information Systems,
Technological Educational Institute of Patras, 26334 Patras, Greece
gkoutson@gmail.com
[3] Department of Mechanical & Water Resources Engineering,
Technological Education Institute of Messolonghi, 30200 Messolonghi, Greece
aliopa@teimes.gr

Abstract. Semantic e-learning aspires to be the next generation of e-learning, since the understanding of learning materials and knowledge semantics allows their advanced representation, manipulation, sharing, exchange and reuse and ultimately promote efficient online experiences for users. In this context, the paper firstly explores some fundamental Semantic Web technologies and then discusses current and potential applications of these technologies in e-learning domain, namely, Semantic portals, Semantic search, personalization, recommendation systems, social software and Web 2.0 tools. Finally, it highlights future research directions and open issues of the field.

Keywords: Semantic e-learning, Semantic Web, Semantic portal, Semantic search, personalization, recommendation systems, social software, Web 2.0.

1 Introduction

In recent years, advances of Information and Communication Technologies (ICTs) and especially the World Wide Web have dramatically affected education. The provision of learning and training over the Web has been widely adopted as a promising solution to lifelong learning and on-the-job training. *E-learning (electronic learning)* stands for all forms of Web-based learning and uses computers and network technologies to create, store, deliver, manage and support online learning courses to anyone, anytime and anywhere [14], [22]. It provides a configurable infrastructure that can integrate learning materials, tools, and services into a single solution for offering training or educational materials quickly, effectively, and economically [58].

Thousands of institutes, universities, organizations, enterprises and schools worldwide have already integrated and are using e-learning applications customised to their requirements, needs and preferences. A particular feature of these efforts is the "on-demand" presentation of learning resources (lessons, exercises, links, etc.) based on multimedia material (text, sound, graphics, video, animation, etc.) and overcoming difficulties in timing, attendance and travelling.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 295–308, 2010.

As the e-learning industry begins to mature, we are seeing products that are far beyond the simple "click-and-read" courses that have characterised the field up to date. Future manifestations of e-learning, including e-learning 2.0 (e-learning based on tools and approaches typical of Web 2.0) [23], will allow reusability and exchanging of learning resources, systematic compilation of online courses from distributing learning content, efficient delivery of learning content in order to enhance learner's knowledge, customization of learning material based on learners' goals, preferences, capabilities, needs, and knowledge, etc. [14]. All these comprise great challenges for the current and future e-learning systems.

To this direction, emerging *Semantic Web technologies* have changed the focus of e-learning systems from *task-based approaches* to *knowledge-intensive* ones [26]. The Semantic Web (SW) is a W3C (World Wide Web Consortium, http://www.w3.org) initiative and according to Berners-Lee et al. [5] comprises *"an extension of the current Web in which information is given well-defined meaning, better enabling computers and people to work in cooperation"*. So, the Semantic Web promises that tomorrow's Web will be a Web of semantics with far greater capabilities than today's Web of text [42]. This means that the documents contain not only content, but also context. The capability of the Semantic Web to add meaning to information, stored in such way that it can be searched and processed and recent advances in Semantic Web technologies provide the mechanisms for semantic knowledge representation, exchange, sharing, reuse and collaboration of e-learning applications [3].

Semantic e-learning is the *"e-learning based on the Semantic Web technologies that can easily provide learning materials in a common format and therefore enhance personalised learning"* [14]. In this context, e-learning systems have the potential to develop descriptions of their processes, as well as rules in order to create content-based and logic-driven information and knowledge value. This ability of representing semantics of knowledge resources (learning objects, lessons, courses, etc.) and their relationship in a standard format can promote the dynamic composition of learning materials and processes and enforce the customization by organizing these resources based on the user's need, such as teacher's preferences or student's profile [30].

The aim of this paper is to argue that Semantic e-learning could be the next generation of e-learning. Firstly, we define Semantic e-learning, explore the literature and all these foundations upon which it is envisioned and demonstrate its close relation with the development of Semantic Web technologies. Moreover, we focus on those directions that support the vision of Semantic e-learning, illustrate the future trends and discuss the open issues in the field.

2 Background

In the majority of past e-learning systems the courses and the educational materials were not dynamic enough, provided a rather restricted feature set or presented complicated structuring and consequently could not respond effectively to the needs and competencies of the learners, resulting in poor online experiences [13]. An answer to this problem that comprises also the current challenge for Web-based learning systems is their enhancement by the integration of adaptive features that allow for the delivery of *personalized learning* [32].

These advanced e-learning applications provide high quality content, efficient structuring, and full support for the varied tasks of all user profiles participating in a typical distance learning scenario. Specifically, depending on the knowledge background of the learner, his strengths and weaknesses, and the preferred learning style and the progress made so far, the system decides what and in which way the content should be presented next. Possible parameters are different learning paths through the content, different ways of presentation of the same content (e.g. with or without audio) or offering a different set of functions which the user interface of the learning system provides to reduce complexity [12], [17].

To achieve this, methods and techniques from various scientific domains and application areas are used. The most well-known are Data Mining, Web Mining, Knowledge Discovery, Knowledge Management, User Modelling, User Profiling, Artificial Intelligence and Agent Technologies, etc. Especially, *Web Mining* is defined as the use of Data Mining techniques for discovering and extracting information from Web documents and services and can be categorised into three areas depending on which part of the Web is mined [27]:

- *Web Content Mining* focuses on the discovery/retrieval of useful information from Web contents/data/documents. Web content data consist of unstructured data (free texts), semi-structured data (HTML documents) and more structured data (data in tables, DB generated HTML pages).
- *Web Structure Mining* focuses on the structure of the hyperlinks within the Web as a whole (inter-document) with the purpose of discovering its underlying link structure. Web structure data consist of the Web site structure itself.
- *Web Usage Mining* mines the secondary data derived from Web users' sessions or behaviours and focuses on techniques that could predict user behaviour while the user interacts with the Web [16]. Web usage data can be server access logs, proxy server logs, browser logs, user profiles, registration data, user sessions or transactions, cookies, user queries, bookmark data, mouse clicks and scrolls, and any other data as the result of interactions.

In the majority of cases, e-learning applications base personalization on *Web Usage Mining*, which undertakes the task of gathering and extracting all required data for constructing and maintaining learners' profiles according to the behaviour of each user (or user groups) as recorded in server logs, as well as on other rules, web site contents and structuring, etc. [37]. The discovered behavioural patterns are usually represented as collections of pages, sessions, items, etc. that are frequently accessed by groups of users with common needs, background, interests, etc. Such patterns can be used to better understand behavioural characteristics of users or user segments, improve the content, organization and structure of the site, create a personalized experience for users by providing dynamic recommendations, etc.

The combination of Web Mining and Semantic Web has created a new and fast-emerging research area of *Semantic Web Mining*. The idea behind using Semantic Web for generating personalized Web experiences is to improve Web Mining by exploiting the new semantic structures [34]. Semantic e-learning uses the power and flexibility of Semantic technologies in order to facilitate large-scale collaboration of e-learning activities and develop tools, standards and environments that support content management, knowledge navigation, experienced-oriented environments, etc.

3 Semantic Web Technologies

In the following sections, we focus on those technologies that define and enable knowledge representation, structure and reasoning, offer exchange mechanisms to allow collaboration and sharing and provide organizations with the means to implement Semantic e-learning. These technologies that underlie the Semantic Web include XML, URIs, RDF, RDFS, Web services, Semantic Web services, ontologies, languages and intelligent agents and promise to incorporate well-defined semantics into e-learning systems.

3.1 XML

Extensible Markup Language, shortened *XML* [8], consists of a set of rules for defining and representing information as *XML documents*, where information structures are indicated by explicit markup. Unlike HTML that controls the way data are displayed, XML facilitates the sharing of structured data and information on the Web. The markup vocabulary and the structures specified for a particular domain create an *XML application*, a formal language for representing information of the domain. The use of XML has extended towards data interchange between software applications.

In e-learning domain, XML technologies seem to provide an open-ended range of solutions. They enable modular creation of learning materials at different levels of granularity, in a way that supports content reuse and sharing and also allow the separation between content and presentation [24]. XML use can be divided into two major categories: the format for data interchange and the format for information assets. The information assets can be further divided into documents and metadata.

3.2 URIs

A *Uniform Resource Identifier (URI)* which *"is a compact string of characters for identifying an abstract or physical resource"* can be used to designate a particular Web resource i.e. *"anything that has identity"* [4]. Furthermore, a URI does not have to map to a real Web address. URIs that refer to objects accessed with existing protocols are known as Uniform Resource Locators (URLs). So, URIs provide a general identification mechanism, as opposed to URLs which are bound to the *location* of a resource. An e-learning system can identify learning objects via URIs in order to retrieve and use them in various learning scenarios.

3.3 RDF and RDFS

Resource Description Framework (RDF) comprises a general purpose language for representing Web information in a minimally constraining, extensible, but meaningful way [10]. It was developed by the W3C and provides a common specification framework to express document metadata in a standardized form that computers can readily process. RDF commonly uses XML for its syntax and URIs to specify entities, concepts, properties, and relations. It is based on the Directed Acyclic Graph (DAG) model. The basic unit of data in RDF is a *triple*, which consists of i) the *subject* (what the data is about), ii) the *property* (an attribute of the subject) and iii) the *actual value*.

RDF Schema (RDFS) is a language for defining RDF vocabularies, which specifies how to handle and label the elements. Generally, the role of a schema as a representational model in the context of Web information is to mediate and adjudicate between human and machine semantics.

The generic structure of RDF makes easier the e-learning data interoperability and evolution because different types of data can be represented using the common graph model, and it also offers greater value for data integration over disparate Web sources of information [56]. For example, RDF can be used to describe e-learning data semantics or an e-learning ontology in order to mediate heterogeneous databases.

3.4 Web Services and Semantic Web Services

Web service is a software system designed to support interoperable machine-to-machine interaction over a network [6]. It is identified by a URL, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using XML-based messages conveyed by Internet protocols. The Web service model consists of three entities, the service provider, the service registry and the service consumer [19].

The service provider creates or simply offers the Web service. The service provider needs to describe the Web service in a standard format, which in turn is XML, and publish it in a central service registry. The service registry contains additional information about the service provider, such as address and contact of the providing company, and technical details about the service. The service consumer retrieves the information from the registry and uses the service description obtained to bind to and invoke the Web service.

In order to achieve communication among e-learning applications running on different platforms and written in different programming languages, standards are needed for each of these operations. As Web services technology evolves, the need of locate and use them in an automate way is a challenge. This can be achieved by adding explicit semantics to their descriptions. *Semantic Web services* are expected to enable applications to dynamically locate others that provide particular services, and to facilitate (semi-) automated cooperation with them [11].

3.5 Ontologies

Ontologies define the terms used to describe and represent an area of knowledge. Hendler mentions that ontology is *"a set of knowledge terms, including the vocabulary, the semantic interconnections, and some simple rules of inference and logic for some particular topic"* [20]. Ontologies comprise the backbone of the Semantic Web and offer a way of representing the semantics of heterogeneous Web resources and enabling the semantics to be used by Web applications and intelligent agents. They fulfil the need to specify descriptions for the following concepts: (i) classes (general things) in various domains of interest, (ii) relationships that can exist among things, and (iii) the properties (or attributes) those things may have. In this way, they support knowledge reusability, since they encode knowledge in a domain and also knowledge that spans domains.

The development of the ontology is akin to the definition of a set of data and their structure. In this content, an ontology can formulate a representation of the learning domain by specifying all of its concepts, the possible relations between them and other properties, conditions or regulations of the domain.

Current research has shown the important role that ontologies can play in the e-learning domain. They can be used for realizing sophisticated e-learning scenarios and improving resources' management, for automatic generation of hypertext structures from distributed metadata, for organizing learning material according to different needs of tutors and learners, for more accurate searching, etc. [7].

3.6 Other Languages

There have been several research efforts to build on RDF and RDFS with knowledge representation languages such as OWL, Simple HTML Ontology Extensions (SHOE), Personal Ontology (Personal-Ont), Ontology Inference Layer (OIL), DARPA Agent Markup Language – Ontology Language (DAML-ONT), DARPA Agent Markup Language + Ontology Inference Layer (DAML-OIL), etc.

Especially, *OWL* that stands for *Web Ontology Language* has been standardized by the W3C as a knowledge representation language for the Semantic Web. It is designed for use by applications that need to process the content of information instead of just presenting information to humans, like e-learning ones. It provides additional vocabulary for describing properties and classes: among others, relations between classes (e.g. disjointness), cardinality (e.g. "exactly one"), equality, richer typing of properties, characteristics of properties (e.g. symmetry), and enumerated classes. OWL documents represent domain ontologies and rules, and allow knowledge sharing among agents through the standard Web services architecture [46].

3.7 Intelligent Agents

Intelligent agents are *"software entities that carry out operations and process information on behalf of a user or another program with some degree of independence or autonomy, directed by some awareness of the user's goals or needs"* [42]. There are various types of agents e.g. for searching, shopping, site management, etc. that have the intrinsic ability to communicate, cooperate, coordinate, negotiate and the ability to learn, as well as the capability to evolve through their interactions with other agents [29].

In the context of the Semantic e-learning, intelligent agents are able to organize, store, retrieve, search, and match information and knowledge for effective collaboration among various participants [46]. So, they can be used for knowledge management to support various learning activities e.g. to discover content that satisfies user's requirements and preferences.

4 Semantic e-Learning Applications

The Web provides an existing and highly available infrastructure for supporting e-learning while the Semantic Web enhances this environment by representing semantics of knowledge resources and their relationships in a standard format. In this section, we focus on how semantics can improve e-learning as well as potential applications that Semantic e-learning will greatly impact.

4.1 Semantic Portals

Web portals serve as integrated gateways through which millions of users can access information, services, and other available applications. However, traditional and current approaches often fail to provide users with the type of information or level of service they require. Limitations concern the ability to create, access, search, extract, interpret, process and maintain information resources. These in their turn lead to high maintenance costs and overheads, limited ability for third parties to reuse the information, problematic nature of adding new types of information, etc. The Semantic Web technologies have the potential of overcoming these limitations and enabling the design and implementation of semantic portals.

Semantic portals are considered as the next generation of Web portals and allow improved information sharing and exchange for a community of users. The resources of these portals can be indexed by using domain ontologies. This allows navigation, search, query and reasoning to fully utilize both textual and semantic information leading to more precise results. Moreover, it supports the easy update of portal's structure, and offers possibilities for sharing and reuse since it separates portal content from structure and provides rich structural links [43].

To this direction, semantic e-learning agents can render support to students, assisting them to successfully organize and perform their studies. For example, they can observe student behaviour (e.g. assessment results, interactions with a virtual experiment, etc.) and provide feedback and links to suitable learning material [38]. Other cases are to answer questions regarding the regulations of study (e.g. does a student possess all requirements to participate in an examination or a course?, is a student allowed to register for his/her thesis?) [18], or to provide a student essay system and a question-answering component that searches for answers in different resources such as ontologies and documents on the Web [39]. All these services and more can be parts of an e-learning semantic portal [28], [31], [52].

4.2 Semantic Search

Semantic Web technologies can make search engines more powerful and effective. The traditional keyword search can be enhanced by adding semantic information based on metadata and ontologies [14]. In this way, simple Web pages are transformed to intelligent, semantically annotated Web pages where searching for a particular information, course, lesson, test or practice is comprehensive and precise. *Semantic search engines* applied in e-learning systems can choose the suitable services to manage the queries, match these queries to learning objects or other knowledge resources metadata and then produce improved results [47], [54], [59].

4.3 Personalization

Personalization features as one of the most promising approaches to alleviate the information overload problem and to provide online users with tailored experiences. In other words, it means *"gathering and storing information about web site visitors* *and analyzing this information in order to deliver the right content in a user-preferred form and layout."* [9]. Recent Web technological advances help e-learning systems to acquire individual learner's information in real-time and with low cost. Based on this information, they construct detailed profiles and provide personalized e-learning services [17], [21], [32], [34], [35], [37], [50], [52]:

- *Personalised content*: Typical adaptations are optional lessons' explanations, personalized recommendations, driven presentations, and more. Used techniques include adaptive selection of Web page (or page fragment) variants, fragment colouring, adaptive stretch-text, adaptive natural language generation, etc.
- *Personalised structure*: It refers to changes in the link structure of hypermedia documents or their presentation. Deployed techniques comprise adaptive link sorting, annotation, hiding/unhiding, disabling/enabling, removal/addition. These adaptations are widely used for producing adaptive recommendations (for lessons, tests, information or navigation), as well as constructing personal views-spaces. Systems attempt to provide pathways through materials by matching domain ontologies with dynamically evolving user models.
- *Personalised presentation and media format*: In this type of personalization the content ideally stays the same, but its format and layout changes (from images to text, text to audio, video to still images). These adaptations are used for Web access through PDAs, mobile phones, sites that cater to handicapped persons, etc.

4.4 Recommendation Systems

Recommendations systems (RSs) comprise the most popular forms of personalization [1]. They have emerged in the middle of 1990's and from novelties used by a few Web sites have changed to important tools incorporated to many applications, especially in the e-commerce domain e.g., Amazon.com, eBay.com, CDNow.com. Specifically, these systems take advantage of users' and/or communities' opinions/ ratings in order to support individuals to identify the information or products most likely to be interesting to them or relevant to their needs and preferences. Using RSs in the e-learning environment can help both tutors to improve the performance of the teaching process and learners to find their suitable online materials.

Semantic Web technologies are foreseen to greatly affect these systems. Next generation personalization and RSs integrate semantic and ontological knowledge into the various steps comprising personalization process i.e. data acquisition, data analysis and personalized output [25], [45], [48], [53]. A characteristic example can be the following: the e-learning system could recommend alternative educational resources based on student searching and studying patterns. In a formal setting, it could query the syllabus and timetable to recommend a plan of study.

4.5 Web 2.0 and Social Software

A significant number of Web-based services, applications, and tools that demonstrate the foundations of the *Web 2.0* concept [40], are already being used to a certain extent in e-learning. These include chat rooms, instant messaging, social networks, blogs (weblogs), wikis, tags and tagging, social bookmarking, multimedia sharing services, content syndication, podcasting, RSS feeds, social search engines, mash ups, social gaming, etc. Most of this software, commonly called *social software*, bases on the fact that human communication and interaction have become as important in the virtual environment as they are in the actual one. Social software is relatively mature, having been in use for a number of years, although new features and capabilities are being added on an e-learning basis [2].

Recently, the *social Semantic Web* has emerged as a paradigm in which ontologies and social software have been combined. Ontologies can provide an effective mean of capturing and integrating knowledge for feedback provisioning, while social software can support pedagogical theories, such as social constructivism [51]. Other areas whereas developments in Semantic Web and social software are beginning to be explored are:

- *Semantic wikis*. It allows users to make formal descriptions of things (similar to Wikipedia) and also annotate these pages with semantic information using languages such as RDF, OWL, etc. [41]. A number of engines are being developed to support this concept including Platypus and SemperWiki [2].
- *Semantic blogging*. It can be used to distribute machine-readable summaries of their content and thus facilitate the aggregation of similar information from a number of sources [15]. For example, RDF semantic data can be used to represent and export blog metadata, which can then be processed by another machine. In the long run the inclusion of this semantic information, by instilling some level of meaning, will allow queries such as "Who in the blogosphere agrees/disagrees with me on this point?" [2].

Finally, *learning or educational communities* possess important place in the e-learning domain. They involve a domain of knowledge defining a set of issues, a community of people who care about this domain, and the shared practice that they develop to be effective in their domain [55]. These communities are typically categorized as communities of purpose, with the purpose being learning and require advance tools to support their communicative needs. The introduction of online communities has proved to be a quite promising concept, allowing the improvement of both the quality of online courses and the attractiveness of Web-based learning environments. Ideally, within the context of a learning community, knowledge and meaning are actively constructed, and the community enhances the acquisition of knowledge and understanding, and satisfies the learning needs of its members. Moreover, communities can counteract the isolation of the independent learner and the associated dropout quota. Members of a learning community may be students, lecturers, tutors, researchers, practitioners and domain experts [36].

5 Future Trends

Semantic e-learning is not a single solution, but a cluster of technologies, techniques, protocols, and processes. Such systems are too complicated to be implemented in the current stage. However, we argue that the next generation of e-learning is Semantic e-learning. To this direction, a number of issues and challenges that still remains unclear should be overcome before Semantic e-leaning vision becomes a reality.

First of all, interoperability features as an extremely important requirement for future e-learning. Interoperability is the ability of ICT systems and of processes they support to exchange data and enable information and knowledge sharing. It appears as the mean for accomplishing the inter-linking of information, systems, applications, and ways of working. Three interoperability levels need to be considered: syntactic, communication and semantic. One step forward to fulfil interoperability is Web services deployment. Despite the several efforts to extend emerging Web services with new features such as composition and content mark-up, full semantic interoperability is not provided yet.

Furthermore, researchers argue on e-learning ontologies' design. This task is not trivial or straightforward and requires the involvement of experts, who have an abstractional thinking and deep knowledge of the domain to be described, in order to provide a shared and common understanding of it. The selection and definition of the concepts and the relation between them, as well as the level of detail is a costly and time-consuming task, since the more analytical the ontology is the more complexity and difficulty it imposes. Moreover, their development and maintenance cost can be prohibitive [57]. It often happens that the ontological decisions embodied in the design of the data repositories may not correspond to those of the user. This is the case for many e-learning environments, where the differences of the various notions may often be indistinguishable. A solution to this can be the use of multiple ontologies, one for each user profile, instead of a single universal ontology [36].

Another issue refers to information sharing that should comply with personal data protection principles, laws and regulations [33]. Generally, it involves the following tasks: digital data collection, storage, processing, transfer, and sharing. This, in its turn, affects the way e-learning architectures are designed and implemented. Moreover, the user privacy threats in an electronic environment are so many that a single solution does not exist. The future challenges and research in the direction of delivering adaptive e-services without jeopardising -but in fact protecting- privacy relate to: standards support, intelligible disclosure of data, disclosure of methods, provision of organizational and technical means for users to modify their user model entries, servers that support anonymity, and adapting user modelling methods to privacy preferences and legislation [49].

Finally, other obstacles that hamper Semantic e-learning are the following: (i) E-learning systems use various terminologies and vocabularies. It is important to detect differences, overlaps and gaps appeared in learning processes and resolve conflicts. (ii) Learning components interact with different ways. The used protocols and how they are integrating in processes comprise critical challenge of the field. (iii) Each e-learning system has its own processes running within and across its environment. This can cause interoperability problems.

6 Conclusion

In recent years, the focus of ICTs is shifting to the applications to help universities, businesses, governments, and other organizations improve and transform their current practices. In this direction, new methods and the technologies supporting those methods are widely adopted. Among the emerging technologies in this competitive digital economy is Semantic e-learning. Its vision is to enable ICT architectures and technologies to support information and knowledge transparent exchange among collaborating e-learning systems. XML-based languages, RDF, ontologies, Web services and other related technologies are utilized in order to accelerate this attempt. Even though research on Semantic e-learning is just beginning, these technologies have the potential to provide a number of benefits over the traditional approaches including improved performance, effective representation and reasoning, maintaining and sharing of learning resources. Finally, there are still a lot of issues that need to be addressed before effective e-learning applications developed (interoperability, security, privacy, other obstacles). Future research activities will focus on these challenges.

References

1. Adomavicius, G., Tuzhilin, A.: Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-art and Possible Extensions. IEEE Transactions on Knowledge and Data Engineering 17(6), 734–749 (2005)
2. Anderson, P.: What is Web 2.0? Ideas, Technologies and Implications for Education. JISC Technology and Standards Watch (2007)
3. Anderson, T., Whitelock, D.: The Educational Semantic Web: Visioning and Practicing the Future of Education. Journal of Interactive Media in Education, 1–15 (2004)
4. Berners-Lee, T., Fielding, R., Masinter, L.: RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax (1998)
5. Berners-Lee, T., Hendler, J., Lassila, O.: The Semantic Web. Scientific American 284(5), 34–43 (2001)
6. Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., Ferris, C., Orchard, D.: Web Services Architecture. W3C Working Group (2004), http://www.w3.org/TR/ws-arch
7. Brase, J., Nejdl, W.: Ontologies and Metadata for eLearning. In: Handbook on Ontologies, pp. 555–573. Springer, Heidelberg (2004)
8. Bray, T., Paoli, J., Sperberg-McQueen, C.M., Maler, E., Yergeau, F., Cowan, J.: Extensible Markup Language (XML), W3C Recommendation (2004), http://www.w3.org/TR/xml11
9. Braynov, S.: Personalization and Customization Technologies. In: Bidgoli, H. (ed.) The Internet Encyclopedia, vol. 3, pp. 51–63. John Wiley & Sons, Chichester (2003)
10. Brickley, D., Guha, R.V.: Resource Description Framework (RDF) Schema Specification 1.0. Candidate Recommendation, W3C (2000)
11. Bruijn, J., Fensel, D., Keller, U., Lara, R.: Using the Web Services Modelling Ontology to Enable Semantic E-business. Communications of ACM 48(12), 43–47 (2005)
12. Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.): Adaptive Web 2007. LNCS, vol. 4321. Springer, Heidelberg (2007)
13. Brusilovsky, P.: Adaptive Hypermedia. User Modeling and User-Adapted Interaction 11, 87–110 (2001)
14. Cao, J., Zhang, D.: Knowledge Management Tools for E-Learning: Semantic Web and Others. In: Cao, J., Zhang, D. (eds.) Intelligent Learning Infrastructure for Knowledge Intensive Organizations, A Semantic Web Perspective, pp. 57–80. Information Science Publishing, Hershey (2006)
15. Cayzer, S.: Semantic Blogging and Decentralized Knowledge Management. Communications of the ACM 47(12), 47–52 (2004)

16. Cooley, R.: Web Usage Mining: Discovery and Application of Interesting Patterns from Web Data. PhD Thesis, Department of Computer Science, University of Minnesota (2000)
17. De Bra, P., Kay, J., Weibelzahl, S. (eds.): Special Issue on Personalization. IEEE Transactions on Learning Technologies 2 (2009)
18. Dunkel, J., Bruns, R.: Semantic E-learning Agents, Supporting E-learning by Semantic Web and Agents Technologies. Enterprise Information Systems, 237–244 (2006)
19. Dustdar, S., Schreiner, W.: A Survey on Web Services Composition. International Journal of Web and Grid Services 1(1), 1–30 (2005)
20. Hendler, J.: Agents and Semantic Web. IEEE Intelligent Systems 16(2), 30–37 (2001)
21. Henze, N., Dolog, P., Nejdl, W.: Reasoning and Ontologies for Personalized E-Learning in the Semantic Web. Educational Technology and Society 7(4), 82–97 (2004)
22. IEEE LTSC: IEEE Learning Technology Standards Committee. IEEE Standards Association (2009), http://ieeeltsc.wordpress.com
23. Isaías, P., Miranda, P., Pífano, S.: Designing E-Learning 2.0 Courses: Recommendations and Guidelines. In: Méndez-Vilas, A., Solano Martín, A., Mesa González, J.A., Mesa González, J. (eds.) Research, Reflections and Innovations in Integrating ICT in Education, Badajoz, Spain, FORMATEX, vol. 2, pp. 1081–1085 (2009)
24. Kanovsky, I., Or-Bach, R.: E-Learning - Using XML Technologies to Meet the Special Characteristics of Higher Education. Journal of Systemics, Cybernetics & Informatics 2(1), 32–36 (2004)
25. Khribi, M., Jemni, M., Nasraoui, O.: Toward a Hybrid Recommender System for E-Learning Personalization Based on Web Usage Mining Techniques and Information Retrieval. In: Bastiaens, T., Carliner, S. (eds.) World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2007, pp. 6136–6145. AACE, Chesapeake (2007)
26. Klein, J., Eseryel, D.: The Corporate Learning Environment. Intelligent Learning Infrastructure for Knowledge Intensive Organizations, A Semantic Web Perspective, pp. 1–38. Information Science Publishing, Hershey (2006)
27. Kosala, R., Blockeel, H.: Web Mining Research: a Survey. SIGKDD Explorations 2(1), 1–15 (2000)
28. Kotzinos, D., Pediaditaki, S., Apostolidis, A., Athanasis, N., Christophides, V.: Online Curriculum on the Semantic Web: the CSD-UoC Portal for Peer-to-Peer E-learning. In: 14th International Conference on World Wide Web, Chiba, Japan, May 10-14, pp. 307–314 (2005)
29. Leuf, B.: The Semantic Web, Crafting Infrastructure for Agency. John Wiley-Sons, Chichester (2006)
30. Lytras, M., Naeve, A.: Semantic E-learning: Synthesizing Fantasies. British Journal of Educational Technology 37(3), 479–491 (2006)
31. Manouselis, N., Abian, A., Carrión, J., Ebner, H., Palmér, M., Naeve, A.: A Semantic Infrastructure to Support a Federation of Agricultural Learning Repositories. In: 8th IEEE International Conference on Advanced Learning Technologies (ICALT 2008), Santander, Cantabria, Spain, July 1-5, pp. 117–119 (2008)
32. Markellos, K., Markellou, P., Rigou, M., Sirmakessis, S., Tsakalidis, A.: Personalized E-learning. Educational Science Journal, Special Issue Lifelong and Distance Learning in Information Society, Pedagogic Department of Crete University (2004)
33. Markellos, K., Markellou, P., Rigou, M., Sirmakessis, S., Tsakalidis, A.: Web Personalization and the Privacy Concern. In: 7th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technologies, Syros, Greece (2004)

34. Markellou, P., Mousourouli, I., Sirmakessis, S., Tsakalidis, A.: Using Semantic Web Mining Technologies for Personalized e-Learning Experiences. In: 4th IASTED International Conference on Web-Based Education, Switzerland, pp. 522–527 (2005a)
35. Markellou, P., Rigou, M., Sirmakessis, S., Tsakalidis, A.: Personalization in the Semantic Web Era: a Glance Ahead. In: 5th International Conference on Data Mining, Text Mining and their Business Applications (Data Mining 2004), Wessex Institute of Technology (UK), Malaga, Spain, September 15-17, pp. 3–11 (2004)
36. Markellou, P., Rigou, M., Sirmakessis, S., Tsakalidis, A.: Shaping Online Learning Communities and the Way Adaptiveness Adds to the Picture. International Journal of Knowledge & Learning (IJKL) 1(1-2), 80–95 (2005b)
37. Markellou, P., Rigou, M., Sirmakessis, S.: Mining for Web Personalization. In: Web Mining: Applications and Techniques, pp. 27–48. Idea Group Publishing, Hershey (2004)
38. Millard, D., Tao, F., Doody, K., Woukeu, A., Davis, H.: The Knowledge Life Cycle for E-learning. Int. J. Cont. Engineering Education and Lifelong Learning 16(1-2), 110–121 (2006)
39. Moreale, E., Vargas-Vera, M.: Semantic Services in e-Learning: an Argumentation Case Study. Educational Technology & Society 7(4), 112–128 (2004)
40. O'Reilly, T.: What is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software (2005), http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html
41. Oren, E., Breslin, J., Decker, S.: How Semantics Make Better Wikis. In: International Conference on World Wide Web, Edinburgh, Scotland, May 23-26 (2006), http://www2006.org/programme/files/xhtml/p171/pp171-oren/pp171-oren-xhtml.html
42. Parker, K.: Enabling Technologies for the Semantic Web. Intelligent Learning Infrastructure for Knowledge Intensive Organizations, A Semantic Web Perspective, pp. 39–56. Information Science Publishing, Hershey (2006)
43. Reynolds, D., Shabajee, P.: Semantic Web Advanced Development for Europe (SWAD-Europe), Deliverable 12.1.5 Semantic Portals Demonstrator, Requirements Specification (2001), http://www.w3.org/2001/sw/Europe/reports/requirements_demo_2/#sec-problem
44. Sampson, D., Lytras, M., Wagner, G., Diaz, P.: Ontologies and the Semantic Web for E-learning. Educational Technology and Society 7(4), 26–28 (2004)
45. Shen, L., Shen, R.: Learning Content Recommendation Service Based-on Simple Sequencing Specification. In: Liu, W., Shi, Y., Li, Q. (eds.) ICWL 2004. LNCS, vol. 3143, pp. 363–370. Springer, Heidelberg (2004)
46. Singh, R., Iyer, L., Salam, A.: Semantic eBusiness. International Journal on Semantic Web & Information Systems 1(1), 19–35 (2005)
47. Taibi, D., Gentile, M., Seta, L.: A Semantic Search Engine for Learning Resources. In: Recent Research Developments in Learning Technologies, FORMATEX (2005)
48. Tan, H., Guo, J., Li, Y.: E-learning Recommendation System. In: International Conference on Computer Science and Software Engineering (CSSE 2008), vol. 5, pp. 430–433 (2008)
49. Teltzrow, M., Kobsa, A.: Impacts of User Privacy Preferences on Personalized Systems: A Comparative Study, Designing Personalized User Experiences for eCommerce, Netherlands. Kluwer Academic Publishers, Dordrecht (2004), http://www.ics.uci.edu/~kobsa/papers/2004-PersUXinECom-kobsa.pdf

50. Thyagharajan, K., Nayak, R.: Adaptive Content Creation for Personalized e-Learning Using Web Services. Journal of Applied Sciences Research, INSInet Publication 3(9), 828–836 (2007)
51. Torniai, C., Jovanovic, J., Gasevic, D., Bateman, S., Hatala, M.: E-Learning Meets the Social Semantic Web. In: 8th IEEE International Conference on Advanced Learning Technologies (ICALT 2008), July 1-5, pp. 389–393 (2008)
52. Vargas-Vera, M., Lytras, M.: Exploiting Semantic Web and Ontologies for Personalized Learning Services: Towards Semantic Web Enabled Learning Portals for Real Learning Experiences. Knowledge and Learning 4(1), 1–16 (2008)
53. Wang, P.: The Analysis and Design of Educational Recommender Systems. In: Crawford, et al. (eds.) International Conference Society for Information Technology and Teacher Education 2007, pp. 2134–2140. AACE, Chesapeake (2007)
54. Wang, Y., Wang, W., Huang, C.: Enhanced Semantic Question Answering System for e-Learning Environment. In: 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 2007), vol. 2, pp. 1023–1028 (2007)
55. Wenger, E., McDermott, R., Snyder, W.: Cultivating Communities of Practice. Harvard Business School Press, Cambridge (2002)
56. Wenya, T., Yuxin, M.: A Semantic Grid Application for E-Learning Data Sharing. In: Li, F., Zhao, J., Shih, T.K., Lau, R., Li, Q., McLeod, D. (eds.) ICWL 2008. LNCS, vol. 5145, pp. 457–467. Springer, Heidelberg (2008)
57. Wilson, R.: The Role of Ontologies in Teaching and Learning. TechWatch (2004)
58. Zhang, D.: Virtual Mentor and the LBA System: Towards Building an Interactive, Personalized, and Intelligent E-learning Environment. Journal of Computer Information Systems 44(3), 35–43 (2004)
59. Zhuhadar, L., Nasraoui, O.: Personalized Cluster-based Semantically Enriched Web Search for E-learning. In: Conference on Information and Knowledge Management, 2nd International Workshop on Ontologies and Information Systems for the Semantic Web, Napa Valey, California, USA, pp. 105–112 (2008)

Supporting Rural Citizens' Access to Knowledge: One More Aspect of e-Democracy

Pavlos Koulouris and Sofoklis Sotiriou

Research and Development Department, Ellinogermaniki Agogi,
Dimitriou Panagea Street, 15351 Pallini, Greece
{pkoulouris,sotiriou}@ea.gr

Abstract. The paper considers the potential offered by lifelong learning as a tool for capacity building and development in rural areas, especially through the exploitation of contemporary technologies. The challenges and opportunities connected with small rural schools are particularly focused upon, and teachers working in them are proposed as ideal change agents potentially powerful to catalyse bottom-up developmental initiatives in the local context. The experiences from a series of relevant teacher professional development initiatives in this direction are presented, and some of the main findings and questions arising are summarised.

Keywords: Lifelong learning, rural areas, teacher development, local initiative, change, capacity building.

1 'Rural Learning': A Vehicle to Development

Rural areas should lie in the heart of efforts for a coherent Europe, since they constitute a vital part of European Union (EU)'s physical make-up and identity. According to the EU Rural Development policy for 2007-2013, more than 91 % of the territory of the Union can be defined as 'rural', and this area is home to more than 56 % of the EU's population. Therefore, rural development cannot but form an important pillar of EU's policies. In this context, Europe's contemporary rural development policies place agriculture in a broader context, including issues such as increasing competitiveness, enhanced quality of life in rural areas, and, eventually, attractiveness of rural areas to young farmers and new residents.

Lifelong learning equipping rural citizens with access to development opportunities is expected to play an important role in this direction. Informed and empowered inhabitants of rural Europe may not easily abandon their space and heritage to move to urban centres. They may evaluate the challenges differently, and respond to them flexibly and creatively. It is a task for the whole of the education and training system to promote such a form of 'rural learning', in formal, non-formal and informal contexts [20].

Education and rural development are indeed closely interlinked in many ways. Better educated rural populations have been shown to achieve greater economic development [3]. Higher educational levels in rural areas are positively related to better

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 309–319, 2010.

income growth, and improvement of rural schools can improve local economic conditions by slowing down or reversing 'brain drain' [4].

2 The Role of New Technologies for Capacity Building in the Rural Space

Worldwide, there is an increasing recognition at the political level of the role Information and Communication Technologies (ICT) can play for development and capacity building in disadvantaged populations and less-favoured areas. UN's World Summit on the Information Society in Geneva (2003) and Tunis (2005) produced an action plan which sets objectives very relevant to the rural space, such as building an inclusive Information Society by reducing the digital divide, and putting the potential of knowledge and ICTs at the service of development. At the European level, the strategic guidelines for rural development for 2007-2013 call for the mainstreaming of the Information Society into rural development policies. Considerable investments are currently made for bridging the digital divide so that rural areas in Europe attain their full potential, quality of rural life is improved and rural economy strengthened [34].

As rural citizens' knowledge and skills constitute basic elements of this new environment, technology-enabled and technology-enhanced lifelong learning ought to be one of the vehicles leading rural communities to local capacity building. Rural citizens should be given opportunities to interact with contemporary knowledge and artefacts in a continuous line of personal involvement from childhood to third age, as well as opportunities to collaborate with each other and across age group borders. In this way the rural community as a whole will produce its own sustainable solutions to create conditions for rural well-being and development.

3 Rural Schools: Challenges and Opportunities

Rural Europe is facing important challenges in terms of access to state-of-the-art learning and Information Society opportunities. Next to the shrinking of rural schools in many parts of Europe, features such as low ICT adoption, low entrepreneurship and vulnerability to unemployment underline the need for more and better lifelong learning opportunities. It would be short-sighted to try to trace the source of these inefficiencies only in the skills of the rural workforce and the provision or not of proper adult education and professional training. People's stances and potential in their rural homelands are also shaped during their course, as students, through the educational system. Rural schools are a key factor that should be mobilised in any attempt to enhance demographic retention and growth of rural areas.

3.1 Rural Schools and Community Development

In Europe, as in the rest of the world, rural schools constitute a point of reference and particular significance in their local context, a potential tool for growth, and a source of vision and hope for the future. For decades, they have provided access to education and a promise for a brighter future to all, including the poorest and the less advantaged, and have kept small and aging communities 'alive'. Rural communities have depended on their schools to serve many social and cultural functions beyond their primary mission of educating children. In an account on the non-educational impact of schools on rural communities, Salant & Waller [32] summarise that the school-community relationship is multi-faceted, with schools having positive economic and social impacts, providing a resource for community development, as well as offering a delivery point for social services. Miller [30] proposes that rural schools, working in partnership with local leaders and residents, can have a positive impact on community viability, especially when students, working alongside adults, are given meaningful opportunities to engage in community-based learning that serves the needs of the community.

The concept of 'social capital' has been increasingly used to describe social organization and resources embedded in the social structure of the rural communities which can facilitate community development. Woodhouse [36], reporting on the findings of an Australian case study, suggests that social capital exerts a positive causal influence on economic development. The concept of social capital can indeed provide a foundation for the understanding of the strategic role schools and youth can play in community development. According to Miller [30], the school represents an important element in the community's social capital rather than merely an educational resource for the community's youth. By building the social capital of the school and youth, the community not only helps to develop responsible citizens, but also creates opportunities for tomorrow's leaders to emerge. Teachers, in particular, can play a central role as agents of innovation and multipliers of social capital in a remote small community [19].

3.2 Difficulties for Rural Schools and Teachers

Despite the crucial role of rural schools, their function is becoming more and more problematic in today's Europe; they suffer the consequences of a constantly widening economic and social gap separating urban and rural regions. The digital divide in particular, i.e. the disadvantage of rural areas in terms of access to the opportunities of the contemporary Information Society, is recognised as a threat for rural Europe [11]. Rural educational establishments experience this threat most dramatically. While education in urban areas has already become a space of innovative applications supported by broadband technologies, the exclusion of remote communities from the contemporary educational opportunities badly affects the "borderers" of the education system.

Schools in rural areas have always faced difficult challenges. The problems have been connected, on the one hand, with the small number of school-age children in today's rural communities, but importantly also with the unwillingness of many new teachers to serve in these schools. Teacher shortage in rural and remote areas and the weaknesses in the provision of training and professional support to these teachers have been documented across time and space [5], [26], [12], [31], [2], [17].

In rural Greece, as in other rural areas through out the world, remote schools function as 'multigrade' [22]. Due to the very small size of the school units, teachers teach more than one age group and possibly more than one subject at the same time. Next to their teaching tasks, they typically also carry out considerable amounts of office work required for the administrative function of the school. The young teachers usually posted to such schools are not adequately prepared through their initial training for these demanding conditions. Personal and professional isolation and the wider 'decay' atmosphere do not offer them any motivation to build ties with the school and the surrounding community.

Nevertheless, small rural schools are characterised by positive potential which a skilful and devoted teacher could turn into advantage for the school and the community. Literature is not scarce that recognises multigrade classrooms as not only an unavoidable, but actually a good-quality alternative option for education [24], [13], [6].

3.3 Using Technologies for Rural Teachers' Professional Development

The need for rural teachers' in-service training is apparent, especially in contexts in which inexperienced newly-appointed teachers serve rural schools for short periods. New knowledge and skills are required, so that the teacher can enhance their teaching and respond to the challenging circumstances.

Providing such professional development opportunities typically proves problematic. It is difficult for educational authorities to offer conventional in-service seminars to remote rural teachers, as round trips between the school and the nearest training centre may be costly or even impossible in the absence of substitute teachers.

Technology-supported distance education emerges as a self-evident option for enhanced accessibility of teacher training programs in rural areas. The literature shows a development of relevant initiatives which has generally followed trends in computer-supported learning, delivering various forms of training content [18], [29], [27], [28], [15], [16].

More recently, satellite telecommunications have been particularly focused upon as a tool for bridging the digital divide [14], [9], including the provision of distance education to large remote audiences [23]. There are many examples from the United States and Australia [7], [8], as well as less developed parts of the world characterised by populations thinly distributed over large areas [1], [10], [25].

4 Our Experience: Facilitating Rural Teachers to Respond to the New Challenges

The context outlined above clearly demonstrates that technology potential should be harnessed to offer solutions for the provision of appropriate distance training and support to rural educators, so that they can better fulfil their demanding and inspirational roles in the rural school and the surrounding community. Adopting this as a basic proposition in our work in the framework of a series of consecutive pioneering European and Greek research projects over the last seven years, our team has designed, piloted in numerous rural locations in Greece and Europe, and extensively evaluated schemes of distance training, support and networking aiming to alleviate the isolation of rural teachers and support them in taking over new developmental roles, exploiting possibilities offered by technologies.

The main questions we have addressed refer to a) the appropriate content of the relevant professional development and support activities; b) the appropriateness of the various available and emerging delivery technologies, given the remote and digitally disadvantageous location of the beneficiaries; and c) the possible extensions to conventional e-learning technologies and practices, which could help the geographically disadvantaged rural educators to learn not only as isolated individuals but also learn from each other, participating in informal learning experiences within a sustainable lifelong learning network.

Our efforts started from an emphasis on teacher development through training content delivered over the web (MUSE project, www.ea.gr/ep/muse), and gradually moved into testing more advanced technologies for broadband delivery over satellite, while continuing to further develop the content [cf. the ZEUS (www.dias.ea.gr); HERMES (www.ea.gr/ep/hermes); RURAL WINGS (www.ruralwings-project.net) projects]. The 'maturity' gained through the implementation of the various training activities and the increasing involvement of remote rural teachers led to the development of a human network (NEMED; www.nemed-network.org) and an increased interest in concepts and tools related to lifelong learning networks (NEMED, RURAL WINGS) and the use of social software and Web 2.0 in this direction (cf. the recently launched SoRuraLL project, www.sorurall.eu).

4.1 Evaluation

Professional development schemes piloted in the above projects have been subjected to close monitoring and evaluation, both in terms of technological appropriateness and pedagogical potential and outcomes. Evaluation objectives typically have included assessing the appropriateness of the choices made during the design stage and the overall effectiveness of the solution at three levels: the technology used, the content of training offered, and the procedures followed. Main instruments towards this have been extensive exchanges with the trainees through surveys based on questionnaires and interviews with the remote teachers and their trainers, as well as field observations and video recordings in the schools and classrooms of the participating teachers. In an overarching case-study oriented approach, the evolution of informants' views, behaviours and stances is observed and interpreted.

Several analyses of quantitative and qualitative data have been conducted in the course of the various projects. They have revealed positive and weak points in the design and implementation, offering rich experiences and good practices for future efforts in the field. Overall, teachers working in remote small rural schools have acknowledged that the piloted schemes have provided them with genuine opportunities for professional development and improved personal competences.

5 A Proposed Framework for Rural Learning through Teacher Development

Based on the accumulated experiences and findings from these projects, in the following we summarise the emerging main issues and recommendations, offering what we believe could serve as a foundation for a comprehensive framework for the realisation of the vision of 'rural learning' as outlined in previous sections.

The basic propositions are:

- Rural teachers should be offered in-service professional development and networking opportunities to enhance their performance as educators and school administrators, as well as community inspirers, development agents and multipliers in the rural context. In this process, rural teachers can learn a lot from each other, through formal and informal interactions and networking.
- The design of the professional development programmes should be grounded on a sound understanding of the rural context in which they are implemented, a thorough analysis of the local needs and an attention to important differences that exist between small rural schools and the 'mainstream' urban educational provision.
- The responsibility and control over the content and processes of the professional development should be passed as much and as soon as possible to the rural teachers themselves. Instead of imposing generic 'solutions', the emphasis should be on facilitating the teachers and their local communities to invent their own solutions to the problems they recognise as pressing or important.
- Teachers should be kept closely involved in the processes of designing the programmes, starting from the early stages of needs analysis through field surveys and workshops, to a continuous 'dialogue' between users and designers in the implementation phase, in consecutive cycles of co-design which fine-tune the programme to user response and decisions.
- The choice of technologies to be used should be seen as a dynamic process, in which the best available solution is selected each time without affecting the pedagogical rational and core objectives of the programme. Aiming to provide ever better access to richer content (e.g. faster or more reliable connectivity) is a major driving force, given the still existing obstacle of the digital divide.

In the light of these general directions, it is worth looking more closely at the points discussed below.

5.1 The Content of Teacher Development Programmes

The content we have found relevant could be described as falling under three major areas: a) ICT skills; b) pedagogy; and c) local development issues.

Professional development schemes piloted in the earlier of our projects aimed mainly at helping multigrade school teachers to develop their professional skills along two main axes: a) use of ICT both for teaching and administrative purposes, an area in which rural teachers are still quite weak; and b) application of teaching approaches which are appropriate for the multigrade classroom.

In later stages, one further important axis has been added in the teacher training curriculum. We have been inviting the rural teacher to become a change agent catalysing innovation and development in the school and the local community, taking initiatives for changing the declining school into a lively node supporting lifelong learning for everyone. The teacher is encouraged to take on a crucial role in the development and implementation of a culture conducive to lifelong learning and innovation in the school and beyond it, making efforts to link school life with the external environment, helping the school to interact with its surroundings, and creating communities of learning within and outside the school. The aim of this aspect of professional development is multi-faceted, targeting diverse competences: better knowledge and understanding of solutions and opportunities of the Information Society, pedagogies specifically adaptable to the 'unusual' settings of the small rural school, as well as in areas that are currently scarcely present even in the most progressive teacher training curricula, such as innovation, change management, local and rural community development.

5.2 The Delivery Channels and Methods

The e-learning environments engaged in the delivery of our professional development programmes have consisted of various technologies. We have often tested various satellite solutions for broadband delivery of rich educational content, in the context of both synchronous (videoconferencing, application sharing, chatting) and asynchronous (web-based learning through structured access to a rich pool of educational content, and networking) activities.

The ZEUS experience clearly showed that earlier one-way satellite data telecommunications (DVB) combined with non-broadband terrestrial infrastructures can support the provision of training and professional development at a distance. Nevertheless, significant technical difficulties, which in limited cases even caused obstacles to the smooth running of training, would have been avoided if a more advanced model of two-way satellite internet provision had been available. Such technologies (DVB-RCS) have been deployed in the HERMES and RURAL WINGS projects, yielding more satisfactory results.

Overall, satellite broadband even in its most advanced state-of-the-art is however a limited resource which seems to lack the smoothness of operation and perceived 'unlimitedness' of contemporary terrestrial DSL broadband, especially when 'heavy' live applications (e.g. multipoint videoconferencing and webstreaming) are used. Still satellite broadband remains the best option for many remote areas before more efficient terrestrial telecommunications become available in a shorter or longer term.

However, although technical specifications do play a crucial role in a distance education scenario, the success or not of the effort depends on the underlying pedagogical design [21]. Our field activities have confirmed this. Various technical problems and faults did slightly decrease teachers' enthusiasm at times, but in the whole they did not lead to a lower appreciation of the deployed solutions.

The training programmes we have produced aim to cater for both flexibility and guidance, both interaction with others and self-paced learning. To this end, we propose a comprehensive model for training delivery, in which the central event for each 'lesson' is a live videoconferencing session, using a synchronous e-learning tool, thus covering the need of isolated teachers for communication and real-time interaction with colleagues and instructors [33]. On average, this synchronous e-learning portion of a 'lesson' takes up about 30% of the overall 'lesson' duration. However, both before and after the live session there is learning activity taking place independently in the working environment of the trainee. Through the use of web-based instruction techniques course participants are offered on-the-job training opportunities through tasks and materials that allow them to work at their own pace, interact with the instructor and other practitioners as needed, and receive individual feedback as they apply information to their own classroom settings. For each lesson, there is introductory information on the topic covered, and preparatory activities. Participants report on their experiences from such activities in the web-based e-learning environment as well as during the synchronous session. The cycle of each lesson closes with post-session consolidation activities.

5.3 The Importance of Networking

Beyond providing formal training, initiatives for rural teachers' professional development should explore methods to develop and foster a learning network which will provide the context for the acquisition and sharing of knowledge in an informal communication process supplementing teachers' formal professional education. The characteristics should be investigated of tools and methodologies which can foster the improvement of teachers' personal competences, and encourage and facilitate a teacher's contributions to the development of the other teachers (lifelong learning network). At the level of technology, the limitations of 'old-generation' e-learning technologies and models should be taken into account, when the issue at stake turns into how to promote and facilitate competence development through networking with peers – a lifelong learning experience of multi-site and episodic nature. It is crucial to identify the features and clarify the main issues connected with the various social media which will be able to support rural teachers, both as individuals and as members of teams within the educational system (an 'organisation' in itself), to further develop their competences making use of the distributed knowledge and learning resources available.

An interesting practical initiative could be Web 2.0 projects initiated and managed by teachers, aiming to develop and foster a learning network between peers. These could develop into pure 'communities of practice' as defined by Wenger [35]: communities characterised by a shared domain of interest, e.g. that of the development of multigrade teaching competences, and an established members' commitment, with teachers engaging in joint activities and discussions, helping each other, sharing information and learning from each other while pursuing their interest in their domain. Members of the community may thus gradually develop a shared repertoire of resources – a shared practice: experiences, stories, tools, ways of addressing recurring problems in their small rural school, etc.

5.4 Inspiring New Leadership Roles for Teachers

'Conventional' teacher training in ICT and pedagogical skills is necessary for rural teachers, but probably not enough if the opportunities for rural development through learning are to be fully exploited. Teachers should be encouraged to recognize new roles for themselves beyond the conventional mere realisation of their teaching duties, seeing themselves as inspirers and managers of a small 'revolution' in the rural school and community, an informal local 'reform', as designers and implementers of innovation matching local needs. Already a prominent member of the small local community, the rural teacher can in this way further and deepen the significance and local leadership of the school. He/she will be the pedagogic innovator, an instructional leader exploring new ways to improve the quality of teaching and learning in the school. Further, beyond the walls of the classroom, the teacher may develop into a facilitator of communities of learning in, around, and outside, the school, for instance by developing synergies between the school, the community and maybe other schools in the area.

The case of making satellite broadband connectivity available to the school (such as in the HERMES and RURAL WINGS projects) is an interesting practical example. This bandwidth ought to become advantage and opportunity for all, and rural teachers are foregrounded as the agents who will enable this. They are expected to act as change agents, managers in charge of driving change in the communities. They need to diagnose and deeply understand the context, the stakeholders, their interests and interrelations, so as to consequently convince them about the need and benefits of change, tackling possible scepticism. In parallel, they act as managers and administrators of a whole community 'Learning Hub', into which they turn their rural schools and technological infrastructures. This may involve the teacher matching the lifelong learning opportunities offered with the needs he may diagnose in the local community and in specific individuals, supporting the community members to produce their own local information and content based services, and thus eventually helping local citizens to become knowledgeable and willing enough to develop their own further projects.

Moving in this direction clearly poses questions and challenges. The content and methods of the relevant teacher training curriculum need to cover diverse areas of competence including knowledge and skills about local development issues and initiatives, skills in generating innovation and managing change, subjects in general which bear no relevance with the usual teacher training content. Ways have to be found to familiarize teachers with a quite different area of expertise and practice. To mention an illustrative example, as potential change managers teachers need to learn practical ways to challenge the status quo by comparing it to an ideal or a vision, translate the vision into a specific change initiative, communicate and defend the need for change, lead and manage change, as well as understanding the cultural dynamics of change.

Serious challenges also arise in connection to possible conflicts with the traditional structures of the educational system and between formal and informal leadership roles. This new approach is inevitably in contradiction with the traditions of a highly centralized educational system, such as the one of Greece. While the system tolerates little decentralisation and autonomy of school units, the teacher is encouraged by our approach to initiate and implement an informal local 'educational reform'. This discrepancy could possibly be a source of tension – not the least in the intrapersonal level, with the teacher having to balance between his formal/recognised and informal/self-initiated leadership roles.

References

1. Al-Sharhan, J.: Education and the Satellite: Possibilities for Saudi Arabia? International Journal of Instructional Media 27(1), 51–56 (2000)
2. Ankrah-Dove, L.: The Deployment and Training of Teachers for Remote Rural Schools in Less-Developed Countries. International Review of Education 28(1), 3–27 (1982)
3. Barkley, D., Henry, M., Haizhen, L.: Does Human Capital Affect Rural Growth? Evidence from the South. In: Beaulieu, L.J., Gibbs, R. (eds.) The Role of Education: Promoting the Economic and Social Vitality of Rural America. Southern Rural Development Center and USDA, Economic Research Service (2005)

4. Beaulieu, L.J., Gibbs, R. (eds.): The Role of Education: Promoting the Economic and Social Vitality of Rural America. Southern Rural Development Center and USDA, Economic Research Service (2005)
5. Benveniste, L.A., McEwan, P.J.: Constraints to Implementing Educational Innovations: The Case of Multigrade Schools. International Review of Education 46(1-2), 31–48 (2000)
6. Boss, S.: Big Sky Legacy. In Montana, Small Schools Aren't a Bold New Idea. They're a Way of Life. Northwest Education Journal 6(2), 34–42 (2000)
7. Boverie, P., Gunawardena, C., Lowe, C., Murrell, W.M.G., Zittle, R.H., Zittle, F.: Designing Satellite Instruction for Elementary Students: Importance of the Classroom Teacher. International Journal of Educational Telecommunications 6(2), 107–122 (2000)
8. Boylan, C., Wallace, A., Richmond, W.: Remote Student Access to Education via Satellite Delivery. Education in Rural Australia 10(1), 2–12 (2000)
9. Cartheron, R.: Reducing the Digital Divide in Europe: Competitiveness of Satellite among Broadband Access Technologies. Vista Advisers, Paris (2003)
10. Cohen, D.: Satellite-Based Computer Network Serves Students on Remote Pacific Islands. Chronicle of Higher Education 48(18), A41–A42 (2002)
11. Cohendet, P.: The Digital Divide in the European Enlarged Economic Scenario: An Assessment of the Socio-economic Effects. University Louis Pasteur, Strasbourg (2003)
12. Coldevin, G., Naidu, S.: In-Service Teacher Education at a Distance: Trends in Third World Development. Open Learning Journal 4(1), 9–15 (1989)
13. Cook, M.: What's So Good about a Small Rural School?.Everything! Education in Rural Australia 10(2), 59–62 (2000)
14. EC, White Paper: Space: A New European Frontier For An Expanding Union: An action plan for implementing the European Space Policy. Office for Official Publications of the European Communities, Luxembourg (2003)
15. Falconer, K.B., Lignugaris-Kraft, B.: A Qualitative Analysis of the Benefits and Limitations of Using Two-way Conferencing Technology to Supervise Preservice Teachers in Remote Locations. Teacher Education and Special Education 25(4), 368–384 (2002)
16. Forbush, D.E., Morgan, R.L.: Instructional Team Training: Delivering Live, Internet Courses To Teachers and Paraprofessionals in Utah, Idaho and Pennsylvania. Rural Special Education Quarterly (Spring 2004)
17. Helge, D.I., Marrs, L.W.: Personnel recruitment and retention in rural America: A growing problem. The Pointer 26(2), 28–33 (1982)
18. Kendal, R.M.: Evaluating the benefits of a computer based telecommunications network: Telementoring and teletraining for educators in rural areas. Journal of Research in Rural Education 8(1), 41–46 (1992)
19. Koulouris, P., Sotiriou, S.: Exploring teacher's innovative leadership roles in small rural schools. In: The Commonwealth Council for Educational Administration and Management (CCEAM) Conference 2006, Nicosia, Cyprus, October 12-17 (2006)
20. Koulouris, P., Sotiriou, S. (eds.): Rural Learning for Development: Experiences from Europe: Report on Rural Learning for Development and Proceedings of the 2007 RuraLEARN Conference and Workshops. EPINOIA, Athens (2007)
21. Lim, D.H.: Perceived Differences between Classroom and Distance Education: Seeking Instructional Strategies for Learning Applications. International Journal of Educational Technology 3, 1 (2002)
22. Little, A.W.: Education for All and Multigrade Teaching: Challenges and Opportunities. Springer, Dordrecht (2006)
23. Littman, M.K.: Satellite Communications in the Telelearning Environment: Innovative Delivery Options for Distance Learning. Journal of Online Learning 11(2), 5–11 (2000)

24. Lloyd, L.: Multiage Classes: What Research Tells Us about Their Suitability for Rural Schools. Education in Rural Australia 12(2), 1–14 (2002)
25. Lorenzo, G.: World Bank's Global Development Learning Network: Sharing Knowledge Electronically between Nations to "Fight Poverty". USDLA Journal 16, 5 (2002)
26. Ludlow, B.L.: Preparing special educational personnel for rural schools: Current practices and future directions. Journal of Research in Rural Education 14(2), 57 (1998)
27. Ludlow, B.L.: Technology and teacher education in special education: disaster or deliverance? Teacher Education and Special Education 24(2), 143–163 (2001)
28. Ludlow, B.L., Duff, M.C.: Webcasting: A New Technology for Training Special Educators in Rural Areas. In: No Child Left Behind: The Vital Role of Rural Schools. Annual National Conference Proceedings of the American Council on Rural Special Education (ACRES), Nevada, March 7-9 (2002)
29. McDevitt, M.A.: A virtual view: Classroom observations at a distance. Journal of Teacher Education 47(3), 191–195 (1996)
30. Miller, B.: The role of rural schools in community development: Policy issues and implications. Journal of Research in Rural Education 11(3), 163–172 (1995)
31. Miller, J., Sidebottom, D.: Teachers: Finding and keeping the best in small and rural districts. AASA, Alexandria (1985)
32. Salant, P., Waller, A.: What Difference Do Local Schools Make? A Literature Review and Bibliography. Annenberg Rural Challenge Policy Program, The Rural School and Community Trust (1998)
33. Shrestha, G.M., Sutphin, H.: Relationship between Interaction and Acceptance in Satellite Video-Conferencing. Journal of Educational Technology Systems 28(1), 43–58 (2000)
34. Sotiriou, S., Koulouris, P.: Bridging the Digital Divide in Rural Communities: Practical Solutions and Policies. In: Proceedings of the Conference, Athens, Greece, May 15-16. EPINOIA, Athens (2008)
35. Wenger, E.: Communities of practice: learning, meaning, and identity. Cambridge University Press, Cambridge (1998)
36. Woodhouse, A.: Social capital and economic development in regional Australia: A case study. Journal of Rural Studies 22, 83–94 (2006)

Evaluating a Greek National Action on Parents' Training on ICT and Internet Safety

Nikos Manouselis[1], Katerina Riviou[2,*] , Nikos Palavitsinis[1],
Vasiliki Giannikopoulou[1], and Panayotis Tsanakas[1]

[1] Greek Research & Technology Network (GRNET S.A.), Athens, Greece
{palavitsinis,nikosm}@grnet.gr
[2] Doukas School S.A., Athens, Greece
kriviou@doukas.gr

Abstract. The Greek national action "Goneis.gr" educates and trains the parents of highschool children on the issue of safer internet, as well as on the use of ICT. Having trained more than 28.300 parents, the initiative aims at providing about 45.000 parents with the same training. Examining the Beneficiaries' degree of satisfaction by the initiative, we conducted a survey in a sample of Beneficiaries that completed the training. This paper introduces the initiative and presents the results of the survey in order to conclude to specific decisions about the future implementation of the initiative which is still running.

Keywords: Training, parents, ICT, internet.

1 Introduction

In summer 2008, a Greek national action called "Goneis.gr: Training the Parents of Highschool Pupils on ICT and Safer Internet" (http://www.goneis.gr) was launched. The "Goneis.gr" (meaning Parents.gr) initiative aims at educating and training the parents of highschool children on the issue of safer Internet. It also educates parents on how they can protect of their children from online threats.

This initiative is co-funded by the Greek Ministry of Economy and Finance and the European Union. More specifically, it concerns the training of the parents of students that enrolled in the obligatory second grade education of Greece (middle school – from 11 to 14 years old) for the school year 2008-2009. It is being implemented by the Greek Research & Technology Network (GRNET), in cooperation with the Ministry of Economy & Finance and the Ministry of Education. The initiative has a budget of 21MEuros and has provided training to over 43.000 parents so far, through 852 Educational Service Providers. It started in summer of 2008 and is ongoing until the end of spring 2009, aiming to train about 45.000 parents all over Greece [2, 3].

Beneficiaries of the programme are the parents of pupils that are enrolled in one of the three years of any type of high school (daily, experimental, musical, etc.), private or public. Beneficiaries of the programme are also the parents of students that study in schools for challenged children. This initiative aims at familiarizing the parents with

[*] Funded by GRNET during the implementation of this study.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 320–328, 2010.

Information and Communication Technologies (ICT), focusing on the Internet, its safer use and its educational applications.

Relevant projects have been identified in other countries as well. A couple of depicting examples include the “Computers in Homes (CIH)” Project in New Zealand, (http://www.computersinhomes.org.nz/christchurch.htm) and the “Egyptian Education Initiative” (http://www.eei.gov.eg/) in Egypt. The Computers in Homes (CIH) Project aims to provide all New Zealand families who are socially and economically disadvantaged with a computer, an Internet connection, relevant training and technical support. At October 2007, 1.398 families had graduated from CIH projects across New Zealand. In Egypt in the Egyptian Education Initiative (EEI) project, a specialised training program for the parents of EEI students took place, covering basic ICT skills and safe use of the Internet and also the capacity was built of 7.864 parents to use ICT tools during the specific training [1, 4].

In this paper we present extended results from the ongoing evaluation of the “Goneis.gr” project. More specifically, we present results from a survey aiming at the parents that completed the program. This paper directly addresses the topic of Training and Education and describes a way in which society can adapt to and adopt the ICT technologies.

2 Goneis.gr Initiative

The initiative’s beneficiaries are provided with free-of-charge home training from specialised instructors, as well as with access to educational packages for autonomous learning through the Internet (e-learning courses). The duration of the home based training is at least five (5) hours and it can take place in more than one visits to the Beneficiary’s house. The content of the e-learning courses has a duration of at least forty (40) teaching hours. In addition, the Beneficiaries have the option to apply for a pre-paid high-speed internet connection (ADSL) for at least two (2) months. In order to participate in the programme, the Beneficiary must have a computer (either a laptop or a desktop) with an Internet connection of any type.

The training of the parents is carried out through the cooperation with education providers that are responsible for the entire training process of each parent as far as the educational aspects are concerned. The education providers were also responsible for the e-learning platform that was used during the training which was implemented and maintained by each education provider. All e-learning platforms had to fulfill some predefined criteria in order to be used in the training procedure.

The home training that the Beneficiaries are entitled to covered the following topics:

- Basic concepts on the use of the Internet, communication and information search.
- Safe use of the Internet and child protection from malicious and inappropriate online content.
- Educational applications of the Internet and services of the Panhellenic School Network.

Additionally, the e-learning courses that the Beneficiaries undertake:

- Cover at least forty (40) teaching hours
- Provide the Beneficiaries with all the necessary knowledge to be able to participate in “Basic ICT Knowledge and PC skills” certification exams.

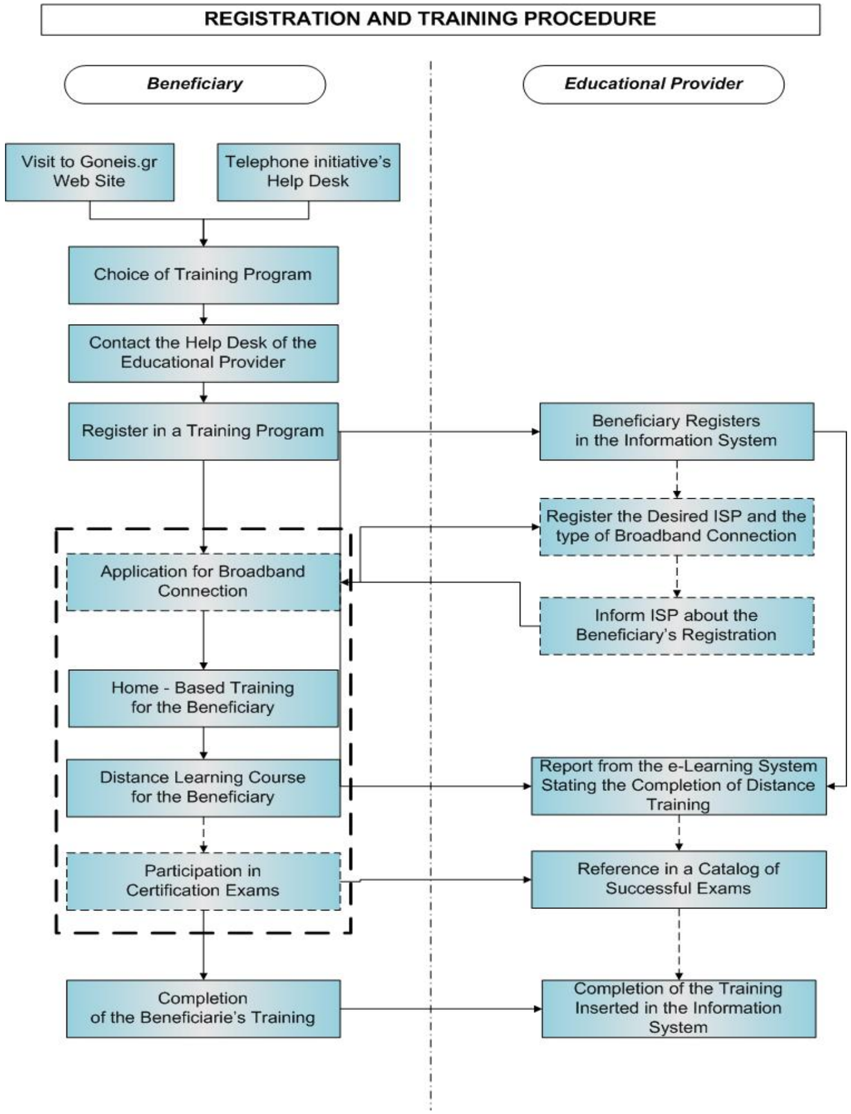

REGISTRATION AND TRAINING PROCEDURE
Beneficiary
Educational Provider
Visit to Goneis.gr Web Site
Telephone initiative's Help Desk
Choice of Training Program
Contact the Help Desk of the Educational Provider
Register in a Training Program
Beneficiary Registers in the Information System
Register the Desired ISP and the type of Broadband Connection
Application for Broadband Connection
Inform ISP about the Beneficiary's Registration
Home - Based Training for the Beneficiary
Distance Learning Course for the Beneficiary
Report from the e-Learning System Stating the Completion of Distance Training
Participation in Certification Exams
Reference in a Catalog of Successful Exams
Completion of the Beneficiarie's Training
Completion of the Training Inserted in the Information System

Fig. 1. Registration and training procedure in Goneis.gr initiative

After the completion of the e-learning courses, the Beneficiaries are entitled to participate (free of charge) in certification exams so as to acquire a certificate on "ICT knowledge and PC skills" in at least three of the units of basic knowledge (i.e. Basic concepts of ICT, Use of PC and File Management, Word Processing, Spreadsheets, Databases, Presentations and Internet Services). In Figure 1 above, the process of registering and training for "Goneis.gr" is presented.

3 Evaluation of Users' Satisfaction

This section aims to analyse the answers provided by the Beneficiaries in the survey that evaluated the initiative through relevant questionnaires deployed. The feedback was gathered through telephone communication. The methodology followed in the survey was also deployed in past relevant surveys (Manouselis & Sampson, 2004; Manouselis et al., 2004). The analysis of the answers provided by the Beneficiaries in the questionnaires provided, is carried out through the use of methods of descriptive statistical analysis (tables and graphical visualisation). For the statistical analysis and the creation of the graphs we used the Microsoft Excel.

From the overall population of about 43.000 parents that have completed their training, approximately 1.500 have been contacted through telephone, and 667 responses (completed questionnaires) were collected. The collection of this data took place during December 2008, thus corresponding to the intermediate evaluation of the programme. In the next pages the most important facts and figures from the Beneficiaries' survey are presented. The evaluation and commentary on each set of graphs and tables, takes place just after the end of each set. From a total of 667 questionnaires, 30 of them were not completed in full (0,04% of the total) so they were not taken under consideration whatsoever. When using the term "Beneficiary" in this part of the paper, we will actually be talking about the Beneficiaries that filled out the questionnaire. From the total of 667 that participated in the survey, 184 (29%) were men and 453 (71/%) were women. 28,1% of the Beneficiaries that participated in the survey, resides and was trained in the Attica region, while 11,46% resides in Thessaloniki region. The Larissa region follows with 4,55%. The other regions were more or less equally represented. Summarising Tables 1 and 2, we note that:

- The Beneficiaries were generally satisfied in high percentages (75% and 74% respectively) by the information provided to them regarding both the training procedures and their obligations and rights.
- The Beneficiaries were pretty satisfied (almost 70% rated with 4 and 5 out of 5) by the instructions provided regarding the registration to the initiative.
- Almost 72% of the Beneficiaries were satisfied by the time it took the registration code to reach them through SMS.
- Finally, 85% of the Beneficiaries stated that they were pretty satisfied by the time between their registration and the start of the training.

Table 1. Satisfaction by the information provided to the Beneficiaries related to…

The training procedures		
1 (lowest)	23	3.62%
2	51	8.03%
3	88	13.86%
4	172	27.09%
5 (highest)	301	47.40%
Their obligations and rights		
1 (lowest)	30	4.73%
2	51	8.04%
3	84	13.25%
4	181	28.55%
5 (highest)	288	45.43%

Table 2. Satisfaction of Beneficiaries by the registration process related to…

The provision of instructions for the registration		
1 (lowest)	19	3.00%
2	33	5.21%
3	77	12.15%
4	132	20.82%
5 (highest)	373	58.83%
The time from registration to receiving the registration code via SMS		
1 (lowest)	51	8.03%
2	43	6.77%
3	83	13.07%
4	127	20.00%
5 (highest)	331	52.13%
The time from registration to the start of training		
1 (lowest)	17	2.69%
2	15	2.37%
3	65	10.27%
4	140	22.12%
5 (highest)	396	62.56%

Table 3. How useful was the knowledge you acquired through the home-training?

Answer	Number of Answers	Percentage
Very much useful	328	52,23%
Useful	278	44,27%
Indifferent	22	3,5%

Table 4. Which specific modules did you choose in the context of distance learning courses?

Answer	Number of Answers	Percentage
Basic ICT concepts	369	13,07%
PC Use and File Management	399	14,13%
Word Processing	566	20,05%
Spreadsheet	496	17,57%
Databases	202	7,16%
Presentations	262	9,28%
Internet Services	529	18,74%

Table 5. The level of users' satisfaction with the material and content of the distance learning courses

Answer	Number of Answers	Percentage
1 (lowest)	9	1,48%
2	21	3,46%
3	41	6,75%
4	217	35,75%
5 (highest)	319	52,55%

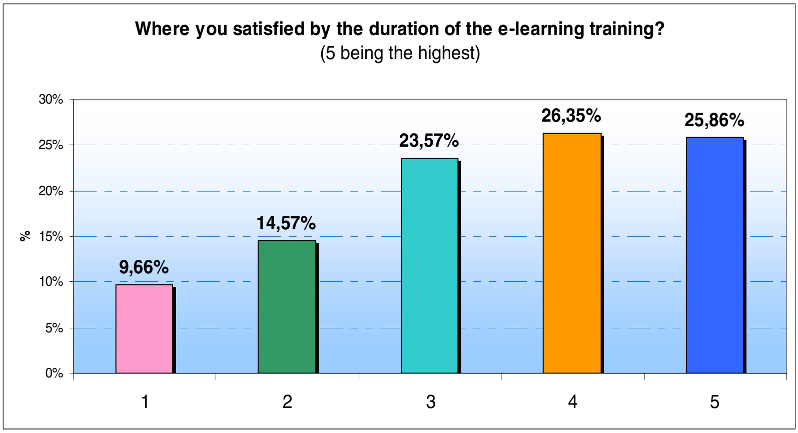


Fig. 2. Percentage distribution of answers to the question “Rate your degree of satisfaction from the duration of the e-learning courses”

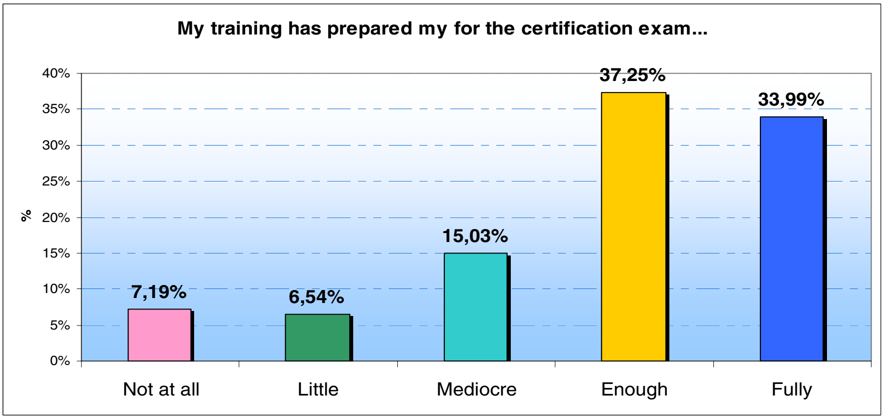


Fig. 3. Percentage distribution of answers to the question “Do you think that the training you received prepared you enough for the certification exams?”

Table 6. Level of satisfaction with the Goneis.gr web portal and its functionalities

Answer	Number of Answers	Percentage
1 (lowest)	0	0%
2	7	1,76%
3	41	10,33%
4	181	46,59%
5 (highest)	168	42,32%

Table 7. Level of satisfaction with the support offered through the help desk

Answer	Number of Answers	Percentage
1 (lowest)	1	0,43%
2	2	0,87%
3	8	3,48%
4	38	16,52%
5 (highest)	181	78,70%

As the related figures and data indicate:

- 52% of the Beneficiaries believe that the new knowledge acquired from the home training are much useful whereas 44% states they are just useful while a mere 3.50% though of the acquired knowledge to be indifferent.
- The most popular module of the e-learning courses is the Word Processing with 20%, while Internet Services follow with 19% and Spreadsheets with 17%.
- 26% of the Beneficiaries are fully satisfied from the duration of the e-learning courses (rated with 5 out of 5) while a similar percentage declared that they are very much satisfied (rated with 4 out of 5).
- 53% of the Beneficiaries are fully satisfied from the content/material provided with the e-learning courses (rated 5 out of 5) whereas 36% rated this with 4 out of 5.
- Percentages of 34% and 30% of the Beneficiaries think that their training prepared them fully and fully enough respectively so that they could handle the certification exams.
- 70% of the Beneficiaries visited the Goneis.gr Web Portal whereas 23% did not visit the portal as they did not need to do so. Only 7% of the Beneficiaries are not informed for the portal's existence.
- 42% of the Beneficiaries graded with "excellent" their degree of satisfaction by the operation of the Goneis.gr Web Portal (rated with 5 out of 5) whereas 46% are very much satisfied (rated 4 out of 5).
- 48% of the Beneficiaries did not need to contact the helpdesk whereas 38% of them did contact the helpdesk to address their questions regarding the initiative. 14% declared that they did not know about the existence of the helpdesk.
- The majority of the Beneficiaries is satisfied by the operation of the helpdesk as 78.7% of those that contacted the helpdesk characterized their degree of satisfaction as "excellent" (rated with 5 out of 5) whereas 17% of them are very much satisfied (rated with 4 out of 5).

Again, as it illustrated by the available data:

- 38% characterised the percentage of knowledge acquired from their participation to the program as very much satisfying whereas 51% though of the knowledge as simply satisfying. Only 11% of the Beneficiaries thought that the acquired knowledge think their participation to the initiative was little.
- 37% of the Beneficiaries are totally satisfied from their participation in the programme (rated 5 out of 5), whereas 45% of them are very satisfied (rated 4 out of 5). 12% of the Beneficiaries are partially satisfied (rated 3 out of 5), while the percentage of them that are less than satisfied only reaches 6%.

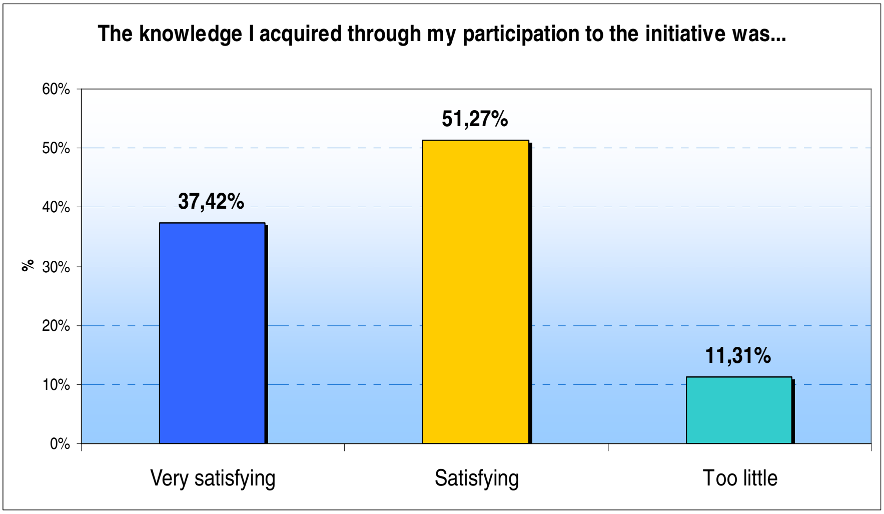


Fig. 4. Percentage distribution of answers to the question “Do you think that the percentage of knowledge acquired though your participation in the initiative was…”

Table 8. Level of satisfaction with the participation in the initiative

Answer	Number of Answers	Percentage
Not at all	16	2,54%
Little	24	3,80%
More or less	78	12,36%
Partially	283	44,85%
Fully	230	36,45%

4 Conclusions

Summarising the main points that concern the evaluation of the Goneis.gr initiative we must state that:

- The respective percentages of Beneficiaries that are more than satisfied with the initiative are over 80% which indicates that the initiative is successfully deployed in all of its aspects (promotion, implementation, administrative, etc.)
- Focusing a little bit on the Beneficiaries, we see that their satisfaction regarding the initiative and its services equals with 4,09 in the 5-grade scale.
- The duration of the home-based training and the e-learning courses is highly appreciated by the Beneficiaries thus indicating that the whole training process is well-designed and implemented.
- The Goneis.gr Web Portal is widely praised both by the Beneficiaries indicating the quality and high functionality of the Web Portal.
- The helpdesk support is also highly appreciated by all participants of the initiative indicating the willingness and high level of support that the helpdesk staff provides.

The Goneis.gr initiative has proven to be very successful thus providing the basis for a possible repetition of the program and/or the extension of the training framework to other population groups that were not addressed in the first implementation of the initiative. The study presented in this paper has already indicated problematic aspects that can be looked at in order to increase the satisfaction of the public and the educational outcomes of the process. Also, some exciting and fruitful opportunities have risen that can multiply the initiative's added value if they are carefully exploited.

References

1. CEN, A Family Guide to Internet. Children Educational Network (2008), `http://kidsafe.com/wp-content/uploads/2009/01/cen-online-safety-guide.pdf` (accessed on 7/2/2009)
2. Eurobarometer, 2008. Flash Eurobarometer 248: Towards a safer use of the Internet for children in the EU – a parents' perspective, European Commission (2008)
3. Harris Interactive-McAfee, Survey on the Usage of the Internet by Teens (2008), `http://www.mcafee.com/us/about/press/corporate/2008/20081022_095000_x.html` (accessed on 9/2/2009)
4. Lenhart, A., Madden, M.: Teens, Privacy, and Online Social Networks. Pew Internet and American Life Project, April 18 (2007), `http://www.pewinternet.org/pdf..rivacy_SNS_Report_Final.pdf` (accessed on 7/2/2009)
5. Manouselis, N., Sampson, D., Charchalos, M., Tsilibaris, X.: Evaluation of the Greek Go-Online Web Portal for e-Business Awareness and Training of vSMEs: Log Files Analysis and User Satisfaction Measurement. In: Proc. of the 9th International Telework Workshop, Crete, Greece (September 2004)
6. Manouselis, N., Sampson, D.: Multiple Dimensions of User Satisfaction as Quality Criteria for Web Portals. In: The Proc. of the IADIS WWW/Internet 2004 Conference, Madrid, Spain (March-October, 2004)

Evaluating a Greek National Action on Students' Training on ICT and Programming Competences

Katerina Riviou[1,*], Katerina Papakonstantinou[2], and Panayotis Tsanakas[2]

[1] Doukas School S.A., Athens, Greece
kriviou@doukas.gr
[2] Greek Research & Technology Network (GRNET S.A.), Athens, Greece
papak@grnet.gr

Abstract. It is well understood that university graduates, regardless of discipline, must have appropriate information and communication technology (ICT) competencies to function and be employable in the modern world. Nevertheless, the results of surveys indicate significant deficiencies in the use of ICT by students of higher education. e-kpaidefteite.gr is an initiative launched by the Greek government that aims to train and certify students of higher education on ICT. This paper presents the results of two separate surveys that took place during the period December 2008 - January 2009. The first survey targeted the students that have completed the programme and the second one the educational providers that participated in the programme and offered the training to the beneficiaries.

Keywords: National action, training, students, ICT.

1 Introduction

According with the Partnership for 21st Century Skills' vision for the 21st Century Student success in the new global digital economy, students should master skills, knowledge and expertise in order to succeed in work and life. Among these skills are Information, Media and Technology Skills [1]. Moreover, it is well understood that university graduates, regardless of discipline, must have appropriate information and communication technology (ICT) competencies to function and be employable in the modern world [2], [3].

Universities nowadays are using more ICT in their teaching and learning environments. According to a survey conducted in university students by University of Rome in the context of "Easy" project the e-learning services utilised the most by students are: course management (timetables, lessons), downloading of tools/slides/papers/articles and communication with teachers. Also, three types of students can be pinpointed according to their technological competencies:

- The students who judge themselves to be competent are a small minority (about 20% of the total).

[*] Funded by GRNET during the implementation of this study.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 329–338, 2010.

- A second group is that of the "needy", who recognise the limits of their current competencies and express interest and need of widening them.
- A third group is made up of those who express an interest in distance learning, but at the same time don't feel the need for acquiring specific competencies [4].

The 2.000 university students surveyed in "SPOT+" project were interested in the use of ICT for information exchange, such as 'to ask questions of experts and relevant people no matter where they are' and 'to share information and ideas with people who have similar interests' [5].

Nevertheless, for an instance an anonymous multiple-choice survey self-assessed the spreadsheet skills of students enrolled in first-year units and the results of the survey indicate significant deficiencies in the use of spreadsheets. There is a significant proportion of students who are unable to use spreadsheets as part of their education at the start of their university studies [6].

Also, if almost everyone across Europe is confident that they can read, write and do arithmetic, they are less so when it comes to new key competencies. Only 58% of respondents said they could use a computer. Half of them said they could not use the Internet. The lack of ICT skills is especially marked in Greece and Portugal with two-thirds of respondents claiming they could not use a computer [7].

In Greece there has been a national initiative dealing with the promotion of ICT use by university students called "Des tin Psifiaka.gr" (http://www.destinpsifiaka.gr/), implemented already three times, which funded the purchase of a personal computer from students that passed the panhellenic exams and enrolled in the tertiary education [8]. In the initial phase of the project (2007), 11.586 students from a total of 13.613 registered ones purchased the personal computer of their choice leading to a project's success rate of 85%. In the second phase of the initiative (2008) the purchases of computers were 13.377 and the project's success rate 99%. In the final phase (2009) the registered beneficiaries were 17.789 and the purchases 15.871, thus leading to a success rate of 89%.

Also, through the national initiative "Diodos" (http://www.diodos.edu.gr/), high-speed internet connection (ADSL) is offered in advantageous price to students of higher education, so that they can search information and data, communicate with fellow students and exchange information regarding running projects, attend e-courses, have access in digital libraries, etc [9]. In January 2007 Greek Research & Technology Network (GRNET) conducted a survey among 4.500 of the beneficiaries and the most important findings are: 92% characterises the initiative as «good» or «very good», 74% thinks of the quality of the service provided as «good» or «very good». Half of the interviewed beneficiaries said that they would get an ADSL connection even if the programme did not exist. Moreover, at the current time active internet connections are estimated about 40.000 and the average number of new daily applications is 150.

Consequently, the two above mentioned actions could be characterised as extremely successful and to this direction, a new major national initiative called "e-kpaidefteite.gr: Students' Training on ICT & Programming Competences" trains and gives the opportunity to students to participate (free of charge) in certification exams so as to acquire a certificate on "ICT knowledge and PC skills". This initiative is co-funded by the Greek Ministry of Economy and Finance and the European Union. It concerns the training of students that enrolled in the third grade education of

Greece for the academic years 2005, 2006, 2007. It is being implemented by the GRNET, in cooperation with the Ministry of Economy and Finance, the Ministry of Education and the Ministry of Development. The initiative has a budget of 36MEuros and has provided training to over 55.000 students, through 939 Educational Service Providers. The training started in the summer of 2008 and ended after an extension in the end of November 2008, aiming at 60.000 students all over Greece.

In this paper we present results from the evaluation of the "e-kpaidefteite.gr" project. More specifically, we present results from the application of two separate surveys. The first one aiming at the Students that completed the programme and the second aiming at the Educational Providers that offered the training. The survey is correspondent to the ongoing one implemented in the initiative "Goneis.gr: Training Parents' Training on ICT & Internet Safety" aiming to train the parents of high school children on the issue of safer Internet and how they can protect their children from online threats [10], [11].

2 e-kpaidefteite.gr National Initiative

The beneficiaries of the initiative are all students that passed the panhellenic examinations and enrolled in departments and schools of third grade education in the academic years 2005, 2006, 2007, as well as the students of the Hellenic Open University, independent of their grade. Beneficiaries are also disabled students that enrolled in 3% percentage in all departments or schools at the same academic period. The initiative aims at familiarising and certifying the students with ICT.

For students to get granted for their training and certification, they have to select the educational package of their choice from the e-kpaidefteite.gr web portal and use their "Personal Number", at their registration in the Educational Provider of their choice with a self-contribution of 10% of the total cost of the training. The justifying documents needed to be given to the educational provider are the identity and the student identification or a certification from the beneficiary's department's secretariat.

The initiative's beneficiaries can be educated and get certification on basic, advanced and specialised ICT skills such as: info search on the net/internet services/content search in digital libraries, e-mail, word processing, spreadsheets, web design, network management, video and image processing programs, etc. Students can choose the teaching method they prefer, that is attending lectures/labs, e-learning courses in the Educational Providers' facilities or at their home and finally a blended method (lectures and e-learning). In any case, training's duration is at least forty (40) hours. After the completion of their training, the Beneficiaries have to participate in certification exams so as to acquire a certificate on the educational packages they have attended, in order to get funded by the initiative.

The training of the students is carried out through the cooperation with educational providers that are responsible for the entire training process of each student as far as the educational aspects are concerned. The Educational Providers are participating in the programme according to a number of pre-defined eligibility criteria and should submit their educational packages online at the relative information system (http://www.eduoffers.gr). The information system was developed with the aim to automate the following actions: educational packages' submission in order to get evaluated, monitoring of the evaluation procedure and beneficiaries' registration in the educational packages of their choice. Educational providers checked the completion of the training by the Beneficiaries, either in the case of face-to-face training (absence keeping), or in case of e-learning by monitoring beneficiaries' log-on hours.

The quality of the training is monitored through a Quality Control mechanism set up by the coordinating organisation. More specifically, sampling checks were implemented based on the training schedule submitted in the information system by the Educational Providers. Specifically for the e-learning courses, the Educational Providers had to state the way they monitor the time Beneficiaries have used the educational packages. If the Monitoring Committee comes up with shortcomings from the Educational Providers' side, penalties are imposed to them.

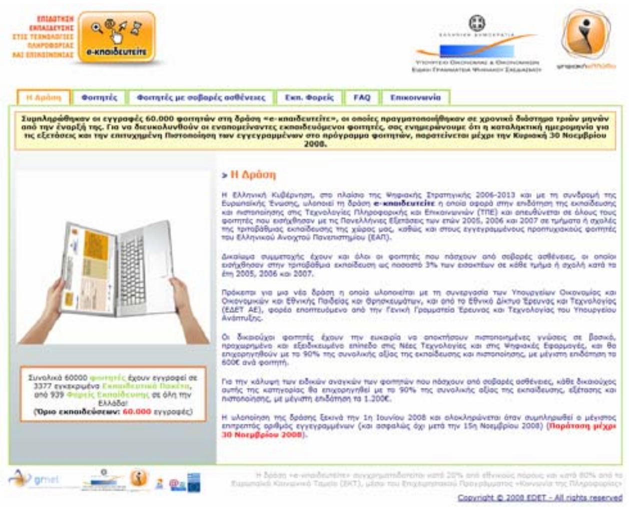
Educational providers submitted their educational packages online, at the relative information system set up by the coordinating organisation, following the procedure described in the manual available on e-kpaidefteite.gr web portal, or the step-by-step hints existing in the system. In any case Educational providers could contact the Helpdesk set up by the coordinating organisation for additional support.

3 e-kpaidefteite.gr Web Portal

A crucial element that defined the success and dissemination of the e-kpaidefteite.gr initiative is the deployment of a web portal that contains all the necessary information for all the involved parties (Beneficiaries and Educational Providers). The structure of the web portal is fairly simple and easy to comprehend, allowing even the most inexperienced users to navigate through the various pages and get all the necessary information regarding their participation in the initiative.

The overall structure of the e-kpaidefteite.gr web portal is the following:

- The Homepage, that presents the logos of the initiative and the participating organisations. It also gives a brief but comprehensive outline of the initiative.
- The Navigation Menu contains hyperlinks to all the main pages of «e-kpaidefteite.gr» web portal and it is included in all the web portal pages. Its options include:
  - o The Action, with information regarding the initiative, its goals and its Beneficiaries.
  - o Students (Beneficiaries), with information regarding the categories of Beneficiaries that can participate in the action, the way in which they can participate and get informed about the educational packages offered.
  - o Disabled Students, with information regarding the way in which they can participate.
  - o Educational Providers, with information regarding their participation in the initiative and the specifications of the educational packages. This page also provides details on the Educational Providers' obligations and the support of the beneficiaries through the establishment of a helpdesk. The Quality Control Mechanism is also presented in this section.
  - o Frequently Asked Questions (FAQ), with answers in frequently asked questions by the Beneficiaries and the Educational Providers.


ΕΠΙΔΟΤΗΣΗ ΕΚΠΑΙΔΕΥΣΗΣ ΣΤΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ
e-κπαιδευτείτε
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΨΗΦΙΑΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ψηφιακή ελλάδα
Η Δράση
Φοιτητές
Φοιτητές με σοβαρές ασθένειες
Εκπ. Φορείς
FAQ
Επικοινωνία
grnet

Συμπληρώθηκαν οι εγγραφές 60.000 φοιτητών στη δράση «e-κπαιδευτείτε», οι οποίες πραγματοποιήθηκαν σε χρονικό διάστημα τριών μηνών από την έναρξή της. Για να διευκολυνθούν οι εναπομείναντες εκπαιδευόμενοι φοιτητές, σας ενημερώνουμε ότι η καταληκτική ημερομηνία για τις εξετάσεις και την επιτυχημένη Πιστοποίηση των εγγεγραμμένων στο πρόγραμμα φοιτητών, παρατείνεται μέχρι την Κυριακή 30 Νοεμβρίου 2008.

> Η Δράση

Η Ελληνική Κυβέρνηση, στο πλαίσιο της Ψηφιακής Στρατηγικής 2006-2013 και με τη συνδρομή της Ευρωπαϊκής Ένωσης, υλοποιεί τη δράση **e-κπαιδευτείτε** η οποία αφορά στην επιδότηση της εκπαίδευσης και πιστοποίησης στις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) και απευθύνεται σε όλους τους φοιτητές που εισήχθησαν με τις Πανελλήνιες Εξετάσεις των ετών 2005, 2006 και 2007 σε τμήματα ή σχολές της τριτοβάθμιας εκπαίδευσης της χώρας μας, καθώς και στους εγγεγραμμένους προπτυχιακούς φοιτητές του Ελληνικού Ανοιχτού Πανεπιστημίου (ΕΑΠ).

Δικαίωμα συμμετοχής έχουν και όλοι οι φοιτητές που πάσχουν από σοβαρές ασθένειες, οι οποίοι εισήχθησαν στην τριτοβάθμια εκπαίδευση ως ποσοστό 3% των εισακτέων σε κάθε τμήμα ή σχολή κατά τα έτη 2005, 2006 και 2007.

Πρόκειται για μια νέα δράση η οποία υλοποιείται με τη συνεργασία των Υπουργείων Οικονομίας και Οικονομικών και Εθνικής Παιδείας και Θρησκευμάτων, και από το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), φορέα εποπτευόμενο από την Γενική Γραμματεία Έρευνας και Τεχνολογίας του Υπουργείου Ανάπτυξης.

Οι δικαιούχοι φοιτητές έχουν την ευκαιρία να αποκτήσουν πιστοποιημένες γνώσεις σε βασικό, προχωρημένο και εξειδικευμένο επίπεδο στις Νέες Τεχνολογίες και στις Ψηφιακές Εφαρμογές, και θα επιχορηγηθούν με το 90% της συνολικής αξίας της εκπαίδευσης και πιστοποίησης, με μέγιστη επιδότηση το 600€ ανά φοιτητή.

Για την κάλυψη των ειδικών αναγκών των φοιτητών που πάσχουν από σοβαρές ασθένειες, κάθε δικαιούχος αυτής της κατηγορίας θα επιχορηγηθεί με το 90% της συνολικής αξίας της εκπαίδευσης, εξέτασης και πιστοποίησης, με μέγιστη επιδότηση τα 1.200€.

Η υλοποίηση της δράσης ξεκινά την 1η Ιουνίου 2008 και ολοκληρώνεται όταν συμπληρωθεί ο μέγιστος επιτρεπτός αριθμός εγγεγραμμένων (και ασφαλώς όχι μετά την 15η Νοεμβρίου 2008) (**Παράταση μέχρι 30 Νοεμβρίου 2008**).

Συνολικά 60000 φοιτητές έχουν εγγραφεί σε 3377 εγκεκριμένα Εκπαιδευτικά Πακέτα, από 939 Φορείς Εκπαίδευσης σε όλη την Ελλάδα!
(**Όριο εκπαιδεύσεων:** **60.000** εγγραφές)

Η δράση «e-κπαιδευτείτε» συγχρηματοδοτείται κατά 20% από εθνικούς πόρους και κατά 80% από το Ευρωπαϊκό Κοινωνικό Ταμείο (ΕΚΤ), μέσω του Επιχειρησιακού Προγράμματος «Κοινωνία της Πληροφορίας»

Copyright © 2008 EDET - All rights reserved

Fig. 1. The e-kpaidefteite.gr Web Portal

- o Communication, with information regarding the ways that the Beneficiaries and Educational Providers can communicate with the coordinating organisation of the initiative.

4 Evaluation of Users' Satisfaction

This section aims to analyse the answers provided by the Beneficiaries and the Educational Providers in the survey that evaluated the initiative through relevant questionnaires deployed. The feedback was gathered through telephone communication in the case of the Beneficiaries and through an online questionnaire in the case of the Educational Providers.

4.1 Methodology

The analysis of the answers provided by the Beneficiaries and the Educational Providers is carried out through the use of methods of descriptive statistical analysis (tables and graphical visualisation).

For the statistical analysis and the creation of the graphs we used the Microsoft Excel, as well as the functions of the open source software LimeSurvey.

4.2 Beneficiaries' Survey

From the overall population of about 55.000 students that have completed their training, approximately 5.141 have been contacted through telephone and 1.556 responses (questionnaires) were collected. The collection of this data took place during 04-08 December 2008.

In the next pages the most important facts and figures from the Beneficiaries' survey are presented. From a total of 1.556 questionnaires, 24 of them were not completed in full (0,01% of the total), so they were not taken under consideration. When using the term "Beneficiary" in this part of the paper, we refer to the Beneficiaries that completed the questionnaire.

From the total of 1.556 Beneficiaries that participated in the survey, 545 (34%) were men and 1.047 (66%) were women.

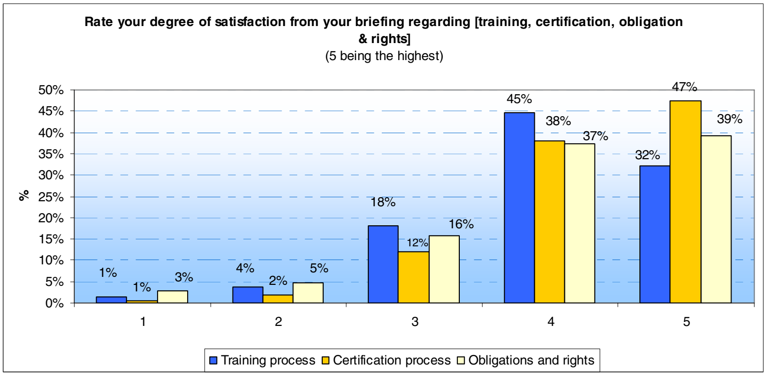


Fig. 2. Percentage distribution of answers to the question "Rate your degree of satisfaction from your briefing regarding: the training, the certification process, your obligations and rights"

Among the most important findings regarding the Beneficiaries' satisfaction on the training and certification process:

- 32% of the Beneficiaries are fully satisfied (rated with 5 out of 5) with the briefing they received regarding the training process, 47% with the briefing regarding the certification process, and 39% with the briefing regarding their obligations and rights (Fig. 2).
- The most popular need regarding ICT was certification for the Beneficiaries' career with percentage 68%, specialised ICT knowledge with 28%, while info search on the net/internet services/content search in digital libraries follows with 21% and simple skills (e-mail, word processing, spreadsheets, etc) with 13%.
- 30% characterised the knowledge acquired from their participation in the programme as very satisfying, whereas 64% thought of the knowledge as merely satisfying. Only 6% of the Beneficiaries thought of the acquired knowledge to be indifferent.
- Percentages of 33% and 58% of the Beneficiaries think that their training prepared them fully and fully enough, respectively, so that they could handle the certification process.
- 40% of the Beneficiaries are fully satisfied with the e-learning content (rated with 5 out of 5), whereas 43% rated it with 4 out of 5.
- Percentages of 66% and 62% of the Beneficiaries are fully satisfied with their tutors' preparation and the promotion of their active participation in the learning process by their tutors respectively (Fig. 3).

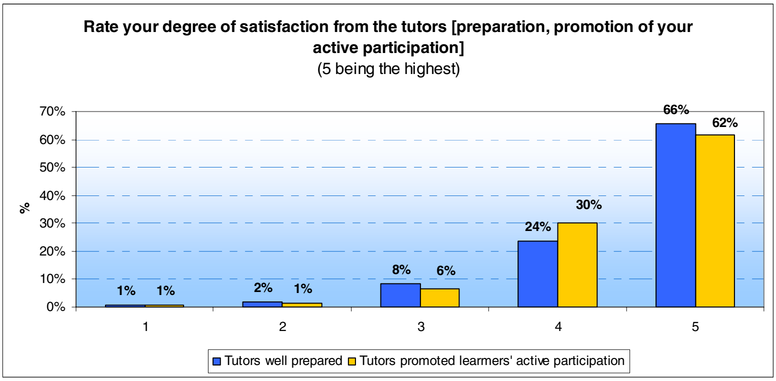


Fig. 3. Percentage distribution of answers to the question "Rate your degree of satisfaction from the tutors regarding their preparation and the promotion of your active participation in the training process"

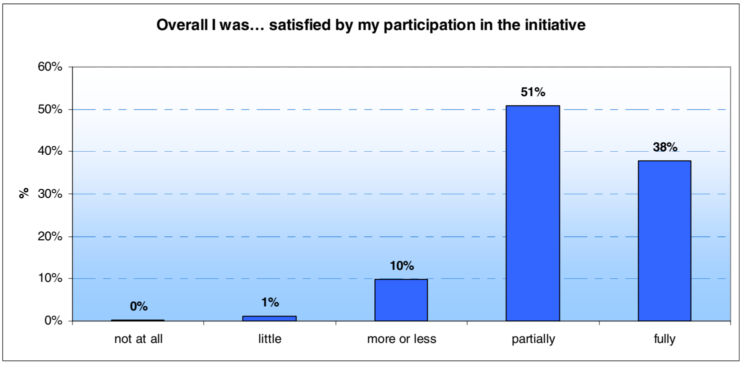


Fig. 4. Percentage distribution of answers to the question "Please rate your overall level of satisfaction from your participation in the initiative"

Among the most important findings regarding the Beneficiaries' satisfaction from the supportive infrastructure:

- 51% of the Beneficiaries are fully satisfied with the technical support and 42% with the facilities where the programme was implemented.
- 79% of the Beneficiaries are fully satisfied with the duration of the initiative, while a percentage of 16% found it insufficient.
- 49% of the Beneficiaries visited the e-kpaidefteite.gr Web Portal whereas 19% did not, since they did not need to do so. 32% of the Beneficiaries were not informed about the portal's existence. 28% of the Beneficiaries graded with "excellent" their degree of satisfaction by the operation of the e-kpaidefteite.gr Web Portal (rated with 5 out of 5), whereas 51% are very satisfied (rated with 4 out of 5).

- 27% of the Beneficiaries did not need to contact the helpdesk, whereas 38% of them did contact the helpdesk to address their questions regarding the initiative. 60% declared that they did not know about the existence of the helpdesk. 53% of the Beneficiaries that contacted the helpdesk characterised their degree of satisfaction as “excellent” (rated with 5 out of 5), whereas 30% of them are very satisfied (rated with 4 out of 5).
- 38% of the Beneficiaries are totally satisfied from their participation in the programme (rated with 5 out of 5), whereas 51% of them are very satisfied (rated 4 out of 5). 10% of the Beneficiaries are partially satisfied (rated with 3 out of 5), while the percentage of the less than satisfied only reaches 1% (Fig. 4).

4.3 Educational Providers’ Survey

The Educational Service Providers that participated in the initiative were 939. After contacting all of them via e-mail, 336 provided their feedback in an online version of the evaluation questionnaire up until late January 2009.

Among the most important findings regarding the Educational Providers’ satisfaction from the initiative:

- 52% of the Educational Providers rated their degree of satisfaction on the e-kpaidefteite.gr web portal as excellent (rated with 5 out of 5), 47% rated their degree of satisfaction by the helpdesk support as excellent, and 51% were fully satisfied with the information system handling their offers (Fig. 5).
- 52% of the Educational Providers are fully satisfied with the initiative as a whole, whereas 42% of them are very satisfied. 5% of the Educational Providers are partially satisfied, while 1% of them are less than satisfied (Fig. 6).

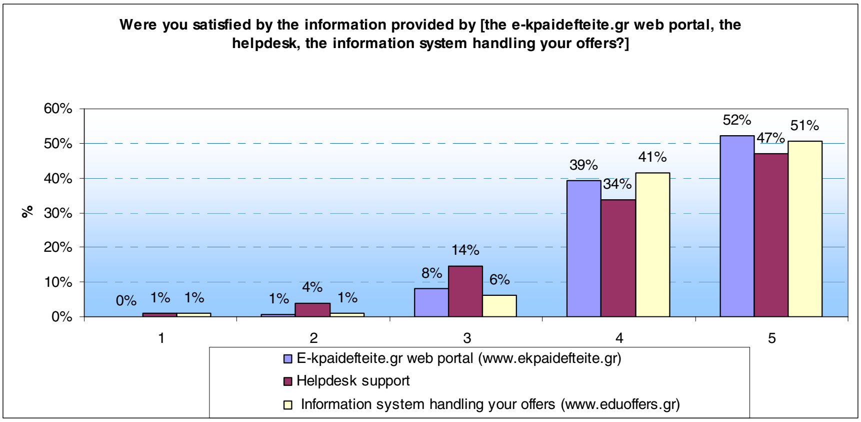


Fig. 5. Percentage distribution of answers to the question “Please rate the degree of your satisfaction from: the e-kpaidefteite.gr Web Portal, the Helpdesk and the information system handling your offers”

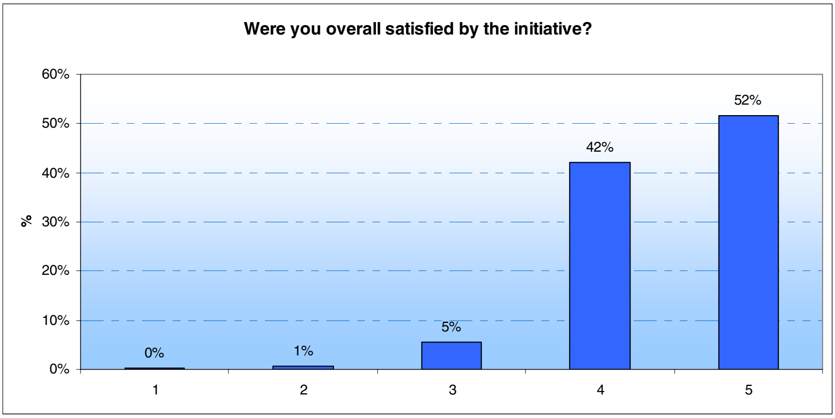


Fig. 6. Percentage distribution of answers to the question “Did the initiative satisfy you as a whole (i.e. in terms of training, organisation, etc)?”

5 Conclusions

Summarising the main points that concern the evaluation of the e-kpaidefteite.gr initiative:

The respective percentages of Beneficiaries and Educational Providers that are more than satisfied with the initiative are over 80%, which indicates that the initiative is successfully deployed in all of its aspects (promotion, implementation, administrative, etc.)

Focusing on the Beneficiaries, their satisfaction regarding the initiative and its services equals with 4,25 in the 5-grade scale, whereas the Educational Providers’ satisfaction is of the same level (4,28 in the 5-grade scale).

The e-kpaidefteite.gr Web Portal is widely praised both by the Beneficiaries and the Educational Providers indicating the quality and high functionality of the Web Portal.

The helpdesk support is also highly appreciated by all participants of the initiative indicating the willingness and high level of support that the helpdesk staff provides.

References

1. Partnership for 21st Century Skills: Framework for 21st Century Learning, http://www.21stcenturyskills.org/documents/framework_flyer_updated_jan_09_final-1.pdf
2. Watson, G., Proctor, R., Finger, G., Lang, W.: Education Students’ Views on the Integration of ICT into their Undergraduate Learning Experiences. In: ETL Conference, Logan Campus, Griffith University (2004), http://www98.griffith.edu.au/dspace/bitstream/10072/2520/1/30269_1.pdf

3. Spathis, Ch.: ICT Use by Students of Business Studies. In: 4th Hellenic Conference with International Participation on Information and Communication Technologies in Education, pp. 655–660. University of Athens, Athens (2004)
4. University of Rome, Faculty of Sociology: Easy, E-Learning European Project, Why conduct a Survey on the Easy Campus Students? (2007), http://www.easy-elearning.net/downloads/final_meeting/Annex_32_9.pdf
5. Mancinelli, E.: Student's Perceptions of ICT Relevance for University Studies (2005), http://www.elearningeuropa.info/directory/index.php?lng=el&page=doc&doc_id=5990&doclng=6
6. Kieran, L.: A Survey of First-Year University Students' Ability to Use Spreadsheets. Spreadsheets in Education (eJSiE) 1(2), 52–66 (2004)
7. IP/03/619, Europeans and Lifelong Learning: Main Findings of a Eurobarometer Survey, European Commission (2003)
8. Greek Research & Technology Network (GRNET S.A.), Des tin Psifiaka Project, http://www.destinpsifiaka.gr/
9. Greek Research & Technology Network (GRNET S.A.), Diodos Project, http://diodos.gsrt.gr/
10. Manouselis, N., Riviou, K., Palavitsinis, N., Giannikopoulou, V.: Goneis.gr: Training Greek Parents on ICT and Safer Internet. In: WSKS 2009. LNCS/CCIS. Springer, Crete (2009)
11. Manouselis, N., Riviou, K., Palavitsinis, N., Giannikopoulou, V., Tsanakas, P.: Evaluating a Greek National Action on Parents' Training on ICT and Internet Safety. In: Sideridis, A.B., Patrikakis, Ch.Z. (eds.) e-Democracy 2009. LNICST, vol. 26, pp. 320–328. Springer, Heidelberg (2009)

Session 9

Collaboration, Social Networking, Blogs

OPSIS: An Open, Preventive and Scalable Migration Information System

George Pentafronimos*, Thanos Karantjias, and Nineta Polemi

University of Piraeus, Informatics Department
80 Karaoli & Dimitriou Str,
185 34 Piraeus, Greece
Tel.: +302104142270
{gpentas,karant,dpolemi}@unipi.gr

Abstract. Existing research initiatives and migration-oriented automated tools and services fail to provide a complete, robust and widely available framework for collaborative development of a common pan-European migration policy and the harmonization of processes and civil status documents formats. Identifying these weaknesses and based on advanced open-source technologies and interactive software tools, we propose an Open, Preventive and Scalable migration Information System, namely OPSIS, that is able to provide a consistent framework for collaboratively harmonizing common migration policies, procedures and data formats related to civil status documents.

Keywords: Migration Information Systems, harmonization, collaboration.

1 Introduction

In recent years of globalization and free-movement, the heterogeneous national migration proposals, policies, practices and procedures become stumbling blocks for implementing a common, balanced, European civil migration policy. Thus, the 18,5 million[1] legal immigrants residing in Europe is an economic non-exploitable asset with major consequences in growth and employment. Aiming at reversing this disappointing situation and ensuring Europe's prosperity, an emerging requirement for policy and decision makers is to collaboratively contribute towards strengthening on one hand the facilitation of legal immigrants to enter and move freely in the European labour markets and on the other, the fight against illegal immigration, smuggling and trafficking of human beings.

Legal, political, technological and societal differences in the Member States as well as the inability of all possible stakeholders to interactively and persistently collaborate in a synchronous manner, leading to their isolation from decision making processes and the formulation of balanced migration proposals, are the main causes blocking the adoption of a common, acceptable, and applicable pan-European migration policy. Therefore, an urgent need is implied for effective, collaborative actions engaging migration

[*] Eurostat 2008.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 341–350, 2010.

policy makers and public administrators in order to identify, model, analyse, monitor and harmonise balanced national migration policies, proposals and practices.

The proposed system, OPSIS, responds to this need since it is a centralized collaborative, balanced migration information tool based on existing standards and open-source software technologies. Offering a user friendly interactive and robust collaboration framework OPSIS constitutes an innovative prototype through which: Public administrators (e.g. Ministries of Interiors, Police, and Municipalities) can report, identify, model, analyze and reengineer their national migration policies, specific procedures, data formats and their organizational structures; Policy and Decision makers (e.g. European Agency of Migration Policies, European Agency for the Management of Operational Cooperation at the External Borders) can monitor and benchmark national practices, build harmonized E.U. procedures, processes and data formats, identify ongoing (legal, security, privacy, organizational, political) gaps and barriers at E.U. level building a common E.U. migration policy; IT developers can be guided upon the necessary governmental processes, procedures and data formats in order to build interoperable, secure, cross border e/m-government services. Thus, OPSIS tool is able to improve migration policy harmonisation processes.

The rest of the paper is organized as follows: Section 2 describes existing research projects and automated migration tools illustrating their deficiencies. In Section 3, all required core design principles are identified, specifying their implementation. Section 4 provides a descriptive OPSIS system architecture overview analyzing its basic components. Finally, Section 5 draws conclusions and provides future research directions.

2 State of the Art

Non-homogeneous migration policies, practices and procedures along with organisational, legal, technological, societal and political differences are main stumbling blocks for E.U. governmental organisations to: monitor, trace and audit illegal movement; legal citizens to practice their civil right to move freely or seek employment in the region and finally to create a common European migration policy.

Recently, several projects have been launched to research and elaborate on the existing problematic situation while the implementation and adoption of Migration Information Systems (MIS) is emerging slowly. Action and development programs funded or co-funded by the E.C. such as the EC-UN Joint Migration [1] and ARGO [2] as well as research projects like Euromed Migration II [3] and those under the MARRI Initiative [4], are mainly aiming at promoting administrative cooperation and supporting civil society organizations and local authorities. Generally, their objectives are to bring together practitioners and further develop networking and partnerships, usually by conducting training actions and staff exchanges, studies, conferences or seminars. Furthermore, PROMNISTAT [5] and DCIM-EU [6] projects focus on the establishment of comparable indicators for data collection on migration issues while the objectives of ERLAIM project [7] are policy-oriented, providing awareness for the integration of immigrants by exchanging good practices, policies and experiences.

Identifying the continuously evolving nature of migration issues as well as the need for adopting automated procedures and widely available technological tools in order to facilitate in a more holistic way the development and future advancement of common migration policies, more sophisticated initiatives have introduced a number of software tools in order to enhance traditional ways of migration information diffusion and exchange. Representative example is MIPEX [8] that provides informative national reports and comparative statistical data, as well as the web-based services offered by the European Civil Registry Network [9] and the Information Exchange System of European Migration Network (EMN) [10] whose main objective is the exchange of Civil Acts documents and other relative data. On the other hand more generic approaches such as the Policy Mix Web Portal [11] and the Common Assessment Framework (CAF) [12] constitute significant sources of information and experience for further analysis and possible interrelation with migration issues.

Unfortunately, most of these tools are isolated and none of them are interoperable with other IT migration systems and collaborative/interactive with the decisions makers so they can use them persistently in order to monitor, analyse, reengineer or harmonise their migration procedures, and processes supporting their national migration policies.

Consequently, there is an urgent, acknowledged need for more holistic and effective collaborative actions among Member States in order to harmonise national migration policies and specific migration procedures adopting more sophisticated methods by fully-exploiting the existing technological advancement. This paper proposes the OPSIS tool, a collaborative, migration information system that provides the opportunity to all stakeholders to identify, model and analyse national migration policies and practices as well as to monitor and harmonise easily procedures and data formats, thus accelerating their efforts towards a common European migration policy.

3 OPSIS Core Design Principles

The fundamental benefit of the OPSIS platform is the consistent usage of a standards-based architecture, which integrates easily modified and expanded functionality, and reengineered services, adopting the following core design and implementation principles.

Modularity: In OPSIS every module is a component of a larger system, and operates within that system independently from the operation of the other components. Consequently, OPSIS is able to decompose an operating problem into a small number of less complex sub-problems, which are connected by a simple structure, and independent enough to allow further work to proceed separately on each item. This way the effect of an abnormal condition, which occurs at run-time in a module, remains confined to it, or at worst it only propagates to a few neighboring ones.

Open Standards, Technologies & Specifications: A primary requirement when designing and implementing the OPSIS prototype was the minimization of costs not only for the current integration but also for every future improvement, due to the fact that governmental organizations (GOs) usually lack of financial resources and IT well trained personnel. Besides, private companies are typically compelled by the realities of profit making, while G.O.s do not have such profit-oriented motivations. Essentially, OPSIS adopts peak technologies and worldwide accepted and mature standards in order to build an *Enterprise Application Integration (EAI)* and Technology framework, providing advanced migration-based services according to *Software-as-a-Service (SaaS)* model [14].

Interoperability: Interconnecting many distributed and heterogeneous enterprise systems, is a difficult task, requiring easily identifiable and publishable e/m-services, as well as interfaces for the establishment of secure and reliable connection points [15]. Interoperability among the core entities of *OPSIS* was achieved by adopting WSs as the core communication protocol, and advanced XML-based technologies. A main difficulty being dealt with was to find a universal and standardize way to interoperate with the different kinds of applications and tools, which adopt the following characteristics: *Proprietary interfaces, Limited communication protocols, Lack of scalability.*

Therefore, in order to achieve interoperability we built a *Middleware Layer*, which integrates truly interoperable mechanisms through the use of an open source *Enterprise Service Bus - ESB* framework [16]. OPSIS ESB is a light weight messaging framework that uses disparate technologies, transports and protocols. It manages all interactions between the various components transparently, stipulating that different components of applications communicate through a common messaging bus [17]. Moreover, semantic interoperability among the different migration-based systems is handled by using standard based ontologies proposed and developed in the platform, based mostly on existing European ones.

Scalability & Extensibility: Advanced enterprise solutions demand the creation of a dependency between business and information technologies in order for GOs to be able to maintain scalable and extensible systems that efficiently support their business activities. OPSIS allows the abstraction of proprietary applications through the use of adapters, brokers, and orchestration engines. The resulting integration architecture is more robust and extensible, especially with the advent of the open Web Services framework and its ability to fully abstract proprietary technology. The use of BPMS systems for modeling all business processes in the core enterprise, organizes the embedded logic of an application into separate and easily changed "state machines" [18]. Adopting JBoss jBPM [23], in order to orientate the integrated migration-based services, our primary goal was to establish a highly agile automation environment, fully capable of adapting to change, which is realized by abstracting the business process logic into its own tier. Thereby, we are able to alleviate other services from the need to repeatedly embed process logic, and support process optimization as a primary source of change for which services can be recomposed.

Reusability: The goals behind service reusability are tied directly to some of the most strategic objectives of service-oriented computing, which are strongly supported by OPSIS. These objectives have as follows: Allow for service logic to be repeatedly leveraged over time so as to achieve an increasingly high return on the initial investment of delivering the service; Increase business agility on a migration-based level by enabling the rapid fulfillment of future business automation requirements through wide-scale service composition; Enable the realization of agnostic service models; Enable the creation of service inventories with a high percentage of these agnostic services.

Addressing this principle was very important when designing and implementing our prototype and its enterprise systems. Rather than embedding functionality that should be deployed across every specific government service, the distributed OPSIS architecture offers advanced and reusable security, storage and Web Services interfaces to application developers in order to easily expand its functionality and build upon it. Our main focus was to offer an innovative framework, in which all essential functions can be easily reused, configured and customized in every e/m-service provided.

4 OPSIS System Overview

In order to address its objectives and accomplish its mission the OPSIS system overall architecture, as depicted in Figure 1, encompasses the following core participants and entities distributed in four distinct layers as follows:

***Layer 1 – OPSIS end-users*:** This first layer consists of the three groups of users mentioned in section 1, namely, *Public Administrators, Policy and Decision Makers* and *IT developers*. Additionally, public administrators are responsible for properly and adequately providing initial content to the system and specifically all the primary information assets comprised at Layer 2 of its architecture, that are necessary for harmonizing migration procedures and civil status documents formats, decision making and policy design.

***Layer 2 – OPSIS Primary Information Assets*:** The OPSIS Primary Information Assets (Figure 1) include the following: Council Directives and Decisions, E.U. Directives and Decisions, E.U. and National Migration Policies, National Migration Procedures and Processes, Civil Status Documents, National and E.U. Mandates, Related Legislation and Policies as well as identified Best Practices.

***Layer 3 – OPSIS services*:** Through the use of the portal the end-users are able to gain access to advanced OPSIS electronic services, as follows:

- *Information Asset Management*: Public administrators are enabled to create and insert to the OPSIS tool migration policies, Directives, practices, procedures, structures and processes. In addition all OPSIS end-users are able to search and browse these information assets, as well as monitor and track changes applied to them in a controlled way. All these activities are supported and provided by the integrated tools of the OPSIS content management component described in subsection 4.1.
- *Governmental Process Modeling*: Public administrators and policy or decision makers take advantage of this service in order to model, further analyse and appropriately manage the information assets contained in the OPSIS platform through the use of a graphical environment capable for interactively designing processes. This service is provided through the Decision Support component and specifically from the integrated Governmental Process Modeling and Management tool.
- *Benchmarking and Assessment*: The end-users of this service are also the public administrators and the policy or decision makers who are enabled to benchmark national practices, policies and procedures, as well as to perform assessments on these assets, in terms of legislation, organizational, political, and security characteristics, in order to identify gaps with respect to E.U. directives and best practices. This service also enables end-users to reengineer their current internal affairs.
- *Semantic interoperability guidance*: IT systems developers and integrators are guided of how to use semantically aware schema definitions in order to build the

basis for an E.U-wide standardisation in migration area. This semantic knowledge is shareable among systems to enable collaborative evolution of National and European ontologies on migration assets. Specifically, this service is provided through the use of properly configured ontology engineering and mapping tools that enable the establishment of a common definition and understanding of migration issues, processes and data formats.

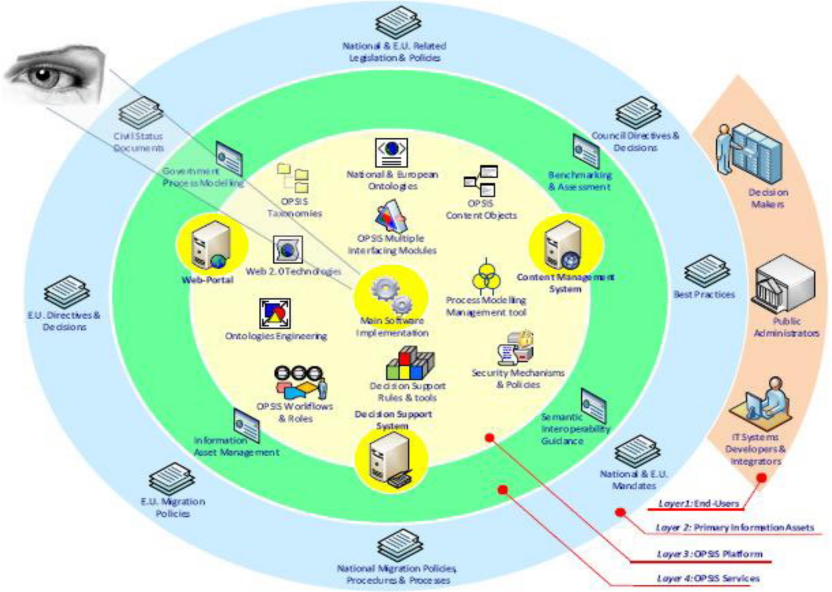

National & E.U. Related Legislation & Policies
Civil Status Documents
Government Process Modelling
Council Directives & Decisions
Benchmarking & Assessment
Decision Makers
OPSIS Taxonomies
National & European Ontologies
OPSIS Content Objects
OPSIS Multiple Interfacing Modules
Web-Portal
Web 2.0 Technologies
Content Management System
Main Software Implementation
Process Modelling Management tool
Best Practices
Public Administrators
E.U. Directives & Decisions
Ontologies Engineering
Security Mechanisms & Policies
OPSIS Workflows & Roles
Decision Support Rules & tools
Decision Support System
Semantic Interoperability Guidance
Information Asset Management
IT Systems Developers & Integrators
National & E.U. Mandates
E.U. Migration Policies
Layer1: End-Users
Layer 2: Primary Information Assets
Layer 3: OPSIS Platform
Layer 4: OPSIS Services
National Migration Policies, Procedures & Processes

Fig. 1. OPSIS Platform Overview

***Layer 4 – The OPSIS Platform*:** Based on open-source solutions and technologies, the core platform of Odysseus consists of three main components:

- *The Content Management System* which undertakes the creation, editing, management and publishing of all the migration-based primary and processed content in a consistently organized fashion.
- *The Decision Support System,* which intends to help public administrators and policy makers to compile useful information from primary raw data, documents, national and E.U. knowledge, and migration decision makers to identify, solve problems, and reach decisions.
- *The Web Portal,* which provides electronic and mobile based point of secure access to OPSIS services, information, and content, retrieved and processed from diverse sources, in a unified and user-friendly way.

4.1 OPSIS Content Management System

The OPSIS CMS, apart from integrating storing, controlling, versioning, and publishing advanced mechanisms and functions, it is responsible for: Defining workflow tasks for collaborative content creation with the use of Web 2.0 technologies (wikis, forum, blogs, etc); Tracking, capturing and publishing public content to different repositories.

As every synchronous content management system it contains a set of multiple tools and information assets as depicted in the following figure. The OPSIS CMS holds the OPSIS taxonomies, the XML-based and e-Gif enabled content objects, and the related tools for the effective collection of data as well. The OPSIS taxonomies considered several previous efforts, compliant with world-wide standards such as the ISO-2788 [19] and BS-8723 [20]. Among these were the *Integrated Public Sector Vocabulary (IPSV)*, the *Taxonomy of Human Services*, the *European Communities Glossary*, and others. Correspondingly, the structure of the OPSIS content objects is based on the Greek and the British e-Gif specifications [21] in order for the framework to enable the seamless flow of information assets and to provide a long term strategy that will be able to adapt in the future. In addition it provides:

- Advanced *content management tools* such as rich text editors, live page editing and scheduling, and advanced document managers.
- *Web 2.0 technologies* with their own set of authorizations, message boards for facilitating conversations around public administration aware topics, blogs for allowing users to convey information and RSS feeds from the last mentioned message boards and blogs within the OPSIS system.
- A *multi-tier search engine* so that end-users are able to search relevant public information throughout the entire web interactive system, within specific portlets such as Wikis, Message Boards, other Web 2.0 aware technologies and even in external integrated applications through its advanced multiple interfacing module.
- Intuitive *front end user interfaces* that share a set of common characteristics to promote user friendliness and accessibility. These are multilingual, in order for users to easily toggle between different language settings.
- *Web publishing tools* so to easily create and manage content, from a simple article of text and images to fully functional web sources.

In OPSIS, the JCR-compliant Alfresco [13] content infrastructure and content management enterprise system, based on known and used standards worldwide, has been properly integrated and configured for the public sector.

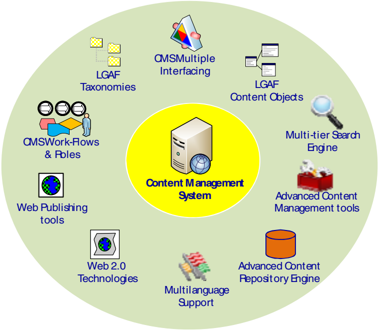


Fig. 2. OPSIS Content Management System Overview

4.2 OPSIS Decision Support System

Through the development of the OPSIS tool, extensive research was conducted in order to design appropriate decision reaching algorithms and patterns for embedding them into the core platform. The end-users of this system are entities acting as consultants for governmental policy makers, governmental organizations themselves and immigrants' bodies. The system is able to gather and present: An inventory of all current information assets (including legacy and relational data sources); Comparative figures such as tables, graphical representations and charts; Projected figures and proposed alternative future solutions based on hypothetical assumptions or the potential for convergence to best and common practices; The consequences of different decision alternatives, given past experience in a context that is described.

The OPSIS DSS allows the decision makers (or their advisors) to modify, complete, or refine the decision suggestions provided by the system, before sending them back to the system for validation. Afterwards the system improves, completes, and refines the suggestions of the decision maker and sends them back to them for validation. The whole process then starts again, until a consolidated solution is generated.

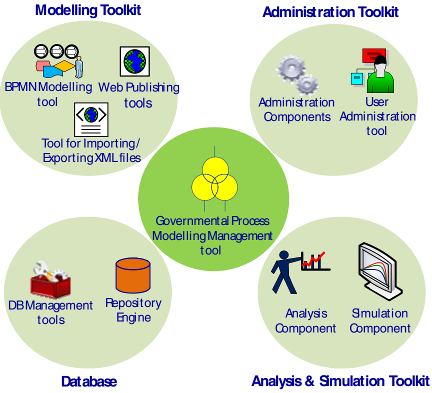


Fig. 3. OPSIS GPMM Overview

Part of the DSS suite of tools is the ***Governmental Process Modelling Management (GPMM)*** tool as depicted in the above figure, which enables experts to design and model complex workflows together in a graphical environment. The GPMM is a dedicated tool for the information acquisition, modelling and design, analysis, simulation, and evaluation of migration procedures and information items. The tool is envisioned to focus on usability, openness, method flexibility (customizability), and model maintainability.

The GPMM tool is designed to support non-technical users such as business analysts, process owners, and process managers, as well as more technically skilled information systems and enterprise architects interested in business processes and business process-related information such as documents, resources, systems, applications, and organizations. It enables the design of the migration-based workflows and governmental processes and consists of four main layers: *The Modelling Toolkit*, which models all migration-based process in order to organize their embedded logic; *The Analysis and Simulation Toolkit*, which allows the investigation of impacts and effects of operation and changes in migration-based process and organisational structures; *The Administration Toolkit*, which manages several configuration settings of the operation environment in which the migration-aware services operate; *The Database*, which stores all the implemented processes and their current status.

4.3 OPSIS Web-Portal

The OPSIS Web Portal provides electronic based point of secure access to OPSIS services, information and content, retrieved and processed from diverse sources, in a unified and user-friendly way. As every synchronous web interactive system, it integrates complex mechanisms and operations, which are transparent to all end users. Automated processing is linked to the operational costs of the migration-aware services for the operating organizations, which satisfy a great number of requests with the need of only a handful of personnel under normal operations. In OPSIS this is leveraged by integrating peak technologies, which give to end-users the opportunity to perform part of processes by themselves.

The use of strong, open source frameworks and rich *User Interface (UI)* technologies such as *Spring Web Flow - SWF*, *Java Server Faces – JSF*, *Ajax4jsf*, *RichFaces* and *Facelets* [22], provide a user friendly web component based architecture, improving system performance. Moreover, they offer OPSIS the opportunity to easily build interactive interfaces with basic form controls and efficient, reusable operations, while future architecture developers will be able to separate the presentation logic from the UI component's business logic.

5 Conclusions-Future Research Directions

Migration policy making and monitoring as a process includes several steps: identification of the current internal policy situation, education and research on existing practices performed in other countries, comparison of processes and documents and heavy decision making and future planning. Also, the increased number of decision makers and stake holders involved in migration policies, increasing and diverged legislations and implemented migration procedures, different organizational structures, large and inhomogeneous legacy systems involved, cause a "chaos" in the monitoring of national policies and the harmonisation of procedures, processes and data formats. Migration Information systems need to be simple, open, reconfigurable and scalable. OPSIS is designed to support all these requirements in order to become a valuable asset and tool to policy makers in their everyday activities.

Integrating and properly orchestrating a number of advanced technologies and open-source software components, OPSIS constitutes an innovative revolutionary Migration Information System, able to strengthen operational pan-European cooperation in fight against illegal immigration and the harmonisation of policies.

Future work in this area involves the enhancement and further development of the OPSIS tool in order to explore its full potential as a holistic open collaborative and interactive system. The idea is to enable all migration related communities and societal groups to participate, express opinions and contribute in the migration policy processes using an open, trustful and widely accessible environment. Sophisticated research and detailed analyses will also focus on the implementation and adoption of a properly customised identity management system.

References

1. EC-UN Joint Migration & Development Initiative, http://www.migration4development.org/
2. ARGO, http://ec.europa.eu/justice_home/funding/2004_2007/argo/funding_argo_en.htm
3. EUROMED Migration II, http://www.euromed-migration.eu/e933/index_eng.html
4. Migration Asylum Refugees Regional Initiative (MARRI), http://www.marri-rc.org/
5. PROMNISTAT project, http://www.prominstat.eu/drupal/?q=node/64
6. International Centre for Migration Policy Development, DCIM-EU project, http://www.icmpd.org/721.html?&no_cache=1&tx_icmpd_pi1[article]=1322&tx_icmpd_pi1[page]=1326
7. European Regional and Local Authorities for the Integration of Migrants (ERLAIM), http://www.erlaim.eu/wcm/erlaim/sezioni/Mission/objectives.htm
8. Migrant Integration Policy Index (MIPEX), http://www.integrationindex.eu/
9. European Civil Registry Network (ECRN), http://www.ecrn.eu/BBB/
10. European Migration Network (EMN), Information Exchange System, http://emn.sarenet.es/
11. Policy Mix for R&D, http://www.policymix.eu/PolicyMixTool/index.cfm
12. European Institute of Public Administration (EIPA), Common Assessment Framework (CAF), http://www.policymix.eu/PolicyMixTool/index.cfm
13. Alfresco, The Open Source Alternative for Enterprise Content Management, http://www.alfresco.com/
14. Fishteyn, D.: Deploying Software as a Service (SaaS), White Paper, http://www.saas.com/homepage/pdf/SaaS.com_Whitepaper_PartI.pdf
15. Kaliontzoglou, A., Sklavos, P., Karantjias, A., Polemi, N.: A secure e-Government platform architecture for small to medium sized public organizations. Electronic Commerce Research & Applications 4(2), 174–186 (2005)
16. Mule Technical Committee, "Mule 2.0", Release Candidate 2, http://mule.mulesource.org
17. Khoshafian, S.: Service Oriented Enterprises, 1st edn. Auerbach Publishing (2006)
18. Pasley, J.: How BPEL and SOA Are Changing Web Services Development. IEEE Internet Computing 9(3), 60–67 (2005)
19. ISO 2788, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?
20. BS 8723, http://www.bsiglobal.com/en/Shop/PublicationDetail/?pid=000000000030094114
21. e-Gif, http://www.e-gif.gov.gr/
22. Karantjias, A., Polemi, N.: An Innovative Platform for complex Secure e/m- Governmental services. In: IJESDF (to appear, 2009)
23. JBoss jBPM, http://www.jboss.com/products/jbpm/

Online Communities: The Case of Immigrants in Greece

Ioannis Panaretou[2], Nikos Karousos[1], Ioannis Kostopoulos[2],
Georgia-Barbara Foteinou[2], and Giorgos Pavlidis[2,3]

[1] Reserach Academic Computer Technology Institute
karousos@cti.gr
[2] University of Patras, Business Administration Department
panaretou@gmail.com, kostopul@patras.gr, gfoteinou@hol.gr,
pvlds01@bma.upatras.gr
[3] Athens Network of Collaborative Experts (ANCE)

Abstract. Immigrants in Greece are an increasing population, very often threatened by poverty and social exclusion. At the same time Greek government has no formal policy concerning their assimilation in Greek society and this situation generates multiple problems in both immigrants and native population. In this work we suggest that new technology can alleviate these effects and we present specific tools and methodologies adopted by ANCE, in order to support online communities and specifically immigrant communities in Greece. This approach has the potential to support immigrant communities' in terms of the organization of personal data, communication, and provision of a working space for dedicated use. The Information System's operational features are also presented, along with other characteristics and state-of-the-art features in order to propose a general direction to the design of online communities' mechanisms.

Keywords: Online Communities, Taxonomies, Social Networking frameworks, collaboration and decision support tools.

1 Introduction

Immigration as a form of social relation and as a process is an independent phenomenon that arises in the context of a specific historic and social framework. Immigration in Greece starts taking place in the early 1970s [1, 2]. Up until 1989 there was no official immigration policy. The first programme that legalised immigrants was introduced in 1998 [3]. The motivation behind immigration is affected by multiple factors, with desirable and in many cases unforeseen consequences, for the immigrants themselves. The Greek participation in the EU, the collapse of the regimes in Eastern Europe, the disintegration of the republic of Yugoslavia and the subsequent economic and social circumstances in these states constitute some of the major factors behind immigration. Currently, Greece is a place of permanent residence and intermediate destination for hundreds of thousands of immigrants [4].

In this work we present an approach adopted by a non-government, non-profit, organization, Athens Network of Collaborative Experts (ANCE) [5], that attempts the

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 351–359, 2010.

creation of the first online community in Greece devoted to the needs of immigrants. It is a multilingual, open sociotechnical network that will inform, expose and offer services related to the problems of immigrants. Moreover, we present and discuss a number of proposed technologies and web-based tools aiming to support multilevel participation.

The term "online community" has no widely accepted definition and many authors reach the conclusion that the term means different things to different people. Some authors stress the social aspects of online communities, while others stress the technical issues related to this phenomenon. According to sociologists there are many attributes which define a community, such as boundaries, population etc. On this paper we focus on the relationships which link together the members of a certain immigrants' community, especially the "weak-tie" relationships that serves communication and social needs.

The ultimate goal of the proposed approach is to help immigrants to communicate with other people of the same ethnic minority, to present them solutions to their common problems and to facilitate their interaction with their representatives and their governments. In addition, immigrants will have the ability to require information about legal and institutional issues and medical care. This attempt could offer support to fellow sufferers and significantly improve the immigrants' sociability [18].

2 The ANCE Approach to the Creation of an Online Community

In general, ANCE adopts a bidirectional approach for the analysis of the immigration phenomenon. The first direction focuses on the problems that immigrants face in their transactions with Greek government and society, while the second one deals with the problems that immigration causes. The complexity is very high because the analysis extends in the ethnicities, the cultural, political and religious identities of the immigrants as well as their social role and activities. What characterises both directions and makes ANCE's effort important is that immigrants never constitute a unified political entity that expresses common views at an individual and collective level. The limited social presence of immigrants happens either through social networks that form around one individual, typically with little activity, or through organisations that are dynamic in space and time even if they are often not visible. Typically at the heart of the first type of networks are activists, while in the second type of networks the central role is played by embassies of countries of descent, friendship communities etc. Both these types of networks constitute an entire "parallel" reality formed by the social relations, views, initiatives and strategies for the social embodiment of immigrants that fuels, and at the same time is fuelled by the constant interaction with the external environment, the state agencies and the local authorities. The existence of these networks affects the architecture, the design and the implementation of the proposed online community.

The aim is for participants to avoid consuming their efforts in resolving secondary problems and demands, and focus their resources in order to exploit the existing social and economic potential to achieve a set of goals. These goals include, but not limited, a) the recognition and establishment of the right of immigrants to access, representation and active participation in online community, b) the cultural alienation and establishment of their basic rights, c) the participation in collective activities in a global labour force concept, d) the development of interpersonal relationships, e) the development of innovative information and solidarity services that affect positively the working and living conditions for immigrants, f) the discovery of new democratic processes, collaborations and ways of transferring good practices from other online communities, g) the establishment of new communication and collaboration routes within the aforementioned networks, h) the independency of place, time and reason of participation in the online community and i) the identification of their comparative advantages and disadvantages.

Some of these goals can be fulfilled through the use of purpose-built information systems which are designed to support the online communities. These systems should have the following special features:

- The systems should be multilingual in order to serve the special needs of immigrants, which constitute a diverse set of users, in order to avoid the digital exclusion.
- The users of the online communities should collaborate and communicate both in synchronous and asynchronous way, according to their availability to use the systems.
- The systems should be easy to use, which means that special usability criteria should be met.
- The systems should be compatible with different operational systems and different devices (PCs, Pocket Pcs, Mobile phones etc.).
- The systems should contain trustworthy mechanisms to control the access and ensure the integrity of communications.
- The systems should contain mechanisms to organize and manage the online communities and the relations of their members.
- System's users, including users with special needs, elder or disabled, must be able to access the system in a equal basis, as it is described by the WAI and EU standards [6].

A detailed presentation of such a system, proposed by ANCE, is described in section 4 of current work.

3 Supporting Tools and Technologies

Towards the creation and the support of an online community, we first focused on the proposition of the appropriate suite of tools that can provide all the required functionality derived from the needs of immigrants. However, the choice of the most appropriate tools for the particular case is not an easy task due to several difficulties, such as the large number of the available tools, the absence of a complete set of requirements and specifications, the low level of ICT awareness of the immigrants, the overall cost of the entire approach, etc. In this context, the research is focusing on the following two critical issues: a) the study of the existing approaches of the classification of the available tools for supporting group and communities and b) the choice of the appropriate set of tools that meet most of the requirements.

3.1 Classification Criteria for Groupware Tools

A number of different taxonomies have been proposed in the last twenty years. These concern the classification of groupware technologies and their functions and they are based on different perspectives. Taxonomies such as the DeSanctis and Gallupe's matrix of time and space [7] have been adopted or revisited by several authors [8][9][10]. Other taxonomies that are based on shared information or functional criteria were also considered in the classification. However, this study is taking into consideration those taxonomies in which the classifiers selectively integrate space and time criteria, accordingly proposing new classification schemas:

Reinhard et al. [11] classified Computer Supported Cooperative Work (CSCW) systems having in mind a set of application, functional and technical criteria (Table 1). The term 'application criteria' is used to describe a system that can provide generic and/or specific tools. Functional criteria are used to describe social aspects of teamwork, such as interaction, distribution, coordination, user specific reactions, visualization and data hiding. Technical criteria are dealing with hardware, software and network support. The architecture of the software components can be centralized, distributed or replicated.

Table 1. Reinhard et al's classification criteria

Application Criteria		Generic	Generic and Specific Tools
Functional Criteria	Interaction	Synchronous Implicit Formal	Asynchronous Explicit Informal
	Distribution	Same place	Different Place
	Coordination	Free	System based
	User specific reactions	Provided	Collaboration transparent
	Visualization Data hiding	Different levels of WYSIWIS Different levels of granularity	
Technical Criteria	Input	Centralized	Replicated
	Output	Centralized	Replicated
	Application	Centralized	Replicated
	Data	Centralized	Replicated

From Coleman's perspective [12] the development of the groupware taxonomy is based on functional criteria and is presented below:

Finally, a classification of community-oriented technologies was published by Étienne Wenger [13]. Wenger selected a variety of technologies to include in a survey by considering the needs of Communities of Practice (CoP). He focused his categorization on shared repertories of resources within a community of practice such as experiences, tools or stories within a CoP. On his study it has been pointed out that the **typical features** useful to a community would be:

Table 2. Coleman's classification criteria

Collaborative Content Management Systems	Learning Content Management Systems
Tacit Knowledge and Intellectual Capital Management	Storage, indexing, valuation and search of information
Real Time Collaboration Tools: Audio/video/data conferencing, virtual classrooms, online presentations	Virtual Team Tools: distributed project management, virtual workplaces and process-oriented tools
Collaborative Customer Resource Management	Application of human agents to commerce through the use of real time collaboration technologies
Portals and Online Communities	Yahoo-groups, Google-groups
Unified and Wireless messaging infrastructures for collaboration:	Wireless collaboration, e-mail-based-services, peer-2-peer, IM/Chat, bulletin boards

a) a homepage (to communicate its existence and activities),
b) a conversation space (to discuss topics related to its domain),
c) an area for floating questions within the community,
d) a directory of members' expertise in the domain,
e) a shared workspace (for eventual synchronous collaboration or meetings),
f) a document repository (for their knowledge base),
g) a search engine (to retrieve what they need in their knowledge base),
h) some community management tools (to monitor members' activity and documents) and
i) a function allowing the creation of sub-communities.

The Wenger's categorization seems the most appropriate for ANCE because the author builds his categorization by putting technology in the context of community needs. Wenger believes that the optimal tools to support the complex activities in a community have to comply with the principle of strategic intent of the technology [13]. This means that both the tools and technologies must support needs such as knowledge exchange, social exchange, conversation - information, and instruction's work.

3.2 Tools and Technologies for Communities: What to Choose?

By looking the existing tools and technologies that can fit all the aforementioned Wenger's typical features, it becomes clear that there is neither a tool nor a framework on the web that can offer the entire set of functionalities. Moreover, it is also obvious that the selection of a specific set of appropriate tools is not the optimal solution either. A particular tool selection may be suitable for a current situation but it is not certain that in future this will be the most appropriate one.

For example, tools such as **mails** and **chats** are absolutely useful and easy to be used· however, the produced knowledge is not obvious and the information retrieval is difficult. **Web Forums** are the most common and widely accepted discussion places. Most of the users are already familiar with such tools while many of these have multilingual support. On the other hand, forums usually require organized communities since they are operating under a strict set of predefined user rules. Moreover they cannot be actually helpful in case of large content (information overdose). **Wikis and Blogs** are the representative tools of the social software. They can support knowledge generation and asynchronous collaboration in an open set of potential users. Both tools require from users, to have reach a high level of maturity concerning both participation and collaboration. **Social Network Frameworks** such as Facebook [14], Myspace [15] etc, are high technology web applications that support networks of people and can integrate with an open set of external applications. These tools are very popular but they are used more by individuals than by predefined online communities. **Online Meeting Software** such as Flashmeeting [16] are very useful in cases of synchronous meetings from distance. They only require bandwidth and some registered free accounts. However, such tools require sufficient meeting experience along with ICT awareness. Finally, **collaboration and decision support tools** such as CoPe_it! [17] can assist users to collaborate in workspaces and support the process of decision taking, although these innovative tools require enough practice and cannot be used by fully unaware users.

While the selection of a set of tools that can cover most of the community's requirements seems a promising solution, we believe that the critical point of the entire procedure is to focus on the framework in which these tools will be integrated than on the tools by themselves. In this context, the question "what tools to select" is now transformed to "how can we integrate an open set of tools and provide services in a very friendly and easy to use way"? Before we answer to this question we have to take into consideration issues that concern the dynamic changing of community's needs, the familiarization of the new community members with the entire systems environment, and finally, the adoption of commonly accepted standards for integration and interoperations with other tools.

Concerning the community's needs, it is a fact that as long as the state of immigrants' life is not stable, their needs will be dynamically changed. Consequently, this will result to new requirements for the functionalities of the whole framework. This means that a flexible system with significant potential for customization have to be designed.

Moreover, the provision of services able to welcome, help and familiarize recently joined members with the community's procedures and environment is also very critical to the success of the attempt. Furthermore, the framework should provide all the required functionality to a specific set of community moderators (or persons with specific roles) in order to aim the new members through both synchronous and asynchronous communication and through the explanation of the individual roles in the community.

From a technical side of view, it is important for the evolution of the whole system (considering cost issues) to be based on common adopted standardized technologies and protocols such as eXtended Markup Language (XML), portal components, web services (WS), Single-Sign-On (SSO), Friend of a Friend Protocol (FOAF) etc. in order to be able to integrate other tools as well as to provide services to external application. Thus, the overall cost of interoperation with other tools will remain low.

4 The Proposed Technical Approach

Considering the above, ANCEs approach aims to the design and implementation of an integrated web-based application framework that can provide the required functionality, and can also be extendable and interoperable with other tools or software modules. This framework will initially encourage potential users to organize their personal data, help them to communicate with other users, and provide them the necessary working space for keeping and publishing personal or public information to others. In this phase all users will be assisted and informed by both system and humans. At a second level, they will be able to participate in collaboration activities, by using “friendly” web-tools, in order to establish a satisfactory level of participation. Collaboration may occurs in both synchronous an asynchronous forms while the appropriate collaboration tools will vary from some commonly used tools to more intelligent ones in the context of web 2.0 technology. The final target of the entire system is to become an active user-driven application that can meet the existing requirements of the on-line community of immigrants and at the same time to be adaptable enough so as to support future user needs

Technically speaking, the framework will be based on a multilingual web-based portal and is going to be integrated with additional functionality (web 2.0 services), focusing on introducing innovative collaboration tools. The main target is to provide novice ways for enhancing participation, knowledge creation and sharing. Having in mind that both customization and dynamic integration with other technologies are very crucial requirements in the particular approach, the selection of the appropriate portal skeleton will be limited to open source platforms that support integration with custom components (portlets, widgets etc) along with fully user interface customization.

The following table presents the initial settings of the proposed approach in correspondence with Wenger’s typical features discussed in the previous paragraph, aiming at the provision of a complete set of functionalities.

Table 3. The proposed solution related to Wenger’s typical features

Wenger’s Typical Features	Proposed Solution
A homepage	The proposed portal
A conversation space	Chat, Messaging, Forum
An area for floating questions within the community	A Blog tool
A directory of members' expertise in the domain	Service for classifying members according to their domain of expertise.
A shared workspace	FlashMeeting and CoPe_it!
A document repository	Wiki and portal
A search engine	Integration with a search engine
Community management tools	Provided or integrated with portal: User and Role modeling component
A function allowing the creation of subcommunities	Provided by portal

Apart from the above, a set of particular specifications will be also taken into consideration during the "design" stage. These specifications involve the enhancement of XML schemas and Web Services, visual integration via portlets, mobile integration, security, privacy, Single-Sign-On and Multilingualism.

Crucial factors for the success of the proposed framework are also simplicity and extendibility. Simplicity will enable usage and participation while extendibility will ensure the necessary follow-up to immigrants' dynamic environment of needs and problems.

Additionally, targeting to keep the cost of the provided framework low - another important success factor - the usage of Open Source software and web tools is considered important.

Finally, a remarkable effort should be given to the initialization of the entire system and the encouragement of the potential users to join the proposed community. The most "drugging" information that can be provided is a throughout database of the legal and institutional framework for immigration in Greece. The key factor is to involve all the appropriate information regarding official immigration policy. In addition, certain divisions of the Greek government, involved in the policy-making for immigrants, should be represented and be reachable, through the portal.

5 Conclusions and Future Work

In this work, we propose a set of technical specifications in the context of a development approach aiming at supporting the changing needs of specific groups of people: immigrants from diverse ethnic origins who live in Greece. Immigrants can play a significant role to the social and economic development of each nation because represent a flexible and cheap workforce and also contribute to the formation of a multicultural and multi-national society [19]. The way they are absorbed and became a "wheel" of each country's production and development chain is a sign of its democracy and civilization level. At present, immigrants in Greece constitute a significant proportion of the local population, but very often, they are excluded from the social life. The utilization of new technologies for this purpose, could alleviate the social isolation, and become a "vehicle" for the minorities to identify their needs and to produce solutions to their common problems. Ethnographic and sociological research is needed for recognizing their special characteristics in order to design a customized IT system. Because of a lack of these data, more common tools and technologies are used in a special combination, so as to support the ANCE's efforts.

Through the proposed approach, immigrants can find a step of communication and participation, being able to work on common problems and concerns. The integration with the Greek legal framework and immigrant-division authorities provides the necessary workspace for further development of the bonds of trust between immigrants and the Greek government.

In the future, this framework can be used as the starting node of an online "workflow" system which will be able to provide e-government services to immigrants. Based on web 2.0 technologies, the system can provide data to governmental online information systems and create the infrastructure for the provision of lever 4, e-Government services. The existence of appropriate data about the immigrants' characteristics is the critical factor for linking immigrants' needs with government services. These data can be gathered and retrieved by the proposed system in a significant degree and also can help immigrants to work collectively as a unified political entity.

ANCE, as an organization that continuously attempt to improve the living conditions of specific communities, can play a significant role towards this direction, by providing its human force in order to disseminate the benefits of the framework use, to engage the end-users of the proposed framework and finally to support the immigrants during the operational period of the system.

References

1. Iosifides, T., King, R.: Socio-Spatial Dynamics and Exclusion of Three Immigrant Groups in the Athens Conurbation. J. of South European Society and Politics 3, 205–227 (2000)
2. Marvakis, A., Parsanoglou, M.P.: Immigrants in Greece, Ellinika Grammata (2001)
3. Elpianna Emmanouilidi: Greek Immigration and Asylum Policy, European Migration Network - EMN (2003)
4. Lianos, T., Kanelopoulos, K., Gregou, M., Gemi, E., Papakonstantinou, P.: Estimation of the Volume of Immigrants that live Permanent in Greece, Institite of Immigration Policy, Greece (2008)
5. Ance Hellas, http://www.ance-hellas.org
6. Web Accessibility Initiative, http://www.w3.org/WAI/
7. DeSanctis, G., Gallupe, B.: A Foundation for the Study of Group Decision Support Systems. Management Science 33(5), 589–609 (1987)
8. Ellis, L., Gibbs, S.J., Rein, G.L.: Groupware: Some Issues and Experiences. Communications of the ACM 34(1), 38–58 (1991)
9. Grudin, J.: CSCW: History and Focus. IEEE Computer 27(5), 19–26 (1994)
10. Dix, A., Finlay, J., Abowd, G., Beale, R.: Human-Computer Interaction, 2nd edn. Prentice Hall Europe, Englewood Cliffs (1998)
11. Reinhard, W., Schweitzer, J., Völksen, G., Weber, M.: CSCW Tools: Concepts and Architectures. IEEE Computer 27(5) (1994)
12. Coleman, D.: Levels of Collaboration. Collaborative Strategies March 2002 Editorial (2002), http://www.collaborate.com/publication/newsletter/publications_newsletter_march02.html (latest visit July 2006)
13. Wenger, E.: Supporting Communities of Practice, A Survey of Community- Oriented Technologies, Version 1.03 (2001)
14. Facebook, http://www.faccebook.com
15. Myspace, http://www.myspace.com/
16. FashMeeting, http://flashmeeting.e2bn.net
17. CoPe_it!, http://copeit.cti.gr
18. Preece, J.: Sociability and usability in online communities: Determining and measuring success. Behavior and Information Technology Journal 20(5), 347–356 (2001)
19. Fakiolas, R., Maratou-Alipanti, L.: Foreign female immigrants in Greece Papers. Sociología (2000)

From Online to Ubiquitous Cities: The Technical Transformation of Virtual Communities

Leonidas Anthopoulos[1] and Panos Fitsilis[2]

[1] PhD, Expert Counselor, Hellenic Ministry of Foreign Affairs,
10671 Athens, Greece
lanthopo@mfa.gr
[2] Professor, Project Management Dept, TEI Larissa,
41100 Larissa, Greece
fitsilis@teilar.gr

Abstract. Various digital city projects, from the online cases (e.g. the America on Line) to the ubiquitous cities of South Korea, have achieved in creating technically 'physical' areas for the virtual communities, which share knowledge of common interest. Moreover, digital cities can succeed in simplifying citizen access to public information and services. Early digital cities deliver 'smart' and social services to citizens even with no digital skills, closing digital divide and establishing digital areas of trust in local communities. This paper presents the evolution of the digital cities, from the web to the ubiquitous architecture. It uses the latest digital city architecture and the current conditions of the digital city of Trikala (Greece), in order to present the evolution procedure of a digital city.

Keywords: e-Government, digital city, ubiquitous city, e-democracy, virtual communities.

1 Introduction

Multiple approaches have been given to the Digital City: *digital environments collecting official and unofficial information from local communities* [1] *and delivering it to the public via web portals are called information cities* [2],[3],[4]. *Networks of organizations, social groups and enterprises located in a city area* are called digital cities. These definitions were given by major case studies such as the America on Line (AOL), the Kyoto's and the Hull's etc., which are analyzed in this paper in order to present the ubiquitous environment that is generated in many areas all over the world, and to describe the transformation of virtual communities.

Although digital cities were initiated as information based systems (web portals, databases, virtual reality applications etc.), they soon evolved to wide(metro)-area information systems (IS) that deliver different kinds of services to the local communities. Their infrastructures concern network equipment (fiber optic channels and wi-fi networks in the city area), service oriented information systems (e.g. e-Government IS, e-Democracy portals, public Agency web applications etc.), public access points (e.g. wireless hotpots, info kiosks etc.), and social service systems (e.g. intelligent

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 360–372, 2010.

transport systems, tele-care and tele-health networks etc.). These environments composed a recent digital city definition [5]: *wide(metro)-area infrastructures and applications that focus in covering local needs and in supporting local community's everyday life. This definition has been evolved to the ubiquitous city or U-city [6]: a city or region with ubiquitous information technology. All information systems are linked, and virtually everything is linked to an information system through technologies such as wireless networking and RFID tags.*

Both recent digital city and U-city approaches face multiple challenges: the opportunity for the digital city to become a) a common interface for public transactions in the city area, b) an area-of-trust for virtual communities where opinions can be generated and forwarded to the political leadership. These approaches can develop a "global e-Government environment" in cities, where citizens can access both local and central public services. This global environment can be called "Metropolitan e-Government environment" and its main targets concern: a) the collection of local information, b) the use of local information for the sustainable development of the city and c) the continuous evaluation and improvement of the architecture, and of the quality of the offered services.

In the first section of this paper we present the transformation of the digital city from the web to a technically 'physical' area based on the ubiquitous computing. We propose an extension of the latest architecture of the digital city, in order to include the 'business' layer with standards and rules concerning operation. Finally, we present the evolution case of the digital city of Trikala (Greece), in order to describe successes and failures concerning digital communities' expectations.

2 The Evolution of the Digital City

Since early 90s different digital cities were implemented all over the world (Table 1). These cities vary from the fully virtual cases -where no physical equipment can be accessed by citizens and where no real boundaries limit digital city area-, to the fully physical cases –where digital and real city share common physical space-. Fully virtual cases involve online cities, knowledge bases and virtual communities. On the other hand, fully physical cases involve the latest digital cities such as Beijing, Seoul and Trikala, together with the ubiquitous cities of South Korea and Japan.

2.1 Virtual Cases

The first virtual case was the America on Line cities (AOL cities) [1], where web environments offered digital information and transactions, together with chatting options. AOL simulated a city via grouping services according to civilian logic. The digital city of Kyoto (Japan) [7],[8] and the digital city of Amsterdam [9] were web environments simulating the city and its local life (streets, enterprises, malls etc.). This version of the digital city offered virtual meeting rooms for specific common interests, inviting citizens to participate. These web approaches were evolved to virtual reality environments [10] operating beyond the physical boundaries of a city.

On the other hand, some major cases that exploit Information and Communication Technologies (ICT) for the social development were implemented: the Copenhagen

Base [11] was a public database containing useful local information. People could initially access the database via the Internet and via text-TV. Today the Copenhagen Base is open to people for data supply and entry. Moreover, the Craigmillar City of Scotland [11] used the ICT to structure groups of citizens who shared knowledge and offered social services to the local community. In Craigmillar –an ex-industrial area-, citizens collaborated in order to handle local needs.

The Smart City [12] refers to a city where the ICT strengthen the freedom of speech and the accessibility to public information and services. In the smart cities the habitants can participate in social events easy and cheap. The smart city approach was initially applied in the case of Brisbane (Australia) and supported the social participation and the close of the digital divide.

The World Foundation of Smart Communities (http://www.smartcommunities.org) is a nonprofit educational organization studying the development of Smart Communities; meaning cities with broadband networks interconnecting their local resources with resources from other geographic areas. The Smart Community uses the ICT in order to improve living and working. Lots of cities from Singapore, Malaysia, Canada, Hong Kong, Spain, German, Ireland, Holland and Saudi Arabia, participate in the Smart Community network.

The Communities of the Future (http://www.communitiesofthefuture.org) is a nonprofit organization defining the digital city as a knowledge democracy. This approach concerns the development of societies, where the novel privileges (privilege to access public information and services), risks (privacy and security) and challenges (social participation) based on the ICT, are analyzed and participation is encouraged. The Knowledge Democracy approach was applied in Blacksbourg (Australia) implementing the Blacksbourg Electronic Village (http://www.bev.net), where habitants with common interests (e.g. citizens, local administration, engineers) are grouped together, composing the neighborhoods entities.

The knowledge based cities [13] is a digital city approach, where the ICT can support local democracy and economy. This approach was applied in Portugal and uses broadband networks developed by telecommunication vendors connecting cities and local economies. Virtual organizations are structured in this network of cities, such as virtual organization for the municipalities, for the enterprises, for the citizens with common interests etc. The interconnected cities structure a regional virtual environment, where cities support each other's progress via the ICT.

The Digital Geography [14] is an approach that extends city physical boundaries and structures teams of interconnected citizens who share knowledge of common interest. The digital geography uses the Internet and the mobile networks to compose digital communities where knowledge is exchanged and where growth is supported. Emphasis is given to the development of Digital States in the same country, which are small-scale digital geographies. Digital geographies are graphically presented with communication zones in the same or in multiple geographic areas.

2.2 Physical Cases

The cases of Hull (UK, www.hullcc.gov.uk) and of Beijing (China) [2] used fiber optic backbones installed in the city, which were called "Metropolitan Area Networks (MAN)". MAN offered broadband access to public information and services from local agencies, aiming in simplifying everyday life. However, Beijing digital city was implemented for the purposes of the Olympic Games of 2008, and initially offered relating information and services. MAN was used in the case of the Digital Metropolis of Antwerp [11], the first digital city in Belgium. The Antwerp city collaborated with the City of Amsterdam, having a MAN too, in order to interconnect their municipal agencies and offer common information and services to their habitants. This group of digital cities supported the diffusion of the ICT for the decision making by the municipal leadership. Geneva city [11] on the other hand, used its MAN to interconnect the foreign enterprises that were located in the area. It then offered the MAN for public use, and constructed a digital market for all local businesses.

Broadband Metropolis such as the Seoul is an extension of the previous -based on the MAN- approaches. Broadband metropolis [15] contains dense fiber optic networks interconnecting public agencies with the citizens and the enterprises. A main fiber optic backbone is installed in the city, while the last mile connection is established with fiber channels (Fiber-to-the-Home, FTTH). Broadband metropolis comprises an area of healthy competition among telecommunication vendors, while it is attractive for private investments. In these digital city cases, financial wealth is established in the city, which is based on broadband investments.

Mobile Cities such as the New York [16], installed wireless broadband networks in the city, which were accessible (free-of-charge) by the habitants. Both e-learning and e-Government services were offered from local or national organizations in the mobile cities.

The Eurocities (http://www.eurocities.org) is a European network of cities, which focus on the development of an inclusive, prosperous and sustainable ICT environment operating in the area of a city. The participating cities exchange their experiences and they cooperate in the development of an open market and in the treatment of corruption in municipal agencies. The result of the Eurocities initiative is the development of prototype digital city, covering local needs in Europe. A public portal called the Demos has been developed, containing information from all participants. Moreover, pilot projects are being implemented concerning e-democracy and decision making applications.

In Trikala (central Greece) a novel approach to the Digital City was given [5], which extended the above cases and older ones [17]: the digital city is an ICT-based environment whose priorities concern a) the availability of digital means that support local needs and transactions, b) the transformation of the local community to a local information society, c) the direct and indirect, official and unofficial information collection, in order to support the sustainable development of the local community. The Trikala case is analyzed further in the next section, supporting the main focus of this paper.

Broadband cost minimization and the simplification of IS installation and maintenance resulted in further digital city cases. Moreover, the “cloud services” and the “ubiquitous computing” solutions offered by the big international ICT vendors, result in the evolution of the Digital City to the Ubiquitous City (or U-city). The U-city architecture is being implemented in South Korea (e.g. New Songdo [18]) and Japan (e.g. Osaka [19]) and delivers information anytime, to anywhere and to anybody, via interconnected information systems and ubiquitous ICT solutions over the city.

Table 1. Virtual and physical Digital City cases and approaches

City	Digital City	Short Description
1. American On Line (AOL)	AOL Cities *(virtual)*	Virtual groups exchanging knowledge over the Internet.
2. Kyoto	Digital City of Kyoto *(virtual)*	City simulation via web and virtual reality interfaces.
3. 4. Amsterdam	Digital City of Amsterdam *(virtual and physical)*	- City simulation via web and virtual reality interfaces. - Metropolitan Area Network installed in the city - Interconnection with Digital City of Antwerp
5. Copenhagen	Copenhagen Base *(virtual)*	Public database covering local needs.
6. Craigmillar	Digital City of Craigmillar *(virtual)*	Groups of citizens sharing knowledge and social services covering local needs
7. Brisbane	Smart City of Brisbane *(virtual)*	- Decision making services. - Virtual groups sharing knowledge
8. Smart Communities	Interconnected cities from even different continents *(virtual)*	Cities interconnected with broadband networks.
9. Blacksbourg	Knowledge Democracy of Blacksbourg *(virtual)*	Environment with knowledge concerning the ICT.
10. Knowledge based cities	Knowledge Based Cities in Portugal *(virtual)*	Regional network of interconnected cities
11. Digital Geographies	*(virtual)*	Virtual teams of users sharing knowledge, who are located in even different countries

Table 1. (*continued*)

12.	Hull	Digital City of Hull *(physical)*	- Metropolitan Area Network - Public portals offering local information and services.
13.	Beijing	Digital City of Beijing *(physical)*	- Fiber optic and wireless broadband networks in the city. - Public services mainly oriented to the Olympic Games.
14.	Antwerp	Digital City of Antwerp *(physical)*	- Metropolitan Area Network - eDemocracy services - Portals offering public information - Interconnection with Digital City of Amsterdam
15.	Geneva	Geneva-MAN *(physical)*	- Metropolitan Area Network - Interconnected market
16.	Seoul	Seoul Broadband Metropolis *(physical)*	- Fiber optic network all over the city (backbone and FTTH)
17.	New York	Mobile City of New York *(physical)*	Wireless broadband network covering the city area.
18.	Eurocities	European city network *(virtual and physical)*	ICT usage and experience exchange for: - Social Participation - Local community evolution - Sustainable development

Table 1. (*continued*)

19.	Trikala	Digital City of Trikala *(physical)*	- ICT solutions to cover local needs - Multitier architecture - Global e-Government environment - The Digital City consists a trusted third party for transactions and knowledge exchange
20.	New Sondgo	U-city of New Sondgo *(physical)*	Ubiquitous information systems in city area
21.	Osaka	U-city of Osaka *(physical)*	Ubiquitous information systems in city area

All of the above refer to either digital environments operating in the physical boundaries of a city or to environments that create virtual communities beyond the geographic area of a city. Although different priorities were given on each case, common ICT infrastructures are used (broadband networks and information systems) and virtual teams of citizens are structured. The analysis of the technologies combined in a digital or in a ubiquitous city is beyond the purposes of this paper.

Digital cities face common challenges, such as the encouragement of the social participation, and the economic and the sustainable growth of the local community. Today, all digital cities focus on the quality and on the variety of the information that they offer to their habitants (public content and services, private content, video-on-demand and other entertainment services, social networks etc.).

3 Investigating the Performance of a Digital City

In order to investigate how a digital city is implemented and performs, we present the case of Trikala, central Greece (e-Trikala). We use the development experiences and the e-Trikala official publications, in order to investigate how well the digital city performs since its beginning in 2005.

In Trikala, local needs were prioritized following the “bottom-up” procedure [20], and they were grouped into the following axes of precedence [5]:

- Local Economy and employment
- Improvement of everyday life concerning public transactions and transportation
- Education, vocational training and life-long learning
- Tourism and culture

On behalf of the municipality, a team of experts discovered funding and designed the necessary projects that could deal with the above axes of precedence. The set of projects delivered city-wide interconnected information systems and broadband networks, together with important public information and services. The logical architecture of the whole environment follows the multi-tier structure [21], inspired by information cities [2], [3], [4], consisting of following layers [5]:
Users layer, containing potential users of the digital city services: end-users (citizens, businesses, students), groups of end-users (local chamber, teams with common interests), servants who offer public and commercial services via the digital city (civil servants, public agencies, enterprises).

- Service layer, including software applications that deliver public information and services to citizens and enterprises. The applications concern web portals, engines executing e-Government, e-Commerce and social (e.g. telecare) services, web services transacting with other information systems (e.g. central e-Government systems, others located beyond city borders etc.), and geospatial services. This layer structures the interface between the habitants and the public administration (local and central ones). However, today no unique interface collecting all available services from digital city platforms exists, meaning that the digital city has not yet succeeded in its initial objectives. This web distribution of the digital city services can cause troubles to the habitants and can lead to information replication.
- Infrastructure layer, containing the local broadband networks (MAN and a metro Wi-Fi), an intelligent transport system, phone centre for public calls, and public access points in the city hall and in other public buildings. Concerning the broadband connectivity, both a MAN and a metro Wi-Fi are installed in the city today. The Wi-Fi is accessed by more than 2,000 registered users and it is based on more than 10 points of access. However, the MAN was implemented with European funding (under the Information Society Framework Programmes (www.infosoc.gr)), and it interconnects only public agencies today. No private organization can access the MAN, nor can FTTH connections extend it to the households and to the local enterprises.
- Information layer, consisting of information and data that is produced and stored in the infrastructure layer. The information can be public, private or both public/private and the digital city can apply policies for security and privacy, in order to define who can access what resource and to protect sensitive information. Today, there is no common data repository in the digital city of Trikala. Each information system belongs to a unique organization, and the information that it is produced and hosted in each one, belongs to that organization. The digital city cannot apply common security and privacy rules to different information systems and can only observe transactions.

Official publications of e-Trikala (www.e-trikala.gr) return useful findings concerning digital city progress and performance: although the e-Trikala case study was an ambitious approach, aiming to interconnect virtual with physical environments [22], only a few of its primary targets have been achieved while they are all reconsidered. After the completion of projects' design by the team of experts, the municipality structured an office responsible for the procurement and for the management of the projects.

Projects have been procured and implemented since 2005. Today, project deliverables operate under pilot conditions, while the municipal office has been evolved to a municipal company, able to exploit project deliverables and knowledge. The municipal company is also responsible for deliverables operation, and for digital city monitoring, reviewing and evolution.

Concerning the broadband access, the initial objectives were that anyone (end-users and groups of end-users) could access the digital city via its broadband networks from everywhere. Today, the metro Wi-Fi covers the 2/3 of city area, and it is open to anyone in its range. Users can access the metro Wi-Fi free-of-charge with the combination of a username and password given to them upon registration. Registration follows the traditional procedure, which demands the physical presence of the user at the municipality, in order to fill-in and to submit an application procedure, meaning that citizens have to obtain and application form document to the municipal authorities. On the other hand, the MAN is accessible only for public organizations, because Greek legislation does not permit private connections yet. It is expected that individuals and the private sector will be able to access the MAN by 2012. Until then, FTTH connections will not be able to extend the MAN, and habitants will access the digital city resources indirectly via the Internet or by phone. The broadband networks' operation is by now a municipal obligation, meaning that monitoring, maintenance and policy application is a difficult procedure that lacks compared to the private sector's competition.

Concerning the offered services no one-stop portal for the digital city exists so far. On the contrary, each project delivered a different but interoperable portal, offering its custom services and information. The municipal company has installed a web portal for the digital city (www.e-trikala.gr), but the web services to the projects portals have not been implemented yet. The reason is that each project deliverable belongs to a different organization of the city, and even hosting on central public infrastructures in the digital city demands legal confirmation.

E-Government progress is weak in e-Trikala case. The digital city has achieved in miniature town hall behavior [23], establishing "vertical connections among municipal agencies", and it offers four (4) services online. The same services are offered to the wider state region, beyond the city boundaries. Moreover, a call center offers helpdesk services to the citizens, concerning public transactions. Other digital public services are offered via the citizen service (KEP) offices (www.kep.gov.gr) and central public agencies, which are executed beyond digital city infrastructures.

However, e-Trikala case performs significantly well regarding social services: telecare and e-health services are widely accepted by citizens with special needs, who have obtained digital devices from the municipality, in order to be monitored online by the local hospital, doctors and psychologists. Heart diseases are monitored effectively by the local hospital, with the use of an information system installed in the infrastructure layer. Health records are collected and transmitted online, and some privacy issues have to be investigated further. Additionally to tele-care and e-health services, the intelligent transport system performs satisfyingly in e-Trikala: the period of testing has passed and statistical analysis on traffic data has been performed. Today, "smart bus stations" located around the city, inform citizens about the estimated departure times of buses.

On the other hand, no Enterprise Architecture has been composed, either common standards or blueprints have been defined for the future ICT projects that will be designed and implemented in the city area. Moreover, security and privacy issues have not been analyzed and each information system follows independent policies and rules. The municipal leadership has emphasized in the implementation of the designed projects, and only recently the development of the municipal company is a strategic direction.

The digital city performs similarly in information layer: the infrastructures do not contain common storage repositories for the information created and used in the city, and each project has its own storage capacities. The reasons concern the possession of the data and the proper legal alignment for public data construction, storage, access and use.

All other public services (e.g. tax and other administrating services) are either offered directly via central systems to which citizens are obliged to access or they are executed with the traditional methods. It is expected that by 2012 a central web portal will operate as a one-stop-shop for public services coming from the inside or the outside of the digital city.

The above findings show that the digital city mainly suffers concerning its management and its approach to all kinds of users. Additionally, ownership issues arise in the area concerning the infrastructure and data, which lead to lack of trust among different virtual organizations and virtual teams.

For these reasons, we propose the extension of the digital city architecture via including the Business layer, which contains the policies, the operating rules and the Enterprise Architecture of the Digital City. This layer defines how each system will be designed, installed and interconnected in the Digital City, while it contains the "WHOs and HOWs" for each new system, and for each transaction executed in the Digital City. Additionally, we suggest the renaming of the user layer into the stakeholders layers, in order to describe even the entities that affect a digital city, without transacting with it (e.g. the political leadership, legal authorities etc.). The logical and physical architectures of the digital city will be transformed to those presented in (Table 2) and (Fig. 1) respectively.

Table 2. The n-tier logical architecture of the Digital City of Trikala

Stakeholders layer *End users, groups of end-users, servants*
Service layer *Web portals, engines, web services, geospatial services*
Business layer *Enterprise Architecture, policies, operating rules*
Infrastructure layer *MAN, metro Wi-Fi, information systems, phone centre, public access points*
Information layer *Public, private, public/private data created and stored*

The digital city environment interconnects all viable and ICT resources in the city and it can deliver information from everywhere to anyone, meaning that it formulates a ubiquitous city. This environment can behave as a global e-Government environment (Metropolitan e-Government environment), with the following characteristics:

- Each citizen has a unique identity in the digital city and he can be authorized once, with the use of the same credentials in order to access different resources.
- Further citizen certificates will not be required for service execution, since any necessary information will be retrieved "transparently" among the digital city systems.
- Authentication tools, local content and services can be available via a common web portal. Habitants use the digital city portal to access local commercial, public or social services.
- Each transaction is executed and monitored by the digital city infrastructures.
- The digital city can be evolved to an "intelligent e-Government environment", since it will be able to "predict" the execution of some public services by monitoring citizen needs (with the consent of the involved parties). For instance, a citizen application for residence movement could be accompanied by records update in tax-systems, by a new service triggering concerning the power Supply Company etc.
- The Digital City is a virtual organization, consisting of various virtual teams [24]. This virtual organization is used for knowledge sharing and exchange, and for decision making.

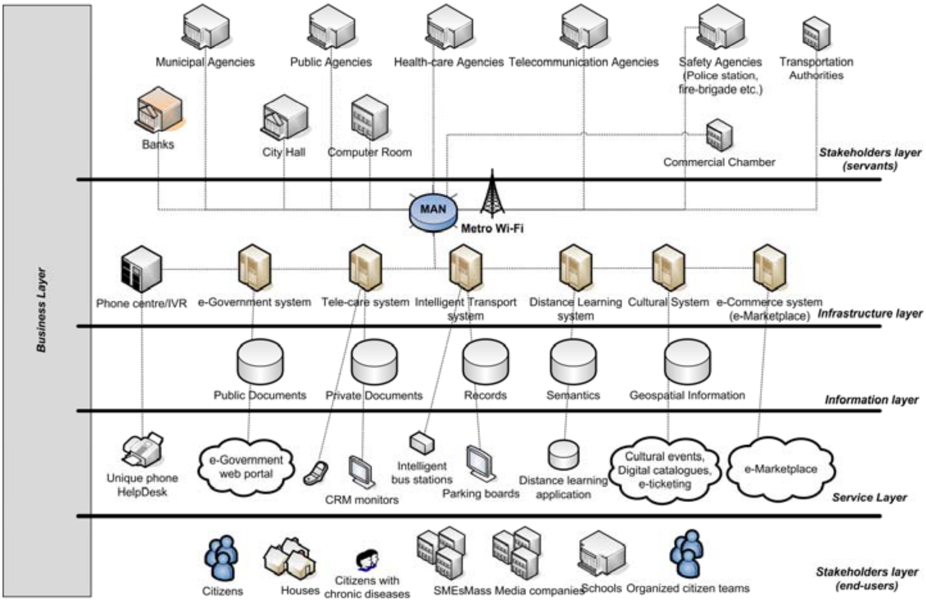


Fig. 1. The physical architecture of the Digital City of Trikala

4 Conclusions

Digital City environments have evolved since the early 90s when they first entered the digital era. Web sites and virtual reality applications transformed to smart and knowledge repositories, which began interacting with groups of citizens inside city boundaries. Then broadband networks and other intelligent technologies were applied over the city, resulting in current digital cities. However, South Korea shows digital city future, with the application of ubiquitous computing in metropolitan environments. In this paper we presented how digital cities have been evolved, and how they can simplify e-Government transactions: we called this environment "Metropolitan e-Government environment", where new challenges concerning e-Government arise. Policies and rules guiding metropolitan transactions will be investigated in future research.

We analyzed the e-Trikala digital city case study: we used its official resources in order to evaluate its performance since 2005; we mentioned the wide acceptance of the social services, as well as with organization and ownership problems in the city. Finally, we proposed extensions for the logical and physical architectures of the digital city, in order to define solutions and to obtain trust among the virtual organizations structured in the digital city. The e-Trikala case can be used as a typical example of the local authorities' success in introducing e-government systems to the benefit of citizens and of local communities.

References

1. Wang, L., Wu, H.: A Framework of Integrating Digital City and Eco-city. School of Business, Hubei University, Wuhan, China (2001), http://www.hku.hk/cupem/asiagis/fall03/Full_Paper/Wang_Lu.pdf (Retrieved, March 2005)
2. Sairamesh, J., Lee, A., Anania, L.: Information Cities. Communications of the ACM 47(2) (February 2004)
3. Sproull, L., Patterson, J.: Making Information Cities Livable. Communications of the ACM 49(2) (February 2004)
4. Widmayer, P.: Building Digital Metropolis: Chicago's Future Networks. IT Professional 1(4), 40–46 (1999)
5. Anthopoulos, L., Tsoukalas, I.A.: The implementation model of a Digital City. The case study of the first Digital City in Greece: e-Trikala. Journal of e-Government 2(2) (2005)
6. Wikipedia: The Definition of the Ubiquitous City (2009), http://en.wikipedia.org/wiki/Ubiquitous_city (retrieved April 28, 2009)
7. Ishida, T.: Digital City Kyoto. Communications of the ACM 45(7) (2002)
8. Ishida, T., Aurigiri, A., Yasuoka, M.: World Digital Cities: Beyond Heterogeneity (2001), http://www.kid.rcast.u-tokyo.ac.jp (Retrieved, April 2005)
9. Lieshout, V.: Configuring the digital city of Amsterdam. New Media & Technology 3(1), 27–52 (2001)
10. Van den Besselaar, P., Beckers, D.: Demographics and Sociographics of the Digital City. In: Ishida, T. (ed.) Community Computing and Support Systems. LNCS, vol. 1519, pp. 108–124. Springer, Heidelberg (1998)

11. Van Bastelaer, B.: Digital Cities and transferability of results. In: 4th EDC Conference on Digital Cities, Salzburg, October 29-30, pp. 61–70 (1998)
12. Partridge, H.: Developing a Human Perspective to the Digital Divide in the Smart City. In: ALIA 2004, challenging ideas, Queensland University of Technology Brisbane, Australia (2004)
13. Mountihno, J., Heitor, M.: Digital Cities and the challenges for a Knowledge-Based View of the Territory: evidence from Portugal. In: Digital 3 Workshop Local Information and Communication Infrastructures: experiences and challenges, Amsterdam, September 18-19 (2003)
14. Zook, M., Dodge, M., Aoyama, Y., Townsend, A.: New Digital Geographies: Information, Communication and Place. In: Geography and Technology, pp. 123–123. Kluwer Academic Publishers, Dordrecht (2004); printed in the Netherlands
15. Townsend, A.: Seoul: Birth of a Broadband Metropolis. Submitted to Environment and Planning B, December 7 (2004)
16. New York City Economic Development Corporation: Telecommunications and Economic Development in New York City: A Plan of Action, `http://newyorkbiz.com/about_us/TelecomPlanMarch2005.pdf` (Retrieved, April 2005)
17. Moon, M.J.: The evolution of e-Government among Municipalities: Rhetoric or Reality? Public Administration Review 62(4) (July/August 2002)
18. Hyang-Sook, C., Byung-Sun, C., Woong-Hee, P.: Ubiquitous-City Business Strategies: The Case of South Korea. In: Management of Engineering and Technology (PICMET 2007). IEEE, Los Alamitos (2007)
19. Osaka ICT Industry: Ubiquitous City Osaka. Online Publication, `http://www.ibpcosaka.or.jp/invest/e/environment/ict/ICT2007e.pdf` (Retrieved April 28, 2009)
20. Anthopoulos, L., Siozos, P., Tsoukalas, I.A.: Applying Participatory Design and Collaboration in Digital Public Services for discovering and re-designing e-Government services. Government Information Quarterly 24(2), 353–376 (2007)
21. LiQi: Digital City-the 21 century's life style. CyberGIS Studio, Peking University, Institute of Remote Sensing & GIS, Peking University, Beijing, China (2001), `http://unpan1.un.org` (Retrieved, April 2005)
22. Einmann, E., Paradiso, M.: When space shrinks - digital communities and ubiquitous society: Digital cities and urban life: A framework for international benchmarking. In: Winter International Symposium on Information and Communication Technologies (WISICT 2004). ACM, New York (2004)
23. Layne, K., Jungwoo, L.: Developing fully functional e-government: A four stage model. Government Information Quarterly 18, 122–136 (2001)
24. Godart, C., Saliou, H., Bignon, J.C.: Asynchronous Coordination of Virtual Teams in Creative Applications (co-design or co-engineering): Requirements and Design Criteria. In: Information Technology for Virtual Enterprises (ITVE 2001) Workshop, pp. 135–142. IEEE, Los Alamitos (2001)

A New Paradigm for Secure Social Lending

Emmanouil Serrelis and Nikolaos Alexandris

Department of Informatics,
University of Piraeus
80 Karaoli & Dimitriou, 18534, Piraeus, Greece
{serrelis,alexandr}@unipi.gr

Abstract. Social Lending is one of the latest trends in Social Networking, offering a communication and financial channel between individual borrowers and lenders. The various Social Lending transaction schemes could be subject to multiple security threats, in both financial and technical terms, which could affect the integrity of the service as well as the trust of citizens. This paper provides an overview of the basic characteristics of Social Lending as well as an analysis the potential security issues suggesting some appropriate corrective measures. The ultimate target is to enforce the Social Lending effort with an information security foundation that could become an appreciable alternative to the “traditional” lending system.

Keywords: Social Lending, P2P Lending, Security, Trust, e-Services.

1 Introduction

Social Lending is also known as peer-to-peer (P2P) and person-to-person lending. It is, in its widest sense, the name given to a certain type of financial transaction which takes place directly between individuals ("peers") without the direct involvement of a traditional financial institution. P2P Lending is more commonly related to lending & borrowing, although other more complex transactions could be made possible. The major technology facilitator of this new trend has been the Internet, which due to its nature can be subject to multiple security threats. This paper analyses the main features and principles of Social Lending aiming to suggest technological and procedural measures that could increase the overall security of this transaction type and, eventually, aid to gain the trust of public as a legitimate alternative of financial transaction [1].

1.1 Evolution of e-Services

In order to illustrate the driving forces of Social Lending and understand its potential market value, one should examine the evolution of e-Services. e-Services are the services provided by an individual to another individual using IT as the provision medium. Any service could be provided with the participation of a third party acting as an intermediate, interpreter or service broker.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 373–385, 2010.

At the beginning, the first e-Services were aiming on individual customers provided by commercial enterprises (Business-to-Consumer – B2C), such as e-shops, e-auction houses, e-banking etc. The next step was to provide e-Services between Businesses (Business-to-Business – B2B), enabling services such as e-procurements and e-invoicing. Inspired by these, governmental and public bodies started to provide services to individual citizens (Government-to-Citizen – G2C), such as e-taxing and e-certificates. Additionally, governmental and public bodies started to provide services to commercial organisations (Government-to-Business – G2B), as well, such as e-information exchange and e-certification. The latest e-Services breed involved services offered between Governments or public bodies (Government-to- Government – G2G). At the same time, a different type of e-Services has been developed between individuals acting as peers (Peer-to-Peer – P2P). This type is e-Services enabled e-File Sharing and many other similar services.

The latest trend of e-Services is inspired by both G2C and P2P, enabling services between individual citizens (Citizen-to-Citizen – C2C) and not just between anonymous Internet users as in the case of P2P. Examples of this kind of services are Wikis, Blogging and the hyper-trend of Social Networking.

1.2 What Is Social Lending

Social Lending is a special case of Social Networking that uses the networking attribute of the web to embrace financial transactions as well. The basic idea with Social Lending is that when someone needs money, other individual users will come with an offer for the loan terms and if the candidate loanne accepts that offer, the loan can be directly given without the intervention of any “traditional” loan party or financial institution, such as a bank.

Alternatively candidate lenders can pool their funds together and lend them at x% interest rate. Some existing web sites offering Social Lending services such as Prosper [2], use a credit score to determine the risk rate and then, based on that risk rate, there can be a bid for the loan according to the loanee’s terms. What makes those sites popular is the "social" aspect which is translated to the ability for the candidate loanee to post his/her story about why they need the money and try to convince the potential lenders.

Social Lending is currently open to any individual person or company to participate (as a lender or borrower) allowing augmentation of the lending communities to a very large scale using the Web technologies. It is closely related to Microcredit which is loaning very small amounts to multiple borrowers.

1.3 Facts and Figures

Having presented the basic idea of Social Lending, it should be stressed that an attempt to secure such an e-Service would be highly appreciated from the lending communities, since there is a dramatic increase on the lending volumes. As mentioned by [3] “In 2005, there were 118 million $ of outstanding peer-to-peer loans. In 2006, there were 269 million $, and, in 2007, a total of 647 million $. The projected amount for 2010 is 5.8 billion $”. Another source [4] reports that the total loan volume on the 30th of January 2009 for P2P Lending Companies was 800 million $ divided to 31 companies around the world. This impressive growth rate signifies that the forthcoming e-era could be nearer than “traditional” financial institutions might think. As Gartner claims in [5] “By 2010, social-banking platforms will have captured 10% of the available market for retail lending and financial planning.” These facts turn the security and trust aspects into two very urgent requirements for Social Lending adoption.

2 Analysis of Social Lending

As it can be expected, the Social Lending trend could bring about several implications and leave additional room for extensions. Apart from the obvious technical and legal issues, there could also be important social and commercial issues and even political implications from the wider adoption of such as a trend. The following paragraphs attempt an analysis of the related issues.

2.1 Social Lending Models

Social Lending appears in two major forms: the "online marketplace" model and the "family and friend" model.

The first model of Person to Person Lending on the Internet makes possible for individual lenders to find individual borrowers and vice-versa. This model relates borrowers with lenders through an auction-like process in which the candidate lender willing to provide the lowest interest rate "wins" the borrower's loan. The marketplace schema may involve other intermediaries (such as specialized web sites) who package and resell the loans, but eventually the loans are sold to individuals (one lender for one borrower) or groups of individuals (many lenders for one borrower).

The second model ("family and friend") relinquishes the auction-like process completely and focuses on borrowers and lenders who already know each other, similarly to the situation where two (or more) friends or business associates formalize a personal loan. While the primary advantage of the marketplace model is the correlation aspect, the family and friend model emphasizes online collaboration, loan formalization and servicing.

This paper is concerned with the first model of Social Lending mainly because the issues of security and trust are of less importance for the second model. This argument is validated by the fact that the related bodies (borrowers and lenders) are already known to each other and thus taking much less risks by participating to that transaction. Another motive for focusing on the first flavor of Social Lending is the fact that most of the current loans are between individuals who were unknown to each other before the transaction.

2.2 Case Studies

There are currently more than forty major p2p lending web sites targeting more than 30 countries globally [6]. While most of them follow similar procedures, in order to demonstrate potential security threats it would be quite useful to present a couple of those cases.

Zopa [7] was launched in March 2005 by several people with previous experience in financial services. It was the first person to person lending and borrowing community in the UK. Zopa currently has over 275,000 members [8] demonstrating a growth of 75000 members during the past 12 months. They claim that by combining a better interest rate to borrowers and a better return for lenders and a more community based approach, Zopa is essentially reinventing a model of friendly societies claiming to provide a more social and ethical financial service closely allied with mutual gain [8]. Zopa's current business model is based on borrowers paying a one percent (1%) exchange fee to Zopa upfront. In practice the site should offer lenders and borrowers value in that they get better rates of interest by cutting out a bank middleman. They also get more control over the lending process and establishing a mutually agreed loan rate. The financial risk for lenders on Zopa is reduced by spreading loans to multiple borrower. Each lender makes loans to at least 50 borrowers, and lenders' exposure to any one borrower is capped at £200. All loans are claimed to be backed by a "legally binding contract," which is a major concern for all participating individuals. If a Zopa borrower defaults on a payment, Zopa will use exactly the same recovery processes that banks use. An optional feature provided by is Zopa is the verification stage, during which they add in information from the candidate lenders credit file (their credit score, their employment history etc) to give a fuller picture of the candidate borrowers.

Prosper [2] has been another very successful case of P2P Lending in US. Until the fall of 2008, Prosper had enabled 25,000 loans between its 750,000 members that averaged $6,000 each, which made about $150 million in serviced loans. However during the past few months Prosper has been a target for shutting down by the US Securities and Exchange Commission (SEC) because the “loan notes issued between January 2006 and October14, 2008 are securities, and Prosper violated Section 5 (a) and 5 (c) of the Securities Act, which prohibits the offer or sale of securities without an effective registration statement or a valid exemption from registration” [9].

The two approaches differ in some key points [10]. Zopa stresses the risk management features to the lenders – investors. This is achieved by spreading the risk across multiple borrowers and forcing lenders to choose one or more borrowers to support lower interest rates. Prosper, unlikely Zopa, directly allows lenders to choose and finance individual borrowers. In this case, the Social Lending nature of the transaction is set off in another manner. Prosper uses a reverse auction to match parts of its loans, and the lenders choose who gets funded based not only on abstract figures (such as credit rating, income and previous lending reputation) but also on a personal statement. This may cause problems in some countries (or states) with interest rate regulations. That is, laws against usurious interest rates which prevent lenders from getting what they consider a suitable return to reimburse them for lending to borrowers with higher risk.

2.3 Issues

The case studies presented in the previous paragraph can become the basis for raising some questions regarding the proper function of the Social Lending schema. These questions are related to the security of transactions, the trust to the Social Lending model, the risk of financial frauds, the legal and regulatory obstacles that could affect the schema as well as the operational specifications that should be implemented to make this model viable. These key issues, as they are portrayed in the following sections, can be categorized to technical, legal, regulatory and operational issues.

2.3.1 Technical

Social Lending could cause a series of technical questions for the development of such a schema. Due to the fact that Social Lending is a form of Social Networking, the basic technology to implement it, is Web 2.0. This is second generation web development and web design, is recognized as a facilitator of communication, information sharing, interoperability and collaboration between the members of on-line community. It has also shown the way to the development and evolution of web-based communities, hosted services, and web applications.

Another very important technical issue is the need for a suitable correlation mechanism that could match the loan demand and the potentially related offers. A related attempt that could be used is [11] which "comprises a demand placement module, a supply providing module, and an algorithm linking the demand placement module to the supply providing module".

For the situations where the loan is spread across multiple lenders or borrowers, an appropriate mechanism for managing the microcredit distribution is essential. A suggested approach comes from [12] which could be adapted to Social Lending.

A different technical issue is the reputation mechanism that can be used for evaluating the risk of giving a loan to a specific individual. On a Social Lending scheme, the potential lenders can be benefited from a credit score of the potential borrower. This credit score is based on a reputation mechanism which evaluates the credit value of the potential borrower by combining factors, such as income, previous defaults and comments from other lenders. Similar approaches have been very useful for eBay [13] where "an online feedback mechanism that encourages buyers and sellers to rate one another seems to have succeeded in encouraging cooperative behavior in an otherwise very risky trading environment".

Apart from these technical issues that are related to the functional aspects, there are also issues related to the security aspects of Social Lending. These comprise the issues of integrity, privacy, confidentiality and anonymity, exposing questions such as:

- How is the transaction protected from a man-in-the-middle attack that could change the terms of the loan?
- How is the transaction protected from a "bad" lender or a "bad" borrower that could change the terms of the loan on his/her favor?
- How is the privacy of the lender and the borrower ensured?
- How is the anonymity of the lender and the borrower ensured, during the terms negotiation phase?
- How can the lenders and the borrowers trust the "intermediate" web site that provides the Social Lending service?

2.3.2 Legal

In addition to the technical issues there are also many legal issues concerning Social Lending. As stated by [14] "the legal framework of the EU member states does not yet appear to be suitable for the growth of microcredit. Statistics on micro-credit are not sufficiently developed in the EU, which is due to the fact that micro-credit is not foreseen either in national or in EU-legislation". This is also valid for US and most of the other countries proven by the rapid rise and fall of related attempts.

The legal questions that should be posed are:

- Are these transactions legally valid?
  - If not, how can these transactions can be legally valid?
- How is the legal responsibility divided between the dealing parties?
  - What is the legal responsibility of the lender?
  - What is the legal responsibility of the borrower?
  - What is the legal responsibility of the intermediate “web site”?
- How are the personal data protected?
- Should there be a tax deduction for these transactions?
  - Who (or how) should take care of tax deductions?

Some parts of these questions are answered by the EC directives 1999/93/EC[15] and 2000/31/EC[16]. However the call for “EU legislation to encourage microcredit schemes” reveals the existing legal gap. With this legislation [17], “EU aims to remove problems caused by competition and money-laundering rules, to allow more EU co-funding, to introduce a harmonised regulatory framework for microcredit providers and to raise their profile”.

2.3.3 Regulatory

On top of the previously mentioned legal issues, there are a series of regulatory concerns. The existing regulatory framework aims to reduce the risk generated by the various financial transactions. It is based on a set of rules regarding risk management which should be followed by any institution offering financial transactions. However this framework may require some sort of enhancement to cover questions such as:

- Should the existing Social Lending web sites follow the existing regulatory framework?
- Should the potential lenders and borrowers follow the existing regulatory framework?
- Which requirement should be asked from any Social Lending web sites?
- Are there any requirements for minimum capital?
- Who (and how) should supervise the Social Lending Market?
  - What should be the role of the National Banks?
  - What should be the role of the International Banks?
- Is Basel II applicable for Social Lending?

2.3.4 Operational

All three sections of the key issues mentioned before have a major effect on the operational aspect of Social Lending. From this perspective, the most important issue here is trust between the dealing parties. This is equally important for all: Lenders need to trust borrowers and the intermediate, borrowers need to trust lenders and the intermediate and the intermediate needs to trust lenders and borrowers.

Special care should be taken for the following issues in order to ensure the transaction:

- Money laundering
- Tax evasion
- Illegal export / import of exchange
- Identity manipulation / exploitation
- Default loans
- Graft

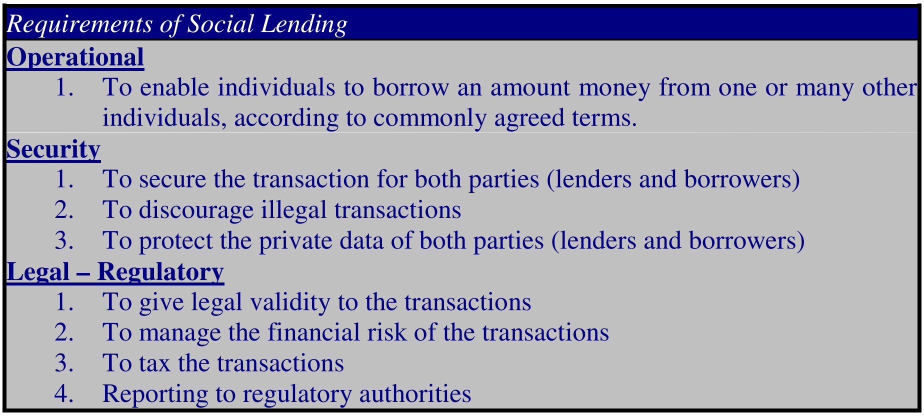
In order to manage the above issues, the following figures should be considered:

- Financial / Credit Risk
- Credit limits

2.4 Specifications

Having mentioned the issues that could affect the delivery of Social Lending services, Table 1 sums the necessary requirements.

Table 1. Requirements of Social Lending



Requirements of Social Lending
Operational
1. To enable individuals to borrow an amount money from one or many other individuals, according to commonly agreed terms.
Security
1. To secure the transaction for both parties (lenders and borrowers)
2. To discourage illegal transactions
3. To protect the private data of both parties (lenders and borrowers)
Legal – Regulatory
1. To give legal validity to the transactions
2. To manage the financial risk of the transactions
3. To tax the transactions
4. Reporting to regulatory authorities

3 Making Social Lending Safer

There are many possible ways of making a Social Lending model better, especially if one considers its multiple variations, but the following section focuses on security.

3.1 e-Services – The Next Generation

As mentioned in previous paragraphs, the latest trend of e-Services is inspired by both G2C and P2P, enabling services between individual citizens (Citizen-to-Citizen – C2C). The “Citizen” label distinguishes individual persons which are part of a traditional society or community from anonymous persons which have no connection relationships with traditional social structures.

The evolution of e-services would enable the provision of a new breed of e-services that would follow the C2C relationships but also benefit from the existence of a trusted intermediate party who could act as a broker between the two dealing parties of lenders and borrowers. This could potentially cover gaps identified in the previous sections and provide greater security and trust to the Social Lending e-service. A possible candidate for the role of the broker can be either a governmental body (such as the ministry of finance, a municipality or a national bank) or an existing private financial institution.

The participation of a broker should not eliminate the benefits coming from the principles of Social Networking. Instead, they should only provide the operating framework in order to achieve greater trust and validity for the loan transactions. A possible expression of this type of e-services could be something like C(2G)C for e-services enabled by governmental bodies and C(2B)C for e-services enabled by private bodies (businesses).

3.2 A New Paradigm

The next generation of e-services could also dictate some useful changes in existing Social Lending implementations.

3.2.1 Overview

The suggested new paradigm of Social Lending would transform the lending process as illustrated in the following scenario.

A candidate wishes to borrow an amount of money, e.g. 20000$. He accesses the Social Lending web site of the broker party and fills in the terms of the loan he wishes to receive. The terms include the amount of money, the loan period, the maximum interest that would be acceptable, his personal information as well as a supportive text that would aim to reason on loan purposes.

Following the completion of all the necessary information, the loan request is now recorded in the web site and can be evaluated by any possible candidate. So far, only the loan information is made available to the potential lenders, keeping the private data of the borrower secured.

At this point, the broker may choose to offer the potential lenders a few hints about the magnitude of the risk exposure that the lenders may face if they decide to provide this loan. This is done by using a reputation scheme similar to the one described in paragraph 2.3.1. The reputation scheme may associate previous defaults, opinions on the borrower from other lenders or the existence of the borrower to a bank “black list”. Additionally, they may require from the borrower to provide supplementary information such as income, existing deposits and list of guarantors.

Having weighed up all above facts, the lenders may now make an offer for the loan. This is done by accessing the web site and “bidding” on the interest which should be lower than the maximum interest that would be acceptable by the borrower. When the individual with the lowest “bid” is found, the period when the loan request is closed. As an optional closing condition, there could be a fixed time period. Now, it is the lender’s turn to be checked by the broker. This assessment will secure that the borrower will get the amount requested with the terms mutually accepted.

When both parties are checked against the broker's reputation database, the loan should be signed. This is done by the use of digital signatures. Each party has his own digital certificate obtained by a trusted third party, according to the PKI model. The e-contract is compiled under the mutually agreed loan terms by the broker, who is acting like a digital notary. The e-contract is digitally signed by both parties and the lender should now transfer the amount agreed within a standard period of time (no more than a few days) to the borrowers account. The borrower is now bound to pay the installments as agreed in the contract.

There are a couple of optional steps in that paradigm of Social Lending. For example, the broker is able to spread the loan to multiple lenders so that the loan could be more easily funded and the risk of a default would not affect greatly the lenders. However, this would increase the operation overhead since each one of the lenders should sign the e-contract. Another optional step could be for the broker to allow the spread of the lender money to multiple borrowers. This tends to transform the lender to a traditional investor who would aim decrease the loan risk by spreading his investment portfolio to multiple targets.

On top of all these, the party acting as the broker is in the position to take advantage of the transaction by introducing a commission for each loan. This could be a standard amount or a percentage on the loan amount. This could make this scheme economically viable while keeping the deposit/loan gap closer than the one offered from the traditional financial institutions such as banks.

Table 2. Organizational Improvements

Organizational Improvements

Broker

1. Establish the role of a broker that would act as in intermediary.
2. The broker can be:
    a. A governmental body (ministry of finance, a municipality or a national bank)
    b. An existing private financial institution
    c. An independent body
    d. A non profit organisation

Legal

1. The legal framework should include on-line signing of private contracts.
2. The regulatory framework Specify and include the financial risk requirements for the brokers.

Broker responsibilities

1. Provide the communication medium between the lenders and the borrowers
2. Certify the identity of the lenders and the borrowers
3. Evaluate the profile of the lenders and the borrowers in terms of credit risk
4. Enable the compilation, signing and distribution of e-contract

Risk reduction

1. Spread loan on many lenders
2. Spread loan on many borrowers
3. Limit loan amount
4. Use reputation (credit score) schemes

Finally, the broker has the ability to perform a tax deduction on the loan based on the tax regulations. However, since tax regulation vary from country to country, this may be difficult to apply in an international level, leaving space for Social Lending legislation to deal with this issue. However, in a national or EU level this could be an interesting option for tax authorities.

3.2.2 Organizational Improvements

The scenario above leads to several suggestions that could improve Social Lending in both organizational and technical terms. The organizational improvements of Social Lending that use the information of the above scenario are summarized in Table 2.

3.2.3 Technical Improvements

The technical improvements of Social Lending combining the information of the above scenario are summarized in Table 3.

Table 3. Technical Improvements

Technical Improvements
Anonymity
1. Keep the personal data of the lenders and the borrowers hidden until they agree on the terms of the loan
Encryption
1. Encrypt the personal data of lenders and borrowers
2. Encrypt the information used in the transaction (amount, interests etc.)
Digital Certificate
1. Assign a digital certificate to each party (lenders and borrowers)
2. Obtain certificate from a Trusted Third Party
Digital Signature
1. Digitally sign the contracts between the lenders and the borrowers using their own certificates
e-Contracts
1. Compile private e-contracts for loans
2. Use the mutually agreed terms
3. Broker to act as a digital notary
Loan Community
1. Development of a wide and trustworthy loan community
2. Use Web 2.0 Technologies
Trust
1. Reputation mechanism based on existing credit evaluation (Banks' "black lists")
2. Anti - Money Laundering Mechanisms

4 Conclusions

The Internet has created some unique new situations and business opportunities for individuals. In today's environment, in which financial crisis left hardly any room for high return investments with relatively low risk, Social Lending can be one of those few opportunities for both lenders and borrowers. This new kind of e-Service uses the Web to create a network of regular people who wish to borrow and lend money to one another, at agreed upon terms that are a result of bidding. These Web sites even allow pools of people to fund loans partially or in full.

This paper has presented the current variations of Social Lending stressing their weak points and suggesting a new approach that is enforcing security and trust by the introduction of a broker role in the C2C relationship. This broker role can be performed either by a governmental – public body or by a private body.

4.1 Benefits

Social Lending models try to bring in again the social features that are neglected in traditional centralized banking models, while offering a balance of social and financial e-service. This is opposed to the strict profit-centric approach of typical financial institutions. They also challenge current practices to benefit from the lack of significant operating costs that are common in other online and offline institutions. Consequently, they accomplish the reduction of infrastructure expenses (such as physical branches) which are common place for traditional lending institutions, such as banks. These increasing savings can be used to narrow the deposit/loan spread.

For instance, a bank may offer to its customers a poor 1% return for any deposit, nevertheless, when they lend those same customer funds (on deposit) to the bank's other customers who need to borrow, they do so at a much higher rate of interest, despite the fact that they keep the difference as a profit. Social Lending aims to correct this anti-social feature and form a community which would allow those who have funds to lend at a better return, while it provides a better interest rate to those who need to borrow, by removing the bank from the equation.

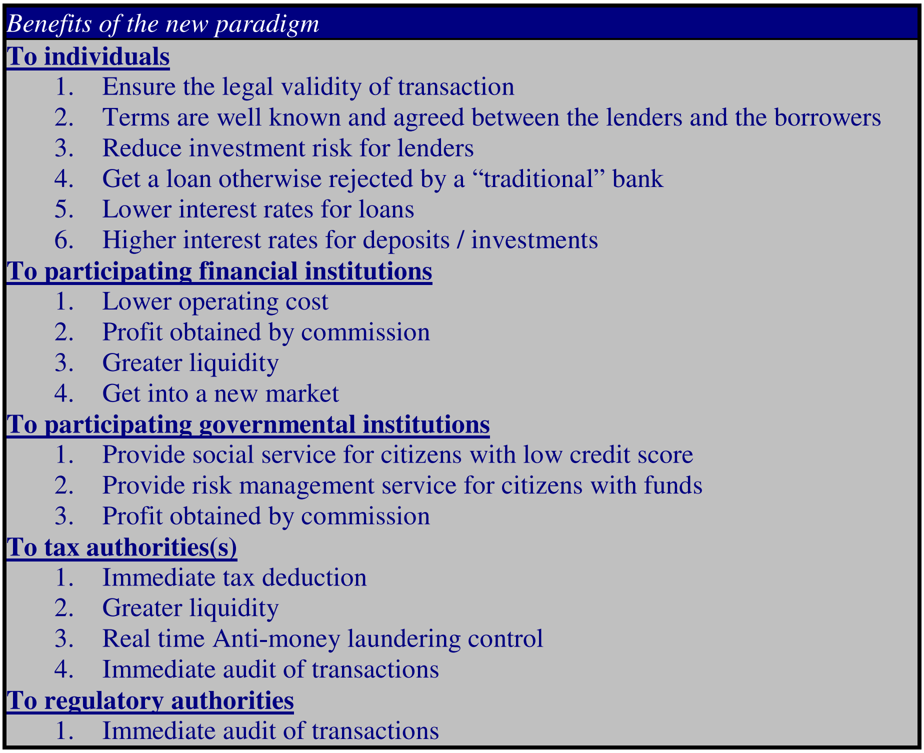
Additionally, this model permits potential lenders to directly manage the distribution of their own funds, as opposed to the traditional bank lending models which pool all funds as one and entirely ignore the individuals who actually own the money from the decision-making process regarding the rates and terms of who may borrow that money, for how long they may borrow it and how they are going to return the money.

The new paradigm described above offers a few advantages comparing to the existing the common Social Lending implementations. These are summarized in Table 4.

4.2 Further Evolution and Improvements

The attempt presented introduced the role of a broker that could act as a security enabler for Social Lending schemes. As it can be understood, this attempt can be further evolved and improved. Since, most of the improvements are technically feasible and available; one should focus on the organizational aspects. A possible expansion could be to investigate the exact operating requirements for an existing financial institution that wishes to act as a broker. This could be very interesting for banks who wish to get into the new market of Social Lending. However should be dealt with caution in order to prevent the cannibalization of their existing markets. Another possible improvement could be to investigate the legal framework and try to suggest a Social

Table 4. Benefits of the new social lending paradigm



Benefits of the new paradigm
To individuals
1. Ensure the legal validity of transaction
2. Terms are well known and agreed between the lenders and the borrowers
3. Reduce investment risk for lenders
4. Get a loan otherwise rejected by a “traditional” bank
5. Lower interest rates for loans
6. Higher interest rates for deposits / investments
To participating financial institutions
1. Lower operating cost
2. Profit obtained by commission
3. Greater liquidity
4. Get into a new market
To participating governmental institutions
1. Provide social service for citizens with low credit score
2. Provide risk management service for citizens with funds
3. Profit obtained by commission
To tax authorities(s)
1. Immediate tax deduction
2. Greater liquidity
3. Real time Anti-money laundering control
4. Immediate audit of transactions
To regulatory authorities
1. Immediate audit of transactions

Lending Implementation in a way that a broker would not need to comply to the regulatory requirements of financial authorities. However the “Holy Grail” of Social Lending would be a variety that would not need any central gathering of the loan information, as in the case of P2P file sharing.

4.3 Summary

Social Lending is one of the latest trends in Social Networking, offering a communication and financial channel between individual borrowers and lenders. Although it has demonstrated a significant growth, it still has several issues, related to security, trust and legal validity. This paper has proposed the introduction of a new role within Social Lending in order to tackle some of these issues. The broker role could be performed by a private or governmental body. So far it seems more possible and legally feasible to adopt the private body scenario, especially in the case where the private body is an existing financial institution. This would result multiple benefits for all participating parties. The second version of the new paradigm of Social Lending, redefines the role of governmental bodies, adding a financial service to public services. This version, although more trustworthy if implemented, is more difficult to be adopted due to political and commercial reasons. In any case, Social Lending is a very hot topic that would interest the online community from social, commercial and political point of view.

References

1. Wikipedia, http://en.wikipedia.org/wiki/Peer-to-peer_lending
2. Prosper Loans Marketplace, http://www.prosper.com/
3. Financial Lifeline, http://www.filife.com/stories/borrowing-from-p2p-lending
4. P2P Banking, http://www.wiseclerk.com/group-news/services-p2p-lending-companies-by-loan-volume-jan-09/
5. Gartner, Inc., http://www.gartner.com/it/page.jsp?id=597907
6. Financial News Publishing Ltd, http://www.vrlknowledgebank.com/reportinfo.php?id=94&page=3
7. Zopa Ltd., http://uk.zopa.com/ZopaWeb/
8. Wired magazine, http://www.wired.com/techbiz/media/news/2005/03/66965
9. Vator, Inc., http://vator.tv/news/show/2008-11-26-sec-calls-for-prosper-to-shut-down
10. Dhand, H., Mehn, G., et al.: Internet Based Social Lending. Communications of the IBIMA 2 (2008)
11. Choudary, V., Gedupudi, R.: Priority bid processor and protocol therefore, US Patent AG06Q4000FI, http://www.faqs.org/patents/app/20090055307
12. Armendáriz, B., Morduch, J.: The Economics of Microfinance. MIT Press, Cambridge (2005)
13. University of Maryland, R. H. Smith School of Business, http://www.rhsmith.umd.edu/faculty/cdell/reputation.html
14. Character Based Lending Project, http://www.chabal.eu/uploads/media/Microfinace_in_Greece_-_Development_of_action_proposal.pdf
15. Directive 1999/93/EC, http://www.signatur.rtr.at/en/legal/directive.html
16. Directive 2000/31/EC, http://ec.europa.eu/internal_market/e-commerce/directive_en.htm
17. European Parliament, Economics Committee, Call for EU legislation to encourage micro-credit schemes, http://www.europarl.europa.eu/pdfs/news/expert/infopress/20090119IPR46575/20090119IPR46575_en.pdf

Techno Generation: Social Networking amongst Youth in South Africa

Antoinette Basson, Yoliswa Makhasi, and Daan van Vuuren

Film and Publication Board
87 Central Street, Houghton, Johannesburg, South Africa
{antoinette,makhasiy}@fpb.gov.za, bmr@unisa.ac.za

Abstract. Internet and cell phones can be considered as new media compared to traditional media types and have become a fundamental part of the lives of many young people across the globe. The exploratory research study investigated the diffusion and adoption of new media innovations among adolescents. It was found that new media have diffused at a high rate among South African adolescents who are not only the innovators in this area, but also changing their life styles to adapt to the new media. Social networking grew to prominence in South Africa especially among the youth. The protection of children from potential harmful exposure and other risks remain a concern and adequate measures need to be initiated and implemented for children to enjoy social networks and other forms of new media. The exploratory research study provided worthwhile and interesting insights into the role of the new media, in the lives of adolescents in South Africa.

Keywords: New media, social networks, child protection.

1 Introduction

One of the most dramatic changes in the world during the past decade has been the arrival of the Internet and cellphones. These media types are regarded as *new media* especially when compared to traditional electronic/broadcast (television and radio) and print (newspapers and magazines) and out-of-home (outdoor and cinema) media. Both the Internet and cellphones have become part of society and are nowadays part of the lives of many adolescents and adults. In fact, Internet and cellphone access has not only changed the communication dynamics, behaviour and habits of adolescents, but has also had an immense impact on many dimensions of business, culture, politics, sport and society. These media types are also increasingly impacting on the way in which interpersonal relationships between people are formed.

The immense change in the media environment, specifically in South Africa over the past few decades, is evident from the following major evolutions in the communication industry of South Africa:

- The first radio broadcast in South Africa took place in 1923, with the South African Railways broadcasting from Johannesburg [1].

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 386–396, 2010.

- Just after the Second World War, the South African Broadcasting Corporation (SABC) introduced commercial radio stations.
- In 1960, an FM radio network in most of the indigenous languages was launched.
- In 1976 television (analogue broadcasting) was introduced.
- In the early 1990s two new mass communication media, namely the Internet and cellphones, were introduced into South Africa, changing interpersonal communication for life.
- In the years to follow the digitalization of personal and mass communication has already changed, and will continue to change interaction between people irrevocably.

These communication changes outlined above clearly reflect the emergence of digital, computerized or networked information and communication technologies, especially during the latter part of the 20th century.

The collective term encompassing these technologies is *new media,* of which the Internet and cellphones (each with its own constantly new and increasingly popular features) are regarded as the 'new' major innovations which have diffused rapidly and have been adopted by the young and the old. The rate of adoption or diffusion has stimulated the need for research, especially among the adolescent population of South Africa.

The Internet, as communication medium, has shown tremendous growth [2]. Currently, the Internet is used by approximately 20 % of the total world population, with North America the continent with the largest penetration (71.1 %) and Europe the second largest (43.4 %). Africa has the lowest usage with only a 4.4 % penetration rate. Clearly, the gap between Africa and the rest of the world, or the low diffusion rate, with regard to Internet connectivity, is huge. However, Africa is the continent showing the greatest potential to further increase Internet connectivity and adoption of this *new media*. This is already clear from the fact that Africa has recorded the highest growth of 1 100 % in Internet access from 2000 to 2008 [3]. Leading the way in this regard is South Africa, which accounts for almost 90 % of all African Internet users [4]. According to the leading South African technology research organisation World Wide Worx [5], Internet users in South Africa at year-end 2008 were estimated at 4.6 million (an approximate 10 % diffusion rate). For year-end 2007, the number of Internet users in South Africa was 4.1 million, for year-end 2006 the number was 3.8 million, and for year-end 2005 Internet users amounted to 3.6 million.

Adolescents are progressively showing increased levels of engagement with this *new media*. Factors contributing to the perceived high rates of diffusion of the Internet among adolescents include the roll-out of Internet access services not only to households, businesses (with specific reference to Internet shopping, Internet Cafes and Wi-Fi hot spots) and communities (e.g. digital villages), but also to schools across South Africa. Undoubtedly, Internet access has changed the communication lifestyle of many adolescents, who nowadays are adept at applying the main features of the Internet.

Not only has the Web developed over time as an information source, but over time various social networks diffused on the Web. The most popular diffusions in this regard include Facebook and MySpace with an estimated 90 plus million active users and 240 million profiles recorded internationally [6] and [7] for each respective network.

The social networking innovation first caught on with South Africans in the form of MySpace.com, but local Internet users seem to be following the worldwide trend of belonging to more than one social network at a time. In South Africa, Facebook has emerged as the major competitor of MySpace. This massive social networking service grew to prominence due to its attractive features and highly appealing tools. In fact, the Web Information company, Alexa, has indicated that Facebook was the highest accessed Website in South Africa in 2007 [8] displacing Google, which for long has been the most accessed Website in South Africa since the new millennium.

To gain some idea of the magnitude of users or diffusion rate, international figures reveal increased interest among users of this communication medium and show that users of the social networking site Facebook have increased from 40 million users in 2005 [9] to over 200 million users in 2007 [10], and is still growing rapidly [11]. South Africans, in particular, have embraced the Internet social networking revolution, with over 50 000 new users signing on to the local Facebook network in 2007.

The Facebook ‘South Africa’ network ranges between 87 000 to 120 000 members [12] and [6]. Most recent figures show that Facebook boasts over 25 million members worldwide [12].

Facebook has also evoked high levels of interest and is a very popular communication medium among South African adolescents. However, the exact magnitude, popularity levels and diffusion rates of Facebook, MySpace and even new innovative cellphone social networks among local adolescents in particular, are rather uncertain or sparse at this stage. There is also very limited public demographic information on South Africa's youth using social networks.

These shortcomings motivated the research study to measure the lifestyle changes of adolescents using social network sites to communicate. How, when, how frequently and for what purposes these networks sites are utilised and how these innovations are adopted and impact on the behaviour of adolescents in particular, were cited, among others, as the main research focus of this study rather than only quantifying the number of adolescents who use Internet features such as email or any of the WWW (FaceBook and MySpace) or cellphone (MXit) social networks.

Internationally, the most recent opinion on adolescents and the new media is that they are the defining users of the Internet. This is particularly evident in the USA where adolescents not only chat and spend more time online than adults, but also use online technologies, such as instant messaging, more often than adults [13]. Worldwide, the Internet and cellphones are also currently used predominantly for interpersonal communication as opposed to their initial primary use for entertainment and information. Most research studies on new communication media have been conducted mainly in the developed part of the world. A good example of early research in this regard was by researchers at the London School of Economics and Political Science in the last years of the previous century [14]. This study was undertaken at the start of the diffusion cycle of cellphones, and the Internet was not as widely used as currently.

Some of the findings of this multi-country (Britain, Israel and 10 countries in Europe) study are also relevant to the current situation in South Africa, especially with regard to the use of and access to computers and the Internet. Findings from the latter study included the following:

- In every one of the 12 countries involved, results showed that children and young people preferred outdoor/social activities to the media. Children and young people preferred being with friends above all else.
- In some countries (Britain, for example) parents and teachers regarded screen media as a threat to the reading of printed material, whilst in some other countries (e.g. Denmark) television viewing was not seen as a threat to the reading of books.
- Major differences were found between countries with regard to the availability of the most recent technological developments. Whereas in Finland a limited number of affluent and rural children had Internet access a decade ago, only tiny minorities had Internet access in Britain and Italy. Social class differences were also prevalent regarding availability and access.
- Across Europe 10 years ago, there was evidence of fragmentation of the television audience and an increasing tendency for family members to watch television alone was evident.

Within the context of dramatic social, economic and developmental changes faced by South Africa, research on adolescents and the new media should take account of the developments emerging from the European examples highlighted above [15].

The need for research on the *new media* (Internet and cellphone and their corresponding features) targeted specifically at the adolescent population of South Africa is imperative. Consequently, the University of South Africa (BMR, Youth Research Unit) in partnership with the Film and Publication Board (FPB), decided to undertake a research study on the incidence and usage of *new media* among adolescents. More specifically, the research study investigates the rate of diffusion of new media in the adolescent market and the extent to which new media innovations have been adopted among adolescents. The study has also been developed to identify the factors that impact on and direct the new media communication behaviour of adolescents.

2 Research Methodology

To facilitate the process of designing a research model for the study, it was decided to first conduct an exploratory research study on new media to gauge the usage and frequency levels of new media among secondary school children in the City of Tshwane (Pretoria).

A non-probability judgmental sampling approach was used in selecting five schools in the City of Tshwane (Pretoria). After permission was granted by the Gauteng Department of Education, the headmasters of the five judgementally selected high schools were approached for participation in the research study. With the assistance of the educators, the questionnaires were distributed to adolescent learners enrolled for grades 8 and 10 to 12 at the respective schools. One class in each grade (grades 8, 10 and 12) was included. The questionnaires were completed during class time under supervision of an educator. Learners were requested to self-complete the questionnaire and return it to the educators, who subsequently returned it to the researchers.

More specifically, the questionnaire addressed the following contemporary research topics:

- access to and adoption, ownership and usage of the Internet and cellphones as major new communication media types
- adoption and usage of new media features such as social networking facilities (e.g. MySpace, FaceBook and MXit) and gaming
- access to and adoption and usage levels of other media such as iPods, MP3 players as well as traditional media, including broadcasting (television and radio) and print media (magazines and newspapers) as well as cinema
- adoption of and participation in communication networks
- advantages experienced due to the diffusion of new media
- factors impacting on adoption or rejection of new media communication practices
- the extent to which the use of new media is consistent with adolescents' expectations, values, norms, image or status profiles

During the initial planning stages the questionnaire was pre - tested as part of the interviewing procedure at the first selected school and rolled-out to the other four schools. The questionnaire consisted of 60 questions and took about 20 minutes to complete. A total of 490 learners completed and returned the questionnaires. Once the questionnaires were completed and retrieved from the five schools, the questionnaires were edited to ensure that they met the desired sampling requirements. Following the editing process, the data on the questionnaires was edge – coded with the help of a carefully designed coding manual. Finally, the data was captured in electronic format and stored for the purpose of analysis.

3 Research Findings

In this research article, some interesting results of the exploratory research study will be presented with specific focus on social networks, MXit and blogs via Internet and cell phones.

3.1 The Internet

In the light of the relatively low access to the Internet in South Africa (10.7 %) amongst adults 16 years and older [16], it is important to gain an idea of the nature and extent of Internet usage amongst adolescents.

In contrast to the reported limited Internet access of adults, more than 85 % of the participating adolescents of the survey reported that they had access to the Internet during the month preceding the survey. Participants were presented with a list of activities on the Internet to indicate the extent to which they participate in these activities. These results are reflected in figure 1.

It is clear from Figure 1 that the Internet is generally used as a tool to access information (68.7 %). The Internet is also used as a source of information for school assignments (39.8 %) and for accessing '*personal information for myself*' (28.8 %). In addition, the Internet is also used by approximately half the participating adolescents to download content (50.2 %) and for playing games (37.3 %).

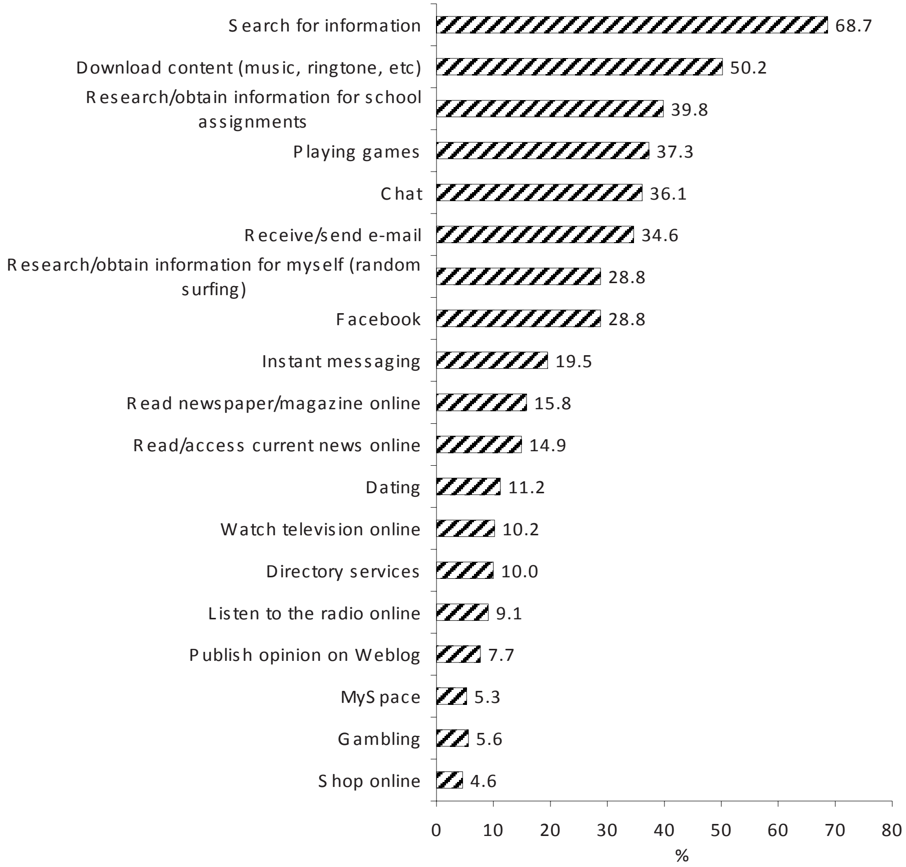


Fig. 1. Activities used on the Internet.

It is noteworthy from Figure 1 that receiving and sending e-mails (34.6 %), 'chatting' (31.1 %) and using Facebook (28.8 %) were mentioned as Internet activities of adolescents.

3.2 Social Networking Sites

The exploratory research study focused on adolescents' use of social networking sites such as Facebook, MySpace and YouTube, each with a series of activities. The research findings are presented in Table 1. It was found that the most preferred social network site for all activities measured was indeed Facebook. On average, approximately 25% of the participating adolescents used Facebook for a number of activities as reflected in Table 1. Facebook is mostly used to chat with friends to learn more about people and to exchange general messages. MySpace was the second most preferred site followed by YouTube.

Overall, uploading photos (55.8%), storing photos (53.1%) and chatting with group friends (51.5%) are more regular activities in which adolescents engage through social networks such as Facebook, MySpace and YouTube.

Table 1. Use of social networking sites

Activities	Facebook	MySpace	YouTube	Other	Total
Upload photos	29.0	12.0	7.7	7.1	55.8
Post opinion	21.8	11.4	4.8	4.6	42.5
Obtain latest social news (fashion, current, etc)	22.2	9.5	6.4	5.6	43.8
Post videos	16.0	10.0	13.5	5.8	45.2
Join groups & chat with group friends	34.0	8.3	2.5	6.6	51.5
Download (ringtones, wallpaper, software, etc)	10.8	11.6	12.2	12.0	46.7
Learn more about people met	30.7	9.1	2.7	4.6	47.1
Exchange general messages	30.1	8.7	2.9	5.2	46.9
Exchange private messages	28.4	9.1	1.9	6.0	45.4
Store photos	27.4	14.5	4.4	6.8	53.1

The continuous development of information and communication technologies and rapid diffusion within the adolescent market create a number of challenges with regard to the protection of children. Besides sharing personal photos via social networks; 36.3% of the participating adolescents confirmed that they have met a ‘cyber friend’ with whom they communicate regularly.

Nearly half (42.2%) confirmed that they have been approached by somebody for ‘something upsetting’. These results confirm substantial exposure of adolescents to potential dangers through their engagement in social networking sites. Research conducted by the Film and Publication Board [17], identified that in most cases upsetting content mostly involves sexual content or nudity and causes great discomfort and distress amongst children.

It has been found that sexual perpetrators are likely to focus on social networking sites, which have become very popular amongst the youth. On social networking sites, children may be approached and groomed, and a slight slip of the mouse or keyboard may give a potential perpetrator all they need to know about a specific child. The explosion of Facebook in South Africa therefore has the potential for opening up a new access point to South African children for sexual perpetrators. A relatively small percentage of participating adolescents (15.4%) in the exploratory research study indicated that they share personal information on the Internet.

Mobile social networks have also attracted much attention in South Africa. The mobile social network MXit, which was developed in South Africa, is allegedly increasingly becoming even more popular than other computer – based social networks such as Facebook and MySpace. Responses received from adolescents participating in the exploratory research study to MXit were extremely positive, with 90.2% affirming awareness and 81.4% affirming usage of MXit. The average time (minutes) spent on MXit per day is reported in Figure 2.

The majority of adolescents (27.1%) spend, on average, between 30 minutes to an hour on MXit per day. It is noteworthy that 22.3% of the participants indicated that they spend between one and two hours per day on MXit. An additional 16.9% of adolescents indicated that they spend more than 121 minutes per day on this new communication medium.

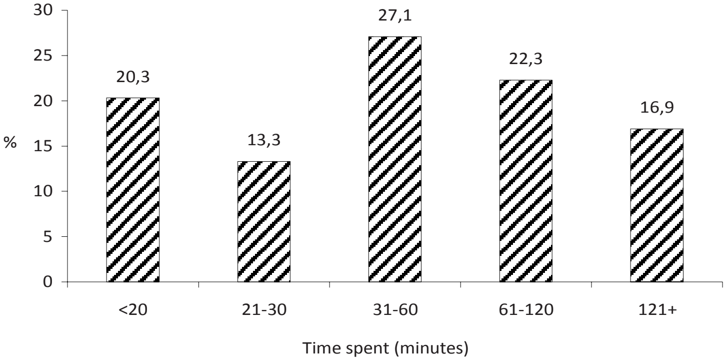


Fig. 2. Average daily time spent (in minutes) on MXit by time category

The exploratory research study explored with whom adolescents spend this communication time. For the study four pre-determined categories of people were identified. These included family, friends, boyfriend/girlfriend not met through cellphone/Internet, and boyfriend/girlfriend met through cellphone/Internet. Participants were able to mention an average of almost 50 friends as MXit contacts. On average, just under 10 contacts were listed for both boyfriend/girlfriend met or *not met* through cellphone contact and the Internet.

It is clear from Figure 3 that communicating with friends takes the bulk of time spent (almost an average of 68 minutes) on MXit per day. Compared to this, participants spend an average of 17 minutes per day communicating with family members (mom, dad and siblings) via MXit. It is noteworthy that nearly 49 minutes per day are spent on communicating with a boyfriend/girlfriend met via the cellphone or Internet; this emphasises the importance of networking among adolescents.

Based on the research results, it is clear that adolescents contact a large number of people via MXit, but also that interpersonal communication on a daily basis via this new medium has become a standard feature of their lives. This method of text communication is not only used for interpersonal communication, but also for entertainment, making appointments/dates and obtaining help with homework. To make appointments/dates is by far the most important additional use of this new medium. MXit is seen as an instant messaging service used widely by adolescents and it is regarded as a major player in the communication bouquet of the youth.

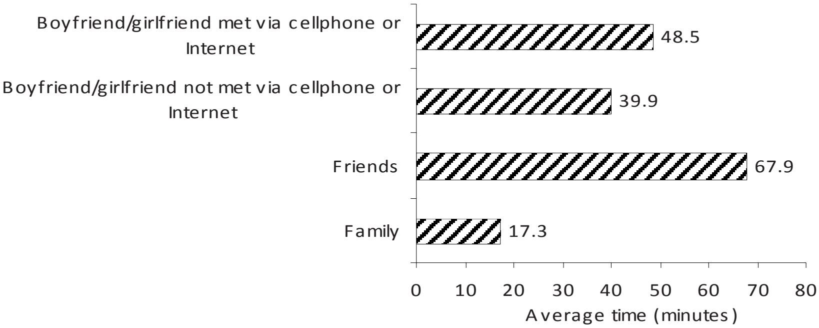


Fig. 3. Average time (in minutes) spent with different individuals

Similar to web-social networking sites, MXit clearly open ways for exploitation. The South African media often report on young people who have suffered abuse through participation on MXit.

3.3 Weblogs

The exploratory research study, in brief, explored the access of adolescents to blogs. Since all blogs are on the Internet by definition, they may be seen as interconnected and socially networked. Almost one in five adolescents (17.1%) who participated in the exploratory research study has their own weblog where they provide commentary or news on a particular subject. Many indicated that they are not familiar with setting up a Weblog or simply do not have the time to provide commentary or share news on a Weblog.

4 Concluding Insights

The exploratory research study investigated the rate of diffusion of *new media* among adolescents and the extent to which new media innovations have been adopted among South African adolescents. In contextualizing the research findings of the exploratory research study in relation to identified international research findings, the following is noteworthy:

- New media have certainly diffused at a high rate among South African adolescents in particular who are anticipated to continue to adopt new innovative media developments at a faster pace than adults. Increasing access to and enthusiastic usage of the new media by adolescents proves that not only are they the innovators in this area, but they are also changing their life styles to adapt to the new media and to use them to their own benefit.
- Socio-economic factors need to be considered when investigating new media trends among the youth.
- The exploratory research study revealed that new media also have psychological/emotional dimensions and are not merely communication media.

Against the backdrop of the relatively low penetration of the Internet in South African society, the finding in this exploratory research study that more than 85 % of the respondents had access to the Internet during the period under investigation is significant. Also significant in this regard is the fact that approximately half the participating adolescents accessed the Internet via their cellphones. Interpersonal communication via the Internet is, as with cellphones, a very important mode of communication to inform and educate the youth in general.

The Internet is used to make new friends, to join ‘chat groups’, to exchange private messages - all activities that are part of adolescent development. In addition to using the Internet to obtain information, interpersonal communication seems to be the main objective in using the system. This coincides with the trends identified by [14] and [18], which point to a shift from using the new media mainly as a source of information for study and research at school, to using it as an interpersonal communication tool.

As mentioned, MXit is a South African developed instant messaging system using cellphones and the Internet, largely used by adolescents. In the exploratory research study, most respondents had access to MXit. The fact that almost 40 % of adolescents spend more than an hour per day on this low cost text messaging system, emphasises the importance of the system in helping adolescents psychologically through an emotionally challenging phase in their development.

This exploratory research study that included five secondary schools is limited in nature but provided worthwhile and interesting insights into *new media*, in the lives of adolescents. The importance of the *new media* is beyond contention. These media will have an escalating impact on the lives of adolescents in South Africa, as well as on the information and communication industry. The most concerning aspect, however, is the adequate protection of children who are able to access the Internet and social networking sites. The more adolescents have access, the more young people will be at risk of receiving inappropriate material, as well as exposure to sexual exploitation. Increased awareness and adequate measures need to be initiated for children to enjoy social networks and to be protected from potentially harmful exposure and experiences.

5 Future Research

The research study will be broadened across South Africa with the specific aim of investigating new media usage and the digital divide between different socio-economic settings. An in-depth qualitative study will be conducted in June 2009 further exploring some of the issues raised during the exploratory phase.

References

1. Van Vuuren, D.P.: Die SAUK se televisiedienste, in Televisie – skyn en werklikheid. Die omstrede medium, onder redaksie van JB du Toit. Tafelberg, Kaapstad (2004a)
2. Intoweb Marketing. Internet history. eTrafic (2007), `http://www.intowebmarketing.co.za`

3. Internet World Stats (2007), `http://www.internetworldstats.com` (accessed 24 March 2009)
4. Kelly, T.: Africa joins the Internet age. The African Internet and Telecom summit. Banjul, The Gambia, June 5-9 (2000)
5. World Wide Worx. 2008. South Africa: Internet usage and marketing report, December 29 (2008), `http://www.worldwideworx.com`
6. Thomas, R.: Facebook vs MySpace: The debate keeps moving ahead. Social Networking, 2 July (2007)
7. Thomas, R.: Worms attack facebook – MySpace users running Microsoft Wondows. Social Networking, 100, August 8 (2008a)
8. Lingham, V.: Facebook hits the #1 spot in South Africa. Synthasite (October 30, 2007)
9. Search engine people [sa]. Mobile web development,
`http://www.intoweb.co.za/articles-mobile-web-dev.html`
(Consulted: 19 March 2009)
10. Intoweb [sa]. Mobile web development,
`http://www.intoweb.co.za/articles-mobile-web-dev.html`
(Consulted: 19 March 2009)
11. Fox, J.: You're Among Friends: College favorite Facebook begins to conquer social networking's final frontier-grownups. Time, 39, July 16 (2007)
12. Reece, C.: Facebook fever grips SA. Nes 24, June 14 (2007)
13. Lenhart, A., Madden, M., Hilton, P.: Teens and technology: Youth are leading the transition to a fully wired and mobile nation. Pew Internet & American Life Project, Washington (2005)
14. Livingstone, S.: Mediated childhoods: A comparative approach to young people's changing media environment in Europe. European Journal of Communication 13(4), 435–456 (1998)
15. Van der Voort, T.H.A., Beentjes, J.W.J., Bovill, M., Gaskell, C., Koolstra, C.M., Livingstone, S., Marseille, N.: Young people's ownership and usage of new and old forms of media in Britain and the Netherlands. Journal of Communication 13(4), 457–477 (1998)
16. SAARF, see South African Advertising Research Foundation
17. Chetty, I., Basson, A.: Exposure of children to sexually explicit content through the Internet and Cellphones. Film and Publication Board Research Report, Houghton (2008)
18. Broddason, T.: Youth and new media in the new millennium. Nordicom Review 2, 105–118 (2006)

Combining Immersive Virtual Worlds and Virtual Learning Environments into an Integrated System for Hosting and Supporting Virtual Conferences

Nikolaos Polychronis, Charalampos Patrikakis, and Athanasios Voulodimos

National Technical University of Athens
nikos.polychronis@gmail.com,
bpatr@telecom.ntua.gr,
thanos@telecom.ntua.gr

Abstract. In this paper, a proposal for hosting and supporting virtual conferences based on the use of state of the art web technologies and computer mediated education software is presented. The proposed system consists of a virtual conference venue hosted in Second Life platform, targeted at hosting synchronous conference sessions, and of a web space created with the use of the e-learning platform Moodle, targeted at serving the needs of asynchronous communication, as well as user and content management. The use of Sloodle (the next generation of Moodle software incorporating virtual world supporting capabilities), which up to now has been used only in traditional education, enables the combination of the virtual conference venue and the conference supporting site into an integrated system that allows for the conduction of successful and cost-effective virtual conferences.

Keywords: Virtual conference, on-line conference, sloodle, moodle, Second Life, immersive virtual world, multi user virtual environment, virtual learning environment, content management system.

1 Introduction

Virtual or on-line conferences are professional educational events that, compared to their face to face counterparts, are considered to be cost-effective, for both organizers and participants, time and space independent, thus convenient to attend and widely accessible. Furthermore, virtual conferences, being completely reliant on technology, usually keep up with most recent technological advancements, taking full advantage of the new possibilities for interaction and knowledge building that open up, when effectively applying up-to-date technology to conference procedures. During the last few years, a wide range of powerful communication tools and applications have emerged, alongside with the rapid increase in broadband connections, the prevalence of Internet and the emergence of Web 2.0. However, these advances have not yet been fully integrated into conference planning and conduction. Careful choice of technology and exploitation of the nowadays available infrastructures and web tools for use with the

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 397–407, 2010.

virtual conference may result in planning and conducting on-line conferences that are more effective in terms of creative interaction and social networking among the participants and yet quite inexpensive and less time consuming to organize and attend.

2 The Virtual Conference

2.1 Definitions and Features

Conferences, in general, are considered to be spaces of academic dialogue alongside journals and books, designed to meet the ongoing educational and training needs of professionals [1]. Either in person or virtual, conferences have to accomplish some major goals. The first goal is to create knowledge through personal, organizational and community learning. The second goal is to develop social networks that can be later used to extend learning beyond the conference and to create valued collegial friendships and relationships [2]. According to Anderson, organizer of the first international online conference to be held, the virtual conference is a professional development activity, modeled upon the face to face professional conference that uses telecommunication technologies to reduce the access barriers to participation posed by time and distance [3]. Like its face to face counterpart, the virtual conference runs on a real-time schedule, with a starting date and a closing time. However, unlike the traditional conference the online event is not tied to a specific geographical location, does not require the participants' physical presence, includes numerous opportunities for interaction with fellow participants, presenters, keynoters and conference hosts and staff, is archivable (discussions in various media can be recorded for future review), and isn't - for the most part - time bound (presentations and forums are available at any time, virtually, whenever the participant logs on) [4].

The format of the virtual conference consists of planned learning activities which may take place synchronously, with all participants interacting at the same time, asynchronously, with interaction supported 24 hours a day, or through some combination of asynchronous and synchronous activities [3]. Asynchronous interaction provides freedom of time (learners are able to participate when, and if, they choose to do so), time for reflection, opportunities for research and opportunities for global communication (no concern for time zones). Synchronous communication provides immediate feedback, as well as rapid problem solving and decision making [5].

2.2 History and Technology

Early on-line conferences were entirely e-mail based because of bandwidth and software limitations. At that time e-mail was the lowest common denominator among internet tools, offering higher access rates, compared to newer, high bandwidth or increased interactivity tools and reaching many of the most remote regions, including some with very low levels of telecommunications infrastructure [3]. The first international online conference to be reported was organized by the International Council for Distance Education (ICDE) in 1992 [6]. For the needs of this conference a central mail distribution list was established at the University Of Calgary in Canada, receiving all the incoming mail and feeding outgoing mail to approximately twenty-five different networks or mail discussion lists for further distribution. The rapid development of computer network technology has since offered online conferences a larger pool of delivery tools. For instance the ICDE 95 online conference used MOOs (Multi-User Dimensions/Dungeons Object Oriented) to provide participants real time interaction. Later conferences included real time audio, video broadcasting and made use of the World Wide Web [7].

Nowadays a wide range of software tools is available, suitable to support the virtual conference, not only in terms of communication and delivery of content, but also as far as content management, user management and creation of social networks is concerned. This range of tools involves from complex commercial products, directly developed for web-conferencing, like Elluminate, content -learning management systems (CMS-LMS) like Moodle, originally developed to enhance traditional education, immersive virtual worlds like Second Life or WOW, social networking Software like Facebook or Flickr and social bookmarking tools, like del.icio.us, to nowadays widely spread Internet tools and technologies like blogs, wikis, podcasts etc. that have turned the web into what it is today.

Technological progress and the emergence of new powerful tools has deeply affected the overall conference format and structure over the years, introducing new ways of interaction, enabling the deployment of more complex activities and adding functionality. While early applications of virtual conferences imitated face to face conferences, it was soon realized that this was "horseless carriage" approach that should be replaced by an approach that ensures understanding and application of technology in ways that optimize its unique strengths and virtues [3].

3 Choosing Technology for Hosting and Supporting Virtual Conferences

3.1 Criteria and Modern Aspects about Technology Use for Conference Conduction

When choosing technology for hosting and supporting virtual conferences, cost effectiveness, time flexibility and remote accessibility are three major factors that should be taken into consideration, because, after all, those are the initial reasons, for which virtual conferences where originally developed. Apart from the above mentioned criteria, the great impact technology and modern software tools can have on the educational and communication - socialization processes when wisely utilized, seems to be the key factor when choosing among the plethora of software tools and network infrastructures available today. Siemens, Tittenberger, and Anderson [1] claim that although planning technology use in conferences is currently in a state of a flux, greater utilization of technology in conferences provides value for extending activities and dialogue, capturing content, supporting conversations, encouraging social networking, enable tagging, fostering backchannel communication and aggregating content. Suter, Alexander and Kaplan [8] insist especially on the ability of new social software technologies to provide a "container" for persistent conversation and also support what might be thought of as the social architecture of a community (of professionals). Finally, the adaptability of the selected software to various needs and specifications, its scalability and its ability to evolve and keep up with emerging technologies and also the ease of use for the end user, seem to be equally critical concepts to be accounted for. Of course previous experience in organizing virtual conferences should be investigated, best practices ought to be taken into account, and any proposed solution should lie close to the mean technical level of its time.

3.2 Technology Review

The combined use of various technologies for supporting different aspects and activities of the same event can be spotted at many contemporary virtual conference events. Usually a software package, or a set of tools, is used for supporting synchronous sessions and live presentations, and a second technology, or a combination of technologies, for supporting the asynchronous activities, registration process etc. Among commercial products, Elluminate[1] (www.elluminate.com) seems to be one of the most common choices, for holding live sessions and presentations, while streaming technologies like podcast are often favored for the delivery of live or recorded audiovisual content. Asynchronous interaction among the participants usually takes place on forum boards, blogs and wikis, while RSS feeds, tagging and bookmarking enhance the participants' experience, enable the aggregation of content and add value to asynchronous conference activities. The use of software packages, like Moodle[2] (www.moodle.com), for supporting a whole range of asynchronous activities, and, at the same time, managing users and safely storing and distributing content (especially documents), through an integrated environment, is also a common practice in contemporary virtual conference conduction.

What may be worth highlighting, is the use of the Multi User Virtual Environment (MUVE) of Second Life (www.secondlife.com) for hosting standalone immersive context sessions or even conferences. At least two cases are being reported:

a) The NMC Series of Online Symposia, held on the New Media Consortium (NMC) Second Life campus, and

b) the IBM's Academy of Technology (AoT) Virtual World Conference and 2008 Annual Meeting, hosted in a secure Second Life environment, with a conference space specially designed by IBM for keynotes, breakout sessions, a simulated Green Data Center, a library, and various areas for community gathering. The experience of participating in a virtual conference in Second Life was highly acclaimed by the IBM's AoT members, especially because of the intense feeling of telepresence the immersive environment of Second Life imparted to them, while cost was reduced to about one fifth [9].

[1] Elluminate, for instance, is used by Webheads in Action Online Convergence (http://wiaoc.org/), Online Connectivism Conference (http://umanitoba.ca/learning_technologies/connectivisim) and the Future of Education (http://umanitoba.ca/learning_technologies/conferences/foe/), K-12 Online Conference (http://k12onlineconference.org/)

[2] Moodle, for instance, is used by Online Connectivism Conference (http://umanitoba.ca/learning_technologies/connectivisim) and the Future of Education (http://umanitoba.ca/learning_technologies/conferences/foe/)

3.3 Assessing Previous Experience and Choosing Technology

Computer mediated asynchronous discussion has proven to be a vital element of most virtual conferences, because it is persistent, it allows participation even after the conference event has finished, it is deeper than real-time discussion, allowing participants to reflect and research before they respond, it is archivable and retrievable and thus accessible to a larger audience, and also time-convenient and space – independent. Live discussion is important for a conference as well, because of its spontaneity and immediacy, allowing for group cohesion and synergy and for creating personal bonds between participants. In that context, the use of virtual worlds, and particularly Second Life, for hosting on-line conferences, making on-line interaction feel like real, seems quite promising, especially after IBM AoT's successful experiment.

Any planning for technology use in conference conduction, taking into consideration previous experience and best practices, should therefore definitely account for forums, blogs and wikis to host asynchronous discussion and should seriously consider utilizing the immersive environment of Second Life for hosting live "feeling like real" meetings. Moreover, it would be ideal if those different technologies supporting the various desirable activities and features of the virtual conference could be, not simply combined, but integrated into a unique and cohesive system: the Sloodle project, reviewed on the next paragraphs, is a software package that attempts that kind of an integration.

4 Sloodle

4.1 Overview and Architecture

SLOODLE (Simulation Linked Object Oriented Distance Learning Environment) is a free plug-in for the popular Open Source web-based virtual learning environment "Moodle", which integrates Moodle and Second Life [10]. Sloodle is open source itself and comprises a large collection of php scripts residing on a Web-server with a database backend [11] and a set of Second Life objects-'tools' compiled in LSL (Linden Script Language), Second Life's built in scripting language. Sloodle is not standalone software but is normally mounted as a module on an existing Moodle installation. Sloodle objects in Second Life communicate with Moodle servers bearing the Sloodle module via e-mail, XML remote procedure calls (XML-RPC), and via HTTP-requests.

4.2 The Sloodle Project

Sloodle software, which is undergoing constant revisions and improvements, is part of an ongoing and growing in popularity and support education-oriented project, initiated at about 2006 by Daniel Livingstone and Jeremy Kemp, trying to investigate how current games technology can help build more immersive and engaging learning environments and on the same time trying to avoid packaging learning content into game form [12]. At that time, there was a rapid growth of interest to be observed, in the use of online virtual worlds, and particularly Second Life, for educational purposes, while powerful features, already existing in learning management systems like Moodle, were not generally used to their fullest. Sloodle creators noticed that each platform (SL and Moodle) offers complementary affordances not available in the other and that connecting the two systems might allow instructional developers and teachers to explore exciting new opportunities for interaction on the web and within the Second Life MUVE [13].

The most important qualities of Sloodle are its dynamics and its constant evolution. Sloodle developers continuously try to improve its form and attributes by exploiting new affordances by emerging technologies, conducting surveys to find out what educators want [11] and receiving constant feedback from a rapidly growing community of Sloodle testers, users, and developers [14].

4.3 Features

At the prospect of introducing Sloodle to virtual conferences, next paragraphs review some of the in-world educational tools and registration/enrolment objects included in Sloodle, which according to the authors' opinion, may prove useful for supporting and enhancing virtual conferences.

Sloodle WebIntercom mirrors chat between Second Life and Moodle, allowing attendants to participate in chats from either environment, and it also archives Second Life chat on the Moodle server [14]. WebIntercom only applies to Second Life's Local Chat with script messages.

Sloodle Toolbar is a Second Life user-interface enhancement, a toolbar that enables blogging to a user's Moodle profile, adds animated classroom gestures to Second Life, and which allows a user to query Moodle for the Moodle identities (if any) of avatars nearby in the 3D virtual space.

Registration Booth checks if avatars are registered in the corresponding Moodle site, and, if not, it helps them register while the *Access Checker Door* controls access to a certain confined space within Second Life.

Vending Machine allows web-controlled and in-world distribution of objects.

Sloodle Presenter is a tool for creating presentations (for lecture, seminar or self-paced tutorial use) in Second Life. The presenter avoids the requirement to upload images into Second Life and allows presentations to combine images, web-pages and videos by streaming the presentation content into Second Life using the media settings. Thus, each slide can either be a webpage or an image or even a video (in Quicktime compatible format) [15]. On the latest versions of Sloodle YouTube support is also available while pdf support is expected to be included in future releases. The development of the *presenter* was based on the HTML On A Prim technology, which was only recently introduced to Second Life, and has been a real revolution, not only because of saving former costs of uploading images on the Second Life servers, but also because it enables new media format to be fed to Second Life.

Sloodle Choice lets participants respond to a poll set up in Moodle (Moodle's *choice activity*) from in-world.

5 Developing a System for Hosting and Supporting a Virtual Conference Based on Sloodle Technology

5.1 The Core Concept

Both Second Life and Moodle feature compelling functions and attributes for the virtual conference organizer, as indicated in section 3.3, and both platforms have been so far used for supporting virtual conferences, as mentioned in section 3.2, but no report of them being used together for the same event has been tracked yet. Sloodle is a software package that enables the integration of Second Life and Moodle into a cohesive, enhanced Virtual Learning Environment, thus it would only sound reasonable to examine the possibility of using Sloodle to integrate both platforms into a complex system for hosting and supporting virtual conferences.

Sloodle has originally been developed for supporting teaching and learning “in the virtual classroom”, aiming at a centralized educational structure, which typically involves a teacher or professor and his or her students, a structure usually met at schools, colleges and universities. Reports from using Sloodle in the virtual classroom have been quite encouraging so far, but no other use of Sloodle outside this context has been reported yet. Conferences constitute educational processes too, but unlike teaching in a classroom, they are based on a decentralized educational structure, where importance lies on collaborative learning and knowledge building and where crucial ideas might be born even during unofficial conversations on the margin of the official event, so conferences may not be what Sloodle creators have originally been aiming at. Nevertheless, conferences do involve activities, a presentation being a typical example, which simulate the teacher–students educational schema; furthermore, the point of teaching inside the virtual classroom, instead of the real one, lies exactly in fostering situated learning, where collaboration, exploration, and construction are important, and transform - decentralize the conventional educational process. Therefore learning in the virtual classroom may not be so different from learning in a conference after all.

Taking into consideration all the aforementioned factors, namely: a) the positive reports about testing Sloodle in the virtual classroom b) the similarities between the virtual classroom and the on-line conference and c) Sloodle’s overall compelling features, it is hereby claimed that *transferring Sloodle technology from the virtual classroom to the conference venue would positively affect and enhance conferences as well and would give virtual conferences a qualitative boost*. A way to implement this transfer is described next.

5.2 Implementation

Sloodle is not a standalone application; it presupposes the use of Second Life and Moodle. Using Sloodle to conduct and support on-line conferences means setting up a system comprising two parts: a web site created with Moodle and some kind of virtual facilities hosted in Second Life, allocating conference activities and supportive functions among the two parts, and finally setting up and configuring Sloodle to interconnect the two parts. An optimal way to do this is hereby suggested, that consists of creating a virtual conference venue in Second Life to host all synchronous activities and a Moodle site to host asynchronous activities, manage registrations and store conference content. Further functionality is achieved by setting up and using the WebIntercom, the Presenter, the Access Checker Door, the Registration Booth, the Sloodle Toolbar and, finally, the Sloodle Choice features described in section 4.3. The following detailed description of the end-system is partially based on a small scale prototype [16] formerly developed for testing purposes. Some screenshots of the prototype implementation are presented later in the paper.

The Virtual Conference Venue

The Virtual Conference Venue is a properly shaped and designed - according to given requirements and specifications- virtual building intended to host live events. A Sloodle Access Checker Door controls the access into the building: only users, who have signed up at the Moodle site and have registered their avatar, are allowed to enter. A Registration Booth outside the building facilitates the registration process for the newcomers. Inside the venue a Vending Machine hands out the Sloodle Toolbar to all users. The Sloodle Toolbar allows for reflection during live conference sessions; participants can take notes during a presentation or discussion and send comments to their personal blog, that can be reviewed later for further investigation or discussion. All synchronous discussions and presentations are hosted in the virtual venue using voice or text. Text based sessions are recorded by Sloodle WebIntercom and automatically saved on the Moodle site for later review. Sessions using voice are recorded using third-party software and manually saved on the web server. In case some attendants cannot log in to Second life due to technical reasons, text is preferred over voice, so that they can join the conversation through the browser based Moodle chat room. Presentations are held on the Sloodle Presenter, allowing both images and videos to be displayed. Sloodle Choice objects, correctly positioned inside or outside the venue, allow organizers/presenters to receive immediate feedback, right after the conference/presentation, on the participants' opinion.

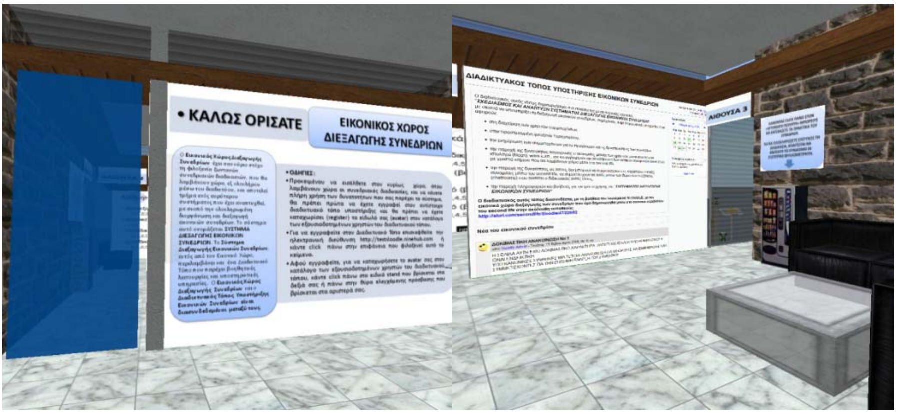

• ΚΑΛΩΣ ΟΡΙΣΑΤΕ
ΕΙΚΟΝΙΚΟΣ ΧΩΡΟΣ ΔΙΕΞΑΓΩΓΗΣ ΣΥΝΕΔΡΙΩΝ
ΔΙΑΔΙΚΤΥΑΚΟΣ ΤΟΠΟΣ ΥΠΟΣΤΗΡΙΞΗΣ ΕΙΚΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ
ΑΙΘΟΥΣΑ 3

Fig. 1. Outside and inside the virtual conference venue's reception room. Outside: Sloodle Access Checker Door controls access into the venue. Inside : Vending Machine links to conference proceedings on the Moodle site, the wall displays Moodle site's frontpage including calendar. [16]

The Moodle Site

The Moodle Site handles registration to the conference through its built-in login interface. Conference events are registered in the built-in calendar and announced on the central page forum board. Various other forum boards may be created for hosting scientific discussion on different conference topics. Content like conference proceedings, individual presentations and live session recordings are stored on the server and distributed to registered users. Through the built-in chat rooms users can join text-based conversation taking place in the Virtual Venue or selectively retrieve past, automatically archived, text-based sessions. Additional web pages inside the site may provide user with useful information and instructions, about how to use the system etc. If desired, content and activities appearing on the Moodle site may be organized into different *Courses* for increasing functionality, though this is up to the organizers' discretion.

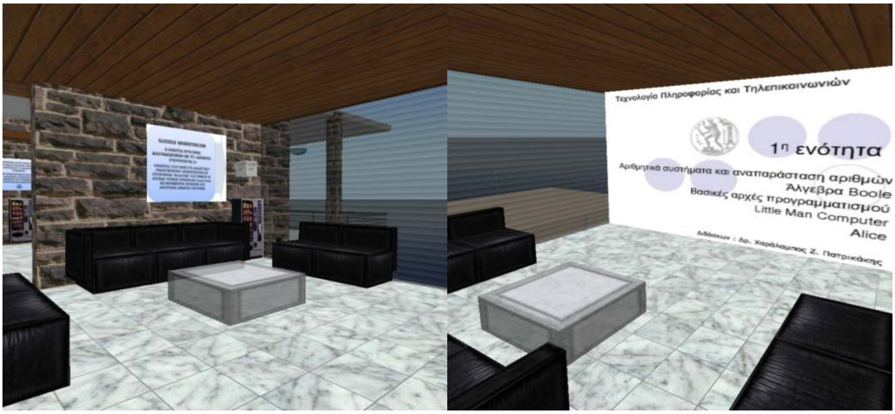

Τεχνολογία Πληροφορίας και Τηλεπικοινωνιών
1η ενότητα
Αριθμητικά συστήματα και αναπαράσταση αριθμών
Άλγεβρα Boole
Βασικές αρχές προγραμματισμού
Little Man Computer
Alice
Διδάσκων : Δρ. Χαράλαμπος Ζ. Πατρικάκης

Fig. 2. Double aspect of a conferencing room inside the virtual conference venue, featuring seats, a presentation screen, Sloodle Webintercom, and a Vending Machine for linking to document repositories [16]

6 Conclusions

Combining two technologies, Moodle and Second Life, formerly only separately used for supporting virtual conferences, and integrating them with the use of Sloodle, so far used for supporting only traditional teaching, into a complex, standalone system, is expected to take on-line conference conduction to a next level.

The proposed system features Second Life's immersive environment, making remote participants feel as if they are really there, and Moodle's wide range of asynchronous communication tools, allowing for a deep, long-lasting and persistent conversation among the experts, plus Moodle's powerful user and content management functions, needed for registering participants, distributing the proceedings, controlling access to resources and activities. Utilization of Sloodle offers additional possibilities for reflection during the live sessions, facilitates direct assessment by the participants, makes recording and archiving live sessions easier, extends access control to the virtual level and allows for richer, cost-effective presentations.

Furthermore, the whole system can be easily built up to meet individual needs and specifications, as both Second Life and Moodle offer great flexibility and adaptivity. Second Life content is exclusively user created, while Moodle, apart from being fully customizable, is open source, which allows for even deeper changes to be implemented.

The overall suggested solution is cost-effective. Sloodle and Moodle software is free, web hosting for small scale deployments is free, while, for any potential large scale virtual conference organizer, saving some space and bandwidth on the corporate or institutional servers shouldn't do any difference. The only costs associated with undertaking such a project, lie in buying land on Second Life, costs which are still far lower than the costs of organizing the real event, while temporary free hosting of small scale creations is also possible.

The most intriguing and compelling part about the technologies chosen is their dynamics. Both Moodle and Sloodle, being open source, are actively supported by a large community of users and developers and therefore are constantly evolving and improving. Permanent feedback from software users helps tracking defects and adjusting software more and more to end users' needs, while emerging technologies are quickly embraced by developers and, when possible, integrated into the software, making the best out of it. Especially, as far as Sloodle is concerned, its constantly growing community of supporters and the fact that the release of new versions bearing brand new features increases in frequency, indicates that there is still a lot to expect and that only difficultly will this piece of software be outdated.

References

1. Siemens, G., Tittenberger, P., Anderson, T.: Conference Connections: Rewiring the Circuit. EDUCAUSE Review 43(2) (2008)
2. Anderson, T.D.: Online Conferences For Professional Development. In: Vrasidas, C., Glass, G.V. (eds.) Online Professional Development for Teachers, pp. 13–29. Information Age Publishing (2004)
3. Anderson, T.D.: The Virtual Conference: Extending Professional Education In Cyberspace. International Journal of Educational Telecommunications 2(2/3), 121–135 (1996)
4. Shimabukuro, J.: What is an Online Conference? The Technology Source (2000)
5. Wilkinson, K.L., Hemby, V.K.: An Examination of Perceptions of the Use of Virtual Conferences in Organizations: The Organizational Systems Research Association (OSRA) and The Association for Business Communication (ABC) Members Speak Out. Information Technology, Learning, and Performance Journal 18(2), 13–23 (2000)
6. Anderson, T., Mason, R.: International Computer Conferencing for Professional Development: The Bangkok Project. American Journal of Distance Education 7(2), 5–18 (1993)
7. Wang, Y.-M.: Online conference: A participant's perspective. T.H.E. Journal 26(8), 70–76 (1999)
8. Suter, V., Alexander, B., Kaplan, P.: Social Software And The Future Of Conferences Right Now. EDUCAUSE Review 40(1), 46–59 (2005)
9. SECOND LIFE GRID, Linden Lab: How Meeting In Second Life Transformed IBM's Technology Elite Into Virtual World Believers, `http://secondlifegrid.net.s3.amazonaws.com/docs/Second_Life_Case_IBM.pdf`

10. Summary: What is SLOODLE?, `http://www.sloodle.org/moodle/file.php/1/UsingSLOODLECheatSheet1.pdf`
11. Livingstone, D., Kemp, J.: Integrating Web-Based and 3D Learning Environments: Second Life Meets Moodle. UPGRADE, European Journal for the Informatics Professional IX(3), 8–14 (2008)
12. Livingstone, D., Kemp, J.: Massively Multi-Learner: Recent Advances in 3D Social Environments. Computing and Information Systems Journal 10(2) (2006)
13. Kemp, J., Livingstone, D.: Putting a Second Life "Metaverse" Skin on Learning Management Systems. In: Second Life Education Workshop at the Second Life Community Convention, pp. 13–18. The University of Paisley, San Francisco (2006)
14. Livingstone, D., Kemp, J., Edgar, E.: From Multi-User Virtual Environment to 3D Virtual Learning Environment. ALT-J, Research in Learning Technology 16(3), 139–150 (2008)
15. SloodleUserDocs (Sloodle wiki, User Documentation), `http://slisweb.sjsu.edu/sl/index.php/SloodleUserDocs`
16. Polychronis, N.K.: Design And Development Of A System For Virtual Conference Conduction. PG Thesis, Athens (2009)

Session 10

Pervasive, Ubiquitous, and Intelligent Computing

Social Network Analysis and Its Applications in Wireless Sensor and Vehicular Networks

Alexis Papadimitriou[1], Dimitrios Katsaros[2], and Yannis Manolopoulos[1]

[1] Department of Informatics, Aristotle University of Thessaloniki
54124 Thessaloniki, Greece
papajim@delab.csd.auth.gr, manolopo@delab.csd.auth.gr
[2] Dept. of Computer & Communication Engineering, University of Thessaly
38221 Volos, Greece
dkatsar@inf.uth.gr

Abstract. Ever since the introduction of wireless sensor networks in the research and development agenda, the corresponding community has been eager to harness the endless possibilities that this new technology has to offer. These micro sensor nodes, whose capabilities have skyrocketed over the last couple of years, have allowed for a wide range of applications to be created; applications that not so long ago would seem impossible, impractical and time-consuming. It would only be logical to expect that researchers from other fields would take an interest in sensor networks, hence expanding the already wide variety of algorithms, theoretical proofs and applications that existed beforehand. Social Network Analysis is one such field, which has instigated a paradigm shift in the way we view sensor nodes.

In this paper, we will present the contribution of Social Network Analysis to sensor networks in terms of theory, algorithms and applications.

Keywords: Social network, sensors, centrality, vehicular networks, topology control.

1 Introduction

In computer science and telecommunications, wireless sensor networks are an active research area. These networks consist of spatially distributed autonomous micro devices, the sensor nodes, which can be programmed to monitor a wide range of chemical, environmental and physical phenomena, such as temperature, vibration, sound, conciseness and object location. Due to their versatility, sensor networks have many applications; usually they involve some kind of monitoring, controlling or tracking. Specifically, there are some industrial areas where sensor networks seem to have had the biggest impact. First of all, they are being used in habitat monitoring, whether that concerns the prevention of fires, observation of groups of animals, monitoring of underwater currents and underground phenomena such as earthquakes. The two most prominent and useful in everyday life areas though, include traffic monitoring and health care. As far as traffic monitoring is concerned, they can be used to alleviate the traffic problems that many cities seem to be facing nowadays, by preventing traffic

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 411–420, 2010.

jams and, in conjunction with a GPS device, offering alternative routes. In health care, sensor networks can be used to monitor patients and assist handicapped people either in hospitals or even in their own homes. A sensor network example and an actual sensor node are illustrated in Figure 1.

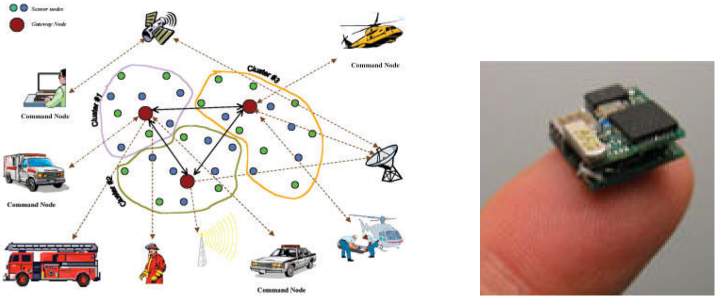


Fig. 1. Sensor networks applications and the Eco sensor node

The characteristics of wireless sensor networks include limited power of the sensor nodes, susceptibility to node failures, node mobility, large scale deployment, dynamic network topology. Depending on the actual application that the sensor network is implemented for, the network administrator needs to evaluate the precedence that each characteristic will have over the others.

As far as the research areas of sensor networks that have been studied over years, these include but are not limited to topology control, cooperative caching, vehicular networks and lately social network analysis. Topology control refers to the concept of trying to maintain network connectivity under certain circumstances. An example would be for the nodes to adjust their transmission power in order to preserve energy. Cooperative caching as a research area was raised as a way to deal with the challenging task of application-level QoS. Since communication cost is almost three times as much as processing cost, we try to reduce communication as much as possible by sharing data between sensors, coordinating cache data and exploiting the aggregate cache space of cooperating sensors. Finally, in vehicular networks, we combine vehicles, used as sensors, and wireless local area network technologies in order to prevent or warn about nearby accidents, advise over traffic jams or inform about vacant parking spots.

As it was mentioned earlier, there is one more research area which has gained more interest lately in the community and was found to have similarities with sensor networks. In social network analysis, social structures are formed, where the nodes are usually represented by individuals or organizations and the links between these nodes are represented by the relationships that exist between these entities. Because of the similarities between them, sensor and social networks can interface both ways. For example, sensor networks can sense and provide information to personalized social applications and social networks analysis can supply algorithms and techniques which can lead to energy saving and efficient storage in sensor networks depending each time on the application being executed.

In this paper, we address the contribution of social network analysis in sensor networks in terms of algorithms and applications. In section 2, the reader will be provided with a more detailed insight in social networks. We will present some of the social network analysis concepts, such as the metrics that are being used in social network analysis and how these affect the design of protocols in sensor networks. In section 3 the previous protocols will be presented along with their corresponding applications so we can assess the impact of social network analysis on sensor networks on a more practical level. In section 4, the paper will provide some of the related work that was already done on the combination of the two areas.

2 Social Network Analysis

Social network analysis [SNA] studies the relationships between people, groups, and other similar entities. Social network analysis views social relationships in terms of *nodes* and *ties*. Nodes are the individual actors within the networks, and ties are the relationships between the actors. There can be many kinds of ties between the nodes. There is a wide variety of applications in sensor networks where the need to identify important components is of great importance. Centrality is a term used to denote such an importance of a node inside a network. There are various measures of centrality and the most prominent of them are going to be presented in the following section.

2.1 Centrality Metrics

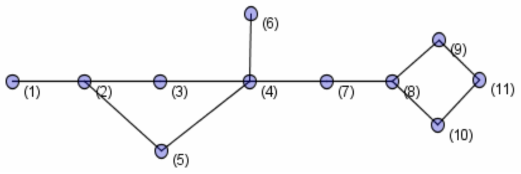
In this section we briefly describe the most important centrality metrics that the sensor network research community has focused on.

Degree centrality (DC). The simplest centrality metric is degree centrality and refers to the number of direct connections a node has to its neighbors. A common misconception is that the more connections the better, but this is not always the case. An important factor is where those connections lead to and how they connect the otherwise unconnected nodes. In Figure 2, node 4 has the highest degree.

Betweenness centrality (BC). Another centrality measure is betweenness. Betweenness assesses the number of shortest paths passing through a given node or edge. A node with high betweenness centrality is more likely to be located on the shortest paths between multiple node pairs in the network and therefore more information needs to be passed through it. Moreover a node with high betweenness centrality plays a crucial role in the connectivity of the network. Node 4 again has the highest rank in betweenness centrality as pointed out in Figure 2.

Closeness centrality (CC). Closeness refers to the property of nodes being closest to every other node in the network, i.e. they have the shortest paths to all others. These nodes have therefore the best visibility in the network and can monitor the information flow. Node 4, being right at the center of the network, has the shortest overall paths to the rest of the nodes as shown in Figure 2.

Bridging centrality (BRC). Bridging centrality identifies bridging nodes, which are located in between highly connected regions. In Figure 2, node 7 plays an important role in connecting the two sub graphs G[1,2,3,4,5,6] and G’[8,9,10,11].



DC	BC	CC	BRC
4	4	4	7
2	7	7	3
8	8	8	5
3	2	3	8
5	3	5	4
7	5	6	2

Fig. 2. The top six nodes are presented according to the respective centrality measure. Choosing a centrality measure involves considering the type of application that the network will satisfy and also the measurements that we are interested in obtaining.

3 Applications to Protocol Design

In section 2 we presented Social Network Theory together with the significant concept of centrality. Having introduced some centrality variants, the next step would be to present the way these variants get involved in several areas of sensor networks, both algorithmically and application wise. The next three subsections present such cases.

3.1 Topology Control

As we mentioned earlier topology control refers to maintaining a topology with certain properties, for example connectivity, while reducing energy consumption and/or maximizing network capacity. This can be achieved in various ways, such as adapting transmission power or choosing the right neighbors to pass information to. The later can be implemented by taking the centrality measures that we mentioned earlier under consideration.

The direct connection between reducing the transmission power and reducing the energy consumption is straightforward. Usually in this case there is a startup phase, where the nodes communicate in order to find the minimum transmission power that they can provide while preserving connectivity at the same time. This phase may be called upon again sometime during the network's lifetime in order to check the state of the network and perhaps adapt to any node failures. Topology control protocols can also construct a logical topology out of the physical communication graph. A node for example can choose to communicate only with a certain subset of its direct neighbors, which the respective topology control algorithm has constructed.

The algorithm that we have proposed in [11] is applied to undirected and weighted graphs and calculates the edge betweenness centrality (EBC) locally. The edge weights are analogous to the energy levels of the respective nodes that each edge connects. An example of the algorithm can be seen in Figure 3.

3.2 Cooperative Caching

As described in earlier sections, WSNs are mainly characterized by resource constraints, variable channel capacity, and in-network processing. Under these restrictions/requirements, the goal of achieving application-level QoS in WSNs becomes a

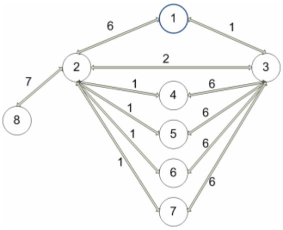


Fig. 3. An example of Edge Betweenness Centrality. The logical neighbors are chosen according to the value of the respective betweenness centrality and the number of two hop neighbors they are connected to. In this case node 1 will choose to broadcast only to node 2, since the edge connecting nodes 1 and 2 has a bigger EBC value than the edge connecting nodes 1 and 3 and all 2-hop neighbors can be reached through node 2.

very challenging task. The technique of *cooperatively caching* content in sensor nodes can address all three characteristics. In cooperative caching, multiple sensor nodes share and coordinate cache data to cut communication cost and exploit the aggregate cache space of cooperating sensors.

Since the battery lifetime can be extended if we manage to reduce the “amount” of communication, caching the useful data for each sensor either in its local store or in the near neighborhood can prolong the network lifetime. Additionally, caching can be very effective in reducing the need for network-wide transmissions, thus reducing the interference and overcoming the variable channel conditions. Finally, it can speed-up the in-network processing, because – as it is emphasized in [1] – the processing and delivery of content are not independent and their interaction has a major impact on the levels of QoS that can be delivered.

The work [2] pointed out the significance of the selection of the sensors that will coordinate the caching decisions, i.e., when/what/where to cache and for how long. Therefore, we need to develop methods to estimate the importance of sensors relative to the network topology. At this point, we can adopt and adapt methods from the field of social network analysis. For instance, betweenness centrality is an appropriate metric for this task, since large values of betweenness for a sensor indicate that this sensor can reach others on relatively short paths, or that this sensor lies on considerable fractions of shortest paths connecting others, i.e., it can control the communication between pairs of other sensors.

Though, betweenness (and also the other aforementioned centrality metrics) has several deficiencies: a) its computation by a sensor requires detailed knowledge of the connectivity of the sensor's one-hop neighbors, i.e., the sensor must exchange the set of its one-hop neighbors with each and every one-hop neighbor; thus larger/more packets travel in the network, b) its calculation, although quite fast, is not a O(1) complexity operation, which might be an issue when the sensornet topology changes quite fast, c) the values of betweenness centrality might be misleading, since it is affected a lot by the existence of isolated nodes in the borders of the network. For instance, in Figure 4, we see that the nodes 3,4,7,6 are equally central with respect to their degree; they all have a degree equal to 4. In addition, if we compute the betweenness centrality for each sensor in the whole graph, then node 7 is the most

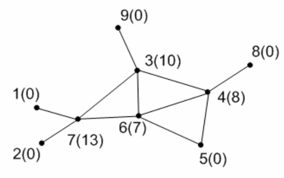


Fig. 4. Betweenness centrality values (the numbers in parentheses) for a small sample graph comprised by 9 nodes

"central" (with betweenness equal to 13), followed by nodes 3,4 and then comes the node 6. This is somehow counter-intuitive, since node 6 has *all network nodes* at its vicinity (at a two-hop distance).

Starting from this observation, we proposed a new centrality metric, the *μ-Power Community Index* (*μ-PCI*) defined as follows:

> The *μ-Power Community Index* of a sensor v is equal to k, if there are no more than μ*k sensors in the μ-hop neighborhood of v with degree equal to or greater than k, and the rest of the sensors within that region have a degree equal to or less than k.

It is clear that sensor nodes which have more connections (larger degree) are more likely to be "powerful", since they can directly affect more other sensor nodes. But, their power depends also on the degrees of their one-hop neighbors. Large values for the *μ-Power Community Index* of a sensor v indicate that this sensor v can reach others on relatively short paths (just like betweenness index), or that the sensor v lies on a dense area of the sensor network (just like the indication provided by the sensors degree). For WSNs applications, a localized version of this metric is more desirable, i.e., μ=1, which is the plain Power Community Index. With this localized version of the definition, then *PCI*(7) = *PCI*(4)=2, whereas *PCI*(6) = *PCI*(3)=3.

Using this definition, high performance cooperative caching protocols for wireless sensor networks can be designed [8] that will be based on the identification of sensors with high *PCI*s.

3.3 Vehicular Networks

Vehicular transportation is, and it is projected to remain, the most popular way for transporting people and goods among places. Although the use of vehicles is more than a century old, it is only recently that the widespread use of vehicles has become a real challenge, which requires the combat of the awful side-effects of road traffic.

In the USA, around 41000 people were killed, and 2.5 millions were injured during 2007; similar statistics hold also for the EU. Worldwide, more than one million people are killed, and more than 50 million are injured in traffic accidents each year. Among the main causes of these deaths and injuries we could mention the bad road conditions, the drivers' misbehavior and traffic jams, with the last ones being also responsible for a tremendous waste of time and of fuel. Though, a significant percentage of this waste in life and resources can be solved by providing appropriate information to the driver or to the vehicle via wireless communications.

The idea of employing wireless communications in vehicles dates back to '80, but recently the resolution of governments and national traffic administrations to allocate wireless spectrum for vehicular communications, along with the wide adoption of standards, like the Dedicated Short Range Communications (DSRC), or the IEEE 802.11 technologies (e.g., 802.11p) has created a real thrust in the field of inter-vehicle communications (IVC) or Vehicular Ad Hoc Networks (VANETs)[1]. VANETs comprise vehicle-to-vehicle and vehicle-to-infrastructure communications based on wireless local area network technologies (see Figure 5). Thus, a vehicle is a sensor-on-wheels (see Figure 6).

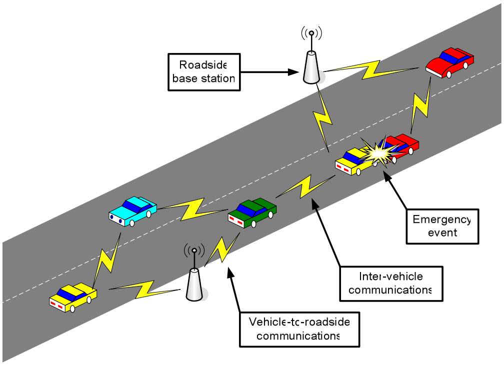

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Fig. 5. Intervehicle communications

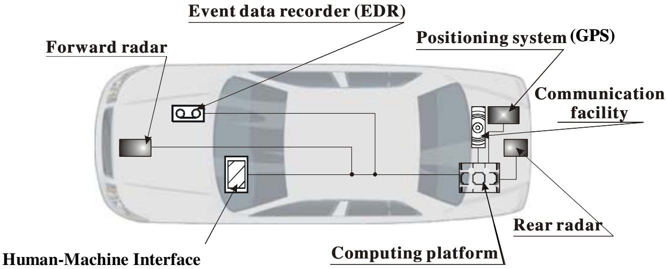


Fig. 6. A modern vehicle

During the process of designing and deploying a VANET, various questions must be answered that pertain to protocol performance and usefulness. For instance, when deciding the placement of roadside proxies [4], in order to reduce the average path length between the vehicles and the access points, we need to know the distribution of the position of vehicles; when performing message routing, the corner-stone question is “which are the highest-quality nodes (vehicles)?” [3] to carry out the forwarding process; when performing geocasting, the question is how we can spread the message

[1] Although the two terms are not identical, in this work we use the term VANET in order to emphasize the ad hoc nature of these wireless networks.

with the minimal number of rebroadcasts so as to reduce collisions and latency; when designing mobility models [5], we need to know the distribution of "synapses" per node, i.e., whether there are any clusters (communities); when the network is disconnected, a significant question concerns the identification of bridge nodes[6] which are encharged with the delivery/ferrying of the messages. All these questions and many more require knowledge of the topological characteristics of the VANET communication graph, where vehicles correspond to vertices and communication links to edges. Despite the fact that such knowledge is of paramount importance, the relevant literature is relatively poor with respect to the study of the characteristics of a VANET communication graph. And this is the place where social network theory comes into play. The measures described in subsection 2.1 can be used for the study of the topological characteristics of a VANET. In the next subsection we provide a glimpse of such results.

3.3.1 Centrality Metrics in VANETs

A VANET is a constantly evolving network, and therefore, one of the main features to examine is its connectivity over time. The study of a VANET requires either large scale (hundreds of thousands) of real vehicle trajectories or realistic vehicle trajectories over real road networks. We favor the second alternative, since currently there are no large scale vehicle trajectories publicly available to fit our needs. Thus, we study the structure and evolution of a VANET communication graph using realistic vehicular traces[2] from the city of Zurich. We have extracted a rectangular street area of size 5X5km^2, which covers the centre of Zurich and which contains around 200000 distinct vehicle trajectories during a 3 hours interval in morning rush hour. We study the networking shape evolution of VANET, by observing snapshots of this network taken at regularly spaced time instances. The generic question we seek to answer is whether "*Centrality metrics do identify "quality" (more central) nodes, and what is the spatial distribution of these nodes?*"

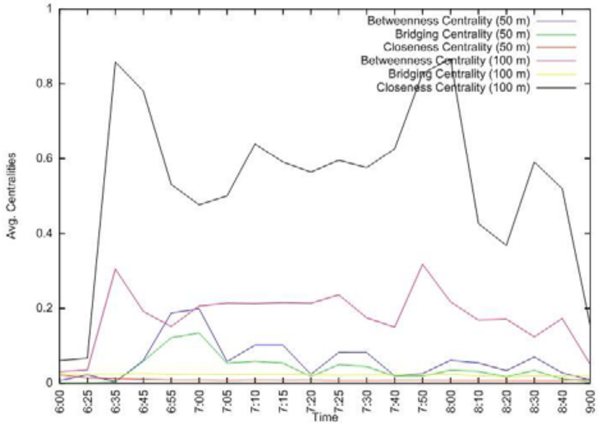


Fig. 7. Betweenness, bridging and closeness centrality over time and range

[2] The traces are publicly available from http://lst.inf.ethz.ch/ad-hoc/car-traces/

The general observation is that the distribution of the centrality metrics is not affected by the communication range; the distributions have similar shapes for transmission ranges T equal to T=50m and T=100m. The centrality metrics reflect quite reliably the variation in traffic conditions, i.e., density and relative positions of the vehicles (see Figure 7). Therefore, *centrality is not an artifact of the communication range, but an indication of the latent "behavior" of the vehicles"*, i.e., road network and drivers' intentions, which ultimately define the network position of the vehicles.

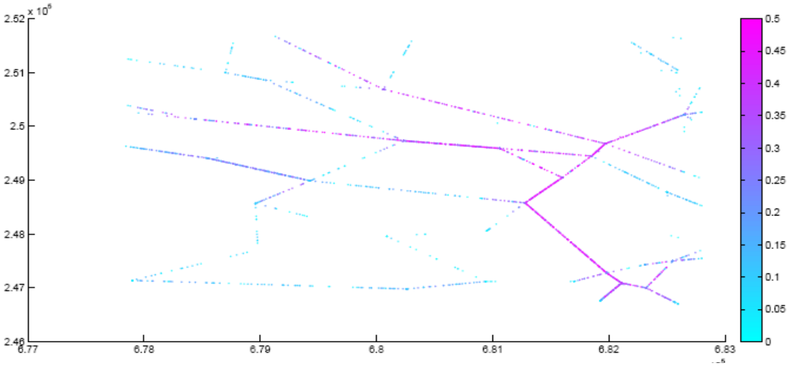


Fig. 8. Betweenness centrality over time and geographic location

Examining carefully the variation of one of the prevalent centrality metrics, i.e., betweenness, we plotted its actual values (instead of averages) as a function of time and geographic location. Due to space limitations, we present the betweenness centrality values at 06:00 and 08:00. The results are illustrated in the graph of Figure 8, which do not reflect the BC values of road junctions, but the BC values of vehicles. Each vehicle takes a color with respect to its betweenness centrality value. Clearly, the road topology is not the decisive parameter for the betweenness, even though it affects it (i.e. the colored lines lie above the roads); it is the case that high centrality values appear at any geographic location independently of the geographic location. Therefore, *the road network alone, e.g., junctions, is not sufficient information to determine the positions of possible "significant" nodes*. A thorough investigation of the connectivity properties of VANET communication graph appear in [7].

4 Related Work

One core concept for the analysis of social networks is centrality. Centrality metrics have been used to identify the role of individual nodes in a network and study their relationship to their neighboring nodes. Even though one of these metrics, betweenness centrality, was introduced in the 70s, the research community did not apply social network techniques to sensor networks until only the last couple of years.

Initially, social network algorithms and measures where used on the premise of global knowledge of the network. In 2006 for example, Hwang et al[9] proposed a centrality metric called Bridging Centrality (BC). The metric focuses on what the authors call bridging nodes, which are the nodes that are located in between highly connected regions and are therefore crucial for the connectivity and routing inside the network. The main drawback of the algorithm was that it was centralized and therefore global network knowledge was necessary.

In 2008, Nanda and Kotz [10] improved the BC algorithm by introducing a distributed version called Localized Bridging Centrality (LBC). As the name suggests, the metric uses only local information to identify the nodes that have a high flow of information through them.

5 Conclusions

The sensor networks applications are practically unlimited. Therefore the need arises for algorithms to be able to store data efficiently, save as much energy as possible and transfer messages with guaranteed delivery. Social Network Analysis can supply such algorithms.

References

1. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey of wireless sensor networks. IEEE Communications Magazine 40(8), 102–116 (2002)
2. Dimokas, N., Katsaros, D., Manolopoulos, Y.: Cooperative caching in wireless multimedia sensor networks. ACM Mobile Networks and Applications 13(3-4), 337–356 (2008)
3. Erramilli, V., Crovella, M., Chaintreau, A., Diot, C.: Delegation forwarding. In: Proceedings of ACM MobiHoc, pp. 251–259 (2008)
4. Li, P., Huang, X., Fang, Y., Lin, P.: Optimal placement of gateways in vehicular networks. IEEE Transactions on Vehicular Technology 56(6), 3421–3430 (2008)
5. Musolesi, M., Mascolo, C.: Designing mobility models based on social network theory. ACM Mobile Computing and Communications Review 11(3), 59–70 (2007)
6. Daly, E.M., Haahr, M.M.: Social network analysis for routing in disconnected delaytolerant MANETs. In: Proceedings of ACM MobiHoc, pp. 32–40 (2007)
7. Pallis, G., Katsaros, D., Dikaiakos, M.D., Loulloudes, N., Tassiulas, L.: On the structure and evolution of vehicular networks. Technical Report (February 2009)
8. Dimokas, N., Katsaros, D., Tassiulas, L., Manolopoulos, Y.: High performance, low complexity cooperative caching in wireless sensor networks. Technical Report (January 2009)
9. Hwang, W., Cho, Y., Zhang, A., Ramanathan, M.: Bridging Centrality: Identifying Bridging Nodes in Scale-free Networks. Technical Report 2006-05, Department of Computer Science and Engineering, University at Buffalo, March 15 (2006)
10. Nanda, S., Kotz, D.: Localized Bridging Centrality for Distributed Network Analysis. In: Proceedings of the 17th International Conference on Computer Communications and Networks (2008)
11. Papadimitriou, A., Katsaros, D., Manolopoulos, Y.: Edge Betweenness Centrality in Sensor Networks. Technical Report (February 2009)

SWEB: An Advanced Mobile Residence Certificate Service

Spyridon Papastergiou, Despina Polemi, and Christos Douligeris

Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou Str,
185 34 Piraeus, Greece
{paps,dpolemi,cdoulig}@unipi.gr

Abstract. The design and development of an enhanced network infrastructure in combination with the adoption of new technologies, standards and architectural styles for the design, development and implementation of new platforms can give a significant push to the deployment of advanced mobile services in the area of public administration. In this context, we present an innovative m-government platform that provides an advanced mobile Residence Certificate service. The proposed platform is an interoperable, affordable, secure and scalable solution that addresses a set of crucial requirements such as security, user friendliness, interoperability, accessibility and scalability.

Keywords: m-government platform, mobile service, security.

1 Introduction

The entry in the ICT Society constitutes a basic strategic choice for all the members of European Union (EU), since it can be considered as the means to achieve economic growth and prosperity. However, the achievement of this objective presupposes two major conditions. The first is the creation of a suitable network infrastructure through the development, engineering, maintenance and operation of high-speed wired and wireless networks that enable the countries to strengthen their fundamental structure. Major initiatives [1], [2] have been launched and implemented in the EU member states towards this direction, creating the proper telecommunications infrastructure.

The second condition concerns the exploitation and adoption of new technologies, standards and architectural styles for the design, development and implementation of new platforms that are able to provide advanced services. These services aim to improve the relations among the involved stakeholders and to create significant revenue for them.

Especially in the area of public administration several activities have been initiated that define standards-based frameworks for the public sector bodies at the national [3], [4] and pan-European levels [5], [6]. The goal of these frameworks [7] is to empower a joined up and web-enabled government, and to improve its flexibility and efficiency. Typically, these frameworks focus on the precise definition of specific standards that should be applied and provides guidelines in the form of specifications that should be followed for the development of governmental platforms and services.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 421–430, 2010.

It should be also noted that most of the projects [8], [9], [10], [11] that are currently run or have been completed in the public sector either cover only the electronic dimension of the government or treat the mobile aspect in a superficial manner. Usually, the latter does not achieve to provide advanced mobile government (m-government) services due to the limitations of the existing mobile devices, thus failing to address several crucial requirements, such as security, in an effective way.

Although, in the past few years mobile phones have been continually improving and at the moment they present rather powerful computing and communication devices capable of executing complex applications. This factor can be considered as the starting point for the deployment of a number of m-government services.

In this context, this paper presents an innovative m-government platform, named SWEB [12], [13], [14], [15], [16] that is based on widely used Web Service-based technologies and Public Key Infrastructure (PKI) in order to address several security and interoperability aspects. SWEB is a secure, interoperable, open, affordable municipal platform upon which an advanced mobile Residence Certificate (mRCertificate) service has been built and offered for use and experimentation. The mRCertificate service enables the citizens of the municipality that hosts the platform to receive a document that proves the existence of a residence for a given citizen in the specific municipality.

The rest of the paper is structured as follows; Section 2 discusses the major requirements as imposed by the mRCertificate service. Section 3 presents the proposed m-government framework illustrating the main entities that it consists of and it describes the SWEB platform. Section 4 describes the main activities performed when a user (citizen) registered in the SWEB platform of his/her municipality uses this platform to request a mRCertificate document. Finally, Section 4 draws some conclusions and presents areas for further research.

2 Requirements of the mRCertificate Service

Residence certification is an important document that it is being issued by municipalities. The included business flow of this service can be considered as a time-consuming process due to the population movements within the same country or/and abroad. The main objective of the proposed mRCertificate service is to cover the needs of a citizen or civil servant to search for, request and receive a municipal mobile document certifying that a particular citizen is registered at the records of a municipality in an efficient and accurate manner. D

In order for the mRCertificate service to be widely accepted by the citizens and the municipalities that will host and operate the SWEB platform has to address a set of requirements. The major requirements that must be fulfilled are the following:

Security: The mRCertificate service has to be secure in all aspects (confidentiality, integrity, authenticity, non-repudiation), so that all users trust the service and feel confident in using it. The adoption of proper advanced security mechanisms such as XML encryption [17], XML Signatures [18] and Timestamping [19] that will undertake the responsibility to secure the exchanged documents and messages creating a trusted framework is considered crucial for the SWEB platform.

User Friendliness and Accessibility: The wireless environment needs to be easily accessible, with user-friendly interfaces. The mobile application of the mRCertificate service has to be designed and developed by properly taking into consideration the constraints that come from the size and the capabilities of the mobile devices. The application should offer a basic functionality while complex operations must be completely transparent to the user.

Interoperability: The mRCertificate service should be interoperable enabling the interconnection with many different infrastructures (e.g. existing legacy systems) of the municipality. For this reason, new technologies that promote the interoperability (i.e. Web Services [20]) and light protocols in the messaging exchange have to be adopted.

Reduced organizational and technical complexity: The mRCertificate service should add a small amount of organizational and technical complexity, concerning financial and temporal parameters. This is achieved by introducing standard solutions, applicable in different municipal organizations that are quick to be adopted and easily customizable to the organization's requirements, trying to diminish the need for maintenance during operation.

Scalability and extensibility: The mRCertificate service has to be simple, open, reconfigurable, scalable and easily extensible. It should be capable to serve a large number of citizens with acceptable levels of quality of service.

3 Proposed m-Government Framework

This section presents the proposed m-government framework illustrating the main entities that participate in it and describing the m-SWEB platform.

3.1 Involved Entities

In this section, a description of the five major entities that constitute the m-Residence Certificate process is provided. A high level representation of the framework is presented in figure 1, highlighting these entities. The Mobile User and the Home-Municipality are the two main entities of the framework that initiate the process and handle the request correspondingly.

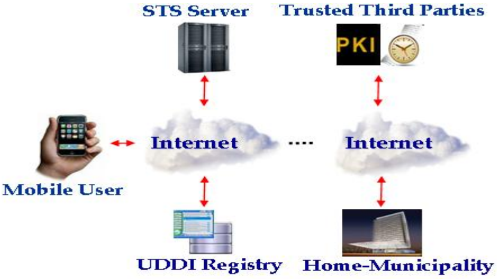


Fig. 1. Entities and Actors

The involved actors are described in the following:

Home-Municipality
This is the municipality that hosts the proposed m-SWEB platform and thus it is able to offer the mRCertificate service to its citizens. It takes the appropriate steps to develop and make available the mobile application required to access the provided service.

Mobile User
The mobile users are citizens that have their residence in the region being under the control of a municipality that has adopted and operates the m-SWEB platform. It should be noted that the user himself may be either a citizen requesting its own residence certificate or a delegate who is allowed to undertake such a request.

Secure Token Service (STS) Server
This entity authenticates users that want to access the provided m-RCertificate service issuing the needed authorization token. Based on this token the "Home-Municipality" is able to grand or deny access to their service.

Trusted Third Party (TTP)
The required TTPs are at a minimum a Certification Authority (CA) and a Registration Authority (RA) offering the PKI services of registration and certification, as well as a Time Stamping Authority (TSA) offering standard based time stamping services.

UDDI Registry
This operator hosts a public UDDI directory where the offered mRCertificate services of the "home-municipalities" are published in order to become publicly available.

3.2 m-SWEB Platform Overview

A major objective of the SWEB platform is to exploit the functionality of the existing legacy systems (e.g. back-office systems, independent applications, databases) of the municipality in order to provide advanced mobile services such as the Residence Certificate service. The basic achievement of the SWEB platform is that is able to overcome the internal obstacles of the legacy systems.

Most of these systems are typically developed based on a centralized model. Therefore, they are usually large and monolithic since their functionality is not well divided into smaller and more manageable modules/procedures. In this context, the legacy systems are not able to provide well-formed standardized interfaces that can be used by remote users in order to access all the available services and provided functionalities.

The innovative design of the SWEB platform architecture aims to hide the complex processes of theses services by providing interoperable and easy-to-use services and to achieve expandability of their functionality and high level of quality by means of system security. This is accomplished by using advanced XML-based technologies, PKI and design methodologies, resulting in an elaborate platform that fulfils several critical requirements and offers a trusted environment to their citizens.

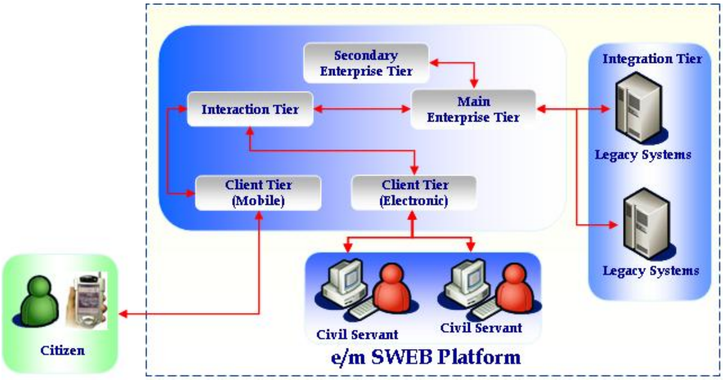


Fig. 2. m-SWEB Platform

In more detail, the architectural overview of the SWEB platform, as depicted in Figure 2, consists of five concrete tiers, which are listed below:

- ✓ The *Interaction Tier* includes all the components that are directly used to communicate with the platform. It includes all the required interfaces for the establishment of the appropriate communication channels with every electronic and mobile entity (e.g. citizens, organizations and civil servants) that want to access the provided m/e-services.
- ✓ The *Main Enterprise Tier* where all basic services and the platform core are deployed. These basic services provide the basic functions that are used by the architecture as a whole to perform primitive tasks. In the SWEB platform the basic services include:
  - o *Security services*, responsible for implementing the needed security mechanism such as the creation and the validation of simple XML digital signatures.
  - o *Transformation services*, which actually handle all the data transformation mechanisms from one form to another.
  - o *Integration services*, responsible for the communication with the legacy infrastructures of the municipality (Integration Tier).
- ✓ The *Secondary Enterprise Tier*, which undertakes the responsibility to manage the choreography of the main platform services (mRCertificate service), and to implement their business logic.
- ✓ The *Integration Tier*, which consists of the required adaptation components that sit “on-top” of the existing/ legacy systems of the municipality.
- ✓ The *Client Tier*, which integrates all the necessary components for accessing the SWEB platform and requesting the m-government services. The client tier differentiates in two concrete nodes:
  - o The *electronic node*, which enables the civil servants to access the pending Residence Certificates via the use of browsers in order to review, approve and sign them.

- The *mobile node*, which consist of a stand alone mobile application that should be downloaded and installed by the mobile users on their mobile devices in order to access the mRCertificate service.

Each one of these tiers contains independent components which communicate with each other through clearly defined operation channels.

4 Mobile Residence Certificate Processes

This Section describes the activities performed by a user (citizen) who communicates with a municipality that hosts the SWEB platform using a mobile device in order to request a Residence Certificate document for a person having its residence in the region being under control of the specific municipality.

The mRCertificate processes are divided into four phases, namely *registration/installation*, m-*Residence Certificate Request submission*, *Request processing/issuance of Residence Certificate* and *Retrieval of Residence Certificate*, comprising the following processes:

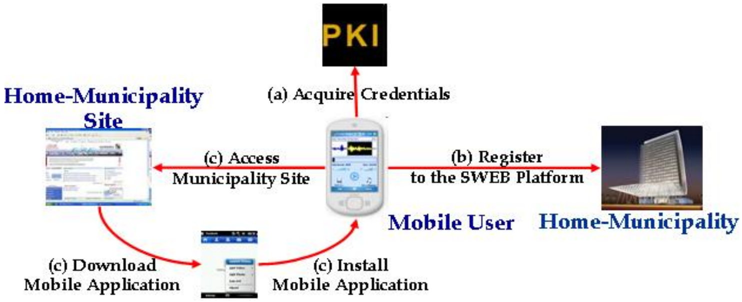

PKI
(a) Acquire Credentials
Home-Municipality Site
(c) Access Municipality Site
(b) Register to the SWEB Platform
Mobile User
Home-Municipality
(c) Download Mobile Application
(c) Install Mobile Application

Fig. 3. Registration/Installation Phase actions

registration/installation
The steps (Figure 3) that take place in this phase include the following:

a. the mobile user's communication with the TTP for the acquisition of the appropriate security credentials. The required credentials are a private key and the corresponding X.509 certificate which are stored locally on the mobile device.
b. The user's communication with the SWEB platform that operates in his/her "home-municipality" to be registered as a valid user.
c. The access to the municipality site in order retrieve and install the mobile application on his/her mobile device.

This is a preparatory phase which contains actions that should be performed before the initiation of the actual mRCertificate service.

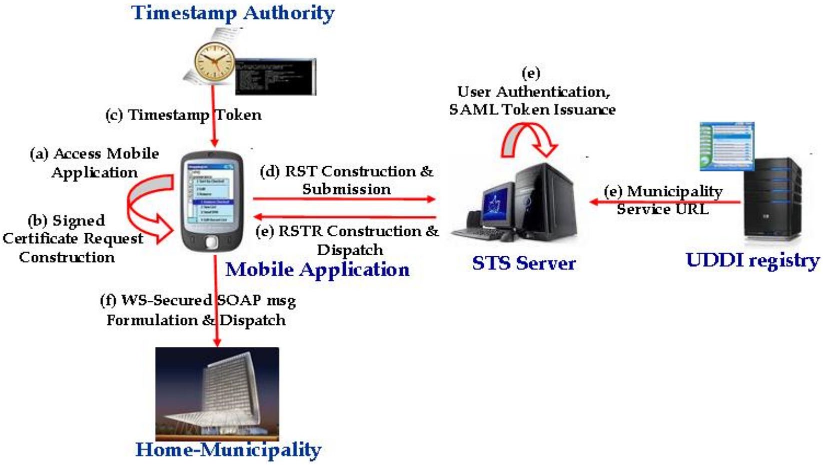

Timestamp Authority
(c) Timestamp Token
(a) Access Mobile Application
(b) Signed Certificate Request Construction
(d) RST Construction & Submission
(e) RSTR Construction & Dispatch
Mobile Application
(e) User Authentication, SAML Token Issuance
(e) Municipality Service URL
STS Server
UDDI registry
(f) WS-Secured SOAP msg Formulation & Dispatch
Home-Municipality

Fig. 4. Residence Certificate Request submission Phase actions

Residence Certificate Request submission
In this phase the mobile user creates a request for a Residence Certificate and submits it to the "home-municipality". The basic actions (Figure 4) that are included in this phase are the following:

- ✓ The User initiates the Mobile Application (MA) and accesses the RCertificate form. The mobile User Interface enables the user to create a RCertificate request supplying the necessary data. This data input is automatically checked for prevention of errors.
- ✓ The MA, following a completely transparent process gathers the form data and formulates the RCertificate request. The signature of the request is formulated based on the cryptographic primitives in the mobile phone, the user's certificate and the RCertificate request data.
- ✓ A timestamp token that corresponds to the signed request is requested from the Time Stamping Authority and the obtained timestamp data is embedded on the generated signature.
- ✓ The MA communicates with the STS server submitting a Request Security Token (RST) [21]. The RST consists of the name of "home-municipality", the requested service (residence certificate) and the user authentication credential (X.509v3 certificate).
- ✓ The STS server, initially, authenticates the user based on the included RST credential and issues an authorization token (SAML token [22]). This token is a short lived credential which contains the role that is assigned to the user by the corresponding "home-municipality". Afterwards, the STS server communicates with the UDDI Registry in order to obtain the URL of the municipality service which, along with the issued SAML token, is packaged in a RST response (RSTR) that is returned to the MA.
- ✓ The MA receives the RSTR and extracts the included information (SAML token and municipality service url). Automatically, a SOAP message is formulated that contains the signed RCertificate request and the SAML token and

the appropriate WS Security extensions are applied to it, so that it becomes encrypted with the municipality's public key, and digitally signed with the user private key. Finally the protected SOAP message is dispatched to the "home-municipality".

Request processing/issuance of Residence Certificate

The reception of the RCertificate request, at the "home-municipality", is a fully automated process that requires no human intervention. The SOAP message containing the request is received and decrypted with the municipality's private key and the validity of its WS Security extensions digital signature is verified, so that the point of origin is validated.

Then the embedded SAML token is extracted and the mobile user's authentication and authorization processes are initiated. According to these processes the signature of the SAML token is validated and the included role is retrieved. Based on this role, the SWEB platform is able to grand or deny access to the requested mRCertificate service. When, these processes have been completed, the platform constructs and sends a reply WS-Secured SOAP message to the Mobile Application with the result of the authentication and the authorization. The Mobile Application receives the SOAP message, decrypts and verifies the applied WS-Security mechanisms and informs the Mobile User.

If the authentication and/or the authorization processes fail the access to the service can not be accomplished and the whole workflow is terminated. Otherwise, the SWEB platform proceeds to the included mRCertificate request processing. The request itself is extracted from the SOAP message and the verification of the applied signature and the validation of the embedded timestamp are performed. Then, the request is sent to the municipality's Legacy System which processes it according to its internal procedures.

The Legacy System takes the decision to approve the received request and issues the corresponding Residence Certificate document. A unique identifier, a "Residence Certificate id", is assigned to the document which finally is stored in the SWEB platform in a list of pending for approval documents.

A Civil Servant of the "home-municipality", who is authorized to access the Residence Certificate pending list, proceeds with the approval process. Initially, the civil servant using a municipal electronic application is authenticated towards the SWEB platform in order to be able to retrieve the pending mRCertficate documents. As soon as, he/she accesses the list, he/she selects each document and verifies, edits (if required) and signs it.

The approved signed mRCertificate document is stored locally in the platform in an approved document list along with the unique identifier. Automatically, an SMS message is created and sent by the platform to the mobile user in order to inform him/her that the submitted request has been handled successfully and the issued mRCertificate document with a specific "Residence Certificate id" is ready for retrieval.

The above functional description illustrates that the most active actors are the complementary primitive services that compose the SWEB platform and handle all the underlying complexity of the request processing, enabling the service' semi-automation. Complete automation cannot be achieved due to the restrictions posed by the service itself that requires the issued mRCertificate document to be monitored by the civil servants responsible for the validity of their content.

Retrieval of Residence Certificate
In this phase the Mobile User receives the SMS notification which informs him/her that the processing of the request has been finished and the resulting document is ready for retrieval. Additionally, the SMS message contains the “Residence Certificate id” which is the unique identifier with which the user is able to request his/her document.

The actual process that the user has to perform in order to retrieve the mRCertificate is similar with the process of the Residence Certificate Request submission phase. The user has to access the RCertificate form and insert the received “Residence Certificate id”. The Mobile Application constructs the corresponding request and signs it using the user’s credential. Then, the user is authenticated towards the STS server retrieving the required authorization token (SAML Assertion) that is embedded in a SOAP message along with the formulated request.

The Mobile Application sends the SOAP message to the SWEB platform which performs the required authentication and authorization processes and returns to the user the requested Residence Certificate document. Once the final document has been dispatched, the platform removes it from the approved document list. Thus, there is not any critical information stored over time locally in the platform.

5 Conclusions and Future Work

The implementation and deployment of advanced m-government services is one of the priorities of the EU member states. It is expected that over the next years there will be a significant push to the deployment of these services having in mind the penetration rate and the performance improvements of the mobile devices.

Identifying this assumption, we have presented an innovative m-government platform that provides an advanced mRCertificate service. The main benefits of this service are that it achieves to simplify a multi-complex process improving the quality of life of its users (citizens), and enabling secure environment for dealing with public authorities from any place and at any time. Additionally, the proposed service can be used by the municipalities as a well-defined example for the design, development and implementation of new advanced composition services that will significantly increase the efficiency of their operations.

Our future research plan is to further investigate all the privacy issues that concern a m-government service taking into account several aspects such as anonymity, pseudonymity and adopting the required mechanisms that are able to address them.

Acknowledgments

This work has been supported by the GSRT (PENED) programme and the IST project SWEB (IST-2006-2.6.5). The authors would like to thank all the participants for valuable discussions and the European Union for funding the SWEB project.

References

1. European Telecommunications Standards Institute, `http://www.etsi.org/`
2. DG Information Society & Media,
   `http://ec.europa.eu/dgs/information_society/index_en.htm`

3. UK government's eGovernment Interoperability Framework (eGif), http://www.govtalk.gov.uk/interoperability/egif.asp
4. German Federal Ministry of Interior, SAGA - Standards and Architectures for e-government Applications, version 2.0 (2003)
5. Electronic interchange of data between administrations: IDA programme, http://europa.eu/scadplus/leg/en/lvb/l24147a.htm
6. Standardisation Action Plan in support of eEurope, http://ec.europa.eu/information_society/programmes/others/index_en.htm#Standard
7. Papastergiou, S., Polemi, D.: A testing process for Interoperability and Conformance of secure Web Services. Radio Communications, published by IN-TECH (to appear) ISBN 978-953-7619-X-X
8. Intelligent Cities (IntelCities), http://www.intelcitiesproject.com/wcm-site/jsps/index.jsp?type=page&cid=5026&cidName=HOME&isAnonymous=true
9. Impact of e-Government on Territorial Government Services (TERREGOV), http://www.terregov.eupm.net/my_spip/index.php
10. Usability-driven open platform for Mobile Government (USE-ME.GOV), http://www.usemegov.org/
11. E.C 6th Framework Programme, Electronic and secure municipal administration for European citizens – eMayor, IST-2004-507217, 2004 (2007), http://www.emayor.org
12. Karantjias, T., Papastergiou, S., Polemi, D.: Design Principles of Secure Federated e/m - Government Framework. International Journal of Electronic Governance/Special Issue on Users and uses of electronic governance (to appear)
13. Pentafronimos, G., Papastergiou, S., Polemi, N.: Interoperability Testing for e-Government Web Services. In: 2nd International Conference on Theory and Practice of Electtronic Governance (ICEGOV 2008), Cairo, Egypt, December 1-4 (2008)
14. Meneklis, V., Papastergiou, S., Douligeris, C., Polemi, D.: Towards advanced e/m-Government platforms. In: International Conference on Information Society (i-Society 2007), Merrillville, Indiana, USA, October 7-11 (2007)
15. Meneklis, V., Douligeris, C.: Extending a Distributed System Architecture with e-Government Modeling Concepts. In: Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), Workshop on Secure e/m Government Enhancing Cooperation with non-EU Regions, Athens, Greece, September 3-7 (2007)
16. Meneklis, V., Douligeris, C.: Enhancing the design of e-Government: Identifying structures and modelling concepts in contemporary platforms. In: 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), Macao, China, December 10-13 (2007)
17. XML Encryption, http://www.w3.org/Encryption/2001/
18. XML Signature Recommendation – XML-DSIG, http://www.w3.org/TR/xmldsig-core/
19. Adams, C., Cain, P., Pinkas, D., Integris, R.: IETF RFC 3161 Time-Stamp Protocol (TSP), http://www.ietf.org/rfc/rfc3161.txt
20. Hartman, B., et al.: Mastering Web Services Security. Wiley Publishing, Chichester
21. OASIS Web Service Secure Exchange Technical Committee, OASIS WS-Trust 1.3, OASIS Standard (2007)
22. Cahill, C.P., et al.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

p-Democracy a Pervasive Majority Rule

Kyriacos A. Antoniades

TEI of Piraeus, Petrou Ralli & Thivon, 12244, Agaleo, Piraeus
kyriacos.antoniades@hotmail.com
http://www.p-democracy.net

Abstract. Today, group decision making in our democratic society uses the non-ranked method. What we need is an improved method that allows decision makers to indicate not only their chosen alternative, but also their order of preference by which all alternatives will be placed. We classify this as a particular Social Choice Function, where choice is a group decision-making methodology in an ideal democratic society that gives the expression of the will of the majority. We use the Eigenvector Function to obtain individual priorities of preferences and Borda's Function to obtain the Ranking or otherwise, the Group Choice. Our conclusions give rise to new directions for pervasive democracy with an innovative degenerative quantum scale to allow even for strong to very strong preferences.

Keywords: Multi Criteria Group Decision Support Systems, Analytic Hierarchy Process, Pervasive Context Aware Activity Based Computing, e-Government, Everyware Development.

Introduction

Decision support systems are nowadays becoming a widespread set of tools for the decision analyst and decision maker, utilized in an ever-increasing number of public and private organizations. Furthermore, today's evolution that come from extensive use of pervasive computing systems, ubiquitous services and ambient intelligence, makes it even more attractive to deploy group decision-aid techniques to achieve democratic operational environments on the productive and social activities that take place in an organization. In addition, we can optimize results by taking into account as many possible views coming from as many different fields of studies and interests. Finally, we can keep up to date to the recent needs of the knowledge age, where specialization of each decision maker involved in the decision-making process play an active role. This paper presents the design, development and implementation of a pervasive multi criteria group decision support system based on the Analytic Hierarchy Process [1] to obtain individual priorities of preferences for each decision maker, whom gives pair wise comparisons of the alternatives in question. We utilize a modified Saaty's scale [2], namely a degenerative quantum scale, which eventually allows us to obtain strong and absolute preferences. Thereafter, we aggregate individual priorities and using Borda's Social Choice Function [3], we obtain the ranking or the group choice for all decision makers participating in the decision process to obtain an expression of the will of the majority.

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 431–440, 2010.

Background and Current Trends

Our main research activities are generally concerned with the effects of human computer interactions with pervasive computing systems as in analogy with electricity for example [1], which we occasionally use but not pay too much attention of its presence. Rick Belluzo [2], general manager of Hewlett-Packard called it “the stage when we take computing for granted. We only notice its absence, rather than its presence”. Louis V. Gerstner [3], Jr., of IBM had also said “Picture a day when billion of people will interact with million of e-businesses via a trillion interconnected devices”. Mark Weiser [4] at the Computer Science Lab at Xerox PARC only just recently coined the idea of pervasive computing in 1988. MIT Project Oxygen [5], Sun [6], Microsoft [7] Adobe [8] and Oracle [9] have also contributed significant research into this field. In addition, there appears to be a growing list of institutions [10] that focus in ubiquitous computing research and development.

The primary research unit in question involves the paradigm of a pervasive information and communication system technologically mediated for collaborative practices in order to aid decision-making. Interdisciplinary areas include Pervasive or Ubiquitous Computing (UbiComp) [11], Everyware Distributed Engineering (EWDE) [12], Computer Supported Cooperative Work (CSCW) [13], Human Computer Interaction (HCI) [14], Multi Criteria Group Decision Support Systems (MCGDSS) [15], Analytic Hierarchy Process (AHP), and e-Participation / e-Government [16]. We accept in the CSCW matrix of location and collaboration that MCGDSS are co-located and synchronous. The purpose is therefore, to extend that notion so they may also become remote and asynchronous. Major research is thus concentrated in the design development and implementation of a Context Aware (CA) Activity Based Computing (ABC) [17] framework based on server-to-server distributed network architecture, relying on Java Enterprise Edition (JEE) [18] to provide the pervasive and persistent platform. Thereafter we design, develop and implement our MCGDSS an embedded platform application, which we call “p-Democracy” [19] as utilized from both decision analysts and decision makers.

Initially, we address the issue of developing user authentication and authorization and device concepts (fingerprint, eye recognition) for identity management in the ABC framework. Security is of outmost important here, so we use Java Authentication and Authorization Services (JAAS) [20], enable Secure Sockets Layer (SSL) and obtain 128-bit Encryption Certificates on the server, to protect the identity of the decision maker. Anonymity is the primordial essence here and not compromised at any costs, assuring privacy, and trust and dependability conditions in order to avoid cyber crime. Specifically, we provide ubiquitous decision support services using our ambient intelligent component, p-Democracy embedded into our ABC framework. We deem that the success of our application lies in the modified Saaty’s scale, which eventually allows decision makers to make strong to absolute preferences in their pair wise comparisons of the alternatives in question.

Contrary to today’s practice and strategy, ubiquitous computers will not just run applications but will elicit them as context aware activities in portable server distributed network architectures to provide simultaneously co-located, remote, synchronous and asynchronous multimodal interactions. It is the dawn of the next generation society of ubiquitous citizens in the "Internet of Things".

Everyware, a Pervasive Platform

Everyware Development first coined by Adam Greenfield [1] in 2006 in which he envisages when "million of people will interact with multitude of devices in a single space at a single time". It is the evolution from Software Development. What we seek is an open source, cross-platform portable, scalable and extensible programming environment. Sun's Java Enterprise Edition (JEE) [2] and Java Mobile Edition (JME) [3] with Eclipse [4] as an Interface Development Environment (IDE) provide such a repository. We use Apache Tomcat [5] as the web application server for p-Democracy and a pervasive system project lifecycle with an automated contingency plan namely subversion supported on Java's HTTP server [6] which can be also used for digital surveillance, tracking and monitoring of user sessions. Tom Taylor's [7] in "Everyware: the future is already here, it is just not well distributed yet" sums our efforts.

The initial goal of this research is therefore concentrated in the design, development and implementation of an ABC framework, that is, a pervasive platform based on Java's Remote Method Invocation (RMI) [8] a hybrid server to server and server to client distributed architecture. Thereafter, primary effort is concentrated into designing, developing and implementing collective user authentication and authorization interfaces with multi modal context aware interactions [9] and thence, extend the security context aware prototype to new user and authentication mechanisms that will allow both multi touch and multi person interactive interfaces. Secondary research focuses on embedding into the framework a set of collective user evaluation interfaces with multimodal interactions using AHP with our innovative degenerative quantum scale that allows strong to absolute preferences in our MCGDSS component. We run field studies of our Application Protocol Interface (API) deployment with examples from both the public and private sector [10].

Everyware Application: p-Democracy

We demonstrate group decision-making using the AHP by a simple five-step method. 1. The Decision Analyst is constrained to structure Hierarchons [1] based only on three level hierarchies, where each level can have no more than 3 or 4 decision elements. We pay particular attention for rank reversal and preservation as to the choice of mode of synthesis i.e. distributive or ideal. 2. The Decision Maker inputs pairwise comparisons of criteria and alternatives using basically, the fundamental scale, considering homogeneity and clustering as to extend or reduce the fundamental scale if required. 3. The Class defined, calculates and outputs relative weights (ranking) of criteria and alternatives, using the eigenvector, estimating consistency in each case. Sensitivity of the principal right eigenvector is ignored as the number of criteria and alternatives are kept to a minimum. 4. The relative weights are areggregated to obtain each individual's overall rankings. 5. The individual overall rankings are thereafter aggregated in order to obtain an overall group ranking.

1 Structure the Hierarchy into Interrelated Decision Elements

This is the most important step of decision-making and that is the structuring of the hierarchy itself. The decision analyst develops the hierarchical representation of the problem. At the top of the hierarchy are the overall objective and the decision alternatives are at the bottom. Between the top and bottom, levels are the relevant criteria. We assign each Hierarchy to specific decision maker or group of decision makers.

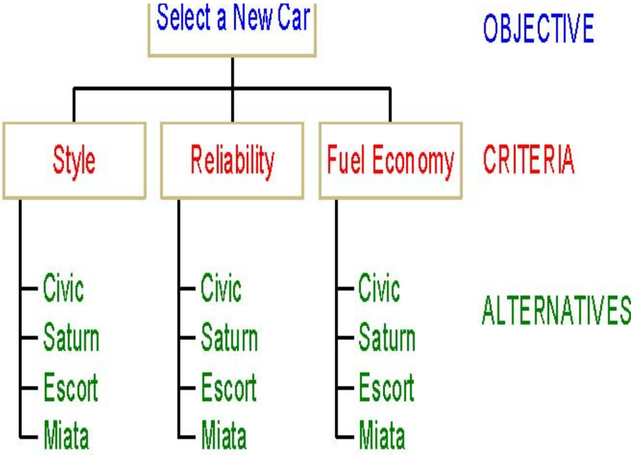


Fig. 1. A Hierarchy and Decision Elements

Example, defining the hierarchy

Objective: Select new car
Criteria: Style, Reliability, Economy
Alternatives: Civic, Saturn, Escort, Miata

2 Collect Pair Wise Comparisons of the Decision Elements

This step generates relational data for comparing the criteria and alternatives. This requires the decision-maker to make pair wise comparisons of homogeneous elements at each level. In the AHP, the fundamental scale of real numbers from 1 to 9 is used to systematically assign preferences in terms of intensity judgments as shown below

Table 1. Saaty's Fundamental Scale

Intensity	**Definition**	**Explanation**
1	**Equal importance**	**contribute equally**
2	Weak	
3	**Moderate importance**	**slightly favor**
4	Moderate plus	
5	**Strong importance**	**strongly favored**
6	Strong plus	
7	**Very strong**	**strongly dominant**
8	Very, very strong	
9	**Extreme importance**	**favored affirmation**
Reciprocals of above	**If element *i* has one of the above nonzero numbers assigned to it when compared with activity j, the *j* has the reciprocal value when compared to *i***	**reasonable assumption**
Rationales	**Ratio arising from the scale**	**consistency**

3 Calculate the Relative Weights of the Decision Elements Using the Eigenvector and Check for Consistency

Utilizing the pair wise comparisons of step 2 an eigenvector method is used to determine the relative priority of each criteria and alternatives in the hierarchy. In addition, a consistency ratio is calculated, using the Eigenvalue and displayed. According to Saaty, small consistency ratios (less than 0.1, that is, 10%) does not drastically affect the rankings. The user has the option of redoing the comparison matrix should the consistency ratio be larger than 10%. If the decision maker knows the actual relative weights of n decision elements, the pair wise comparison matrix would be depicted as shown for matrix A. Assuming we are given **n** stones, $\mathbf{A_1,\ldots,A_n}$, whith weights $\mathbf{w_1,\ldots,w_n}$, respectively, the matrix will contain the ratios of the weights of each ratio with respect to all others. The smaller of each pair of ratios is used as the unit and the larger one is measured in terms of multiples of that unit:

This leads to the eigenvalue equation:

$$A \,.\, W = n \,.\, W$$

The solution of the above called the principal eigenvector of **A** which is the normalization of any column of **A**. Where,

A →vector comparison matrix
W→$(w_1,w_2,w_3,\ldots,w_n)_T$ vector of relative weights. The right eigenvector of matrix **A**
n → scalar eigenvalue (principal maximum)of matrix **A**

The matrix

$$\boldsymbol{A = a_{ij}, a_{ij} = w_i/w_j, i,j = 1,\ldots,n},$$

Satisfies the reciprocal property if a is twice more preferable than b, b is twice more

$$A = \begin{array}{c} 1 \\ 2 \\ 3 \\ \cdot \\ \cdot \\ \cdot \\ n \end{array} \begin{bmatrix} w_1/w_1 & w_1/w_2 & w_1/w_3 & \ldots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & w_2/w_3 & \ldots & w_2/w_n \\ w_3/w_1 & w_3/w_2 & w_3/w_3 & \ldots & w_3/w_n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ w_n/w_1 & w_n/w_2 & w_n/w_3 & \ldots & w_n/w_n \end{bmatrix}$$

preferable than c, then a is four times more preferable than c (cardinal scale).

$$\boldsymbol{a_{ji} = 1/a_{ij}}$$

$$\begin{bmatrix} w_1/w_1 & w_1/w_2 & w_1/w_3 & \ldots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & w_2/w_3 & \ldots & w_2/w_n \\ w_3/w_1 & w_3/w_2 & w_3/w_3 & \ldots & w_3/w_n \\ \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & & \\ w_n/w_1 & w_n/w_2 & w_n/w_3 & \ldots & w_n/w_n \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix} = n * \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix}$$

Is *consistent* provided the following condition is satisfied:

$$\boldsymbol{a_{jk} = a_{ik}/a_{ij}, i, j, k = 1,\ldots,n}$$

$$\sum_{i=1}^{n} w_i = 1$$

4 Aggregate the Relative Weights of the Decision Elements to Arrive at an Overall Individual Ranking

In this step, the priorities of the lowest level alternatives relative to the top most objective are determined and displayed, which serves as a ratings of decision alternatives in achieving the objective. The final output from is the relative priorities of the bottom most (in the hierarchy) alternatives relative to the overall objective (top level of hierarchy). The composite relative weight vector of elements at the k_{th} level w.r.t. the first computed by :

$$\prod_{i=2}^{k} B_i \qquad C[1,k] =$$

Where:

C[1,k]→vector of composite weights of elements at level k w.r.t. element on level 1.
B_i →$\mathbf{n}_{\mathbf{i-1}}$ **x** $\mathbf{n}_{\mathbf{i}}$ matrix of vector ***W***

5 Aggregate the Overall Individual Rankings for Each Hierarchon to Obtain Group Ranking

After having obtained the individual rankings for a particular hierarchon, we can then aggregate these results for all decision makers to obtain the group ranking. The simplest way to do this is to use Borda's positional method. The basic idea is to add the individual ranking matrix for every decision maker. For each individual ranking, we assign one point for lowest ranked, two for the second lowest, three for the third an so forth. The Group Ranking, *Rg*, is obtained by adding all the points assigned for each of the individual rankings and ranking highest, this time, the rank with the most points, second with the next most points and so forth.

Given k individual rankings we choose Borda's coefficients, $r_1, r_2, r_3, \ldots, r_k$ such that, $r_1 > r_2 > r_3 > \ldots$

$> r_{k,}$, $c \in S$ list r_i, Score $B_i(c)$ *with* a total Borda Score, $B(c)$ defined as:

For each decision maker,

The Scale Solution

Considering Saaty's 1 – 9 linear scale we observe that it yields correct results provided that the comparison of pair wise matrices show moderate importance (weak preference). For example, if:

A = 2xB
B = 3xC
Then,
C = 1/6xA

In order to be consistent and is applicable on this scale. Assuming 10 % acceptable inconsistency, then the range of acceptable values occur when:

$$B(c) = \sum_{i=1}^{k} B_i(c)$$

C= 1/7xA 3.2%
C= 1/5xA 0.4%
C= 1/4xA 2.0%
C= 1/3xA 5.6%

However, if:

A = 3xB
B = 4xC
Then,
C = 1/12xA

We cannot be consistent; unfortunately, this is not applicable, as we exceed the original scale. Considering even:

A = 9xB
B = 9xC
Then,
C = 1/81xA

The scale in this case squares. Here, we seek methods to overcome this constraint. Assuming that decision making lends itself to quantized preferences, then a statistical approach for, say, a decision that comprises of two elements and one member would be analogous to throwing a coin once, whereas the elements represent combinations and the members represent permutations. Therefore, if the number of members were increased it would be the same as if we increased the number of throws. For example, a decision comprising two elements and one member **(e = 2, i = 1):**

e-number of elements = 2
(i.e. a combination of 2 probabilities, e.g. Heads or Tails)

i-number of members = 1
(possible permutations)

Where,

$$\mathbf{e = \{1, 2\}}$$

Assuming that the events are:

$$\mathbf{p(1 \cap 2) = p(1) \times p(2)} \text{ i.e. independent}$$

And

$$\mathbf{p(1 \cup 2) = p(1) + p(2)} \text{ i.e. mutually exclusive}$$

For a decision comprising of three elements and one member, it would be analogous to a throw of a dice. As the number of members increase, so would the number of throws. In case that a decision comprises of four elements and one member, this would be analogous to a twenty-four faced dice thrown once; increasing the members, increases the number of throws. Therefore, if we use:

$$_{i}\mathbf{p}_{\mathbf{e}} = \mathbf{e!}_{i}$$

We end up with a dual parity degenerative quantum scale[1]. This translates to, when a pair of comparison matrixes are in the same preference direction then the resulting reciprocal matrix derives from the multiplication of the previous pairs. For example, if:

A = 9xB
B = 9xC
Then,
C = 1/81xA

When the pair of comparison matrixes is in the opposite preference directions then the resulting reciprocal matrix derives from the addition of the previous pairs. For example, if:

A = 9xB
B = 1/3xC
Then,
C = 6xA

6 Conclusions

We extended the design, development and implementation of collective user interfaces with multi modal interactions. We provided innovative techniques, methods and mechanisms for evaluating these interfaces and interactions. We obtained empirical data from real life situations coming from both the public and private sector. Most of all, this research was perceived as a methodology for facilitating human contact, building knowledge and skills for improving conditions and quality of work, formalizing international research collaboration for business and overall societal related quality and relevance. Community orientated, it will be an end for cultural enhancement of ubiquitous citizens whom their choices and opinions will provide consistency, sustainability and autonomy to the system itself.

References

Introduction

1. Saaty, T.: Models Methods and Applications of the Analytic Hierarchy Process. International Series. Kluwer Academic Publishers, Dordrecht (2001)
2. Saaty, T.: Deriving the AHP 1-9 Scale from First Principles. In: ISAHP 2001, Berne, Switzerland (2001)
3. Dwork, C., Kumar, R., Naor, M., Sivakumar, D.: Rank Aggregation Methods for the Web, Hong Kong, May 1-5 (2001)

Background and current Trends

1. Roure De, D.: Semantic Grid and Pervasive Computing, IPv6 Global Summit in Madrid (2003)
2. Belluzo, D.: http://www.informit.com/articles/article.aspx?p=165227
3. Gerstner, L.: http://en.wikipedia.org/wiki/Lou_Gerstner
4. Weiser, M.: http://en.wikipedia.org/wiki/Mark_Weiser
5. MIT Project Oxygen, http://www.oxygen.lcs.mit.edu/
6. Sun, http://www.sun.com
7. Microsoft, http://www.microsoft.com
8. Adobe, http://www.adobe.com
9. Oracle, http://www.oracle.com
10. List of Ubiquitous Research Centers
11. http://en.wikipedia.org/wiki/List_of_ubiquitous_computing_research_centers
12. Ubiquitous Computing, http://en.wikipedia.org/wiki/Ubiquitous_computing

13. Everyware, http://www.slideshare.net/dmje/everyware-the-future-is-already-here-its-just-not-well-distributed-yet
14. Computer Supported Cooperative Work, http://en.wikipedia.org/wiki/CSCW
15. Human Computer Interaction
16. http://en.wikipedia.org/wiki/Human-computer_interaction
17. Antoniades, A.K.: A Prototype Multi Criteria Group Decision Support System Using the Analytic Hierarchy Process. In: 1st International Scientific Conference on Information Technology and Quality (2004)
18. e-Government, http://www.epractice.eu/en/eGovernment
19. Bardram, E.J., Christensen, B.H.: Pervasive Computing Support for Hospitals: An Overview of the Activity Based Computing Project. IEEE Pervasive Computing 6(1), 44–51 (2007)
20. The Java EE Tutorial, http://java.sun.com/javaee/5/docs/tutorial/doc/index.html
21. p-Democracy, http://www.p-democracy.net (to be completed in September)
22. Java Authentication and Authorization Services
23. http://java.sun.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html

Everyware, a Pervasive Platform

1. Adam Greenfield, http://en.wikipedia.org/wiki/Adam_Greenfield
2. Java EE Containers, http://java.sun.com/javaee/5/docs/tutorial/doc/bnabo.html
3. Java ME, http://java.sun.com/javame/index.jsp
4. Eclipse, http://www.eclipse.org/
5. Tomcat Sever, http://www.coreservlets.com/Apache-Tomcat-Tutorial/eclipse.html
6. HTTP Server, http://httpd.apache.org/docs/2.0/
7. Taylor, T.: http://tomtaylor.co.uk/about/
8. RMI, http://java.sun.com/docs/books/tutorial/rmi/index.html
9. Bardram, E.J.: The Trouble with Login – On usability and Computer Security in Ubiquitous Computing. Personal and Ubiquitous Computing 9(6), 357–367 (2005)
10. Field studies (to be published)

Everyware Application: p-Democracy

1. Saaty, L.T., Forman, H.E.: The Hierarchon. A Dictionary of Hierarchies. V of the AHP Series. RWS Publication (2003) ISBN: 0-9620317-5-5

Group Monitoring in Mobile Ad-Hoc Networks

Albana Gaba, Spyros Voulgaris, and Maarten van Steen

Vrije Universiteit Amsterdam
{agaba,spyros,steen}@cs.vu.nl

Abstract. Maintaining bonds of cohesion between members of small groups in densely populated venues (e.g., a family in an amusement park, or some friends in a stadium) is increasingly gaining interest, both as a safety measure against malicious activity and as a convenient tool to prevent group splitting. Note that the use of mobile phones is often ruled out in such scenarios, due to extreme network load. Current solutions are typically based on custom installations of antennas, centralized control, and user devices with high transmission power.

In this work we propose a novel method for anonymously spreading presence information among group members in dense environments, based on a completely decentralized mobile ad hoc network approach. Our system operates independently of any infrastructure and is targetted at resource constrained, inexpensive and expendable user devices. Quite importantly, our system protects the privacy of its users, both for their safety and for ethical reasons.

Keywords: Ad hoc, MANET, group monitoring, presence management.

1 Introduction

Advancements in hardware technologies have led to tiny wireless devices equipped with sensing capabilities, location aware, and able to communicate with each other. These wireless devices have enabled many new applications running in various environments, from military to civilian, that typically monitor events in large scale.

In this paper we focus on the design issues required for building a system that allows people to monitor the presence of each other in crowded areas (e.g., families in an amusement park, friends in a concert). We envision a decentralized system where each person carries a wireless device, collectively forming an ad-hoc network. Group members exchange messages indicating presence information, like location, by relaying them through the ad-hoc network.

The described scenario imposes several requirements. First, sharing confidential data over an untrusted medium, such as the wireless network, may leak information about the persons to third parties. More specifically, adversaries can observe and manipulate the content of packets sent over the network. Even with encryption, though, adversaries may deduce sensitive information by analyzing the traffic of packets and/or by tracing packets from source to destination. In particular, location information of the parties involved in the communication

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 441–451, 2010.

can be deduced. In addition, the routing of packets may be disturbed. For instance, by selectively dropping packets, a targetted group may not receive any fresh messages from a specific member. In case the contents of the message are not well protected, messages may be altered or replayed in a way to mislead group members regarding their peers. For instance, a child that is far from its group, could appear to be in the vicinity.

In addition, the density of the network and the mobility may impact significantly the performance of the delivery of the messages, which may be degraded according to the conditions of the network. The system should be able to work even in harsh environment conditions and tolerate delays and packet loss. The work presented in this paper is independent of the underlying radio technology, as long as it supports message broadcasting. However, low-power radio devices are preferred to more energy-hungry radio technologies, such as Wi-Fi.

In this paper we present our ongoing work on autonomic group monitoring in highly populated areas. We discuss requirements and challenges that derive from building such a system, like issues related to the network characteristics, communication between nodes, etc. In particular, we focus on privacy and anonymity issues concerning group communication.

2 System Model

2.1 Overview

For our application, we assume a crowd of people each carrying a small networked device, such as an electronic badge. Each person belongs to one group and is capable of exchanging messages with its group members. In addition, we assume that there is no pre-installed communication infrastructure. This means that messages should be communicated through the network formed by the crowd as a whole. The main purpose of our application is to allow group members to monitor each other's presence. To this end, each group member periodically transmits presence information such as its relative or absolute location coordinates. This information can then be used by the receiver for further processing. For example, a recipient may conclude that a member is too far away from the others, or may deduce the movement of a group member, and so on. To make this work, we need to meet a number of rather stringent requirements.

These requirements are broadly grouped in the ones related to *privacy* and the *technical* ones, and are laid out in the following two sections.

2.2 Privacy Related Requirements

Privacy plays a central role to our application. In short, group members should share presence information among themselves and with no one else. That is, no data should leak to other nodes, including group member identities as well as the information exchanged.

Anonymity of Nodes. A fundamental aspect of privacy is the anonymity of group members. That is, the identity of the source and recipient(s) of aired messages should not be disclosed to adversary nodes. There are a number of reasons for that.

First, to prevent adversaries from tracking down individual persons. If an adversary is capable of recognizing the identity of the person who issued a message, he can use our application to track down that person based on the messages he is sending. This is crucial for safety. For instance, it may be possible to detect when group members are isolated from the rest of the group, and therefore more vulnerable. This is vertically opposite to the goals of our application, which aims at protecting persons from malicious activity.

Second, to prevent attacks directed at specific groups. By being able to read the sender or receiver identifiers in aired messages, an adversary could *selectively* tamper with the messages of a specific group. For instance, he could drop, delay, or corrupt messages of a particular group, or he could replay them with wrong information.

Finally, node anonymity is important for keeping group composition undisclosed to third parties. Exposing the sender and receiver identities in traveling messages could unmask group membership, by revealing the sender/receiver relationships.

It should be clear from the above that messages should not lead back to any node (sender/receiver) or group identifier. Therefore, source and destination nodes should remain anonymous.

Message Authenticity. It should not be possible for an adversary to *impersonate* a legitimate person, that is, generate messages that appear to be coming from that person. Consider a scenario where a member of a group is drifting away, while an adversary's instrumented device (falsely) assures the other members of the group that their friend is nearby. This would annul the principal goal of our application.

Thus, recipients of a message should be able to confirm the authenticity of the message. This implies some sort of encryption regarding the sender identity, as we will see in Section 4, that prevents adversaries from impersonating legitimate users. As it turns out, the goals of node anonymity and authenticity of messages are closely related.

Message Content Encryption. The information conveyed in the exchanged messages should not be exposed to adversaries. Similarly to message authenticity, this requires some sort of encryption of the messages, to avoid *eavesdropping*. If the content of the messages is not protected, then eavesdroppers can monitor the group members as if they were group members.

2.3 Technical Requirements

Here we list the technical requirements for our system.

Independence from Any Infrastructure. One of the basic requirements for our system is to operate in an autonomous, self-contained manner, not dependent on any type of custom infrastructure or telecommunication providers.

The system should be usable anywhere, without requiring the preinstallation of any type of infrastructure. Consider, for instance, a school trip to the countryside, a company picnic, a family visiting a crowded beach, or other outdoor activities. Financing the installation of infrastructure at such places would be a serious issue for the deployment of our system.

It can be argued, however, that in most developed countries GSM and GPRS coverage spans the whole land, including distant areas in the countryside. Even if we take GPRS for granted, the cost involved with it, as well as the need to have one mobile phone per monitored entity (e.g., children, pets, etc.) may be a restrictive factor. This becomes more clear in the scenario of a trip to a foreign country. Current roaming charges would form a prohibitive barrier to the frequent (once every few seconds) reporting of presence information. Additionally, our system should also work in very crowded areas, like a concert, where the capacity of the existing GSM infrastructure is usually exceeded.

Node Mobility and Density. The application is required to operate in highly mobile environments. Mobility is inherent in the scenarios we are targetting, such as amusements parks, shopping centers, etc.

Additionally, our system should operate well under high concentration of people, where infrastructure based networks typically run out of capacity.

Unobtrusive Devices. We target at tiny, unobtrusive devices (e.g., bracelets) that can be easily carried by anyone, including children or even pets. In addition, the devices are required to be inexpensive as this would allow them to be massively affordable. The small size of the devices imposes a serious limitation on their battery capacity, so minimal energy consumption is crucial to their sustainability. As a consequence, handheld devices such as smart phones, PDAs, etc., that rely on Wi-Fi medium access, are ruled out. The high energy consumption of Wi-Fi interfaces presents a significant barrier in building tiny, unobtrusive devices that keep communicating for a suffiently long duration (e.g., a full day or more).

A representative architecture that fits the aforementioned requirements is the resource-constrained, low-power architecture of the Berkeley nodes [1]. Equipped with an 8 MHz micro-controller processor, 10kB of RAM, 1 MB of external flash memory and a 256 kbps data rate radio, these devices can compute simple operations in an energy-efficient manner. They have shorter communication range, compared to Wi-Fi devices, that can reach up to 100 meters, but this is not an obstacle for the connectivity in our network as we assume highly populated networks.

Timely Delivery. It is important that people receive timely updates about the state of their group members. This implies that the ratio of undelivered packets should be kept low, and should gracefully degrade with the distance of group members. Furthermore, if the network reliability degrades, it should be detectable, allowing people to rely on other means for monitoring each other.

3 System Design

In this section we discuss the impact of the application requirements on the design decisions.

We consider the following *adversary model.* One or more adversaries eavesdrop the messages delivered through the wireless medium and, when necessary, move from one place to another. The adversaries, equipped with powerful devices, are capable of computing with high probability the direct (one-hop) sender of a message. To this end, special electronics, such as directional antennas and spectrum analyzers, can be used to compute the angle of arrival and the received signal strength of a message and infer its direct sender. Successively, in order to efficiently locate and track people, the adversaries may share this information with each other in a private way using long-range wireless communications and correlate the overheard data.

3.1 No Node Identifiers

Communication between nodes should not undermine the privacy of the people involved. Based on the messages nodes exchange, third parties should not be able to detect locations, motion patterns, or any data related to the nodes. Moreover, sender-receiver relationships, that is, the composition of groups, should not be revealed. This would allow adversaries to trace target people or even groups from distance.

Along these lines and in order to safeguard user anonymity, one of our design choices is to prevent node identities from appearing unencrypted in messages. Doing so would constitute a major threat to user anonymity, as explained below.

If the identity of nodes can be revealed to third parties, then their messages may be traced and therefore the privacy of individual nodes may be violated. Typically, a source node includes its ID in the clear in its messages so that they are recognized by the receivers. However, an adversary node can exploit this feature, and by standing nearby a target node it can figure out the ID of that node. Thereafter, this adversary, or a network of collaborating adversaries, could track that node in space and time by following the flow of its messages in the network. Additionally, they could selectively *suppress*, *corrupt*, *delay*, or *replay* at a different time messages of given nodes. Even worse, if the sender ID is accessible and the data is not protected well enough, an adversary could *impersonate* a legitimate user, sending misleading messages to its group partners. For instance, if location information is included in messages, an adversary could make a node appear to be nearby while it is far away, by impersonating it, or by replaying its old messages.

Group composition, that is, the set of source-destination relationships, should remain undisclosed to third parties. If it is possible to identify the source nodes of the messages (as seen before) and the nodes that compose a group (*communication patterns*), even if the exchanged data is not accessible, multiple adversaries can analyze the traffic of messages on the paths that link source nodes to destinations and monitor the locations and the movements of the whole group. As a consequence, it may be possible to detect when group members are isolated from the rest of the group. Moreover, similarly to what said about single nodes, the exchanged messages may be captured and suppressed selectively, but at a group level. For example a determined node can be isolated in a way that its messages are dropped for all the destinations. On the other hand, if the content of the messages is not protected, then eavesdroppers can monitor the group members just as internal group nodes.

3.2 No Point-to-Point Routing

The restriction on including unencrypted node IDs in messages has a direct impact on the applicability of classic routing protocols. Most point-to-point routing protocols operate based on addresses, and, at a minimum, the *recipient address* of a message should be readable by any intermediate node. As such, address-based point-to-point routing protocols are deemed unsuitable for our application.

Some point-to-point routing protocols, such as geographic routing [7], operate without using explicit node addresses. Even these protocols, however, are inappropriate for our application. For instance, in the case of geographic routing, disclosing the location of the destination—even without its address—is sufficient to reveal the actual person; let alone the difficulty of knowing a person's exact location to send it a message.

In the generic case of point-to-point routing, a team of collaborating adversaries could track a message from its source to its destination, inferring the group membership. Figuring out that a node is the source of a message is trivial to accomplish by capturing all messages broadcast around the node's location. If the message is first broadcast by the node, then this node is the source of the message. If it has been heard before, then this node is just forwarding that message. Similarly, for inferring the recipient, the adversaries could follow the propagation of a message until the last time it is forwarded. Unless the message was lost or some other routing problem occurred, the recipient is within one hop of the last node forwarding the message.

In addition to the privacy related issues preventing the use of routing, node mobility and network size further strengthen the arguments against it. Routing in dynamic networks is not very efficient, and often involves a large overhead in the type of floods to (re-)discover routes to relocated nodes.

3.3 Gossip-Based Message Propagation

A key design choice in our application is the use of gossiping to propagate messages. This is favored by a number of reasons in addition to the unsuitability of routing protocols discussed in the previous section.

First, gossiping is ideal for dense networks, as it completely eliminates the need for flooding. Each node broadcasts messages at a steady period, avoiding transmission bursts. Second, redundancy is an inherent property of gossiping. Redundancy is crucial for multihop communication in dynamic networks, such as the ones we are targeting here. This is particularly important in highly mobile

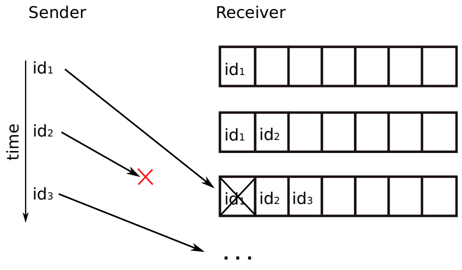


Fig. 1. Window of expected IDs

environments. Third, gossiping propagates a message without revealing its recipient. Finally, gossiping constitutes a very simple technique for disseminating information in a fully decentralized fashion, which makes it appealing for our large network of resource-constrained devices.

4 Anonymous Communications

Our goal is to design a system that allows nodes to send messages in a way that only the intended recipients are able to observe and decipher. Therefore, we propose the following protocol.

During its lifetime, each node uses IDs out of a custom *secret sequence* to mark its messages. The ID space is long enough to guarantee a unique ID per message, among contemporary messages, with very high probability. To establish an one-way communication between two nodes, the sender S shares in advance its secret sequence of IDs with the receiver R, and the two nodes synchronize their clocks. Given that messages are transmitted periodically, with a known period, the receiver R is in a position to know at any given moment what message IDs to expect in S's messages, as it can estimate which IDs from the sequence S used to mark its last few messages.

Under ideal conditions (i.e., no message losses, no delays), the receiver R would get the expected IDs (messages) from S on time and in the order they were sent. In practice, however, messages do get dropped, or experience variable delays otherwise, due to multi-hop propagation. To cope with network unreliability, R keeps a window of *expected* IDs from S. As shown in Fig. 1, at every interval R inserts the next ID from S's sequence to the window, which is also the ID S uses to mark its new message. As messages arrive, the IDs in the respective window are looked-up, and if matched, the message is known (with very high probability) to have originated at S. An ID (message) is considered to be lost when it does not arrive within a maximum time T. The window size may be dynamic depending on the latency of the network.

Rather than storing whole sequences of IDs, nodes use iterative functions that generate such sequences on the fly. In particular, we adopt Pseudo Random Number Generators (PRNG) for that goal. A PRNG is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is completely deterministic and can be reproduced by using the same set of initial values, called the PRNG's seed. The characteristics of PRNGs turn out to fit our requirements for sequences of one-time IDs, as shown below:

- *unpredictable*, by observing a sub-sequence of one-time IDs originated by a specific node it is hard to predict the successive ones,
- *unobservable*, by observing any sub-sequence of one-time IDs it is not possible to draw any conclusion about relationships between IDs,
- *reproducible*, it is possible to reproduce the same sequence of IDs by other nodes,
- *simple*, given the constrained resources of the nodes, it is required that inexpensive algorithms are employed to generate the sequence of IDs.

The result of employing a one-time ID for each message is that no information, like the sender or recipient identity, can be deduced by eavesdroppers who analyze the traffic of messages or trace them hop-by-hop. Exception is made when the adversary is within the communication range of a sender and can directly observe its messages. But even in this case, if adversaries trace the identified message, it is not possible to find the recipient. Also, since the successive messages have different IDs there is no new information gained by capturing one-hop messages.

4.1 Discussion

Pseudo Random Number Generators exist in a wide range and differ in complexity according to the purpose they are used for. For lack of space we will see only two of them. The simplest ones are the Linear Congruential Generators, mainly used for simulations. Successive values are computed by $id_{k+1} = (A * id_k + B) \ mod \ N$, where A, B, and N are fixed parameters, and id_0 is the seed. LCGs have shown to be predictable when *enough* consecutive output values are observed [3]. A more complex PRNG is Blum Blum Shub [2]. Successive values are computed by $id_{k+1} = id_k^2 \ mod \ N$, where N is a fixed product of two large primes and id_0 is the seed. BBS provides strong guarantees of unpredictability, but is slower than LCGs, as it requires that $log_2 n$ bits are extracted from each id_k. According to the characteristics of the system one may choose the PRNG that is best suitable.

Authentication of Messages. A node R accepts every incoming message whose ID matches the window of expected IDs of node S. In this context, we should consider the case that R might validate messages generated by other nodes, but whose ID happens to coincide with some entry in the window. To this end, the ratio between the ID space and the network size should be set appropriately in order to minimize the risk of collisions between IDs. But even when an ID collision occurs, it only affects an isolated message rather than the whole series of messages from a given sender.

Data Protection. As a result of employing one-time IDs, we obtain messages unobservable to anyone but the group members. This means that no correlation can be made between the overheard messages. Therefore, according to the level of confidentiality we want to achieve, if the exchanged information does not lead to any specific node in the network, we may opt to use inexpensive encryption algorithms (e.g., stream cyphers), if at all.

Alternative Solution. Using encryption would be an alternative to our protocol. Before sending a message, nodes would encrypt it entirely with a symmetric key shared with the intended recipients, making it unreadable for anyone else. However, a node would have to attempt to decrypt *every* message it sees, in search of decipherable messages encrypted by its friends. Although a viable solution, it appears to be more complex compared to our PRNG based approach. As we are striving for low power and resource constrained devices, we opt to employ the PNRG approach. Nevertheless, it is left as future work to assess the efficiency of each approach, particularly when the algorithms are implemented in hardware.

5 Related Work

The problem of node location privacy as a consequence of traffic analysis and packet tracing has increasingly gained the attention of the research community. In [4], Deng et al address the problem of hiding the location of the receiver (i.e., base station) in a sensor network. Assuming that the traffic of the whole network is directed towards the base station, they concentrate on protecting the system from traffic analysis through measurements of traffic rates at various locations. Randomized routing and fake message injection are introduced to prevent an adversary from locating the network sink based on the observed traffic patterns. The same problem of hiding the sink location in sensor networks is addressed in [5], with the difference that they focus on packet tracing attacks, which come as result of multi-hop deliveries from sources to the sink. In [6], the problem of source location privacy is studied in a sensor network. The adversary traces back the packets received at the base station, hop-by-hop up to the source. The authors introduce *phantom routing* that consists of a combination of random walk with flooding/shortest-path routing when the message approaches the base station.

In [9], the impact of anonymity as a result of mobility is studied and some anonymity-preserving routing protocols are compared. Anonymity in MANETs has been studied in ANODR [8], MASK [12], RIOMO [10], ARM [11]. These works concentrate on routing on demand in mobile ad-hoc networks. The basic idea behind anonymous routing is that nodes keep an entry for each anonymous RREQ they forward in order to recognize it on the way back (RREP) and forward it to the right neighbor. The network and computation assumptions these protocols make are prohibitely expensive to be adopted in resource-constrained networks. For instance, in ANODR, a fresh public/private key pair is generated for each RREQ by the forwarding nodes, and messages grow in size as they are forwarded along the path. Along these lines, the other protocols assume encryption/decryption of every RREQ and RREP message forwarded. In [12] large storage is required to keep a set of pseudonyms. In addition, the aforementioned protocols make assumptions such as limited mobility, reliable communication, and symmetric links, which are not realistic in our model.

6 Conclusions and Future Work

In this paper we sketched the design of a system for monitoring group members in a mobile ad-hoc network. After a first consideration of the factors that charachterize the system, we pointed out the possible constraints and challenges that such system might face. Particular focus is devoted to the privacy of nodes involved in these communications, such as location and sender-receiver identity. We proposed an anonymity scheme where nodes use anonymous messages that do not lead to any information concerning the communicating parties or related to other messages. The ultimate goal of the proposed system is to ensure unobservability of the messages exchanged between group members while adding low overhead in computation resources, storage or message size. In the future we propose to implement such system and run experiments on nodes to assess the efficiency of our protocol.

References

[1] http://webs.cs.berkeley.edu/tos/

[2] Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo random number generator. SIAM J. Comput. 15(2), 364–383 (1986)

[3] Boyar, J.: Inferring sequences produced by pseudo-random number generators. J. ACM 36(1), 129–141 (1989)

[4] Deng, J., Han, R., Mishra, S.: Countermeasures against traffic analysis attacks in wireless sensor networks. In: SECURECOMM 2005: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Washington, DC, USA, pp. 113–126. IEEE Computer Society, Los Alamitos (2005)

[5] Jian, Y., Chen, S., Zhang, Z., Zhang, L.: Protecting receiver-location privacy in wireless sensor networks. In: INFOCOM, pp. 1955–1963 (2007)

[6] Kamat, P., Zhang, Y., Trappe, W., Ozturk, C.: Enhancing source-location privacy in sensor network routing. In: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, June 2005, pp. 599–608 (2005)

[7] Karp, B., Kung, H.T.: Gpsr: greedy perimeter stateless routing for wireless networks. In: MobiCom 2000: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 243–254. ACM, New York (2000)

[8] Kong, J., Hong, X.: Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In: MobiHoc 2003: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pp. 291–302. ACM, New York (2003)

[9] Kong, J., Hong, X., Sanadidi, M.Y., Gerla, M.: Mobility changes anonymity: Mobile ad hoc networks need efficient anonymous routing. In: IEEE Symposium on Computers and Communications, pp. 57–62 (2005)

[10] Rahman, S.M.M., Nasser, N., Inomata, A., Okamoto, T., Mambo, M., Okamoto, E.: Anonymous authentication and secure communication protocol for wireless mobile ad hoc networks. John Wiley & Sons, Ltd., Chichester (2008)

[11] Seys, S., Preneel, B.: Arm: Anonymous routing protocol for mobile ad hoc networks. In: AINA 2006: Proceedings of the 20th International Conference on Advanced Information Networking and Applications, Washington, DC, USA, pp. 133–137. IEEE Computer Society, Los Alamitos (2006)

[12] Zhang, Y., Liu, W., Wenjing, L.: Anonymous communications in mobile ad hoc networks. In: INFOCOM 2005: 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (2005)

Author Index