Helmut Reimer
Norbert Pohlmann
Wolfgang Schneider *Eds.*

ISSE 2013 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2013 Conference

ISSE
INFORMATION SECURITY SOLUTIONS EUROPE

eema
www.eema.org

TeleTrusT
Pioneers in IT security.

Springer Vieweg

ISSE 2013 Securing Electronic Business Processes

Helmut Reimer • Norbert Pohlmann
Wolfgang Schneider (Eds.)

ISSE 2013 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2013 Conference

Springer Vieweg

Editors

Helmut Reimer
TeleTrusT – Bundesverband IT-Sicherheit e.V.
Erfurt, Germany

Wolfgang Schneider
Darmstadt, Germany

Norbert Pohlmann
Gelsenkirchen, Germany

ISBN 978-3-658-03370-5
ISBN 978-3-658-03371-2 (eBook)
DOI 10.1007/978-3-658-03371-2

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2013950028

Springer Vieweg

Typesetting: Oliver Reimer, Jena

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Contents

Human Factors, Awareness & Privacy, Regulations & Policies 59

Security Management 131

Cybersecurity, Cybercrime, Critical Infrastructures 195

Mobile Security & Applications

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the tenth ISSE book – another mark of the event's success – and with about 25 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ammar Alkassar**, Sirrix AG (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **John Colley**, EMEA & (ISC)2 (United Kingdom)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, KU Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Michael Hartmann**, SAP (Germany)
- **Jeremy Hilton**, Cranfield University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Marc Kleff**, Siemens Enterprise Communications (Germany)

- **Hasse Kristiansen**, Ernst & Young (Norway)
- **Jaap Kuipers**, Id Network (The Netherlands)
- **Manuel Medina**, ENISA
- **Patrick Michaelis**, Research In Motion (Germany)
- **Norbert Pohlmann** (chairman), Institute for Internet Security, Westfälische Hochschule, Gelsenkirchen (Germany)
- **Bart Preneel**, KU Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Marc Sel,** PWC (Belgium)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **Claire Vishik**, Intel (United Kingdom)
- **Erik R. van Zuuren**, Deloitte (Belgium)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

TeleTrusT – IT Security Association Germany

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities.

TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is carrier of the "European Bridge CA" (provision of public key certificates for secure e-mail communication), the quality seal "IT Security made in Germany" and runs the IT expert certification program "TeleTrusT Information Security Professional (T.I.S.P.)". TeleTrusT is member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year's European Security Conference ISSE is being organized in collaboration with eema and LSEC and supported by the European Commission and ENISA.

Contact:

TeleTrusT – IT Security Association Germany
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17, 10115 Berlin, GERMANY
Tel.: +49 30 4005 4306, Fax: +49 30 4005 4311
http://www.teletrust.de

EEMA

Since 1987 EEMA has been Europe's leading independent, association for eID and Security. To keep in step with industry developments and member requirements, it recently reinvented itself to focus more specifically on Cyber security and eID technologies and services. Since then, EEMA has become the leading eID and Identity forum in Europe operating across both private and public sector in Europe, working with its European members, governmental bodies, partners, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA also partners with the European Commission, ENISA, TeleTrusT, BCS, LSec and TDL, and involves its members in collaborative European commission projects such as STORK 1 & 2 (eID interoperability) pan-European project; a three year project – SSEDIC – Scoping the Single European Digital Identity Community and has recently won two other FP7 projects – Future ID and Cloud for Europe.

EEMA is the lead organization for the renowned ISSE conference (Information and Security Solutions Europe) and conducts many studies for the EU on interoperability of eID and other related issues. EEMA holds a number of ID related conferences during the year and these are well attended by its members and non-members alike for instance "Trust in the Digital World" in partnership with TDL and "Digital Enterprise Europe" as well as many one day events throughout Europe.

EEMA's remit is to educate and inform over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its members is available to other members free of charge.

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a member of EEMA, and any employee of that organisation is then able to participate in EEMA activities. Examples of organisations taking advantage of EEMA membership are Siemens, Hoffman la Roche, Volvo, ING, RaboBank, KPMG, Deloitte, Novartis, TOTAL, Ericson, Adobe, Magyar Telecom Rt, Nets, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

Cloud Security, Trust Services, eId & Access Management

Draft of a Dynamic Malware Detection System on Trustworthy Endpoints

Andreas Speier · Christofer Fein · David Bothe
Eric Reich · Norbert Pohlmann

Institute for Internet Security
Westphalian University of Applied Sciences Gelsenkirchen
{speier | fein | bothe | reich | pohlmann}@internet-sicherheit.de

Abstract

Malware infected computer systems can be found with increasing evidence in private and commercial fields of use. Always exposed to the risk of a "Lying End-Point", an already manipulated security application that pretends to run on a clean computer system, the demand for new security solutions continues to rise. Project iTES ("innovative Trustworthy Endpoint Security"), government-funded by the German Federal Ministry of Education and Research, introduces a new system to enhance security while preserving usability. Based on an existing virtualized system which diversifies the software to a specific form of use, the project aims to develop new sensors to monitor the system dynamically and deliver real-time responses.

1 Introduction

Malware infected computer systems can be found with increasing evidence in private and commercial fields of use. Even technically advanced countries fall victim to severe damages caused by malicious software. Prevention of such attacks has to result in hardening computer systems against malware activity. Critical applications like online banking and e-commerce introduce a profitable field for criminal individuals, which significantly raises the need for trusted data processing even more. Conventional security solutions available today already offer thorough countermeasures, but are often exposed to manipulation by malware themselves. Always being subject to the risk of a "Lying End-Point", an already manipulated security application that pretends to run on a clean computer system [SSDD07], the demand for new security solutions continues to rise.

Project iTES[1] introduces a new system to enhance security while preserving usability. The system architecture needs to guarantee the reliability of a security solution with provable integrity to prevent attacks. Typical computer systems will be assembled regarding private used and professional used software components to serve as a reference for behavior analysis (see section 2.4).

Common Trusted Computing technologies combined with virtualization create a secure software environment to isolate malware, which provides a basis for innovative and trustworthy security systems. A core intention of iTES is to combine already existing security technologies and

[1] http://ites-project.org

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_1, © Springer Fachmedien Wiesbaden 2013

advance them through innovative developments. Continuous usage of security software will be fortified by virtualization and integrity-measures of its components. Another important part is the development of software sensors (see section 2.5) for dynamic malware behavior analysis and detection by a security software guest system.

In section 2.3 the architecture of a physical client is outlined. The inner structure, like the main security concept (see section 2.1-2.2) and the software sensors (see section 2.5) are described in detail. The software separation is mentioned in section 2.3.

The secure environment with the multiple client concept and the central component are described in general in section 3.

2 System Architecture

Common trusted computing technologies offer manipulation detection and possibilities to attest configurations of computer systems. Virtualization adds the separation of single applications within strong isolated compartments. The hypervisor is the interface between the host system and a virtualized guest system. In our system this interface is also intended to integrate sensors to perform dynamic malware analysis (see section 2.4).

2.1 Integrity

Proving the integrity is one of the main goals in securing a system. The integrity of the guest system has to be examined before the startup routine by calculating checksums of the virtual machine configuration files. A complete check of the virtual machine image is a time consuming task and may take several minutes as shown in table 1. In the shown example a single 13 GB OS image has been subjected to the hash algorithms shown, on a middle class business notebook using some well-known hash algorithms. On a system as described in this paper, there will be at least four guest system images. Therefore a smarter integrity check has to be developed to perform rapidly before the virtual machines are permissible to be started. A pre-boot investigation will be done on security relevant components of the virtualized system. These components have to be compared with their pre-defined secure states. A deviation from the defined initial state has to be identified as abnormal configuration [Pohl08]. In this case the virtual machines start procedure has to be denied and the configuration of the system as a whole must be reestablished as described in section 2.2.

Table 1: Mean checksum calculation time (s) on 13GB image file, read from disk

Algorithm / Disk Technology	**HDD**	**SSD**
md5	~112 s	~49 s
sha1	~128 s	~85 s
sha256	~117 s	~51 s
sha512	~120 s	~61 s

2.2 Availability

System security includes integrity and confidentiality, but also to steadily provide defined services [ALRL04]. Abnormal changes to a system can influence the availability of a special service, or the system itself. In this case the service or the whole system must be restored. The work of this project will also concentrate on developing several ways for system remediation. Simply restoring a previous virtual machine snapshot has to be the worst case method in case of a detected malicious anomaly. This leads to the loss of all user data, stored on the specific virtual machine. Developing intelligent methods to restore minor parts of the system is one aim of this project.

2.3 Client Architecture

The architecture needs a separated compartments for different types of tasks. Implementing these environments provides strong isolation that can – in case of an infection – prevent malware from spreading inside the system and affecting security critical components. Malware in one compartment can compromise a single virtual machine, but not the entire system [Micr10].

Therefore one of the first steps during the project was to identify the different software products frequently used on computer systems in home and work environments. We analyzed different usage statistics to compile a comprehensive list of employed software packages and their corresponding versions by the end of September 2012 ([StOwl12], [Stai12], [Webm12]). Due to the virtualized architecture of the client system we had to categorize the software into different compartments. The aims of the different compartments were chosen to achieve the highest possible usability while prioritizing security concerns. The main software categories for the user of the system are:

- Internet related software
- Office related software
- Work related software
- Banking software
- Browser
- Email

The client architecture will include an additional compartment for security and data analysis software as described in section 2.4.

2.3.1 Internet Related Software

Internet related software is software that needs to be connected to the Internet to perform well. This includes instant messengers for communication, P2P software for file sharing or content on demand services to retrieve multimedia content. The connection to the Internet is a high risk for software and data stored inside this compartment. Using sensitive data inside this compartment is not recommended.

2.3.2 Office Related Software

Office related software is software that is used in a secure work environment and can run without a direct Internet connection. This includes office suites [Webm12], document readers, multimedia software and image processing tools. The aim is to separate common malware infected software from the Internet to preserve the security of sensible data, e.g. invoices transmitted as PDF documents.

2.3.3 Work Related Software

Special applications are needed in specific professional fields. Different types of software like CAD tools, accounting or IDE software can be installed in this compartment, which is built to isolate this mainly unknown and not controlled software.

2.3.4 Banking Software

A banking suite is placed in a special compartment. Due to security reasons, no other software is installed alongside. Banking tasks can be performed securely without being influenced by security issues caused by other software.

2.3.5 Browser

A special compartment is erected to support secure Internet browsing. The separation from other software components impedes infection of and from these components. By enforcing this barrier between the different tasks, the security for handling sensitive tasks like e-commerce is provided.

2.3.6 Email

This compartment is made for email handling only. A secure e-mail client provides a barrier for malware distributed by email attachments like keyloggers and scareware. The combination with a policy based data flow management results in a usable environment regarding the handling of attachments, which can be opened in other appropriate compartments.

2.4 Client Security

It is possible to group the different compartments into security level based domains, providing different levels of connectivity, e.g. to the network as illustrated in figure 1.

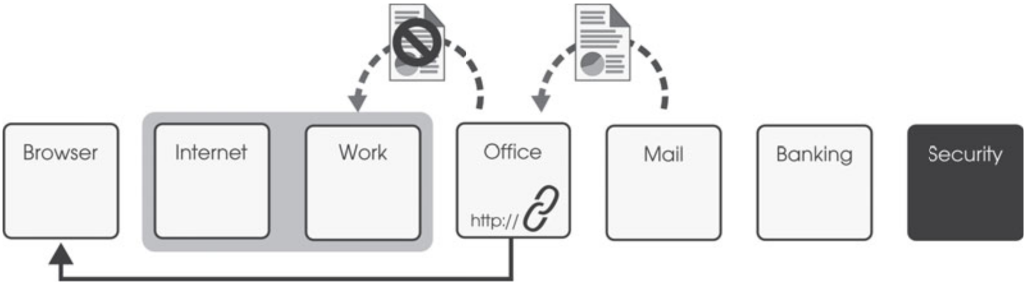


Fig. 1: Compartment Overview

The host internal communication between these domains, e.g. for copy and paste functions, are managed by a predefined set of patterns. For usability reasons, the functionality of clicking a link in an offline compartment or the ability to send files as mail attachments is provided through a policy based data flow management. This will verify the source of the data and redirect it based on its internal rules to the browsing or email compartment. Consider a situation where an employee receives a purchase order by email containing a HTTPS-link to a prepared shopping cart. Using this web-link, the system will enforce a forwarding to a secure browsing compartment by some policy. This avoids risks like the interception of credit card information possible in an insecure environment.

Another special type of compartment is the “High Security Compartment” providing an isolated environment for security related software such as firewall, anti-virus and sensor data processing software. Communication with this compartment is only allowed in one direction for sensor data (see section 5). The security compartment is not usable for the standard user, but for the system manager. This inhibits accidental changes and targeted attacks of malware against security software [MSMP10].

A conservative anti-virus tool matches the signatures of a specific file with its database to identify and classify malware. These signatures are created in an automated way by security software vendors on known malware samples. The Problem is, that obfuscated malware can change the binary code, with the result that the signature changes [ESKK08]. If this sample was not found by security software before, the malware can perform the intended malicious actions on a system. The approach of analyzing malware without its execution is called static analysis.

Static analysis can be performed on different representations like source code or binary code. Due to the restricted availability of malware source code, static analysis on binary code leads to multiple problems e.g. in context of self-modifying malware and runtime dependent execution values [ESKK08].

The second approach is to analyze the runtime behavior of malware within a running environment. This is called dynamic malware analysis. Dynamic analysis is a way to observe the action of executed malware on different ways. This includes e. g. function call monitoring, function parameter analysis, information flow tracking and instruction tracing [ESKK08].

Our aim is to transfer dynamic malware analysis into a trustworthy system of endpoints in combination with conservative static analysis techniques to get a real time response system. Intensive data analysis and gathering data with the assistance of software sensors are not resource-efficient tasks for a system with virtual guests. One professed goal is to preserve usability, while enhance security by behavior analysis.

2.5 Software Sensors

In general, software sensors in this project can be divided into two categories: in-box and out-box sensors.

In-box sensors are placed inside the virtual machine. The gathered data from this location is mainly generated in the user space and sent to the analysis software residing inside the “High Security Compartment”.

The disadvantage of internal sensors is the danger of them being manipulated by malware into generating a benign data stream. This problem is known as the “Lying End-Point” [SSDD07]. To face this issue the project also uses out-box sensors, which, assuming a correct working hypervisor, cannot be manipulated by running malware inside the virtual machine. The aim is to produce a corresponding out-box sensor for each data flow an in-box sensor produces. This complement is used to validate the internal information flow. Manipulation of the in-box sensors should be recognized by this approach.

The developed sensors will be evaluated for their usability in productive systems by the following concerns: In-box sensors are also in danger of being detected by malware scanning the system for security software and may incite a different behavior. The development of out-box sensors for productive systems is very important, because they cannot be detected by malware searching for security software. These sensors will use a hypervisor interface for monitoring vital parts of the guest system by using virtual machine introspection [GaRo03]. The disadvantage of out-box sensors is that they are more cost intensive in terms of system resources.

3 Overall Architecture

The overall architecture is modeled with a company like environment in mind, employing several physical client systems with a central management entity. This architecture provides some advantages over a stand-alone solution: Changes in the compartment arrangement can be managed easily from a central instance, enabling convenient administration and a consistent security policy throughout the entire system. The centralized management of the compartment configuration improves security by preventing misconfiguration of individual client systems.

Observing a single client only yields a limited view of its behavior, making it difficult to identify malicious activities solely relying on the analysis performed inside its own "High Security Compartment". To improve the classification of behavior the gathered data should optionally be sent to a central entity called the "Central Component". By aggregating the data generated by multiple client systems comparison and anomaly detection methods can be employed, allowing a vastly improved a broader view on the global system state.

The communication between client nodes and the central entity should be performed using two different modes of operation. A verbose mode will be used to transmit every collected data item, yielding a vast amount of input data e.g. for machine learning algorithms.

A less communication intense approach will only transmit behavioral records once an anomaly has already been detected by the client sided "High Security Compartment". The data then is subjected to further analysis by the "Central Component".

Due to the client being able to run in not trustworthy environments, the entire communication traffic will be protected using TLS, providing the confidentiality of the data and the authenticity of the client's identity. For the purposes of authenticity, digital certificates will be used, which provide the verifiability of the client's identity.

4 Conclusion

Behavior sensitive malware analysis on physical clients is a major step forward in security system development. Our system architecture will combine this dynamic approach with a detection technique based on the experience of multiple clients, trusted computing approaches and an arrangement of virtual guests in on one physical client.

First detection will be done with analysis software in the “High Security Compartments” on each physical client. A system wide entity, the “Central Component”, will gather all information about the state of each physical client. Optionally an auxiliary analysis will be made on this high performance computer system. Every anomalous incident will be identified and classified to gather information for all clients of the system. The use of virtual machines for different software classes will prevent the spreading of malware. Trusted computing technologies like assurance of virtual image integrity will help to attest a secure security state of the whole system.

The main theoretical design work for this framework is done and the implementation is in progress. A usable prototype with underlying distributed system will be available soon.

The present overview of the project benefits from the input of student assistants and our project partners. These are: Chair of System Security (Ruhr University Bochum), Sirrix AG security technologies and Avira Operations GmbH & Co. KG. We also thank the German Federal Ministry of Education and Research for funding.

References

[ALRL04] Avizienis, Algirdas and Laprie, Jean-Claude. and Randell, Brian and Landwehr, Carl: Basic Concepts and Taxonomy of Dependable and Secure. In IEEE Transactions on Dependable and Secure Computing Vol. 1, No. 1. 2004, S. 11-33.

[ESKK08] Egele, Manuel and Scholte, Theodoor and Kirda, Engin and Kruegel, Christopher: A survey on automated dynamic malware-analysis techniques and tools. In: ACM Computing Surveys, vol. 44. s.l. : ACM New York, 2008.

[GaRo03] Garfinkel, Tal and Rosenblum, Mendel. A virtual machine introspection based architecture for intrusion detection. In: Proc. Network and Distributet Systems Security Symposium. 2003.

[Micr10] Microsoft. Intel TXT Homepage. [Online] 29. 04 2010.

[MSMP10] Microsoft. Microsoft Malware Protection Center – Encyclopedia TrojanDownloader:Win32/Perka.A. [Online] 29. 04 2010.

[Pohl08] Pohlmann, Norbert. Trusted computing. Ein Weg zu neuen IT-Sicherheitsarchitekturen. s.l. : Vieweg, 2008.

[SSDD07] Sahita, Ravi and Savagaonkar, Uday R. and Dewan, Prashant and Durham, David: Mitigating the Lying-Endpoint Problem in Virtualized Network Access Frameworks. In: Managing Virtualization of Networks and Services. Berlin, Heidelberg : Springer, 2007, S. 135-146.

[Stai12] Statista.com. Statista Messenger Statistics. [Online] 10. 10. 2012.

[StOw12] StatOwl.com. StatOwl Browser Statistics. [Online] 12. 10 2012.

[Webm12] WebmasterPro.com. WebmasterPro Office Suits Statistics. [Online] 10. 10. 2012.

The Evolution of Authentication

Rolf Lindemann

4151 Middlefield Road, Palo Alto 94303, CA, USA
Nok Nok Labs, Inc.
rolf@noknok.com

Abstract

An analysis of 6 million accounts showed that 10,000 common passwords would have access to 99.8% of the accounts. When looking at passwords for banking accounts, it can be found that 73% of users shared their online banking password with at least one non-financial site, which means that when the non-banking site gets hacked, the banking account is threatened. And it's not only about security. According to a recent study conducted by the Ponemon Institute, more than 45% of the online transactions fail "Very Frequently" or "Frequently" due to authentication problems. Passwords do not work, yet no other technologies have been broadly deployed, why is that?

Current alternative technologies require their respective proprietary server technology. The current authentication architecture therefore consists of 'silos' comprising the authentication method, the related client implementation and the related server technology. Instead of having a competition for better user authentication methods, authentication companies are faced with a battle for the best server technology.

Other current challenges with Authentication include the need for flexibility. Today it is used for electronically initiating high value money transactions and for accessing the personal purchase history in an online bookshop. The security needs are different. The ongoing adoption of mobile devices and the BYOD trend lead to an increasingly heterogeneous authentication landscape. There is no one approach that can meet these diverse requirements.

The FIDO Alliance, a new industry working group, has been founded to define an open, interoperable set of mechanisms that reduce the reliance on passwords.

1 Motivation

Passwords don't work: In 2007, the average user had 25 accounts, used 6.5 passwords and performed logins 8 times a day [1]. Today, things are much worse. An analysis of 6 million accounts showed that 10,000 common passwords would have access to 99.8% of the accounts [2]. This basically means that only 0.2% of the users chose strong passwords and it means that passwords provide an effective security equivalent to 5 digit PINs. Even when looking at passwords for banking accounts only, it can be found that 73% of users shared their online banking password with at least one non-financial site [3], which means that when the non-banking site gets hacked, the banking account is threatened.

"Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks." [4].

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_2, © Springer Fachmedien Wiesbaden 2013

The password problem seems to be an important issue to solve: "Account and service hijacking, usually with stolen credentials, remains a top threat" [4]. It's not only about security. According to a recent study, more than 45% of the online transactions fail "Very Frequently" or "Frequently" due to authentication problems [5].

Several proposals to replace passwords have been made. A good analysis can be found in [6].

Silos of Authentication: Current alternative technologies require their respective proprietary server technology. The current authentication architecture therefore consists of silos comprising the authentication method, the related client implementation and the related server technology.

Innovative authentication methods proposed by the research community are not widely deployed, as in addition to the client implementation the complete server soft-ware needs to be implemented and deployed. Instead of having a competition for better user authentication methods, authentication companies are faced with a battle for the best server technology.

Heterogeneous Authentication Needs: Authentication is used for electronically initiating high value money transactions and for accessing the personal purchase history in an online bookshop. The security needs are different.

Users might authenticate using standalone PCs, tablets or smart phones. The employer might control some devices; others might be controlled by the user [7]. Increased adoption of mobile devices and the BYOD trend lead to an increasingly heterogeneous authentication landscape. The one authentication method satisfying all needs seems to be out of reach.

Trustworthy Client Environment: Client side malware could capture and disclose passwords or OTPs. It could alter transactions to be confirmed after being displayed or it could misuse authenticated communication channels to perform unintended actions. Authentication – even with username and password – needs at least one trustworthy component at the client side.

2 Related Work

A survey of (basic) authentication protocols can be found in [8]. The principle of hardware attestation is mentioned in [9] and it has been implemented and widely deployed by Trusted Platform Modules (TPMs).

As well as research into specific user authentication methods, the research community has tried to standardize authentication. The following standards are related:

- PKCS#15, achieving smart card profile interoperability by introducing a meta card profile;
- PKCS#11 (RSA Laboratories, 2009), achieving cryptographic token interoperability by providing a unified API;
- GSS-API (RFC 1508, RFC 2078, RFC 2743, Kitten working group), generic security service API. Achieving interoperability by allowing applications to use a shared module, i.e. effectively reducing the number of implementations;
- ISO/IEC 24727 is a set of programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use.

The aspect of supporting a variety of authentication methods for network access authentication is approached by the Extensible Authentication Protocol (EAP, RFC 3748). This protocol is designed for situations in which IP layer connectivity may not be available. "Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED" [10].

The Initiative for Open Authentication (OATH) is an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication (see www.openauthentication.org). Besides the OATH Reference Architecture [11], this initiative has published standards documents regarding an HMAC-Based OTP Algorithm (RFC 4226), Time-based One-time password Algorithm (RFC 6238), OATH Challenge/Response Algorithm (RFC 6287), and two pro-visioning standards (Portable Symmetric Key Container RFC 6030 and Dynamic Symmetric Key Provisioning Protocol RFC 6063).

In the case that a user has authenticated to the first relying party (typically called Identity Provider, IdP), this authentication can be federated to other relying parties (® Federation). Popular federation protocols are SAML, OpenID, and OpenID Connect. Related to these federation protocols is the web authorization protocol OAuth. An initial authentication (of the resource owner in this case) is leveraged here as well.

The FIDO protocol is concerned with authenticating the user to the first relying party ("first-mile authentication"); federation is about leveraging this "first-mile authentication" to other relying parties ("second mile authentication").

3 The FIDO Approach

We propose to (a) separate the user authentication method from the authentication protocol and (b) to define an attestation method in order to proof the FIDO Authenticator type to the relying party. Given this information, the relying party is able to infer the related assurance level (e.g. as defined in [12]. The assurance level can be fed into internal risk management systems. The relying party can then add implicit authentication methods as needed.

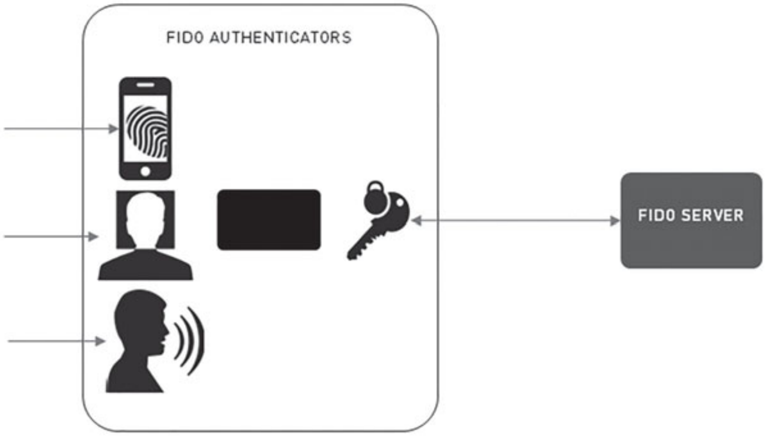


Fig. 1: Mapping Arbitrary User Authentication Methods to Cryptographic Authentication

In the FIDO approach, standardized challenge response based cryptographic authentication schemes are used between the FIDO Authenticator (controlled by the user) and the FIDO Server (controlled by the relying party). The FIDO Authenticator can implement any user authentication method, but it has to cryptographically attest itself to the relying party. The security relevant functions are centralized into the FIDO Authenticator.

3.1 FIDO Protocol

Starting from this challenge response based authentication scheme, the FIDO Universal Authentication Factor protocol supports the following functionality:

1. Discovery
2. Registration
3. Authentication
4. Transaction Confirmation

The discovery enables relying parties to understand the user authentication methods (more specifically the FIDO Authenticators) supported by the FIDO User Device. The relying party can specify a policy for selecting FIDO Authenticators best suited for the specific purpose.

The Registration operation binds the FIDO Authenticator to a specific entity. This might be an existing user identity already present in the system or it might be a user identity to be created.

The Authentication operation supports a single or multiple FIDO Authenticators to be involved. Each FIDO Authenticator might be implemented to represent either simple or strong authentication / two factor authentication as defined by [13] [14]. The Authentication operation is used to establish an authenticated channel between the Browser / App and the relying party Web Server.

The Transaction Confirmation allows the user to see and authenticate a particular well-defined transaction to the relying party. It is more secure as it doesn't rely on a Web Browser / App to not misuse an authenticated channel.

This leads to the following reference architecture:

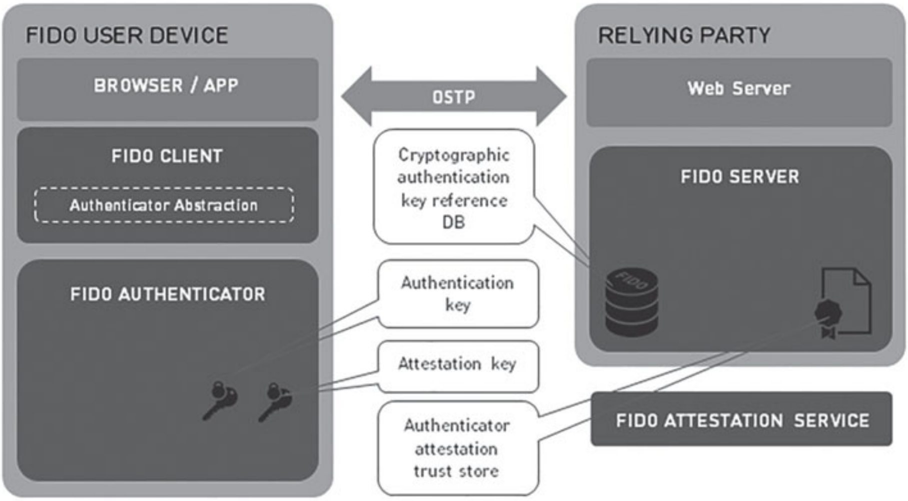
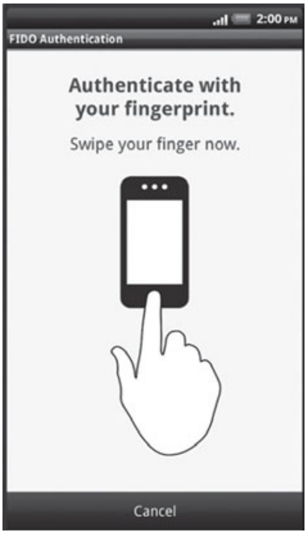


Fig. 2: FIDO Building Blocks

The FIDO Authenticator is a concept. It might be implemented as a software component running on the FIDO User Device, it might be implemented as a dedicated hard-ware token (e.g. smart card or USB crypto device), it might be implemented as software leveraging cryptographic capabilities of TPMs or Secure Elements or it might even be implemented as software running inside a Trusted Execution Environment.

The User Authentication method could leverage any hardware support available on the FIDO User Device, e.g. Microphones (® Speaker Recognition), Cameras (® Face Recognition), Fingerprint Sensors, or behavioral biometrics, see [15] [16].

3.2 Impact on User Experience



Authenticate with your fingerprint.

Swipe your finger now.

Fig 3: FIDO Authenticator

The user experience is mainly dominated by the user authentication method. For example, entering strong passwords on a smart phone leads to bad user experience [17]. Bad user experience might lead to poor security as many users opt for convenience rather than security [18].

FIDO Authenticators could implement any user authentication method. Such methods can be optimized for particular use cases and for the devices they are running on. In some situations, the user authentication method should be non-intrusive, so continuous authentication [19] [20] could be an option. In other situations a more precise user authentication method might be desirable, so the use of fingerprints or dedicated hardware tokens (such as smart cards) might be more suitable.

Due to the separation of user authentication method and authentication protocol, the change of the user method doesn't have any impact on the authentication server – as long as the assurance level is acceptable in the given context.

3.3 Attestation

Passwords, OTPs and other bearer tokens [21] can be submitted by legitimate users or phishing servers. For the risk of a transaction, this makes a significant difference.

The relying party is typically interested in estimating the risk of a transaction. This risk depends on the transaction volume and on the assurance level of the authentication. The assurance level depends on (a) the authentication method and (b) the certainty that the legitimate user controls the relevant portions of the client device. In the case of Transaction Confirmation (see above), this could be limited to the FIDO Authenticator. In the case of Authentication it will also include the Browser / App or User Agent in general. Risk based authentication [22] methods try to estimate (b). Authenticator attestation provides a cryptographic proof of the FIDO Authenticator being used to the relying party.

Using hardware attestation is not new, e.g. see [23]. In Public Key Infrastructures (PKIs), the hardware verification is typically being performed by the Certificate Authority before issuing the user certificate. The device policy is typically included into the user certificate as Certificate Policy OID (e.g. "id-fpki-certpcy-pivi-hardware" in the case of Federal Bridge CA, see [24]). User registration/identification and hardware attestation are combined into a single certificate. Relying parties verify such certificate policies included in the user certificate when validating the user certificates.

In non-PKI environments, hardware attestation and user registration/identification have to be separated. Trusted platform modules already support the concept of (pure) attestation [25] [26].

4 The Need for a Trusted Client Side Component

As previously mentioned, authentication requires at least one trustworthy client side component. In the case of FIDO this is the FIDO Authenticator. The security relevant functions are centralized into it. The most important security functions are:

1. Securely maintaining the attestation key and only using it for attesting newly generated authentication keys.
2. Securely maintaining the cryptographic authentication keys and
    a. Enforcing proper user authentication before unlocking the authentication key for authentications and
    b. Restricting its usage to cryptographic operations on defined clear-text message structures.

Use of secure hardware will significantly improve overall assurance level.

Existing secure hardware platforms include Smart Cards [27], TPMs [28], Secure Elements [29], and Trusted Execution Environments (TEEs [30]).

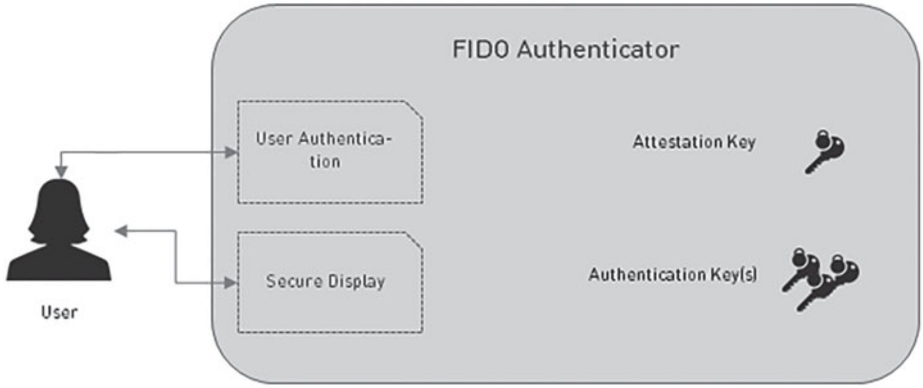


Fig. 4: Logical FIDO Authenticator Architecture

Some secure hardware can be accessed through standardized APIs e.g. PKCS#11 [31], or Microsoft Crypto API Next Generation [32]. Such APIs allow secure generation and storage of (authentication) keys (e.g. RSA keys). However, as the concept of attestation is missing by those APIs, there is no way for a relying party to be sure that a key has been generated by a specific secure hardware. Software generated keys would look the same.

Other secure hardware, e.g. ISO7816 compliant smart cards, or TPMs either sup-port the concept of attestation by default (TPMs) or can be initialized to support that concept (e.g. by using secure messaging). For Java Cards (Oracle), applets can be implemented to provide the security related functions of an Authenticator, i.e. Attestation, Authentication and PIN based user authentication.

Implementing all aspects of the FIDO Authenticator (i.e. User Authentication, Secure Display, Authentication and Attestation) in a TEE *and* storing the keys in a Secure Element exclusively accessible by a FIDO Authenticator Trusted Application would lead to the highest assurance level.

5 Conclusion

We have presented a new authentication framework providing an effective separation between the local user-to-authenticator authentication and the authenticator-to-relying party authentication. It supports a broad range of authentication methods and assurance levels while still letting the relying party define the acceptable assurance level for a particular context. This framework complements federation protocols by providing a solid basis for the "first-mile authentication".

The FIDO authentication framework is designed to support several important security and privacy properties, including non-linkability, resilience to leaks from other verifiers, resilience to phishing, no trusted third party etc. (see [6] for definition of these terms).

Based on this framework, relying parties can deploy even novel user authentication methods without changing the server side infrastructure.

Further development of this framework is driven by the FIDO Alliance (www.fidoalliance.org).

References

[1] Dinei Florêncio and Cormac Herley, Microsoft Research, „A Large-Scale Study of Web Password Habits," Redmond, 2007.

[2] M. Burnett, „More Top Worst Passwords," 20 June 2011. [Online]. Available: http://xato.net/passwords/more-top-worst-passwords/. [Accessed 3 April 2013].

[3] Trusteer, Inc., „Reused Login Credentials," New York, 2010.

[4] Cloud Security Alliance, „Top Threats to Cloud Computing, v1.0," 2010.

[5] Ponemon Institute LLC, „Moving Beyond Passwords: Consumer Attitudes on Online Authentcation – A Study of US, UK and German Consumers," 2013.

[6] C. H. P. C. v. O. F. S. Joseph Bonneau, "The Quest to Replace Passwords – A Framework for Comparative Evaluation of Web Authentication Schemes," in Proceedings of IEEE Symposium on Security and Privacy, Oakland, 2012.

[7] David A. Willis, Gartner, „Bring Your Own Device: The Facts and the Future," Gartner, 2013.

[8] J. C. a. J. Jacob, „A Survey of Authentication Protocol Literature: Version 1.0," 1997.

[9] Benjie Chen and Robert Morris; MIT Laboratory for Computer Science, "Certifying Program Execution with Secure Processors," in USENIX HotOS Workshop, 2003.

[10] B. Aboba, Microsoft; L. Blunk, Merit Network, Inc.; J. Vollbrecht, Vollbrecht Consulting LLC; J. Carlson, Sun; H. Levkowetz, ipUnplugged, „Extensible Authentication Protocol (EAP), RFC3748," Network Working Group, The Internet Society, 2004.

[11] Initiative for Open Authentication (OATH), „OATH Reference Architecture, Release 2.0," 2007.

[12] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk; Computer Security Division, Information Technology Laboratory and Sabari Gupta, Emad A. Nabbus; Electrosoft Services, Inc., „Electronic Authentication Guideline," National Institute of Standards and Technology (NIST), 2013.

[13] European Central Bank, „Recommendations for the Security of Internet Payments," Frankfurt am Main, 2012.

[14] FFIEC, „Supplement to Authentication in an Internet Banking Environment," Arlington, 2005.

[15] B. S. M. S. Obaidat, "Keystroke Dynamics Based Authentication," in Biometrics. Personal Identification in Networked Society, Kluwer Academic Publishers, pp. 213-229.

[16] BehavioSec, „Measuring FAR/FRR/EER in Continuous Authentication," Stockholm, Sweden, 2009.

[17] Florian Schaub, Ruben Deyhle, Michael Weber; Institute of Media Informatics, Ulm University, 89069 Ulm, Germany, „Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms," Ulm, Germany, 2012.

[18] Confident Technologies, „Mobile (In)Security – A Survey of Security Habits on Smartphones and Tablets," 2011.

[19] Koichiro Niinuma, Fujitsi Laboratories, Kawasaki, Japan; Anil K. Jain, Department of Computer Science & Engineering, Michigan State University, East Lansing, MI, USA, „Continuous User Authentication Using Temporal Information," 2009.

[20] Martha E. Crosby and Custis S. Ikehara; University of Hawaii/Manoa (USA), „Continuous identity authentication using multimodal physiological sensors," 2004.

[21] M. Jones, Microsoft; D. Hardt, Independent, „The OAuth 2.0 AuthorizationFramework: Bearer Token Usage (RFC6750)," Internet Engineering Task Force (IETF), 2012.

[22] Gregory D. Williamson, GE Money – America's, "Enhanced Authentication In Online Banking," Journal of Economic Crime Management, pp. Fall 2006, Volume 4, Issue 2, 2006.

[23] Vivek Haldar, Deepak Chandra, and Michael Franz; Department of Computer Science, University of California, „Semantic Remote Attestation – A Virtual Machine directed approach to Trusted Computing," Irvine, CA, USA, 2004.

[24] Federal Public Key Infrastructure Policy Authority, „United States Federal PKI – X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI)," 2011.

[25] Trusted Computing Group, „Trusted Platform Module (TPM) Summary," 2008.

[26] C. Bare, „Attestation and Trusted Computing," 2006.

[27] ISO/IEC, „ISO/IEC 7816-8 Commands for security operations," 2004.

[28] Trusted Computing Group, „Trusted Platform Module Library – Part 1 Archutecture," 2013.

[29] GlobalPlatform, „Secure Element Access Control," 2012.

[30] ARM Limited, „ARM Security Technology – Building a Secure System using TrustZone Technology," 2009.

[31] RSA Laboratories, „PKCS#11 Base Functionality v2.30: Cryptoki – Draft 4," 2009.

[32] Microsoft, „Cryptography API: Next Generation," [Online]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/aa376210%28v=vs.85%29.aspx. [Accessed 3 May 2013].

[33] Sally Hudson, IDC, „Worldwide Identity and Access Management Market 2011-2015 Forecast," Framingham, 2011.

[34] Sharon A. Mertz, Chad Eschinger, Tom Eid, Yanna Dharmasthira, Chris Pang, Laurie F. Wurster, Tsuyoshi Ebina, Hai Hong Swinehart; Gartner, „Forecast: Software as a Service, All Regions, 2010-2015," 2011.

[35] Stefan Ried, Ph.D.; Holger Kisker with Pascal Matzke, Andrew Bartels, Miroslaw Lisserman; Forrester Research, „Sizing The Cloud – A BT Futures Report," 2011.

[36] John C. McCarthy with Christopher Mines, Pascal Matzke, Yahor Darashkevich; Forrester Research, „Mobile App Internet Recasts The Software And Services Landscape – A BT Futures Report," 2011.

[37] KPMG, „2011 KPMG Mobile Payments Outlook," 2011.

[38] Cloud Security Alliance, „Security Guidance for Critical Areas of Focus in Cloud Computing v2.1," 2009.

[39] Oracle, „Java Card Technology," [Online]. Available: http://www.oracle.com/technetwork/java/javacard/overview/index-jsp-140503.html. [Accessed 3 May 2013].

[40] Sascha Rehbock and Ray Hunt, Computer Science and Software Engineering University of Canterbury, „Trustworthy Clients: Architectural Approaches for Extending TNC to Web-Based Environments," Christchurch, New Zealand, 2008.

[41] Leicher, A., Schmidt, A.U., Shah, Y. and Cha, I., "Trusted computing enhanced user authentication with OpenID and trustworthy user interface," Int. J. Internet Technology and Secured Transactions, vol. Vol.3, no. No.4, pp. 331 – 353, 2011.

[42] Stuart E. Schechter, MIT Lincoln Laboratoy; Rachna Dhamija, Hardvard University & Commerce Net; Andy Ozment, MIT Loncoln Laboratory & Univeriesty of Cambridge; Ian Fischer, Harvard University, „The Emperor's New Security Indicators," 2007.

[43] K. N. Elbert, „Understanding Consumers' Visual Attention Patterns Online: An Eye Tracking Analysis of Web Trust Seal Effects On Visual Attention and Choice," 2013.

[44] Václav Matyáš and Zdeněk Říha, Faculty of Informatics, Masaryk University Brno, Czech Republic, „Biometric Authentication – Security and Usability," 2002.

Security Challenges of Current Federated eID Architectures

Libor Neumann

ANECT a.s., Vídeňská 125, 619 00 Brno, Czech Republic
Libor.Neumann@anect.com

Abstract

The paper deals with security analysis of target assets protection in IT systems using federated eID technologies.

The main topic of the analysis is asset protection in a target IT system using federated eID system for IAM (Identity and Access Management), particularly for authentication.

The analysis deals with the well-known federated eID technologies i.e. oAuth, OpenId, SAML, SCIM, WS-federation and WS-trust.

The issue of relationship between target system data channel (data channel between authenticated user and target system) and authentication result of federated eID system (assertion) is analysed.

1 Introduction

This system-based security analysis has been motivated by our expectation to learn from current solutions and by a hope that it will be possible to use the results in new external authentication technology development [Neum07], [Neum08], [Neum12].

The analysis target is security of target assets, i.e. assets of the target system or application.

Authentication systems can be divided into two basic system architectures:

- **Internal authentication** – the authentication is integrated into the target system or application. The asset protection is solved integrally with authentication in the target system. This is the first architecture from the historical point of view. We can find the origin in minicomputer era. The architecture decreases security and increases complexity for end users with growing number of target applications.
  Currently, end user limits create an inviolable barrier of the architecture.
- **External authentication** – the authentication is an external service. It can be shared by many target systems and applications. It could significantly simplify the use for end users. This is a new architecture, growing particularly in the 21st century in the form of federated authentication systems.
  The issue of secure linking (binding) of external authentication results with target assets protection has to be solved in this case.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_3, © Springer Fachmedien Wiesbaden 2013

The security of the whole solution is determined by the weakest component of the solution i.e. the authentication itself and by the integration with the target application as well.

The paper deals with the system security analysis focusing on target assets protection when federated eID architecture is used.

The analysis is based on published standards including federated eID standards and standards of related technologies.

2 Security Target

The motivation of authentication is to make ICT assets accessible to authorized users and to protect them from attackers. The data channel protection is necessary (not sufficient) condition of asset protection in the case of remote access.

The subject of the analysis is protection of the data channel used to access the protected assets by an authorized user using a federated eID system.

It deals with the data channel between the end user workstation and the target application provided by the "Relying Party".

3 Analysis of Federated eID Architectures

The following well-known federated eID standards have been analysed: oAuth [Hard12], OpenId [Open07], SAML [OASI05a], [OASI05b], [OASI08], [OASI10], [OASI12], SCIM [SCIM13], WS-federation [OASI09], WS-trust [OASI07].

The system analysis of the standards shows that all of them are limited to Web technologies; a specific feature of HTTP communication implemented in Web browsers is used as a basic system communication element. The data connectivity between servers through end user browser based on HTTP redirect (or similar browser-based methods) is the key functionality of the communication infrastructure required by all of the analysed federated eID standards.

It is directly related to the essence of the federated eID i.e. to its topology. The Identity Provider is placed at a different location from the Relying Party (the target system or application). The federated eID architecture requires communication between at least three points in the cyber space.

Other kinds of client software used for remote communication do not support the required communication feature e.g. SSH terminal, VPN client, remote desktop client, WiFi client.

All of the analysed standards focus on data transfer (related to authentication) between the Relying Party (target system or application) and the Identity Provider.

The analysis of the federated eID standards has focused on features important for system based security.

The analysed features:

- Authentication executed by Identity Provider and the relation between the authentication and the data set transferred as a result of the authentication (assertion),
- The way of the data set (assertion) transfer between Identity Provider and Relying Party,
- Completeness of the data transfer securing; dependence on other technologies or standards,
- Linking (binding) the authentication results with target data channel protection i.e. with target assets protection.

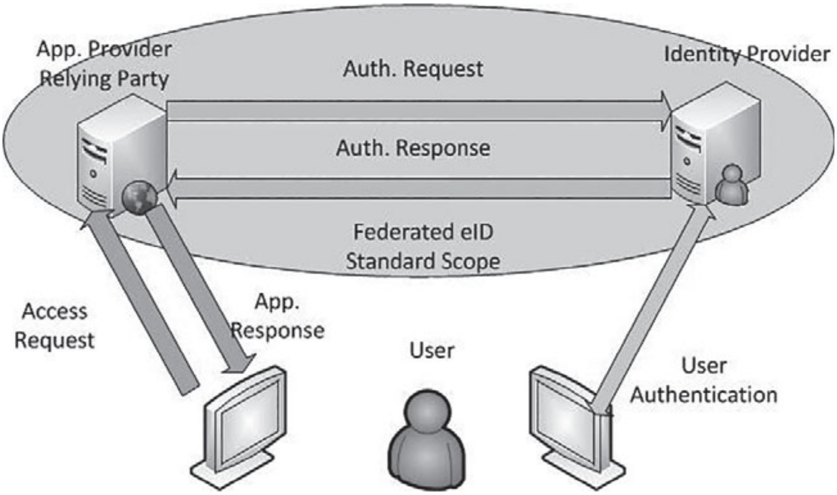


Fig. 1: Federated eID data layer

Table 1: The analysis results.

	oAuth	OpenId	SAML	SCIM	WS-federation	WS-trust
Is authentication included in the standard?	Explicitly NO	Explicitly NO	Explicitly NO	Uses oAuth	Explicitly NO – references to WS-trust	Security is explicitly excluded
Authentication result (assertion) transfer	Implicitly bearer	Implicitly bearer	Explicitly bearer or holder-of-key	N/A	Implicitly bearer	Implicitly bearer
Secured data channel use (TLS/SSL) or other lower layer safeguarding	TLS/SSL explicitly required	TLS/SSL strongly recommended	TLS/SSL strongly recommended TLS/SSL with X.509 PKI required with holder-of-key	oAuth explicitly required	WS-trust and WS-security explicitly required	N/A
Linking the target data channel with authentication	NO	NO	YES in case of holder-of-key use	N/A	NO	NO

The analysis results summary:

- No analysed standard includes user authentication in its scope. The scope of security analysis of the federated eID excludes the authentication security and security of the link between the authentication result and the assertions.
- The bearer assertion transfer is used in all the cases. Holder-of-key is a supported option only in the SAML case.
- No architecture includes all deeper layers. All of them rely on the security of something else, usually TLS/SSL security.
- Only the SAML holder-of-key profile offers tools potentially enabling a link between the target data channel and authenticated user (Channel Binding).

4 Security Model

A specific security model has to be used for federated eID architecture. It reflects the specific secured HTTP communication used i.e. the two layer data channel existence. It consists of a transparent encrypted layer (TLS, SSL) and an application data layer (HTTP, HTML, XML, etc.) used by the target applications.

The security model consists of two basic parts. The target asset protection security model is described in chapter 4.1. The basic general federated eID security model is described in section 4.2 along with specific models focusing on specific assertion transport methods (bearer and holder-of-key).

The models are used for a security threat analysis of target assets using a federated eID technology.

4.1 Assets Protection Security Model

It is a well-known fact that it is impossible to enforce any security measure without authentication in the case of remote access. This is true for data channel protection as well. No secure communication can exist if the data channel is not authenticated (if it is unknown who is on the opposite site of the channel).

The target assets can be protected in the case of secured web communication (HTTPS – i.e. an open data layer HTTP transferred by an underlying encrypted TLS/SSL layer) only if the encrypted layer (channel) has been authenticated. That is a required condition, not a sufficient one.

The encrypted layer (channel) security cannot be obtained by authentication on the application data layer. The attacker can be anywhere on the encrypted channel, having access to any application layer data including authentication one.

The attacker can enable the user to do authentication on the application layer and use the authenticated application session to access protected assets or, worse yet, the attacker can obtain user's authentication secrets (like loginname and password) and abuse them separately.

The analysis of TLS standards [AlWZ10], [Badr09], [Barn11], [BlGo07], [BrHo10], [DiRe06], [DiRe08], [ErTs05], [FrKK11], [FuBl08], [HaFu07], [Hoff12], [HoJB12], [HoSc12], [Jose11], [Kero10], [MaGi11], [MeHu99], [NiAT02], [Resc10], [SaMB06], [Sant06], [SiAH08], [ToAN05], [TuPo11], [TWMP07], [Will07], [WMVW12] shows two options of linking the TLS encrypted layer with the upper data channel layer:

- Double authentication – The TLS/SSL encrypted channel authentication done before communication with the target application and the second authentication on the application layer
- Channel Bindings – Using the authenticated TLS/SSL encrypted channel for application layer data channel authentication (Channel Bindings to Secure Channels).

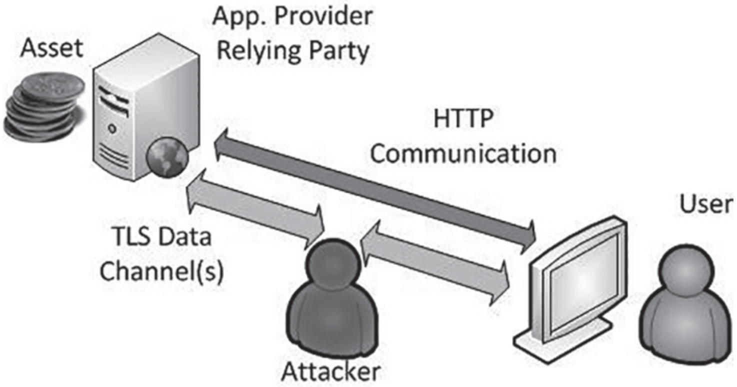


Fig. 2: Target assets protection security model.

The first option is the standard way. The second one is supported by the new standards; the general standard RFC 5056 [Will07] and the TLS specific one RFC 5929 [AlWZ10].

Therefore we have the same two system options in the case of TLS integration with federated eID:

- Double authentication – independent TLS encrypted channel authentication and federated eID authentication on the application layer
- Channel bindings – use of authenticated TLS by a federated eID authentication

The first option is the current standard and brings up the question of security and usefulness, the question of user experience and limits of target assets protection. It will be analysed in the next chapter.

The second option could be enabled only if the channel bindings defined by TLS are supported by federated eID systems.

The analysis of federated eID standards provides a negative answer. The opposite possibility i.e. to use application layer authentication (like federated eID) to authenticate the TLS layer (secure channel bindings to data channel) is not supported by the analysed TLS standards.

The SAML holder-of-key profile is the only option in federated eID standards where the link between the TLS/SSL channel and the application layer authentication is described. The relationship is solved by the first option – see chapter Holder of Key.

4.2 Federated eID Security Model

Security Considerations in federated eID standards describe a wide range of threats i.e. Client Impersonation, Man-in-the-Middle Attacks, Phishing Attacks, Cross-Site Request Forgery, Clickjacking, Open Redirectors, Misuse of Access Token to Impersonate Resource Owner in Implicit Flow – oAuth [Hard12], Eavesdropping Attacks, Man-in-the-Middle Attacks, Rogue Relying Party Proxying – OpenId [Open07], Stolen Assertion, Theft of the Bearer Token, Man-in-the-Middle, Impersonation without Reauthentication – SAML [OASI05b].

The target of security model is not full security threat analysis of federated eID architectures. It would be very complex. The following areas should be included in that complex model:

- Selection of Identity provider
- Authentication to Identity provider
- Link between authentication and authentication assertion
- Assertion transfer
- Link between target data channel and assertion

The link between the target data channel and assertion was discussed in the previous chapter.

The security model is focused on the area which is not mentioned or not adequately discussed in the federated eID standards or it is supposed as a precondition. It is the area of underlying security infrastructure (e.g. secure channel use, encryption, signing).

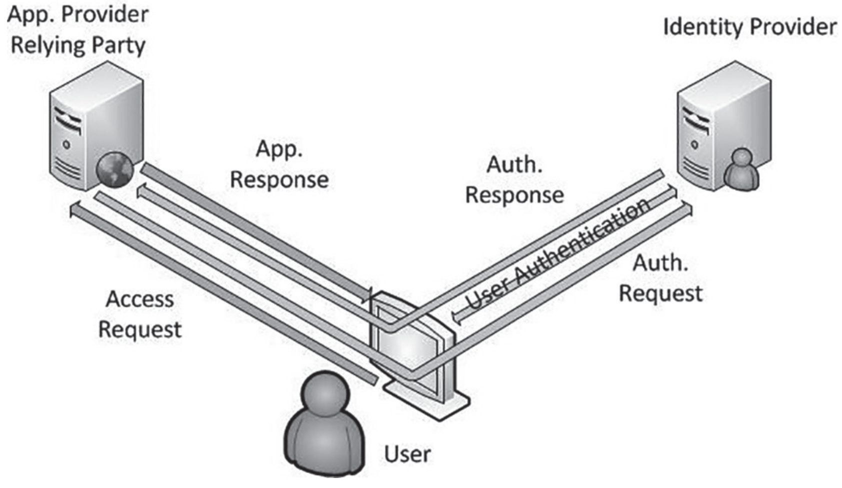


Fig. 3: Idealised view of federated eID.

Figure 3 describes the idealised view used in the security analysis described in federated eID standards. The idea is that something secures the communication between the Relying Party (target application) and the Identity Provider through the Web client of the authenticated user, i.e. that the same user is authenticated by the Identity provider and access the target assets.

This idea can be legitimate in the following cases:

- The communication is in a secured environment i.e. the attacker is excluded by other (not described) security measures e.g. the communication occurs inside a protected internal network,
- The data channels used for communication are secured.

We know that the encrypted layer channel can be secured only if it is authenticated.

Federated eID standards use two different ways of assertion transfer with significantly different security features:

- Bearer
- Holder of Key

The options are analysed in the following separate chapters.

4.2.1 Bearer

This is the assertion transfer method supported by all of the analysed federated eID standards. It is based on the following idea: who delivers the assertion (the result of authentication) is the subject of authentication done by the Identity Provider.

It means that any attacker gaining a copy of assertion can be accepted as an authenticated user if the assertion is applied in the defined time window.

The security model deals with the attacker possibilities to gain the assertion using separation of the encryption layer (SSL/TLS) from the application data channel (HTTP) weakness. We suppose that the encryption layer is not authenticated in both parts of communication i.e. between the Relying Party and the Web browser and between the Web browser and the Identity Provider.

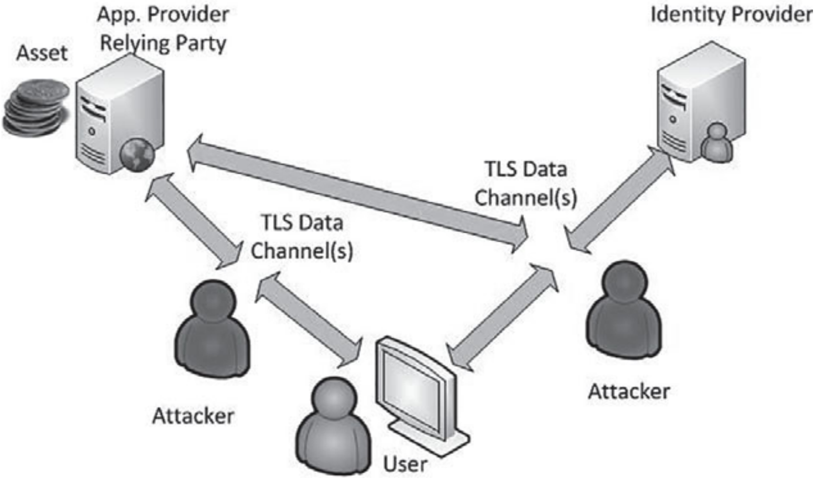


Fig. 4: Simplified security model of federated eID using bearer assertion transfer.

If no (or unreliable) authentication of the TLS/SSL channel is done in both communication segments, the attacker is able to access the application layer and gain access to the application layer data including the assertion.

The Bearer method relies on the expectation that this attack will not be used. No security measure is offered (except for the limited time during which the assertion is valid).

The Fig. 4 shows the places where an attacker can abuse the described weakness.

The situation is similar to the situation described in the previous chapter. But they are two different data channels. It is more difficult to protect them and easier to abuse them than in the previous (target asset) case.

4.2.2 Holder of Key

The significant security risks related to the bearer assertion transfer are known [WiBu11]. The Holder-of-key method was designed to remove this security weakness.

The Holder-of-key deals with the interaction of assertion transfer on the application layer with TLS encrypted channels authentication used to transfer the assertion message.

SAML is the only federated eID architecture supporting the Holder-of-key assertion transfer (SAML uses the term "confirmation method").

Only the Holder-of-key assertion transfer enables fulfilling requirements of the highest QAA level by [WiBu11].

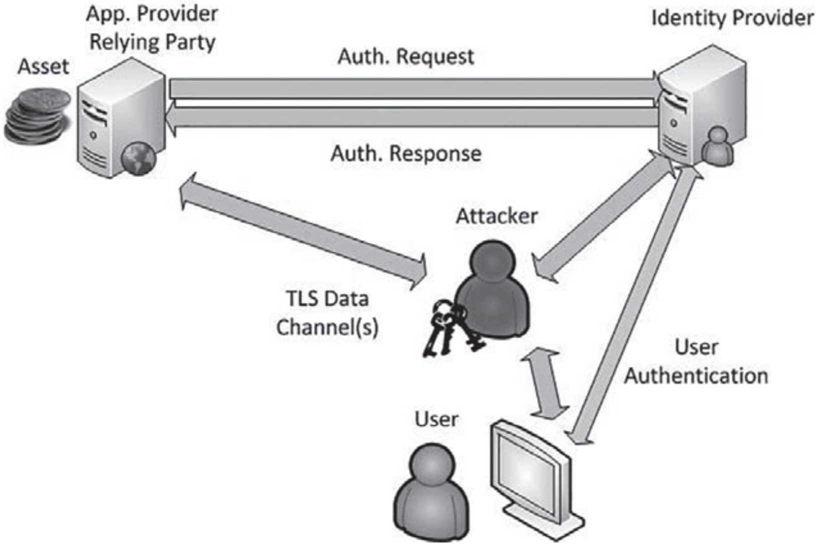


Fig. 5: Holder-of-key security model.

Authentication of both encrypted TLS channels used for assertion transfer is the elementary principle of Holder-of-key. Both authentications have to use the same private key linked to the same X.509 certificate. The supported authentication technologies are limited by TLS authentication standards in real world.

The target application layer has to check if the authenticated certificates used in TLS authentication on both TLS channels are equal (i.e. if they belong to the same private key). This should exclude MITM and other attacks on both TLS channels.

However, if we take into account that authentication to Identity Provider is excluded from the scope of federated eID standard i.e. it is generally independent to the authentication of TLS channel, we are in a similar situation to what was discussed in chapter Assets Protection Security Model. The only difference is: the issue now is not on the Relying Party side of the federated eID topology, but on the Identity Provider side. Figure 5 shows the model.

If the authentication with Identity Provider is not linked with the TLS authentication, attackers can use their own keys to protect TLS and abuse the result of Identity Provider authentication to attack the target assets successfully.

Federated eID standards do not deal with this issue.

There are several possibilities how to eliminate the threat. They require two or three authentications of the user including two TLS X.509 PKI authentications. In all the cases it is a question of additional value of federated eID if a strong direct PKI authentication must be used by the Relying Party and the user.

5 Conclusion

Limited Security

The target asset security cannot be higher than authentication security made by Identity Provider. The federated eID excludes authentication with the Identity Provider and therefore it can only add security threats. The target assets security can be limited by additional threats of federated eID.

Authentication Deadlock

It is surprising to find that federated eID security is conditioned by lower layer security (encrypted layer security – TLS/SSL). Federated eID cannot work in a secure way without secured data channels. Federated eID relies on the secured transport layer.

This dependence creates an authentication (security) deadlock. The secured TLS/SSL channel cannot be created without authentication of the channel. Therefore authentication using the federated eID technology requires previous authentication of all the used underlying secure channels.

Target Channel Protection

No federated eID architecture deals with target assets protection. No link between target data channel and authentication supported by federated eID is included in the standards.

The only exception that could be mentioned is the Holder-of-key profile in SAML standard where X.509 PKI authentication has to be used. The federated eID seems to be an additional complexity and possible additional threats only in this specific case.

User Effects

Federated eID has a positive effect in the case of password-based authentication from end user´s point of view. It is a weak authentication option. Federated eID brings additional security threats and advantages for attackers in this option.

There are no or very debatable effects in the case of device-based authentication from end user´s perspective. The same or better effects could be achieved by using the available computing power in the device.

Federated eID Concept

Federated eID is the well-known design and implementation of the external service oriented authentication/eID. The external service oriented authentication is a very important and needed concept, particularly from user´s point of view.

The federated eID concept is limited by design to Web based target systems only. No other type of target application is able to use federated eID.

The analysis results show that the security weaknesses of the federated eID design are significant e.g. they miss strong protection of target assets. It seems that such weaknesses cannot be repaired by adding new security measures or modifications. A system redesign and use of significantly different concept would be needed.

5.1 General Conclusions

Authentication is atomic security element

Authentication technology must not rely on security of another system (e.g. communication layer security). All the required security has to be solved inside the authentication system. Authentication can rely on unsecured underlying systems only.

If the description of any authentication system includes requirements to other systems, such as signing, encryption or confidentiality, it should be a security deadlock. The solution should not be considered secure and/or functional.

Authentication topology

Target assets protection requires authentication in exactly the same topology as the topology of the target data channel.

It is the necessary condition of target assets protection. The authentication in a different topology cannot substitute it.

External authentication

The binding between the target data channel and the external authentication has to be solved if the external authentication is used to protect remote access to target assets.

References

[AlWZ10] Altman, J., Williams, N., Zhu, L.: RFC 5929, Channel Bindings for TLS, Internet Engineering Task Force (IETF), July 2010

[Badr09] Badra, M.: RFC 5487, Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode, IETF Trust, March 2009

[Barn11] Barnes, R.: RFC 6394, „Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)", IETF, October 2011

[BlGo07] Blumenthal, U., Goel, P.: RFC 4785, Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS), The IETF Trust, January 2007

[BrHo10] Brown, M., Housley, R.: RFC 5878, Transport Layer Security (TLS) Authorization Extensions, IETF Trust, May 2010

[DiRe06] Dierks, T., Rescorla, E.: RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, The Internet Society, April 2006

[DiRe08] Dierks, T., Rescorla, E.: RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, The IETF Trust, August 2008

[Hard12] D. Hardt, Ed.: „The OAuth 2.0 Authorization Framework", Internet Engineering Task Force (IETF), Request for Comments: 6749, October 2012

[ErTs05] Eronen, P., Tschofenig, H.: RFC 4279, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), The Internet Society, December 2005

[FrKK11] Freier, A., Karlton, P., Kocher, P.: RFC 6101, The Secure Sockets Layer (SSL) Protocol Version 3.0, IETF, August 2011

[FuBl08] Funk, P., Blake-Wilson, S.: RFC 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), The IETF Trust , August 2008

[HaFu07] Hanna, Steve, Funk, Paul: draft – Key Agility Extensions for EAP-TTLSv0, The IETF Trust, September 24, 2007

[Hoff12] Hoffman, P.: RFC 6358, „Additional Master Secret Inputs for TLS", IETF, January 2012

[HoJB12] Hodges, J., Jackson, C., Barth, A.: RFC 6797, „HTTP Strict Transport Security (HSTS)", IETF, November 2012

[HoSc12] Hoffman, P., Schlyter, J.: RFC 6698, „The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", IETF, August 2012

[Jose11] Josefsson, S.: RFC 6251, „Using Kerberos Version 5 over the Transport Layer Security (TLS) Protocol", IETF, May 2011

[Kero10] Keromytis, A.: RFC 6042, Transport Layer Security (TLS) Authorization Using KeyNote, IETF Trust , October 2010

[MaGi11] Mavrogiannopoulos, N., Gillmor, D.: RFC 6091, Using OpenPGP Keys for Transport Layer Security (TLS) Authentication, IETF Trust, February 2011

[MeHu99] Medvinsky, A., Hur, M.: RFC 2712, Addition of Kerberos Cipher Suites to Transport Layer Security (TLS), The Internet Society, October 1999

[Neum07] Neumann, Libor: An analysis of e-identity organizational and technological solutions within a single European information space. In: e-Challenges e-2007, The Hague, Netherlands, 2007, pp. 1326-1333.

[Neum08] Neumann, Libor: Anonymous, Liberal, and User-Centric Electronic Identity – A New, Systematic Design of eID Infrastructure, In: e-Challenges e-2008, 22-24 October 2008, Stockholm, Sweden.

[Neum12] Neumann, Libor et al.: Strong Authentication of Humans and Machines in Policy Controlled Cloud Computing Environment Using Automatic Cyber Identity, In: ISSE 2012 Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2012 Conference, Springer Vieweg, 2012, pp 195-206.

[NiAT02] Niemi, A., Arkko, J., Torvinen, V.: RFC 3310, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), The Internet Society, September 2002

[Open07] OpenID: „OpenID Authentication 2.0 – Final“, December 5, 2007

[OASI05a] OASIS: „Profiles for the OASIS Security Assertion Markup Language (SAML)V2.0“, OASIS Standard, 15 March 2005

[OASI05b] OASIS: „Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0“, OASIS Standard, 15 March 2005

[OASI07] OASIS: „WS-Trust 1.3“, OASIS Standard, 19 March 2007

[OASI08] OASIS: „Security Assertion Markup Language (SAML) V2.0 Technical Overview“, Committee Draft 02, 25 March 2008

[OASI09] OASIS: „Web Services Federation Language (WS-Federation) Version 1.2“, OASIS Standard, 22 May 2009

[OASI10] OASIS: „SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0“, Committee Specification 02, 10 August 2010

[OASI12] OASIS: „SAML V2.0 Kerberos Web Browser SSO Profile Version 1.0“, Committee Specification 01, 07 February 2012

[Resc10] Rescorla, E.: RFC 5705, Keying Material Exporters for Transport Layer Security (TLS), IETF Trust, March 2010

[SaMB06] Santesson, S., Medvinsky, A., Ball, J.: RFC 4681, TLS User Mapping Extension, The Internet Society, October 2006

[Sant06] Santesson, S.: RFC 4680, TLS Handshake Message for Supplemental Data, The Internet Society, September 2006

[SCIM13] SCIM: „System for Cross-domain Identity Management“, http://www.simplecloud.info/

[SiAH08] Simon, D., Aboba, B., Hurst, R.: RFC 5216, The EAP-TLS Authentication Protocol, The IETF Trust, March 2008

[ToAN05] Torvinen, V., Arkko, J., Naslund, M.: RFC 4169, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2, The Internet Society, November 2005

[TuPo11] Turner, S., Polk, T.: RFC 6176, „Prohibiting Secure Sockets Layer (SSL) Version 2.0“, IETF, March 2011

[TWMP07]Taylor, D., Wu, T., Mavrogiannopoulos, N., Perrin, T.: RFC 5054, Using the Secure Remote Password (SRP) Protocol for TLS Authentication, The IETF Trust, November 2007

[WiBu11] William E. Burr, et al.: „Electronic Authentication Guideline“, Special Publication 800-63-1, NIST- National Institute of Standards and Technology, December 2011

[Will07] Williams N.: – RFC 5056, On the Use of Channel Bindings to Secure Channels, The IETF Trust, November 2007.

[WMVW12] Winter, S., McCauley, M., Venaas, S., Wierenga, K.: RFC 6614, „Transport Layer Security (TLS) Encryption for RADIUS“,IETF, May 2012

Worldbank's Secure eID Toolkit for Africa

Marc Sel · Tomas Clemente Sanchez

PricewaterhouseCoopers Enterprise Advisory
{marc.sel | tomas.clemente.sanchez}@pwc.be

Abstract

This article provides a high-level functional and technical overview of the Worldbank's Toolkit project 'Secure Electronic Identity for Africa'. The Toolkit project was initiated by the Worldbank in 2012, with sponsorship of the French government. Its aim is to provide African nations with a guidebook addressing all required elements to establish a secure electronic identity system in their country. The Toolkit is expected to be publicly announced in 2013. Implementation funding is to be provided through a PPP (Public Private Partnership) including participation from the Worldbank.

The Tookit proposes a mixed ecosystem of government and private sector operators such as MNOs (Mobile Network Operators). It combines elements such as the collaboration of government entities such as a National Identity Register, other registers such as an Election Committee Register and Registers of Births and Deaths, various private Trust Service Providers, and a combination of mobile (e.g. SIM/USIM) and non-mobile (e.g. PKI) technologies as well as biometrics.

1 Introduction

1.1 Worldbank

The Worldbank supports countries in many areas, including through the use of focussed ICT deployment. For this purpose, Worldbank identified three ICT Strategy Pillars: transform, innovate and connect. 'Transform' aims at making development more open and accountable, and at improving service delivery. 'Innovate' addresses the developing of competitive IT-based service industries and the fostering of innovation. Finally, 'Connect' focuses on afordable access to broadband.

1.2 The Toolkit

In 2012, the World Bank launched a study to create a toolkit on secure eID systems. The toolkit aims at giving practical know-how to African governments on building national eID systems that can help deliver social services on mobile platforms. PricewaterhouseCoopers was invited to conduct this study. The Toolkit is expected to be publicly announced in the second half of 2013, most likely in a potential pilot country.

The project includes technology and regulatory assessments (at global, regional and national level), the creation of selection criteria for African launch country, deep dive case studies, interviews and on-line collaboration [LinkedIn].

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_4, © Springer Fachmedien Wiesbaden 2013

The project is structured in three phases: conducting interviews, performing an eID scan, and Toolkit elaboration. This should later be followed by one or more pilot implementations, and subsequent deployments.

2 Interviews

The study started with interviews in East, West and South Africa, as well as Europe. Managing Directors from various national identification authorities as well as from ICT promoting entities and regulatory bodies were interviewed.

Even though the national ID infrastructures in the studied African counties are in different development stages, all the interviewed government officials agree that the usage of mobile eIDs would be beneficial for their countries. They see it as an opportunity to provide a variety of government services, such as voting, taxation, or social services. As the main advantage of such solution, they emphasise a relatively high mobile phone penetration, even in rural areas, which would enable high availability of the offered services. As one of the key requirements of a future eID solution, they highlight the fraud detection and prevention, which would provide trustworthiness of the government services. On the other hand, the government officials share concerns about the infrastructure problems, such as lack of electricity in some areas, low level of technical education of their citizens, low security and privacy awareness, the lack of regulatory frameworks and a low level of collaboration between the mobile network operators.

On the other hand, the interviewed eID experts, coming both from academic and industry backgrounds, express a general agreement that the existing eID technology is able to mitigate many of the identified risks, especially the ones related to security and privacy. However, the consensus is that the technology must be properly managed, supported and regulated. For instance, binding a Subscriber Identity Module (SIM) card to an individual or the existence of a civil registration system are the prerequisites for a valid mobile eID scheme. In case a single eID registry is lacking, information might be provided from other registers such as Election Committee Registers and Registers of Births and Deaths.

The eID experts all share the view that it is necessary to tailor the eID solution in order to meet the country specific needs. Therefore, it is important to come up with a generic solution which offers a wide set of options and to use it as a starting point for customization of the country-specific solutions. In order to do so, it is important to refer to the successful MeID projects such as the one in Sri Lanka (Dialog Connect), but also to the global examples of successful eID roll outs. By learning from their experience and the variety of offered solutions, it would be possible to define a generic solution that could capture the needs of all the countries in the scope of the World Bank Study.

The experience for the Mobile eID scheme in Africa can be gathered from multiple approaches and technologies used for the national eID projects worldwide. The prominent examples are the "driving licence" based identification used in UK and USA, and the various EU approaches offering examples of smart card, soft certificate, mobile or even username/password based identification schemes. Another approach that is particularly interested is the Indian UIDA approach, due its focus to enrol people from rural and underprivileged communities, and its large scale use of biometrics.

3 eID scan

Parallel to the interviews we conducted a stock-taking study on the current eID landscape. The goal was to take stock of the current and the emerging uses of eID and good practices around the world, and use these experiences as guidance to identify the major hurdles when adopting eID. Particular focus was on how these experiences where changing the traditional approach to public service delivery and accountability. The scan addressed:

1. eID overview. This part summarizes the main uses of eID in US, EU, India, and Japan and describes their different approaches to eID according to their particular situational factors (i.e. cultural background, technical means, resistance, ..). Subsequently the main applications of eID today are summarized (i.e. e-identity, e-banking, e-passports, e-ticketing), and the business models used (i.e. government driven, commercial, partnerships...).
2. Major technological trends in mobile eID. The "mobile electronic identity" was identified as an approach which holds a great potential to the African situation thanks to its capacity to be "portable" and self-contained. We reviewed the different types of mobile eID credentials (smart cards, USIMs, Secure Elements) and the technical solutions allowing implementation of them (mobile phone based, Server based, Software based or Token based)
3. Case studies. To gain an understanding of the experiences of successful eID implementations, a number of case studies on the introduction of eID at the national level have been conducted. This includes five high-level cases on Austria, Belgium, Turkey, Finland and The Netherlands as well as three deep-dive case studies on Estonia, India and Nigeria. These were selected because they are either "success stories" in the field of eID (e.g. Austria, Belgium and Estonia) or because of the similar economic and socio-cultural factors to African countries (i.e. India or Nigeria).

The deep-dive studies provide a combination of historical background, strategic choices, actors constellations and business and implementation models that allows for the explanation of some, but by no means all, of the complexities related to the adoption of a national eID. The studies provide as well an analysis on the "practical implementation" of the respective eID systems in the countries under studies, including details on the legal and technical frameworks put in place.

The main lessons that we can draw this analysis are:

- A successful form of private-public partnership can lead to the provisioning of services that make use of trust services both in private and public sector. A broad service catalogue contributes to the adoption by a broader public.
- The adoption by broad sectors of the population is a fundamental step forward towards the success of a national eID program, and public awareness campaigns play a key role in overcoming any initial resistance and enhancing the adoption of eID services by the population.

The size of the population is a significant factor. In Estonia, a relatively small country the implementation of eID systems has been fast (partly due to the adoption of consolidated commercial eID solutions). In the Indian case, given the size of the population, the technical resources mobilized are huge, but still covering the whole country remains a daunting task.

4 Technology aspects

4.1 Core assumptions

The eID solution should be based on an Identity Repository that is operating according to government regulation. This repository should contain all identities of citizens, and optionally of registered foreigners. In case a Mobile eID (MeID) approach is taken, this solution will base itself upon/link to a subset of the full identity repository. We assume that the selection of the credential medium (e.g. smart card, SIM in a mobile phone, etc) will be a consequence of the envisaged eID functionality. In case an MeID solution is selected, it should be possible to establish multiple mobile identity repositories (M-IDREP), to cater for multiple Mobile Network Operators (MNOs). Such M-IDREPs should not interfere with the normal course of business of the MNOs and their current Home and Visitor Location Registers (HLR/VLR).

4.2 Assumptions with regard to technology

It is commonly accepted that achieving absolute security is impossible. The state-of-the-art is typically illustrated by a leap-frog situation, where new security solutions are constantly challenged and attacked. Some solutions stand for a long time, others not.

People can be coerced or bribed, and as such may insert an element of insecurity in a system. Even if one would design, manufacture and deploy a perfectly secure smart card or SIM for identity purpose, the people involved in the production chain still remain vulnerable to various types of non-technical attack. Furthermore, people might evade the use of technology if they do not see the benefit or if they seek to avoid side-effects e.g., when technology threatens their privacy.

Electronic ID cards and passports are traditionally based on PKI and document security. However, as technology continues to evolve, governments may prefer to make use of emerging technologies including those commonly referred to as Privacy Enhancement Technologies (PETs). We assume that credentials (including private keys) should be stored on a mobile device (alternatively on a traditional Personal Computer, a traditional Smart Card or a Host Security Module (HSM)). The credential store should be adequately protected in function of its use.

Finally, the information on the card/saved in the chip is an authenticated copy. The master copy of the information is stored in the identity repository. This master database can be a real or a virtual database, i.e., distributed over various organisations.

4.3 Technology foundation

The technology foundation includes:

- eID applications for use by personnel to capture citizen information;
- Back-office IT infrastructure and eID database;
- Communications infrastructure for linkage of eID central office with field offices;
- ID mediums such as smartcards (and possibly mobile phones); and
- Authentication and POS devices (including biometric devices, smartcard readers, etc.).

A solution based on this foundation leads to the following high-level framework (fig 1):

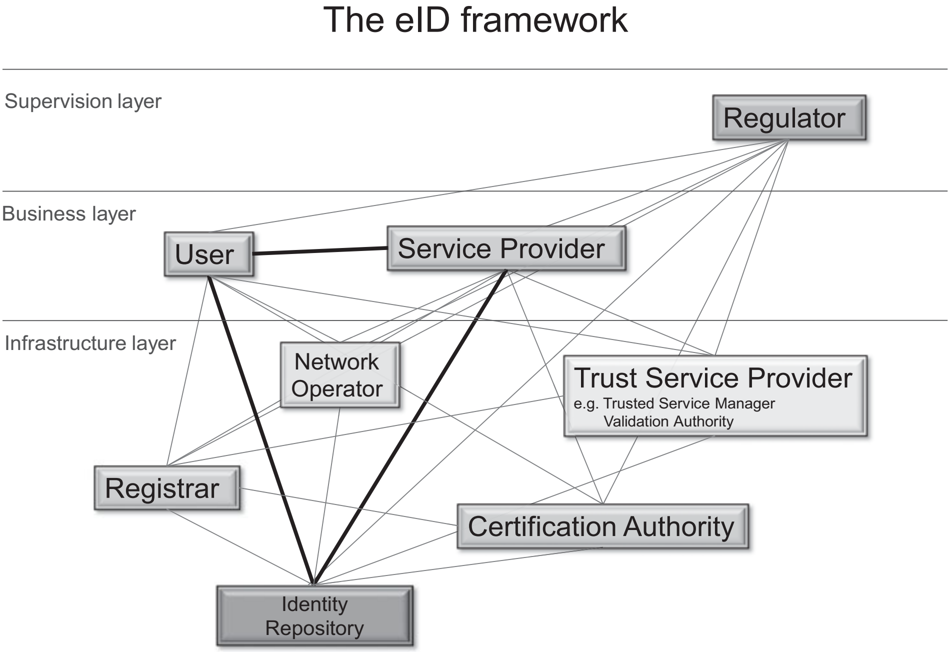


Fig. 1: The eID framework proposed by the Toolkit

In the case of a Mobile eID scheme, the above actors are complemented by the mobile identity repository, and one or more MNOs, enabling the communication, and optionally also fulfilling other functions (potentially acting as Registrar, as Certification Authority, as Trust Service Manager[1] or Trust Services Provider).

4.4 Core technology activities

We now briefly discuss the core technology activities that need to be performed to implement the landscape illustrated above. Complementary activities are addressed in the Toolkit but not discussed here.

4.4.1 eID scheme and responsibliities

Based on the objectives established by the stakeholders, the functionality of the eID scheme and its issuer need to be defined. Key elements include design and definition of:

- The roles, responsibilities and liabilities of all participants;
- The issuer function;
- The types of credentials that will be supported.

Roles, responsibilities and liabilities of all participants need to be defined, preferably through a legal scheme. Functional services offered under the eID Scheme, and types of applications envis-

[1] We use the notion of TSM as defined by Global Platform

aged to be supported by the scheme should consider: business goals, issuance and full lifecycle of the eID and its supporting credentials, including approval and support for the credentials on the network and on the phone or other deployment platform. Furthermore the operation of the infrastructure (identity repository, CA, Trust Services Providers, TSM) and development and support of applications should be defined. Key elements to define include:

- Desired legal effect, and relationship with legal context, laws and regulations;
- List of participants, and the roles and R&L (responsibility and liability) of these participants;
- Conformity assessment requirements on trusted hardware/software;
- Technical standards;
- Trust model and validation rules.

As the issuer is fundamental to the eID scheme, this function needs careful design. The issuer may or may not group elements of the various functions such as Registrar, Mobile Identity Repository, Identity Repository and Trust Services Provider. The issuer function can be fulfilled according to many alternatives, including by a dedicated legal entity, a government institution, or a Mobile Network Operator. It may be organised in a centralised or decentralised model. Each model has its strengths, weaknesses, and associated costs. A centralised model allows easier control over safeguarding the breeder documents, but may require citizens to travel a long distance, or may require careful planning to avoid long queues. A decentralised model is closer to the citizen, but requires decentralised personalisation equipment, which comes at a cost. Obviously, combinations are possible. The following briefly describes a combined issuing approach:

- A citizen is sponsored by someone from a local issuing office (or someone who has a relationship to it). The citizen then receives an email saying they've been invited;
- The email contains a link for the individual to schedule an appointment at a registration office;
- During the scheduled appointment at the registration office, the citizen's enrolment documents are verified and his biometric information captured; Information from complementary registers such as an Election Committee Register, a Register of Births and Deaths, a Social Security register, or a register from a Utility company or an MNO may provide additional background;
- The office adjudicates an individual by performing a criminal history check. Subsequently the office issues a request to a central function to personalise the credential;
- The credential is personalised and shipped to the location specified by the citizen's sponsor. The citizen is notified and asked to make an appointment to activate and pick up the credential;
- The office finishes the electronic personalization of the credential and loads the certificate and biometrics to the chip.

Care should be taken to balance the issuer's responsibilities with its liabilities. For example, when the issuer has no or very limited control over the registration process, the types of credentials, or the CA and Trust Model, his liabilities need to be clearly described and documented.

Obviously, there are many alternatives possible with regard to the credential. Traditional Smart Cards are a popular type of eID credential. They have the disadvantage of requiring a reader, which often means a PC or Kiosque is needed, as well as the installation of a device driver and sometimes middleware (which adapts the card's software architecture to the business application). SIM cards are another popular credential. Traditionally, the mobile infrastructure belonged to a MNO, was dedicated to its traffic, and could be considered a closed system. In GSM/3G, the authentication mechanisms such as Authentication and Key Agreement (AKA) assumed an implicit trust relation between the Authentication Centre (AuC) and the VLR/SGSN, and a trust relation between VLR/SGSN and the subscriber based on the shared key K. However, to achieve identity authentication and non-repudiation in an Internet ecosystem we need to introduce some form of asymmetrical credential. For this there are many different approaches possible. An asymmetrical credential (typically including a private key) could be stored in a credential platform under local control of the Citizen:

- In the UICC, which is typically owned by a MNO. This would imply that the MeID on-card application would be provided by the government and the UICC should be multi-application UICC, and the MNO would accept responsibility for the lifecycle of the MeID application onboard its UICC;
- In an embedded Secure Element, which should preferably be multi-application, since it cannot be relied upon that a dedicated handset will be manufactured and maintained to support the MeID application for a particular country only; the responsibility for the lifecycle of the MeID application should then likely be agreed with the handset manufacturer, or a TSM-style solution should be implemented;
- On a secure µSD card, which could either be single (MeID–only) or multi-application. In this case, the responsibility for the MeID application's lifecycle should be defined;

The credential could equally be stored under control of the Citizen, but in a centralised authentication or signature engine. Furthermore, for Internet application protocols, through the use of 3GPP GAA/GBA and its interworking architecture with the Liberty Alliance, OpenID Connect, or similar protocols, asymmetrical protocols could be leveraged.

As there are many alternatives possible, we refer to these in general using the name 'credential platform'. The eID Scheme may also select a 'virtual' credential, i.e., it can define high-level eID specifications, and certify various implementations on different platforms. The eID Scheme should preferably also propose different levels of security, such as STORK's four different QAA levels [STORK]. This would on one hand allow citizens to select the credential platform they prefer, while on the other hand allow Service Providers to specify minimal security levels for their applications.

4.4.2 eID business applications and credentials

Applications are capable of consuming eID services need to be defined. These can be both "stand alone" (using your credential without network connectivity) as well as integrated in other electronic transactions. Typical applications may include e.g.:

- Confirmation of identity (authentication);
- Recognition of life-events (birth, marriage, adoption, divorce, death);
- Identity as enabler: access to services and benefits, with NFC also access to physical locations;
- Confirmation of attributes: „I'm over 18", „I have the right to access this information, including e.g. a drop box", „I have paid for this service", „I can participate in this group".

From an eID perspective, there might be specific requirements on the citizen that are function of the selected technology, e.g. a Smart Card will require a reader (which needs to be connected to a host platform). The reader can be contact or contactless, in function of the selected card. The reader will establish the communication between the on-card application and a host application, e.g. residing on a Personal Computer, or on a Server. From a Mobile eID perspective, there are no specific requirements on the citizen, except the assumption that he/she is registered in the identity repository, has a mobile phone from an MNO participating in the MeID scheme, and a matching credential platform (typically the right type of SIM). It should be decided whether requirements for accessibility (e.g. blind people) should be taken into account. There are at least two main alternatives.

Alternative 1 Asymmetric credential on the phone

The credential platform could be implemented in the UICC, which may store the MeID credential. It is common to distinguish between the SIM, the UICC, the USIM and the ISIM:

- In 2G GSM, the hardware (ICC) and software (Subscriber Identity Module) are tightly integrated and the abbreviation SIM was typically used to refer to both aspects together;
- In 3G, the hardware is referred to UICC, while the UMTS SIM is referred to as the USIM (Universal SIM) and an IMS (IP Multimedia System)-capable SIM is called an ISIM;

As many UICCs are now multi-application, it is possible to load applications onto the card after distribution, typically via OTA (Over The Air).

Alternatively, the credential platform may be implemented in a Secure Element, in a secure µSD card, or equivalent solution. Java Card and MULTOS became popular implementation bases for such a Secure Element. It is relevant to consider the Global Platform suggested approach[2,] where a Trust Service Manager (TSM) governs the installation of applications on-card. There can be multiple security domains for multiple application issuers, all coexisting on the same physical card.

Alternative 2 Asymmetric credential on a central server

The asymmetric credential may alternatively be stored in a central HSM, and the mobile phone then authenticates against the central server. In such a set-up, the user authenticates himself against the phone (e.g. with a PIN), which enables the usage of a symmetric secret key stored on the phone. Please note that this is typically a dedicated key, and not the key K from the phone, since this one is reserved for MNO phone-to-network authentication. Using the symmetric secret key on the phone, the user authenticates himself against the central server. The central server delivers an authentication ticket to the application that the end users intend to use.

Obviously, for a particular country it may be relevant to offer both alternatives. This would allow the citizen freedom of choice, which leads to higher adoption rates.

Local applications

The stand-alone application on the phone should allow identification and authentication of a citizen. This should support:

- First line inspection, an examination done without tools or aids that involves easily identifiable visual (or other) features for rapid inspection at the point of usage;
- Second line inspection, an examination that requires the use of a tool or instrument (e.g., a reader, a scanner, an application) to discern a genuine from a fake credential; in case

[2] The integration of the ETSI framework and the Application management framework of GlobalPlatform is standardized in the GP UICC configuration

biometrics would be stored within the credential, these could be read out and compared to a life capture;

- Third line of inspection, an examination in a specialised laboratory. In-depth logical and physical inspection of the identity safeguards by experts.

On-line applications on the phone follow the client/server model, and consider the application-level protocol stack (SMS, TCP/IP, or a combination).

4.4.3 Service Provider MeID applications

A service provider can be defined as a private or public entity (or a combination) that offers a certain service to a citizen. This service could come in the form of a browse-able website or the server part of a client/server application (either through SSL or through signed or encrypted SMS). This can be freely chosen by the service provider.

The service provider can make its service available through an **SSL enabled website or server application.** When the service provider makes an SSL-enabled web site or server application available to a citizen, PKI/SSL good practices should be followed. It is up to the service provider to ensure that the functionality offered by the website or application is viewable on the citizen's device. If a service provider opts to use an application rather than a website, it is up to the service provider to ensure that the application is made available to the citizen. Service providers could also publish a service that can be accessed through the **signed or encrypted SMS**, which would eliminate the need for IP-based network connectivity for both citizens and service providers. The citizen would sign or encrypt an SMS, using one of the private keys contained on his SIM card, and send the SMS to the service provider. Again, PKI good practices should be followed.

4.4.4 The eID infrastructure

As the design of the eID infrastructure depends on the vision and scheme, we will discuss only the key aspects of the most important components. The **identity repository** is preferably under control of the government. It contains all relevant information about a person required by legislation, such as name, gender, address and possible biometric information such as a photograph or fingerprints. Each person is identified by a unique identification code. This identification code (or a derived pseudonym) can be used to link with other databases (for example MNOs, health service providers, etc.). The need for anonymous or pseudonymous services should be considered here. The identity repository may include the **registrar** functionality. It may equally include the required **CA** functionality such as cryptographic root keys and citizen's certificates. In case the CA functionality is not included in the identity repository, it can be provided as a service.

The **Mobile Identity Repository** and its relationship with the identity repository should ensure that all information contained in the M-IDREP should be accurate, integer and synchronised with the identity repository. It should respect privacy regulations, and all information contained within it should be adequately protected. The M-IDREP would make use of the citizen identity repository, but would not be part of it. It is better to separate the two, as they both serve a different purpose: the citizen identity repository would eventually contain information about all citizens, and can be used by a variety of applications. The mobile identity repository would be used solely for registering and issuing the subset of mobile ID's. For the Mobile Network Operator, key aspects to be addressed include:

- Type of SIM/UICC in use;
- The MNO's willingness to move to other cards if required;
- The choice whether the MNO will act as the Issuer or not;
- The relationship between the MNO and the TSM;
- Importance of key renewal.

The **Certification Authority** is used to securely create, manage, distribute, use, store and revoke digital certificates. Among its many components, it typically includes the core Certification Authorities components such as the root and operational keys and signers, the Registration Authorities (RA's) and web services where the CRL or OCSP can be consulted. A CA can be considered as the entity that actually creates, signs and issues certificates, while the RA only performs registration-related tasks on behalf of the CA. Generally, it enters into an agreement with the CA to collect and verify each subscriber's identity and information that is to be entered into the certificate. In the MeID scheme, the CA can operate its own RAs, or can make use of the registrar's function of the identity repository. The CA would be used to offer certificates both to citizens and certain applications. Of course, it would offer standard services such as OCSP checking and CRL publishing. Under no circumstances should the CA have access to a citizen's **private key**. A citizen's private keys should remain in the sole possession of the citizen, securely stored on his or her mobile device.

With regard to Trust Service Providers, what is required depends on the vision, scheme and selected Trust Model.

5 Sample application of the Toolkit's framework

Worldbank, together with its partners and sponsors, envisages the launching of the toolkit in a specific country. To improve the probability of a successful outcome of such launch, reflections were made on those issues that need to be addressed prior to a launch. These include the existence of an appropriate regulatory framework, including supporting laws and civil repository system, as well as public private partnership (PPP) model. Other issues are the existence of a national identity database, mobile network operator collaboration and ensuring that the objectives of both government and private parties are met. Furthermore in case a mobile phone-based solution would be selected, extensive mobile penetration, portability of the mobile phone numbers between the mobile network operators, and the security of the networks as well as of the SIM/USIM need to be considered. The list of potential candidate counties include but is not limited to: Nigeria, Ghana, Rwanda, Gabon, Senegal, Togo, Ethiopia, Tanzania and Burkina Faso.

When evaluating the situation in a potential candidate country, following points can be expected to require particular attention (see fig. 2). At the supervision layer, the existence of multiple registers is often reflected in silo legislation. Furthermore, eSecurity (eg cryptographic functionality for authentication, signature, validation, etc) is often not sufficiently regulated to support legal effect of electronic transactions. Electronic credentials are not commonly deployed, and eGovernment applications may be limited. There might be no local CA or TSPs, and there might be no single reliable source of identity and authentication. On the other hand, there might be many partial sources, each focussing on specific parts of the population (birth, election, healthcare, death, passport, ...).

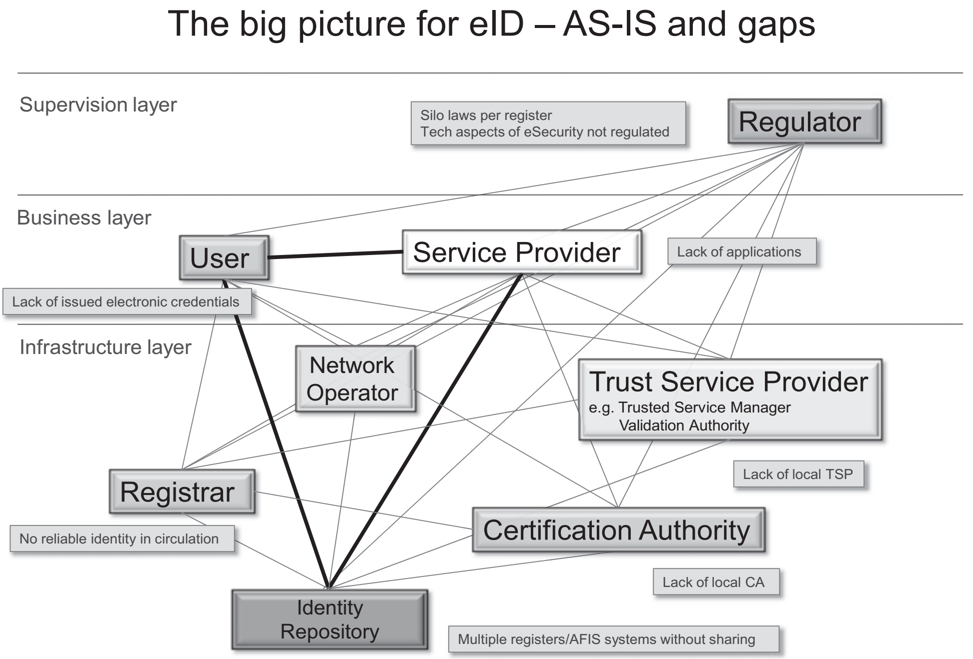


Fig. 2: The eID framework with sample gaps

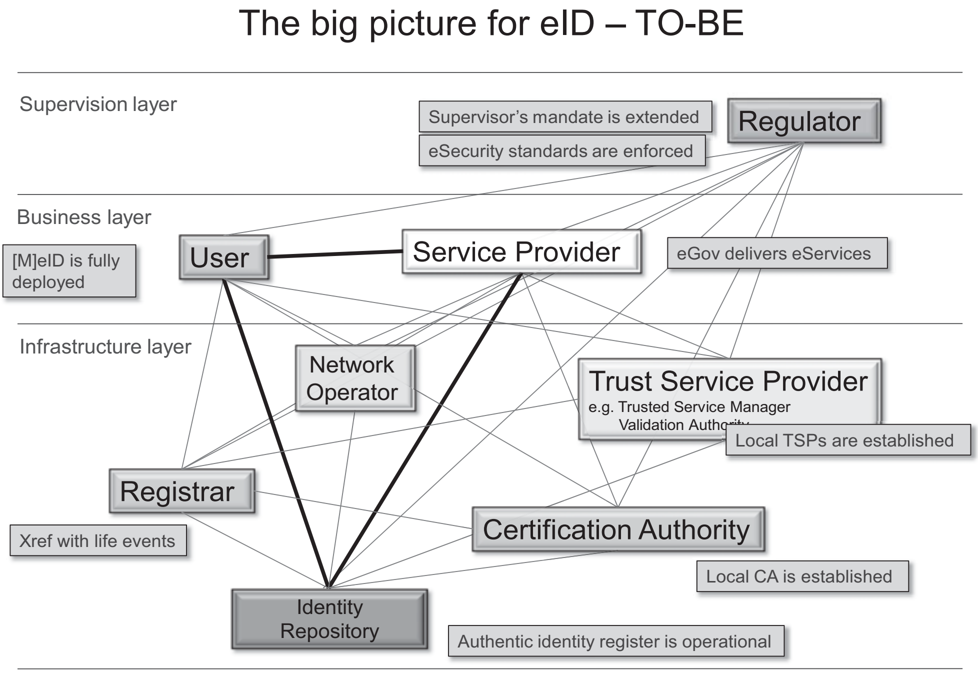


Fig. 3: The eID framework with sample actions

The framework can then also be used to identify the key activities that need to be undertaken (see fig. 3). At the supervision layer, the Supervisor's mandate may have to be extended to cover all relevant aspects, and eSecurity standards are to be defined and enforced. At the business layer, the [M]eID credential is to be deployed, and eGovernment services should be available in those areas offering most value. At the infrastructure layer, CA's and TSPs need to be established, and the Registrar function of the CA should make use of the possible cross-reference information that can be offered from the various registers such as Birth and Death, and potentially any other available registers. Finally, a recognised authentic identity register should be established as the foundation.

6 Conclusion

With regard to the key technology features of a [M]eID solution, the Toolkit proposes a framework model to allow the distribution of roles and responsibilities of the various stakeholders and participants across different layers and components.

The eID Scheme may select a 'virtual' credential, i.e., it can define high-level eID specifications, and certify various implementations on different platforms. The eID Scheme may also propose different levels of security, each of which can be implemented on different platforms. This would on one hand allow citizens to select the credential platform they prefer, while on the other hand allow Service Providers to specify minimal security levels for their applications. In order to offset some of the challenges of the Registrar function, cross-referencing with well-established registers is recommended.

It is recommended that a country applying the toolkit should strive to organise an implementation project in at least three parallel tracks that should have common objectives. Implementing technology should go hand in hand with implementing the business model(s) and applications, as well as the required regulation.

References

[LinkedIn] LinkedIn group: http://www.linkedin.com/groups?gid=4627623

[STORK] http://www.eid-stork.eu es well as http://www.eid-stork2.eu

The INDI Ecosystem of privacy-aware, user-centric Identity

Lefteris Leontaridis[1,2] · Thomas Andersson[2] · Herbert Leitold[3]
Bernd Zwattendorfer[3] · Shuzhe Yang[4] · Pasi Lindholm[5]

[1]Netsmart SA
lld@netsmart.gr

[2]IKED
{lefteris.leontaridis | thomas.andersson}@iked.org

[3]Technische Universität Graz
{herbert.leitold | bernd.zwattendorfer}@a-sit.at

[4]Goethe Universität Frankfurt
Shuzhe.Yang@m-chair.net

[5]NorthID Oy
pasi.lindholm@northid.com

Abstract

This paper presents a Roadmap to a Personalized Identity Management Ecosystem Infrastructure supporting Individualized Digital Identities (INDIs). The INDI ecosystem can enhance privacy by giving individual persons the ability to control with whom they share their identity data and under what conditions, while acting in a private, public or professional capacity themselves or through an authorized proxy. The role of intermediate Operators in a market for privacy-aware identity services offering individual choice is a key concept underpinning the INDI vision and is expected to contribute to the emergence of privacy-sensitive business models that differentiate from current data aggregation practices of commercial actors. The conceptualization and roadmapping was conducted by the GINI-SA project (2010-2012) that presented its outcomes and recommendations towards the main stakeholder communities: Industry, Government and Research. The material contained in the paper was extracted from the deliverables of the GINI-SA project as referenced. The GINI consortium is now engaged with the follow up stage devoted to implementation as its key partners continue to work together under a cooperation agreement aiming to continue promoting the GINI vision and lead to its implementation.

1 Introduction and Background

Information and communication technologies (ICT) exert a major societal and economic impact on virtually all countries and industries. They increasingly influence our daily lives and are in the process of transforming societies around the world. New applications and services are contin-

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_5, © Springer Fachmedien Wiesbaden 2013

uously becoming available online. Their maturity varies from simple informational services to sophisticated online transactions in e-Commerce, e-Government, e-Learning, e-Health, and so forth. With convergence, fixed and mobile networks are fusing whereas social networks are on the rise and others yet to evolve.

Despite the evidence of positive impacts, however, yet unresolved issues hinder a fulfillment of the potential benefits of ICT. This applies particularly to the fundamental task of achieving reliability, trust, integrity and accountability in connection with identity management and related services. Despite its importance, thus far there has been a lack of progress in putting in place a comprehensive framework for effective services development in this area. As a consequence, much digital communication is now plagued by a patchwork of half-hearted identity solutions, which is interrelated with the presence of other outstanding challenges such as accountability, security, traceability, interoperability, and lack of trust.

Against this backdrop, research undertaken by the GINI-SA project has identified the potential benefits at hand from putting in place orderly conditions for operator services meeting with the diverse needs of a multicorner model that comprise individual users, relying parties and data bases. The GINI Roadmap [GINI 5.1] has outlined timelines and milestones of a process for realising such an objective.

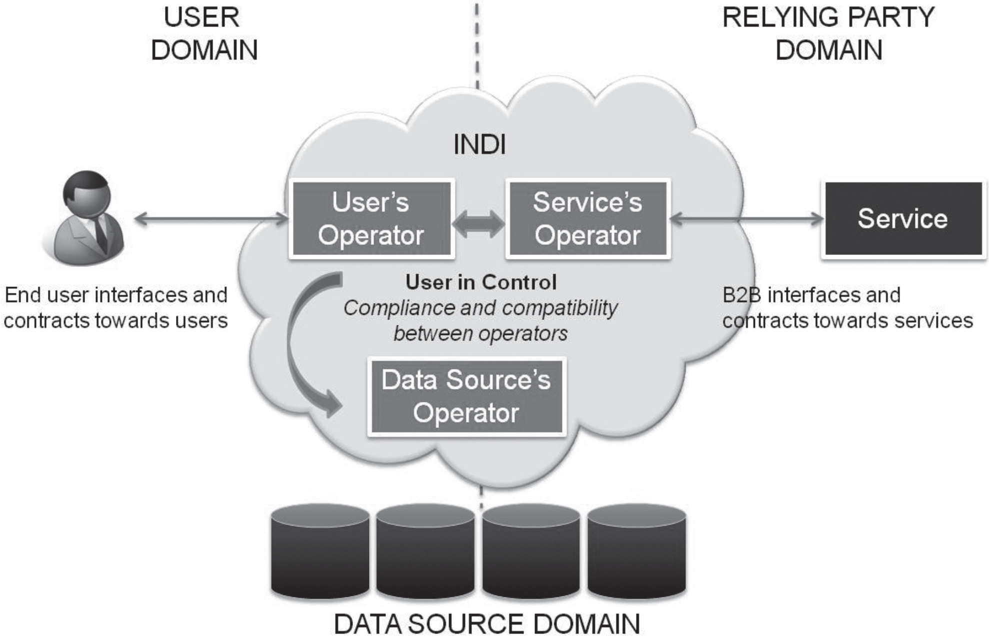

USER DOMAIN
RELYING PARTY DOMAIN
INDI
User's Operator
Service's Operator
Service
End user interfaces and contracts towards users
User in Control
Compliance and compatibility between operators
B2B interfaces and contracts towards services
Data Source's Operator
DATA SOURCE DOMAIN

Fig. 1: The multi-Operator model for an INDI ecosystem [GINI 5.1]

In practice citizens only have limited control and knowledge of how and where their identity data are collected, stored and processed digitally, resulting in severe problems with privacy, lack of trust, high transaction costs and economic inefficiency. No international market has yet evolved for user-centric identity services with viable business models that factor in the protection of privacy. A digital identity ecosystem needs to emerge, capable of enabling citizens to exercise control over their digital identities and to exploit the commercial potential of more effective utilization of user data.

Given the advance of cloud computing and interoperbility between systems and data bases, the potential benefits of the INDI ecosystem are becoming acute. Progress requires, however, determining the prerequisites for viable operator functions serving users, relying parties and databases in a secure and reliable manner. This in turn hinges on working out the architecture for inter-operator functions in the multi-corner model, outlined in Figure 1.

The GINI vision for an Individualized Digital Identity (INDI) ecosystem allows for a decentralised structure with flexibility and the capacity to handle changes in technology and government requirements, without being overly legalistic and without single points of failure. At the same time, there is need of over-archiching coordination and certification of the individual actors. This shall be integrated through a certificaton mechanism, issuing and administering User Certificates for individuals, organizations, Web-Servers, etc. Putting that in place will require transaction interfaces to users, organizations, companies, relaying parties and players on the eCommerce and ePayment scene.

2 Methodology

GINI-SA set out to develop a series of research results on technology, legal and regulatory, privacy, and business aspects of a user-centric identity ecosystem. A synthetic approach with a view to final recommendations and roadmapping was based on the linkages between the different dimensions and their combination for the realization of the INDI ecosystem.

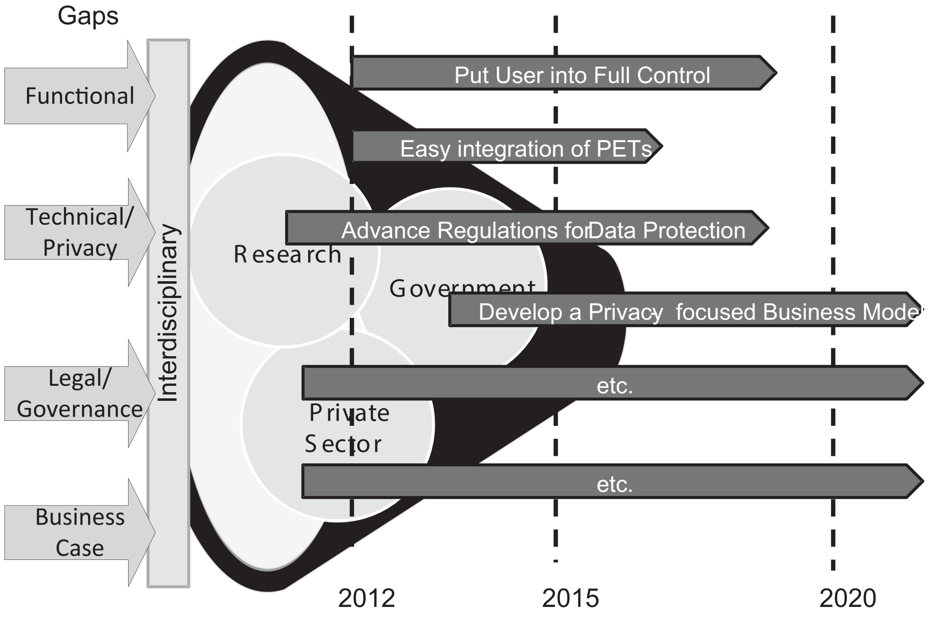


Fig. 2: Synthetic approach to GINI Roadmapping [GINI 5.1]

The GINI roadmapping methodology [GINI 5.1] started out with the gaps identified in the "technology gaps for longer-term research" document [GINI 2.2] and elsewhere in the GINI-SA project deliverables, ultimately compiled in the GINI roadmap [GINI 5.1]. An interdisciplinary approach is required to achieve synthesis of the drivers and expectations that flow from each of the main stakeholder groups – in Figure 2 depicted as Research, Government, and Industry – and lead on to future actions and developments associated with the key projected outcomes:

1. Putting users in control
2. Easy integration of Privacy Enhancing Technologies (PETs)
3. Advance regulation for Data Protection
4. Emergence of Privacy-focused Business Models
5. Vendor neutrality

3 GINI Vision – The INDI Ecosystem

As illustrated in [GINI 5.2], we refer to an Individual Digital Identity (INDI) as an identity claimed in the digital world by an individual who creates, manages and uses it. Individuals have the ability to establish and manage an INDI and to decide where and when to use it – while interacting with other individuals or entities. As a result, users are able to present their chosen, verified and verifiable, partial digital identity to other individuals or entities that constitute the relying parties with which they wish to build trust relationships in order to perform transactions for personal, business or official purposes.

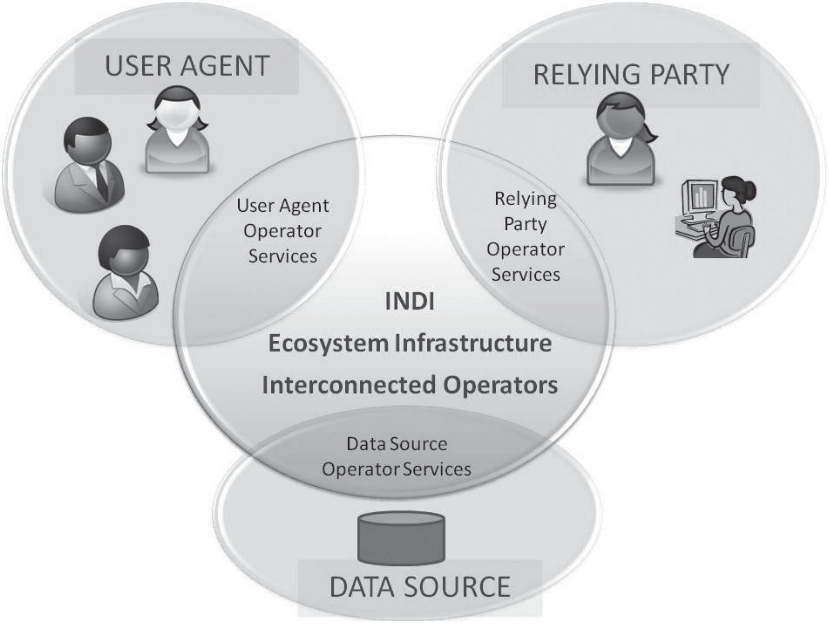

USER AGENT
RELYING PARTY
User Agent Operator Services
Relying Party Operator Services
INDI
Ecosystem Infrastructure
Interconnected Operators
Data Source Operator Services
DATA SOURCE

Fig. 3: INDI Ecosystem Infrastructure [GINI 5.2]

The INDI is a digital identity that is:

- Self-created by the individual;
- Self-managed throughout its lifecycle;
- Presented to relying parties (entities or other individuals) partly or wholly, depending on interaction requirements and trust relationships established;
- Verifiable against varied and variable data sources chosen by the individual and trusted by the relying party.

Within the INDI ecosystem (Fig. 3), three types of actors would interact with one another:

- An individual would need to access and manage the INDI and its use in various types of context through a User Agent interface where choices can be made about which data source to use and what identity attributes to disclose in each setting;
- A Relying Party would need its own interface whereby to accept and verify the use of an INDI and carry out its own side of the negotiation that establishes the trust relationship;
- Data sources such as authoritative identity registries or other types of identity service providers (e.g., from the financial sector, other business sectors, social media etc. would need to implement interfaces for attribute and assertion services in order to be used for verification and/or attribute exchange between individual users and relying parties.

GINI envisions these interfaces to be provided to the main actors through an infrastructure of interconnected INDI Operators. These are entities that provide INDI services and deploy INDI interfaces to the relevant actors, as seen in Figure 4 below:

In a nutshell, the vision has been summarized in [GINI 5.2] as articulated below:

> *GINI vision: Individuals' identities are self-created and self-managed throughout the whole lifecycle. Partial or full identities can be presented to any relying party (entities or other individuals) if appropriate trust relationships exist. The identities are verifiable against variable data sources chosen by the individual and trusted by the relying party. In the entire identity management system the individuals have maximum control of their digital identities.*

A critical aspect has to do with legal matters as digital interaction keeps growing within as well as beyond national borders, raising issues of international technical/legal interoperability, and transparency. Neither national nor international frameworks of the current time are up to the task of tackling the outstanding vulnerabilities.

Policymakers have fundamentally different views on the role of governments versus markets. Meanwhile, while the Internet is not bound by national borders, cybercrime along with various unethical behaviours originate in countries with particularly weak legislative tools.

4 A Multi-operator Market

Sometimes the operators co-operate to create more attractive markets. The basic idea is to connect the operators in such a way that the whole network is reachable with one single contract. The model is often called "four-corner model", because in this model, the user and the service provider (or other user) may have contracts with different operators and they can still interact (Fig. 4).

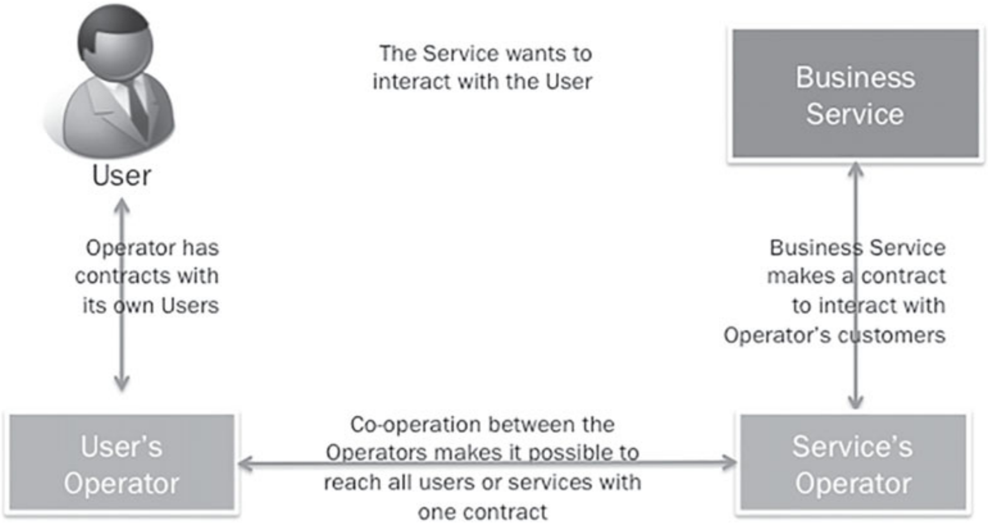

User
The Service wants to interact with the User
Business Service
Operator has contracts with its own Users
Business Service makes a contract to interact with Operator's customers
User's Operator
Co-operation between the Operators makes it possible to reach all users or services with one contract
Service's Operator

Fig. 4: Multi-operator Business Model [GINI 5.1]

A classic example of operator co-operators is the international telephone network, where the local operators co-operate internationally to enable long-distance calls (currently, it would be very difficult to imagine that with a normal telephone you would need to know the operator of the receiver of the call). Although the business model for Internet connection service providers follows multi-operator business model, it is common in many specialised Internet services that the competing service operators do not interact.

Another example of a multi-operator network is the international card payment network. The user can get the credit card from his local bank and use it in a foreign shop, which has a contract with their local banks. The banks have agreed on four-corner model and money settling between the banks and created a global infrastructure, which can be accessed through a single contract.

Although the credit card payments are a great example, they have also revealed one of the challenges of the four-corner model. As the card payment fee is always charged from the merchant, the banks have created a transfer fee system, where also the card issuer bank gets part of the fee. Although there is fierce competition for the consumers and for the merchants, the transfer fee mechanism sets a fixed fee, which is always included in the transaction. In time, that fee has not changed much and the authorities have decided to force the credit card industry transfer fees down. Similar discussion seems to take place with the mobile operator roaming fees.

The solution to the transfer fee problem is open pricing, where there is no transfer fee related to the actual service fee. However, it is very clear that once transfer fee has been used for a while, it is very difficult to change to open pricing.

4.1 Benefits and Drawbacks

Multi-operator business model has several benefits:

- It is much easier to create critical mass, when every new contract adds the total number of users or services;
- If the users or services can reach the whole network with one contract, the competing operators are true alternatives, which fosters competition;
- If one contract is required to access the whole network, the administrative burden of service provider and users goes down.

The multi-operator business models also have some clear challenges:

- Multi-operator market will not emerge by its own and it might be impossible to achieve a common understanding of the market between the competing operators;
- Agreement between the operators might be difficult to achieve, if the service is not standardised well – this allies to both business model and technical standards;
- Transfer fees might lock the pricing in such a way that the competition is no more real;
- There might be difficulties to find responsible operator, when something goes wrong in a multi-operator transaction;
- There is no geographical separation of operators such it does exist for telecom operators. In online markets this is not the case, and may also be a significant hurdle towards the adoption of a multi-operator model.

4.2 Possible Development Scenarios

The following characteristics are common in markets that are driven by two-sided market models:

- Competition between the operators is active – all operators compete in the same market field;
- If the service is widely accepted, reaching critical mass may be very quick;
- Since customers may choose their operators from those available, customers tend to switch operator to one that is more suitable for the customer's needs;
- Standardisation work is active to achieve better and easier co-operation between the operators;
- Innovation of one operator often benefits the entire market field.

5 Roadmapping Timelines

The actions are divided into short, mid, and long-term actions and are illustrated via timelines. We derive the timelines directly from the recommendations that have been developed throughout the project.

5.1 Research Timeline

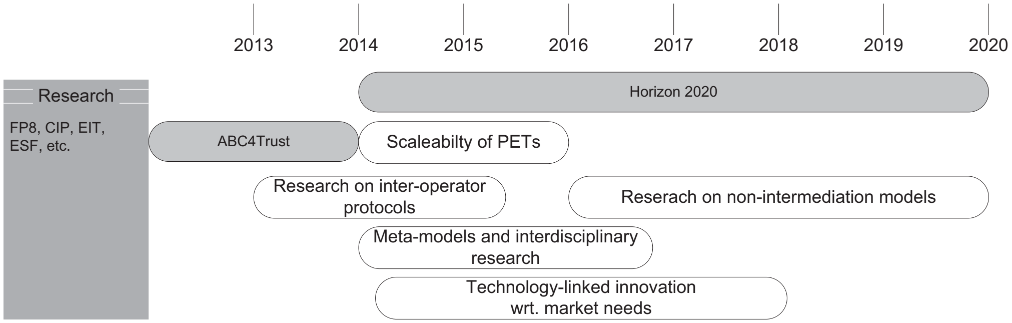


Fig. 5: Research action roadmap [GINI 5.1]

In this section a timeline of further research and development at a European level will be given. Particular attention will be given to the plans of the European Commission to go beyond the FP7 projects into Horizon 2020.

Recommendations that have been developed in the project and the corresponding suggestions on its timeline are:

1. Further research is needed on protocols for inter-operator and multi-operator communication. It must be investigated whether SAML might be sufficient for an INDI ecosystem, as it was developed for the corporate paradigm of identity and access management. Further research work is required on other protocols such as OpenID, OAuth, or the e-operating model [EPC] in order to assess if they could satisfy the requirements of a multi-operator model.
2. Further research is required on increasing the scalability and usability of Privacy Enhancing Technologies (PETs), such as the use of anonymous credentias. In addition, research is needed to investigate whether PETs are able to evolve to support a multi-operator model.
3. Further R&D work is needed on trust meta-models using innovative interdisciplinary approaches involving more than technology but also social sciences, with a strong dimension for international cooperation.
4. Further R&D work is needed on the encouragement and nurturing of technology-linked innovation, particularly on behavioural motivation drivers. Advances are needed on better understanding what is required for raising user awareness of identity management and privacy issues, and on exploring what associated market demand may arise from such awareness under different circumstances. International cooperation should be pursued in this area to account for cultural differences.
5. Further research is needed on non-intermediation ecosystems that would allow participating entities to interact directly between then without any intermediary involved.

Given these recommendations and indicative duration, Figure 5 [GINI 5.1] casts the actions across a timeline perspective. Note, that the grey block “Horizon 2020” is an existing initiative. It is not influenced by GINI-SA, but indicated as an important programme that can support the INDI vision.

5.2 Institutional and Governmental Timeline

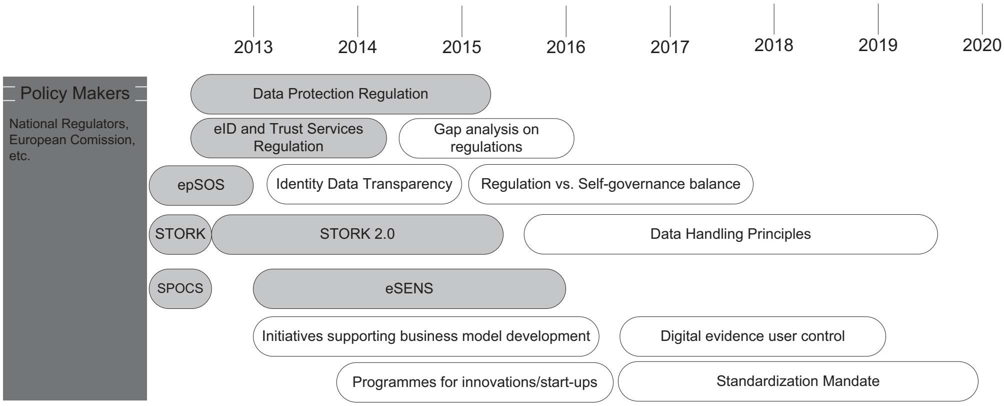

2013
2014
2015
2016
2017
2018
2019
2020
Policy Makers
National Regulators, European Comission, etc.
Data Protection Regulation
eID and Trust Services Regulation
Gap analysis on regulations
epSOS
Identity Data Transparency
Regulation vs. Self-governance balance
STORK
STORK 2.0
Data Handling Principles
SPOCS
eSENS
Initiatives supporting business model development
Digital evidence user control
Programmes for innovations/start-ups
Standardization Mandate

Fig.6: Policy action roadmap [GINI 5.1]

The recommendations given to policy makers are listed below. To derive a roadmap, we provide indicative timelines in Figure 6 above.

1. Data handling principles and decisions by governments will be pivotal for the emergence of an INDI-like ecosystem:
   a. Governments should allow their citizens to own their identity data, which resides in public registries, and should give those individuals the right and the facilities to control, under conditions that safeguard the public interest, the whole life cycle of identity data including enrolment, access, modification, re-use, or erasure. Apart from the obvious public good of respecting what can be considered as a basic human right, such moves by governments will actually facilitate the provision of eGovernment services by the public domain. Furthermore, they will increase the productivity of the public sector by reducing bureaucracy, minimise regulatory complexity and turn regulatory requirements into enablers rather than obstacles to cross-border interoperability, thereby reducing identity-related errors.
   b. Governments should build INDI-compliant Attribute Services on top of public data registries, so that these become accessible from other relevant actors within an INDI ecosystem. Policies must be put in place, as part of the ecosystem governance, in order to allow only privacy-respecting parties to gain access to those Attribute Services after obtaining the consent of the data owners.
   c. Governments should begin to accept INDIs for eGovernment services. There are already such providers but a move by governments to accept INDI-type eIDs for some eGovernment operations will dramatically increase the market scope, foster innovation and supply more choice for citizens and consumers.
2. Governments should put pressure on businesses to be transparent in the enrolment and transfer processes of identity data.
3. The best combination between government regulation and industry self-governance should be analysed and a process capable of underpinning the evolution of the best mix should be defined.Different governance models involving cooperation between the public and private sectors should be explored.

4. Governments should support initiatives that foster innovation and experimentation in the development of new business models while taking action to support interoperability among Operators (see Recommendations for Industry in Section 5.3).
5. Governments should ensure that digital evidence protects individuals, in contrast with today's situation where they are forced to rely on evidence produced and owned by service providers, thus preventing them from pursuing potential violations of their privacy. Creating user awareness of privacy issues can enable them to make informed choices. This is especially important since users seem willing to disclose personal information to gain an economic advantage.
6. Governments should work out the best way to foster innovative start-ups motivated by developing new services and taking them to market exploringnew and potentially disruptivebusiness models. While existing EC-supported programmes could already be used or adapted to fill this purpose, they need to be complemented with new instruments. National government initiatives as well as schemes promoting cross-regional and global collaboration should be explored and synergies with EU-wide initiatives should be leveraged.
7. The European Commission's Data Protection Regulation and the eID and eSignature Regulation need to be further analysed in case of gaps relating to the GINI ecosystem.
8. Governments should foster the adoption of standards to support existing policies and regulations. Standardization mandates should be created involving a broad group of interested parties, such as customers, industry, etc.

The GINI-SA project has examined the role of different actors in implementing these actions. In particular, a Roadmap and timeplan for the steps ahead have been worked out [GINI 5.1]. A snapshot and further development of this plan is presented in the next section. Figure 6 at the beginning of this section gives a roadmap setting the recommendations into a time-relation. As major on-going initiatives that revision of the Data Protection Directive and the revision of the Signature Directive to a comprehensive eID and Trust Services Regulation is indicated as grey boxes (including assumptions for its completion).

5.3 Industry/Market Timelines

GINI-SA has developed the following recommendations on industry. For each of the recommendations we give an indicative timeline. The likely timelines for implementing these recommendations are illustrated as a roadmap in Figure 7

1. Concerted collaboration (e.g interest groups, forums) should be initiated between ICT market players and potential service providers such as Cloud Operators and various identity intermediaries to build consensus and common understanding on what is required for broad industry-wide agreements on issues such as:
   a. Requirements for ensuring user-centricity and user control in the area of identity and attribute provision;
   b. Ways forward exploring to what extent an INDI-like ecosystem can be built around existing infrastructure, or what new infrastructure components need to be developed;
   c. Privacy-enhancement principles and rights of individuals including, but not limiting to, the requirements of the upcoming privacy-related regulation in the EU, so that the trust framework underpinning an INDI-like ecosystem may take shape.

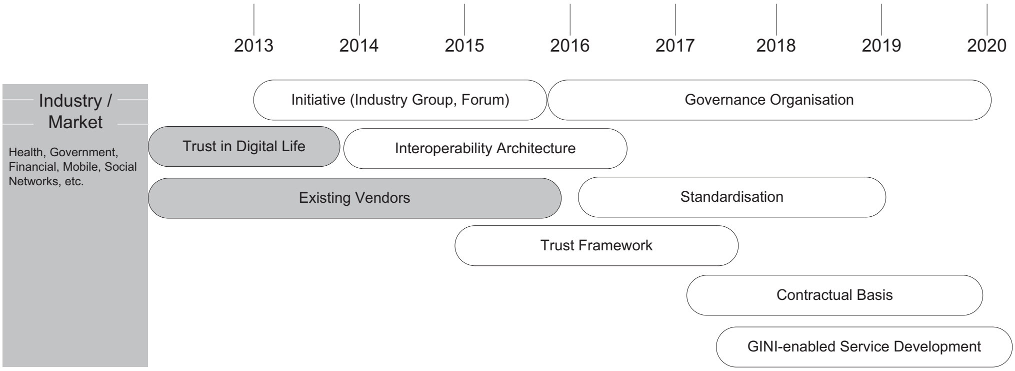


Fig. 7: Industry action roadmap [GINI 5.1]

2. Industry-wide standardisation initiatives should be undertaken, supported by major technology and service providers, in order to define various dimensions of inter-operator interfaces concerning:
   a. Interoperability and data handling processes ensuring privacy for users and confidentiality for relying parties;
   b. Portability specifications, aiming for compliance with upcoming EU regulation;
   c. Protocols, APIs, auditing and security for cross-operator relaying of claims and assertions.
3. Agreements on the GINI inter-operator architecture should be achieved, addressing funcamental aspects such as:
   a. Interface specifications between interacting entities such as operators and users, business services, or data sources;
   b. The inter-operator communication protocols and message must be defined;
   c. Interoperability must be achieved between operators to guarantee a fully-fledged INDI ecosystem across domains, sectors, or borders.
4. A thoroughly defined trust framework should be created, fostering the adoption and provision of an interoperable INDI ecosystem based on an inter-operator interoperability architecture.
5. A governance framework for self-regulation of industry should be agreed, addressing the necessary elements of ecosystem-wide operations based on:
   a. A trust meta-model underpinning user-centricity and privacy-enhancing requirements (see points 1 and 4 above);
   b. Inter-operator agreements for the relaying of claims and assertions, including possible charges (or lack thereof) and other conditions;
   c. Infrastructure interoperability around standardized inter-operator interfaces (see point 2 above).
6. Contracts between operators and their customers (users, businesses, data sources) should be carried out for allowing appropriate service provisioning.
7. GINI-enabled services should be designed and developed for penetrating the electronic identity market.

6 Conclusions

It is far from trivial to establish the infrastructure required for INDI. A multi-operator infrastructure is naturally more complex than a solution which is based on a single service provider. However, INDI offers the benefits that follow from not having to confront users with the complexity of the infrastructure nor with the nitty-gritty of the inter-actor relations that denote the system, but to allow such matters to be shielded behind the operator user interface.

No international identity service market has evolved on its own because of the mostly given local nature of the identity management, low revenue potential of the strong authentication services and security-driven clumsy implementations. GINI project believes that the market will not evolve by its own in the future either. However, the market can be created with help of a coordinated effort of operators, which specialise in the identity management. These operators will create INDI market and infrastructure.

An INDI Operator Market can become an international infrastructure, which requires multi-operator co-operation for many reasons:

- Market experience has shown that it is difficult to create critical mass for identity services with an operator-centric business model;
- Identity data is scattered and context-dependent, hence it is not a preferable scenario that all identity data would be collected to the databases of one single service provider;
- Internet is international by nature and in order to create attractive applications, they need to be international – in practise creation of international identity application is not possible without operator co-operation.

INDI business models will be based on multi-operator business model, which is two-sided or even multi-sided. In order to promote competition, we suggest that transfer fees were not used from the beginning, but open pricing would be introduced from the beginning of INDI implementation.

Summarizing the main recommendations included in [GINI-D5.1] and [GINI D5.2] as well as in Chapter 5 above, we propose the following main actions to be taken up by relevant actors to make the GINI vision of a user-centric identity management system become reality:

- Research Community: Foster research on security and privacy-reserving technologies to allow for broader-adoption and applicability in GINI multi-operator architectures.
- Governmental/Institutional Community: Governments should follow the GINI vision and allow their citizens to own their identity data, which resides in public registries, and should give those individuals the right and the facilities to control, under conditions that satisfy the public interest, the whole life cycle of identity data including insertion, access, modification, re-use, or erasure of identity data.
- Industrial/Market Community: Agreements on the GINI multi-operator architecture should be achieved. Based on concerted collaborations between interest groups and GINI stakeholders topics such as standardization, the establishment of a trust framework, or governance organisation must be addressed. GINI-enabled end user services must be developed and deployed with high volumes of users and transactions.

Acknowledgements – Disclaimers

GINI-SA has been funded with support from the European Commission under the 7th Framework Programme Theme ICT 2009.7.3 ICT for Governance and Policy Modelling (contract no: 258630). Any opinions, results, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the European Commission.

References

[GINI 5.1] D5.1 – A longer-term research and implementation roadmap towards a fully user-centric INDI ecosystem, GINI-SA FP7 project 258630, 2012.

[GINI 5.2] D5.2 – White Paper on the establishment of an INDI Operator Market across the EU, GINI-SA FP7 project 258630, 2012.

[GINI 2.2] D2.2b: Technology Gaps for Longer-Term Research, GINI-SA FP7 project 258630, 2012.

[EPC] EPC e-Mandates e-Operating Model – High Level Definition, http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=400, 2010

Human Factors, Awareness & Privacy, Regulations & Policies

Enhancing Transparency with Distributed Privacy-Preserving Logging

Roel Peeters[1] · Tobias Pulls[2] · Karel Wouters[1]

[1]KU Leuven & iMinds, COSIC (Belgium)
{roel.peeters | karel.wouters}@esat.kuleuven.be

[2]Karlstad University, PriSec (Sweden)
tobias.pulls@kau.se

Abstract

Transparency of data processing is often a requirement for compliance to legislation and/or business requirements. Furthermore, it has recognised as a key privacy principle, for example in the European Data Protection Directive. At the same time, transparency of the data processing should be limited to the users involved in order to minimise the leakage of sensitive business information and privacy of the employees (if any) performing the data processing.

We propose a cryptographic logging solution, making the resulting log data publicly accessible, that can be used by data subjects to gain insight in the data processing that takes place on their personal data, without disclosing any information about data processing on other users' data. Our proposed solution can handle arbitrary distributed processes, dynamically continuing the logging from one data processor to the next. Committing to the logged data is irrevocable, and will result in log data that can be verified by the data subject, the data processor and a third party with respect to integrity. Moreover, our solution allows data processors to offload storage and interaction with users to dedicated log servers. Finally, we show that our scheme is applicable in practice, providing performance results for a prototype implementation.

1 Introduction

Transparency is recognised as a key privacy principle, e.g., in the EU Data Protection Directive 95/46/EC Articles 7, 10, and 11; and in the Swedish Patient Data Act ("Patientdatalagen") SFS (2008:355). The Swedish Patient Data Act states that every patient have the right to see who has accessed their electronic healthcare record (EHR), i.e., access logs to EHRs have to be kept and made available to patients. This kind of transparency of data processing is often a requirement for compliance with legislation and/or business requirements, as well in healthcare as in other sectors, e.g., bookkeeping in the financial sector. Transparency of data processing, in general, may increase end-users' trust in the data processor[1], especially if the data processing is distributed as in cloud computing [KJM+11]. The need for building trust is also a big part in why transparency towards citizens is a key element of eGovernment services [UN12].

[1] We use the technical terminology of data processor and user, as opposed to the EU Data Protection Directive in which a more formal/legal terminology (data controller, data subject) is used.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_6, © Springer Fachmedien Wiesbaden 2013

One, if not the primary, role of a *privacy policy* is to inform potential users about how personal data will be processed by a data processor. It should state what personal data is requested for which purpose, whether the data will be forwarded to third-parties, how long the data will be retained, and so on. A potential user reads a privacy policy *before* any data is disclosed, so that a user can give *informed consent* to the data processing by the service provider. The scheme presented in this paper is used by a user *after* the user disclosed data to a data processor. Our scheme can provide a user with a description of the *actual data processing* that took place on the user's data. Conceptually, access to this information enables a user to *verify* that the actual data processing of the data processor are in line with the privacy policy. Figure 1 depicts this setting for the user Alice and data processor Bob.

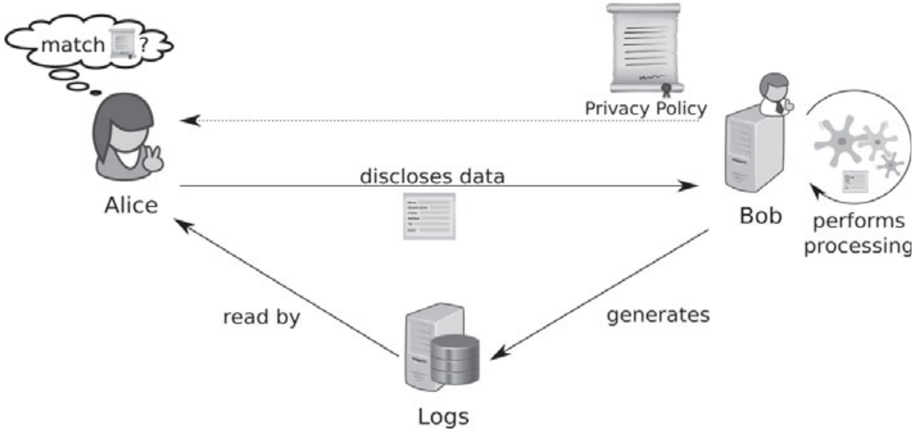


Fig. 1: Transparent data processing.

When attempting to make data processing transparent and determining what an adequate level of transparency is, there are a number of social and economic issues that need to be taken into account beyond (sometimes purely) technical considerations of *what* to make transparent to *whom*. For example, employees of a data processor may experience the requirement of transparency as a breach of their own privacy [Robe09]. For data processors, as recognised in recital 41 of the EU Data Protection Directive, too detailed descriptions of data processing risk revealing business-sensitive information of the data processor, such as trade secrets.

Most commercially deployed logging systems operate on a single system and focus on a single goal: providing deep and fast analysis into massive amounts of log data, for System Information and Event Management (SIEM) purposes: e.g., to detect system malfunctioning and security breaches. Some of these logging systems include cryptographic methods to validate the log's integrity in a simple way.

Our proposed logging scheme focuses on which guarantees and services can be delivered to the end-user of a data processor, based on the events that this data processor logs for its users. Furthermore, by only allowing the user whose personal data is being processed to read the logged information, the negative effects of transparency (e.g., logs cannot be misused to monitor the employees' performance) are minimised. Compared to commercially available logging systems, this is more than a shift of focus; it introduces very challenging questions about trust, privacy and confidentiality. Adapting existing logging systems to answer these questions is far from trivial as these questions touch the core of the logging system.

The paper is structured as follows: in Section 2, we present our design goals and rationale. Section 3 introduces our proposed logging scheme. We present a performance evaluation of our prototype implementation in Section 4. Our solution is compared to related work in Section 5. Finally, Section 6 provides concluding remarks.

2 Design Goals and Rationale

When implementing a log system for transparency of data processing, there are several privacy and security issues that need to be addressed. Take for example the case of electronic healthcare records: knowing who has accessed a patient's medical records is sensitive information. In fact, even knowing that a person has been a patient at a particular medical institution may be sensitive. So, not only the content of the log entries is sensitive information, but also merely the fact that log entries exist for a certain individual (a patient in this example) can be sensitive information. Furthermore, imagine the case of an attacker (such as malicious medical personnel) illegitimately accessing EHRs. In such a case, the offenders are likely to attempt to cover the traces of their actions, for example by deleting the generated log entries. Therefore, alterations to log entries need to be detectable. Similar arguments can be made for the case of business-sensitive information being logged for a company.

The content of log entries is submitted by the data processor, to a log server. The logging of data can be completely outsourced and aims to minimise impact on existing processing infrastructure. Coupling of the process to the logging is loose. Log entries are fully confidential, and hold identification and authentication metadata, allowing only that end user to identify the log entries related to a certain process, and to check the integrity of the logged data. The data processor ensures the confidentiality of the data to be logged, also keeping these data confidential for the log server. The log server adds the identifying and authentication metadata, both for the end user and data processor, ensuring the integrity of the log trail. The log process is also auditable: a log server can be forced to reproduce the entire set of log entries, related to a user or the data processor that generated the data to be logged. In other words, neither data processor nor log server needs to be completely trusted.

The log server keeps a *state* that is *updated* each time a log entry is created in such a way that it is hard to recover the previous state values once an update is complete. This is the mechanism at the core of our *prior to compromise* adversary model: we assume that log servers (and data processors) are *initially* trusted and will at some point in time *t* become compromised by an adversary. Due to the fact that the state kept by log servers is continuously updated as log entries are created, an adversary is unable to reconstruct prior states needed for successfully manipulating log entries created prior to compromising the log server. Fig. 2 illustrates the interplay between log entries, the log server's state, and our adversarial model.

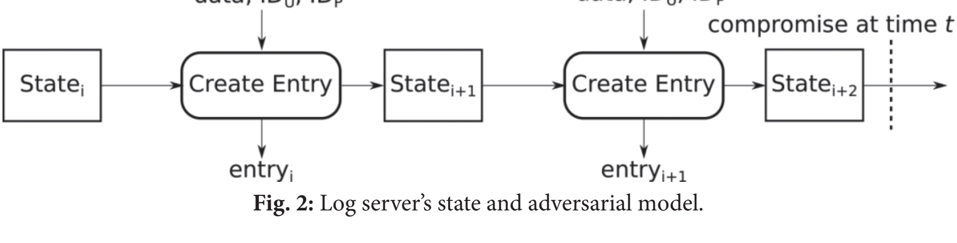


Fig. 2: Log server's state and adversarial model.

To ensure the "anonymity" of the logged data, we need more than just confidentiality. Especially if one is to serve the logged data publicly. It should be impossible for attackers given only the logged data to link multiple entries concerning the same end user together.

Finally, we need to take another important aspect of data processing in account, namely that it is often distributed. Data concerning users may be shared by the data processor to other data processors for additional processing. Also, each data processor can be logging to different log servers. This means that there should be support for distributed processes, such that these can be logged and the logging scheme itself can also be distributed across several log servers. An example of such a distributed setting is depicted in Fig. 3. Alice discloses data to Bob, the initial data processor. Bob then shares (part of) Alice's data with the downstream data processor Charlie, who in turn shares (part of) Alice's data with data processors Dave and Eve. While data processors Bob, Charlie, Dave and Eve process Alice's data, all of them continuously log descriptions of their processing (dashed lines) to their, potentially different, log servers. Alice can later reconstruct the *log trail* of the data processing on her data.

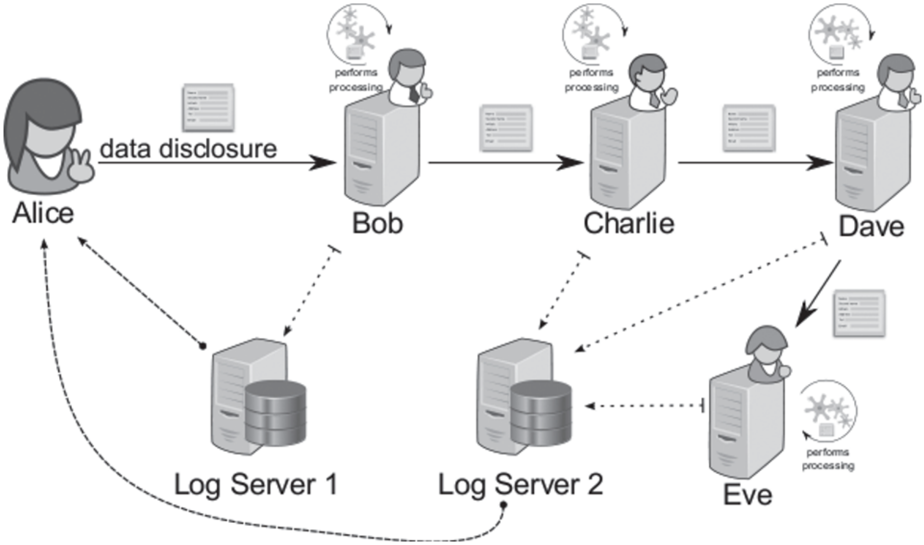


Fig. 3: Distributed Logging.

For distributed processes, also the user identifiers used across the different data processors should be unlinkable to ensure maximal anonymity of the logged data.

To conclude, a logging system for transparency should have the following security and privacy properties:

- **Forward-Integrity:** any changes (including deletion[2]) of entries committed to the log prior to the log server's compromise can be detected.
- **Confidentiality:** given a log entry, only the user the log entry concerns can read the logged data.

[2] Schemes that do not support deletion detection are subject to so-called truncation attacks, for which the adversary can delete one or more consecutive entries at the end of a log.

- **Unlinkability of Log Entries:** given the log and the current state of the log server, no two entries in this log that relate to the same user (or data processor when multiple data processors are using the same log server) can be linked.
- **Support for Distributed Processes:** logging for the user continues when going from one data processor to the next, the log trail can be reconstructed across the different data processors.
- **Unlinkability of User Identifiers:** in case of distributed processes, user identifiers used across multiple data processors are unlinkable.

3 Our Logging Scheme

In this section we present our logging scheme. First we give an overview of the internals of the log server and then we discuss the most important logging operations.

3.1 Log Server

The log server in our logging scheme, depicted in Fig. 4, stores all log entries and keeps state information, which is updated with each new log entry, for each registered user and data processor.

A log entry consists of five fields:

- **Data:** The data field contains the actual data to be logged in an encrypted form, such that only the user can derive the plaintext.
- **IC(U):** The *index chain* field for the user serves as an identifier for the log entry for the user. The values of this field create a chain that links all log entries for the user together. Only the user can reconstruct this chain.
- **DC(U):** The *data chain* field for the user allows the user to verify the validity of this log entry. All entries that were created for this user are chained together, leading to cumulative verification.
- **IC(P):** The index chain field for the data processor.
- **DC(P):** The data chain for the data processor.

A state consists of four fields:

- **ID:** The identity of the user/data processor. This identity also serves as a public encryption key for the user/data processor, for which they have the corresponding private decryption key.
- **DC:** The current data chain intermediate for this user/data processor. This intermediate will be used while constructing the next log entry for this user/data processor.
- **IC:** The current index chain intermediate for this user/data processor. This intermediate will be used while constructing the next log entry for this user/data processor.
- **AK:** The current authentication key for this user/data processor. This value will be used while the next log entry for this user/data processor. This value will also be used to update the state (DC, IC and AK fields) for this user/data processor.

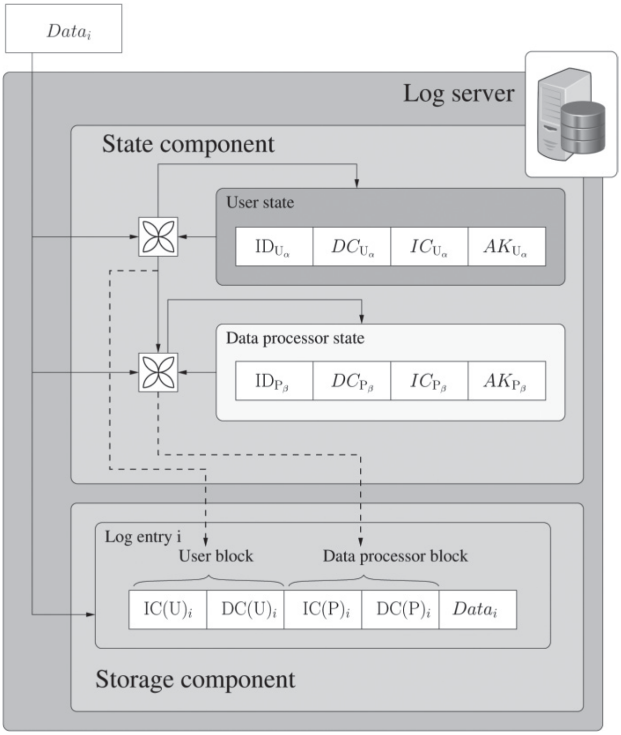


Fig. 4: Log server.

3.2 Start Logging

Before a data processor can start logging data for a user, the user needs to be set up at the log server. The user will present his identity to the data processor, which in turn passes it on to the log server. The log server initialises the user's state for this identifier and returns the initial authentication key to the user through the data processor. The user will need this initial authentication key to reconstruct his log trail (see section 3.5).

To keep the initial authentication key hidden from the data processor, it is encrypted under the user's identity, which also serves as public encryption key in our scheme. The user knows the corresponding private decryption key and can thus obtain the initial authentication key. To guarantee the origin of the initial authentication key, it is signed by the log server prior to encryption.

3.3 Creating Log Entries

When a data processor performs processing on a user's disclosed data, it logs a description of the processing to the log trail of the user located at the log server used by the data processor. The data processor first signs the data to log (to prove the origin to the user) and then encrypts the data and signature under the identity (public encryption key) of the user. Next, the data processor sends the resulting ciphertext, together with the user identifier to the log server who creates a log entry for this user.

A log entry consists of three parts: the user block, the data processor block and the data. The data is the ciphertext as provided by the data processor. The user block and data processor block are in part derived from the internal state kept by the log server.

A graphical overview of how the user block is generated and the user's state is updated, is given in Fig. 5. The index chain field is derived from the state kept by the log server. The data chain field is derived from index field from the log entry, together with the state kept by the log server. The authentication key is used to update the index and data chain intermediates, before the authentication key itself is updated. The data processor block is generated in a similar manner. The log server only needs to do symmetric key operations: hashes and MACs, which makes that creating a log entry is very efficient at the log server.

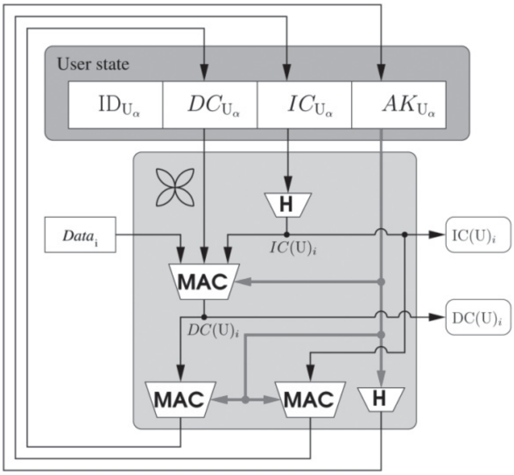


Fig. 5: Detail of creating a log entry: create the user block of the log entry and update the user's state.

3.4 Forking

For a data processor to involve another data processor in the processing of a user's data, the data processor needs to fork the transparency logging of data processing to the other data processor. When forking, the data processor needs to blind the public key that serves as an identifier for the user to prevent the transparency logging from being linked at both data processors for the user. Blinding a public key is done by applying a random blinding factor, which is passed on to the user. This blinding factor together with his original private key will allow the user to decrypt messages that are encrypted under this new blinded public key.

Forking is a protocol between two data processors A and B with their respective log servers. Data processor B will set up a new user at its log server for the blinded identity as provided by data processor A. Data processor B will sign (to prove its involvement in the forking to the user) the resulting ciphertext from its log server, before sending it back to data processor A. Data processor A will then create a new log entry at its log server that contains a forking marker, the identity of data processor B, the signed ciphertext and the blinding factor.

3.5 Log Trail Reconstruction

When the user disclosed data to the data processor, the user initiated the start logging protocol (see section 3.2), generating a user identifier and obtaining the initial authentication key from the data processor in the process. To reconstruct the log trail, the user first downloads all log entries, stored at the log server used by this data processor, linked to his identifier.

Starting from the initial identity chain field, derived from his identity and the initial authentication key, all following identity chain fields can be computed by evolving the identity chain field and authentication key in the same manner as the log server. The user can request all log entries where it can provide a valid identity chain field for.

Now the user can validate his log trail by evolving the data chain field from log entry to log entry. After validating the integrity of the log trail, the data fields of the log entries are decrypted and the signature of the data processor is checked.

The user can also request the latest identity chain intermediate in the log server's state. This mechanism allows the user to detect truncation attacks, in which the attacker deletes one or more consecutive log entries at the end of the chain.

In case the user comes across a forking marker, the user first verifies the signature by data processor B. Then he creates a new private key using the blinding factor, which can be used to decrypt the ciphertext, containing the initial authentication key at log server B. Now he can also reconstruct and validate his log trail at log server B.

4 Performance Evaluation

We used ECIES for public-key encryption and ECDSA for signature generation on the NIST P-256 elliptic curve. The selected hash function is SHA-256, which is also used in an HMAC construction to generate MACs. For these selected cryptographic key lengths, long term protection (from 2013 to 2040) is ensured [Ecry12].

A prototype of our scheme was implemented in the programming language Go. The first benchmarks are performed on a mid-range laptop (quad core 2.6GHz CPU and 8GB DDR3 RAM). Using Go's built-in benchmarking functionality, which will run a test until it is ``timed reliably'', we created Table 1 that provides a benchmark of the algorithms that make up our logging scheme. The benchmark shows that the main bottlenecks are operations related to encryption and signatures. As a consequence, data processors perform the bulk of the work when creating log entries. For log servers, creating log entries is fast. The only relatively costly operation at the log server is the setup of a user (which is also part of forking, i.e., log server B), needed to start logging for a new user, which presumably will be relatively infrequent. Decryption and verification for users are relatively costly.

Table 1: Benchmark of algorithms.

	Time [ms]	**Comments**
Start logging (log server)	25	
Create a log entry – data processor – log server	15 14,9 0,1	1 KiB data
Forking – data processor A – log server A – data processor B – log server B	45,3 15,2 0,1 5 25	From data processor A with log server A to data processor B with log server B
Verify log trail (user)	180	10 entries of 1 KiB data

To get a better idea of how our scheme would perform in practice as a deployed system, we extended our implementation:

- First, we transformed the data processor to a standalone service (similar to a Syslog server) to which other systems at the data processor send messages that should be logged. The data processor and log server *communicate securely* over a TLS connection. The data processor service is also offered over TLS.
- Next, we introduced the concept of *transactions*, analogous to transactions in relational databases. At the data processor service, starting a transaction creates a new buffer for messages to log for users. A transaction can then be *committed*, which takes all messages in the buffer and creates log entries of them. At a log server, a transaction buffer works in a similar way: a data processor can create a buffer of messages for users that can be committed to create log entries. Transactions at a log server enable the data processor to send messages to the buffer in parallel, since the order in which log entries are created are determined first when the transaction is committed, not when a log entry arrives at the log server.
- For the transaction buffers at a data processor we also added support for *parallelism*. When a data processor receives a message for a user to put into a transaction buffer, the processor spawns a new Go routine (lightweight thread) that performs the signing and encryption of the message for the user in the background. This way the data processor service can instantly acknowledge that a message has been stored in atransaction buffer, enabling the caller to return to its data processing. The computationally demanding cryptographic operations are then completed in the background of the service while waiting for the transaction to be committed.

The log server and the data processor were run in two different settings: local (L) and remote (R). The local experiment was run on the earlier described laptop. For the remote experiment, the log server was run at Amazon EC2 (Ireland) using a medium instance, the data processor in a private cloud at a Karlstad University (Sweden). The latency between the data processor and the log server at Amazon was on average 45.7 ms with a standard deviation of 0.3 ms. Table 2 shows the *goodput*, which is the throughput measured with respect to the data to be logged, for both the local and remote setting at 100 log entries per transaction. The average log entry generation time does not scale linearly with the size of the logged data. This is mainly due to the fact that the data to be logged is first signed and then encrypted before being sent to the log server, which involves relatively costly operations on the elliptic curve. The increased time in the remote setting is most likely due to the increased latency and potential bottlenecks at our Amazon EC2 instance.

Table 2: The goodput at 100 log entries per transaction.

Log entry size	1 KiB	10 KiB	100 KiB
Local setting	87 KiB/s	842 KiB/s	4149 KiB/s
Remote setting	52 KiB/s	497 KiB/s	1525 KiB/s

5 Related Work

The earliest work, to our knowledge, on achieving transparency of data processing by using cryptographic systems from the secure logging area is by Sackmann et al. [SaSA06]. Trusted auditors use secure logs of data processing as so called "privacy evidence" to compare the actual processing with the processing stated in a privacy policy that users have consented to. Wouters et al. [WSLP08] and Hedbom et al. [HPHL10] look at transparency logging schemes from another angle than the work of Sackmann et al.: users take on the primary role of auditors of the logged data that relates to them, removing the need for trusted auditors. Since log entries now relate to different users who are actively participating in the scheme, the setting becomes user-centric. This new setting leads to new privacy threats, in addition to the potential threats to privacy posed by the actual contents of log entries. Wouters et al. address the linkability issue between logs at different log servers in a distributed setting, while Hedbom et al. address the linkability between log entries in one log at one log server. These schemes (including our proposal in this paper) build upon the secure logging system by Schneier and Kelsey [SchK98]. A thorough review of related work in the secure logging area can be found in Pulls et al. [PWVG12].

In the context of privacy policy languages, Bournez and Ardagna [BouA11] identified the need for so called "sticky logs" (analogous to sticky policies that "stick" to data) that travel with disclosed data as the data is shared by data processors. These logs should contain a history of how the disclosed data have been used, whom it has been shared with, and so on.

Table 3 gives a comparison of our proposal to the related work, for the desirable properties as identified in section 2.

Table 3: Comparison.

	Forward-Integrity	**Confidentiality**	**Unlinkability Log Entries**	**Support Distributed**	**Unlinkability User Identifiers**
[SchK98]	Partial (truncation attack possible)	Yes	No	No	N/A
[SaSA06]	Partial (truncation attack possible)	Yes	No	No	N/A
[WSLP08]	No	Yes	No	Yes	Yes
[HPHL10]	Yes	Yes	Yes	No	N/A
[BouA11]	No	No	N/A	Yes	N/A
Our proposal	Yes	Yes	Yes	Yes	Yes

6 Conclusion

We introduced a privacy-preserving distributed logging scheme which can be used to enhance transparency of data processing. Our scheme generates a log trail for a user, typically the data subject of the process that is logged. Dynamic and distributed processes can be logged to distributed log servers. The log entries are world-readable, but the strong cryptographic properties of the underlying scheme ensure confidentiality and unlinkability in a broad sense. Last, but not least, we implemented our scheme in a robust prototype implementation and evaluated its performance. The initial timing results show that the scheme can be used in practice.

Acknowledgements

This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). Tobias Pulls has received funding from the Seventh Framework Programme for Research of the European Community under grant agreement no. 317550.

References

[BouA11] Bournez, Carine; and Ardagna, Claudio A.: Policy Requirements and State of the Art. Camenisch, Fischer-Hübner and Rannenberg: Privacy and Identity Management for Life, ISBN 978-3-642-20316-9, Springer, 2011, p. 295-312.

[Ecry12] ECRYPT II: Yearly Report on Algorithms and Keysizes (2012). D.SPA.20 Rev. 1.0, ICT-2007-216676 ECRYPT II, 2012.

[HPHL10] Hedbom, Hans; Pulls, Tobias; Hjärtquist, Peter; and Lavèn, Andreas: Adding Secure Transparency Logging to the PRIME Core. Bezzi, Duquenoy, Fischer-Hübner, Hansen and Zhang: Privacy and Identity Management for Life, ISBN 978-3-642-14281-9, Springer, 2010, p. 299-314

[KJM+11] Ko, Ryan K.L.; Jagadpramana, Peter; Mowbray, Miranda; Pearson, Siani; Kirchberg, Markus; Liang, Qianhui; and Leek, Bu-Sung: TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In: Proceedings of EuroPKI 2011. Camenisch and Costas: LNCS 6711, Springer, 2011, p. 584-588.

[PWVG12] Pulls, Tobias; Wouters, Karel; Vliegen, Jo; and Grahn, Christian: Distributed Privacy-Preserving Log Trails. Karlstad University Studies 2012:24, 2012.

[Robe09] Roberts, John: No one is perfect: The limits of transparency and an ethic for 'intelligent' accountability. Accounting, Organizations and Society 34(8), 2009.

[SaSA06] Sackmann, Stefan; Strüker, Jens; and Accorsi, Rafael: Personalization in Privacy-Aware Highly Dynamic Systems. Communications of the ACM 49(9), ACM, 2006, p. 32-38.

[SchK98] Schneier, Bruce; and Kelsey, John: Personalization Cryptographic Support for Secure Logs on Untrusted Machines. In: USENIX Security Symposium. USENIX, 1998, p. 53-62.

[UN12] United Nations Department of Economic and Social Affairs: UN e-Government Survey 2012. E-Government for the People. ISBN 978-92-1-055353-7, 2012.

[WSLP08] Wouters, Karel; Simoens, Koen; Lathouwers, Danny; Preneel, Bart: Secure and Privacy-Friendly Logging for eGovernment Services. In: ARES. IEEE Computer Society, 2008, p. 1091-1096.

Data Protection and Data Security by Design Applied to Financial Intelligence

Paolo Balboni[1] · Udo Kroon[2] · Milda Macenaite[3]

[1,3] European Privacy Association
Square de Meeus, 37
4th Floor 1000 Brussels, Belgium
{pbalboni | info }@europeanprivacy.eu

[2] FIU.NET
c/o Eisenhowerlaan 73, P.O. Box 90850
2509 LW The Hague, The Netherlands
udo.kroon@fiu.net

Abstract

EU Financial Intelligence Units ('FIUs') have recently started using the Ma^{3}tch technology as additional feature to the existing exchange of information via the FIU.NET decentralised computer network. The authors of the paper analyse this concrete case of data processing as a possible practical implementation of the data protection and data security by design principle. They conclude that the Ma^{3}tch technology can be seen as a valuable example of data protection and data security by design, as it can guarantee its fundamental elements such as data anonymisation, data minimisation and data security. Therefore, it is able not only to improve the exchange of information among FIUs and allow for the data processing in line with the applicable data protection requirements, but also remarkably enhance privacy of related data subjects. At the same time, the case study clearly shows that data protection and data security by design need to be supported and complemented by appropriate organizational and technical procedures to assure that the technology solutions devised to protect privacy will in reality do so.

1 Introduction

On both sides of the Atlantic the legislators encourage companies to use Privacy by Design to guarantee substantive and procedural consumer privacy protection at all stages of the development of their ICT products [Comm10; Fede12]. In order to do so, companies are expected to embed privacy protection systematically into their practices, from the planning stage to the deployment, use and ultimate disposal of their technologies. The EU has recently expressly included the principle of "Privacy by Design" into the revised data protection legal framework (the "**Draft Regulation**") [Comm12]. It requires companies as data controllers, and technology designers and producers, to "built in" privacy and data protection principles into the design of the ICTs from the planning stage in order to ensure that, by default, only personal data necessary for specific purposes are processed and data are not retained beyond the minimum necessary as regards their quantity and retention time, and other necessary tools to enable users to better protect the personal data, such as access controls and encryption. Furthermore, data controllers are obliged

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_7, © Springer Fachmedien Wiesbaden 2013

to adopt internal policies and to implement appropriate measures in order to demonstrate their compliance with this principle.

The authors will look at Privacy by Design from a very practical point of view, by analysing a case study on FIUs using the Ma^{3}tch technology. This technology is an additional feature to the existing exchange of information via FIU.NET, a decentralised computer network, used by FIUs in the European Union in their fight against money laundering and terrorist financing. Ma^{3}tch technology will be presented, analysed, and evaluated from the perspective of personal data protection. In doing so, the authors aim to answer the following research questions: How have the data protection requirements been taken into account when designing the technology? Does it comply with the data protection legislation? Are there any specific points to consider in relation to the rights and obligations based on the European legislative framework?

For the sake of clarity, it is important to mention that the analysis of privacy and data protection aspects related to the existing exchange of information via the FIU.NET decentralised computer network falls out of the scope of this paper. The authors analyse only data processing operations carried out via the Ma^{3}tch technology, assuming that previous data collection and storage as well as successive data exchange after a positive match are in compliance with the applicable laws.

The paper is structured as follows. Section 2 provides a description of the Ma^{3}tch technology. Section 3 shortly describes the relevant legal duties and obligations for FIUs, if in the course of their activities in which they process personal data. Section 4 deals with the main Privacy by Design features of the Ma^{3}tch technology – data anonymisation, data minimisation and data security. Section 5 highlights some points of concern for the technology being used improperly. The last section provides conclusions on the privacy and data protection implications on Ma^{3}tch technology.

2 Description of Ma^{3}tch technology

FIUs as central, national units in the EU Member States, for the purposes of combating money laundering and terrorism financing, need to assemble and analyse information on any facts which might indicate these crimes. As their core function, FIUs receive, and to a certain extent, request, analyse and disseminate to the competent authorities (e.g. law enforcement, prosecutorial authorities) financial information concerning suspected proceeds of crime and potential financing of terrorism, or information required by national legislation [Coun00; Parl05].

In this process FIUs face a challenge of dealing with two somewhat conflicting interests at stake: FIUs must know more about EU citizens and process their personal, often sensitive, data, for fighting money laundering and terrorism financing, while guaranteeing strong and effective protection of their privacy and personal data. When gathering intelligence, FIUs must cooperate and may request information exchange from FIUs in other Member States. To receive such information, FIUs use the FIU.NET decentralised computer network. FIU.NET enables exchange of information on EU citizens among national FIUs. Such exchange of information is regulated by a significant number of privacy and data protection regulations, resulting in a rather intricate legal framework [Schr09].

Recently, a new way of intelligent information and knowledge sharing – Ma^{3}tch – has been developed. The Ma^{3}tch is a technology which aims at improving the exchange of information among national FIUs by excluding unnecessary requests, improving timeliness and enhancing privacy. It thus seeks to provide an innovative solution that can serve both aims by way of autonomous and anonymous data analysis: guaranteeing FIUs' interest to collect information and protecting privacy and personal data of EU citizens.

Ma^{3}tch (autonomous anonymous analysis) [Kroo13] allows connected FIUs to 'match' their data with that of the other FIUs in order to check whether other FIUs have information on a particular individual in their databases, to conduct joint analyses for detection of relations and networks and to identify trends and threats between the distributed data sources.

This is achieved through the creation of anonymous filters that can for example be used to determine approximation matches between FIUs without the need for any FIU to share or expose personal data (not even reference data) beyond its own premises. In essence, Ma^{3}tch filters capture the 'characteristics' of the original data.

If the Ma^{3}tch technology is applied to a list of 4 records containing personal details, the result is a filter like "Nm0a". This is not an encryption and it is more than just hashing. It can be defined as 'hashing' the hash. Encrypted text can be decrypted. Hashed text is irreversible, but can potentially be traced back (for example using 'rainbow tables'). 'Hashing' multiple hashed values in a single filter is irreversible and it cannot be traced back to single individuals. Once the filter (e.g., "Nm0a") is created there is no possibility of tracing back the original content of the filter.

By way of example, the Dutch FIU enters the name and other information about a specific subject into the FIU.NET system to start an information exchange with the Belgian FIU (i.e., the Dutch FIU is 'creating a case'). The reason for this exchange with the Belgian FIU is the fact that the data subject under investigation has the Belgian nationality. As soon as the Dutch FIU enters the data in FIU.NET, the Ma^{3}tch technology reveals within a few milliseconds (timeliness) that two other FIUs may (depending on the selected degree of approximation, e.g. 90% accuracy) have information on this subject as well. The possible hits are found in the anonymous filters the other FIUs have shared with the Dutch FIU (e.g., "fkafkjALKJDFa87qoefauya87qoefauyALKJDFa8afkjALKJDF") through the Ma^{3}tch technology in FIU.NET. At this stage, none of the other FIUs even know that the Dutch FIU has information on a specific data subject (improving privacy). The only FIUs that know this fact are the Belgian and two other relevant FIUs, once the Dutch FIU started the regular process for the exchange of information between FIUs (improving privacy and excluding unnecessary requests to other FIUs).

Core Ma^{3}tch principles are autonomy and decentralization. These principles guarantee that only information owners have full control and data governance on the information sources they connect. This allows all parties to include personal data otherwise not possible, which maximises the analysis results. Information is only physically distributed (controlled by the owner) to parties that 'need to know'. The distributed architecture enhances information security, scalability and reliability, as there is no single point of failure.

Foundation for the Ma^{3}tch is the dynamic decentralised information oriented architecture: a privacy by design framework that builds a virtual information cloud between all parties connected to the network. The resulting virtual platform bridges and harmonizes legal, organisational, informational and technological differences between autonomous governed parties by shaping a virtual enterprise and information architecture without infringing upon local governance, privacy, security and confidentiality. The decentralized information oriented architecture consists of 5 layers (also see Figure 1):

1. A data access layer connects any kind of data or service. Parties can connect local information as is to the virtual information cloud (mitigates many implementation barriers).
2. A data virtualization layer virtualises diverging data domains or services into uniform (standardised or generic) virtual data elements (harmonises information).
3. A processing layer virtually integrates information with other parties and provides standardised local data processing and analysis capabilities (harmonises technology).
4. A governance layer guarantees local autonomy and maximises information that parties are able, allowed and willing to contribute (harmonises governance and processes).
5. An exchange layer directly connects parties (direct bilateral connections guarantee that there is no intermediary data storage, and no third party involved imposes or limits capabilities).

Information remains decentralised under (physical and logical) control of each information owner. This guarantees that other parties cannot access to the information, but information can be virtually integrated and analysed (when and where allowed) to identify relevant ‘need to know’ information and knowledge. Information is only physically stored and accessible where and when access to that information is needed and allowed.

The layered architecture enhances flexibility and the ability to quickly adapt to emerging changes throughout the network. Ma^{3}tch uses dynamic distributed agents for its (anonymous) analysis. Agents are programs that are given small and well-defined (analysis) tasks that run in the processing layer. Local agents transform information and personal data into anonymised data structures that can be (selectively) shared. At the destination the agents can then integrate the anonymous filters with local information sources. Ma^{3}tch agents can be used for any kind of shared or distributed integral analysis (operational, strategic, social networks, geo-tagging, etc.) without moving sensitive information beyond the premises of the information owners. Instead of moving information to a service, services are moved to the information.

For example, distributed information on international money flows can be analysed by setting up Ma^{3}tch agents that anonymise local sensitive information by aggregating individual financial records into a money flow filter describing the ‘characteristics’ of the money flows. Next Ma^{3}tch distributes the results to (selected) parties throughout the network. There the anonymous information is integrated with local information to identify similar (suspicious) money flows. This entire (iterative) process can be automated with minimal effort and maximal results as all parties share the same virtual enterprise architecture. This also means the results are harmonized and can be used for an integral view on suspicious money flows, trends and threats. In a similar way knowledge can be automatically extracted, distributed and applied throughout the network (for example using neural networks to identify suspicious activities).

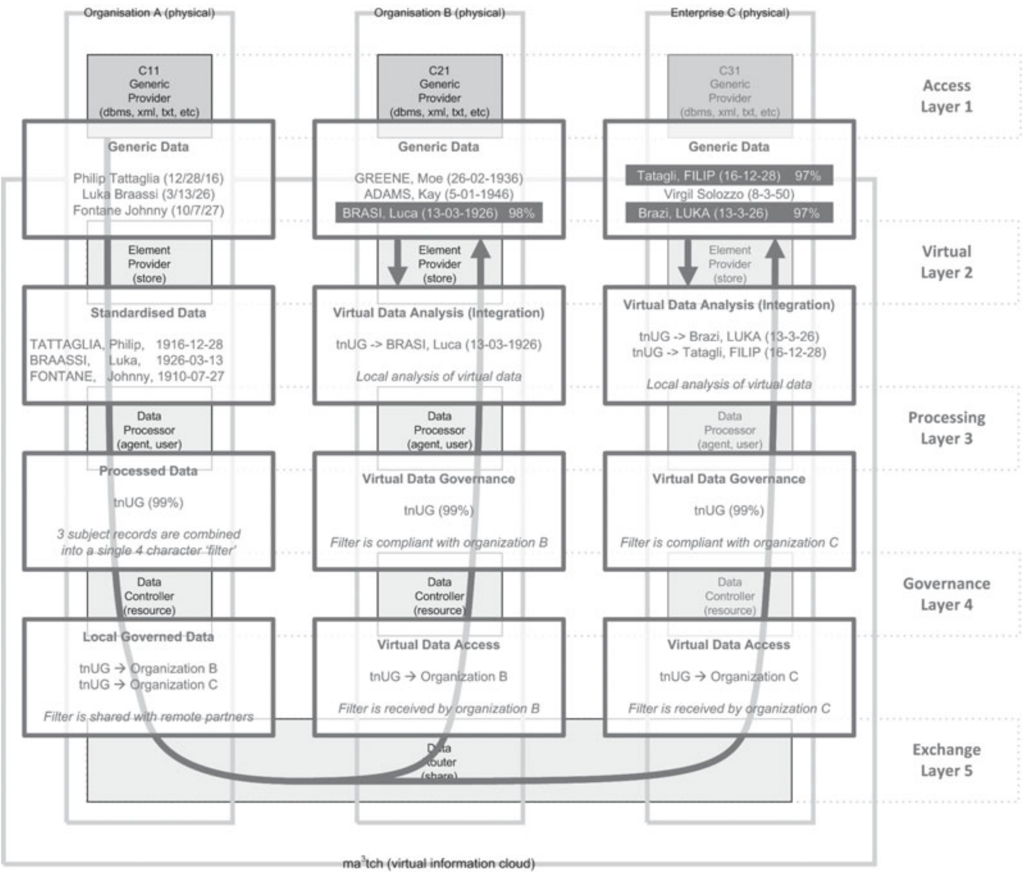

Organisation A (physical)
Organisation B (physical)
Enterprise C (physical)
C11 Generic Provider (dbms, xml, txt, etc)
C21 Generic Provider (dbms, xml, txt, etc)
C31 Generic Provider (dbms, xml, txt, etc)
Access Layer 1
Generic Data
Philip Tattaglia (12/28/16)
Luka Braassi (3/13/26)
Fontane Johnny (10/7/27)
Generic Data
GREENE, Moe (26-02-1936)
ADAMS, Kay (5-01-1946)
BRASI, Luca (13-03-1926) 98%
Generic Data
Tatagli, FILIP (16-12-28) 97%
Virgil Solozzo (8-3-50)
Brazi, LUKA (13-3-26) 97%
Element Provider (store)
Element Provider (store)
Element Provider (store)
Virtual Layer 2
Standardised Data
TATTAGLIA, Philip, 1916-12-28
BRAASSI, Luka, 1926-03-13
FONTANE, Johnny, 1910-07-27
Virtual Data Analysis (Integration)
tnUG -> BRASI, Luca (13-03-1926)
Local analysis of virtual data
Virtual Data Analysis (Integration)
tnUG -> Brazi, LUKA (13-3-26)
tnUG -> Tatagli, FILIP (16-12-28)
Local analysis of virtual data
Data Processor (agent, user)
Data Processor (agent, user)
Data Processor (agent, user)
Processing Layer 3
Processed Data
tnUG (99%)
3 subject records are combined into a single 4 character 'filter'
Virtual Data Governance
tnUG (99%)
Filter is compliant with organization B
Virtual Data Governance
tnUG (99%)
Filter is compliant with organization C
Data Controller (resource)
Data Controller (resource)
Data Controller (resource)
Governance Layer 4
Local Governed Data
tnUG → Organization B
tnUG → Organization C
Filter is shared with remote partners
Virtual Data Access
tnUG → Organization B
Filter is received by organization B
Virtual Data Access
tnUG → Organization C
Filter is received by organization C
Data Router (share)
Exchange Layer 5
ma³tch (virtual information cloud)

Fig. 1: Ma^{3}tch process using dynamic decentralised information oriented architecture

In many cases it is crucial to know in real time when and where to find relevant information. Identification of relevant information between distributed parties in real time uses the same process as before. Depending on the needs (transliteration, approximation, permutations, error correction, fuzzy logic, etc.) a single anonymous filter is constructed that captures the 'characteristics' for all (or a selection of) personal data records. Figure 1 shows an example how 3 personal data records (Organisation A) are transformed into a single anonymised filter (tnUG, 99% precision) that is distributed with the other parties for (fuzzy logic) matching with their own local personal data [Kroo08]. The filter reveals 3 possible hits with 2 other distributed databases. An iterative process is then (manually or automatically) initiated to validate hits and build a dynamic distributed case for real time integration within the (custom) distributed systems and databases of involved parties.

Each information owner controls what data are included in the filter, how long the filter is valid, what the precision of the filter is, with which parties the filter is shared, and after a hit if, when and what personal data are exchanged. The fact that information is only stored when and where access to that information is needed maximises autonomy, subsidiarity and proportionality. Only cases that are identified by the involved FIUs as suspicious are forwarded to law enforcement. A similar process can be set up to 'ma^{3}tch' FIU output to the customers (law enforcement) needs.

With Ma^{3}tch there is no need to exchange bulk information to achieve integral data fusion and analysis between parties, and there is no need to entrust personal data to a third party. Timeliness increases as relevant information is identified in real time, and is pushed or pulled when needed: no unnecessary information needs to be processed, cleaned or reviewed. Quality and reliability are enhanced as information can be processed, interpreted and checked for compliance at the source.

Ma^{3}tch enforces the principle of Privacy by Design and combines local autonomy with harmonization. This opens many other opportunities, for example anonymously Ma^{3}tching information and knowledge with external national or international parties (police, banks, business registers, telecom providers, etc.). Furthermore, parties can jointly acquire anonymous and uniform access to (commercial) service providers (databases, geo-tagging, open source searching, entity extraction, data analysis, etc.).

Ma^{3}tch minimises financial, legal, organisational, technical and informational implementation barriers, and maximises the information and knowledge position of all parties connected to the virtual cloud. As connected parties share a common virtual enterprise architecture (and virtual information architecture), they can jointly develop or acquire new (commercial) information sources and services cost effectively, and seamlessly integrate these with their internal systems and databases supporting privacy, security or confidentiality. It reduces individual costs and further enhances and harmonizes their capabilities. It enables the EU FIUs to act and operate as a single virtual enterprise.

3 Data protection obligations applicable to the FIUs

According to the international legal framework, which is applicable to the exchange of personal data between the EU FIUs, FIUs, as data controllers, have a number of duties and obligations to comply with.

1. *Purpose specification and collection limitation*
   FIUs may collect personal data only for specified, explicit and legitimate purposes in the performance of their tasks and process these data for the same purposes for which data were collected.[1] Accordingly, FIUs are legally required to erase personal data or make anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. FIUs may choose to block personal data instead of erasing them if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure.[2]
2. *Data quality*
   FIUs must process data lawfully and the data they process must be adequate, relevant and not excessive in relation to the purposes for which they are collected.[3] Moreover, data FIUs process must be accurate. They need to rectify if data are inaccurate and, where possible

[1] Art. 6(b) of the Directive 95/46/EC; Article 3(1) of the Council Framework Decision 2008/977/JHA; Art. 5(1) of the Council Decision 2000/642/JHA; Art. 5(b) of the Convention ETS. No.108; Article 46(7) of the Convention CETS No. 198

[2] Art. 4(2) and 4(3) of the Council Framework Decision 2008/977/JHA

[3] Art. 6(a) and (c) of the Directive 95/46/EC; Art.3 (1) of the Council Framework Decision 2008/977/JHA; Art. 5 of the Convention ETS. No. 108

and necessary, to make them complete or update.[4] FIUs must take all reasonable steps to ensure that personal data, which are inaccurate, incomplete or no longer up to date, are not transmitted or made available. To that end, as far as practicable, they need to verify the quality of personal data before they are transmitted or made available.[5] If it emerges that incorrect data have been transmitted or data have been unlawfully transmitted, FIUs must notify the recipient without delay. The data must be rectified, erased, or blocked without delay.[6] In addition, FIUs are required to establish appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of the data.[7]

3. *Openness and individual participation, unless legislative measures restrict these rights*
   A number of legislations require data controllers to inform the data subject regarding the collection or processing of their personal data.[8] However, for FIUs, such duty would be inconsistent with the confidentiality they need to maintain in order not to compromise their efforts to fight against money laundering and terrorism financing. In fact, when personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law, request the other Member State to not to inform the data subject.[9] In practice, national laws allow for derogation to limit or exclude the duty to provide information in certain circumstances.
   Similarly, the law provides no direct right of access[10] to FIUs, but allows for indirect access that may be exercised by the supervisory authority. Data subjects, at reasonable intervals, may obtain from the FIU or from the national supervisory authority a confirmation as to whether data relating to him or her have been transmitted, who the recipients are and how his or her data are processed. Alternatively, data subjects may refer to the supervisory authority with a request to proceed with the verification of information concerning them.[11] Subsequently, the authority notifies the data subject who has made such request that it has carried out verification without providing any further information. The reason for such restrictions of access relate to an aim to ensure the protection of the anonymity of the reporting source and safeguard him or her from attacks or reprisals. In addition, data subjects must be provided with the right to rectification, erasure or blocking of their data. According to the national laws, data subjects may exercise this right directly against the FIU or through the intermediary of the competent national supervisory authority.[12]
4. *Security safeguards and accountability*
   FIUs, just like any data controllers, must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the process-

[4] Art. 6(d) of the Directive 95/46/EC; Art. 4(1) of the Council Framework Decision 2008/977/JHA; Art. 5 of the Convention ETS. No. 108

[5] Art. 6(d) of the Directive 95/46/EC; Art. 8(1) of the Council Framework Decision 2008/977/JHA

[6] Art. 8(2) of the Council Framework Decision 2008/977/JHA

[7] Art. 5 of the Council Framework Decision 2008/977/JHA

[8] Art. 10 of the Directive 95/46/EC; Art. 16(1) of the Council Framework Decision 2008/977/JHA; Art. 8 of the Convention ETS. No. 108

[9] Art. 16(1) of the Council Framework Decision 2008/977/JHA;

[10] Art. 12 of the Directive 95/46/EC, Art. 8 of the Convention ETS. No. 108.

[11] Art. 17 of the Council Framework Decision 2008/977/JHA

[12] Art. 12(b) of the Directive 95/46/EC; Art. 18 of the Council Framework Decision 2008/977/JHA; Art. 8 of the Convention ETS. No. 108

ing and the nature of the data to be protected.[13] In respect of automated data processing, FIUs shall implement measures designed to: guarantee equipment access control, data media control, storage control, user control, data access control, communication control, input control, transport control, recovery, integrity.[14] More precisely, FIUs are required to log or document all transmissions of personal data for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.[15] In addition, they must communicate logs or documentation on request to the competent supervisory authority in charge of data protection.[16]

4 Privacy by Design features in Ma^{3}tch technology

4.1 Data anonymisation

Anonymous data are data that, originally or after being processed, cannot be directly or indirectly connected to an identified or identifiable individual. In contrast, personal data, are data that directly or indirectly identify an individual.[17] As established in the Article 2(a) of Directive 95/46/EC "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[18] In essence, the distinction between personal data and anonymous data depends on the possible connection, i.e. on the possibility to re-associate the data to a specific data subject. For instance, aggregated data about a large group of people are anonymous data. Identification has to be understood in a broad sense. Reference via a unique number is an example. It is not necessary to know the name of a person. Recognition is sufficient. The important issue is that it is possible to single-out an individual in a group based on the available data. As a result, a pseudonym or nickname does not lead to anonymity of the individual. Pseudonyms are indirectly identifying the individual and must be considered as personal data.

Anonymising data are sufficient when the data cannot be reversed to the original identifying data. Data are considered anonymous when an unreasonable effort (amount of time and manpower) is required to (re)turn the data into personally-identifiable data. In other words, the likelihood of making a connection between data and a data subject is measured in relation to the time, cost and technical means necessary to do so [Coun97; Albr12]. The test of identifiability is a dynamic one and should consider the state-of-the-art in technology at the time of the processing. The technical threshold at which sensitive information will be considered identifiable is lower, as it warrants a higher level of protection [KeLS09].

[13] Art. 17 of the Directive 95/46/EC; Art. 22 of the Council Framework Decision 2008/977/JHA; Art. 5(4) of the Council Decision 2000/642/JHA; Art. 7 of the Convention ETS. No. 108; Art. 46(10) of the Convention CETS No. 198)

[14] Art. 22(2) of the Council Framework Decision 2008/977/JHA

[15] Art. 10(1) of the Council Framework Decision 2008/977/JHA

[16] Art. 10(2) of the Council Framework Decision 2008/977/JHA

[17] For a more detailed definition of personal data see Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136.

[18] Even though Directive 95/46/EC is not directly applicable to FIUs, this definition of personal data is the core definition in the European legal framework concerning data processing.

If it can be established that Ma^{3}tch compares completely anonymous profiles and no personal data are processed, many data protection duties and obligations fall away for FIUs. Otherwise, as in case of ordinary personal data exchanges, FIUs are obliged to abide by data protection requirements described in Section 3 above. Recital 26 of the Preamble of the Directive 95/46/EC explicitly states that: "[t]he principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." Moreover, anonymity of personal data provides important benefits for the protection of personal data and can be seen as a way to advance one's right to privacy [KeLS09]. Anonymised data transfers ensure a higher level of privacy and are particularly beneficial when processing sensitive personal data [NiPD03]. Anonymisation helps to enforce the principle of data minimisation. The anonymisation techniques eliminate personal data or identifying data from the processing if the purpose sought in the individual case can be achieved by using anonymous data.

Ma^{3}tch as an autonomous analysis technology is created to match data from various decentralised autonomous resources. The matching is performed in the following steps: 1) FIU converts personal data into a uniform anonymised filter; 2) the anonymisation of personal data is achieved through a combination of anonymisation algorithms, space efficient probabilistic data structures, hashing, fuzzy logic and approximation technologies. As mentioned above, this procedure can be defined as 'hashing' the hash. This is an irreversible process. Furthermore, it does not allow tracing data back to individuals. However, the data processed by the requesting FIU are personal data. Data that are not filtered with the Ma^{3}tch technology are also personal data for both the requesting FIU and the providing FIU. Processing of these data needs of course to be in compliance with the regulatory framework.

4.2 Data minimisation

Through Ma^{3}tch, relevant information is anonymously identified, combined, analysed and applied in real time throughout the entire network. In case of an existing match, i.e. indication of money laundering and terrorism financing, an ordinary exchange of necessary information with related parties is initiated (instead of exchanging everything). This system follows the logic of an existing hit/no hit system, which is used in cross-border cooperation among EU countries' police and judicial authorities to combat terrorism and cross-border crime. The set-up of the hit/no hit system makes it possible to compare anonymous profiles and to exchange additional personal data only after a hit. Recital 18 of the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ([2008] OJ L 210 , 06/08/2008 P. 001-0011.) recognises a hit/no hit system as an adequate system regarding personal data protection: "*The hit/no hit system provides for a structure of comparing anonymous profiles, where additional personal data is exchanged only after a hit, the supply and receipt of which is governed by national law, including the legal assistance rules. This set-up guarantees an adequate system of data protection, it being understood that the supply of personal data to another Member State requires an adequate level of data protection on the part of the receiving Member States*". When using the Ma^{3}tch technology, data are anonymised by so called 'hashing' the hash functionality. In this way the Ma^{3}tch technology enables the comparison of anonymous profiles without directly exchanging personal data (automatically). Ma^{3}tch has thus the main features of a hit/no hit system.

From the personal data protection point of view, Ma^{3}tch seems to even improve the hit/no hit system. In this respect, the hit/no-hit is a procedure whereby the parties grant each other limited access to the reference data in their national databases and the right to use these data to conduct automated checks. The personal information related to the reference data is not available to the requesting party.[19] Practically, "requesting Member States will receive an answer mainly to indicate HIT or NO-HIT along with an identification number in case of a HIT, which does not contain any personal information. The further investigation after the notification of a HIT will be conducted at bilateral level pursuant to the existing national legal and organisational regulations of the respective Member States' sites."[20]

With Ma^{3}tch, there is not even the need to grant limited access to reference data. The reference data is transformed into a single filter that contains the 'characteristics' of the data. Only such filter (not containing privacy sensitive information it is built from) is shared. Other parties then can 'match' against these characteristics. For example, a 'filter' could be created which contains the following 'characteristic' related to the information/data: *"this filter does not contain any last names that start with an A, D or M"*. The filter can then be used by other parties to identify that this database does not have information on 'John Doe', but may have information on 'Alexander Bell'.

To summarise, Ma^{3}tch minimises the need for personal data exchange. Potentially fewer requests for personal data sharing are made using Ma^{3}tch as initial anonymous and standardised exchange of filters guarantees more effective communication.

4.3 Data security

FIUs, just like any data controllers, are legally required to guarantee data security by employing appropriate technical and organisational measures. More precisely, according to Article 46(10) of the Convention No. 198, FIUs must undertake measures, including security measures, to ensure that information transmitted is not accessible by any other authorities, agencies or departments. Security measures must protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmission over a network.[21] This is precisely what Ma^{3}tch does. The data are anonymised through the creation of 'filters' shared with other FIUs. This makes the data unintelligible in case of loss or unauthorised disclosure, since filters cannot be returned into the original data.

Moreover, instead of physically centralising, integrating and unifying information (e.g., all data owners providing all their information to a central authority and then authenticate to provide access to relevant information users), Ma^{3}tch operates based on a decentralised information architecture, i.e., FIU.NET. This enables standardised processing of distributed information to be connected with the information without the need to bring the information physically together. In other words, it enables 'virtual information integration'. Data held by or accessible to FIUs or

[19] Stepping up cross-border cooperation (Prüm Decision) http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm

[20] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. [2008] OJ L 210 of 06/08/2008, p. 28.

[21] Art. 17 of the Directive 95/46/EC; Art. 22 of the Council Framework Decision 2008/977/JHA; Art. 5(4) of the Council Decision 2000/642/JHA; Art. 7 of the Convention ETS. No. 108; Art. 46(10) of the Convention CETS no. 198.

other participating parties are distributed and processed locally. Data owners have continuous control of data storage, sharing, availability, usage, handling, and any other operations as autonomous data controllers. Each of the owners has the ability to enforce its internal rules and security measures and guarantee compliance with applicable legislative requirements. Thus, for example, each FIU guarantees that information under its control is processed according to the national personal data protection requirements and is protected from unauthorised or wrongful use by third parties. It also carry out risk management and audits and retrieve tracking history and rollback regarding the system configurations that process the information.

Therefore, autonomous and controlled information access as well as decentralised information processing strengthen each other to maximise privacy (information remains physically distributed and only locally accessible). Virtually information is unified and it enables 'integrated' processing of the decentralized and autonomously controlled information. The results are compatible and can be exchanged and combined with local information to maximise collective intelligence (knowledge and understanding).

5 Potential drawbacks of Ma^{3}tch technology

Although from the perspective of limiting data processing, securing data against loss or unauthorised access and purpose specification, the Ma^{3}tch technology may provide a valuable solution, there are also a number of points to be taken into consideration in relation to the rights and obligations FIUs have based on the European legislative framework on how to use Ma^{3}tch in a way that assures that a technology, which is designed to protect privacy, will in reality do so.

Ma^{3}tch may provide the functionality of automated data exchange in case of a 'hit' in the system. Such functionality should be disabled or used very carefully, since this may infringe upon the autonomy of the participating FIUs and thus may conflict with the data protection duties and obligations applicable to FIUs.

In using Ma^{3}tch, it is essential to keep filters up-to-date in the FIUs' databases. In other words, FIUs must update 'filters' every time original data are changed in order to meet the requirement of data quality. Moreover, an expiry date can be attached so that the filter is automatically deleted from the system after a specified period. In this way FIUs would comply with the obligation to establish appropriate time limits for the erasure of personal data (Article 5 of the Council Framework Decision 2008/977/JHA). Alternatively, FIUs can perform periodic reviews in order to avoid excessive data retention and fulfil FIUs duties as data controllers to guarantee the data quality.

Finally, filters are unintelligible, but the hit resulting from a match allows the FIU that has created the relevant case to know that other FIUs have matching information concerning the data subject. Even though the exact information is not exchanged, the fact that other FIUs have the data concerning an individual (in case of a match) is information in itself. The one who made a reference to the system receives notification and knows whom it is concerned with, so the knowledge that another FIU has information concerning an individual can be linked to this individual, as the requesting FIU knows the identity of the individual. In this respect, the Ma^{3}tch technology may be in conflict with the purpose specification principle, which obliges FIUs to collect personal data only for specified, explicit and legitimate purpose while carrying out their specific tasks (see Section 3). When cases (references to the system) are generated without a specific ground, the purpose specification principle is violated. There is no specific purpose for the processing since it is processed for the reason of another purpose. As a result, the processing is illegitimate because the FIU operates beyond its relevant tasks and in breach of its legal duties. Such practices may be avoided through internal checking mechanisms (e.g., monitoring, documentation of transmissions) or logging of cases (reference to the system). These log files and/or documentation of transmissions are legally required in the context of security safeguards by Art. 10(1) of the Council Framework Decision 2008/977/JHA.

6 Conclusions and recommendations

This paper has explored the presence of the fundamental elements of the Privacy by Design principle in the Ma^{3}tch technology and its use by FIUs to improve the exchange of information via FIU.NET decentralised computer network. It is possible to conclude that the main data protection requirements have been taken into account when designing this complex system of intelligence sharing, which guarantees data anonymisation, data minimisation and data security.

The Ma^{3}tch technology can therefore be seen as a valuable example of Privacy by Design. It may not only be able to improve the exchange of information among FIUs and allow for the data processing to be in line with applicable data protection requirements, but it may also substantially enhance privacy of related data subjects. At the same time, the case study clearly shows that Privacy by Design needs to be supported and complemented by appropriate organisational and technical procedures to assure that the technology solutions devised to protect privacy would in fact do so.

The Ma^{3}tch technology may be applied not only to financial intelligence, but also on a broader scale, i.e. to any national or international cooperation between governmental and/or commercial organizations. Ma^{3}tch can enhance both privacy, as well as the information position and analysis capabilities. Examples include (combination and analysis of) financial data, passenger data, telecom data, biomedical data, law enforcement data, tax data, and other sensitive but relevant information.

References

[A29WP07] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136.

[Albr12] Albrecht, Jan Philipp (Committee on Civil Liberties, Justice and Home Affairs): Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012)0011 e C7-0025/2012e2012/0011(COD).

[Comm10] European Commission: A Digital Agenda for Europe. 26/8/2010 [2010] OJ COM(2010) 245 final/2;

[Comm12] European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). [2012]OJ COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[Coun00] Council of the European Union: Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. [2000] OJ L 271 , 24/10/2000 P. 0004 – 0006

[Coun97] Council Recommendation (EC) R97/5 of February 13, 1997, on the protection of medical data

[Fede12] Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers. March 2012. available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[KeLS09] Kerr, I., Lucock, C., Steeves V.(Eds.): Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society. Oxford: Oxford University Press, 2009.

[Kroo08] Kroon, U.: Intersect Research Project. 2008. available at http://intersect.crowndesign.nl

[Kroo13] Kroon, U. (forthcoming), Privacy and Knowledge: Dynamic Networked Collective Intelligence

[NiPD03] Nicoll, C.; Prins, J. E. J.; van Dellen, M. J. M. (Eds.): Digital Anonymity and the Law: Tensions and Dimensions, Information Technology and Law Series. T.M.C. Asser Press, 2003.

[Parl05] European Parliament and the Council: Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. 26 October 2005. [2005] OJ L 309, 25.11.2005, p. 15–36.

[Schr09] Schreuders, E.: The Legal Aspects of Cooperation between FIUs using FIU.NET. 2009.

A security Taxonomy that facilitates Protecting an industrial ICT Production and how it really provides Transparency

Eberhard von Faber [1(+2)] · Wolfgang Behnsen [1]

[1] T-Systems
{Eberhard.Faber | Wolfgang.Behnsen}@t-systems.com

[2] Brandenburg University of Applied Science
Eberhard.vonFaber@fh-brandenburg.de

Abstract

The *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* is a reference architecture for protecting ICT services [EvFWB12]. User organizations are enabled to compare offerings and assess risks. ICT service providers receive a comprehensive template for implementing and maintaining all security measures, including those relating to service management. The architecture also introduces a *Security Taxonomy* on Level 4 of its hierarchy of security standards. This taxonomy is explained in this paper. The structure or organization model assigns security measures to production areas. It considers state-of-the-art service management processes (ITIL) and integrates ICT security management and IT service management. The taxonomy supports division of labor and assignment of responsibility within a large-scale ICT production. The taxonomy is compatible with all types of ICT services and service models since it allows easy identification and selection of the relevant security documentation. The taxonomy is modular and derived from specific criteria. The latter result from challenges in day-to-day business and consider interests and requirements both from user organizations and from ICT service providers.

1 Motivation

Existing security standards such as [ISO27002] (Annex A of [ISO27001])

- do not match with ICT production processes[1]
  (Note: ITIL is the commonly used approach of structuring an ICT production),
- are not sufficiently modular
  (Note: Large-scale ICT production is characterised by a high degree of division of labor),
- do not provide a flexible interface between consuming entity (user organization) and producing entity (ICT service provider)
  (Note: Cloud computing models are exceptions, but there are many other deployment models that need to be supported).

Moreover, not only the standards just mentioned identify and consider several security areas but do not provide a structure that explains their relation and interdependencies.

[1] ICT: Information and Communication Technology

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_8, © Springer Fachmedien Wiesbaden 2013

Therefore, the *ESARIS Security Taxonomy* is being introduced. This taxonomy is one element of the *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* which was the subject of the authors' previous contribution in this series (see [EvFWB12]). ESARIS looks at ICT security from the perspective of an ICT service provider. ICT service providers require uniform models and standards according to which they protect ICT services which they produce for their customers. We take customers to mean solely large user enterprises since only these businesses conduct differentiated risk management with ICT procurement. The models and standards of ESARIS were also developed for large-scale ICT production, which is characterized by consistent division of work and process orientation. Simple ICT infrastructures and services can be controlled according to other existing processes.

The need for a new industrial approach is tied up with the following four distinctive features (refer to Fig. 1).

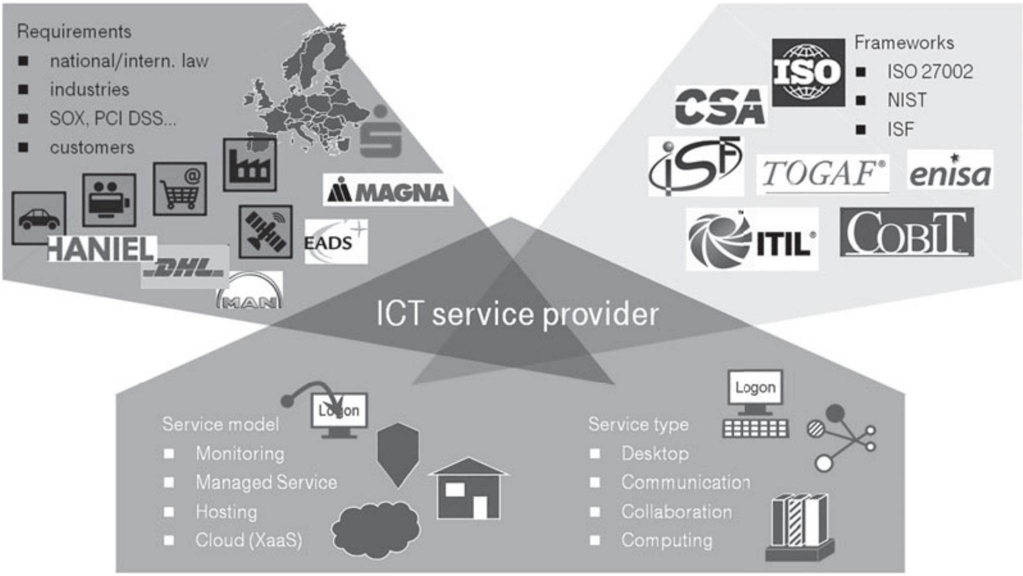


Fig. 1: ICT service providers must consider the whole market

A) Service types: A wealth of different ICT services exist (in the areas of Desktop, Networks and Computing). Each requires its own types of specific security measures. If the provider offers a host of ICT services, modules need to be defined that can be combined on a service-dependent basis. This modularity and granularity has hitherto not been available, e.g. with ISO/IEC 27002.

B) Service models: ICT services are, for instance, produced with dedicated systems or in the cloud. Yet in practice the division of labor between user organizations and the ICT service provider turns out to be much more differentiated. In addition to the basic models, service levels and other agreements determine how the user organization's and the provider's service processes build on each other. This diversity cannot be mapped using General Terms and Conditions (GTC). The security measures must therefore be defined so that they support all possible service models. That means, for instance, that lifecycle-dependent services must be separated from the provisioning of the primary function. Other approaches such as the IT-Grundschutz [BSI-GS] combine these areas as an inseparable component with good reason since they are focused, as well as the aforementioned ISO standard, on a single organization with mainly in-house ICT production. By contrast, we need to look at a flexible division of labor, which is more complex than simply integrating a supplier's elements as a fixed component.

C) Requirements: The necessary new ordering schemas must, however, not just fit with the products and their production methods. An ICT service provider is placed in a basically different situation than any organization covering its own needs only. The ICT service provider serves a large number of customers and is therefore confronted with a host of different requirements, since their customers come from various industries, pursue different business models and are subject to different laws, ordinances and regulations. The provider must (demonstrably) meet all requirements. Therefore, the provider must use a schema which can be matched to disparate requirements profiles.

D) Basic structure: Requirements and measures cannot be matched by comparing unstructured lists or catalogues of security measures. The operational security and risk management of an organization that is largely dependent on ICT services requires greater quality. Measures can only be understood in their context. The existence, for instance, of a firewall initially means nothing in terms of actually achieved security. All security measures that are contained in best practices, standards and other literature must be interpreted, adapted and accordingly implemented in order to take into account the context in which they are used. They must be supplemented where necessary with references and dependencies as well as with details that reflect their specific contribution to the security of the ICT service. The service provider must document this context information in order to demonstrate trustworthiness (cogently).

2 Condition

The *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* comprises a hierarchy of security standards [EvFWB12]. This ensures top management commitment as well as step-wise refinement of requirements and integration of security controls. ESARIS introduces five levels of security standards.

The Security Taxonomy described in this paper provides a structure for Level 4 and below.

The security standards in Level 4 (called *ICT Security Standards*) are used both for communicating with customers and for controlling service and production of ICT services. This fundamental decision is called the *ESARIS Concept of Double Direction Standards* [EvFWB12]. Only if the identical specification is used it can be ensured that the ICT services actually meet the security requirements of the customers and that promises to customers can actually be fulfilled.

These facts were subject of the authors' previous contribution in this series (see [EvFWB12]).

3 Criteria

As a result, a new security taxonomy is introduced. This ordering schema must provide room for the description of all security measures that are required to protect ICT services. The *ESARIS Security Taxonomy* is built to manage the complexity of protecting an industrial ICT service production. The taxonomy helps to find the required information; whereas a monolithic documentation would not allow appropriate use of its contents.

It is essential to decide on a structure of areas (logic) and decide which security topics, themes or aspects are to be described in each area. The areas will be described in different *ICT Security Standards* so that the taxonomy is also the taxonomy of *ICT Security Standards*. Each *ICT Security Standard* comprises several security measures.

Criteria are developed to build the required taxonomy. Guiding questions from a fictive auditor or customer were used as a starting point. These questions ensure that the result is practical and useful instead of solely academic or l'art pour l'art. The questions were grouped into five criteria.

The first criterion is entitled "relevance and dissemination". This criterion mainly relates to customer interests. The security measures in each area shall address a concrete security issue which is actually being raised. It responds to a question or concern that is of interest. The context, purpose and effect become clear from studying the security measure. Each area (and *ICT Security Standard*) shall respond to customers' questions and concerns and provide clear and understandable answers.

The second criterion is entitled "granularity of description, number of areas". This criterion mainly addresses the needs of the provider. The security measures in each area shall be formulated in order to provide as much freedom as possible for implementation. It is largely implementation-independent in order to allow industrialized production and continued technical progress. The documentation may not need to be changed if, e.g. new versions of software or new product components emerge.

The third criterion is entitled "responsibility and responsiveness". It asks for an approach that enables the identification of teams or people who are responsible for the security measures being described. Furthermore, the structure of the standards will allow the extraction of information relevant for a specific ICT service. This means that the security measures will be attached to ICT service elements or to platforms or general supporting services used for many ICT service elements. From this criterion, it is also concluded that references and dependencies between individual standards will be minimized as far as possible. Therefore, each standard will stand alone as far as possible and have its own significance independent from others.

The fourth criterion is entitled "integration into portfolio and business". The security measures must not be incoherent, isolated features that may or may not be added. Instead, security will be integrated into the provider's standard business and offering portfolio. This means that the security taxonomy shall allow assigning security measures to ICT services or, more precisely, to the functional elements an ICT service consists of.

The fifth criterion is entitled "commitment and completeness". The documentation of the security measures will facilitate the provisioning of evidence of coverage and completeness. The *ICT Security Standards* cover all relevant aspects across all technical disciplines and throughout the entire life-cycle. The level of detail chosen (confer criterion two) is just high enough to allow provisioning of the evidence to customers.

To summarize, the structure must meet the following requirements or criteria: it

- addresses a single security issue and provides clear, understandable answers,

- provides clear guidance on the implementation and usage of the security measure so that
  - the guidance is specific enough to prevent errors and misunderstandings,
  - but is flexible enough to provide scope for technical progress and improvements,
- supports the service provider's division of work and its in-house organization to ensure smooth implementation and maintenance of measures,
- is compatible (as noted above) with all ICT services and service models, which the service provider offers,
- covers all relevant areas, which influence the security of the ICT services and therefore offers a complete set of measures.

A taxonomy for organizing or structuring the security measures was developed on the basis of the above criteria. The second criterion relates more to the level of detail, but also affects how the classification schema must be structured.

4 Result

The new security taxonomy includes 31 areas, each of which has been assigned its own name and separate icon. Each area is described by a separate *ICT Security Standard*. The structure of each standard is also again uniform and standardized on an end-to-end basis. There is a uniform format even for the description of the security measures. This end-to-end structuring and modularity is the key to optimum usability, clarity and minimal time/effort in terms of maintenance in particular.

The taxonomy comprises two parts. Part 1 of the structure comprises all areas that are associated with ICT services and their functionality. Part 2 of the structure comprises all areas associated with general services common to several or all ICT services.

Part 2 of the taxonomy (see Fig. 2) contains all cross-functional aspects which apply to several or all ICT services and/or technology areas. The reasons are:

- Production processes and life-cycle practices should be unique in all areas in industrial ICT production. ITIL is an overall standard that is implemented independent from the individual ICT services being offered to customers.
- Security strategy, risk management, and co-operation with customers are elements of the provider's general approach and also common to all ICT services that are offered to customers. The same holds for provisioning of security evidence (with security reporting) as well as for incident handling.

Details are provided below.

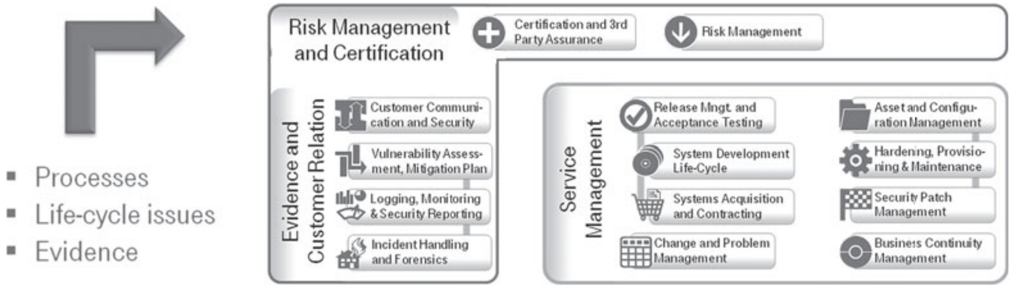
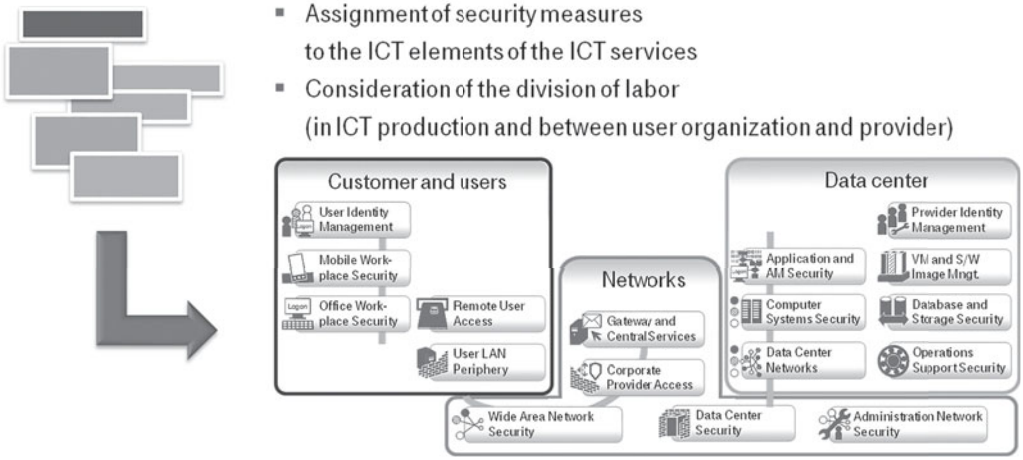

Processes
Life-cycle issues
Evidence
Risk Management and Certification
Certification and 3rd Party Assurance
Risk Management
Evidence and Customer Relation
Customer Communication and Security
Vulnerability Assessment, Mitigation Plan
Logging, Monitoring & Security Reporting
Incident Handling and Forensics
Service Management
Release Mngt. and Acceptance Testing
System Development Life-Cycle
Systems Acquisition and Contracting
Change and Problem Management
Asset and Configuration Management
Hardening, Provisioning & Maintenance
Security Patch Management
Business Continuity Management

Fig. 2: Taxonomy part 2 – areas associated with services common to all ICT services

Part 1 of the taxonomy (see Fig. 3) addresses all security measures that are associated to the ICT services and their functionality. The structure must ensure the following:

- Modules need to be defined that can be combined on a service-dependent basis. It must be possible to easily select the modules or areas that are relevant for a given ICT service and a specific ICT service model. This means that the structure must be compatible with all ICT services and service models, which the service provider offers.
- The structure must also match with the internal organization and division of labor in its large-scale ICT production. This allows departments and teams of the provider to easily select the modules or areas that are relevant for them. The separation into different areas and individual *ICT Security Standards* is required in order to ensure that responsibility and responsiveness is guaranteed. If monolithic documents are used instead, the required 1:1 assignment between topics and teams would not exist in practice. The result: white spots or overlapping responsibility in large sections, both having the same negative effect.



- Assignment of security measures to the ICT elements of the ICT services
- Consideration of the division of labor (in ICT production and between user organization and provider)

Customer and users
User Identity Management
Mobile Workplace Security
Office Workplace Security
Remote User Access
User LAN Periphery
Networks
Gateway and Central Services
Corporate Provider Access
Data center
Provider Identity Management
Application and AM Security
VM and S/W Image Mngt.
Computer Systems Security
Database and Storage Security
Data Center Networks
Operations Support Security
Wide Area Network Security
Data Center Security
Administration Network Security

Fig. 3: Taxonomy part 1 – areas associated with ICT services and functionality

Part 1 and its standards are directly linked with ICT services and the associated technical functionality. It follows the basic structure with the data center on the right-hand side, the customer and users with their workplaces on the left-hand side and the connecting wide area networks in the middle. This division into a) workplaces and user side, b) network and communications services as well as c) ICT services from the data center corresponds to the structure of the portfolio of large ICT service providers, and thus enables the relevant modules for the offered service to be selected. Precisely for this reason, each of the three clusters (a through c) will be further divided up. At the same time, this has the advantage that individual pieces of work and technology areas are analyzed separately. This reduces the complexity and supports the method of production with a substantial division-of-work element in the case of a large service provider.

Fig. 4 shows the full *ESARIS Security Taxonomy* (Part 1 and 2).

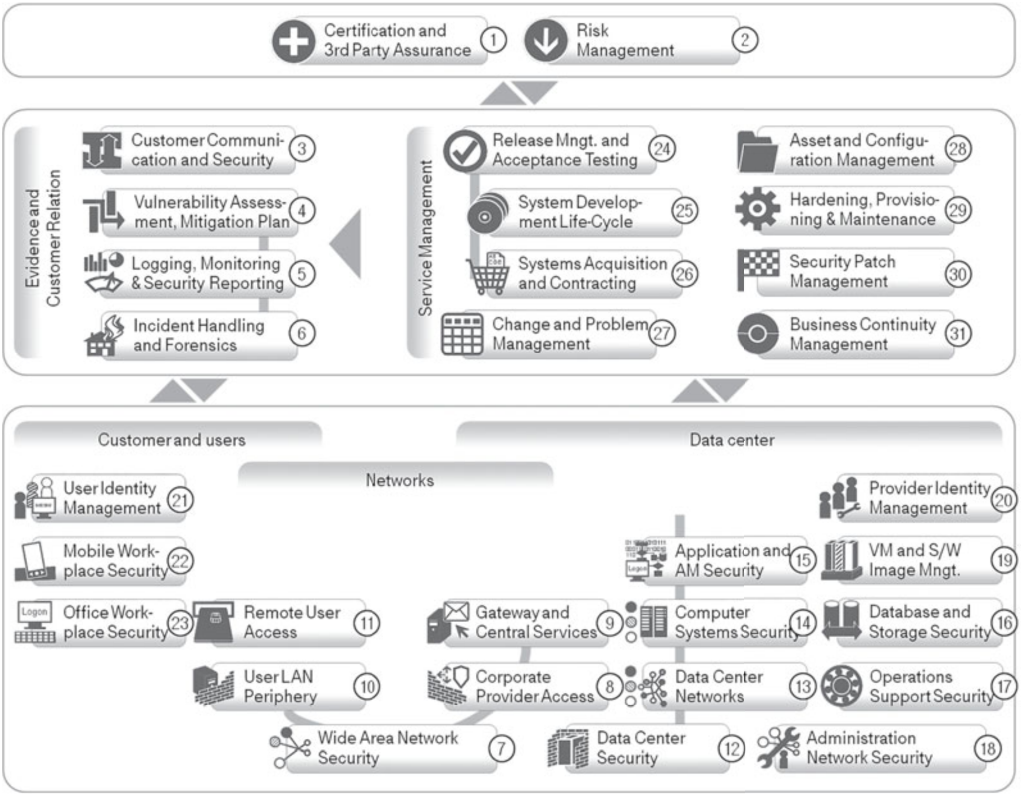

Certification and 3rd Party Assurance 1
Risk Management 2
Evidence and Customer Relation
Customer Communication and Security 3
Vulnerability Assessment, Mitigation Plan 4
Logging, Monitoring & Security Reporting 5
Incident Handling and Forensics 6
Service Management
Release Mngt. and Acceptance Testing 24
System Development Life-Cycle 25
Systems Acquisition and Contracting 26
Change and Problem Management 27
Asset and Configuration Management 28
Hardening, Provisioning & Maintenance 29
Security Patch Management 30
Business Continuity Management 31
Customer and users
Data center
Networks
User Identity Management 21
Mobile Workplace Security 22
Office Workplace Security 23
Logon
Remote User Access 11
User LAN Periphery 10
Wide Area Network Security 7
Gateway and Central Services 9
Corporate Provider Access 8
Application and AM Security 15
Computer Systems Security 14
Data Center Networks 13
Data Center Security 12
Provider Identity Management 20
VM and S/W Image Mngt. 19
Database and Storage Security 16
Operations Support Security 17
Administration Network Security 18

Fig. 4: *ESARIS Security Taxonomy* (Level 4 in the security standards hierarchy)

We will look at the cluster *data center* in slightly more detail. Initially the primary ICT stack is depicted here comprising: (13) the internal data center networks, (14) the computer systems with operating systems and possible virtualization layers as well as (15) the applications with other components such as special middleware. – These are supplemented by other elements in a secondary ICT stack: (16) Database management systems (DBMS) and centralized storage are assigned to this stack. (17) Operations support systems are also centralized. If virtualization is used in a multi-tenant platform ("cloud"), the (19) management of software images and virtual machines is added.

The other areas form the periphery of the stack. The first describes (12) the aspect of data-center security (physical protection). Users gain logical access via a wide area network. The protection on the outer edge of the data center consists of (8) standard elements such as firewalls and gateways as well as (9) other centralized elements such as authentication services or application-related proxies and filter solutions. The ICT service provider's operating personnel (administrators) use (18) a different access with a separate infrastructure. The administrators require (20) digital identities and authorizations for access; this includes registration, allocation and administration, etc.

As already mentioned, users receive access to the IT services via wide area networks whose security aspects are described in (7). The protection of the transport path must not be seen independently of the endpoints, but covers more than just these. User organizations utilize (10) a separate gateway infrastructure to connect to a wide area network such as the Internet. Individual users connect via (11) a remote user access. In both cases the actual ICT service is used on a terminal device dubbed "workplace". Here a distinction is drawn between (23) workplaces, which are used at a fixed point in the office and are connected with the in-house LAN, and those (22) which are also used wirelessly, in other words also support connections with other (especially) public networks. In order to protect access to the workplaces and the other ICT services used with this access, (21) digital identities and authorizations are necessary, which includes the associated administration and the related issues.

This taxonomy has decisive advantages. It optimally supports the ICT production and actually provides transparency for the user organizations. At least three different networks are identifiable, which are operated by the ICT service provider for very different purposes and consequently must satisfy very different requirements. ISO/IEC 27002 and Annex A of ISO/IEC 27001 naturally also address network security, but do not distinguish any usage scenarios and hence only include one uniform set of requirements. The same also applies to other areas since the outsourcing and service models are not mapped.

Part 2 in the security taxonomy (upper half of Fig. 4) contains all cross-functional aspects which apply to several or all ICT services and/or technology areas. Here the aspects relating to service management according to ITIL should be mentioned first in this respect. General questions regarding security throughout the lifecycle are described in four areas: They address (27) changes to ICT components and systems as well as (24) setting up entire systems and basic changes to existing systems (releases). In this respect, (25) security is analyzed during development as well as (26) the security of the bought-in components and services. The more technical part of service management also includes four areas: These range from (28) asset and configuration management, (29) hardening, provisioning and maintenance as well as (30) the ongoing updating of systems by importing patches to (31) business continuity management.

Aspects of safety and incident management in the narrow sense are also only mapped once since these tasks are relevant across-the-board and cross-functionally for every combination of individual ICT services. The individual areas are (3) security at the customer interface, (4) vulnerability management, (5) logging, monitoring and security reporting as well as (6) incident handling together with forensics. – Finally, as cross-functional aspects, (2) risk management and (1) questions of certification, handling audits and other documentary evidence are addressed.

5 Realization

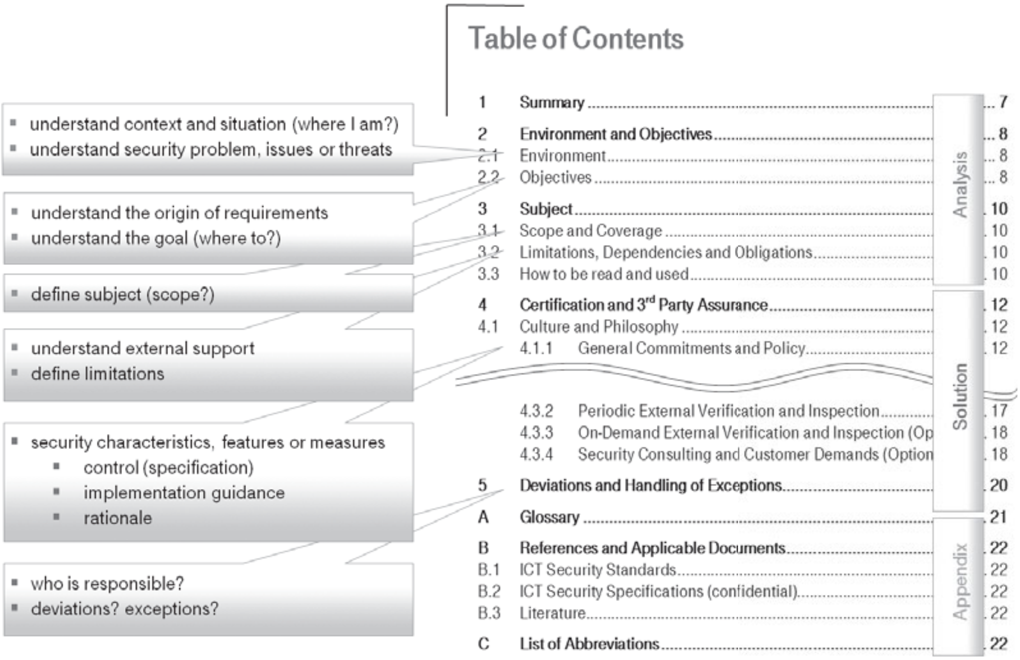
The *ICT Security Standards* describe security measures that are in place to protect the ICT services delivered by the ICT service provider. All standards are structured in exactly the same way. They provide a definition of a security target and specify the solution in terms of security measures. This structure and the obligation to use it throughout Level 4 have several advantages. The specification concept

- helps to ensure that all standards contain the required information, and
- facilitates the handling of the standards; in particular, required information can be found more easily.

The structure of the *ICT Security Standards* is shown in Fig. 5. Each *ICT Security Standard* is organized as follows:

- security problem definition,
- security objective identification,
- scope and coverage clarification,
- identification of external support (dependencies with other standards),
- definition of security measures with implementation guidance and rationale,
- responsibilities and possible deviations.

Chapter 4 in each *ICT Security Standard* provides the description of about 15-20 security measures. The security measures are also described in a standardized fashion. Note that chapters 2 and 3 are very important and significant for the understanding and application of the security measures. These chapters also maintain the structure and philosophy or the *ESARIS Security Taxonomy*.



- understand context and situation (where I am?)
- understand security problem, issues or threats

- understand the origin of requirements
- understand the goal (where to?)

- define subject (scope?)

- understand external support
- define limitations

- security characteristics, features or measures
  - control (specification)
  - implementation guidance
  - rationale

- who is responsible?
- deviations? exceptions?

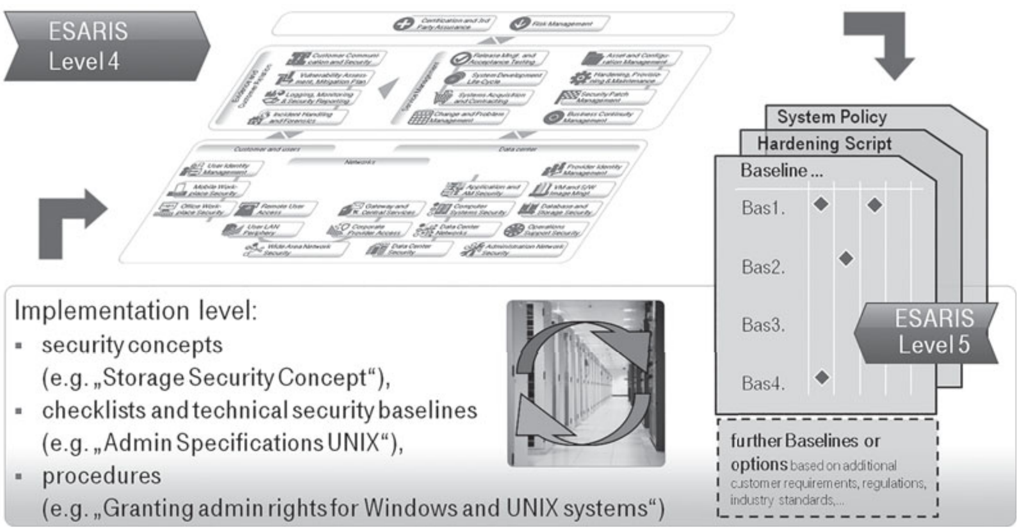
Table of Contents

1 Summary ... 7
2 Environment and Objectives ... 8
2.1 Environment ... 8
2.2 Objectives ... 8
3 Subject ... 10
3.1 Scope and Coverage ... 10
3.2 Limitations, Dependencies and Obligations ... 10
3.3 How to be read and used ... 10
4 Certification and 3rd Party Assurance ... 12
4.1 Culture and Philosophy ... 12
4.1.1 General Commitments and Policy ... 12
4.3.2 Periodic External Verification and Inspection ... 17
4.3.3 On-Demand External Verification and Inspection (Op ... 18
4.3.4 Security Consulting and Customer Demands (Option ... 18
5 Deviations and Handling of Exceptions ... 20
A Glossary ... 21
B References and Applicable Documents ... 22
B.1 ICT Security Standards ... 22
B.2 ICT Security Specifications (confidential) ... 22
B.3 Literature ... 22
C List of Abbreviations ... 22

Fig. 5: Component of the *ESARIS Security Specification Concept*

The *ICT Security Standards* and their security measures are further refined in Level 5 of the *Hierarchy of Security Standards*. The documents on Level 5 are called *ICT Security Baselines* (refer to Fig. 6). There are different types including

- policy papers,
- security concepts,
- tutorials,
- guidance documents,
- work instructions and
- checklists.


ESARIS
Level 4
Certification and 3rd Party Assurance
Risk Management
Customer Communication and Security
Vulnerability Assessment, Mitigation Plan
Logging, Monitoring & Security Reporting
Incident Handling and Forensics
Release Mngt. and Acceptance Testing
System Development Life-Cycle
Systems Acquisition and Contracting
Change and Problem Management
Asset and Configuration Management
Hardening, Provisioning & Maintenance
Security Patch Management
Business Continuity Management
Service Management
Customer and users
Networks
Data center
User Identity Management
Mobile Workplace Security
Office Workplace Security
Remote User Access
User LAN Periphery
Wide Area Network Security
Gateway and Central Services
Corporate Provider Access
Data Center Security
Provider Identity Management
Application and AM Security
VM and S/W Image Mngt
Computer Systems Security
Database and Storage Security
Data Center Networks
Operations Support Security
Administration Network Security
System Policy
Hardening Script
Baseline ...
Bas1.
Bas2.
Bas3.
Bas4.
ESARIS
Level 5

Implementation level:

- security concepts (e.g. „Storage Security Concept“),
- checklists and technical security baselines (e.g. „Admin Specifications UNIX“),
- procedures (e.g. „Granting admin rights for Windows and UNIX systems“)

further Baselines or options based on additional customer requirements, regulations, industry standards,...

Fig. 6: Refinement in Level 5 with *ICT Security Baselines*

Two examples are considered from Part 2 of the *ESARIS Security Taxonomy* (upper half). The *ESARIS Security Taxonomy* comprises the area Change and Problem Management (No. 27 in Fig. 4). In an industrial ICT production all changes that are applied to ICT elements must be conducted in line with the Change Management process (ITIL). The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality and consequently to improve the day-to-day operations of the organization. This requires a clear definition of the process and its activities and the inclusion of security as well.

The corresponding *ICT Security Standard* (Level 4) stipulates security measures for this process. Roles and responsibilities are not primarily designed to consider information security, but must be chosen and enabled to deal with this subject. The Change Management requires the support of workflow tools. Changes require formal request and approval before being implemented. Here, the extent of the change and its impact need to be estimated and documented. A risk assessment is mandatory within the Change Management process in order to minimize negative impacts. The corresponding *ICT Security Baselines* (Level 5) include a process tutorial, guidance documents for e.g. the roles change coordinator, change approver and change manager, a work instruction for the risk assessment as well as a checklist including the change risk calculator.

Security incidents are one major source of change requests. Security incidents are managed in the Incident Management process being described in the area Incident Handling and Forensics (No. 6 in Fig. 4). Incident handling is of complex nature and is also performed in a common process (ITIL) with defined roles and responsibilities. The corresponding *ICT Security Standard* stipulates e.g. the identification of sources and the provisioning of an “inbox” (usually as a User Help Desk service), the pre-qualification of incidents, the security rating, further assessment as well as prioritization and closing. The corresponding *ICT Security Baselines* (Level 5) include a guidance document and a checklist e.g. for the Manager-on-Duty (MoD service), the User Help Desk (UHD) and for the ticket agent and the incident solver. Other *ICT Security Baselines* (Level 5) are a work instruction for the security rating and a checklist with a tool for calculating the urgency based upon e.g. the security rating.

These examples show ESARIS' hierarchical nature, its structural approach and the complete coverage of all security aspects that affect the security of ICT service provisioning. Security measures are refined to a level that actually directs activities in modern ICT production.

6 Summary

Main characteristics of the *ESARIS Security Taxonomy* are shown in Fig. 7 (SDM means Service Delivery Management; CS stands for Computing Services, TS for Telecommunication Services and DS for Desktop Services).

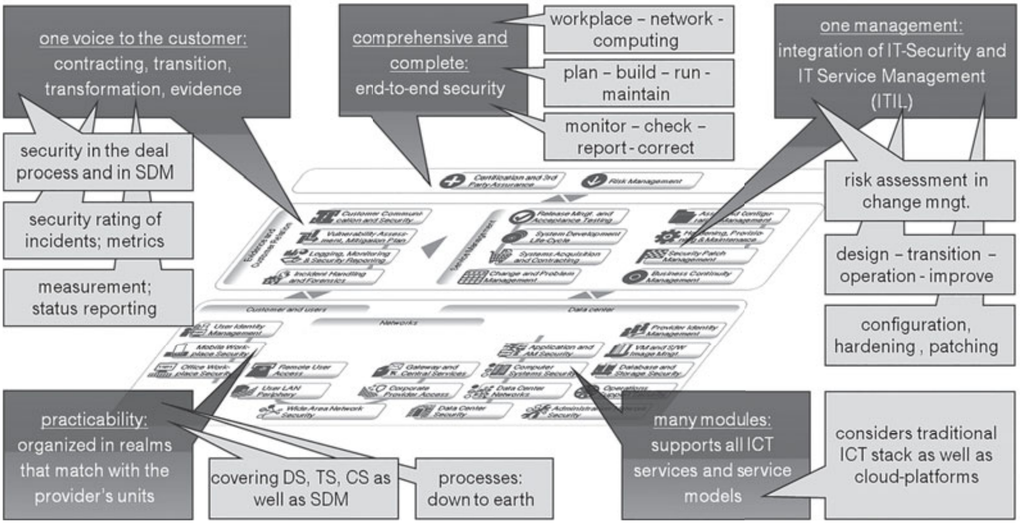

one voice to the customer:
contracting, transition, transformation, evidence
comprehensive and complete:
end-to-end security
workplace – network - computing
plan – build – run - maintain
monitor – check – report - correct
one management:
integration of IT-Security and IT Service Management (ITIL)
security in the deal process and in SDM
security rating of incidents; metrics
measurement; status reporting
risk assessment in change mngt.
design – transition – operation - improve
configuration, hardening , patching
Certification and 3rd Party Assurance
Risk Management
Customer Communication and Security
Vulnerability Assessment, Mitigation Plan
Logging, Monitoring & Security Reporting
Incident Handling and Forensics
Release Mngt. and Acceptance Testing
System Development Life Cycle
Systems Acquisition and Contracting
Change and Problem Management
Hardening, Provisioning & Maintenance
Security Patch Management
Business Continuity Management
Service Management
Customer and users
Networks
Data center
User Identity Management
Mobile Workplace Security
Office Workplace Security
Remote User Access
User LAN Periphery
Wide Area Network Security
Gateway and Central Services
Corporate Provider Access
Data Center Security
Application and AM Security
Computer Systems Security
Data Center Networks
Provider Identity Management
VM and S/W Image Mngt.
Database and Storage Security
Operations Support
Administration Security
practicability:
organized in realms that match with the provider's units
covering DS, TS, CS as well as SDM
processes: down to earth
many modules:
supports all ICT services and service models
considers traditional ICT stack as well as cloud-platforms

Fig. 7: Important characteristics of the *ESARIS Security Taxonomy*

The division into individual areas supports effective implementation in ICT production. It is however also necessary because the division of work between ICT service provider and user organization may be totally different. Not all solutions are managed completely by the ICT service provider. Frequently, the user organization takes over part of the tasks or several service providers divide these up between them. The security taxonomy must support all service models and have a suitable modular structure: If the ICT service provider bears responsibility for a piece of work, the security measures defined in the corresponding area are relevant for the user. Depending on the service type, service model and the details of the agreed division of labor, the areas and measures can be selected and set out in the contract. The user organization gains the necessary transparency. And the ICT service provider knows which security measures it must provide in order to meet its customers' requirements. The precise methods for this kind of matching as well as many other basic concepts and methods are described in a recently published book [EvFWB13]. It also includes many very specific details to protect an industrialized ICT production environment.

The *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* provides a comprehensive, end-to-end hierarchical and modular solution. It was developed by T-Systems in order to control and structure the security of a complex production landscape.

References

[ISO27001] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements

[ISO27002] ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management

[BSI-GS] IT-Grundschutz Catalogues; German Federal Office for Information Security (BSI); www.bsi.bund.de

[EvFWB13] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond, A Workable Architectural Approach to Equilibrate Buyers and Providers; Springer Vieweg, 2013, ISBN-978-3-658-00068-4

[EvFWB12] Eberhard von Faber and Wolfgang Behnsen: A Systematic Holistic Approach for Providers to Deliver Secure ICT Services; in: H. Reimer, N. Pohlmann, W. Schneider (Editors): ISSE 2012 – Securing Electronic Business Processes, Springer Vieweg (2012), ISBN: 978-3-658-00332-6, p. 80 – 88

A Practical Signature Policy Framework

Jon Ølnes

Unibridge AS, Rosenholmveien 25
N-1414 Trollåsen, Norway
jon.olnes@unibridge.no

Abstract

An electronic signature is always used in a context. In the EU, a lot of emphasis has been placed on legal admissibility of at least qualified signatures, and on standards for technical interoperability of esignatures. The main obstacles to use of esignatures today are probably a lack of mutual understanding of how to use them in a given process (organisational interoperability) and missing specifications on the semantic interpretation (the meaning and implications) of esignatures in the process. A signature policy is a means to specify the conditions for use of esignatures. This paper suggests a framework for specification of practically useful signature policies to simplify interoperability, emphasising that the formation of a single signature policy document for all conditions may not be the best option.

1 Introduction

An electronic signature (advanced/qualified signature according to the EU eSignature Directive [EU99] are considered) is always used in a context, e.g. as part of a business process. In practice, the receiver of a signed document must perform two operations:

1. Check that the signature is valid (cryptographically correct and certificates valid);
2. Check that a valid signature can be accepted for the task at hand.

The concept of signature policy has been introduced as a means to specify and capture (preserve) the context. [ETSI-102-041] defines a signature policy as a “set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid”. As seen, this definition does not separate between valid and accepted. While there has not been much use of signature policies, there is now renewed focus in light of the proposal for a new EU regulation in the areas of eID, esignature and trust services [COMM12].

This paper describes the signature policy framework developed by the PEPPOL project (Pan-European Public Procurement On-Line) [PEPPOL-D1.3]. The framework is a list of possible elements for signature policies, with clear semantics and alternative values specified for each element. Policies can then be formed by selecting necessary elements and allowed values.

PEPPOL’s framework specifies elements of four independent signature policy parts:

1. Signatures in business processes – when and how to sign in a (business) process;
2. Commitment rules and authorisations – as required and/or implied by signatures;
3. Signing policy – the rules to be followed by the signer;
4. Signature verification policy – the rules to be followed by the verifier (the relying party).

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_9, © Springer Fachmedien Wiesbaden 2013

The parts can be related to the European Interoperability Framework [EIF10] in that the first part addresses legal and organisational interoperability, the second addresses semantic interoperability, while the two last ones are about technical interoperability. While there has been considerable focus in the EU on ensuring legal admissibility of at least qualified signatures, and on standards for technical interoperability of esignatures, considerably less work has been done on the equally important semantic and organisational interoperability levels.

PEPPOL's main recommendations for signature policies are:

- Separation of signature verification and signature acceptance: Determining validity of a signature is the first step, concerning technical interoperability only. Deciding whether or not a valid signature can be accepted is a separate process involving all four interoperability layers of the European Interoperability Framework.
- Do not insist on a comprehensive signature policy document: The important issue is to make conditions clear, not that this is done in one specific, formal way.
- Make conditions easy to specify and easy to understand: A signature policy shall make life easier to the actors involved, not more complicated.
- Do not over-specify: While a signature policy framework must be comprehensive, real policies should select and specify rules only for the necessary elements. Do not pose strict rules and limitations unless it is necessary; flexibility is a good rule.

In this paper, we first describe esignature interoperability in the context of the European Interoperability Framework followed by background on signature policies and PEPPOL's need for such policies. Then, PEPPOL's pragmatic approach at the policy development process is presented. Finally, the four parts of the signature policy framework are briefly discussed and conclusions and suggestions for further work sums up the paper.

2 The EIF and eSignatures

The challenges in esignature interoperability can be described by reference to the four interoperability levels defined by the European Interoperability Framework (EIF) [EIF10], quoting:

- Legal interoperability: Aligned legislation so that exchanged data is accorded proper legal weight,
- Organisational interoperability: Co-ordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal,
- Semantic interoperability: Precise meaning of exchanged information which is preserved and understood by all parties,
- Technical interoperability: Planning of technical issues involved in linking computer systems and services.

The bulk of work in esignature interoperability in the EU has focussed on the legal and technical levels. The EU esignature directive [EU99] has established the principle of legal admissibility of at least qualified signatures, to be enhanced by the proposed new regulation [COMM12] when approved. Standards have been developed by CEN and ETSI. The standards are currently being revised [ETSI-001-604].

In comparison, organisational and semantic interoperability of esignature use has received little attention; how to use esignatures in (business) processes and what semantic meaning to assign to a signature. The context for use of esignatures must be specified at all four levels, i.e. a signature policy framework must enable policies that can span all the levels.

Organisational and semantic interoperability of esignatures must be described in context of the process in question; this cannot be described by a generic, technical esignature specification. One of the suggestions of this paper is to provide generic building blocks that can be used to specify use of esignatures as a building block of business process/protocol specifications.

3 Background on Signature Policies

The concept of signature policies was introduced around the year 2000. In 2002-2003, ETSI published a set of technical reports (not standards) [ETSI-102-041] [ETSI-102-045] [ETSI-102-038] [ETSI-102-272]. The ETSI reports specify that a signature policy shall be made available in human readable form; optionally and in parts also in machine processable form. The last two documents referred above specify XML and ASN.1 formats for machine processable parts of signature polices. Furthermore, it is stated that the signature policy should be one document that can be uniquely referenced by an OID (object identifier) or an URI. The ETSI signature format standards C/X/PAdES [ETSI-101-733] [ETSI-101-903] [ETSI-102-778] all include an EPES (Explicit Policy Electronic Signature) format that extends the BES (Basic Electronic Signature) by a reference to a signature policy. The EPES format may, as BES, be extended to more advanced formats.

It is fair to say that the idea of formalising signature policies has not caught on. The technical reports are fairly old and not much referred to. Possible reasons are not analysed in detail in this paper. It is likely that the concept, as it is currently defined by the ETSI reports, is simply not practically useful.

As far as we know, the only EU Member State that has extensive use of signature policies and the EPES formats is Slovakia [SVK-SP-QES] but work is on-going in some other MSs.

From 2008 to 2011, two European projects reinvestigated the signature policy idea: PEPPOL and CROBIES (Cross-Border Interoperability of eSignatures). PEPPOL and CROBIES co-operated and exchanged ideas and the results of the projects are fairly well aligned. Realising the weaknesses of the old ETSI approach, both PEPPOL and CROBIES developed new concepts for signature policy frameworks rather than adjusting the ETSI reports.

A European Norm (will be published as EN 319 172, planned mid-2014) for signature policies shall be developed by ETSI according to the rationalised framework for signature standardisation [ETSI-001-604]. The EN is planned as a multipart standard consisting of a signature policy framework and specific signature policy "profiles". The results of PEPPOL [PEPPOL-D1.3] and CROBIES [CROBIES5.1] are major input to this standard along with the existing ETSI reports. Core persons from PEPPOL and CROBIES participate in the ETSI work.

4 PEPPOL's Need for Signature Policies

The PEPPOL project studied use of esignatures in cross-border tendering for public procurement as a case study to develop solutions that should work for cross-border esignatures in general. A summary of PEPPOL's esignature work can be found in [Olnes12].

In 2009, [IDABC09] found 15 EU Member States with operational e-tendering services; 6 required qualified signature, 2 required advanced signature supported by a qualified certificate, 6 required (at least formally; in reality requirements may be more strict) advanced signature with no requirement on certificate, 1 required only authentication ("simple" esignature). Further investigating matters, PEPPOL discovered that signature requirements were usually underspecified concerning which documents to sign (e.g. all documents of a tender or only the cover letter) and how to apply signatures.

If the tendering process is flexible in accepting different alternatives, this need not be a large problem; as a minimum the situation implies an uncertainty to an actor that wants to submit a tender. However a signature not applied according to requirements may result in a right – or even a legal obligation – to discard a tender. Tenderers based in the country where the call is published will usually know the procedures, but tenderers from other countries need guidance.

Addressing this problem, it became clear to PEPPOL that the concept of signature policy is exactly what is needed to describe the rules for use of signatures in the tendering processes. As a result the signature policy framework presented in this paper was developed.

5 A Pragmatic Approach at Signature Policies

5.1 Do not Mandate an Explicit Policy Document

The ETSI reports require a separate signature policy document that contains all conditions and is assigned a unique identifier (OID or URI). The identifier, together with the hash value of the policy document, can be referenced using an EPES signature format, providing a strong, signed binding between the signed document and the signature policy.

An explicit policy document may be difficult to read and understand by a user, who cannot be expected to be an expert on signatures. The context of a signature can be captured in different ways: in the content of the document that is signed, in the environment of the signing process, such as instructions on a web site or written documentation (e.g. in a call for tender). The need for explicit, formalised signature policies must be viewed in this perspective. It may be argued that a specification of a business process should include specification of signature requirements as an integral part; not as a separate signature policy document.

The main issue is to make the conditions clear to the actors in an easily understandable and transparent way. The desired WYSIWYS (What You See Is What You Sign) property is not only about the content to be signed but also about awareness of the conditions for signing.

As an example, for public procurement tendering signature requirements can be stated in connection with the invitation to tender. One may refer to a separate document (a signature policy) but it is perhaps easier to state the requirements "inline" with the description of the tendering process and other requirements. Conditions are made clear by an "implicit" signature policy. A standardised signature policy framework is still useful as a checklist.

Without an explicit signature policy document to refer to, the EPES signature formats cannot be used and preservation of the connection between signature and signature policy must be managed by other means. For a tendering process, the published documents will be preserved, which should be sufficient as a link to the conditions for signing. However, in other cases preservation of evidence may be more difficult; e.g. showing in retrospect exactly the instructions that a user saw on a web page before signing the document presented.

The problem should not be exaggerated. While we do not discuss in detail the issue of preserving context without an explicit signature policy document, the view of the esignature team of PEPPOL is that such implicit/contextual reference to a signature policy is sufficient in most cases at least for public procurement. The important issue is that policy requirements are clearly stated, readily available and thus expected to be known by all relevant parties.

5.2 Pick and Choose from a Comprehensive Framework

A signature policy framework should identify and specify all elements that may be necessary for a signature policy. When forming a real signature policy, only necessary parts should be included. Limitations should be given only when necessary; flexibility is an advantage. If a signature policy document is formed, then it is important to also define administrative attributes of the policy such as identifier, version, policy owner, date of issue etc.

The elements from the signature policy framework can be used to form the content list and the content of a signature policy document; just delete the elements not needed or leave them open and set values for the remaining elements. Alternatively, select the elements needed and make sure that they are covered with appropriate values "inline" in other documentation for the business process. As yet another alternative, select the elements necessary for a (formal) specification of a protocol or process and include the elements in the specification. This option may be particularly relevant for specifications that are machine processable.

The latter two alternatives point at the fact that a signature policy framework must specify elements that are reusable in different contexts at the level of individual elements.

The need to explicitly specify signature requirements may vary. Requirements may range from "evident" (little room for doubt on the context) and "flexible" (few strict requirements) to "complex" (difficult to understand) and "rigorous" (deviations from the prescribed requirements not allowed). Different users may perceive a process differently; e.g. a domestic user may find a process "evident", while a foreign user, not knowing the legal context, cultural aspects etc., may perceive the same process as "complex". When stating requirements, such issues should be kept in mind.

5.3 Human Involvement is not always the Case

The ETSI reports on signature policies assume a human user that is able to evaluate the policy and its implications. Although automated processing of policy elements is envisaged, a complete signature policy is required to be in human readable form.

Using PEPPOL as an example, tendering is today largely a manual process using documents to be read by humans (e.g. PDF format). However, other procurement processes such as ordering and invoicing are in PEPPOL specified as automated exchange of structured documents (XML format) between the IT-systems of the organisations involved.

PEPPOL contributes protocols and formats to the standardisation work of the CEN BII workshop [CEN-16073-1]. At present, these specifications cover signatures only at a very basic level by referring to XML digital signatures. Hopefully, future work can enhance this to use of the XAdES standard format and signature policy elements from the PEPPOL framework. In the pick and choose approach described above, individual processable specification elements should be extracted and referred to in protocol specifications, Thus, one may specify e.g. how to sign in an ordering protocol. Inclusion of individual elements this way is more complicated if one insists on compiling one signature policy document.

5.4 Top-Down Signature Policy Development Process

[CROBIES5.1] suggests a phased, top-down approach to signature policy development:

- Phase 1: The Business Rules design phase describes the conditions under which signatures will be used within a business or application domain and process.
- Phase 2: The eSignature Implementation Rules design phase shall identify for each signature the associated management, procedural, operational and technical rules, including creation, validation and long-term aspects.
- Phase 3: The Signature Policy Documents design phase sums up all decisions into a human readable and, as far as relevant, machine processable forms.

PEPPOL also envisages that a top-down approach will be used in most cases starting from the signature needs of business protocols and business scenarios. The process is not formalised by PEPPOL (the CROBIES approach can be a good starting point) but will look something like:

1. Describe the process, e.g. a tendering process for public procurement.
2. Determine legal requirements for signatures in the process and add requirements resulting from risk analysis and other sources like best practice.
3. Map this to signature requirements for each step of the business protocol and for each part (document) exchanged in a step; including whether or not a container signature can be used (e.g. signing a zip-file instead of signing each document).
4. State requirements for multiple signatures and their relationships.
5. For each signature required (or desired, or optional), state the commitment implied by the signature including authorisations needed.
6. Specify for what period of time a certificate used for signing must remain valid.
7. Specify signing requirements, e.g. format requirements, certificate and esignature quality requirements and cryptographic algorithms or quality.
8. State the verification process that will be applied and describe requirements and solutions for archival, including archival format and later verification of an archive record.

As stated earlier: Do not over-specify; specify only the necessary parts.

5.5 Who Owns a Signature Policy?

The ETSI reports [ETSI-102-041] [ETSI-102-045] may give the impression that the signer usually is the actor that (specifies and) refers to a signature policy. The receiver is supposed to consult this policy to see if the conditions are acceptable. In PEPPOL's case of tendering, it is quite obvious that it is the receiver (the public sector contracting authority) that sets the rules. The signer (the tenderer) must adhere to these requirements.

Tendering in public procurement is an example of a process that may be subject to signature requirements imposed by laws, regulations or "the authorities" rather than by the individual contracting authority. Requirements may be stated through a standardised set of signature policies that fulfil national regulations. The Slovak approach [SVK-SP-QES] is an example.

Such "centrally defined" requirements favour formalised signature policy documents that can be referred to in different contexts. But even if such policy documents exist, they need not be explicitly referred to. Their use may be as a starting point for stating compliant requirements, e.g. "inline" in a call for tender. By referring to an explicit policy document one incurs that all actors have explicit knowledge of the document – not only of the requirements it contains.

6 Structuring the Signature Policy Framework

PEPPOL's signature policy framework consists of four different parts as shown in the figure below – typical elements (not all elements) shown for each part:

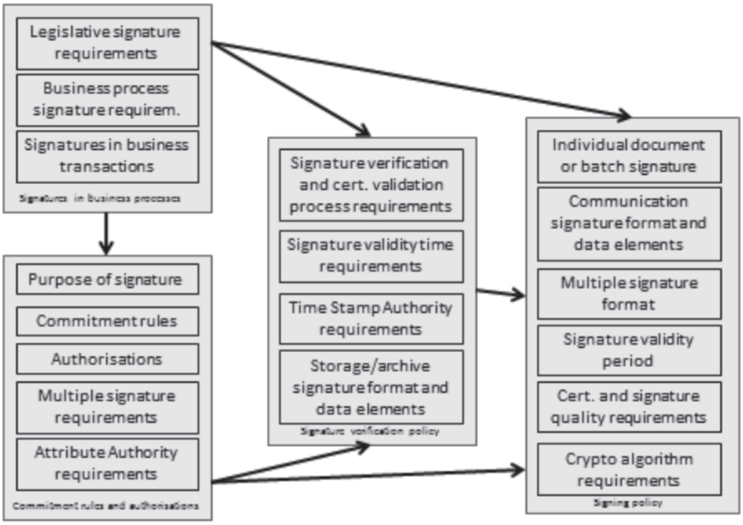

Legislative signature requirements
Business process signature requirem.
Signatures in business transactions
Signatures in business processes
Purpose of signature
Commitment rules
Authorisations
Multiple signature requirements
Attribute Authority requirements
Commitment rules and authorisations
Signature verification and cert. validation process requirements
Signature validity time requirements
Time Stamp Authority requirements
Storage/archive signature format and data elements
Signature verification policy
Individual document or batch signature
Communication signature format and data elements
Multiple signature format
Signature validity period
Cert. and signature quality requirements
Crypto algorithm requirements
Signing policy

Fig. 1: Signature policy framework parts and some typical elements

- *Signatures in business processes:* At the topmost level it must be possible to express use of signatures in business processes in a precise way. This is related to both the legal interoperability and the organisational interoperability levels of the EIF [EIF10].
- *Commitment rules and authorisations:* At the second level is specification of the meaning (semantics – semantic interoperability level of the EIF) of signatures including commitments and authorisations implied by signing something.

- *Signing policy:* At the third level (technical interoperability level of EIF) are the technical requirements that the signer must adhere to in order to produce an acceptable signature, including quality requirements for signature and certificate.
- *Signature verification policy*: Also at the third level are the technical requirements imposed on the verifier(s) of a signature (the relying party).

The parts are related as follows: The "signatures in business processes" category may pose requirements on all other parts, e.g. legislative requirements for technical implementation of signatures. The "commitment rules and authorisations" part may pose requirements on how to sign or verify. "Signature verification policy" may only be fulfilled if elements of the "signing policy" are fulfilled. These are only relationships at a coarse level. More detailed relationships may be specified between signature policy elements inside or across signature policy parts.

6.1 Legal Considerations – Legal Level

A process or transaction using an esignature may be subject to explicit legal requirements. National law, having supreme value in national context, must ensure that legal requirements do not block cross-border interoperability. The following principles can be stated, using EU Member States as examples:

- The signature policy applied must comply with its referred legislation.
- The signature policy shall as far as possible be specified independently from legislation. In particular, the policy shall not refer to specific national approval/accreditation/supervision schemes, specifications, profiles or other elements that one cannot expect foreign certificate issuers or users to comply with.
- Requirements shall as far as possible be stated in general terms that can be fulfilled by actors in other Member States. As an example, a policy rule may, based on national legislation, require a qualified signature but in this case the policy shall not refer to particular requirements imposed on issuers of qualified certificates in the particular Member State.
- The signature policy shall as far as possible avoid requirements that are likely to cause conflicts with legislations of other Member States.
- The signature policy shall as far as possible be non-discriminatory with respect to esignatures from other Member States, i.e. it should be possible to fulfil the policy based on products and services that can reasonably be assumed to be available in any Member State.
- It is recognised that that there are limitations to the previous bullet point; e.g. qualified signature may be required by some Member States but products and services supporting qualified signature are not currently available in all Member States.

As a general principle, a necessary assumption is also:

- The national approval status of a certificate or esignature in one Member State shall be accepted by other Member States. This particularly applies to qualified certificates and qualified signatures but the principle should be the same for non-qualified solutions.

PEPPOL's signature policy framework contains elements to specify the legislation that applies and other reasons for using signatures in a process. The following should be noted:

- A business process may require an advanced signature in one country but not in another.
- For a cross-border process, the actors must select a legislation to refer to. For public procurement, the contracting authority's legislation will usually be referred to.
- Legislative requirements may in some countries extend to detailed technical requirements.

- Even if not mandated by the selected legislation, an actor may wish to use a signature in order to comply with his own, local legislation and the resulting normal business practices.

Whenever legal interoperability at the level of national laws is not possible, PEPPOL's recommendation is to seek a situation where international contract law can be applied.

6.2 Signatures in Processes – Organisational Level

Esignatures are used in a business process for one of three reasons: There is a legal requirement to sign, a risk evaluation concludes with a signature requirement, esignature is a convenient (e.g. user friendly) mechanism. The two latter (risk and convenience) may also refer to best practice recommendations for use of esignatures. A definition of a business process is given by CEN BII [CEN-16073-1] as follows:

- The choreography of the business process(es), i.e. a detailed description of the way the business partners collaborate to play their respective roles and share responsibilities to achieve mutually agreed goals with the support of their respective information systems;
- The electronic business transactions exchanged as part of the business process and the sequence in which these transactions are exchanged;
- The business rules governing the execution of that business process(es), its business collaborations and business transactions, as well as any constraints on information elements used in the transaction data models;
- The information content of the electronic business transactions exchanged by pointing to a given data model for each of the business transactions.

Requirements for signatures may be part of the business process choreography on an overall level, at the level of business transactions, and related to governing business rules. The bullet point on information content is less relevant as esignature as a mechanism should be independent from the data model and information content actually referred to.

A requirement for use of signatures may be stated both at the choreography level and for each transaction as follows:

Signature required: List of values: Shall, should, may, shall not be signed.

A default value should be assumed if no explicit statement is given, e.g. that a business protocol step *may* be signed. Unless explicitly instructed not to sign, a sender may independently decide to sign in protocol step.

For a multi-part transaction, the signature policy element above may be replicated for each part to indicate the need to sign each individual part. As an example, a call for tender may specify that the tender letter shall be signed while attachments may be unsigned, or that all parts shall be signed.

When several parts of a multi-part message are signed, there is a need to specify whether or not a batch signature shall or can be used, such as assembling all documents in a zip-file and signing the zip-file or otherwise signing several "documents" in one operation.

Batch signature allowed: List of values: Shall, should, may, shall not be used.

If not allowed, each part must be individually signed whenever signature is required. If multiple signatures are used, one may specify scenarios that apply "inner" signatures to each document together with an "outer" batch signature.

Requirements for multiple signatures in a business process are difficult to formalise. PEPPOL has largely left this for further study but specifies as a minimum the following:

> *Content previously signed: Required, optional, not allowed.*

Required means that at least one other actor must have signed in advance, e.g. the other party signs the contract first. Optional may for example mean that the sequence of the signatures is irrelevant. Not allowed means that this actor signs first. More elaborate policies defining sequences of signatures may be defined. Note that by applying commitment rules as defined below, one should be able to define many rules applying to such sequences. The technical details on how to apply signatures on a previously signed element are covered by the signing rules.

PEPPOL further suggests defining the following element:

> *Multiple signatures for same actor: Required, optional, not allowed.*

If required or optional, commitment rules should be applied individually to each signature. Further signature policy elements could be defined to this effect. Not allowed means that one signature (usually one person) must represent sufficient privileges alone.

6.3 Commitments and Authorisations – Semantic Level

Rules regarding commitment and authorisations may be specified for each individual signature. PEPPOL's signature policy framework does not contain elements to combine authorisations from several signatures; this must be specified by the business protocol rules.

In the current situation, a personal signature must be assumed. The proposal for a new EU regulation in the eID and esignature area [COMM12] makes the distinction between a personal *esignature* and an *eseal* produced by a legal person. Further work on signature policies must include elements to specify whether a signature or a seal is required, either as a business process rule or as a commitment and authorisation rule.

Use of attribute authorities and attribute certificates is left for further study by PEPPOL. This may include X.509 attribute certificates, SAML tokens or XACML tokens or others. Furthermore, requirements for use of other trusted services such as notaries are left for further study.

One way of stating a commitment is to use a statement in the same way as is often done for PDF signatures [ETSI-102-778]. Examples are "I approve the content" or "I am the author". A set of general statement may be defined plus it may be possible to extend by separate definitions or free text statements.

> *Signature purpose: List of statements, possibly also free form statement.*

Note that an esignature may be anything from a transport signature (authentication and integrity protection mechanism) to a legally binding signature on a contract.

There may be a further need to specify authorisations necessary – like the ability to sign on behalf of the company for the sum implied by a contract.

> *Authorisation statement: List of statements to select from, possibly one or more statements that shall be included, possibly also free form statement.*

Examples: "I am managing director for company NN", "I am authorised to sign this contract on behalf of company NN". This may point at a need for multiple signatures where the combination of authorisations attributed to different persons is needed to achieve the task.

Attributes concerning company, roles and authorisations should be regarded as claims that in a given context may have to be supported by assertions of a given assurance level.

> *Assurance level for company, role, authorisations: Selection of alternatives.*

Appropriate assurance level can be specified in a number of ways, including use of external sources for attestations. As an example, six approaches for use of esignatures for a submitted tender have been outlined by PEPPOL:

- A signature of sufficient quality is accepted. The risk of mistakes is low and if something is wrong a strong proof exists through the signature.
- A registration process binds name in certificate to role and authorisation for the organisation. Requirements to the process are described by [PEPPOL-D1.3] but not repeated here.
- Binding between names and roles/authorisations are "automatically" established by means of certified documents such as a VCD (Virtual Company Dossier as defined by PEPPOL) or attestations from business registers.
- Use of employee certificate that includes an organisation's name (and unique identifier) in addition to the name of the person.
- Use of eseal that includes only organisation name and unique identifier, no person name.
- Combination of an inner, personal signature and an outer eseal attesting to authorisations.

6.4 Signing Policy – Technical Level

6.4.1 SDO Format

By applying one or more signatures, one creates a signed data object (SDO). A requirement on the signer is to produce an SDO that can be accepted by the receiver. The signer creates a communication SDO, which may be different from storage SDO that goes into an archive and can be created at verification time by adding attributes.

> *Communication signature format: Selection of allowed formats, or restrictions.*

This should refer to profiles/formats of XAdES [ETSI-101-903], CAdES [ETSI-101-733] and PAdES [ETSI-102-778]. As a starting point, PEPPOL recommends placing few format requirements on the sender; the sender should be allowed to sign using the format supported by local software. An issue for a signer policy may be e.g.: I have a PDF document, shall I sign by a PAdES signature or is a CAdES signature allowed?

Further signature policy requirements may restrict signature type (wrapping, detached, embedded). One cannot really say that different signature types imply different semantics for the meaning of the signature. PEPPOL thus recommends not restricting signature type use unless necessary for application of multiple signatures where some alternatives are cumbersome.

More detailed requirements may specify information elements to include in the SDO. This is not outlined here but examples are: Elements of data to be signed, rules for inclusion of certificates and path information, rules for signer's inclusion of revocation status information (OCSP or CRL), and rules for signing time and use of time stamps.

6.4.2 Multiple Signatures

Signing a document that is previously signed can be done in three ways: parallel signature, i.e. the signature covers document content but not previous signatures, sequential signature, i.e. the signature covers document content and previous signatures, or countersignature, i.e. the signature covers one or more previous signatures but not document content.

It is clearly possible to assign different meaning (semantics) to the different variants, e.g. a countersignature attests to the correctness of a previous signature, not to the correctness of the document content. A sequential signature emphasises the ordering of the signatures.

Multiple signature format: Parallel, Sequential, Countersignature.

In the current state of signing software and user understanding, PEPPOL suggests not placing too much emphasis on the possible semantics of multiple signature formats but rather to make the purpose of each signature explicit by use of "commitment rules" policy elements (see above). Allowing or denying use of countersignatures may be an exception.

Multiple signature scenarios can be made almost arbitrary complex by mixing parallel, sequential and countersignatures using different SDO formats and signature types. A simple example is a PDF document signed first using an embedded PAdES signature, and then wrapped in a CAdES SDO for the second signature. Although SDO formats may be specified independently for each signature, a prudent advice is to try to avoid too complex scenarios.

6.4.3 Certificate and Signature Quality Requirements

Requirements on quality and approval status of certificates and signatures are crucial in many cases, e.g. requirements for qualified signature or advanced signature using a qualified certificate, or requirements at lower quality levels. PEPPOL has developed a quality classification scheme [PEPPOL-D1.3] [OlBuAn09] that can be used as a starting point for specification of quality requirements. CROBIES also addressed this issue.

Furthermore, cryptographic quality may be important, implying policy elements defined for hash algorithm, public key algorithm and key length, and/or crypto suites (hash and crypto).

A signature policy should not place restrictions on certificate content unless there are strong reasons for restricting e.g. naming formats. However, a signature validation policy may require that a signature remains valid for a period of time (unless it is unexpectedly revoked), e.g. until a tender is opened. This poses a requirement on the signer and should be reflected in the signing policy.

6.5 Signature Verification Policy – Technical Level

This part of the signature policy is in principle local to the relying party but there may still be a need to state the policy requirements at least for informational purposes. Detailed technical requirements on the verification process can be defined, such as revocation checking, path processing and revocation grace period. This is not further described here. Verification result may be represented both in human readable form and as an XML report.

Timing issues are important for verification. A signature may be required to be valid at the time of signing (possibly supported by a TSA time stamp from the signer), at the time of first verification (e.g. at the time of opening a tender), or at some later time (e.g. until the end of the business process). When signature verification is done, the SDO may be extended by adding verification information and a time stamp. The resulting format can be subject to policy requirements for archival/storage SDO format.

7 Conclusion

As part of the signature work in the PEPPOL project, a comprehensive signature policy framework has been specified. The recommendation is to pick and choose elements from a framework in order to specify the conditions for signing in a particular business process. The elements selected can either be gathered in a separate signature policy document, or be used "inline" in the appropriate places of process/protocol descriptions. With reference to the European Interoperability Framework [EIF10], the goal is to specify conditions for esignature interoperability at all levels: legal, organisational, semantic and technical.

The signature policy framework needs further work concerning details on semantics and representation. Presumably this will be provided through the on-going work in ETSI on a European Norm on a signature policy framework; the work of PEPPOL and the CROBIES project are major inputs to this work.

References

[CEN-16073-1] CEN CWA 16703-1, Business Interoperability Interfaces for Public Procurement in Europe – Part 1: Profile Overview. January 2010.

[COMM12] Commission of the European Communities, Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM(2012) 238/2, June 2012.

[CROBIES5.1] Study on Cross-Border Interoperability of eSignatures (CROBIES), Guidelines and Guidance for Cross-border and Interoperable Implementation of Electronic Signatures. CROBIES deliverable 5.1, July 2010.

[EIF10] ISA programme, European Interoperability Framework for European Public Services, v2.0, December 2010.

[ETSI-001-604] ETSI SR 001 604 v1.1.1 (2012-07). Rationalised Framework for Electronic Signature Standardisation.

[ETSI-102-038] ETSI TR 102 038 V.1.1.1 (2002-04) Electronic Signature and Infrastructure (ESI) – XML Format for Signature Policies.

[ETSI-102-041] ETSI TR 102 041 V.1.1.1 (2002-02) Electronic Signature and Infrastructure (ESI) – Signature Policies Report.

[ETSI-102-045] ETSI TR 102 045 V.1.1.1 (2003-03) Electronic Signature and Infrastructure (ESI) – Signature Policy for Extended Business Model

[ETSI-102-272] ETSI TR 102 272 V.1.1.1 (2003-12) Electronic Signature and Infrastructure (ESI) – ASN.1 Format for Signature Policies.

[ETSI-101-733] ETSI TS 101 733 V.1.7.4 (2008-07) Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

[ETSI-101-903] ETSI TS 101 903 V.1.3.2 (2006-03) Electronic Signature and Infrastructure (ESI) – XML Advanced Electronic Signatures (XAdES).

[ETSI-102-778] ETSI TS 102 778 V.1.1.1 (2009-07). Electronic Signature and Infrastructure (ESI) – PDF Advanced Electronic Signature Profiles (PAdES), Parts 1-5.

[EU99] EU: Community Framework for Electronic Signatures. Directive 1999/93/EC of the European Parliament and of the Council, 1999.

[IDABC09] IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications (Final Study and 32 National Profiles), December 2009.

[Olnes12] J.Ølnes, PEPPOL – Experience from Four Years Work on eSignature Interoperability, Proceedings of the ISSE 2012 Conference, October 2012.

[OlBuAn09] J.Ølnes, L.Buene, A.Andresen, H.Grindheim, J.Apitzsch, A.Rossi, A General Quality Classification System for eIDs and e-Signatures, Proceedings of the ISSE 2009 Conference, October 2009.

[PEPPOL-D1.3] PEPPOL Deliverable D1.3: Demonstrator and Functional Specifications for Cross-Border Use of eSignatures in Public Procurement. September 2011.

[SVK-SP-QES] Slovak National Security Agency, Signature Policies for QES, version 1.1, December 2007.

Facing the Upheaval: Changing Dynamics for Security Governance in the EU

Yves le Roux

Member of the (ISC)² Europe Middle East and Africa Advisory Board
CA Technologies
Tour Opus 12, 4 place des Pyramides, La Défense 9
92914 Paris La Défense Cedex.
Yves.leroux@ca.com

Abstract

Information Security is becoming the victim of the disruptive change introduced by the latest trends in Information technology: Bring Your Own Device (BYOD), Cloud Computing and Social Networking. Today a corporation's systems development, and therefore that of its technical security controls, is slipping away from the carefully planned IT strategy.

For the information security professional, this makes for a very challenging management landscape.

This paper outlines the changing dynamics for security governance brought about by the shifts currently taking place in IT technology against the context of the developing expectations coming from our increasingly active policy makers. It offers the first published focus on the EMEA findings of the 2013 (ISC) ² Workforce Study, citing the experience of 3229 people in the region with responsibility for information security, including analysis for Germany, France and the United Kingdom. Findings confirm the shift in IT:

- Virtually all companies have some level of cloud computing,
- Almost half of companies that allow any user device to access their corporate networks,
- Social media too is evolving from its beginning as a consumer platform with approved business use.

Survey insights look at the impact of these developments and stresses in the ability to defend and recover from attack. At the light of these results, we will review and comment the various policy proposals currently under discussions in the various EU instances

1 A Changing Landscape

The "good old days" are gone forever.

Those were the days when IT environments were more predictable and easier to control. The user population and their access patterns were more easily defined. Stick a firewall in front of key systems, create some controls around who can access what, and you're done.

The world is far different now. Cloud adoption, mobility and the consumerization of IT are transforming many business activities for enterprise employees, partners and customers. However, as we leverage these new capabilities, we face a highly fragmented IT environment that is quickly

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_10, © Springer Fachmedien Wiesbaden 2013

overtaking the comfortable security perimeter of firewalls and virtual private networks (VPNs) we so carefully constructed over the last decade.

IDC forecast that by 2015, about 24 per cent of all new business software purchases will be of the service-enabled type. And as we know, much Software as a Service (SaaS) purchases are made by business users, completely bypassing IT and security organizations. Previously, this "shadow IT" environment was about a business user buying a server, getting an IP address and installing a stealth application. Now, a crafty marketing person needs only a credit card to start pushing corporate data to cloud storage! Furthermore, in June 2013, a research conducted by the Ponemon Institute on behalf of Thales e-Security has shown that 53% of businesses transfer sensitive or confidential data to the cloud.

And devices are proliferating. According to a February 2012 report by Forrester, 52 per cent of all information workers now use three or more devices for work and many of these are not owned by the enterprise. Forrester further states that in four years, 350 million employees will use smartphones — 200 million of them not supplied by the business. Maintaining a high level of security is obviously difficult, given these statistics.

The social media sites have moved beyond the novelty stage and into the mainstream. They have become so pervasive that they have emerged as effective tools within the corporate setting as well. The line separating the recreational use of these tools from legitimate business purposes has become increasingly blurred. The potential legal issues that can arise from social networking activities run the gamut. Privacy, unauthorized activities, and intellectual property issues stand top-of-mind for many individuals and enterprises. Other areas, such as content ownership, regulatory compliance, and even criminal activity, are impacted by social media, too.

More data is being collected, processed and transferred than ever before. Data is collected by billions of connected devices, people and sensors that record trillions of transactions and behaviours each day. The unprecedented amount of data being generated is created in multiple ways. Data is actively collected from individuals who provide it in traditional ways (by filling out forms, surveys, registrations and so on). They are also passively collected as a by-product of other activities (for example Web browsing, location information from phones and credit card purchases). The increasing use of machine-to-machine transactions, which do not involve human interaction, is generating significant amounts of data about individuals. With more than 6 billion people connected to mobile devices, an increasing variety of data is also becoming capable of being linked to individual identity. Smartphones are now able to capture and track an individual's location patterns as well as help create new levels of authentication. All of this data is further analysed and commingled to create inferred data. The potential for new value creation from allowing data to flow and combine with other data needs to be balanced against the potential risks and intrusions this could cause.

With the increased popularity of DevOps over the past few years, many organizations have been merging their IT operations and development teams. By doing so, experts say, the software-deployment cycle is compressed from many months to days. The trade-off for moving that quickly, however, is the potential for weakened security. For example, if a build were not properly secured, those errors would be replicated quickly; or if code isn't tested by the Quality Assurance team, security-related software mistakes are more likely to slip by. Such errors may not worry others, but they are of critical concern to security officers, who are already running a number of steps behind most deployments.

2 The Current State in Europe Middle East and Africa

The International Information Systems Security Certification Consortium, Inc., (ISC) $^{2®}$ conduct every year a Global Information Security Workforce Study (GISWS) [ISC213]. The GISWS is the largest study of its kind and provides detailed insight into important trends and opportunities within the information security profession. For this conference, we have focus on the EMEA findings. Due to the changing landscape, this year's survey intensified its focus on the risk and response to secure software development, cloud computing, BYOD and social media.

2.1 Secure Software Development

It is interesting to notice that secure software development, more than any other discipline, is where the largest gap between risk and response attention by the information security profession exists. According to survey respondents, insecure software was a contributor in approximately one-third of the 60 percent of detected security breaches. In the other 40 percent of detected breaches, insecure software's role was uncertain either because post-breach forensics were inconclusive, or the survey respondents were not privy to the forensics. Regardless of this uncertainty, along with insecure software's unquantifiable attribution in undetected breaches, information security professionals are certain that their concerns regarding insecure software are justified.

The next question is what is being done to mitigate or resolve the risk of insecure software? This mitigation begins by being involved in software development, procurement, and outsourcing. Only 11 per cent of the information workforces from the EMEA region are personally involved in software development activities as more than 50 per cent report that their organization is involved in software development. Notably, significantly more in France (39%) have no involvement at all in software development activities. Among the small proportion of information security workforce personally involved in software development or procurement, requirement specification (77%) is the most common area of involvement, yet with those from the Middle East showing significantly lower involvement (59%) than their counterparts.

This is a signal of a gap between risk and response by information security professionals and their organizations.

Unless software and information security professionals' involvement is deepened in secure software development, procurement, and outsourcing; and training and education permeates the ranks of software development functions, the risks associated with insecure software will remain. Furthermore, deepening engagements in software development cannot occur in isolation or be the exclusive responsibility of the information security workforce. Other relevant functional groups—software developers, application owners, and the quality assurance and testing teams—must internalize secure software development best practices and engage, as standard operating procedure, with information security professionals. While expertise in the information security discipline varies across groups, all groups must be responsible in order for the risk and consequences of insecure software to decrease.

2.2 Cloud Computing

Selection among cloud computing approaches corresponds to the high level of risk currently associated with the cloud. Overall, private cloud computing is the most prevalent approach to the cloud computing use (38 %), followed by software as a service (20%). With private cloud computing services, the cloud customer retains more control over the cloud infrastructure and how that infrastructure is secured than other approaches

Regarding cloud computing those within the EMEA region are concerned about are confidential or sensitive data loss or leakage and exposure of confidential or sensitive information to unauthorized systems or personnel. Yet, of notable mention, those in South Africa are more concerned about cloud computing than others in the EMEA region.

Fifty-eight per cent of the EMEA information security workforce agree that cloud computing is increasing the demand of information security professionals—notably more prevalent among those in South Africa (69%) and the Middle East (68%).

Approximately three-fourths of the EMEA information security workforce agree that cloud computing requires new skill sets—an opinion slightly less prevalent among those in France and the United Kingdom. The very high percentage of respondents choosing " An enhanced understanding of cloud security guidelines and reference architectures " skills is indicative that there remains considerable ambiguity regarding cloud related risks. Furthermore, with cloud services providers not bound by industry standards or regulations with regard to security practices and procedures, general understanding of potential cloud risks would be incomplete in assessing risk. A thorough understanding of each potential cloud service provider would be required to adequately assess risk across providers.

2.3 Mobile Security and Bring-Your-Own-Device (BYOD)

On a worldwide basis, approval for use of user-owned devices, according to this survey, is more than 50 per cent. Differences in allowance do exist, primarily among verticals. For example, 67 per cent of respondents in government state user-owned devices are not allowed. In the private sector, 47 per cent of respondents in banking, insurance, and finance verticals state user-owned devices are not allowed. At the other end, education is most permissive, with 86 per cent of education respondents claiming user-owned devices (employee and business partners combined) are allowed.

The information security workforces' organizations in France and Germany are much more strict about BYOD, as more than half do not allow any user devices access to their network. Yet, significantly fewer information security workforces' organizations in South Africa report the same strict policy. Despite allowing BYOD, approximately three-quarters of the EMEA information security workforce consider BYOD a significant security risk to their organizations. Among those who allow BYOD, approximately 50 per cent have end user license agreements, to which they are enforced both toward employees and toward business partners. Notably, those in France are significantly less likely to enforce end user license agreements toward business partners. Beyond these agreements, a growing number of security technologies are used. Furthermore, all mobile security technologies listed in the 2011 survey (encryption, remote lock and wipe, MDM, mobile anti-malware, and DRM) had a greater per cent of respondents claiming use in 2013. Also as a sign of expanding security technologies in use are the modest percentages assigned to technologies that were in their commercial infancy in 2011, such as secure containerization or secure sandbox, with 20 per cent of respondents stating it is used in the 2013 survey? Encryption and VPNs are the top technology solutions employed to mitigate risks associated with mobile device usage by the information security workforce in the EMEA region; the former slightly more significant in Germany, the United Kingdom, and South Africa and the latter in France.

Development of new skills in mobile security and BYOD by information security professionals was noted as required by 74 per cent of respondents. This opinion has little variation by company size, job title, or industry vertical.

2.4 Social Media

The security concern with social media is less than BYOD and cloud computing. Nevertheless, there is sufficient concern that a majority of information security professionals take action to manage the risk emanating from social media use. The most prominent means to limit access to social media is by using content filtering and website blocking technologies. The prominence of these technologies is greater with larger companies than small. Not surprisingly, higher proportions of medium, large, and very large companies surveyed use this technology for social media access control than small companies. Also as expected, survey respondents in the banking, insurance, and finance verticals expressed greater use (82 per cent) of these technologies than any other vertical. Respondents in the education vertical are the most permissive in social media access; 59 per cent state their organizations have no social media restrictions.

In EMEA, LinkedIn is the most common social media (74%) used for personal reasons during work hours. Interestingly, Xing is significantly more in Germany (60%) than in other EMEA countries (29%). Overall, the information security workforce in the EMEA region is moderately concerned about security threats via social media.

3 European Union initiatives

According to Eurostat, In January 2010, 27 % of enterprises in the EU 27 countries had a formally defined Information and Communication Technologies (ICT) security policy with a plan for regular review; the corresponding shares in Sweden, Norway and Denmark were over 40 %.

According to the World Economic Forum, there is an estimated 10% likelihood of a major critical information infrastructure breakdown in the coming decade, which could cause damages of $250 billion.

3.1 Data Protection Regulation

In the field of Personal Data protection, Clouds cross borders, and so does the data they hold. In January 2012, the European Commission proposed a Regulation to replace a Directive: that means a single set of rules for Europe, not 27 different ones. Alongside that, under the new rules you will get a one-stop-shop of enforcement. So that, even if an operator is active in several EU countries, it will only have to deal with one data protection authority – the one where its main base is. This will be a great progress. Proposed binding corporate rules will potentially reduce legal ambiguity surrounding data transfers, and joint operations on the part of supervisory authorities will reduce bureaucratic burdens. But, it poses a number of challlenges for companies:

- The designation of a data protection Officer (DPO). This obligation will apply to all public sector bodies and enterprises with 250 or more employees, as well as to companies whose core activity involves the monitoring of data subjects.
- Notifications to regulators which would have to be made " without undue delay and, where feasible, not later than 72 hours after having become aware of it", whilst notifications to individuals would have to be made simply "without undue delay".
- The 'right to be forgotten'; giving individuals a general right to force organisations to delete personal data stored about them "without delay".
- The right to data portability giving the right to obtain a copy of his/her personal data which are processed electronically and in a 'structured and commonly used format' for further use and the right for individuals to transmit their personal data from one provider to another.

Furthermore, in June 2013, after the PRISM leakage,Justice Commissioner Reding has indicated to the European Parliament that she would not object if the parliament were to reinstate of Article 42 (which was removed from the draft Commission proposal by US lobbying) and would require authorisation in every instance where the communications of an EU citizen were requested by US agencies from service providers based in the USA

Consequently, US companies with subsidiaries in Europe will be caught between two legal regimes. The US demands that they maintain secrecy about its requests for personal data. But in the EU, they are required to notify the person in question that the US is requesting their information.

As a consequence, in the European Parliament, well over 4,000 amendments have been tabled. Ideological and political divisions emerged among European Parliament political groups as they debated amendments on the draft EU data protection bill. As a result, the orientation vote on the EU's data protection regulation will take place either in September or October. The vote was originally intended in early 2013.

Ireland as EU president from January to June 2013, at the end of May, released a draft compromise text that deals with some of the flaws in the original proposed Regulation. Reports from Paris suggest that the Irish compromise would still not be acceptable to France. Belgium, Germany, Italy and Spain may also still have concerns.

Consequently, we may expect an adoption in 2015 or even 2016 with an enforcement two years after the adoption

3.2 European Cybersecurity Strategy

In February 2013, The European Commission has published a cybersecurity strategy alongside a Commission proposed directive on Network and Information Security (NIS).

The cybersecurity strategy – "An Open, Safe and Secure Cyberspace" – represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks.

The strategy articulates the EU's vision of cyber-security in terms of five priorities:

- Achieving cyber resilience

- Drastically reducing cybercrime
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Developing the industrial and technological resources for cyber-security
- Establishing a coherent international cyberspace policy for the European Union and promoting core EU values

The proposed NIS Directive is a key component of the overall strategy and would require all Member States, key internet enablers and critical infrastructure operators such as e-commerce platforms and social networks and operators in energy, transport, banking and healthcare services to ensure a secure and trustworthy digital environment throughout the EU. The proposed Directive lays down measures including:

(a) Member State must adopt a NIS strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;

(b) Creating a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews;

(c) Operators of critical infrastructures in some sectors (financial services, transport, energy, and health), enablers of information society services (notably: app stores e-commerce platforms, Internet payment, cloud computing, search engines, social networks) and public administrations must adopt risk management practices and report major security incidents on their core services.

Interestingly, on June 17th 2013, Peter Hustinx, European Data Protection Supervisor (EDPS), said: “There is no security without privacy. So I am delighted that the EU strategy recognises that it is not a case of privacy versus cyber security but rather privacy and data protection are guiding principles for it. However, the ambitions of the strategy are not reflected in how it will be implemented. We acknowledge that cyber security issues have to be addressed at an international level through international standards and cooperation. Nevertheless, if the EU wants to cooperate with other countries, including the USA, on cyber security, it must necessarily be on the basis of mutual trust and respect for fundamental rights, a foundation which currently appears compromised.”

3.3 ENISA New Regulation

On June 18th 2013, ENISA received a new Regulation, granting it a seven year mandate with an expanded set of duties. The new Regulation enshrines ENISA’s achievements in areas such as Computer Emergency Response Teams (CERTs) in Member States, and its world-class cyber security exercises, such as Cyber Europe 2012, with 600 participants from across Europe.

Other key points of the new Regulation include:

- Providing ENISA with a strong interface with the fight against cybercrime – focusing on prevention and detection – with Europol’s European Cybercrime Centre (EC3)
- ENISA supporting the development of EU cyber security policy and legislation
- The Agency supporting research, development and standardisation, with EU standards for risk management and the security of electronic products, networks and services

- ENISA supporting the prevention and detection of, and response to cross-border cyber-threats
- Aligning ENISA more closely to the EU Regulatory process, providing EU countries and Institutions with assistance and advice

This will provide European Information Security Officers with a centre of excellence on all matters concerning network and information security.

4 Conclusion

The goal of security and risk strategy is to anticipate possible future events and situations and build security and risk strategy and infrastructure that will provide sufficient protection for the enterprise in all probable scenarios. This is a difficult process that is part science and part dark art.

Pratically, Information Security Officer will have to shelter their organizations from a highly dynamic threat environment through a renewed sense of discipline as regulators, executives, and shareholders increasingly turn the microscope on their IT security practices.

References

[ISC213] Global Information Security Workforce Study 2013. https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf.

Alternative Authentication – What does it really Provide?

Steve Pannifer

Consult Hyperion
Tweed House, 12 The Mount
Guildford, GU2 4HN, UK
steve.pannifer@chyp.com

Abstract

In recent years many new technologies and techniques have been developed for authenticating individuals attempting to access digital services. Some of these appear to offer new, innovative and flexible ways to improve security, potentially removing the need for relatively expensive hardware devices. We explore some the characteristics of these new methods in relation to the requirements of some example business services. Our intention is not to provide a full or detailed assessment of the methods but rather to provide an initial view which we hope will stimulate further debate.

1 Introduction

Two key technology trends are driving changes in the way we authenticate ourselves online:

- **Cloud services**: As more services become cloud-based traditional notions of information security are challenged. For example, when an enterprise places corporate assets in the cloud, the perimeter of that organisation becomes less clearly defined. It has been said that "identity is the new security perimeter" [1]. The trend to move consumer financial services into the cloud (e.g. via online wallets) is particularly interesting [2]. Effective authentication to such services is critical to mitigate fraud. Previously authentication often relied on devices (smart cards, OTP tokens). Newer products often do not use such devices to avoid the cost of deploying and managing devices, meaning that alternative authentication methods are required.
- **Multiple devices**: Consumers are becoming used to interacting with online services in a variety of contexts using multiple devices and channels [3]. This implies the need for a portable identity that can be used whichever device or channel a consumer is on at that point in time. From an authentication point of view, this would appear to suggest that tying the individual to a specific device may not be the right approach.

Existing conventional authentication technologies are not always well suited in these new environments:

- Passwords are cumbersome to use which encourages bad practice [4]
- Smart cards and One Time Password devices can be cumbersome to use and the need for a separate hardware device may be inconvenient

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_11, © Springer Fachmedien Wiesbaden 2013

There are numerous alternative techniques that are being used to help with authentication in these new environments, such as risk-based authentication, location and device fingerprinting.

Starting from the established principles of two-factor authentication, we consider the types of authentication that can be achieved with these alternative authentication technologies. We consider the requirements of some example business services and compare these against the apparent capabilities of various authentication technologies. Whilst it is recognised that these technologies are already playing an important role in securing services, we will ask if they should be described as "authentication" in the conventional sense.

The following alternative authentication methods are considered:

- **Risk Based Authentication**: Using transactional information, which is compared to the profile of the user to calculate a risk score for the service request. If the score indicates a low risk the user may be allowed to access the service directly. If the score indicates a higher risk the user may be required to undergo additional authentication steps.
- **Knowledge Based Authentication (KBA)**: Asking the user a set of personal questions that typically only they will be able to answer. KBA can be "static", based on a fixed set of pre-registered questions or "dynamic", generated from a wider collection of personal information.
- **Physiological Biometrics**: Measuring physical human characteristics such as fingerprint, voice print and retina.
- **Behavioural Biometrics**: Measuring human characteristics related to the behaviour of the person, e.g. keystroke dynamics.
- **Location**: Determining that the geographic location of the user corresponds to the expected location of the identity being claimed.
- **Device fingerprinting**: Checking various device attributes (e.g. device identifiers, software versions, network addresses) to ensure that service is being accessed from a known and expected device.

We do not consider the use of a cryptographic hardware token contained within a device (e.g. a SIM in a mobile handset) for identifying the device as "device fingerprinting". The use of such a token is considered as a more conventional "what you have" authentication factor.

This paper does not discuss how the strength of the above methods is measured, or the level of assurance that can be achieved by each of them. Instead we focus on the characteristics of the methods; what they do or do not provide regardless of the level of assurance achieved.

2 What is an Authentication Factor?

Ideally an authentication factor needs to exhibit two key characteristics [5]:

- **Based on a secret**: This could be a secret the user knows (e.g. a secret password) or a secret the user possesses (e.g. a secret key inside a tamper resistant smart card). Some authentication techniques use data that is private rather than secret. This is data that is usually only available to the user, and a limited number of other people, but could be discovered by malicious parties (e.g. mother's maiden name can be found, fingerprints can be copied).

- **They must be unique**: This enables that each user can be distinguished from each other user. With some weaker authentication factors (e.g. a PIN) the system may not ensure that every user is unique. There needs to be a sufficient level of uniqueness and unpredictability so that a user cannot claim that the authentication was of someone else.

The following table considers, for the alternative authentication technologies listed above, whether they are secret and unique, or not:

Table 1: Do alternative authentication methods meet criteria for an authentication factor?

Method	Secret or Private?	Unique?
Risk Based Authentication	Neither	Not unique
Knowledge Based Authentication	Private	Not unique
Physiological Biometrics	Private	Unique
Behavioural Biometrics	Private	Unique
Location	Neither	Not Unique
Device fingerprinting	Neither	Unique

None of the methods being considered are based on a secret (i.e. something that only the user knows). Most of the methods use private information. Three methods do not use either secret or private data, namely:

- Risk Based Authentication, as the transactional data being used to authenticate the transaction will as a minimum be known to the service being accessed (e.g. a merchant) but may also be known to intermediaries involved in the transaction (e.g. a price comparison site or marketplace). In addition it may be possible to find out the data about the user (e.g. by searching public records)
- Location, as the user's location will be known to other individuals in the vicinity of the user;
- Device fingerprinting, as the data can be read from the device by applications loaded onto the device or potentially from transaction data sent from the device.

With regards to uniqueness, biometric methods are specifically designed and tuned to maximise the uniqueness of the characteristic being measured. Issues such as false positives and false negatives do exist and are well documented. We assume that an acceptable level of uniqueness can be achieved. Similarly device fingerprinting will often seek to use globally unique device identifiers which are unique.

The other methods are not unique:

- Risk Based Authentication and Knowledge Based Authentication, use data that could be the same for multiple individuals. Two people could buy the same item (transactional information). Two people could have pets with the same name. Conventional user chosen passwords, by comparison, may not be unique but if chosen well should not be predictable. Clearly practice does not match theory in this case, which is why it is necessary to consider alternatives to passwords.
- Location is not unique due to the limitations of technology. Civilian GPS systems for example are typically accurate to within a few metres. This does not prevent another individual appearing to be in the same location. To be truly unique it would be necessary to know the precise volume of 3-dimensional space occupied by the individual.

From the above list of alternative authentication methods, only biometric methods can be considered as true authentication factors according to the conventional definition. This does not mean the other methods do not have an important role to play in securing services. Instead it indicates accepted models for understanding and qualifying authentication related services may need to adapt.

3 The importance of binding

A second aspect of authentication technologies is the binding of the "token" to the individual. In conventional authentication, binding is a discrete event that occurs at the time the token is issued to the subject (i.e. end-user), most likely as part of the registration and enrolment process. If at some point the token needs to be revoked, replaced or renewed these actions are performed in discrete defined events.

For behavioural or contextual authentication methods, however, binding is not a discrete event at a point in time. Instead behaviours need to be monitored and an understanding of the behavioural characteristic built up (or learnt). An individual's behaviour may also change over time, meaning that in many cases the binding becomes a continuous process.

The following table considers, for the methods in question, whether the binding to individuals is a discrete event or a continuous process:

Table 2: Is binding a discrete event or continuous process?

Method	**Binding?**
Risk based Authentication	Continuous
Knowledge Based Authentication	Discrete
Physiological Biometrics	Discrete
Behavioural Biometrics	Continuous
Location	Continuous
Device fingerprinting	Discrete

Whether binding is continuous or a discrete event should not affect the legitimacy of the method as an authentication factor. Instead it requires us to think in new ways about how to measure the quality of the binding process.

4 Authentication Requirements of Real Services

There are many different types of service that require some element of authentication. The authentication requirements of these varying services may be quite different. For example a logon service is usually concerned with ensuring that a known registered user, linked with an account on the system, is accessing the service. In contrast a digital signature verification service is usually concerned with ensuring that the digital signature is authentic and that sufficient evidence can be stored for non-repudiation purposes.

In this section, we characterise the authentication requirements of a range of example services where authentication is important. We will then examine whether or not the alternative authentication methods meet those requirements.

The following high level requirements are considered. They describe at a business level, four different aspects of authentication.

- **Positive**: Does the service require that the claimed identity is explicitly authenticated or can the service tolerate a level of ambiguity with respect to the identity?
- **Verifiable**: Does the service need to collect and record verifiable evidence for later use, for example, in the case of a dispute?
- **Continuous**: Does the service need to be sure that the user is authentic for a period of time (e.g. a session) or at a specific point in time (e.g. a transaction)?
- **Protected**: Does it matter if the authentication credentials are shared (or stolen) ordoes the service need to confirm that the specific authorised user is using the provided credential?

This list is not definitive, however the above requirements were chosen as they provide a sufficient range to demonstrate that the requirements of services differ and as a consequence not all authentication methods are relevant in all scenarios.

For each use case, the relevance of each of the above requirements is assessed as one of:

- "Y" meaning the requirement is applicable
- "N" meaning the requirement is not normally applicable
- "?" meaning the requirement may be applicable in some circumstances and not in others.

We thus identify whether certain authentication mechanisms, on the face of it, lend themselves to certain types of service.

4.1 Use Case: Enterprise Logon

The first use case we consider is Enterprise Logon. In this use case we are considering the access made by an employee to their employers' systems including VPN access, email and file servers. In these scenarios, specific known individuals (i.e. employees) with specific accounts are entitled to gain access to the system.

The following table asks whether the four high level requirements under consideration are applicable to this use case:

Table 3: Enterprise Logon Authentication Requirements

Criteria	Applicability?	Rationale
Positive	Y	Enterprises usually require their systems to be accessible only to known and defined employees and contractors. Specific access controls will be granted on the basis of these known identities.
Verifiable	N	Typically enterprise systems will keep audit logs of system usage. These are used for internal information security purposes. They will not typically contain verifiable (i.e. non-reputable) evidence.
Continuous	?	Currently no. It is a discrete event whose result is a secure session over which the employee can access services. The ability to authenticate the employee continuously is likely to be of interest to employers especially those who experience abuse of services as a result of an employee using another employee's account or workstation.
Protected	?	Currently no. Employee contracts and staff policies will be used to ensure employees report missing credentials and prevent sharing. Mechanisms to prevent abuse may be of interest to employees but these could introduce privacy issues if employees are monitored.

4.2 Use Case: Consumer Payments

This use case considers consumer payments such as using a credit card to pay for goods or services on an e-commerce site.

The following table asks whether the four high level requirements under consideration are applicable to this use case:

Table 4: Consumer Payments Authentication Requirements

Criteria	Applicability?	Rationale
Positive	?	Positive authentication of the customer is not always a requirement in consumer payments. The business requirement is often to ensure the legitimate customer can always pay and to reduce friction to the legitimate customer. This can mean that in some situations the customer may be identified (e.g. by entering a card number) but not authenticated (e.g. by entering a password). Often the consumer payments organisations will only introduce additional security when fraud is identified as a problem. There is a balance to be struck between convenience and security, which is determined by the payments organisations approach to risk.
Verifiable	?	The card schemes have well defined liability rules in place. These generally cause liability to flow to the weakest point in the transaction (e.g. if the merchant can, but chooses not to use a better authentication, then they will be liable). In some cases transactions may not be authenticated and so no evidence is stored for later verification.
Continuous	N	Consumer payments are transactional and therefore any authentication that is required will be performed at the point of the transaction.
Protected	Y	The use of systems to monitor transaction characteristics, in order to detect abuse, is widespread. This is tied very closely to the approach of "positive" authentication. As the aim is to make payments easy for legitimate customers, alternative measures are required to detect when problems occur.

4.3 Use Case: Contract Signing

This use case considers digitally signing a contract. Typically this will involve an authentication technology being used to bind the user, the contract, and the user's intent to agree with the contract.

The following table asks whether the four high level requirements under consideration are applicable to this use case:

Table 5: Contract Signing Authentication Requirements

Criteria	Applicability?	Rationale
Positive	Y	Contracts are signed by defined legal entities and hence it will usually be necessary to verify the legal identity of the counterparty.
Verifiable	Y	We do not address whether the use of a particular technology, and the evidence it generates, can be considered as legally binding according to current legislation. The requirement for verifiability is closely linked to the legal status of a digital signature. Instead, we are really asking, at a high level, does this authentication method generate evidence that has the potential to be recognised legally.
Continuous	N	Each contract signing will be a discrete event. After time if a contract needs to be renewed this will be another discrete event.
Protected	?	Due to the binding nature of legal agreements we would expect that individuals or organisations will be concerned to protect their identities from misuse. As with age verification below, there may be some circumstances where consumers (rightly or wrongly) would allow their identity to be shared, e.g. for agreeing terms and conditions relating to a retail service.

4.4 Use Case: Age Verification

This use case considers age verification, which could relate to the delivery of digital content or physical goods or other services. It may not be necessary to know the user's real legal identity (e.g. name and address) or even their date of birth. Instead the objective is to show that the user is in the appropriate age bracket for the service in question.

The following table asks whether the four high level requirements under consideration are applicable to this use case:

Table 6: Age Verification Authentication Requirements

Criteria	Applicability?	Rationale
Positive	Y	Services such as gambling and adult content may be legally required to positively ascertain that the user is of an appropriate age. Similarly it is likely to be highly desirable to positively determine that users accessing services targeted at children are indeed children.
Verifiable	?	Where age is verified anonymously, it will not be possible to verify after the fact that a particular individual was authenticated correctly. It is more likely that a service provider will need to provide evidence that they have appropriate controls in place and that they were active at a particular point in time.
Continuous	?	Some age restricted services such as streaming video is a continuous, as opposed to discrete, activity. Other services, e.g. purchasing alcohol, will be discrete single event activities. Therefore the requirement for continuous authentication will vary between services.
Protected	?	Anecdotally we would expect sharing of age verification credentials to be a common issue. For example, children may attempt to use the credentials of their parents. This would imply that there is a need for mechanisms to detect and prevent the misuse of such credentials. It is unclear however if such mechanisms are commonly used at present.

5 Characteristics of Authentication Technologies

In the following table we consider whether characteristics of the alternative authentication technologies in question address the potential high level business requirements of authentication services.

Table 7: Characteristics of Authentication Technologies

	Risk Based Authentication	Knowledge Based Authentication	Physiological Biometrics	Behavioural Biometrics	Location	Device Fingerprinting
Positive	N	Y	Y	N	N	Y
Verifiable	N	N	Y	N	N	N
Continuous	Y	N	N	Y	Y	Y
Protected	Y	N	N	Y	N	N

The above scoring represents our view on the general capabilities of these authentication methods.

In general, the contextual methods (risk, behavioural and location bases methods) can provide continuous authentication and can be used to detect abuse (due to unexpected context or behaviour).

Similarly the "asserted" methods (knowledge based, biometrics) provide positive authentication and in some cases evidence that would be difficult to deny in the event of a dispute.

Device fingerprinting is different in that it provides a positive assertion of the device (which could be linked to an individual) but can potentially be continuously and non-invasively interrogated during a session.

6 Which Technologies suit which services?

Having analysed which authentication requirements apply to which services and considered whether the characteristics of specific technologies address those requirements, the following table maps these topics together, i.e. which authentication technologies suit which services.

The scores in the following table should be interpreted as follows:

- Y, means every "Y" or "?" score in the corresponding Use Case table above has a corresponding "Y" in the technologies table (table 8), i.e. the technology meets or exceeds the requirements of service;
- N, means some "Y" or "?" scores in the corresponding Use Case table above have a corresponding "N" in the technologies table (table 8), i.e. the technology does not meet the requirements of the service;
- "?", means that neither a "Y" or "N" score could be given, i.e. the technology may in some circumstances meet the requirements of service but in others may not.

Table 8: Mapping of Authentication Technologies to Use Cases

	Risk Based Authentication	**Knowledge Based Authentication**	**Physiological Biometrics**	**Behavioural Biometrics**	**Location**	**Device Fingerprinting**
Enterprise Logon	N	?	?	N	N	N
Consumer Payment	?	N	N	?	N	?
Contract Signing	N	N	?	N	N	N
Age Verification	N	?	?	N	N	?

The table clearly shows that there is no exact match between the alternative authentication methods and the services considered. There are however a number of combinations where there may be a match depending on the characteristics of a specific implementation and the specific requirements of the services. There are other combinations where there appears to be a clear mismatch between technology and service.

The following specific observations are made:

- No alternative authentication method exactly meets the requirements of any one service. Therefore it is likely that multiple mechanisms will be required. This is consistent with a multiple factor approach to authentication. Instead of simply increasing authentication strength with multiple factors, however, it appears that the different characteristics of authentication methods are required to meet the needs of the solution.
- There may be services for which a purely risk based approach to authentication may be acceptable, at least in some circumstances (as per the "?" score for Consumer Payments). For example, a payments service may allow transactions that are in keeping with a customer's previously established purchasing behaviour without the need for additional authentication, to improve the consumer experience. We believe these services will be those where any losses sit with the service provider (as is often the case in payments) who will then be able to manage their own risk down to an acceptable level. If the consumer stands to incur a loss (which could be a non-financial loss, such as loss of reputation) then more implicit forms of authentication may be less appropriate. Further research is required to corroborate this hypothesis.
- There are some applications for which the majority of the alternative authentication methods we have considered do not appear to apply. Applications requiring non-repudiation of transactions, such as contract signing, require evidence to be generated that cannot be disputed. Apart from physiological biometrics, the alternative authentication methods do not generate indisputable evidence.
- Location does not appear to meet the requirements of any of the services examined. This arises because location only addresses one of the business requirements considered in this paper, namely "Continuous Authentication". This is however consistent with the view that location is not an authentication factor but potentially a very useful risk reduction method.

7 Conclusion

Developers of digital and mobile service have a wide range of authentication-related methods to choose from. Choosing the correct methods requires a clear understanding of the business requirements of the service in question. These requirements can vary widely between services. It is likely that business requirements will include ensuring that the service is easy to use, which will in all probability be in conflict with other requirements to add adequate levels of authentication. It is likely that many services will need to use multiple authentication methods to address the varying requirements of the service, as well as to increase the overall level of assurance. In these cases, it appears likely that a combination of conventional authentication factors supported by the alternative techniques considered here may be necessary.

References

[1] http://www.csoonline.com/article/716354/identity-is-the-new-perimeter

[2] http://www.chyp.com/media/blog-entry/hey-you-get-off-of-my-cloud

[3] http://www.gartner.com/newsroom/id/2070515

[4] http://www.guardian.co.uk/technology/2008/nov/13/internet-passwords

[5] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

Security Management

Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment

Claire Vishik[1] · Frederick Sheldon[2] · David Ott[1]

[1]Intel Corporation
{claire.vishik | david.e.ott}@intel.com

[2]Oak Ridge National Laboratory
sheldonft@ornl.gov

Abstract

Cybersecurity practice lags behind cyber technology achievements. Solutions designed to address many problems may and do exist but frequently cannot be broadly deployed due to economic constraints. Whereas security economics focuses on the cost/benefit analysis and supply/demand, we believe that more sophisticated theoretical approaches, such as economic modeling, rarely utilized, would derive greater societal benefits. Unfortunately, today technologists pursuing interesting and elegant solutions have little knowledge of the feasibility for broad deployment of their results and cannot anticipate the influences of other technologies, existing infrastructure, and technology evolution, nor bring the solutions lifecycle into the equation. Additionally, potentially viable solutions are not adopted because the risk perceptions by potential providers and users far outweighs the economic incentives to support introduction/adoption of new best practices and technologies that are not well enough defined. In some cases, there is no alignment with predominant and future business models as well as regulatory and policy requirements.

This paper provides an overview of the economics of security, reviewing work that helped to define economic models for the Internet economy from the 1990s. We bring forward examples of potential use of theoretical economics in defining metrics for emerging technology areas, positioning infrastructure investment, and building real-time response capability as part of software development. These diverse examples help us understand the gaps in current research. Filling these gaps will be instrumental for defining viable economic incentives, economic policies, regulations as well as early-stage technology development approaches, that can speed up commercialization and deployment of new technologies in cybersecurity.

1 Introduction

Applications of theoretical economics to the introduction of new security technologies already exist. Studies of asymmetric information in computing environments, models of monetary economics, economic models for liability, as well as exploration of the economic positioning of informational products in general could be helpful in evaluating available options and defining the nature of optimal economic incentives. These studies may also help to establish the metrics necessary to build a multidisciplinary scientific framework for examining prospective security technologies and design relevant economic incentives.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_12, © Springer Fachmedien Wiesbaden 2013

This paper examines the theoretical foundation of cybersecurity economics. We begin with a review of research in theoretical economics that emerged in response to the Internet economy, analyze gaps within current studies about cyber-economics and cybersecurity incentives, examine cases where deeper economic understanding could influence the development of new technologies both directly and via targeted economic incentives. We conclude that the absence of a solid theoretical foundation in the economics of security negatively impacts the work on more concrete problems. We expect that the theoretical examination of the foundations of security economics will permit industry and regulators to start a dialog toward developing new approaches to cybersecurity incentives. Progress in this area should allow technology developers to link those incentives to technology evolution and consequently speed up the emergence and adoption of their most valuable security protection features.

2 Current Studies In Cybersecurity Economics

In the 1990s, with the advent of Internet-based communications and electronic commerce, there was a burst in research toward modeling the economic attributes of the emerging field of electronic commerce. Theoretical foundations for the economics of electronic information [PRIE94] and optimal business models of such were studied. Starting from the mid-90s, various theoretical studies were also published on the economics of security and privacy (e.g. [ANDE01], [GORD02], [VARI95]), but today the focus remains less on theoretical and more on the general aspects of business [CaRa07], and the attitudes of users ([HeHe06], [GaGh05], [PoEB06]). These topics are important, but we suspect that research in cybersecurity would benefit if a theoretical foundation for the economics of security were more developed.

2.1 Exchange/Monetary Economies and Asymmetric Information

Let us examine in general terms how various types of economies operate. These ideas formed the foundation of the economic thought in the 90s, although many of them appeared more than a hundred years ago. Differences between monetary and exchange economies have been discussed of study for a long time. Among the factors affecting direct exchange of goods, *double coincidence of wants* can be seen as the core source of inefficiency in exchange markets. First described by Jevons in 1875 [JEVO20], *double coincidence of wants* explains that both agents involved in an exchange transaction without a recognizable currency need to engage in additional "search" activities. The agents have to locate another agent that not only has the desirable commodity, but also wants to exchange it for the commodity that the first agent can offer. These requirements increase the waiting periods before transactions can occur and make transactions less efficient.

Double coincidence of wants alone is not the only factor that limits the efficiency of exchange markets. In principle, we can create special markets where pairs of products or artifacts can be exchanged [BaMa96]. This method increases the number of markets and is costly, yet still possible. These unsophisticated approaches appear to have a strong influence on modern security technologies as each innovation is developed independently to resolve a singular well-defined issue. Current trust markets are therefore costly and inefficient and require greater efforts on the part of operators to establish trustworthiness.

Other inefficiency problems exist associated with exchange economies besides the "search effort." Some researchers, e.g., [BaMa96] believe that the main issue is asymmetric information, unequal knowledge of buyers and sellers about the value of artifacts offered in pure exchanges. Because of the lack of expertise and inability to recognize intrinsic and market value of artifacts within a market, agents consequently assume that there is a high risk associated with any transaction [AKER73]. The increased perception of risks can result in a situation that causes no transaction(s) to occur [AKER73]. Indeed, the asymmetric information problem can be a powerful inhibitor. These concerns are present in cybersecurity markets involving, e.g., threat information exchanges. The full value of this information can be determined only when an exchange has been completed and the value transferred [BaHa89, PRIE94].

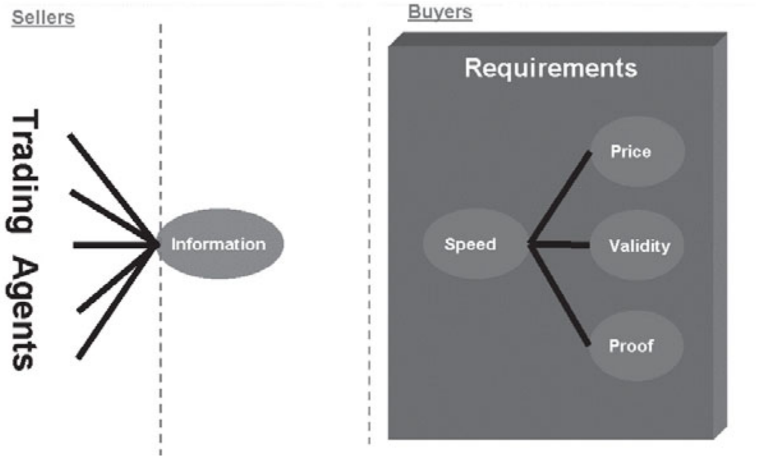


Fig. 1: Asymmetric Information and Market Requirements.

Intermediation is recognized as a model helping markets resolve the issue of asymmetric information. Marketing theory views intermediaries as "organizations that support exchanges between producers and consumers, increasing the efficiency of the exchange process by aggregating transactions to create economies of scale and scope" [WILL87]. A very important role of trusted intermediaries that is also crucial for security and trust markets is improving the quality in a market [WiWr94]. An important additional function, per [BoPi95], is to eliminate friction and therefore increase trust among market participants. Bhattacharya and Hagerty [BaHa89] see the role of intermediaries as regulators between the agents in a market, another function that is particularly important in security markets. The research points to mediated markets for security, with trusted third parties, and indicates that economic incentives need to be defined keeping this model in mind.

Development of the fundamental view on exchange, monetary, mediated, and aggregated markets helped to shape the first stage of the digital economy by developing practical business models, regulations and incentives. We expect that the same broad theoretical assessment will happen for cybersecurity economics leading to new models, tools, regulations and economically viable incentives. However, numerous gaps in cybersecurity economics remain. Some of them are listed below.

2.2 Gaps

Lacking broadly applicable economic models and frameworks: Moore [MOOR10], while acknowledging an increase in the study of security economics, contends that many issues arise simply because the economic models used today lack coherence and defending organizations don't bear the full cost of their failure . Moore claims that misaligned incentives slow down the introduction of new cybersecurity defenses. The recent convergence of infrastructures using varying security models and having diverse security requirements, while cost effective, place an additional burden on cybersecurity defenses. A framework is needed that can explain and predict the economic burdens as well as the (in)efficiencies in security. An example research question could be: what are the economic consequences of merging separate infrastructures (e.g., physical and cyber-physical infrastructures)?

Economic models for security and its concomitant verification infrastructure: Many of the technologies that could increase the safety of the computing environment today and improve the defenders‘ positioning in cybersecurity require significant infrastructure investment. Federated identities, cloud encryption, multi-tenant cloud environments and trusted computing are only a few examples of technologies that require a verification infrastructure to implement their vision in full. However, we do not have a comprehensive understanding of the economic positioning of such infrastructures, delaying meaningful deployment of many technologies.

Economic impact of adverse events: Modeling the impact of information security breaches or other adverse events is a more developed area than those listed above, but we still lack reliable answers from the existing models. Much of the risk analysis associated with security events continues to be ad hoc, and reliable models for estimating the cost of adverse security activity will improve the situation [TAFW13].

Understanding economic practice for designing viable economic incentives: Design of economic incentives that can be linked to existing and developing cybersecurity technologies remains an emerging topic. WEIS-2013 included a number of papers focusing on economic incentives, an encouraging sign of increasing interest. Wellam et. al. [WeKD13] observe that game-theoretical analysis of network security has been mostly represented by highly stylized models and proposes a simulation based approach to better understand the economics of compliance. Ashgari et. al. [AEAE13] offer an interesting perspective on improving SSL/TLS flaws in HTTPS protocol through the analysis of a potential market for such certificates. Based on their findings, they propose a combination of regulatory response and targeted economic incentives to modify HTTPS design.

Insufficient understanding of economic practice to design cybersecurity economic policies and regulations. With the theory of cybersecurity economic incentives still immature, theoretical work on cybersecurity policies and regulatory frameworks remain weak. For example, liability has been the most common tool considered as the primary economic lever of cybersecurity regulations. However, researchers have consistently pointed to the limitations of this approach. For example, [HuMC13] concludes that, on the whole, the cost of implementing liability as an economic incentive outweighs the potential benefits from this approach.

2.3 Research that could fill the gaps in cyber-economics

Based on the analysis of literature in economics, technologies, and policy studies, it is clear that, while there is significant interest in security economics as well as the economic incentives for cybersecurity, the field has not experienced the same level of activity as the research in Internet markets. Fifteen years ago, increased understanding of the unique nature of the Internet economy led to seminal theoretical studies that helped define predominant market models for the digital economy and link them to specific business models and thereby enabling/stimulating concomitant technology deployment. These technologies and usage models affected every aspect of everyday life.

The study of security economics, in contrast, has focused on narrower problems or moved directly to frameworks for economic policy and regulations, without establishing reliable theoretical foundations of the economics of security that could lead, among other benefits, to the design of better economic incentives.

To move the field forward, several activities can be proposed:

1. Continue to build the theory of the cybersecurity market, as a foundation for multi-disciplinary work in adjacent areas.
2. Link the theoretical foundations of cybersecurity economics with concrete technologies tailored toward introducing tools to analyze the economic viability of new approaches early in the development cycle.
3. Collect information and examples from technology development case studies to gain better insight into the connection between technologies and economics.
4. Use both theoretical foundations and practical examples of cybersecurity markets to define economic incentives that will have the greatest and most focused impact.
5. Use both theoretical and empirical knowledge acquired from item 4 above to help define regulatory approaches to cyber-economic incentives.

3 Defender-Practitioner point of view

The sections below focus on linking economic incentives to practical technology development tasks.

3.1 Defender-Practitioner Stakeholder View

There are many influencing economic factors to weigh from the defender-practitioner stakeholder point-of-view that involve cost combined with development/deployment models. Some examples include the cost of countermeasures themselves, the cost of training and the cost of maintenance. Meanwhile we must better anticipate the total cost from a compromise. The return on investment in countermeasures is essentially impact costs (i.e., the costs from violating confidentiality/privacy, integrity and availability requirements). The natural question arises about choosing the main risks that must be monitored in deciding on security investments. To answer this question, we must investigate the cost/benefits to the attacker/defender to better estimate the likelihood that a threat will emerge and whether it will be thwarted. This assessment can provide key information for building theoretical economic models for cybersecurity.

3.1.1 Measuring Security

A research community has emerged around economic approaches (embodied by the annual Economics of Information Security workshops or WEIS). Metrics based on the expected cost required to compromise a system can help guide system designers. However, for most computing systems, these metrics' parameters are somewhat arbitrary [StBE11]. Limited foundational understanding of the economic factors playing into these situations causes this subjectivity.

An example economic metric is cost-based IDS (Intrusion Detection System). IDSs have become critical in securing computer system infrastructures. IDS developers strive to maximize the detection accuracy and bandwidth of deployed systems in realistic environments. The goal is to develop efficient detectors with high true-positive rates while minimizing false-negative and false-positive rates.

Toward this goal, researchers have defined cost-based detection metrics for IDSs. For each network event determined to be an attack, this approach estimates a response cost and a damage cost on the basis of factors such as the criticality of the targeted system component. If the damage cost is greater than the response cost, the system might initiate a response. These metrics in total define a cost-based metric for system defense that's closely related to "stop loss" metrics employed in fraud and risk management systems for financial-transaction systems. These metrics can be used to parameterize more general economic models.

3.1.2 Risk Assessment Methodology

Complex systems (e.g., e-government, cyber physical systems) configured to deliver service or otherwise interact with a variety of parties or stakeholders are typically designed to balance functional and non-functional requirements. Stakeholders of such systems demand maximum reliability and security. We have developed an approach that allows analysts to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns, the so-called mean failure cost (MFC) [ShAM09, AASM10]. The stakeholder mission, in the context of our approach, is defined by the set of system requirements that must be satisfied [AbSG10]. Moreover, MFC comprehends security requirements, stakeholder's stakes, system architecture (i.e., set of components that support those requirements/stakes), and threat emergence probabilities.

Mission assurance is a full life-cycle engineering process that is an essential element of risk assessment [HeSP04]. Public and private operations do not differ significantly in their mission assurance needs; we all need cyber information operations that are reliable, available, survivable, and secure [Whit09, Rhod10]. We borrow from the methods used in securing organizations to improve our ability to provide accurate and timely assessments [YaGr08, GrFS09]. Organizations use a risk assessment and management process to identify and mitigate risks to assure their organizational mission(s) [Pipk00]. Risk management provides a structured and transparent process to identify critical resources, and to estimate threats and vulnerabilities that may intersect to cause harm or increase the likelihood of undesirable events. Moreover, the process estimates the likelihood of security violations and evaluates tradeoffs among control measures used to mitigate the risks, and periodically revisits the analyses as needed. However, the quality of the analysis is strongly dependent on the accuracy of the inputs to the process.

In earlier studies, we have described models of critical cyber physical infrastructure that allow an analyst to estimate the security of a system in terms of the impact of loss per stakeholder resulting from security breakdowns. In the recent times, we have considered more the methodology associated with how to identify, monitor and estimate risk probability and impact within the energy sector (i.e., different smart grid stakeholders). Our constructive method leverages currently available standards and defined failure scenarios. We've applied the Cyberspace Security Econometrics System (CSES, a cascade of linear models including stakes, dependency and impact matrices) within the five-step NIST CSWG (Cyber Security Working Group) methodology to estimate the MFC / day for a utility, AMI (automated metering infrastructure) vendor, CKMS (cryptographic key management system) provider and including corporate and residential customers. Such estimates are useful for gaining insights into trading-off the many issues associated with comparing design choices and/or courses of action with respect to mitigations as well as in making designed-in-security related decisions. The CSWG methodology employs the following steps: 1) selection of use cases with cyber security considerations; 2) Performance of a risk assessment; 3) Setting boundaries – the beginnings of a security architecture; 4) High-level security requirements; and 5) Conformity testing and certification [ASH+13].

3.1.3 Economic Impact of AMI Failure Scenarios

Information security (IS) continues to evolve in response to disruptive changes with a persistent focus on information-centric controls. A healthy debate is needed to address balancing endpoint and network protection, with a goal of improved enterprise / business risk management. IS analysis can be performed using game theory implemented as dynamic simulations of Agent-Based Models (ABMs). Such simulations can be verified against the results from game theory analysis and further used to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets. We've concentrated our analysis on the automated metering infrastructure (AMI) domain of which the National Electric Sector Cyber security Organization Resource (NESCOR) working group has currently documented 29 failure scenarios. The strategy for the game was developed by selecting/analyzing five representative failure scenarios of the twenty-nine. We classified each of the five into one or more of three specific threats that may affect the confidentiality, integrity or availability of the system. The preliminary analysis using our ABM game theoretic simulation (publication of the results is pending) demonstrated that the AMI functional domain was simply and accurately modeled, the game theoretic rules were decomposed and analyzed as to their respective impacts (confidentiality, integrity, and availability) on the AMI network.

3.1.4 Attacker-Defender Agent Based Simulations (AD-ABS)

A few groups of researchers have recently advocated game theoretic approaches to making designed-in-security decisions [RSD+10]. Game theory provides mathematical tools and models for investigating multi-player strategic decision-making. Another technique that is promising is the application of simulations [Gint09]. Lye and Wing [LyWi05], presented a game theoretic method for analyzing the security of computer networks modeling attacker-defender interactions as a two-player stochastic game for which best-response strategies (Nash Equilibriums) were computed. Mahimkar and Shmatikov [MaSh05] proposed a new protocol for preventing malicious bandwidth consumption and demonstrated how game-based formal methods can be successfully used to verify availability-related security properties of network protocols. Liu et al. [LiZY05] presented a general incentive-based method to model attacker intent, objectives, and strategies (AIOS) and a game theoretic approach to infer AIOS. They invented an AIOS formalization to capture the inherent interdependency between AIOS and defender's objectives and strategies in such a way that AIOS can be "automatically" inferred. Schlicher [ShAb12] expanded on these studies by presenting a generalized computational game theoretic simulation engine using ABMs. In the simulation, where the active components of the model, referred to as agents, engage in interactions on a scenario-by-scenario basis.

ABMs have been used to simulate evolutionary game theory involving multiple players in both cooperative and competitive or adversarial postures [Bona02, Nowa07]. ABMs bring significant benefits when: (1) interactions between the agents are complex, nonlinear, discontinuous or discrete; (2) space is crucial and the agents' positions are not fixed; (3) the population is heterogeneous; (4) the topology of the interactions are complex; or (5) the agents exhibit complex behavior, including learning and adaptation [Bona02, Nowa07]. The agents in the simulation include the attacker and the defender or administrator. The agents perform actions that can change the state of the enterprise system. For each state, agents are limited in the actions they can perform. Depending on the scenario, the attacker executes one of many actions with an associated probability of deciding to do the action and a probability that the action will be successful once the decision has been committed. Within each time unit, the simulator thread visits each agent giving them the opportunity to perform an action or not [ShAb12].

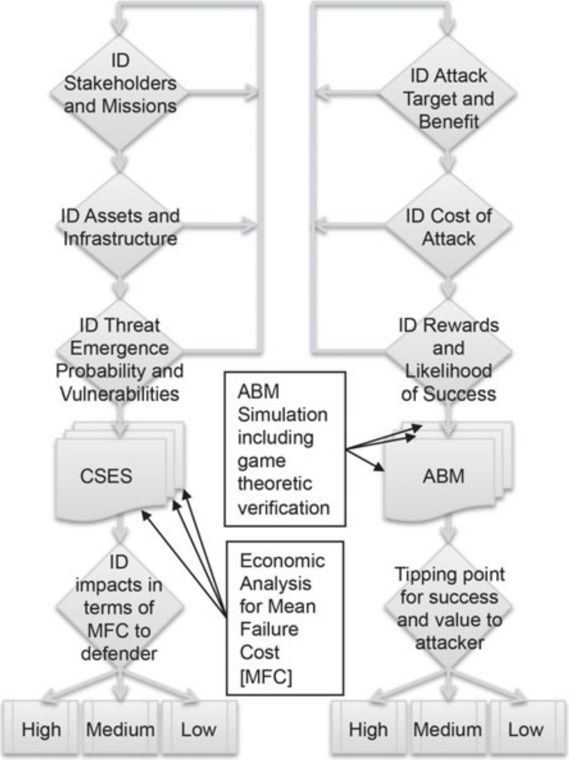

ID Stakeholders and Missions
ID Assets and Infrastructure
ID Threat Emergence Probability and Vulnerabilities
CSES
ID impacts in terms of MFC to defender
High
Medium
Low
ID Attack Target and Benefit
ID Cost of Attack
ID Rewards and Likelihood of Success
ABM
Tipping point for success and value to attacker
High
Medium
Low
ABM Simulation including game theoretic verification
Economic Analysis for Mean Failure Cost [MFC]

Fig. 2: Linking ABM-Sim with economic impacts.

3.1.5 Correlating AD-ABS with an Economic Impact Assessment

When considering the cost of mitigations as they address either some of the most pernicious or the most likely of threats we need quantitative indications of reliability, performance, and/or safety/security (aka resiliency). The CSES approach accounts for (i.e., by deriving MFC) the criticality of each requirement as a function of one or more stakeholders' interest in that requirement, the underlying infrastructure (component-by-component) and an estimate of the likelihood of threats (combined with an existing vulnerability) emerging. By using the AD-ABS approach (Fig 2) we hope to establish a methology for discovering insights through sensitivity analysis (perhaps as an approximation of the vertex cover problem) the set of paths of least resistance to disrupting/failing a mission requirement. In this way, we can have higher confidence and precision for estimates of threat emergence probability. Then, combined with the results from CSES, we plan to develop a comprehensive bottom line basis for asset owners to decide in what and how much to invest, choosing courses of action that reduce the most risks for the lowest cost.

3.1.6 Increasing Reliance on Advanced Technology

Increasing reliance on smart grid advanced technology capabilities and the worsening threat environment mean that asset owners are under pressure to invest more in information/cyber security.

A challenge is that the choices are hard: money is tight, objectives are not clear, and there are many relevant experts and stakeholders. A significant proportion of the research in security economics is about helping people and organizations make better security investment and policy decisions. Yet there is no clear guidance or method that helps those asset owners understand the cost of implementing security mitigations (i.e., pricing), nor a clear basis for return on investment (ROI). One question that is coming up more and more is the impact of methods (using economic/cost models) that are based on Cost/ROI/MFC (mean failure cost) in helping decision makers choose from alternative courses of action and investments.

The opportunity: The smart grid (energy delivery system) provides a basis for looking at a realistic security problem and it's associated (information/cyber and physicial) infrastructure toward encompassing the broad range of different factions included as justifications for the decisions that such stakeholders must make. The security professional is an important and influential stakeholder in the organization's decision-making process and arguably has a more complete understanding of the problem. They also may be more suitable for persuading a broader business audience in regards to hardening the critical infrastructure and potentially avoiding costly calamities.

The theoretical foundation: Cases similar to the one presented above can feed important information for adjusting assumptions and techniques in theoretical models evaluating more general economic mechanisms. These mechanisms, in turn, can be applied to improve and validate metrics and risk analysis for concrete situations.

4 Preparing Infrastructure to Implement Reasonable Economic Incentives

The scale of economic loss from attacks on cyber infrastructure is often proportional to the time lag between appearance and remediation. It is also related to the verification mechanisms that can be enabled in single or multiple domains. Organizations with significant vulnerabilities and weak detection mechanisms can incur substantial losses when a successful attack makes its appearance and then goes unnoticed or un-remediated for a significant period of time. For example, a substantial time lag may give an attacker opportunity to gather extensive business data, to discover the right archive for intellectual property, or to execute elaborate system disruption schemes tailored to infrastructure characteristics and operation. Vulnerabilities can also be exacerbated when components of the mission-critical and remediation systems cannot be verified.

In this section, we consider trust infrastructures and the role of software instrumentation as case studies in the dynamics of economic incentives for cybersecurity. A discussion of "weak" and "strong" models is intended to bring out the broader theme that research is needed on frameworks for making security instrumentation more visible and measurable. With this, infrastructure providers are given economic incentives that can advance the state of cybersecurity.

4.1 Trust Infrastructure and economics of cybersecurity

Security infrastructure is needed to support the ability of users, devices, and systems to be reliably authenticated and their capabilities established and verified in single or multiple domains. This infrastructure is also necessary to ensure that elements of transactions can be reliably verified in order to be trusted. Infrastructure of this type, including CAs (Certificate Authorities), directories, identity management systems, policy management/enforcement frameworks, and other elements, is necessary to carry out many functions.

Trust infrastructure can be presented as a market, with credentials representing products or currency, depending on the model, and agents involved in transactions exchanging these credentials for the right to use or access systems. Parallels with economic models of exchange, monetary, and intermediated markets can be striking and, potentially, similar models appear as likely solutions. However, these similarities can be misleading.

Using market approaches to study trust infrastructures is helpful in analysis, but new modeling techniques need to be developed. An interesting avenue for research is to examine the connections between economics of technology and specific technology features, in addition to defining working business models for technologies that require a significant infrastructure component. Once this connection is established, it may be possible to create incentives designed to encourage the development of deployable new technologies in cybersecurity.

4.1.1 Detecting and Integrating New Business Models

New business models usually emerge from practice. Occasionally, new business models are theoretically developed and then successfully introduced into markets. Vickery auctions, currently used in spectrum managements, are an example of such top-down introductions.

There is abundant literature on the changes in the modern process of innovation. Many papers and reports, from the 1990s or more recent, allude to this paradigm shift ([DRUC94], [Arth96]). However, even the general trends in the emergence of the new models for the Internet-influenced environment continue to be elusive [MORO02]. There is evidence that "disintermediation" and direct transactions among agents are growing in importance [ANTH06], but there is also ample proof that the trend towards intermediation and aggregation continues to dominate [KlAl05]. Although the big picture may not appear consistent, seemingly opposing trends are not necessarily at variance with one another; they can be complementary.

Building infrastructures requires considerable investment, risk mitigation mechanisms, and economic incentives to enable the new markets. In addition, non-technical requirements for such infrastructures, including support for privacy features and compliance with legal and regulatory frameworks, make theoretical work in the area especially important. As many frameworks (e.g. Trusted Computing) rely on infrastructure to implement their full potential, viable operational models become crucial in developing technologies ready for deployment, and useful economic models can help predict the best operational approaches.

We now move to a different example: code instrumentation for faster response to potential security issues. This case calls for a different economic model, one that incentivizes high-risk/high reward technology development efforts, but doesn't necessarily require significant infrastructure.

4.2 Code Instrumentation and Economic Incentives

Strategies for reducing the time lag between a successful attack and detection can take many forms. Here we consider an approach we call *code instrumentation*. In its weakest form, code instrumentation might consist simply of software development practices that help to reduce the potential for successful attacks. Some examples might be reducing the length of security critical code sections, checking function return values, using restrictive data types, adding bounds and other types of sanity checks, and overwriting buffer contents before releasing memory. Such practices require programmer awareness of the issues, discipline in coding practices, and often peer review to identify oversights and weaknesses.

While such practices would seem universally desirable, *economic incentives* often and perhaps surprisingly prevent them from being realized. Software vendors may be well aware of best practices for robust security and, to some degree, ask their developers to observe such practices. But, fully instrumented code requires investment in terms of programmer time and resource expertise. Such investment may be a challenge to justify for a variety of reasons that we outline briefly here.

First, one might expect the loss of reputation to motivate secure code instrumentation practices, especially in the context of software licensing where customers retain the option of canceling software services in an ongoing manner. In fact, this may be the case, but only to a point. Even well-regarded software vendors regularly develop patches in response to newly discovered attack vectors. They are, in a sense, expected. A software vendor may thus choose to release software before it has been fully instrumented, or without any intention of fully instrumenting it. Instrumentation may not be worth the investment, given a world that can accept the need for ongoing remediation as vulnerabilities are discovered. However, a *convincing* argument that the impact of compromise could be catastrophically costly may be a very important rationale in creating/discovering economic incentives (e.g., a disruption of electricity has been shown to cost billions of dollars in the case of the Northeast Blackout of 2003[1]).

Equally as challenging is the problem of messaging code instrumentation for customer sell-up. Suppose the software vender decides to invest in robust code instrumentation. The investment must necessarily be reflected in the price of the software, which must cover all expenses incurred by development. But customers may not be willing to accept the price when compared to other competitive offerings in the marketplace. All vendors claim their products have been designed with security in mind, and a customer has no way to observe or judge the underlying source code

[1] https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

in a meaningful way. Without a way to monetize the code instrumentation investment, again software vendors may find it hard to justify the expense.

The creation of standards is often cited as a means to promote good security practices and to message the investment to software customers. With standards, a software vendor can invest in secure code instrumentation practices and then make the claim that their software complies with a recognizable standard and therefore should be valued accordingly. While perhaps true, there are additional dynamics that come into play. A software vendor who complies with the standard has little incentive to invest in code instrumentation practices not explicitly required by the standard. In a sense, the same problem of economic incentives is revisited: without a meaningful way to message further investment to customers, the expense is difficult to justify. Furthermore, standards may discourage additional innovation in code instrumentation by causing customers to focus only on compliance as a cure-all solution. If the software product is in compliance, then all other considerations are superfluous. Highly original solutions or solutions that reach beyond the current state of the art (as defined by the standard) may be eclipsed.

4.3 The Case for Research on Code Instrumentation Frameworks

While defining economic incentives surrounding code instrumentation would appear difficult, we believe there is much to be learned about better approaches to cybersecurity. A key insight here is the need for frameworks that make security features and mechanisms both *visible* and *measurable*. Without visibility, customers cannot identify a feature as a viable option for additional investment. Without measurability, software venders cannot make claims that differentiate the quality and effectiveness of their approach within a competitive marketplace. As a result, there is thin or no justification for investing in better approaches for security.

Applied to code instrumentation, the key underlying problem in the weak model described above is the software vendor's inability to translate coding practices to a visible feature or measurable result with tangible value to their customer. The absence of successful attacks, of course, may be valued, but only to a point since the customer cannot determine which underlying features were really significant or whether a less pricey competitor could have provided the same service for less.

The solution implied by this analysis is what we refer to as the *strong model* of code instrumentation. In this model, code instrumentation includes various "hooks" and "code structures" designed to interact with an external agent to monitor secure software operation. The specific code paradigms are an open question to be addressed by the security research community. One might, for example, generate events that monitor control flow, memory address usage, data structure integrity, subsystem interaction, communication exchanges, I/O activity, code logic within critical sections, and so on. Instrumentation could be highly application-specific, focusing on the sensitive components of the software product or service, and generating information tailored to key concerns for the nature of the usage context.

The nature and functionality of the observing agent, likewise, is an open question for the security research community. Components of the agent could be implemented in hardware or software, and a trusted framework is assumed. The function of the agent is to process software events and data provided by the executing software. The agent then uses the information to monitor software operation in a manner that both visible and measurable. Again, the focus and metrics involved might be application-specific in nature, reflecting specific portions of the software architecture that are sensitive or critical from a security standpoint.

Experiences from empowering early technology development through economic analysis evaluating available paths are enlightening. Choices to be made at these defining stages can be analyzed for their cost and economic impact, to ensure that optimal decisions are taken. Applicability to a certain class of economic models could be examined early, if the theoretical foundation could be devised to deal with this class of problems.

5 Conclusions and Next Steps

We began this paper with a discussion of approaches to devising economic incentives for the development of new cybersecurity technologies and operational models as well as obstacles to effective development of such incentives. After examining many achievements in the field of cyber-economics and some of the gaps in the current work, we are forced to conclude that, at this time, we still lack theoretical foundation in economic assessment of cybersecurity techniques.

Although illuminating research has been performed in the area of incentives, especially research focusing on liabilities, in the absence of the strong theoretical foundation for cybersecurity economics, these efforts can provide mere examples of what is possible; they lack a broader analysis of benefits and negative consequences of using these approaches to incentives. Some research has shown that focus on liability is misplaced, and other avenues to designing viable incentives need to be explored.

Thus, we believe that work on a broad theoretical economic framework for cybersecurity should come first, similar to the explosion of research in the 1990s that defined the Internet economy. From this theoretical foundation, economic incentives theory will emerge.

At the same time, we continue to believe that study of economic elements of new technologies, new deployment techniques, new risk metrics, rigorous/systematic accounting for the cost of impacts of security breakdowns and new infrastructures will enrich the emerging economic theory in this area. This paper offers a few examples of such studies. Such efforts will remain necessary to guide and apply emerging theoretical research.

Acknowledgement

This manuscript has been authored by UT-Battelle, a contractor of the U.S. Government (USG) under Department of Energy (DOE) Contract DE-AC05-00OR22725. The USG retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for USG purposes.

References

[AEAE13] Asghari, Hadi, et al. "Security Economics in the HTTPS Value Chain." Available at SSRN 2277806 (2013).

[Aker73] Akerlof, G. A. "The Market for "Lemons": Quality Uncertainty and The Market Mechanism," Quarterly Journal of Economics, 1973, 488-500.

[Ande01] Anderson, R., "Why Information Security is Hard-An Economic Perspective," In Proc. 17th Annual Computer Security Applications Conference (Dec. 10 – 14, 2001), IEEE CS, Wash. DC, 358.

[Arth96] Arthur, W. B. "Increasing Returns and the New World of Business." Harvard Business Review, July-Aug. 1996, 74(4), pp. 100-109.

[BaMa96] Bannerjee, A. and Maskin, E., "Fiat Money in the Kitoyaka-Wright Model," Quarterly Journal of Economics, 111 (4) 1996, p. 9551005.

[BaHa89] Bhattacharya, S. & Hagerty, K. Dealerships, training externalities, and general equilibrium. In Prescott, E.C.and Wallace, N. (eds.). Contractual Arrangements for Intertemporal Trade. Minnesota Series in Macroeconomics, Minneapolis: University of Minnesota Press, 1989.

[BoJe08] Bojanc, R. and Jerman-Blaič, B., "Towards a standard approach for quantifying an ICT security investment," Comput. Stand. Interfaces 30, 4 (May. 2008), 216-222.

[BoPi95] Bose, G. and Pingle, M. Stores. Economic Theory, 6 (1995), p. 251-262.

[CaRa07] Cavusoglu, H., and Raghunathan, S., "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," IEEE TSE, 33:3 (Mar. '07), 171-185.

[CAVU07] Cavusoglu, H., and Raghunathan, S. 2007. Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. IEEE Trans. Softw. Eng. 33, 3 (Mar. 2007), 171-185.

[Druc94] Drucker, P.F. The Theory of Business. Harvard Business Review, September/October 1994, pp. 95-104.

[GaGh05] Gal-Or, E. and Ghose, A. 2005. The Economic Incentives for Sharing Security Information. Info. Sys. Research 16, 2 (Jun. 2005), 186-208.

[HeHe06] Herrmann, P. and Herrmann, G. 2006. Security requirement analysis of business processes. Electronic Commerce Research 6, 3-4 (Oct. 2006), 305-335

[Jevo20] Jevons, W.S., "Money and the mechanism of exchange," New York:D. Appleton, 1920.

[KlAl05] Klos, T. B. and Alkemade, F. 2005. Trusted intermediating agents in electronic trade networks. In Proceedings of the Fourth international Joint Conference on Autonomobus Agents and Multiagent Systems (The Netherlands, July 25 – 29, 2005). AAMAS '05. ACM, New York, NY, 1249-1250

[MeDM07] Merwe, J.V.D., Dawoud, D, and McDonald, S, "A survey on peer-to-peer key management for mobile ad hoc networks," ACM Comp. Surveys, 39:1, 2007.

[MOOR10] Moore, T., "Introducing the Economics of Cybersecurity: Principles and Policy Options." Proc. Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, 2010.

[PoEB06] Poindexter, J. C., Earp, J. B., and Baumer, D. L., "An experimental economics approach toward quantifying online privacy choices," Information Systems Frontiers 8, 5 (Dec. 2006), 363-374.

[Prie94] Priest, W. C. An information framework for the planning and design of the information highways. Center for Information, Technology, and Society, February, 1994.

[TAFW13] Thomas, R.C., et al. "How Bad Is It?–A Branching Activity Model to Estimate the Impact of Information Security Breaches," WEIS 2013.

[Vari95] Varian, H. R., "Economic Mechanism Design for Computerized Agents," In The First Usenix Workshop on Electronic Commerce, New York: Usenix Assoc., 1995, p. 13-21.

[Will87] Williamson, S. D., "Recent developments in modeling financial intermediation," Federal Reserve Bank of Minneapolis, Quarterly Review, 11, Summer (1987), 19-29.

[WiWr94] Williamson, S. and Wright, R., "Barter and Monetary Exchange under Private Information," The American Economic Review, March (1994), p. 101-123.

[WeKD13] Wellman, Michael P., Tae Hyung Kim, and Quang Duong. "Analyzing Incentives for Protocol Compliance in Complex Domains: A Case Study of Introduction-Based Routing." arXiv preprint arXiv:1306.0388 (2013).

[StBE11] Stolfo, S., Bellovin, S. M. and Evans, D., "Measuring Security," IEEE Security & Privacy, pp. 60-65, May/June 2011.

[ShAM09] Sheldon, F. T., Abercrombie, R. K. and Mili A., "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," in Proceedings of 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, 2009, pp. 1-10.

[AASM10] Aissa, A. B., Abercrombie, R. K., Sheldon, F. T. and Mili, A., "Quantifying Security Threats And Their Potential Impacts: A Case Study," Innovations in Systems and Software Engineering, vol. 6, pp. 269-281, 2010.

[AbSG10] Abercrombie, R. K., Sheldon, F. T. and Grimaila, M. R., "A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance," in IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, Mpls, MN, 2010, pp. 1153-1158.

[HeSP04] Hefner, R., Silva, H., and Patrican, R., "Mission Assurance and Capability Maturity Model Integration (CMMI)," presented CMMI Tech. Conf. & User Grp. Meeting, 2004.

[Whit09] "Cyberspace Policy RevIew – Assuring a Trusted and Resilient Information and Communications Infrastructure," ed: The White House, 2009, p. 76.

[Rhod10] Rhodes, K., Cybersecurity Must start with Mission Assurance. Washington Technology. Available: http://washingtontechnology.com/Articles/2010/01/13/Predict-globally-protect-locally.aspx-?s=wtdaily_190110&Page=1, 2010.

[YaGr08] Yates, H. and Grimaila, M. R., "A Systematic Approach to Securing our Space Assets," High Frontier Journal, vol. 4, pp. 48-53, 2008.

[GrFS09] Grimaila, M. R., Fortson, L. W. and Sutton, J. L., "Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process," Proc. of 2009 Int'l Conf. on Security and Management (SAM09), Las Vegas, NV, 2009, pp. 386-391.

[Pipk00] Pipkin, D. L., Information Security Protecting the Global Enterprise: Hewlett-Packard Company, 2000.

[ASH+13] Abercrombie, R. K., Sheldon, F. T., Hauser, K. R., Lantz, M. W., and Mili, A., "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," in 2013 46th Hawaii Int'l Conf. on System Sciences (HICSS), Wailea, Maui, HI USA, 2013, pp. 1802-1811

[RSD+10] Roy, S., Ellis, Shiva, C., S., Dasgupta, D., Shandilya, V., and Wu, Q. S., "A Survey of Game Theory as Applied to Network Security," in 43rd Hawaii International Conference on Systems Sciences Vols 1-5, ed, 2010, pp. 880-889.

[Gint09] Gintis, H., Thee Bounds of Reason: Game Theory and the Unification of the Behavioral Sciences: Princeton University Press, 2009.

[GORD02] Gordon, L. A. and Loeb, M. P. 2002. The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5, 4 (Nov. 2002), 438-457.

[LyWi05] Lye, K. and Wing, J. M., "Game strategies in network security," International Journal of Information Security, vol. 4, pp. 71-86, 2005.

[MaSh05] Mahimkar, A. and Shmatikov, V., "Game-based analysis of denial-of-service prevention protocols," in Computer Security Foundations, 2005. CSFW-18 2005. 18th IEEE Workshop, 2005, pp. 287-301.

[LiZY05] Liu, P., Zang, W. and Yu, M., "Incentive-based modeling and inference of attacker intent, objectives, and strategies," ACM Trans. Inf. Syst. Secur., vol. 8, pp. 78-118, 2005.

[ShAb12] Schlicher, B. G. and Abercrombie, R. K., "Information Security Analysis Using Game Theory and Simulation," in WORLDCOMP'12 – The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing; SAM'12 – 2012 International Conference on Security and Management, Las Vegas, NV, 2012, pp. 540-546.

[Bona02] Bonabeau, E., "Agent-Based Modeling: Methods and Techniques for Simulating Human Systems," Proc. of Nat. Academy of Sciences, 99:3, pp. 7280-7287, 2002.

[Nowa07] Nowak, A., "On Stochastic Games in Economics," Mathematical Methods of Operations Research, vol. 66, pp. 513-530, 2007.

Executive Career Paths in Information Security Management

Peter Berlich

Lucerne University of Applied Sciences and Arts
PO Box 2940, 6002 Luzern, Switzerland
peter.berlich@hslu.ch

Abstract

The Chief Information Security Officer (CISO) is facing particular career challenges, being rooted in a quickly changing field where managerial tasks are applied to a highly specialized technical foundation. The objective of this study is to explore individuals' careers that led them to aspire to and achieve the role.

22 current and former CISOs have been interviewed for this project. One can identify four segments of career patterns, based upon a broad classification into a preference for problem solving or organization building. Orthogonally, one can identify the orientation of the individual's Psychological Contract towards the employing organization and its representatives, or towards the professional community at large.

Many respondents displayed signs of protean career management in their career history and in the description of their plans going forward. While individuals may not always consciously realize it the need to manage their own career is prominently ingrained in their career philosophy and aspiration. Shared concerns were a requirement for active career management and potentially career limiting decisions.

This study provides a reference framework for security management careers, based on established structural and psychological concepts from the field of career research. Statistically representative analysis and longitudinal studies can be based upon this framework but are not attempted here.

1 Introduction

1.1 The Role of the Chief Information Security Officer

The Chief Information Security Officer (CISO) governs Information Security within a corporation. The CISO is facing particular career challenges, being rooted in a quickly changing field where managerial tasks are applied to a highly specialized technical foundation.

The perception of the CISO role is conflicted, in that it is seen as strategically important for the success of the same company and simultaneously as an operational inhibitor and a safeguard for tactical issues. The CISO role profile is dichotomous and ambiguous when it comes to balancing technical and managerial focus, and it requires a degree of skill and experience in both.

CISO appointments are occasionally made in an ad-hoc manner and similarly CISOs may not see themselves valued by the corporation. Owing to a dynamically expanding job market, the demographics of the Information Security field is sketchy. Progression from technical to management roles is still common.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_13, © Springer Fachmedien Wiesbaden 2013

The objective of this study is to explore individuals' careers that led them to aspire to and achieve the role.

1.2 Research Objective

From the diversity described above, as well as its general absence in the available literature, one can conclude that no clearly defined career path into a CISO role appears to have emerged so far. Externally, the role is shaped by the professional dynamics of an emerging role and career path and the emerging norms of a professional community, the internal dynamics of the business. However, it will be the perspective of the individual, not that of the hiring organization that will be central to this study.

If a common career path has not yet emerged then what has taken its place, i.e. how does an individual aspiring to the role of CISO accomplish this goal? Even in the absence of self-directed aspiration, at least the question must be asked as to what were the reasons for being selected for, and accepting the role. Conversely, being assigned the title of CISO will influence the individual's perception of the role, and the role will shape the individual. In other words, the question implies a way of personal development.

2 Career Concepts

2.1 Career Motivation and Career Choice

A number of models have been proposed to explain career preferences. Taking into consideration only models allowing for a level of empirical verification [OsFi96], notable examples are Holland's theory of occupational choice [Holl97] and Schein's Career Anchors model, e.g. [Sche96]. The latter has been widely applied and is based upon a number of indicators relating to tangible, externally observable behaviors. This allows testing motivation without having to rely on interpretation of responses.

[Sche93] initially postulated a set of five exclusive and stable "Career Anchors", internalized goals describing an individual's career motivators. Indicators can be loosely classified by how individuals choose to grow, how they see reward and recognition, and their expectations regarding their work. The Career Anchors model is phenomenological and provides no justification as to why the "anchors" would be a suitable (e.g. relevant, comprehensive and non-overlapping) description of career motivations. Nor does Schein attempt to force the "anchors" into a formalistic pattern, as could be said of [Holl97]. The Career Anchors model has been criticized based on the strength of its empirical foundation but has found experimental validation. [StFr07] A phenomenological approach matches the scope and objectives of this study, as it permits a pragmatic description.

2.2 Psychological Contract

The Psychological Contract describes a belief system about the employment relationship present in employer and employee rather than relying exclusively on a prescient description of expected outcomes (but not necessarily shared in every aspect). It describes a set of implied, informal mutual obligations and is the basis for the sustained, voluntary engagement of an employee that is required in today's organizational structures. The Psychological Contract is voluntary on both sides and it is expected to evolve over time. [Rous95]

[Rous04] describes the three main types of Psychological Contract, naming them the relational, transactional and hybrid type. The relational Psychological Contract describes a relationship of mutually expected loyalty, in which both sides behave in consistency with an expected long-term relationship, sharing economical risk and reward. A relational Psychological Contract can be vulnerable to violations because of the high expectations and stakes involved. A transactional Psychological Contract on the other hand, is focused on a narrower band of expectations, both in terms of scope and duration. It is more volatile but also more flexible, and doesn't imply a sharing of risk and reward. A transactional Psychological Contract may be terminated sooner and on shorter notice. It can be seen as appropriate for employees whose tasks are not central to the organization. A hybrid or balanced Psychological Contract implies shared risk but allows for greater flexibility and frequent renegotiation.

[Baru04] mentions four dimensions of career success, namely internal and external perception, organizational and social perception. Erosion of traditional career models between 1970 and 1985, as described by [Baru03] – cited from [Baru04] – have thrown individuals back on their own resources in terms of career goals, expectations and success. The emergent career paradigms of the protean (self-directed) and boundary-less career (traversing several organizations and possibly sectors and roles over a career life-span) hit middle managers between the ages of 35 to 50 ("Desert Generation") who had built their career on the assumption of a traditional, linear career paradigm, breaking relational Psychological Contracts. Generations moving into management after 1985, according to the same source, would have been prepared for the change and moved closer to a protean (autonomous) career design. Such a career design would indicate the presence of a more flexible, i.e. balanced or transactional Psychological Contract.

According to [Sche78] – cited from [Park98] – the Psychological Contract is expressed by the organization, among more tangible aspects like salary increase and promotion, by taking the individual into confidence and sharing organizational secrets. For a manager of Information Security, whose role by definition includes not just knowing but being trusted to investigate organizational secrets, a strong Psychological Contract can therefore be seen as a prerequisite for their role.

2.3 Career Patterns

Non-linear career paths are of special interest for a study of CISO careers, especially those effected before the wider availability of formal education. As described in [Sche68] and [Sche71], individuals can traverse hierarchical, inclusive and functional boundaries in the course of their careers. This gives rise to the categories of vertical, radial and circumferential movements. The commonly accepted career paradigm is that of vertical progression, to which the other kinds are merely accessory (e.g. in order to gain and demonstrate experience in different business segments).

[Rapo03] – cited from [WaSK81] – describes four types of prototypical career patterns. In an Incremental Career, individuals are rising gradually through the levels of the hierarchy. A Metamorphic Career is characterized by a fast rising and entrepreneurial posture but with a transactional view on each subsequent role and organizational environment. In a Tangential Career the concept of hierarchical progression is abandoned in favor of personal autonomy within the organization. A Humanist Career abandons the concept of a hierarchical progression in lieu of greater liberty to pursue ambitions outside the organization.

Arguably, the limited scope of the Information Security function within an enterprise forces those individuals with an inclination to develop their career within the field to pursue a boundary-less, cross-organizational career. [JoDe96] – cited from [Baru04] – describe competencies, strategies and challenges of the boundary-less career, such as cultivating a reputation and building social capital, knowing the industry and moving on before becoming trapped in a role or status. In addition to being cross-organizational, CISO careers can be cross-geographical. While not an attribute of the CISO role per se, the fact that it is commonly positioned as a headquarter function gives rise to a positioning as a "global manager". While [Baru02] criticizes the concept he concedes the existence of a "global mindset" [Baru04], which would at least influence the self-perception of the individual in question.

2.4 Social Construct of the CISO Role

The perception of a role will determine which individuals apply for or are being selected for a role. Two aspects can be distinguished, the corporate (internal) perception of the CISO and the cultural (external) reception. In turn, these expectations will have the potential shape the Psychological Contract.

Internal perception is shaped by interaction with the CISO, as well as experience with the perceived needs that led to the creation of the role. Conversely, the CISO can situationally be perceived as an obstacle on the grounds of zealotry, becoming an inhibitor, deficient communicative skills and resulting lack of organizational integration, and internal competition for power. In [EiHP08] the authors postulate an existing disconnect between the CISO and the rest of the organization, corollary to an antagonistic perception of the CISO.

This perception of the CISO role that individuals aspiring to a CISO career are confronted with is not uniformly positive within the organization, but carries appreciation within the professional community. It may therefore attract individuals with an involvement in the subject matter per se, rather than those looking for a broader management career.

2.5 Functional and Managerial Aspects

In contrast to the widely held perception that "Management is a practice, not a science" [Druc74], the Information Security Manager's role is at least in many ways a work of engineering. Commonly accepted standards, such as [ISO05] are used to prescribe and measure his or her actions and results. A broad base of national and international standards has been established for the management of Information Security, e.g. [Bitk07]. Given the relatively recent history of the domain it is unsurprising that the maturity of implementation varies considerably between businesses. [Sipo02].

From a purely practical perspective, the role may include additional common managerial responsibilities of people management, financial management, operational management and change leadership. Different models for allocating the Information Security function and responsibility within an enterprise exist. These will be determined by commonalities of skill, balance of power and the strategic view of the company. Common reporting lines include the CIO, the CFO or the CEO. [Fros08]

Based on research of job adverts, c.f. [Berl07] and [Whit08], IT Security skills are the most common explicit requirement, followed by communication skills, technical experience and leadership skills. An extremely broadly compiled set of functional requirements is a key component of many adverts.

3 Research Process

3.1 Objectives and Methodology

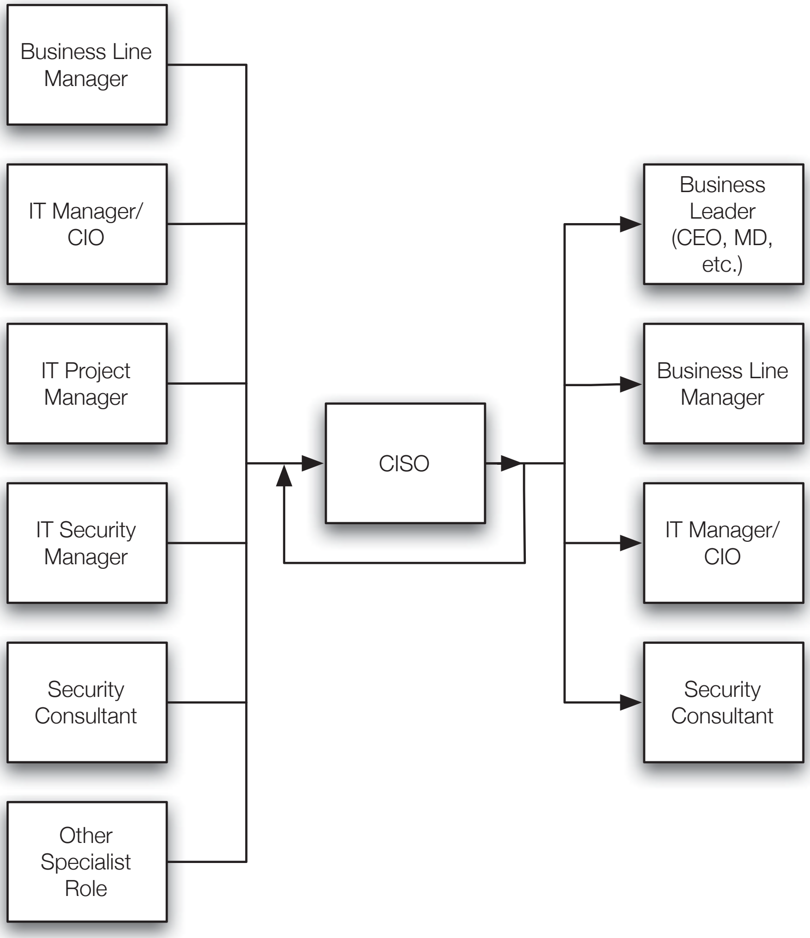


Fig. 1: Career Paths Emerged From Sample

Principally, it would be possible to conduct a quantitative study on CISO career motivations. However such a study would suffer from difficulties in selecting a representative sample based upon the relatively limited population and also limited information on career demographics.

In order to analyze the career of the CISO one therefore has to rely on an inductive approach in order to collect and interpret data. CISO career paths will have to be described and analyzed, identifying in particular the key decision moments leading to the appointment into the CISO role. Once these have been identified, drivers and motivators for each decision can be attributed. The narrative of the key decision points in individuals' careers will allow a motivational analysis. It is the objective of this study to identify "typical" motivational situations, not individual ones, so no individual psychometric analysis will be performed.

Based on the study's exploratory research objective, a Grounded Theory approach [GlSt99] was chosen to identify key themes and paradigms in the CISO career. The base set will be cross-sectional, with the complexity (number of questions) and scope (maximum number of candidates) of the interview process being mainly resource constrained. Grounded Theory allows the formation of a concept of the CISO career and the motivations directing it.

3.2 Research Design, Sample and Conduct

The main body of the interview script is composed of questions and cues of a descriptive nature. Exploratory questions are being used where they serve to further explore career motivations and conditions, but not to describe causes or effects. Interview questions are covering the main subject areas:

- Career narrative
- Career motivators
- Psychological Contract

22 current and former CISOs have been interviewed for this project. For the purposes of this study, a CISO was defined as someone bearing of having born the formal or de-facto Information Security Management or Information Risk Management responsibility for a business or business division. Information gathered from their career history and personal interviews have provided a number of key conclusions.

Individuals' background was often, but not exclusively in IT and IT management roles. The hiring process was broadly seen as an ad-hoc decision, in which factors like personal preference and serendipity played a bigger role than strategic career decisions and targeted grooming for the position.

Elements of circular and lateral career moves were common in many careers. In the interviews, individuals often described elements of protean and boundary-less careers, which were broadly seen as a positive element of the CISO career.

Nonetheless, most respondents described their career history as a linear succession and progression of roles with a tangible increase in influence over time.

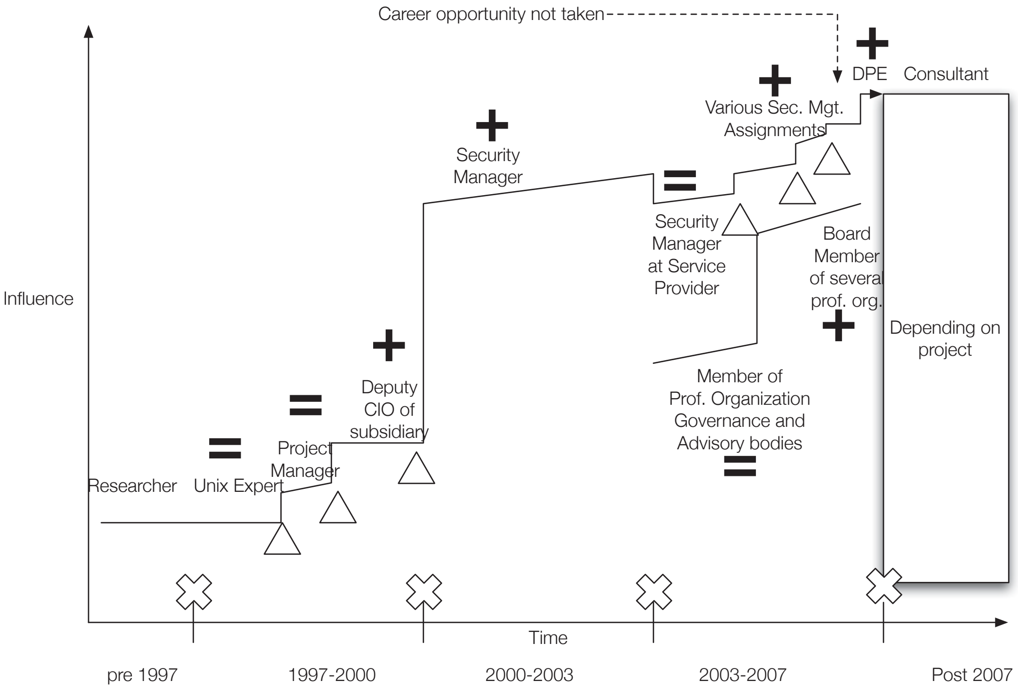

Career opportunity not taken
Influence
Time
Researcher
Unix Expert
Project Manager
Deputy CIO of subsidiary
Security Manager
Security Manager at Service Provider
Various Sec. Mgt. Assignments
DPE
Consultant
Board Member of several prof. org.
Member of Prof. Organization Governance and Advisory bodies
Depending on project
pre 1997
1997-2000
2000-2003
2003-2007
Post 2007

Fig. 2: Sample Career Map

4 Analysis

A dichotomy mentioned earlier is that between a technical/functional and a managerial/entrepreneurial view of the CISO role. Together with the fact that "Managerial Competence" and "Technical Competence" was a key subject in the interviews, this creates a natural classification.

From the analysis and correlation of interview responses, one can identify four segments of career patterns, based upon a broad classification into a preference for problem solving or organization building. Without ignoring the importance of situational aspects and the fact that the CISO role requires a balance between the two, participants often expressed a clear preference as to where their comfort zone lay. Orthogonally, one can identify the orientation of the individual's Psychological Contract towards the employing organization and its representatives, or towards the professional community at large.

Based upon this classification system, four key groups were identified aiming for either:

1. Perfection in their service to a specific organization, driven by a functional focus combined with a relational Psychological Contract
2. A managerial career aspiration, in which the CISO role was but a stepping stone, driven by a managerial focus combined with a relational Psychological Contract
3. Dedication to the cause of Information Security at large, driven by a functional focus combined with a transactional Psychological Contract

4. Inclination to perform serial organization building within the realm of the same role, driven by a functional focus combined with a transactional Psychological Contract

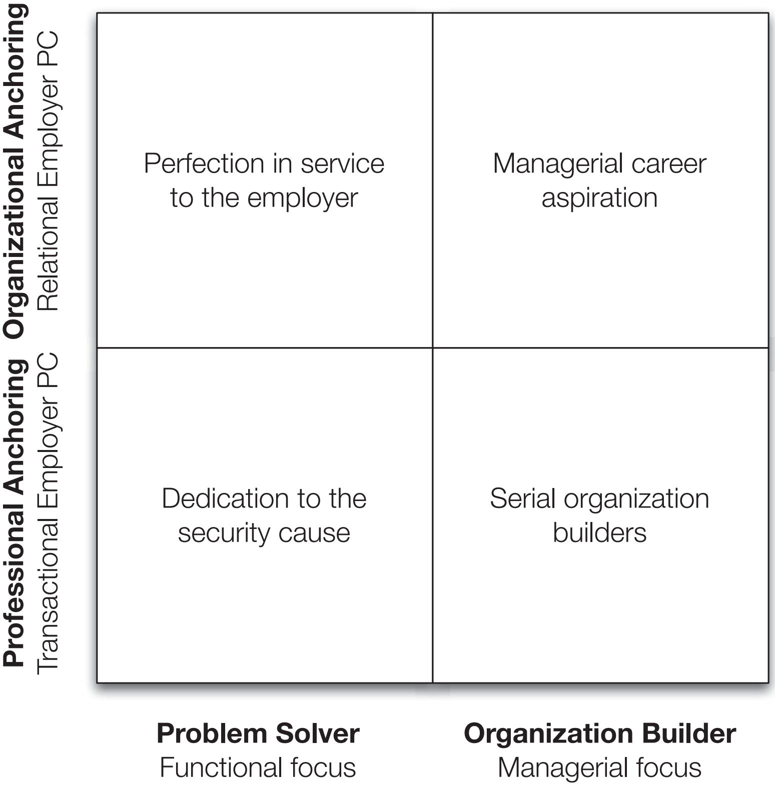

Organizational Anchoring
Relational Employer PC
Professional Anchoring
Transactional Employer PC
Perfection in service to the employer
Managerial career aspiration
Dedication to the security cause
Serial organization builders
Problem Solver
Functional focus
Organization Builder
Managerial focus

Fig. 3: Career Segments

It is important to note that three out of four classes will keep the individual within the general realm of the Information Security Profession, while the fourth one ("Managerial aspiration") would often result in a career in IT, at least as far as the individuals interviewed in this study were concerned. Again, this reflects the close affinity of the Information Security profession with the IT profession already described for the career path leading into a CISO role. Some participants described this process as either (and often enthusiastically) a question of personal preference or conversely as a perceived career lock-in that left respondents feeling they were left with a lack of options.

4.1 Aspiration to Perfection in Service

In this segment, a relational Psychological Contract with the employer is combined with a focus on problem solving. Paraphrased quotes from interviews (sampled from different respondents) include:

> *Rank and status are not very important for me, and my career is the result of coincidences. I am expanding my technical knowledge. The company needs to take care of*

> *its employees. My relationship with my employer has intensified over time. I am not looking for rewards. The work I am doing is richly gratifying.*

This career would remain in the CISO role, or perhaps move on to another, similar role. The functional development focus would match the tangential career, were it not for the fact that the role of the CISO is anything but tangential, but a role that is central to the organization, also in structural ways, i.e. it is often located at corporate Headquarters. The concept of a Spiral Career fits these individuals better, who have achieved their role by demonstrating functional competency rather than managerial prowess.

4.2 Managerial Career Aspiration

Individuals in this segment have a preference for managerial tasks but maintain a strong Psychological Contract with their employer. In their expectation is the CISO role is a transitory career stage, as described similarly in [Park98]. It can be reflected in a development to a business leader, line manager or IT manager.

Paraphrased quotes from interviews include:

> *This is a decision point for me on starting a new linear career or preparing for a lateral move. I see myself as a leader. A CISO doesn't easily collect transferable skills. I am no longer in love with technology. I feel I have reached what I can achieve in this role, and I want to move on. I have stayed with the company, because I wanted to.*

While many interviewees with a managerial focus professed to have a technological background, the reverse was a rare exception. I.e. a development from managerial to technological or functional focus, while not unheard of, appears to be a less common direction for career development within the sample.

4.3 Dedication to the Security Cause

Individuals in this segment combine a problem solving focus with a transactional Psychological Contract. This is often mirrored in their attitude towards the peer group or profession as their "true" home. A number of representatives of this segment were present in the interview sample. They did generally manage their career actively, but with little apparent regard for building a linear progression, even though this was sometimes claimed in the interview.

In some cases the segmentation was not so clear-cut. In these cases one might assume that the transactional Psychological Contract could perhaps be "repaired" in the future, which would revert representatives to a career again more rooted in an organization.

Paraphrased quotes from interviews include:

> *Career to me means to progressively increase job satisfaction. I don't have a plan for the time after my current role. I sometimes accepted positions that decreased my influence because it gave me an interesting challenge. I will stay in Information Security. I enjoy explaining something to people. I am a problem solver. But I don't want to focus my career only on one organization.*

A parallel can be drawn to the humanist career described in Subsection 2.1.3 for this segment. The characteristic of aiming for a higher objective while putting less emphasis on formal career development fits the pattern. However, the pattern would have developed in a later career phase as the incumbent managed to accomplish an important station within the organization he or she is working for.

4.4 Serial Organization Builders

A small number of individuals had a managerial focus but a transactional Psychological Contract. In this situation, they would find it hard to build a traditional career within a single organization.

Paraphrased statements include:

> *I would perhaps describe myself as an internal entrepreneur. Once I had awoken as a leader I sought out leadership opportunities. When I saw how little everybody else knew that grew my ambition. I figured that if I could set up a program once I could do it again. None of my moves was planned. I took opportunities as they came up. At one point I realized how important my peer network is to my career.*

The group of "Serial CISOs" was small within the sample, and their careers had evolved without planning but as a collusion of personal career situation (being at the right place at the right time), capabilities (being able to shape a new-found role) and the dynamic development of the Information Security profession and the CISO role over a period of time. They took an active view of managing their own career and actively sought a status of seniority within the peer group. It could be said that the peer group was their actual frame of reference, i.e. that they were building a career within that peer group, not within employing organizations. They typically left organizations for "better offers" with more responsibility or better salary, but within the same segment.

It did not always become entirely clear however whether this type of career had been a matter of personal choice, or circumstance. The transactional Psychological Contract would per se allow both options. None of the "Serial CISOs" in this study attested to ever having expressed their career strategy to potential employers. The career pattern for these individuals can be described as a metamorphic career. They have emancipated themselves from fixed organizational and professional contexts and would appear to be closer to free agents within the system. They can have the professional characteristics of consultants or interim managers.

5 Interpretations

Many respondents displayed signs of protean career management in their career history and in the description of their plans going forward. While individuals may not always consciously realize it the need to manage their own career is prominently ingrained in their career philosophy and aspiration.

A subgroup of interviewees interpreted the CISO career as a veiled technical career in the guise of a management role. A number of interviewees expressed their opinion that the CISO role was a potential career trap, in which they saw either themselves or others caught up in. (This applied also for some interviewees who had successfully transitioned into another role.)

Enthusiasm about and identification with the Information Security profession was a vivid, tangible element in many interviews. One interpretation of this would relate to the fact that technical career paths are associated with a strong sense of involvement. [Bail77]

5.1 Implications for Individuals

All in all, the way individuals manages their career can have a strong effect on how they will manage the CISO role. A CISO with a transactional Psychological Contract can be expected to be prone to refer to the "community standard" as an "absolute truth" and take a stance against political pressure. A more relational Psychological Contract may trigger more pragmatic behavior. There is a case for either kind of behavior, both strategic and situational, so whether or not it fits with the situation or corporate culture will need to be decided by the individual in line with his or her values.

Moreover, a mutually relational Psychological Contract will help the CISO in his or her role. Because the CISO relies on some of the relational aspects – especially the sharing of organizational secrets – to be effective, a more transactional stance may bear certain risks in terms of effectiveness, which need to be compensated/mitigated.

If a transactional Psychological Contract has developed then there is a strong incentive to build a protean, boundary-less career in order to overcome the risks associated with a weak (mutual) attachment with the employer and the probability of frequent job moves. The individual will benefit from clarity on his or her expectations.

5.2 Implications for Corporations

An ad-hoc appointment process, as it was described in several interviews, is incompatible with a role of the standing of the CISO within the corporation. Career development opportunities should be offered to CISOs that are aligned with their specialization and their ambitions. The fact that the CISO is at risk of being isolated within his or her career within the company cannot count as an excuse if the corporation is serious about attracting talent to this role.

The description of career paths allows a description of suitable resource pools from which CISOs can be recruited, including not just security experts but also IT and business line managers.

5.3 Implications for Professional Bodies

Professional associations have a key role to play in enabling growth and bridging knowledge between organizations. Some CISOs will turn to these bodies to further their career development or for learning. Others will stay focused on their employer and therefore refrain from getting involved. These bodies have a responsibility they need to ensure they are meeting.

Common services of professional associations include education and professional certifications, as well as networking opportunities and job platforms. However these broad offerings are commonly tailored to a traditional and highly functionally focused populace of CISOs. This implies an opportunity to expand offerings into tools that help CISOs develop beyond their role and, ultimately, beyond their profession. Where professional associations feel that this is not their core competency, other professional associations and MBA schools can take their place.

6 Conclusion

It is plausible to generalize these findings for other careers in technical management that are equally reliant on both the professional aptitude in a certain field and managerial capabilities. It would be misleading to restrict parallels on managers in executive or Board roles, the principle of allowing for a personal preference to deal with either the subject matter or managerial problems, and to differentiate between a relational and a transactional manifestation of the Psychological Contract remains equally applicable.

In this context, it is an open question whether any of the segments shown is, in and by itself, more desirable to a corporation looking to attract a technical manager or officer. As an assumption, the selection process may favor candidates professing a desire to either stay in a role or move along a traditional, linear career line. However there might be an opportunity for both the potential employer and the prospective employee to implement a different model, based more upon an interim management paradigm.

In other words, a market might develop for the "Serial CISOs" that enables corporations to tap into the external talent pool rather than trying to groom talent internally. This model however would be contingent on an employment strategy prepared to also release talent periodically.

References

[Bail77] Bailyn, L.: Involvement and Accomodation in Technical Careers: An Inquiry into the Relation to Work at Mid-Career, in J Van Maanen (ed), Organizational careers: Some new perspectives, John Wiley & Sons, 1997, 109-132

[Baru02] Baruch, Y.: No such thing as a global manager, Business Horizons, 2002, 45(1):36-42.

[Baru03] Baruch, Y.: The Desert Generation, Personnel Review, 2003, 32(5/6).

[Baru04] Baruch, Y.: Managing careers: Theory and practice, Prentice Hall, 2004.

[Berl07] Berlich, P.: How to Recruit the Right Security Professional and How to be the Person that Gets Recruited, presentation at SecureCapeTown 2007

[Berl10] Berlich, P.: Exploring Executive Career Paths in Information Security (Thesis, unpublished), Henley Business School, 2010

[Bitk07] Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk. Berlin, Germany, BITKOM, 2007

[Druc74] Drucker, P.: Management: Tasks, Responsibilities, Practices, Butterworth-Heinemann Ltd., 1974

[EiHP08] Eichstädt, U. & Haucke, A. & Pieper, A.: Aus der Abwehr in den Beichtstuhl. Enclosure to <kes> 2/2008

[Fros08] The 2008 (ISC)^2 Global Information Security Workforce Study. Frost & Sullivan and (ISC)^2, 2008

[GlSt99] Glaser, B.G. & Strauss, A.L.: The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine de Gruyter, 1999

[Holl97] Holland, J.L.: Making vocational choices: a theory of vocational personalities and work environments, 3rd ed. Psychological Assessment Resources, 1997

[ISO05] ISO/IEC 27002:2005 Information security management systems – Requirements, 2005

[JoDe96] Jones, C.; DeFillipi, R.J.: Back to the future in film: Combining industry and self-knowledge to meet career challenges of the 21st century, Academy of Management Executive, 10(4):91.

[OsFi96] Osipow, S.H. & Fitzgerald, L.F.: Theories of career development, Allyn and Bacon, 1996

[Park98] Parkinson, A.P.: The Changing Nature of the Employment Relationship: mapping a subjective terrain of the psychological contract (Thesis). Henley Management College, 1998

[Rapo03] Rapoport, R.: Mid-Career Development, Routledge, 2003

[Rous95] Rousseau, D.M.: Psychological contracts in organizations: Understanding written and unwritten agreements, Sage, 1995

[Rous04] Rousseau, D.M.: Psychological Contracts in the Workplace: Understanding the Ties That Motivate, Academy of Management Executive, 2004, 18(1):120-7

[Sche68] Schein, E.H.: The Individual, the Organization, and the Career: A Conceptual Scheme, Alfred P. Sloan School of Management, 1968

[Sche71] Schein, E.H.: The Individual, the Organization, and the Career – a Conceptual Scheme, The Journal of Applied Behavioral Science, 1971, 7(4):401-26.

[Sche78] Schein, E.H.: Career Dynamics: Matching Individual and Organizational Needs, Addison-Wesley, 1978

[Sche93] Schein, E.H.: Career Anchors: Discovering your real values, Pfeiffer & Co, 1993

[Sche96] Schein, E.H.: Career anchors revisited: Implications for career development in the 21st century. The Academy of Management Executive, 1996

[Sipo02] Siponen, M.T.: Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria, Information Management & Computer Security, 2002, 10(5):210-24.

[StFr07] Steele, C. & Francis-Smythe, J.: Proceedings of the British Psychological Society's 2007 Occupational Psychology Conference, British Psychological Society, 2007

[WaSK81] Watts, A.G. & Super, D.E. & Kidd, J.M.: Career Development in Britain, Hobsons Publishing PLC, 1981

[Whit08] Whitten, D.: The Chief Information Security Officer: An Analysis of the Skills Required for Success, Journal of Computer Information Systems, 2008, 48(3):15-9.

Positioning Information Security Roles, Processes and Interactions

Dimitrios Papadopoulos[1] · Bernhard M. Hämmerli[2]

[1]Gjovik University College
Biskot188@hotmail.com

[2]Acris GmbH
bmhaemmerli@acris.ch

Abstract

All information security professionals around the globe acknowledge that "everyone is responsible for information security" in a company. This trivial statement looks clever but hides core challenges, "Who is everyone? How does everyone contribute or challenge information security?"

In our researched project we researched in-depth roles, processes and interaction in the corporate information security, by creating a framework for crystal clear defined roles and its associated security obligations and responsibilities. 20 corporate roles are analyzed from management and security perspective; classical interactions between information security roles leveraging and turning down security are given in case studies. Furthermore we generated structured tasks descriptions of the roles and open the road to the fulfillment of an information security consultants dream by creating Job descriptions including its security responsibilities!

We justified the necessity of defining roles and by introducing benefits of this approach:

1. Avoiding unnecessary conflicts and internal politics by establishing security organization with inclusion of all employees' duties.
2. Increasing security-level, efficiency and productivity by assigning clearly responsibilities.
3. Achieving good information security governance by encouraging coordinated team effort and mutual control.

Illustrative corporate examples demonstrate the need to supplement traditional corporate information security governance frameworks with roles and responsibilities for all positions.

1 A new Era of Information Security

We live in a modern world, where society has found a way to adapt to the rapid advance of technology using it in its advantage, providing a safe, secure and balanced environment to live in, in most parts of the globe.

The people in the developed countries of the world found a harmony between nature, technology and society. While nature is unpredictable and yet can't be totally controlled, people found a way to mitigate the risks and protect themselves from it, however the technology and society is well controlled by people. People live in a well-organized society where ground rules are established

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_14, © Springer Fachmedien Wiesbaden 2013

and proper communications of those rules is in place providing a harmonized ecosystem. In which people elect the government, a government that establish the laws, the police departments and courts, which assure that the laws are obeyed and followed. However this ecosystem would collapse if people didn't possess an immanence sense of responsibility! Nothing would work if people were not responsible in our society. Whether this is a doctor saving a patient's life or a person driving a car on a road where children play, it is and always will be the sense of responsibility, combined of course with other people's characteristics such as ethics, beliefs etc. that drives a person to follow the rules create a harmonized ecosystem. The government is responsible to the people that elected it, the police and court authorities are responsible to the government and this creates an inner endless circle of responsibilities. But why we describe all this?

Corporation versus Governance:
A company is no different then a society. It is as well an ecosystem, with the top management also known as C-level executives playing the role of the government, policies, procedures and line managers playing the role of the police and court authority and the employees those of the people. The difference is that a company's goal is different from a society's, that of producing revenue. That's the responsibility of each and every member of a company to play his role and contribute to the process of generating revenue. We speak of revenue which is the ultimate goal but also a requirement for a company. A requirement set by its investors. Investors that are investing their money in a company create a need for protection. This need for protection is establish by laws, laws that will protect the people and their interests. Here is where information security enters the scene playing a vital role. Information security is the solution-means to the legal requirement of the protections of the investors and their investment. We define Information security as "a legal requirement that is met by the use of technology. " However information security is not something new, we have well established frameworks-solutions for information security governance in companies. Unfortunately we often see that the current information security models eventually fail. There are many various reasons for these failures but we wont go into details on these aspects but rather keep the fact. Having this fact in mind we took a holistic view on the bigger picture, we compare the companies with the society there lies the answer! In the society we have crystal clear roles and responsibilities, people know what to do and how to do it when it comes to the safety, the security and the balance of the society. Something that in corporation's level is clearly lacking.

Lack of knowledge:
Although the trivial fact that everyone is responsible for security is acknowledge by all the security professionals around the globe. There is no framework, analysis, research on what appears to be an insignificant word, "everyone". Who is everyone? How do they contribute or challenge corporate information security? That is what we explored. It is common knowledge that every company uses a sort of organizational structure and has crystal clear responsibilities assigned to the business units, managers, personnel etc., assuring that everyone contributes to the revenue process. But is it really remarkable that many neglect the problem, that all contribute to the revenue generation, by knowing their role and responsibilities, but few bare the challenging task to protect it! Which leads us to raise the question: "Are the CISO and security department magicians?" or is it time to realize that information security is a joint effort and responsibility. It is time to have security related responsibilities combined with the already management oriented responsibilities every company has. Thus, what roles and responsibilities study comes to contribute.

2 Chief Financial Officer

The role of Chief Financial Officer came to life in the late 1970s as a response to a new law the American government introduced. During those early years, the CFO was acting as the company's ambassador to its investors and financial analysts. His primary tasks were to manage relationships between shareholders and to assure that their expectations were met regarding the companies stock value among other things, such as managing sales, acquisitions, divestitures and ultimately generate revenue for the company. Furthermore, as the role evolved more and more responsibilities were added. The development of accounting gimmicks to lower taxes, the participation in strategic and operational decisions, the evaluation of business unit performance and invention of new ways to increase capital in the company as well as its protection from adversaries' takeover attempts, became routine things in a CFO's daily-diary.

New Responsibilities:
In the modern world and in the year 2013 we find that the CFO's role has changed from that of day-to-day management into that of a strategic thinker, shaping company's value and exit plan strategy, although it still inherits the characteristics of the previous years. The CFO is still responsible for overseeing all the "ancient" functions to come with the name. One of the newly duties of the CFO's role is dealing with information security. The CFO is one of the most important roles when it comes to security, he "sets" budgets, recommends cuts, provides the means for other departments to implement projects and run processes. Thus said, we understand that he/she is the person who will provide the IT budget, which usually will include the information security budget. Therefore, his understanding and beliefs about security are things that will either help security develop or become a serious drawback. Lack of security awareness and understanding will lead to costs cutting from the security budget and tie the hands of the CISO into managing the security threats of the company. Therefore, the starting point is the budget.

CFO and Security:
In order to set a budget for security the CFO has to understand and accept for a fact that security is not just an IT risk but it is a real business risk, therefore it has to be treated as such. It is a CFO's responsibility to deal with business risks and find ways to mitigate. That will put security on the top of the risk list. A CFO has to understand that security is a continuous process that means that security is a continuous risk and needs constant investment and improvement in order to be mitigated. Thus, a CFO has to acknowledge and fully understand a philosophy that [HoMi10] "The purpose of risk management is to improve the future, not to explain the past." Risk management is just the beginning! Compliance, Merges and Acquisitions, disaster recovery and business continuity plans among others things connect the CFO to information security. We can't go deeper into the analysis of each responsibility of the CFO but rather list them synoptically in table 1 & 2 below and refer you to the detailed study [DiPa13].

3 Chief Human Resources officer

What is a company without people? Can it exist without people? Of course not. They are the alpha and the omega of a company, they make the company. It's their existence that gives breath to any kind of operations or procedures. Thus, creates a need of a person to manage all of these people. That's the reason companies have a Chief Human Resources Officer.

Table 1: CFO Responsibilities

CFO Management Responsibilities	Task brief description
1. Business Strategy	Assess annual organizational performance. Assist in establishing yearly objectives and goals. Oversees strategic long-term budgetary planning and costs management in alignment with the board of Directors.
2. Financial Planning and Analysis	Conducts regular financial planning reports. Conducts analysis of financial conditions of the company and forecasts financial expectations. Develop and execute analysis of various business initiatives. Develop and maintain capital budget.
3. Finance and Accounting	Oversee cash flow planning and ensure availability of funds as needed. Oversee cash, investment, and asset management. Ensure legal and regulatory compliance regarding all financial functions. Lead the development of accounting gimmicks to lower taxes and increase revenue.
4. Insurance and Real Estate	Manage company's insurance program. Manage the company's real estate affairs.
5. Merges and Acquisitions	Plan, develop and execute merges and acquisitions. Conduct analysis, forecast and provide future outcome of penitential merges and acquisitions.
6. Business value and Exit plan strategy	Conduct analysis recommend innovations to grow business value and companies stock value. Develop and oversee the exit plan strategy for the company.

Old versus new:

Employees are considered as valuable resources for a company, but the fact is that they are people, which make it impossible for them to be treated like other material resources. Each and every one of them has their own special characteristics and requires a different approach and treatment. Thus, what the CHRO brings to the table, he humanizes the company's life and introduces human values in the company. But is he just a manager who deals with the employees' everyday? It was so some years ago where a CHRO was responsible for bringing employees and hiring the best employees that serves the needs of the company. Nowadays, they do far more then just bring new faces to the company. Today's CHRO is a complex role that has many requirements and expectations. He is a business partner, driver and talent developer, governance asset, employee recruiter, manager and evaluator. We wont analyze these functions of the role as they are analyzed in our full study [DiPa13]. But rather continue to see why the CHRO makes a difference regarding information security. Nowadays, it is not a secret that CHRO tend to be really well informed about the latest employee legislation, but they usually have no or very limited knowledge of information security. However, the CHRO plays a vital role on information security.

Table 2: CFO Responsibilities

Security Related Responsibilities	Brief Description
1. Security Culture	A CFO should be a security aware person. Allocate appropriate resources and funding for continuous improvement of security. Treat security as a business risk.
2. DRP and BCM	Participate and assist the CISO in the development of Disaster Recovery, Business Continuity strategies and plans.
3. Compliance	Oversee and enforce compliance with regulations to avoid fines and penalties.
4. Ensure financial assets security	Ensure that financial deals, contracts, auctions, forecasts, product launch dates and prices are things that are within the information that has to be protected and can affect the financial well being of a company.
5. Information Security in M&A	Ensure proper Information security infrastructure exists in the acquired company and compliance with regulations is in place and in order.
6. Bring-your-own-device policies	They raise a lot of security concerns and issues, such as data loss, inappropriate usage of devices, unauthorized access to non personal devices of the company and many more yet not fully revealed threats and risks that need to be handled and mitigated. If the CFOs haven't started to pay attention, now's the time to do it!

Employee characteristics:

Every employee that is hired has its own character, personality, education,"παιδεία»(pedia) an ancient Greek word that cannot be translated but means the way that a child is raised. How his character is shaped according to the principles, the beliefs, the values of his parents and the surrounding society he is living in. A person's honesty, dignity, self-respect and respect of others are characteristics that he gains from his early childhood and accompany him through his entire life. The way of thinking, the way of living, the traditions and principles differ from country to country and that what makes people different. Of course every person has a different way of life and different experiences but still, a country shapes the character of its people.

Reducing the Risks:

The CHRO is the person in charge for the hiring process of a company. Therefore it is essential for him to know all the above information for a person. Knowing the cultural background of the employees is essential for security and it gives you way more information about a person then from a curriculum vitae or an interview. It reduces the risk of employing personnel likely to present a security concern. Companies spend a lot of money to protect themselves from outside attackers but most of them forget about the insider threat and human errors, which eventually lead to information security breach and failure. Thus, where the CHRO plays a vital role by reducing the risk of hiring the wrong people and simultaneously being in an ideal position to drive security messages, policies and procedures. Here we would like to quote a phrase from Paulo Coelho. In an interview a reporter asked him whether he could describe the aim of his book in one sentence. "If I could do that, there is no need for me to write a whole book." Thus said, we can't go deeper in CHRO analysis in this paper without describing the whole study. Therefore, we will list the findings of our study of the CHRO role [DiPa13] listed in tables 3 & 4 below.

Table 3: CHRO Responsibilities

CHRO Management Responsibilities	**Task brief description**
1. CHRO a value creator.	The CHRO is a talent developer, he is a coach that will assist, guide, reward and motivate the employees in order to maximize their efficiency and productivity to assist the company achieve its goals.
2. Excellent recruiter	The CHRO has to be a great analyst and judge of character in order to hire the right people for the right position.
3. Business partner and strategist.	A CHRO as a C-level executive is a business partner, a key advisor to the board of directors and the CEO in the shaping of the companies strategy towards the companies goals and objectives.
4. Performance evaluator	A CHRO will evaluate the employees' performance and take appropriate measures if necessary.
5. Balancer	A person who will solve any conflicts that might rise between employees, despite their rank, top level employees or simple staff and create a happy and friendly working environment.
6. Manager	The CHRO will assist and oversee the daily governance functions of a company, such as arrange board meetings, interact with employees, ensure regulatory compliance and oversee and assure high quality human resources services that include enhancing controls for human capital processes and mitigating risk around HR.

Table 4: CHRO Responsibilities

Security Related Responsibilities	**Brief Description**
1. Excellent scouter and character analyst.	Knowing the cultural background of a potential employee reduces the risk of employing personnel likely to present a security concern.
2. Employees Awareness and education driver	The CHRO is in an ideal position to drive security messages, policies and procedures.
3. Hiring, Termination and Relocations keeper	The CHRO keeps track of the access privileges an employer has, had to perform his duties and when those have to be terminated.
4. Identity and authentication	The CHRO has to establish that applicants and contractors are who they claim to be.
5. Valuable asset and advisor for security.	The role of the CHRO is to assist and provide counsel and solutions interacting with the CISO in order to mitigate all facing risks.
6. Security incidents investigation asset.	The CHRO will provide valuable insight, in understanding the elements of the job, and they will help prepare the investigator to ask the right questions, and help preserve the rights of the suspect employee.
7. Solid understanding of information Security	The CHRO has to have a very good understanding of what Information Security means to the company and what kind of people and skill-set are needed to perform such job.

4 Cyber Warfare

Today we hear all around us the term cyber attacks on a daily basis. We have seen a group of hackers named "Anonymous" perform various "Denial of Service" attacks and defacement attacks on various Government's web servers and private corporations. On 27th April 2007 Estonia was the victim of one of the biggest coordinated cyber attacks where it also affected the general public. A foreign government was considered to be the initiator of this attack. We have seen other examples of such attacks like: Titan Rain which was a series of coordinated attacks on American computer systems in 2003, Flame which is a Data-stealing malware that was used for targeted cyber espionage initially in Middle Eastern countries and afterwards spread into Europe and USA. It is labeled as one of the most complex malware ever found, Stuxnet is a computer worm which targeted Iran's nuclear facility which was designed to affect exclusively Siemens supervisory control and data acquisition systems (SCADA) that control and monitor industrial, MiniDuke a highly customized malicious that used a PDF exploit in Adobe Reader creating a backdoor was used to attack NATO and European governments and institutions. These are just some of the few ways today's wars have been transferred to cyber space and terror scenarios have already been developed claiming that a multifaceted cyber attack coordinated professionally could take down air traffic control systems, telecommunication grids, create a chaos in the stock market and even deny people from basic needs such as water, electricity and even emergency services such as ambulance dispatch, fire departments and police if the radio bands are silenced.

This scenario as terrifying as it sounds, with the rapid advance of technology and the constant evolution of networks is not far from becoming a reality. The modern world categorizes these threats with a buzzword as "The advanced persistent threat (APT)". The APT acronym is constantly misused in the IT security scene and a misconception is generated, people tend to think that APT is a sophisticated malware attack. However it is not the sophistication of the malware rather the attacker's determination and resources he is willing to allocate to succeed in his mission. That is the real threat of the APT, It is not a what, but who? The power of the APT lies in the competence, resources and motivation an attacker has who will never stop until he reaches his objectives, whether this is theft of intellectual property or damaging a country or company, he will adapt to the security measures you have deployed and will find a way to breach information security or he will quit if the costs of the attack exceed the value of the prize he is after.

Companies Cyber warfare:
We speak of a cyber war between governments where intelligence gathering and espionage is common practice. This is no different between companies. Cyber attacks on companies are a commonality in our modern world. Attacks such as data theft could be used to blackmail the owners of a company in order not to release the data captured which would expose the information security failure of the company and damage her reputation. The attacker could also threaten the company in performing denial of service attacks taking the company temporary out of business. Both of these cases result in money lost for the company. Cyber threats are a new and evolving source of risks and most of the companies aren't yet prepared to mitigate and handle such risks. There is no secure company in any sector and the threat is growing but nobody can say that the world had not been warned. The world Economic Forum (WEF) in 2012 placed cyber attacks on the top five threats the world is facing, next to threats of weapons of mass destruction, they emphasize that cyber threats shouldn't be underestimated. Written below is an example of how a company can become can become cyber savvy and mitigate one of the most emerging threats the world and companies are facing by having a crystal clear delegation of roles and responsibilities.

Roles & Responsibilities:
The CEO has to understand the risks and the opportunities that the cyber world presents and lead the way to the company's entrance to the virtual world. The CRO has to conduct constant risk assessments of the cyber threats and with the collaboration of the CISO and CIO to ensure that the IT department is constantly evolving its capabilities to deal with cyber risks. The CISO has to

cooperate with other C- level executives and line managers, from which most importantly with the CHRO and the COO in order to develop an awareness campaign and educate the users about the current emerging cyber world and the risks it hides. The CEO with the board of directors has to invest in the development of cyber skills. This means shaping the strategy of the company in order to mitigate the threats by having experts handling the threats. As a consequence, the responsibility of the CHRO is to recruit talented people and to collaborate with the CISO in the development of a plan on providing constant education and cyber skills development of employees, because it is difficult to recruit an expert with those skills in the current market therefore companies have to create their own.

The CEO and board of directors have to allocate resources on the cyber threat and ensure its mitigation like any other threat the company faces and one of the core measures is to sponsor the creation of a Cyber incident response team a team that will be able to monitor, gather intelligence about the constant evolving cyber threats and prepare plans to mitigate them communicating from board level to business operations and even cooperating with other companies to strengthen their knowledge and share expertise. In addition, the company's strategy should be aggressive and active against attackers defending the company with legal means prosecuting the attackers. Thus, the requirement of a great CLO who will be well informed on cyber laws and requirements. Last but not least the CMO has to communicate publicly about cyber threats, incidents and responses promoting the cyber threats risks and promoting an information security awareness and culture.

5 Delegation of Duties

In this section we would like tell you a real life story. An intern was working in a big commercial bank and the director of the branch as well as the deputy director and some senior officers with access privileges to the banks systems due to their overloaded work schedule trusted the intern with their user-IDs and passwords and asked him to perform various tasks for them on a daily basis. Thus a very familiar situation to many people working in a network environment where users privileges and access controls are in place, people do share credentials in order to get a job done. This is a huge mistake and exposes the company's information security to various risks. In the case of the intern, the highest-level officer is the branch director, in many other companies the same situation could happen where a CEO gives his credentials to his secretary or somebody else to do some tasks for him. But lets analyze this situation further, what could the intern or anyone else in the same position do. There are three possible courses of actions a person can do:

1. It's your boss, so it's okay to do this.
2. Ignore the request and hope he forgets.
3. Decline the request and remind your supervisor that it is against security policy.

Choice Dilemma:
The intern chose at first option number two, but this never works. Unfortunately for him, he had no other choice but to accept the trust of the director and the senior officers and hopping that nothing goes wrong. If something did go wrong and an incident did occur, during the investigation he would be the first to take the blame, because he is the weakest link in the circle. The management would face the constituencies for giving out the passwords and would be held accountable but the intern would have to go and prove that he did nothing wrong and that was

a risk for him personally, as specially as it was in the interns case a financial bank where large amounts of money are processed on a daily basis and he could end up facing criminal charges and possibly pay settlements to the bank if any money was lost or stolen.

A lot of us would here raise a question? Why it is that the intern didn't choose the correct answer that is obviously the third option? This is not a choice made only by the intern, but many other employees who don't dare to choose that option although it is the correct choice. There are two explanations, one is that the users don't have security awareness and education which means that they have never read or familiarize themselves with the security policy of the company or because they trust, respect, fear their supervisor and know that a possible answer like that would endanger their relationship with them, something that will lead to possible disadvantages or change of behavior of the supervisor towards them.

Lessons learned:
This example illustrates a very common situation that happens in every company where we have delegations of duties and hierarchical roles distribution. This situation is tough to handle because of its nature and it is based on the relationship between people. Information security can be compromised and exposed by such behavior on some occasions or in the intern's case, luckily everything ends with a happy end. These delegations of roles and responsibilities is a risky game and the CISO has to be a balancer in between managers, C-level executives, supervisor, directors and users ensuring that all are educated and understand the consequences both for the company and themselves on a personal level of such behavior. Thus, understanding that the access controls and user privileges are there for a reason, the same reason we have different roles in a company, therefore avoiding the credentials sharing is a must for every company.

6 Why Roles & Responsibilities make a difference?

We covered only a small part of the studied roles just to illustrate our research [DiPa13], however we demonstrated the necessity of the roles and their responsibilities. And as any other two way relationships wherever there is a need for something there should be a benefit from the solution. Among many others we list bellow the key benefits that crystal clear roles and responsibilities delegation and definition bring to information security governance as a supplement.

1. They establish an organizational structure avoiding chaos, unnecessary internal politics and display compliance with internal policies, laws and regulations.
2. They mitigate the risk of information security staff being a single point of failure and ensure and promote C-level executives support for information security as well as establish formal communication channels with them.
3. Improve security & business processes: By assigning clear responsibilities: security level increases and processes improve becoming more efficient and more productive.
4. They enable greater allocation of company's resources minimizing the costs of provision of adequate information security functions.
5. Achieving good information security governance by encouraging coordinated team effort and mutual control.

7 Conclusion

We opened Pandora's box on an area that clearly lacks research. Thus, of roles and responsibilities. It is essential for companies to understand that everyone within a company is responsible for information security. There can't and shouldn't be only one person to blame if something goes wrong. Security is an overall process and everyone, one way or another, has to contribute in order to make it work. Any control measures can collapse in seconds if people don't understand that they also play a role in the information scene.

References

[DiPa13] Papadopoulos, Dimitrios: Positioning the roles, interfaces and processes in the information security scene, Information Security Management, Gjovik University College 2013.

[HoMi10] Hoehl, Michael: Creating a monthly information security scorecard for CIO and CFO. SANS Institute InfoSec Reading Room. 2010.

Safe Browsing

Norbert Schirmer

Sirrix AG security technologies
n.schirmer@sirrix.com

Abstract

Browsing the Web is an indispensible tool in everyday business life. On the same PC, which we use for browsing, we work on sensitive data, e.g. personal data or internal business critical information. The immense benefits from using the Web are threatened by the continuously evolving risk of attacks to the browser. These attacks exploit the capabilities of modern browsers and inject malware into the internal network. The protection mechanisms of the browser and the operating system fail short and do not deliver an adequate level of security. In this article we discuss several attempts to secure Web browsing under the aspect of security, Web functionality, usability, efforts and costs, recovery in case of an infection and mobile use.

1 Introduction

Using the Internet, especially the Web is an integral part of everyday business life. The same PC is used for browsing, as well as to work on sensitive data, from personal data, to internal business critical or research data. The immense benefits of the Internet have to face the ever growing threat of attacks to Web browsers. These attacks misuse the possibilities of modern browsers and inject malware into the internal infrastructure of enterprises or government agencies. Sensitive data may leak via the Web browser to the Internet. Besides the progress in functionality, the browser development in the recent years can be viewed as a constant battle against the various attack scenarios. At the latest when the Internet became "active" with the introduction of "Web 2.0", the balance between threats and profits got lost. "Active Content" is omnipresent in modern Web sites, which meanwhile behave like fully featured applications. Programming interfaces like JavaScript, Java, Active X or Flash allow accessing the PC of the user, in particular the file system or the Web cam. Malware like Trojans or viruses can misuse these powerful tools to access sensitive information.

Enterprises and government agencies are in the dilemma to either restrict the Internet access or to find an alternative solution to live with the threats. In this article we discuss various approaches.

2 The Threat of Active Content

Technically, active content is program code which is integrated into a Web site and is downloaded and executed by the browser. Unknown, external program code is executed on the desktop PC right in the heart of the internal infrastructure (Intranet). If this program code contains malware, it is also executed. The execution of the code is transparent to the user, and already happens as the Web site is loaded. It does not require an additional user interaction (like opening an attachment

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_15, © Springer Fachmedien Wiesbaden 2013

of an email). By viewing a Web site alone, the user risks to infect the PC with malware. This is known as "Drive by Download" and is nowadays the major gateway for malware infections.

It is important to note, that malware is not only distributed by untrustworthy Web portals, but also indirectly via trusted Web portals, without knowledge of the provider. This can happen via rented advertisement space, or security vulnerabilities of the Web servers. A typical landing page of a news portal contacts around 50 Web servers, which could all have their own security vulnerabilities.

Usually, once a security vulnerability becomes public, a patch is provided. But it takes time for these patches to be developed in the first place and then even more time to be distributed and deployed on the Web servers. This is equally true for the security vulnerabilities in browsers and operating systems. Security measures like malware scanners or intrusion detection systems have to be updated regularly. And even then, they are only effective against known threats and known vulnerabilities. To protect against new attacks, so called "zero day exploits" these security measures systematically have to fail short.

The threats of active content are well known by the browser manufacturers. Again and again they improve the browser inherent mechanisms to protect against the impact of malware. However, these protection mechanisms fail short. All security measures of the well-known browsers are regularly exploited[1]. Because of this situation, browsing the Web poises a notable threat for enterprises or governmental agencies.

Enterprises and governmental agencies face the trade-off between the productive usage of the Web and the protection of sensitive data and the internal infrastructure. We discuss various approaches to remedy this situation. The central security objective is the protection of the sensitive information and the internal infrastructure, including its availability. We distinguish the following aspects:

- **Security**: Here we look at the confidentiality of the internal data, which is processed on the desktop PCs and the integrity of the internal infrastructure (Intranet)
- **Web functionality**: We compare the solutions with respect to possible restrictions in Web functionality. For example if active content is completely blocked, some Web sites can become completely unusable.
- **Usability**: Here we focus on the general usability of the solution independent of the Web functionality it offers. For example, if the user is able to use the desktop PC for browsing, or if an separate Internet terminal has to be used.
- **Efforts and costs**: Here we subsume both the efforts and costs of acquiring, installing and maintaining the solutions.
- **Availability** of the Internet and **recovery** from an infection: In case of a successful attack recovery means have to be present to regain a clean state. Depending on the security measures, different parts of the infrastructure can be affected by an infection, which has severe impact on the availability of infrastructure and the efforts of the recovery.
- **Mobile use**: This aspects looks into the capabilities of the solution to support the mobile use from laptops outside of the infrastructure. The mobile use case becomes more and more standard and therefor a proper protection against attacks from the Internet has to

[1] http://www.heise.de/newsticker/meldung/Google-Chrome-auf-Ansage-geknackt-1434161.html, http://www.heise.de/newsticker/meldung/Pwn2own-Wettbewerb-Safari-IE8-und-Firefox-gehackt-207855.html

be granted. As a security concept is only as strong as its weakest chain it would be fatal to ignore the mobile use case in the security concept.

3 Approaches

3.1 No Web Access

The most consequent approach is to completely disable the access to the Web, and therefor to all its threats. This also covers possible indirect distribution of malware, e.g. by downloading files to a USB stick. This complete denial of the Web is only practical for (parts) of enterprises or governmental agencies with a very high security needs.

Pros:
- Ultimate security

Cons:
- Impractical for most stakeholders

3.2 Physical Isolation of Intranet and Internet

A quite consequent approach is the isolation of Intranet and Internet by physical means. To access the Internet a dedicated PC with a dedicated network is used. The PCs and the network traffic for Intranet and Internet is thus physically isolated from each other. A direct infection of the Intranet and the work PC from the Internet PC and its network is thus impossible. However, via indirect means like downloading files to a USB stick the internal network can still be infected.

This secure solution has some major drawbacks. Firstly, the user has the burden to work with two distinct PCs. In the best case every employee has his own two PCs at the same desktop. As this means a huge effort and doubles the price in PC hardware and software licences, it is more likely that only a few dedicated Internet PCs have to be shared among the employees. Besides these hard and software costs, there is also an immense administrative overhead, as the hard and software has to be maintained independently, when the isolation is properly employed. Moreover, there is a need of a proper security concept and a recovery strategy for the Internet PCs and infrastructure. To protect against an infection and to maintain the availability of the Internet the Web functionality may be restricted, e.g. by disabling active content. For the mobile use this solution is infeasible, as this would imply the use of two laptops, one for browsing and one for work.

Pros:
- High security via physical isolation

Cons:
- Bad usability, as distinct PCs have to be used
- Infeasible for mobile use
- High costs by redundant hardware
- High administrative costs
- Laborious / costly recovery of the Internet PCs in case of an infection

3.3 Remote Controlled Browsers System (ReCoBS)

This solution (cf. Figure 1) also follows the principle of isolation. For browsing the Web dedicated terminal servers are used [BSI06]. On the desktop PC no Web browser is running at all. Instead a remote connection to the terminal server is established. Only the terminal server has access to the Internet. The browser is merely executed on the terminal server, on the desktop PC it is only displayed. To display the browser on the desktop PC a network connection to the terminal server is needed. However via this internal network connection only graphic and audio data is transferred (Terminal Server Protocol), which comes from the execution of the browser on the terminal server. In this setup there is no physical isolation of the networks, but the attack surface is considerably reduced compared to a browser running on the desktop PC, as the execution of the potentially dangerous active content is confined to the terminal server. As the browser is not executed on the desktop PC it cannot harm the PC. Attacks from the Internet only affect the terminal server. To confine the malware on the terminal server additional security measures have to be in place to isolate it from the internal network (e.g. firewalls). Typically the terminal server is placed in the demilitarized zone (DMZ).

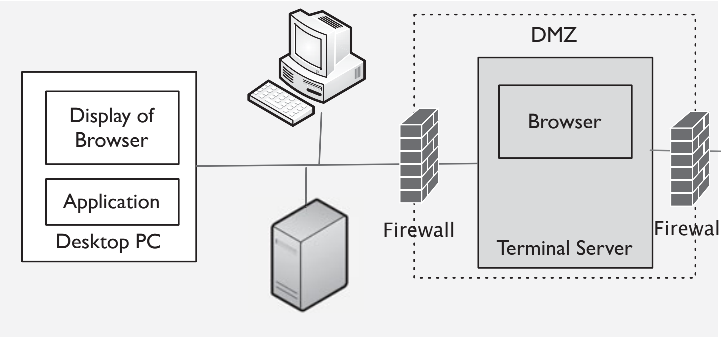


Fig. 1: ReCoBS topology: the browser is executed remotely on a dedicated terminal server and is only displayed on the PC

For the terminal server a proper recovery strategy has to be in place, to clean the server after an infection from malware and to guarantee the availability of the Internet. This can be achieved by rebooting the server from a clean disk image.

Compared to the approach with physically isolated PCs the usability of the system is improved as the user can operate the browser from his ordinary desktop PC. Moreover, unrestricted Web functionality can be offered by the solution, as the terminal server can be regarded as a "victim machine" and an infection of the server can be tolerated, as long as a proper recovery strategy is in place. Some comfort restrictions with regards to multimedia content may have to be tolerated by the users, as the solution comes with a notable bandwidth overhead. This is the price of the transformation of the Internet traffic to pure graphic and audio data by the Terminal Server Protocol.

The costs for the terminal servers are considerable, as the hardware has to be powerful enough to support the browser sessions of all users. To scale to a high number of users, clusters of servers may be needed. This also has high demands on the network bandwidth of the server (cluster). The transformation of the Internet traffic to pure graphic and audio data demands 5 to 10 times of the bandwidth.

This solution is not suitable for mobile use and the use with low bandwidth connections in general. It is technically possible to connect the laptop via VPN to the internal network, but the bandwidth is typically too limited for the traffic generated between the laptop and the terminal sever.

Pros:

- High security
- Good usability, full Web functionality

Cons:

- High costs
- High administrative overhead
- Insufficient for mobile use, and low bandwidth connections

3.4 Protection of Web Access via Proxy / Firewall

In this variant the Web browser is directly executed on the desktop PC and has access to the Intranet as well as the Internet. The protection of the Intranet from the Internet is implemented at the perimeter from Internet to Intranet. Typically a so called demilitarized zone (DMZ) is installed, where firewalls and proxy server monitor and filter the traffic between Intranet and Internet. For browsing the Web, this means that the browser does not directly access the Internet, but is routed via a Web proxy within the DMZ. This proxy controls the traffic from and to the Internet (cf. Figure 2).

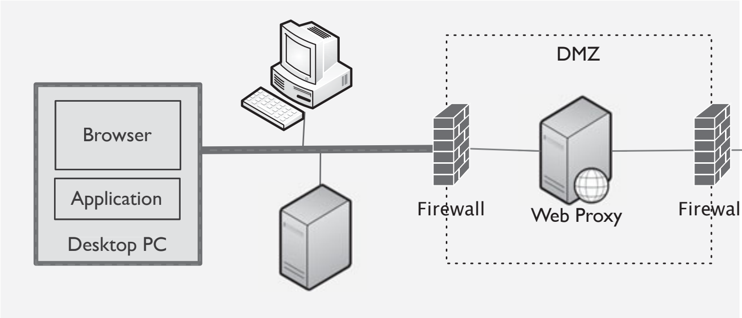


Fig. 2: The Web traffic is controlled and filtered by a proxy within the DMZ.

With this setup it is possible to centrally monitor all Internet traffic for malware and to filter active content from the traffic to protect the Intranet. How effective this protection is, crucially depends on the detection rate of the employed malware scanner in the proxy. This class of security measures is at most effective for the detection of well-known threats, but is ineffective for novel attacks, so called “zero day exploits”.

With respect to filtering active content the administrator constantly has to deal with the trade-off between usability and security. A very secure setting, like filtering all active content, may render many Web sites useless, and thus has a decisive impact on the productive usage of the Internet. To maintain productivity it is likely that a more liberal setting has to be chosen, which than has severe security drawbacks. Additionally to the malware scanners on the proxy, there are scanners on the desktop PCs themselves. For these the same rational applies as for the proxy, with respect to the detection rate and the ineffectiveness against zero day exploits.

To support mobile use, two variants are possible. By using VPN the laptop can be connected with the internal network and from there the usual proxy / firewall settings are applied. An issue with this setup are mobile Web-based Wi-Fi hotspots, like in cafes, hotels, train stations or airports. To connect to the Wi-Fi hotspot a browser is needed in the first place. Only after the successful browser based login to the hotspot, the Internet connection and the VPN connection can be established. One faces a chicken / egg problem. Without a browser, no VPN (because one has to login into the hotspot), and without a VPN, no browsing (and thus no possibility to log into the hotspot). To remedy the situation the support for Wi-Fi hotspot can be turned down completely. Then mobile access is limited to other technologies like UMTS. The alternative is to allow Internet access without the use of the central firewall and proxy in the mobile use case. The remote firewall should then be replaced by a "client firewall" on the mobile PC itself. It has to be ensured that the security policy of the client firewall matches the policy of the central firewall, to keep the additional security risk tolerable.

Pros:

- Can be enforced centrally
- Easy to use

Cons:

- Hard to deal with the trade-off between usability and security
- Ineffective against zero day exploits
- Issue with Wi-Fi hotspot in mobile scenarios
- Threat to compromise whole infrastructure in case of an malware infection

3.5 Protection via Browser Settings and Sandboxing

The browser manufactures are aware of the threats of the Internet and constantly try to improve the security of their browsers. All browsers offer settings to configure and restrict the use of active content. Here one faces the same trade-off between security and usability as in case of the proxy / firewall solution. In this context browsers offer a "zone" concept, to allow different security settings depending on the classification of the Website with respect to its trustworthiness. However, these zone models can be circumvented by attacks like "cross-site-scripting" which exploit vulnerabilities in Web browsers and Web servers to inject non-trustworthy content into trustworthy sites.

Another attempt of the browser manufacturers to increase security is the implementation of sandboxing mechanisms, which aim to confine the potential damage of malware. The term sandboxing does not refer to a uniform solution, but is a combination of various mechanisms offered by the operating system. For example, the separation of the browser into different operating system processes, or the restriction of the permissions of the browser. With those mechanisms it can be prohibited that active content in the browser can create or open files on the PC. Unfortunately this kind of sandboxing only provides limited security as it is regularly broken by malware. [2]

In general sandboxing suffers from the complexity of the browser as well as the underlying operating system. One tries to secure each individual functionality of a modern browser with a dedicated sandboxing mechanism offered by the operating system. In this complex setting it is

[2] http://www.heise.de/newsticker/meldung/Google-Chrome-auf-Ansage-geknackt-1434161.html, http://www.heise.de/newsticker/meldung/Pwn2own-Wettbewerb-Safari-IE8-und-Firefox-gehackt-207855.html

not surprising that there are always new vulnerabilities and possible attacks, as the sandboxing mechanisms do not provide an effective isolation of the complete browser at once, but try to individually secure each single functionality of the browser.

For mobile use this solution has no restriction, because all mechanisms work locally in the browser anyway.

Pros:

- No additional costs
- Good usability
- No restriction for mobile use

Cons:

- Low level of security
- Hard to manage trade-off between security and Web functionality
- Sandboxing regularly gets broken
- Threat for the complete infrastructure in case of an malware infection

3.6 Live CD with Web Browser

The idea of a live CD for Web browsing is to shutdown the PC and reboot the system directly from a CD[3]. The booted system is equipped with a browser and is configured such that it does not access the hard drive of the PC. If this protection of the hard drive is not circumvented, malware cannot persistently infect the system, as there is no means to write the CD itself. Such a live CD can be based on a free system like Linux to avoid additional costs for software licences.

The Web functionality is not restricted by this approach, but the overall usability is poor as it is not possible to simultaneously browse the Web and use the same PC for working. This approach does not provide any isolation of the Intranet and the Internet. During a Web session active malware can access the Intranet resources and can cause damage there. Here additional security measures have to be in place.

This approach is suitable for mobile use.

Pros:

- Easy to setup
- Mobile use possible

Cons:

- Limited usability, as no simultaneous browsing and working is possible
- Security level only acceptable when additional security measures for network isolation are in place

[3] https://www.bsi.bund.de/DE/Themen/ProdukteTools/SecuritySurfCD/securitysurfcd_node.html

3.7 Isolation of Browser via Virtualisation

This approach follows the idea of physical isolation, but implements it via virtualisation [GoeSeSchi11, So11, WeSchi11, Schi13]. Instead of a separated PC for Internet browsing a virtual PC is created on the desktop PC (cf. Figure 3). With virtualisation two isolated workspaces are provided on the same hardware, one for browsing the Web, and one for working. While the ordinary applications are directly executed on the operating system, the browser is executed within a virtual machine, which has a separate operating system. The virtualisation layer governs all accesses to the hardware. The operating system and the browser executed in the virtual machine have no direct access to the bare hardware, but only to the virtualised hardware. Thus the browser is confined in the virtual machine and isolated from the rest of the system.

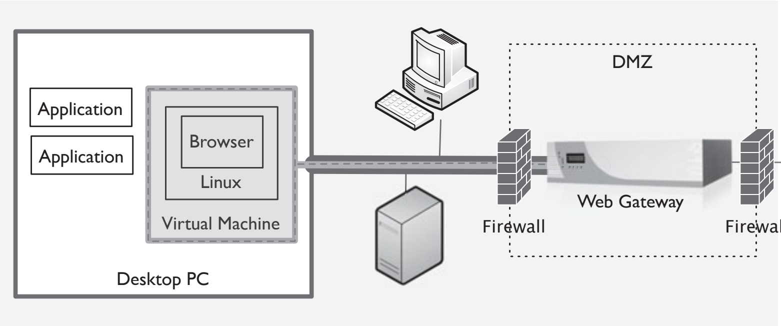


Fig. 3: Browser in the Box: the browser is isolated by virtualisation, the network is isolated by VPN

While the security properties of the isolated physical Internet PC are preserved, the usability is improved significantly, as the virtualised browser can be used like any application on the desktop PC. Active content can be offered unrestricted, as potential damage of malware only affects the virtual machine and not the desktop PC itself.

As the virtual machine has its own operating system, additional security measures are straightforward. Firstly, a heterogeneous environment is achieved by using different operating systems in the virtual machine and the desktop PC. For example Linux can be used in the virtual machine on a Windows PC. Attacks against windows are futile in the Linux virtual machine. Moreover, the operating system in the virtual machine can be minimized and hardened as its only purpose is to run the browser. Thereby the attack surface can be reduced significantly.

Besides these basic security properties, virtualisation offers new functionality which can be employed to improve security, availability and maintainability even more. As the virtualisation layer has the control over the complete virtual hardware it is possible to store and fix the complete state (memory and hard drive) of the virtual hardware. This snapshot can be used to store a clean starting state of the browser. When the browser is temporarily infected during a Web session, it can be cleaned be restoring the clean snapshot. As this reset is a lightweight operation it can be executed on every start of the browser. A recovery of an infected Internet PC or a terminal server is replaced by restarting the virtual browser.

By using virtualisation it is unnecessary to employ additional redundant hardware, which lowers the costs. In contrast to the sandboxing mechanisms of a browser, virtualisation offers strong isolation properties. Not single functions and programs are protected individually, but the complete access to the hardware is governed and isolated. The virtual browser runs on its own virtual operating system, which only has access to the hardware resources offered by the virtualisation layer. Malware can only infect the virtual environment und thus attacks are futile.

Virtualisation alone only isolates the browser from the desktop PC. However, the overall goal is to isolate the complete Intranet from the Internet. Otherwise malware could not attack the desktop PC itself, but could attack the internal infrastructure via the network. To enforce isolation of the networks the virtual browser is connected to a Web gateway via a VPN connection. Only the Web gateway has access to the Internet. With this setup the browser can only access resources from the Internet. The complete Intranet is unreachable from the browser. With this technology an isolated virtual "browser net" is created within the Intranet.

The mobile use is fully supported by this solution, as the virtualisation runs locally on the PC. Hence the browser is isolated also during mobile use. In case a VPN connection to the Intranet is established, this connection can be used to benefit from the isolation of the networks. As only ordinary Internet traffic is routed through this connection, the bandwidth issues of the terminal server solutions do not show up here. Moreover, the chicken / egg problem of the proxy / firewall solution can be solved in this approach. The virtual browser is first started to establish the Wi-Fi connection on the hotspot, afterwards a VPN connection to the Web gateway is established for continuing the browser session.

Pros:

- High security level, via multilevel security (security in the depth): isolation via virtualisation and VPN, hardened operating system in the virtual machine
- Low costs and good scalability by using client (desktop PC) resources
- High availability, recovery automatically via snapshot mechanism
- Unrestricted mobile use, with high security
- Low costs of the solution by using standard product

Cons:

- Maintenance and deployment of VMs has to be managed
- Internal Web portals (Intranet) have to use a separate browser

4 Conclusion

Table 1 summarizes the results. The viability of a solution depends on the security needs and the functional and operational requirements. Approaches where the administrator is in charge to balance the trade-off between security and usability are critical. The use of active content is already standard today and we foresee that in the future the role of active content will be even more dominant, e.g. in the upcoming era of HTML 5. A strict policy to filter all active content will therefor render most Web sites useless, and thus a productive use of the Web is not possible anymore. On the other hand the execution of active content remains a major threat to Web browsers. The table illustrates how this dilemma can be solved. To achieve an adequate level of security, while maintaining the productive use of the Web one should obey to the following rational: ***Not the browser has to be secured against attacks from the Web, but the rest of the system and infrastructure has to be secured against the browser going wild.*** The complexity of a modern browser offers a large attack surface, which will be exploited by malware. Hence, we recommend approaches that isolate the browser from the rest of the system. The solution to isolate the browser via virtualisation has some attractive benefits. A high level of security is achieved, while its decentralised architecture employs the computing power of the PC and simultaneously has only low bandwidth overhead on the Internet traffic. Hence the solution is also viable for challenging environments with low bandwidth connections, as in the case of mobile use or of distributed locations with branch offices.

Table 1: Comparison of Approaches

Approach	**Security**	**Web-Functionality**	**Usability**	**Mobile Use**	**Effort / Cost**	**Victims of infection**
No Internet	highest	-	-	-	-	-
Physical Isolation	very high	unrestricted	low	infeasible	very high	only Internet PCs
Terminal Server	high	minor restrictions[1]	high	infeasible	high	only terminal server
Proxy / Firewall	high – low[2]	major – minor-restrictions[2]	high	restricted[3]	medium	complete Intranet
Browser Settings / Sandboxing	low	major – minor restrictions[2]	high	unrestricted	minimal	complete Intranet
Live-CD	medium	unrestricted	low	unrestricted	low	live-system – Intranet[4]
Isolation via Virtualisation	high	unrestricted	high	unrestricted	medium	only virtual machines

1 Restrictions for multimedia content
2 Depending on configuration
3 e.g. via VPN and internal network, or via personal firewall on the laptop
4 the intranet is threatened, in case no mechanism for network isolation is implemented

References

[BSI06] Bundesamt für Sicherheit in der Informationstechnik. Remote Controlled Browser Systems (ReCoBS) – Grundlagen und Anforderungen. Version 2.0. Juni 2006.4

[GoeSeSchi11] Christoph Göricke, Marcel Selhorst , Norbert Schirmer. Browser in the Box (BITB) – Eine virtuelle Surfumgebung für Behörden, Unternehmen und Privatanwender 12th German IT Security Congress, Bonn-Bad Godesberg, Mai 2011.

[So11] Robert Sorensen. Secure Browsing Environment. SANS Institute. September 2011.

[WeSchi11] Marion Weber, Norbert Schirmer. Browser in the Box – BitBox; Safer Surfen – Freies Internet am Arbeitsplatz aber trotzdem geschützt. <kes> Die Zeitschrift für Informations-Sicherheit. Nr. 5, Oktober 2011.

[Schi13] Norbert Schirmer. Safer Surfen 3.0 – Mit neuem Ansatz zum sicheren Internetzugang. <kes> special. Die Zeitschrift für Informations-Sicherheit. Mai 2013.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?__blob=publicationFile

Security Compliance Monitoring – The next Evolution of Information Security Management?!

Marko Vogel · Vinzent Broer

KPMG AG Wirtschaftsprüfungsgesellschaft
Alfredstrasse 277
D-45133 Essen, Germany
{mvogel | vbroer}@kpmg.com

Abstract

The status of information security becomes more and more relevant for management representatives. Therefore, the information security function has to provide relevant information in a way business understands. Furthermore, the demand for accurate and timely information about security compliance or key information risks is increasing.

Normally, senior management receives nowadays feedback regarding the information security status based on different heterogeneous ways like internal/external audit reports, self assessment reports, control assessment reports or specific system reporting.

SCM is a tool-based approach that correlates security information from different sources, assesses this information based on relevant controls, enriches the results with business context information, and provides meaningful views to stakeholders for making an informed decision.

The paper describes the methodology for security compliance monitoring as well as technical aspects like an overall architecture. In addition to describing each component in detail, the paper outlines a use case for a complex risk-based control example in the telecommunication industry and how SCM has been used to address this management issue.

1 Introduction

The increasing risk due to information security related incidents becomes more and more important for senior management representatives of most organisations. An increasing number of data loss incidents – as one type of security related incidents – illustrates the trend of higher probability of such events (see Fig. 1). There is not one day a newspaper or online headline is not reporting about such an event anymore.

Furthermore, the type of attacks are becoming more focused and sophisticated. The most recent Symantec Internet Security Threat Report reveals – amongst others – the following highlights (see [Syma13]):

- 42% increase in targeted attacks in 2012
- 31% of all targeted attacks aimed at businesses with less than 250 employees

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_16, © Springer Fachmedien Wiesbaden 2013

- Spam volume continued to decrease, with 69% of all email being spam
- 5,291 new vulnerabilities discovered in 2012, 415 of them on mobile operating systems

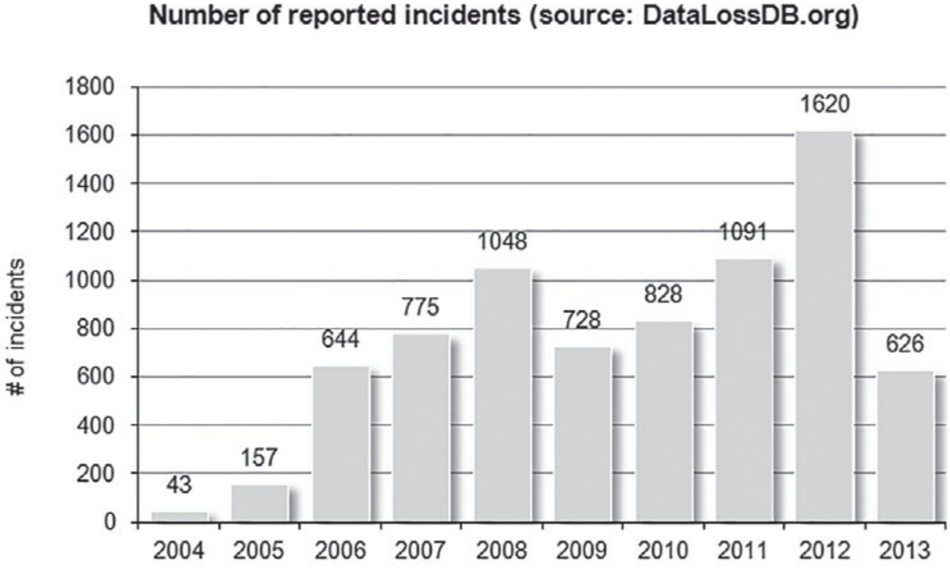


Fig. 1: Data loss incidents [Data13]

But the reason for most incidents is still a lack of enforcement of basic security controls.

The following table summarizes the most frequently reasons for failure in the area of information security as published by the German Federal Office for Information Security (see also [BuSI12]):

Table 1: Most recent security failures of organisations

Reason	Description
Poor information security management	• Strategic importance of information security is not understood • Processes to maintain a security status are not established • Security policies are not documented • Monitoring and detective controls are not in place
Poor configuration of IT systems	• Access rights are not restricted accordingly • IT systems are not configured properly
Unsecure network and internet connection	• Sensitive systems are not separated adequately from open networks
Inobservance of security requirements	• Security countermeasures are neglected for comfort reasons • Users and administrators are not trained sufficiently
Poor system maintenance	• Available patches are not installed
Incautious use of passwords and security features	• Passwords are used incautious • Available security features are not used
Poor protection against theft and natural hazard	• Facilities and IT systems are poorly protected against theft and natural hazard

These facts stress the importance of an accurate and timely management reporting of the status of information security within an organisation.

2 Current Status of Information Security Reporting

In most organisations information security reporting about the current compliance status of IT systems and relevant high risks is done in a very heterogeneous way. Information about the compliance status of an IT system is normally provided to management in form of system audits, self assessment reporting, control assessment reporting or topic-specific system reporting. All of these reporting methods have their strength and weaknesses:

- While **audits** provide a high quality of analysis and reporting they are normally focused only on a limited scope (one or a few systems or processes). Furthermore, audits are mostly based on manual activities and are therefore time and resource consuming.
- **Self Assessment Reporting** is normally based on maturity models and/or check lists. Self assessments can cover a broader scope like the entire organization, but are limited in depth of assessment as only some high level questions are answered by responsible subject matter experts. This type of information gathering is – like for audits – a point in time assessment. Furthermore, KPGM's project experience shows that the quality of results is low as most stakeholders are too optimistic or try to show good performance within their area of responsibility.
- **Control Assessment Reporting** e.g. as part of SOX testing. Control assessments are in most cases only implemented in the area of "internal controls over financial reporting" and based on pre-defined activities including spot checks to assess the effectiveness of relevant controls. The quality of results is high and normally covering a defined time period e.g. current year, but these assessments are also only performed once or a few times a year.
- **Regular, topic-specific System Reporting:** Many systems or security tools create their own reporting that provide only detailed – and most times technical – information, not intended to be presented to a senior management audience. The scope is limited and reporting is system specific, not addressing the complexity of most risk scenarios.

Based on our discussions with management representatives of different organisations we have identified certain typical requirements regarding security compliance reporting that are not sufficiently addressed by the aforementioned methods:

- Accurate information about the security compliance status
- Continuous monitoring of compliance to ensure 100% effectiveness over time
- (Near) real-time detection of non-compliance status
- Ability to report defined risk scenarios involving multiple IT systems

The following figure illustrates relevant characteristics of reporting methods and compares it with the "security compliance monitoring"-approach (SCM) as described in more detail in the following sections.

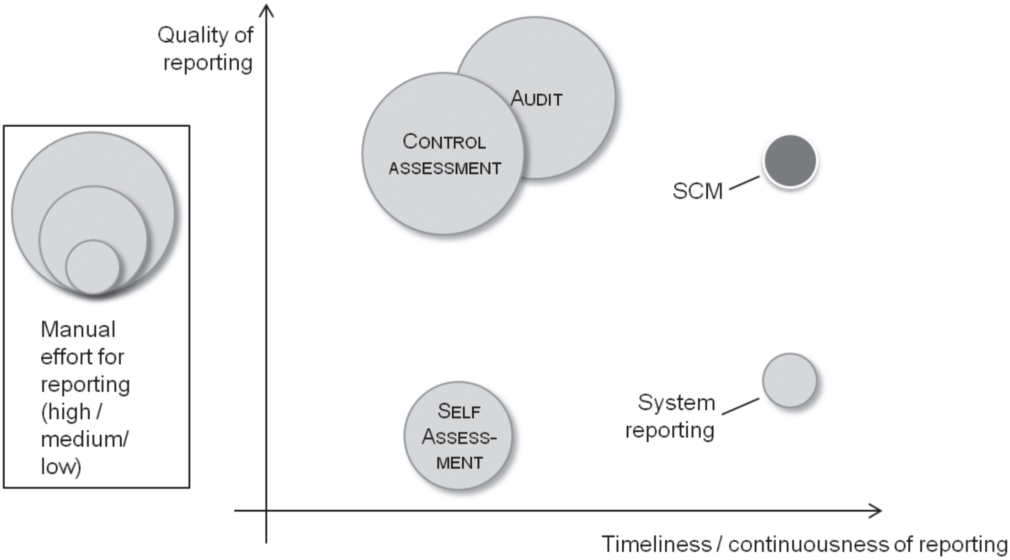

Quality of reporting
Audit
Control assessment
SCM
Manual effort for reporting (high / medium/ low)
Self Assess-ment
System reporting
Timeliness / continuousness of reporting

Fig. 2: Comparison of reporting methods

3 Security Compliance Monitoring (SCM)

SCM is a tool-based approach that correlates security information from different sources, assesses this information based on relevant controls, enriches the results with business context information, and provides meaningful views to stakeholders for making an informed decision. SCM is another step to transform information security from a technical domain into a process management domain by using similar approaches and techniques.

SCM is designed to monitor and evaluate the status of security controls based on IT system data related to the following key domains as outlined in Table 2:

Table 2: SCM domains

Domain	Description
Compliance	Controls of this domain are related to compliance with legal and regulatory requirements or applicable standards (like ISO/IEC 27002) and internal policies. Controls in this area cover typically aspects like secure system configuration, appropriate patch level and access related controls.
Risk Management	Controls of this domain address critical risk scenarios spanning information from multiple systems. A typical example is discussed in more detail in section 5.
Performance	Controls of this domain monitor performance related security parameter like SLAs in outsourcing scenarios.

Fig. 3 outlines the four main elements of the SCM approach. Key aspects of each are described in more detail in the following sections.

The module *Collector* (see section 3.1 for more details) collects all required information from IT systems and applications such as SAP, Oracle databases or MS Windows servers and sends them to the central analyses server. The module *Controls* allows the definition of standard controls including the related audit procedure and detailed checks (see section 3.2 for more details). The module *Analytics* (see section 3.3 for more details) is the core component and evaluates the collected system information based on the corresponding control definitions and provides the control results to the *Reporting* module. The *Reporting* module provides detailed reports on the one hand and a dashboard on the other hand (see section 3.4 for more details).

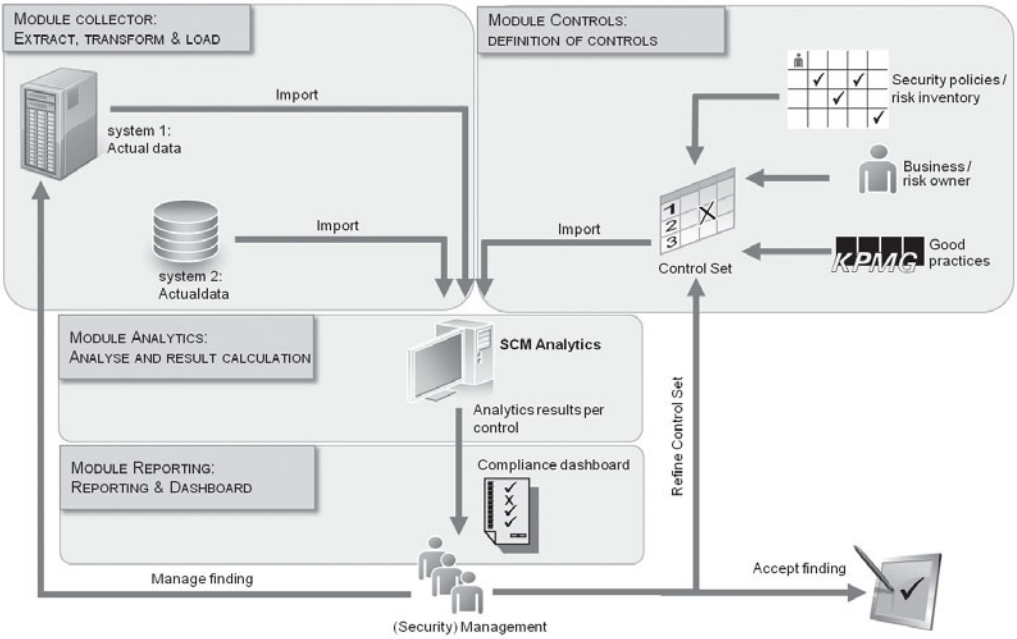


Fig. 3: Overview SCM modules

What does SCM differentiate from other security tools?

While most security tools are designed for a special technical security capability (see Table 3 for an overview of typical security capabilities including a mapping to tools) SCM is designed to correlate security related information from different sources and evaluate against business focused security controls.

Table 3: Mapping of security capabilities and tools

Technical security capabilities	**SIEM tool**	**IDS / IPS tool**	**Vulnerability scanner**
Analysis of system configuration	-	-	-
Analysis of log data	X	-	-
Analysis of network data	-	X	-
Vulnerability analysis	-	-	X
Detection of cyber attacks	X	X	-

Fig. 4 summarizes the context and key data sources for SCM. While SCM has its own reporting capabilities it is not limited to those. All relevant information can also be provided to other management reporting tools like GRC tools.

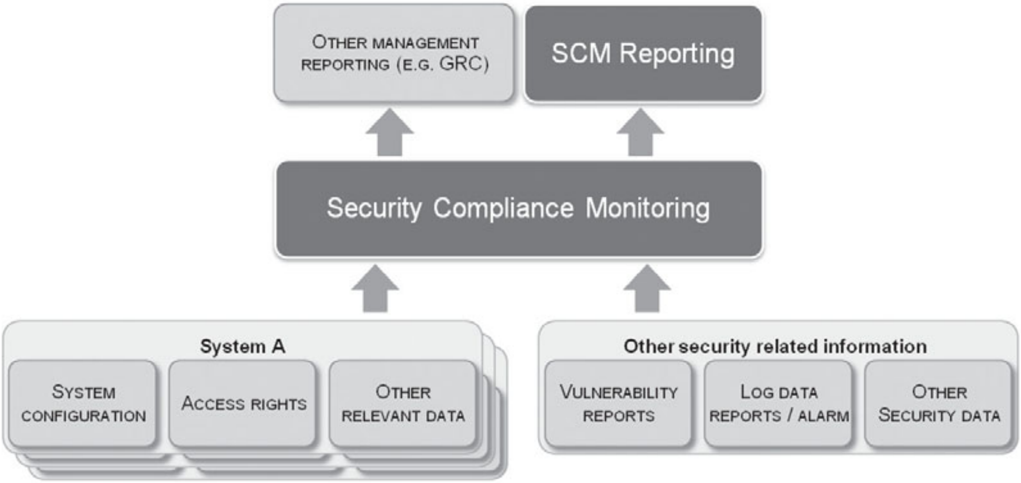


Fig. 4: SCM context

3.1 Module Collector

The *SCM Host Collector* performs the necessary tasks on the host system. It controls the scripts and modules designed to gather data from a distinct application (e.g. SAP) or database (e.g. Oracle). The *SCM Host Collector* receives a system specific property file defining the structure of the target system and related data. Once all data is collected the module creates a file that is sent via FTPS. Based on this generic structure the *Collector* can collect all types of data or reports from different systems including other security tools.

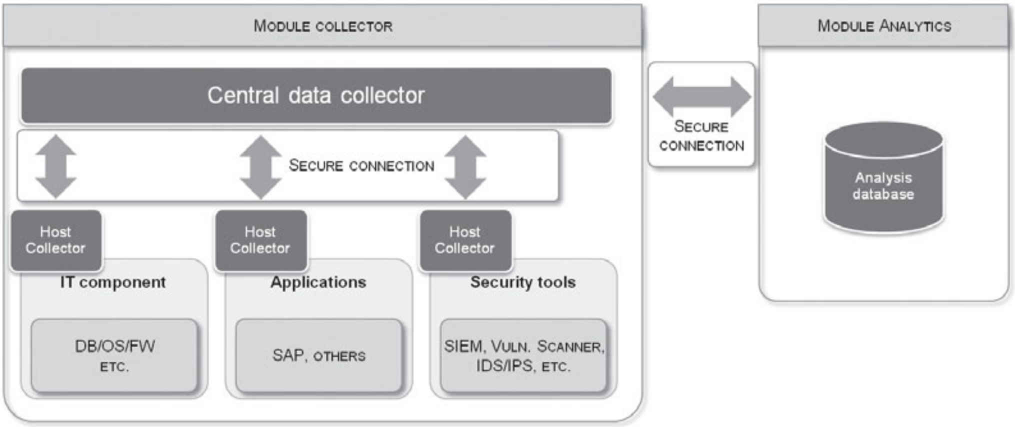


Fig. 5: Collector overview

3.2 Module Controls

This module is used to define the relevant controls to be monitored. It includes a pre-defined set of controls e.g. controls for SOX compliance for SAP ERP systems. Those types of controls are defined based on a pre-defined structure including the target value, risk descriptions, control objective and recommendations (see Table 4 for an example).

Table 4: Control example

Control element	Description
Risk	Unauthorized/inappropriate access to the organization's relevant financial reporting applications or data.
Control objective	Logical access to IT computing resources is appropriately restricted by the implementation of authentication mechanisms. A minimum rule set for passwords ensures the necessary complexity to determine the authenticity of a user and provides individual accountability.
Target value	Minimum password length: 8 Acceptable password change interval: 90 days Password Syntax rules: Minimum required character combination (letter/number/special characters) -> 2 out of 3 Prohibited password: Company name, ...
Recommendation	Set the password rules to the following minimum target values to prevent unauthorized/inappropriate access to the organization's relevant financial reporting applications or data: See list of target values above

Furthermore, this module allows the definition of more complex controls covering data of multiple systems. The following risk scenario illustrates the use of such controls:

Traders in banks have to take holidays to prevent fraudulent activities. During their holiday they should not be able to access their systems. This ensures that they do not continuously manipulate their trades to hide fraudulent activities.

This control could be implemented by

1. Checking that they take holidays (in the HR system), and
2. Are not able to access the premises during that time (check in the physical access control system), and
3. Do not have remote access during that time (check the remote access system or web application system), and
4. Do not have primary access during that time (normally check the active directory system for windows logon)

These types of controls are complex and must be tailored to the individual risk scenario and IT environment of the organisation (see section 5 for another detailed use case description).

3.3 Module Analytics

The module *Analytics* uses the input from the module *Collector* (actual data) and from the module *Controls* (target values) to assess the control result for each system or system component (e.g. application, database, operating system). The module *Analytics* allows the processing of control assessments in three tiers: 1 – control, 2 – audit procedure, 3 – check. A control can have one or more audit procedures and every audit procedure can have several checks. Based on this structure it is possible to analyse even complex risk scenarios.

The following list illustrates some of the necessary steps for the aforementioned control example "password complexity". Be aware that these steps are SAP specific due to the specific configuration of SAP:

1. Audit procedure 1: minimum length
    a. Check existence of a user defined value and compare with target value. If there is no user defined value
    b. Check existence of system default value and compare with target value
2. Audit procedure 2: password change interval
    a. Check ...

For compliance related controls the result on the different levels is normally binary, e.g. either the password length is greater than or equal to the target value or not. If all mandatory checks are true the audit procedure is true. The control is true if all mandatory audit procedures are true.

In addition to this binary model more complex models to evaluate controls are reasonable, e.g. the actual value is scored against a threshold model and mapped to a standardized assessment scheme e.g. traffic light scheme with three different states (red, amber, green).

3.4 Module Reporting

The module *Reporting* basically provides two different types of reporting:

1. Dashboard
   The objective of the dashboard is to provide an **aggregated view** of the detailed information to relevant stakeholder **to support decision making**. Depending on the stakeholder different views with different information and level of detail are necessary.
2. Report
   The objective of the Reports is to provide detailed information about controls, their results including risks, actual vs. target values, recommendations, etc. per relevant entity (e.g. one/multiple system; subset of controls per compliance domain, etc.).

The following part focuses on key aspects for dashboard views.

The key input for the module *Reporting* is the result of a control analysis per IT system or component. Aspects of historical information and trend analysis are not discusses in this paper.

A first key item is to add other relevant structural information like organisational structure, IT process structure, etc. to be able to put the input into relevant context.

Another key aspect is to define an aggregation model. This model defines how a single control result for a single IT component is aggregated to e.g. a system result, a technology domain result, a security domain result, an overall organisation result. A typical aggregation model is based on weighting factors to calculate a weighted average score for the next level (e.g. ten controls are performed for an IT system. Each control result is considered with the factor 10% (weighting factor) for the overall IT system score).

In addition, to be able to use the aggregation model consistently across all levels and views a consistent scoring model is necessary. A well-known score model is 1-3 for a traffic light scheme with three different states (red, amber, green). Thresholds are used to map control results to this score model (e.g. for the aforementioned example the thresholds might be: green – not more than one IT system control is failing; amber – 2 to up to 4 system controls are failing; red – more than 4 system controls are failing).

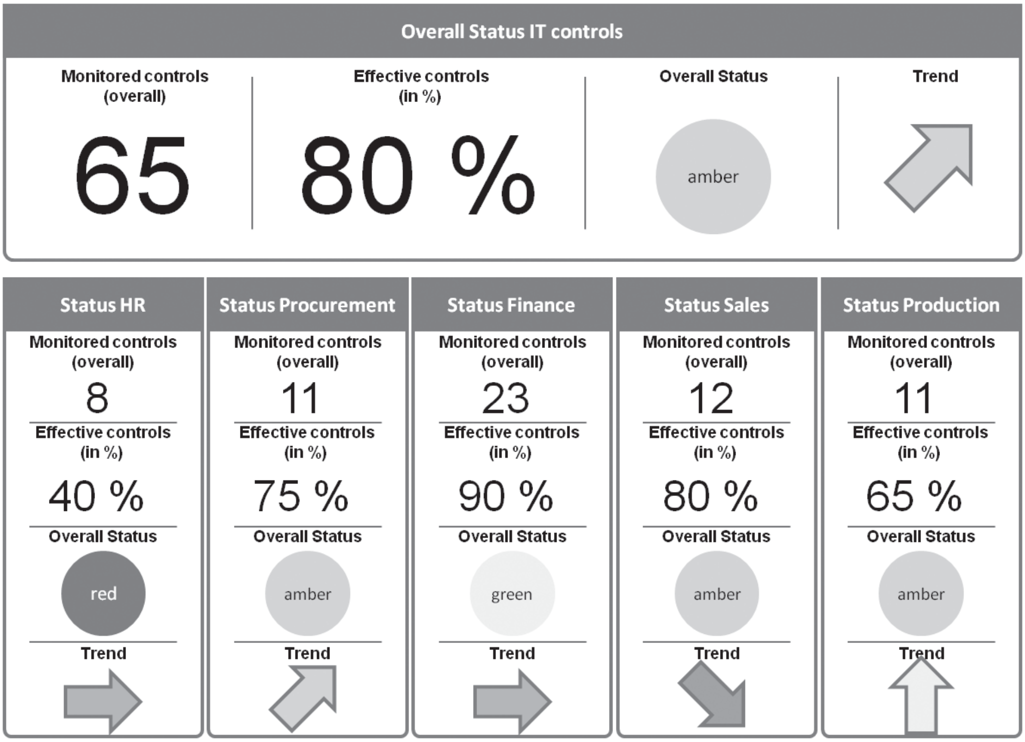
The scoring model and the aggregation model has to be discussed with the organisations' stakeholders as it reflects the priorities (aggregation model) and risk appetite (scoring model) of the organisation. Based on our experience it is important that the initial models are reviewed after 6 month as stakeholders need some experience with those models and the related consequence.

The last aspect discussed in this paper is the need for customized and focused views per stakeholder. The following table outlines key aspects for different stakeholders relevant for their views.

Table 5: Stakeholder and views (examples)

Stakeholder	View (key aspects)
Chief Information Security Officer (CISO)	The CISO is interested in the overall status of all information security related controls across the entire organisation. His view might be based on the ISO/IEC 27002 control framework. Relevant drill downs for him are Organisational based (e.g. per business unit, service provider, legal entity), or Security domain based (e.g. per control domain of ISO/IEC 27002), or Technology group based (e.g. per technology domain like applications, database, operating system, network, client/mobile, etc.)
Chief Financial Officer (CFO)	The CFO is interested in the overall status of all SOX (Sarbanes-Oxley Act) related controls across the entire organisation. His view might be based on the COBIT control framework (Control Objectives for Information and Related Technology). Relevant drill downs for him are Organisational based (e.g. per SOX-relevant business unit, service provider, legal entity), or Control domain based (e.g. per control domain of COBIT), or Technology based (e.g. per simplified technology domain like applications vs. IT Infrastructure)
Chief Information Officer (CIO)	The CIO is interested in the overall status of all IT related controls across the entire IT landscape. Relevant drill downs for him are Control framework based (e.g. SOX; COBIT, ISO/IEC 27002, privacy framework, PCI DSS (Payment Card Industry – Data Security Standard), or Process based (e.g. per IT process like change management, configuration management), or Technology group based (e.g. per technology domain like application, database, operating system, network, client/mobile, etc.)
Process Manager "Change Management"	The Process Manager "Change Management" is interested in the overall status of all change management related controls across the entire IT landscape. Relevant drill downs for him are Control based (e.g. per change management control), or Technology based (e.g. per technology domain like application, database, operating system, network, client/mobile, etc.), or System based (e.g. per critical system)
Manager "database services"	The Manager "database services" is interested in the overall status of all database related controls across the entire IT landscape. Relevant drill downs for him are Control based (e.g. per database control), or System based (e.g. per (critical) Database Management System)

The example dashboard in Fig. 6 illustrates one organisational view and key information. It provides the status of all 65 SOX relevant IT controls for the organisation including a traffic light indicator (overall status) and trend information. The drill down is per organisational unit and allows the stakeholder to identify relevant areas of concern. In this case the HR department has to take actions to improve the compliance status. Further drill downs are available to identify the relevant control area or IT system (not included in Fig. 6).



Overall Status IT controls

Monitored controls (overall)	Effective controls (in %)	Overall Status	Trend
65	80 %	amber	↗

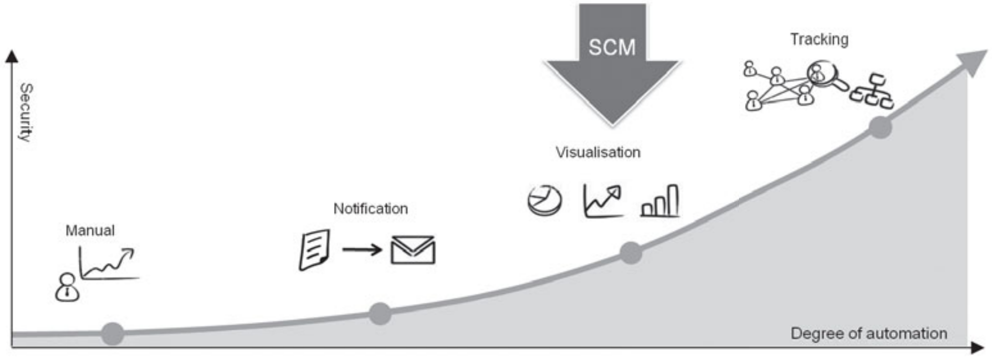
	Status HR	Status Procurement	Status Finance	Status Sales	Status Production
Monitored controls (overall)	8	11	23	12	11
Effective controls (in %)	40 %	75 %	90 %	80 %	65 %
Overall Status	red	amber	green	amber	amber
Trend	→	↗	→	↘	↑

Fig. 6: Dashboard example – organisational view

4 Maturity Model for Security Monitoring and Reporting

Typically, organisations mature over time with respect to security compliance monitoring. KPMG has developed a maturity model to assess the current state, and define the future state of monitoring and reporting capabilities.

Fig. 7 illustrates this maturity model and ranks SCM within that model. Key aspects of SCM's maturity level are strong visualisation capabilities with the ability to drill down to a level of detail the stakeholder feels comfortable with and comprehensive views and analytical capabilities, e.g. across systems or system independent views.



- Manual data extraction and analysis
- Manual reporting and tracking
- Manual escalation
- Initiated based on incidents or ad hoc inquiries

- Automatic data extraction and analysis
- Automatic reporting and report distribution per Email (e.g. excel ,pdf)
- Detailed level and silo view
- Manual tracking and escalation

- Visualisation and benchmarking
- Drill down to detailed levels
- Self service BI capabilities
- Comprehensive views and analysis capabilities
- Manual tracking and escalation

- Complete integration (e.g. incident management process)
- End-2-end process enforcement and reporting
- Tool-based tracking and escalation

Fig. 7: Maturity model

5 Use Case

A strong motivation for the development of the SCM approach and related tools was the need of KPMG's clients to monitor and analyse critical risk scenarios across systems in near real time. The following use case demonstrates the use of SCM in such a scenario:

Telecommunication industry:

Call centre agents are dealing with customers and have therefore access to CRM systems (Customer Relationship Management) with sensitive customer information such as contract or contact related information. Especially the contract end date is valuable information for competitors in this industry.

Opening a customer file is daily business for call centre agents as part of their daily routine. Therefore, monitoring access to and within the CRM system alone for identifying inappropriate access to customer information is not enough. A review of the process itself helps to detect better control mechanisms. Normally, a customer is calling the call centre to address an issue. His call is routed via the CTI system (Computer Telephony Integration) to a specific available call centre agent. The call centre agent is using the CRM system to support the customer e.g. opening a ticket or documenting the activities for further reference (see also Fig. 8*).*

According to this process description, the following (simplified) SCM control could be designed: For each event of opening a customer file in the CRM system by an agent a corresponding call event in the CTI system for this agent should exist. SCM correlates those events in near real time, and detects and reports agents accessing large number of customer files without having a corresponding call. This approach helps to identify potential privacy incidents and decreases the financial risk significantly.

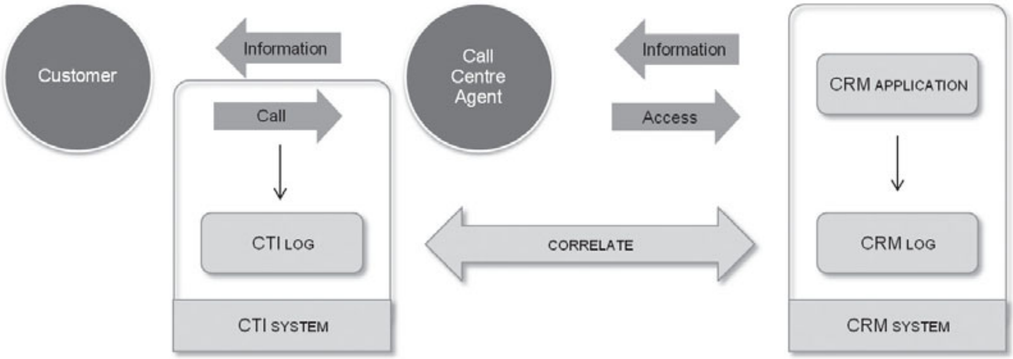


Fig. 8: Use case telecommunication industry

6 Conclusion

The status of information security becomes more and more relevant for management representatives. Therefore, the information security function has to provide relevant information in a way business understands. Furthermore, the demand for accurate and timely information about security compliance or key information risks is increasing.

SCM is a tool-based approach that correlates security information from different sources, assesses this information based on relevant controls, enriches the results with business context information, and provides meaningful views to stakeholders for making an informed decision. Basically, SCM is another step to transform information security from a technical domain into a process management domain by using similar approaches and techniques.

References

[BuSI12] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany): Leitfaden Informationssicherheit (Guideline Information Security), Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2012

[Data13] Dataloss.org: Data Loss Statistics, http://datalossdb.org/statistics, 2013

[Syma13] Symantec: Internet Security Threat Report, Symantec, Mountain View, 2013 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Cybersecurity, Cybercrime, Critical Infrastructures

Digital Forensics as a Big Data Challenge

Alessandro Guarino

StudioAG
a.guarino@studioag.eu

Abstract

Digital Forensics, as a science and part of the forensic sciences, is facing new challenges that may well render established models and practices obsolete. The dimensions of potential digital evidence supports has grown exponentially, be it hard disks in desktop and laptops or solid state memories in mobile devices like smartphones and tablets, even while latency times lag behind. Cloud services are now sources of potential evidence in a vast range of investigations and network traffic also follows a growing trend and in cyber security the necessity of sifting through vast amount of data quickly is now paramount. On a higher level investigations – and intelligence analysis – can profit from sophisticated analysis of such datasets as social network structures, corpora of text to be analysed for authorship and attribution. All of the above highlights the convergence between so-called data science and digital forensics, to tack the fundamental challenge of analyse vast amount of data ("big data") in actionable time while at the same time preserving forensic principles in order for the results to be presented in a court of law. The paper, after introducing digital forensics and data science, explores the challenges above and proceed to propose how techniques and algorithms used in big data analysis can be adapted to the unique context of digital forensics, ranging from the managing of evidence via Map-Reduce to machine learning techniques for triage and analysis of big forensic disk images and network traffic dumps. In the conclusion the paper proposes a model to integrate this new paradigm into established forensic standards and best practices and tries to foresee future trends.

1 Introduction

1.1 Digital Forensics

What is digital forensics? We report here one of the most useful definitions of digital forensics formulated. It was developed during the first Digital Forensics Research Workshop (DFRWS) in 2001 and it is still very much relevant today:

> *Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.[Pear01]*

This formulation stresses first and foremost the scientific nature of digital forensics methods, in a point in time when the discipline was transitioning from being a "craft" to an established field and rightful part of the forensic sciences. At that point digital forensics was also transitioning from being mainly practised in separated environments such as law enforcement bodies and enterprise audit offices to a unified field. Nowadays this process is very advanced and it can be

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_17, © Springer Fachmedien Wiesbaden 2013

said that digital forensics principles, procedures and methods are shared by a large part of its practitioners, coming from different backgrounds (criminal prosecution, defence consultants, corporate investigators and compliance officers). Applying scientifically valid methods implies important concepts and principles to be respected when dealing with digital evidence. Among others we can cite:

- Previous validation of tools and procedures. Tools and procedures should be validated by experiment prior to their application on actual evidence.
- Reliability. Processes should yield consistent results and tools should present consistent behaviour over time.
- Repeatability. Processes should generate the same results when applied to the same test environment.
- Documentation. Forensic activities should be well-documented, from the inception to the end of evidence life-cycle. On one hand strict chain-of-custody procedures should be enforced to assure evidence integrity and the other hand complete documentation of every activity is necessary to ensure repeatability by other analysts.
- Preservation of evidence – Digital evidence is easily altered and its integrity must be preserved at all times, from the very first stages of operations, to avoid spoliation and degradation. Both technical (e.g. hashing) and organizational (e.g. clear accountability for operators) measures are to be taken.

These basic tenets are currently being challenged in many ways by the shifting technological and legal landscape practitioners have to confront with. While this paper shall not dwell much on the legal side of things, this is also obviously something that is always to be considered in forensics.

Regarding the phases that usually make up the forensic workflow, we refer here again to the only international standard available[ISO12] and describe them as follows:

- Identification. This process includes the search, recognition and documentation of the physical devices on the scene potentially containing digital evidence.[ISO12]
- Collection – Devices identified in the previous phase can be collected and transferred to an analysis facility or acquired (next step) on site.
- Acquisition – This process involves producing an image of a source of potential evidence, ideally identical to the original.
- Preservation – Evidence integrity, both physical and logical, must be ensured at all times.
- Analysis – Interpretation of the data from the evidence acquired. It usually depends on the context, the aims or the focus of the investigation and can range from malware analysis to image forensics, database forensics, and a lot more of application-specifics areas. On a higher level analysis could include content analysis via for instance forensics linguistics or sentiment analysis techniques.
- Reporting – Communication and/or dissemination of the results of the digital investigation to the parties concerned.

1.2 Data Science

Data Science is an emerging field basically growing at the intersection between statistical techniques and machine learning, completing this toolbox with domain specific knowledge, having as fuel big datasets. Hal Varian gave a concise definition of the field:

[Data science is] the ability to take data – to be able to understand it, to process it, to extract value from it, to visualize it, to communicate it.[Vari09]

We can see here the complete cycle of data management and understand that data science in general is concerned with the collection, preparation, analysis, visualization, communication and preservation of large sets of information; this is a paraphrase of another insightful definition by Jeffrey Stanton of Syracuse University School of Information Studies. The parallels with the digital forensics workflow are clear but the mention in both definition of visualization deserves to be stressed. Visualization is mostly never mentioned in digital forensics guidelines and standards but as the object of analysis move towards "Big Data", it will necessarily become one of the most useful tools in the analyst's box, for instance in the prioritization phase but also for dissemination and reporting: visual communication is probably the most efficient way into a human's brain but this channel is underused by most of today forensic practitioners.

If Data Science is concerned with "Big Data", what is Big Data anyway? After all big is a relative concept and prone to change with time. Any data that is difficult to manage and work with, or in other words datasets so big that for them conventional tools – e.g. relational databases – are not practical or useful.[ISAC13] From the point of view of data science the challenges of managing big data can be summarized as three Vs: Volume (size), Velocity (needed for interactivity), Variety (different sources of data). In the next paragraph we shall see how this three challenges dovetail nicely with the digital forensics context.

2 Challenges

"Golden Age" is a common definition for the period in the history of digital forensics that went roughly from the 1990s to the first decade of the twenty-first century. During that period the technological landscape was dominated by the personal computer, and mostly by a single architecture – x86 plus Windows – and data stored in hard drives represented the vast majority of evidence, so much so that "Computer Forensics" was the accepted term for the discipline. Also the storage size allowed for complete bitwise forensic copies of the evidence for subsequent analysis in the lab. The relative uniformity of the evidence nature facilitated the development of the digital forensic principles outlined above and enshrined in several guidelines and eventually in the ISO/IEC 27037 standard. Inevitably anyway they lagged behind the real-world developments: recent years brought many challenges to the "standard model", first among them the explosion in the average size of the evidence examined for a single case. Historical motivations for this include:

- A dramatic drop of hard drives and solid state storage cost (currently estimated at $80 per Terabyte) and consequently an increase in storage size per computer or device;
- Substantial increase in magnetic storage density and diffusion of solid-state removable media (USB sticks, SD and others memory cards etc) in smartphones, notebooks, cameras and many other kinds of devices;
- Worldwide huge penetration of personal mobile devices like smartphones and tablets, not only in Europe and America, but also in Africa – where they constitute the main communication mode in many areas – and obviously in Asia;
- Introduction and increasing adoption by individuals and businesses of cloud services – Infrastructure services (IAAS), platform services (PAAS) and applications (SAAS) – made possible in part by virtualization technology enabled in turn by the modern multi-core processors;

- Network traffic is ever more part of the evidence in cases and the sheer size of it has – again – obviously increased in the last decade, both on the Internet and on 3G-4G mobile networks, with practical but also ethical and political implications;
- Connectivity is rapidly becoming ubiquitous and the "Internet of things" is near, especially considering the transition to IPv6 in the near future. Even when not networked, sensors are everywhere, from appliances to security cameras, from GPS receivers to embedded systems in cars, from smart meters to Industrial Control Systems.

To give a few quantitative examples of the trend, in 2008 the FBI Regional Computer Forensics Laboratories (RCFLs) Annual Report[FBI08] explained that the agency's RCFLs processed 27 percent more data than they did during the preceding year; the 2010 Report gave an average case size of 0.4 Terabytes. According to a recent (2013) informal survey among forensic professionals on Forensic Focus, half of the cases involve more than on Terabyte of data, with one in five over five Terabytes in size.

The simple quantity of evidence associated to a case is not the only measure of its complexity and the growing in size is not the only challenge that digital forensics is facing: evidence is becoming more and more heterogeneous in nature and provenience, following the evolving trends in computing. The workflow phase impacted by this new aspect is clearly analysis where, even when proper prioritization is applied, it is necessary to sort through diverse categories and source of evidence, structured and unstructured. Data sources themselves are much more differentiated than in the past: it is common now for a case to include evidence originating from personal computers, servers, cloud services, phones and other mobile devices, digital cameras, even embedded systems and industrial control systems. File formats

3 Rethinking Digital Forensics

In order to face the many challenges but also to leverage the opportunities it is encountering the discipline of digital forensics have to rethink in some ways established principles and reorganize well-known workflows, even include and use tools not previously considered viable for forensic use – concerns regarding the security of some machine learning algorithms has been voiced, for instance in [BBC+08]. On the other hand forensic analysts' skills need to be rounded up to make better use of these new tools in the first place but also to help integrate them in forensic best practices and validate them. The dissemination of "big data" skills will have to include all actors in the evidence lifecycle, starting with Digital Evidence First Responders (DEFRs), as identification and prioritization will see their importance increased and skilled operators will be needed from the very first steps of the investigation.

3.1 Principles

Well-established principles shall need to undergo at least a partial extension and rethinking because of the challenges of Big Data.

- Validation and reliability of tools and methods gain even more relevance in a big data scenario because of the size and variety of datasets, coupled with the use of cutting-edge algorithms that still need validation efforts, including a body of test work first on methods and then on tools in controlled environments and on test datasets before their use in court.

- Repeatability has long been a basic tenet in digital forensics but most probably we will be forced to abandon it, at least in its strictest sense, for a significant part of evidence acquisition and analysis. Already repeatability stricto sensu is impossible to achieve in nearly all instance of forensic acquisition of mobile devices and the same applies to cloud forensics. When Machine Learning tools and methods become widespread, reliance on previous validation will be paramount. As an aside, this stresses once more the importance of using open methods and tools that can be independently and scientifically validated as opposed to black box tools or – worse – LE-reserved ones.
- As for documentation, its importance for a sound investigation is even greater when we see non-repeatable operations and live analysis routinely be part of the investigation process. Published data about validation results of tools and methods used – or at least pointers to it – should be integral part of the investigation report.

3.2 Workflow

Keeping in mind how the forensic principles may need to evolve, we present here a brief summary of the forensics workflow and how each phase may have to adapt to big data scenarios. ISO/IEC 27037 International Standard covers the identification, collection, acquisition and preservation of digital evidence (or, literally, "potential" evidence). Analysis and disposal are not covered by this standard, but will be in future – in development – guidelines in the 27xxx series.

Identification and collection
Here the challenge is selecting evidence timely, right on the scene. Guidelines for proper prioritization of evidence should be further developed, abandoning the copy-all paradygm and strict evidence integrity in favor of appropriate triage procedures: this implies skimming through all the (potential) evidence right at the beginning and selecting relevent parts. First responders' skills will be even more critical that they currently are and, in corporate environments, also preparation procedures.

Acquisition
When classic bitwise imaging is not feasible due to the evidence size, prioritization procedures or "triage" can be conducted, properly justified and documented because integrity is not absolute anymore and the original source has been modified, if only by selecting what to acquire. Visualization can be a very useful tool, both for low-level filesystem analysis and higher level content analysis. Volume of evidence is a challenge because dedicated hardware is required for acquisition – be it storage or online traffic – while in the not so distant past an acquisition machine could be built with off-the-shelf hardware and software. Variety poses a challenge of a slightly different kind, especially when acquiring mobile devices, due to the huge number of physical connectors and platforms.

Preservation
Again, preservation of all evidence in a secure way and complying with legal requirements, calls for quite a substantial investment for forensic labs working on a significant number of cases.

Analysis
Integrating methods and tools from data science implies surpassing the "sausage factory" forensics still widespread today, where under-skilled operators rely heavily on point and click all-in-one tools to perform the analysis. Analysts shall need to include a plurality of tools in their

panoply and not only that, but understand and evaluate the algorithms and implementations they are based upon. The absolute need for highly skilled analysts and operators is clear, and suitable professional qualifications will develop to certify this.

Reporting
The final report for an analysis conducted using data science concepts should contain accurate evaluations of tools, methods used, including data from the validation process and accurate documentation is even more fundamental as strict repeatability becomes very hard to uphold.

3.3 Some tools for tackling the Big Data Challenge

At this stage, due also to the fast-changing landscape in data science, it is hard to systematically categorize its tools and techniques. We review here some of them.

Map-Reduce is a framework used for massive parallel tasks. This works well when the datasets does not involve a lot of internal correlation. This does not seem to be the case for digital evidence in general but a task like file fragment classification is suited to be modelled in a Map-Reduce paradigm. Attribution of file fragments – coming from a filesystem image or from unallocated space – to specific file types is a common task in forensics: machine learning classification algorithms – e.g. logistic regression, support vector machines – can be adapted to M-R if the analyst forgoes the possible correlations among single fragments. A combined approach where a classification algorithm is combined for instance with a decision tree method probably would yeld higher accuracy.

Decision trees and random forests are fruitfully brought to bear in fraud detection software, where the objective is to find in a vast dataset the statistical outliers – in this case anomalous transactions, or, in another application, anomalous browsing behaviour.

In audio forensics unsupervised learning techniques under the general definition of “blind signal separation” give good results in separating two superimposed speakers or a voice from background noise. They rely on mathematical underpinning to find, among possible solutions, the least correlated signals.

In image forensics again classification techniques are useful to automatically review big sets of hundreds or thousands of image files, for instance to separate suspect images from the rest.

Neural Networks are suited for complex patter recognition in network forensics. A supervised approach is used, where successive snapshots of the file system are used to train the network to recognize normal behaviour of an application. After the event the system can be used to automatically build an execution timeline on a forensic image of a filesystem.[KhCY07] Neural Networks have also been used to analyse network traffic but in this case the results still do not present high levels of accuracy.

Natural Language Processing (NLP) techniques, including Bayesian classifiers and unsupervised algorithms for clustering like k-means, has been successfully employed for authorship verification or classification of large bodies of unstructured texts, emails in particular.

4 Conclusion

The challenges of big data evidence already at present highlight the necessity of revising tenets and procedures firmly established in digital forensics. New validation procedures, analysts' training, analysis workflow shall be needed in order to confront the mutated landscape. Furthermore, few forensic tools implement for instance machine learning algorithms or, from the other side, most machine learning tools and library are not suitable and/or validated for forensic work, so there still exists a wide space for development of innovative tools leveraging Machine Learning methods.

References

[BBC+08] Barreno, M. et al.: "Open Problems in the Security of Learning". In: D. Balfanz and J. Staddon, eds., AISec, ACM, 2008, p.19-26

[FBI08] FBI: "RCFL Program Annual Report for Fiscal Year 2008", FBI 2008. http://www.fbi.gov/news/stories/2009/august/rcfls_081809

[FBI10] FBI: "RCFL Program Annual Report for Fiscal Year 2010", FBI 2010.

[ISAC13] ISACA: "What Is Big Data and What Does It Have to Do with IT Audit?", ISACA Journal, 2013, p.23-25

[ISO12] ISO/IEC 27037 International Standard

[KhCY07] Khan, M. and Chatwin, C. and Young, R.: "A framework for post-event timeline reconstruction using neural networks" Digital Investigation 4, 2007

[Pear01] Pearson, G.: "A Road Map for Digital Forensic Research". In: Report from DFRWS 2001, First Digital Forensic Research Workshop, 2001.

[Vari09] Varian, Hal in: The McKinsey Quarterly, Jan 2009

Security in Critical Infrastructures – Future Precondition for Operating License?

Dr. Willi Kafitz · Volker Burgers

Siemens Enterprise Communications GmbH & Co KG
Lyoner Str. 27, D-60528 Frankfurt/Main,
Heerdter Lohweg 35, D-40549 Düsseldorf
{willi.kafitz | volker.burgers}@siemens-enterprise.com

Abstract

Today, expanding digitalization and networking in many living and working areas is an inexorable process. It concerns infrastructures which are essential for modern societies and thus classified as critical. These infrastructures must be well-secured against erratic behavior. This especially applies to electronic attacks from criminal or foreign organizations. Very critical is electricity in that regard, because many areas depend on power. Through modern process IT and future ICT-based smart grids, energy suppliers are prone to cyber-attacks. In the industrial sectors, on a national level and on an European level there are several regulative and legal activities to be found in order to make information security independent of business hazards and to define the security level by legal acts. For this purpose we have well-defined national and international standards. In particular the ISO/IEC 27000 standard framework has been complemented in the last years by documents regarding industrial sectors e.g. power supply. Everything points to the requirement that some markets and market roles are so important for economic impact that the security level should be reviewed by independent organizations under governmental supervision. In the future many enterprises may have to accept that external audits, certification and frequent recertification is a binding requirement for doing business in critical market roles. Operation permit necessarily requires information security.

1 Introduction

On behalf of the German association Bitkom, the Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer institute for system and innovation research) published a study called „Gesamtwirtschaftliche Potentiale intelligenter Netze in Deutschland" (Overall economic potential of smart networks in Germany) [Fraun12]. Use of smart networks leads to an increase in efficiency and impetus towards expansion in several economic areas to the extent of 55´7 billion Euros. One of the components is smart grid, defined as ICT controlled electrical power supply, adding 9 billion Euros. It is oriented on creating availability not consumption.[1] Most of the industrial sectors like power supply, health care, traffic and so on are critical infrastructures which are very important for national economies. Current and future overlaps like cloud computing, machine-to-machine communication, smart cities to the point of "internet of things" lead to the notion that more and smarter use of IT and digital networks, as well as the connection

[1] [Fraun12], Gesamtwirtschaftliche Potentiale intelligenter Netze in Deutschland, Seite 5

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_18, © Springer Fachmedien Wiesbaden 2013

from sensors to the internet, will be an unstoppable process in order to realize its full potential in efficiency and growth.

The level of digitalization and networking will define the degree of dependency on IT at the application level [TTT12]: operational aspects become more and more important in process IT (SCADA). Possible failures and breakdowns of components, which will be unavoidable, must be controlled in a smart way. "Warm" restart and error recovery are necessary requirements for today's high security risk energy supply. Many cross-departmental business processes are not able to function without IT (e.g. intra-day market of electrical power with short-term flexibility). In addition, one should not forget the synchronous person-to-person communication: Terms like Voice-over IP (VoIP), Unified Communication (UC), Communication enabled Business Processes (CEBP) show that this kind of communication has become one ICT application among many.

All general tendencies, trends, infrastructures, scenarios and pictures of the future have one thing in common: digitalization and digital networking on the one hand requires a strong sense of security on the other.

In a company, managed by applying rules of economic values, a company is able to decide on their own if they take a risk or if they protect themselves from that risk. This especially applies to information security risks. If there are no legal requirements such as data privacy, the company is allowed to decide for themselves if they put measures of protection in place or if they take a risk. National economy requires the security of regulated industrial and important governmental areas. Their critical infrastructures have to have adequate and veritable security levels to make sure that IT risks do not have a possible negative national economic impact.

The paper at hand discusses the requirements and steps to implement such a system.

2 Security aspects

2.1 General threats

An important issue are cyber-attacks as a danger for the public. It is a prerequisite for national and international boards, organizations and moreover the legislative to protect critical infrastructures actively.

Cyber attacks are an important issue but other possibilities are also able to cause impact:

- Human error
- Lack of interoperability or in contrast to this
- Technical monoculture
- Lack of fault tolerance
- Lack of protocol conformity and capacity
- Complexity
- Compatibility (up- and downward)
- ….

At this point the subject matter shall only be IT security risks in critical infrastructures. Taking a closer look at examples taken from the field of power supply is always a good idea to illustrate the subject matter:

This article is meant to focus on IT-risks through cyber attacks, but other triggers often show how dangerous power outages can be for an economy. They may even affect human lives in the end. IT-risks are not necessarily restricted to the ongoing digitalization of the net control, ICT is key to many parts of the energy supply chain, thus various risks can arise. Here, we will outline three possible scenarios in regard of their corresponding cases.

IT risk in market communication: IT is used in long-term contracts within the energy market, in short-term intra-day market, in EDI-connections between market partner, billing and invoicing of the customer contracts and in contracts with generators, billing of control area, accounting grid and grid tax.

IT risks in grid planning and grid use: At the moment energy flow must be controlled over all operation resources. This is the task of the process IT and it reaches from the coordination center and control room to actively controlling e.g. voltage or frequency. In the control room and SCADA systems, security questions have gained importance because more and more IT is used for several tasks. Strict separation of process IT (PIT) impact and commercial IT (CIT) impact is not possible and does not make sense. IT-based midterm predictions of the balance of energy demands have an impact on grid planning; requirements for an effective asset management in short-term field maintenance or long-term maintenance planning are based on IT. Recording, plausibility and consolidation of metering data creates connections between PIT and CIT and therefore the need to secure PIT and CIT.

IT risks in voice communication: In case of a crisis, public networks, but also private networks for wired and wireless personal communication, are important e.g. for business continuity management (BCM). This communication is mostly based on TCP/IP networks with the same need for availability, security and privacy.

2.2 Examples

As an example of life-threatening situations caused by a power outage, the failure in July 2011 in eastern China can be mentioned here. Many security measures failed due to the power outage, resulting in a crash of two high speed trains.

The disruption of 82 power poles caused by freezing rain and heavy snowfall on November 25th and 26th in 2005 caused a blackout in Münsterland (Germany) for several days. 250,000 people were affected by the blackout.[2] This kind of risk caused by the embrittling effect on steel masts and the question if this natural catastrophe could have been prevented will not be discussed in this paper, but it shows the serious and unavoidable consequences such a failure can cause.

On May 2nd 2013, a critical state of the Austrian power grid occurred which could only be solved five days later.[3] At first, the situation was classified as an “attack” and showed all characteristics of a distributed denial of service attack (DDoS). Actually, an extensive status request of the southern German gas distribution system led to dramatic failures in the Austrian power distribution system itself. Ring communication caused a significant overload of data communication. The communication protocol was not able to dissolve the ring communication properly. Only after complex operations “by hand”, e.g. separation of communication connections and through

[2] http://www.zdf.de/Terra-Xpress/Blackout-im-M%C3%BCnsterland-8788812.html

[3] http://fm4.orf.at/stories/1717900/

knowledge from the "old days" of manual system control, the situation could ultimately be resolved. After that, the system was in a non-manageable mode for a few days. Due to skills and a piece of luck, an extensive black-out was avoided. This incident is a good example of the combination of many circumstances that – even without criminal intend – hazard situations may arise. Human mistakes were a trigger. Apparently gas and power systems were connected over a logical high application layer, which further boosted the initial human mistake. Monocultures were affected, but were probably not the trigger. At least the protocol was not capable to handle modern requirements. Through technical advancement, several components in the system have been changed from ISO 60870-5-101 (serial connection) to ISO 60870-5-105 (digital TCP/IP variant), which caused an additional dynamic to the failure. From the technical point of view, one has to keep a telecontrol scenario in mind.

Additionally, the organizational handling of this failure, the communication between authorities, suppliers and vendors, has to be analyzed during a final evaluation.

2.3 Organized crime

Numerous examples and incidents show that criminally- or nationally-motivated cyber-attacks have become a serious threat. During the last couple of years, attackers' profiles have changed significantly. Technically versed students or pupils are not "prototype" attackers anymore; moreover, organized crime or national intelligence organizations with enormous resources are attackers nowadays. Apparently, single companies can even be blackmailed these days.

A transmission network operator in Germany was attacked by eastern European hackers. Even though the power supply was not affected directly, the organized criminals managed to cause significant damage and confusion. The next step in the attacks could even affect countries.

Stuxnet has been in the press for a long time. It is a perfect example of a successful cyber-attack and apparently it is not an isolated case. Less known is a malware called Duqu [ENISA11]. Duqu is a computer worm which was originally detected in September 2011, but its potential is not fully known yet. The industry believes that Duqu was programmed by the same experts who have created Stuxnet, or that the experts had at least access to the Stuxnet source code. Experts think, Duqu may cause similar attacks like Stuxnet or that Duqu and Stuxnet in combination may have the ability to pursue further highly destructive tasks.[4]

Foremost, public discussions regarding the surveillance projects PRISM (Planning Tool for Resource Integration, Synchronization and Management) or the British intelligence service TEMPORA show the potential usage of resources not only for US intelligence organizations. Data privacy is still an important aspect, but is not necessarily important for an analysis. Recriminations for cyber-attacks suggest that the use of enormous resources is not explicitly restricted to surveillance projects but – as the examples clearly illustrates – also for attempts at manipulation.

Huge projects on a national scale such as PRISM create requisites in terms of gathering information- and methods for successful cyber-attacks. It seems that many attempts in developed countries are already happening. As long as they are motivated by political interest, you may be able to differentiate between "friend and enemy". This becomes even more complicated if its motivation is purely economic. A CSIS survey conducted by McAfee in 2011, asking 200 companies from the

[4] Enisa Annex II Security aspects in smart grid, Seite 6

energy sector in 14 countries, stated that 59% have been affected by stuxnet at some point. Further aspects in the study show that „80 percent had faced a large-scale denial-of-service attack, and 85 percent had experienced network infiltrations". [CSIS11] One has to point out: stuxnet, as politically-motivated and focused on cyber-attacks, was not designed to create economic damage in this area.

Various threats on digitally-controlled critical infrastructures ultimately require creating a legal national and international framework in order to have a common basis for initiated measures being auditable and enforceable in regard to enterprises, institutions and industry.

3 Legal framework

3.1 EU-level

The European agency ENISA (European Network and Information Security Agency) was founded back in 2004 by the EU-regulation no. 460/2004 [ENISA04]. The legal foundation[5] combines a series of EU-directives to face the challenges of network and information security and links them with the new agency. An example is the directive 2002/58/EG from March 7th, 2002 (Data privacy directive), but also other directives in the area of telecommunication regulation. The ENISA mandate was meant to run for seven years; it has been extended twice, the last time with extended competences, during the plenary session of the European parliament on April 16th, 2013 [ENISA 13]. [6] In the existing mandate of the agency, further defined in the EU regulation 526/2013 from May 19th, 2013, there are already comprehensive duties and responsibilities mentioned which are inter alia motivated by the protection of critical infrastructures.[7]

The act does not specify a duty to inform other member states in the sense of a registration. But ENISA has to fulfill its responsibility, e.g. to coordinate national CERTs (Computer Emergency Response Teams) or to build an early warning system, only if a thorough, constructive and systematic collaboration with national agencies leads to an extensive overview of the situation (see Article 2, goals of the EU-regulation 526/2013). Nonetheless, all impressive work results and achievements in the international collaboration in the area of information security do not show a systematic, measurable and structured information flow yet.

This gap shall be closed by means of another directive and a corresponding working paper, which is available in a draft status at the agency responsible.

1. Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union [8]
2. Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace

Briefly and succinctly, the directives claim that all member states have to have an approved cyber security strategy as well as institutions for enforcement in place. Germany partially fulfills these requirements:

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[6] http://www.europarl.europa.eu/news/en/pressroom/content/20130416IPR07353/html/ENISA-a-new-mandate-to-face-the-challenges-of-network-and-information-security

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:DE:PDF

[8] Deutsches Dokument siehe http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf

- UP KRITIS: With the implementation plan KRITIS (critical infrastructures), Germany has an existing national strategic foundation for the protection of critical infrastructures. [UPKR05]
- Cyber defense center: Associated with the BSI and managed by the BSI president, but an independent instance, has the duty to ward off electronic attacks.

In order to be fully compliant with the demands of the EU-directive draft, legal foundation and competences are missing that go beyond the federal administration.

One might point out attempts in the US under the name CISPA (Cyber Intelligence Sharing and Protection Act).[9]

3.2 On a national level – Germany

The German Federal Ministry of the Interior released the 2nd draft of a so-called IT-security act on March 5th, 2013 ("Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme").[10] The first draft had already been released and was in the hands of the committee members at the end of 2012. After an interdepartmental vote failed, due to resistance of the Federal Department of Commerce, the second draft has officially been released on the web site of the Federal Ministry of the Interior. A further hearing took place on July 14th. Currently, the unions and lobby groups in question work on commenting the second draft and they accompany the legislative process respectively. However, an adoption of the act within this legislative period (2009-2013) seems highly unlikely. The bill is considered a "skeleton law". Especially federal agencies like the BSI are meant to receive extensive resources and competencies, in order to audit and enforce a high security level in critical infrastructure industries. In the context of a cross-departmental registration of security incidents in both directions, a full exchange of information between corresponding authorities and industries shall take place. It is the objective to receive a comprehensive picture and the cyber defense between security agencies, industry, experts and vendors shall be optimized in the end.

The discussion within the industry, represented by selected operators of critical infrastructures, is more advanced. Today, banks are audited by the federal supervision agency for finance (BaFin) in regard to so-called operational risks. The BaFin circular 10/2012 contains the minimum requirements for risk management (ma-risk) and addresses IT-risks on an abstract level as well. [11]

The crisis reaction center for IT-security in the insurance industry is already established. Thereby, communication between companies and the BSI is realized through a single point of contact on the organizational side and contains alarm mechanisms and registration structures.[12]

Other industry specific standards such as security standards in hospitals, ISO 80001 for medical equipment in networks, become more and more legally and politically mandatory for the regulatory agencies.

Particularly the energy industry is considered as a critical infrastructure. A major outage would have effects on almost every sector of public life as well as the economy. Especially the importance

[9] http://www.gpo.gov/fdsys/pkg/BILLS-113hr624rfs/pdf/BILLS-113hr624rfs.pdf

[10] http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html

[11] http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html

[12] See e.g http://www.gdv.de/2012/07/das-krisenreaktionszentrum-fuer-it-sicherheit-der-versicherer-ist-vorbildhaft/

and dependency on information and communication technology, like mentioned before, gains more and more importance, also in regard to process IT. This importance is reflected in the 2005 adoption of the energy industry act [EnWG11] due to an own clause in §11:

> *(1a) A secure operation of an energy supply network especially includes an appropriate protection against threats to telecommunication and information technology used in network control. The regulation authority creates, in consultation with the BSI, a catalogue of security requirements for publication. An appropriate protection of a network operator can be suspected, if the catalogue is implemented and documented. The compliance may be assessed by the regulation authority. The regulation authority is able to require changes in documentation, content and design, due to §29 article 1 sentence 3.* [13]

But this legal regulation "only" applies to operators; this means it is only applicable to transport networks and distribution networks for electricity and gas. Other market roles have not been regulated yet. The start of the energy change to smart grids in Germany is meant to be realized by so-called smart metering gateways. Here, metering data is sent to authorized receivers. This helps to create flexible payment models and a secure interface to controllable downstream systems like power stations, photovoltaic stations, components of house automation respectively facility management or energy storage.

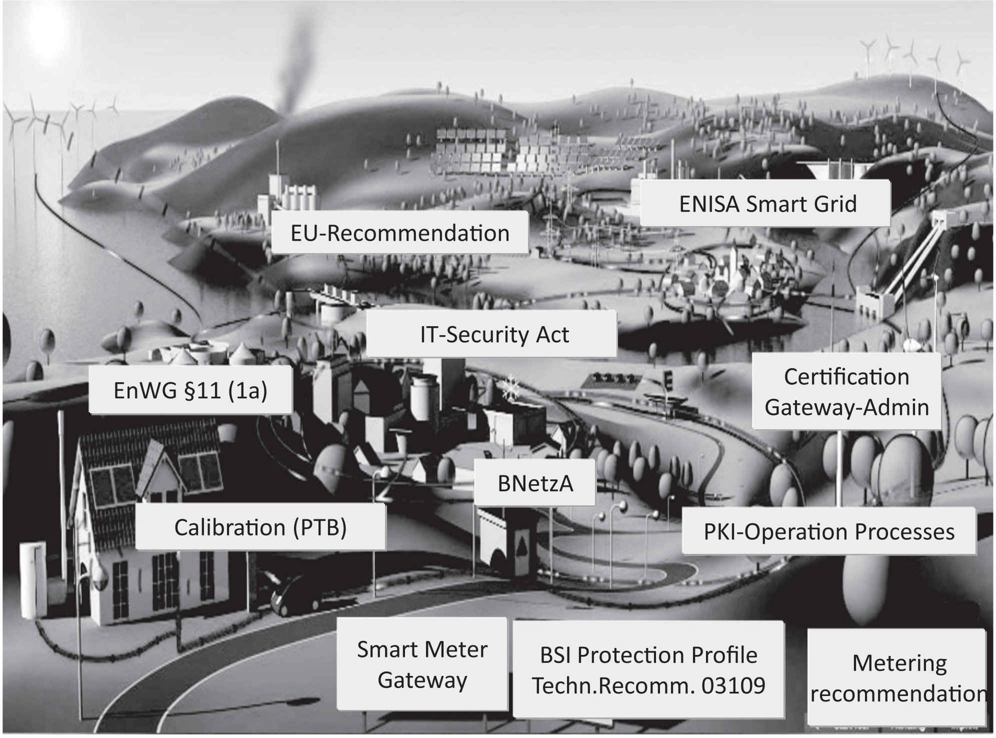


Fig. 1: "Landscape" of regulatory security requirements in the energy industry[14]

[13] http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf

[14] Backround: (e-energy promotion project of the Federal ministry of Economics (e-energy-Förderprojekte des Bundesministeriums für Wirtschaft in Deutschland (BMWi))

To the consumer resp. prosumer data inspection must be granted (EnWG §21h). The smart metering gateway is the decentralized interface to the future smart grid; but it is placed, like measure systems today, in an insecure environment. BSI and BMWi have created a security profile for a smart metering gateway (BSI-CC-PP-0073)[15] considering Common Criteria and have created a technical (interoperability-) guideline BSI TR 03109.[16]

The gateway administrator role is especially important for security. The legislator wants to fulfill this through special security guidelines in organizational and technical regards. The question remains, if all 900 system operators, which are capable of measuring operations these days, will fulfill these extensive requirements completely.

Thus, legal foundations will be created, to ensure minimal requirements information security in critical infrastructures on a European level as well as on a national level (e.g. Germany). In Germany, the ICT-driven energy change will result in much risk potential in the energy supply sector. In other countries, usage of process IT is constantly on the rise. It is mandatory that the energy industry has to be secured with high priority, independent of political aspirations that focus on all critical infrastructures. IT-security has to be a main topic in all countries on their way to implementing smart grids.

4 Political orientation

4.1 Discussion of the requirements

From a business point of view, information security may fall more or less under a certain entrepreneurial risk. There are only few laws or binding regulations imposing a defined state of information security. Specific boundaries are set through the data privacy act and corresponding directives on the European level, like the before mentioned directive 2002/58/EG. Through the control and transparency in business act (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG) executive management is personally liable in case of gross negligence. But then again, the act itself is, due to circumstances surrounding its origin in the year 1998 (after the East Asia crisis, shortly before the feared millennium), very general and hard to enforce. Even more adoptable are the insurance law requirements in case of damage. Gross negligence of a policy holder may lead to a case where the insurer will be prevented from paying.

Only in case of other outside influences or events, requirements for individual industrial sectors of national economies become visible. The energy sector has always had a leading role. In addition to mains operation and gateway administration at the meter operator (with the question of whoever will have this role unanswered at this point), old and new market roles have to be assessed in regard to new security requirements. In view of the national economic importance, implications and vulnerability through cyber-attacks, different political security requirements have to be met. This concerns areas from gas storage operators to supra-regional transmission providers.

[15] https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html

[16] https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html

4.2 Standards and proof of conformity

One might suspect that energy suppliers have to fulfill governmental requirements. After being committed to the requirements of the IT security act other industrial sectors and organizations with critical infrastructures will have verifiable legal requirements to do so as well.

The Federal Office for Security in Information Technology has created a powerful instrument with the IT Baseline Protection Catalogs[17] and further documents. They can be used by many enterprises and governmental entities to protect IT infrastructures from small servers up to high-end electronic data processing centers (EDPC) against security threats. Organizational and technical requirements have been taken into consideration. Substantial documents regarding security organization, best practice, risk and emergency management and business continuity management are available.

- BSI-Standard 100-1: Information Security Management System (ISMS)
- BSI-Standard 100-2: IT Baseline Protection Catalog
- BSI-Standard 100-3: Risk Analysis based on IT Baseline Protection Catalog
- BSI-Standard 100-4: Emergency Management

But especially in regard of the process IT, requirements have come up which cannot be appropriately handled with the IT Baseline Protection Catalog. This is the reason why many enterprises decided to use the ISO/IEC standard framework as a line of action for information security. It is the better choice for major enterprises and especially for international operating companies. ISO/IEC 27001 defines the organizational structure of an Information Security Management System (ISMS). Annex A offers a checklist with controls explained in detail in ISO/IEC 27002. This is a widespread standard specification and elementary enough as a basis for action. However, controls should be completed and specified for particular industrial sector requirements. Therefore, specific needs of the telecommunication sector are considered in ISO/IEC 27011:2008. Similar based on the 27002 method and DIN SPEC 27009 energy industry needs were developed in ISO/IEC TR 27019.

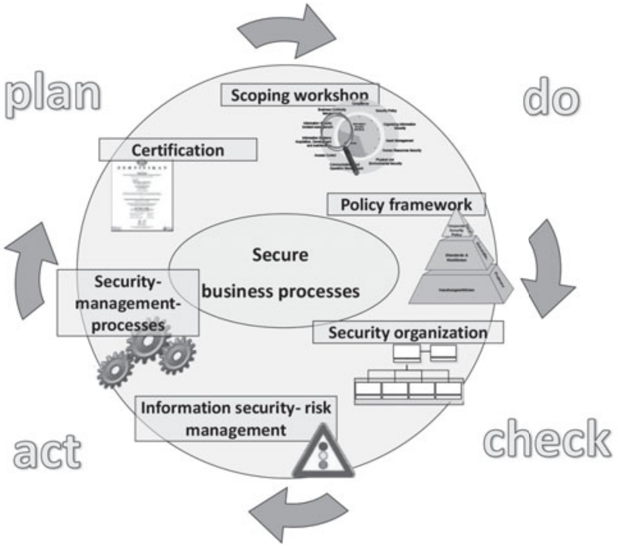


Fig. 2: ISMS-process

[17] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Operators of critical infrastructures shall be committed to these standards and should have to document their actions accordingly. This is especially necessary when it comes to the market role of the energy industry, considering their overall importance for the economy. Thus, an economically motivated scope for the implementation of organizational and technical measures is restricted to a minimum. Entrepreneurial risk must not affect uninterrupted service.

5 Conclusion

National and international standards will define the benchmark for security requirements in critical infrastructures in the future. Critical market roles will need a proof of security compliance by means of external certification. This proof will be a requirement for a business operation permission in this market role. Certification will be conducted by an external auditor, who requires a governmental auditor qualification in the respective country.

ISO/IEC 27006 defines the requirements for the auditor organization; ISO/IEC 27007 and ISO/IEC 27008 are in a test status. These are elements of the standard framework providing reproducible criteria for audit and for the auditor.

Only an ISMS will create the organizational principle for organizations with critical infrastructures to create a registration on a national level. This cross-departmental registration will be a powerful network to ward off cyber-attacks. Information regarding cyber-attacks in one's own company could be forwarded swiftly and efficiently. External information could be checked if it is relevant for one's own institution.

On a technical level, the ISO 27000 standard and its extensions are a powerful instrument which can be used in a responsible way, ensuring a complete security cycle – reviewed again at any time.

Cyber-attacks pose serious threats that have to be fought off properly. In the future, security measures should become a part of compliance requirements. Whether or not a business section is compliant to the requirements shall be evaluated in the interest of national security and eventually documented by a certificate.

Due to the enormous importance regarding the welfare of a society connected to the outlined new threats, we – more as an interested expert group – mean to support all steps helping to secure our critical infrastructures and make them less vulnerable.

References

[BSIGS13] BSI Grundschutzhandbuch, (http://www.bsi.bund.de) (IT Baseline Protection Catalogs from the Federal Office for Security in Information Technology)

[BSIPP13] Protection Profile for Smart Meters, (http://www.bsi.bund.de)

[BSITR13] BSI Technische Richtlinie, TR 03109, (http://www.bsi.bund.de) (Technical Guidelines for Smart Metering Gateways)

[CISIS11] In the Dark: Crucial Industries Confront Cyberattacks; Center for Strategic and International Studies (CSIS) for McAfee, Washington and Santa Clara 2011, p. 5, (http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf)

[ENISA04] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency Official Journal L 077 , 13/03/2004 P. 0001 – 0011

[ENISA11] Enisa Annex II Security aspects in smart grid

[ENISA13] German: VERORDNUNG (EU) Nr. 526/2013 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004

English: REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

[EnWG11] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), geändert durch Artikel 4 des Gesetzes vom 31. Mai 2013 (BGBl. I S. 1388) (German Electricity and Gas Supply Act)

[Fraun12] Hrsg./Contact Bernd Beckert, Gesamtwirtschaftliche Potentiale intelligenter Netze in Deutschland, Fraunhofer ISI, Karlsruhe, (http://www.bitkom.org/files/documents/Studie_Intelligente_Netze(2).pdf) (Fraunhofer ISI, Overall economic potential of smart networks in Germany

[ISO27-13] ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC TR 27019, http://www.iso27001security.com/html/27019.html

[UPKR05] Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, Hrsg. Bundesministerium des Innern, (http://www.kritis.bund.de) (Federal Ministry of the Interior, Implementation Guideline for the National Strategy to Protect Critical Infrastructures)

[TTT12] Hrsg. TeleTrusT – Bundesverband IT-Sicherheit e.V., TeleTrusT-Eckpunktepapier “Smart Grid Security”, 2012, (www.teletrust.de/publikationen/broschueren/smart-grids) (German Federal Association for IT Security, Basic Point Paper “Smart Grid Security”)

Abbreviations

BCM	Business Continuity Management
BSI	Federal Office for Security in Information Technology
EDPC	Electronic data processing center
ENISA	European Network and Information Security Agency
ICT	Information and Communication Technology
ISMS	Information Security Management System, towards ISO/IEC 27001 or BSI-Standard 100-1
SCADA	Supervisory Control and Data Acquisition
Smart Grid	In the meaning: automatic ICT-based controlling of offer and use of electrical power mostly from volatile energy resources.
SMGW	Smart Metering Gateway
UC	Unified Communication, Integration of several communication methods in a homogeneous application level
UP KRITIS	Implementation Guideline for the National Strategy to Protect Critical Infrastructures

A Practical Approach for an IT Security Risk Analysis in Hospitals

Levona Eckstein · Reiner Kraft

Fraunhofer Institute for Secure Information Technology SIT
{levona.eckstein | reiner.kraft}@sit.fraunhofer.de

Abstract

Hospitals are indispensable institutions for public healthcare and part of society's critical infrastructures. The increasing use of information technology and networks creates new dependencies and risks that could affect medical service availability. A systematic analysis of risks associated with IT will help to determine the risks for critical processes caused by IT disruptions or failures.

This paper outlines a practical risk analysis approach with focus on the risks associated with the dependency on hospital IT. The method was developed within the project "Risk analysis hospital IT" ("Risikoanalyse Krankenhaus-IT" – RiKrIT) launched by the Federal Office for Security in Information Technology (BSI), the Federal Office for Civil Protection and Disaster Assistance (BBK), the Senate Department for Health, Environment and Consumer Protection of the State of Berlin, and the Unfallkrankenhaus Berlin (ukb).

1 Introduction

Hospitals are indispensable institutions of healthcare and the public health sector and thus part of our society's critical infrastructures. Disruptions and failures of these facilities and their processes can lead to dramatic impacts on patient care and public health and could endanger human life. Thus the hospital's management has the responsibility and a legal obligation to assure the availability of medical services and their corresponding processes.

Operational risks are highly associated with the dependencies on other external critical infrastructures like water and energy supply. The increasing use of hospital information technology creates new dependencies as well and can lead to an increased critical process failure risk.

More and more administrative processes and treatment processes in hospitals are supported by information technology (IT).The spectrum ranges from specialized hospital information systems (e.g. clinical information system – CIS, radiologic information systems – RIS) over Electronic Health Records (EHR) to medical devices. Moreover, the diverse IT systems in a hospital are linked together thus forming a network that has interfaces to the internet and other public networks. The integration of various medical devices into the hospital IT network is playing an increasingly important role as well. In particular, medical devices for imaging procedures (surgical cameras, computed tomography scanners, X-ray machines and others) are designed to exchange electronic information with other devices.

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_19, © Springer Fachmedien Wiesbaden 2013

All of this increases the IT and network criticality of a modern hospital's core procedures substantially. Incorrect hardware configurations, inadequate malware protection and unauthorized access to IT systems are just some examples of potential hazards that may result in the impairment or loss of process availability.

The security incidents published in the last years indicate that the situation for hospitals has become more critical due to IT security risks and that this has to be taken very seriously. The following two published incidents reflect the importance of protecting the hospital IT infrastructure against potential IT threats and vulnerabilities:

- California 2005 – a former network administrator of a hospital service provider penetrates the network, disables the backup function and deletes electronic health records.[1]
- Netherland 2010 – the entire computer network in a Dutch hospital in Horn has to be shut down as a result of a virus attack. Many employees have no access to the hospital system. Only emergency operations will be performed.[2]

With respect to the growing dependencies on hospital IT and the changing threat situation, a systematic approach for identifying and assessing the risks associated with IT becomes a major issue for hospitals to ensure resiliency. It must also be a part of existing management processes such as for risk management.

Because of the importance hospital IT has gained over the last few years numerous standards and guidance for the healthcare sector have been developed and published to meet the specific information security requirements in this critical sector (e.g. ISO 27799:2008 [ISO08b] and IEC 80001-1:2010 [IEC10], focussed on risk management in the context of medical devices integrated in IT networks).

The German Federal Office for Civil Protection and Disaster Assistance has also developed a guide for risk management in hospitals [BBK08] to support the implementation of sector specific risk management processes. This guide outlines major hazards to the disruption-free functioning of health care facilities, e.g. natural events or possible risks caused by the interdependency of external critical infrastructures. It also mentions the hospital IT infrastructure as a risk factor with regard to the functioning of critical processes, but does not analyse the IT risks in detail. Therefore, the Federal Office for Civil Protection and Disaster Assistance, the Federal Office for Security in Information Technology, the Senate Department for Health, Environment and Consumer Protection of the State of Berlin and the Unfallkrankenhaus Berlin (ukb) have initiated the "Risk analysis hospital IT (RiKrIT)" project to develop a method for an IT specific risk analysis focusing on critical processes and their IT dependency, which will be presented in this paper.

2 Phases and Steps

The method consists of four phases representing the necessary activities to perform a successful IT-related risk analysis in a hospital. The following table gives an overview of the phases and individual working steps.

[1] www.gulli.com/news/5922-san-diego-63-monate-haft-fuer-boeswilligen-hack-aus-rache-2008-06-14

[2] www.heise.de/-1122484

Table 1: Overview of the phases and individual working steps

Phase	Individual working steps
Preparatory activities	Step 1: Initialise the IT risk management process Step 2: Define protection goals Step 3: Define the investigation area Step 4: Identify processes
Analysing the criticality of processes and IT	Step 5: Identify critical processes Step 6: Identify the IT support Step 7: Identify critical IT dependencies Step 8: Identify critical IT components
Identifying and assessing risks	Step 9: Identify risk scenarios Step 10: Estimate occurrence probabilities Step 11: Estimate possible damages Step 12: Determine the risk value Step 13: Consider existing measures
Handling risks	Step 14: Decide on risks treatment Step 15: Decide on protection measures and substitute procedures

This paper outlines the key steps of the risk analysis approach:

1. Define protection goals to outline the normative frame of reference for the risk evaluation;
2. Identify critical processes and IT resources to set the focus on those targets that have a significant impact on fulfilling the protection goals;
3. Identify and assess risks for detecting those threats and vulnerabilities that can lead to failures or malfunctions of critical IT resources and thereby the supported processes;
4. Risk treatment, especially the selection of measures to mitigate given risks.

3 Definition of Protection Goals

As one of the preparatory activities of the risk management process protection goals should be defined and in doing so also the target information security state of an application area. Protection goals are the strategic answers to the question which level of reliability a certain institution and their organisational units should go for.

Protection goals can address different aspects of an organisation. In the case of hospitals, for example, it can address (1) a medical care which fulfils the needs of the patients as well as (2) the financial situation and survivability of the institution. The risk analysis approach outlined in this paper is focussed on the first aspect, the ability to guarantee adequate patient care. Nevertheless, the second aspect, the existence of the institution, also has to be kept in mind, especially because hospitals play an important role in the management of such crises which affect the physical integrity of a population to a larger extend.

In the context of IT risk analysis, protection goals are usually based on certain basic concepts of information security: confidentiality, integrity, and availability are the ones used mostly, but others like authenticity, liability, or accountability may be useful too, depending on the context of the analysis. Furthermore, protection requirements are typically defined with the help of categories. For example, the IT-Grundschutz methodology [BSI08a] uses a classification into the three protection requirements "normal", "high" and "very high" which then have to be refined depending on a concrete application context, for example based on the impact to a patient's physical integrity as described in the following:

- Protection requirement "normal" – only temporary physical injuries which do not affect the well-being of the patient are possible.
- Protection requirement "high" – permanent physical injuries are possible, but they present no danger to a patient's life or the patient's capacity to act.
- Protection requirement "very high" – permanent physical injuries are possible compromising a patient's life or a patient's capacity to act.

In the context of the medical treatment process, it is absolutely necessary to guarantee the availability and integrity of information and IT linked to this process. Wrong or made too late medical decisions and reactions can otherwise lead to severe consequences for a patient's physical integrity. Data confidentiality has to be considered as well, because a security breach of this goal can have medical consequences. This is reflected in Table 1 which shows some example definitions of the requirements availability, integrity, and confidentiality related to the subordinated goal Protection of Patient.

Table 2: Protection goals and requirements – example definitions

Goal/Requirement	**Protection of Patient**
Subordinated	IT incidents must not lead to a quantitative or qualitative reduced treatment, which cause a worsening in the health condition of a patient.
Availability	The medical care capacity and all that is necessary for their maintenance should not be affected by IT failures or problems.
Integrity	The integrity of the data necessary to provide health care for a patient must not be compromised by IT problems.
Confidentiality	IT incidents should not cause data to be accessible to unauthorised persons if its confidentiality is necessary • For the availability or integrity of information and IT, or • The treatment and health care of a patient.

4 Identification of Critical Processes and IT

The relevance of information technology in a hospital depends on its role in supporting the diverse medical and non-medical tasks this kind of institution is concerned with. For the effectiveness of IT-related risk analysis, it is important to focus on those processes and IT resources which have a major impact on the task fulfilment of a given hospital. To identify these critical elements of the IT infrastructure, it is necessary to analyse first the criticality of a clinic's medical and non-medical processes and to identify then the IT dependencies of these processes.

An overview over the hospital's processes is therefore necessary for the subsequent risk analysis. Like in any other organisation, these processes can by classified into three groups:

- Core processes – all processes which are directly related to the ambulant and stationary patient care e.g. medical diagnostics, surgery, intensive care;

- Support processes – all processes which are necessary for the performance of the core processes, but have no direct customer (in this case: patient) value like ac-counting and finance, human resources, IT administration and support, logistics;
- Management processes – all processes which control the core processes and have a focus on the associated organisational roles and tasks like strategic planning, auditing, and quality assurance.

Usually, the main focus of the IT risk analysis is set on the core and support processes.

A hospital's organisational structure and procedures may be good starting points for identifying critical processes and IT dependencies. These institutions are usually organised along two principles. Under the professional aspect they consist of medical services, nursing services (including for example physiotherapeutic service), and administrative services (including technical and logistic services). Besides this kind of division, a hospital is structured into

- Clinics, each of them headed by a chief physician,
- Stations as the primary location of the stationary patient care,
- Ambulances which provide short time consulting, various kinds of diagnostic and therapeutic procedures (around the clock opened interdisciplinary emergency ambulances are a special case), and
- Special service points like X-ray, laboratory, nuclear medicine or surgery.

A hospital's core processes are usually organized across these organisational units in a more or less modified way. This could lead to some difficulties in the survey and analysis of the criticality of processes and necessary IT resources, which is usually performed in interviews and questionnaires with the representatives of a hospital's organisational units. A business process oriented analysis, however, needs a holistic and comprehensive view on the individual steps and sub-processes of the hospital process map. In a similar fashion, it has to be taken into consideration that the impact of IT components (applications, systems, networks, related infrastructure and services) on the business processes requires that the supported processes have to be analysed in full. Dependencies between the processes und cumulative effects resulting from the relevance of an IT component could be ignored.

To be efficient, the number of processes and objects which should be subjects of a risk analysis has to be reduced to those which have the highest criticality. For this selection the definitions of protection goals and their refinements can be used – for example the answers to questions like "After which time can IT interruptions have severe physical consequences for a patient", "What can happen if data is injured", "How sensitive is the confidentiality of data for the treatment process". For example, in an analysis of critical hospital processes, which has been performed within the RiKrIT project using the criteria mentioned above, the following sub-processes have been identified as critical:

- All sub-processes of the intensive care unit,
- The processes treatment and documentation in the areas cardiology and left cardiac catheter,
- All sub-processes in the diagnostic laboratories.

All these processes are strongly supported by specialised IT applications, partially including interfaces to medical technology for diagnostic data import or the control of these technical systems. The proper functioning of these applications depends on technical components like servers, clients, or the network. The focus of the IT risk analysis is set on these critical components. Figure 1 illustrates these relations.

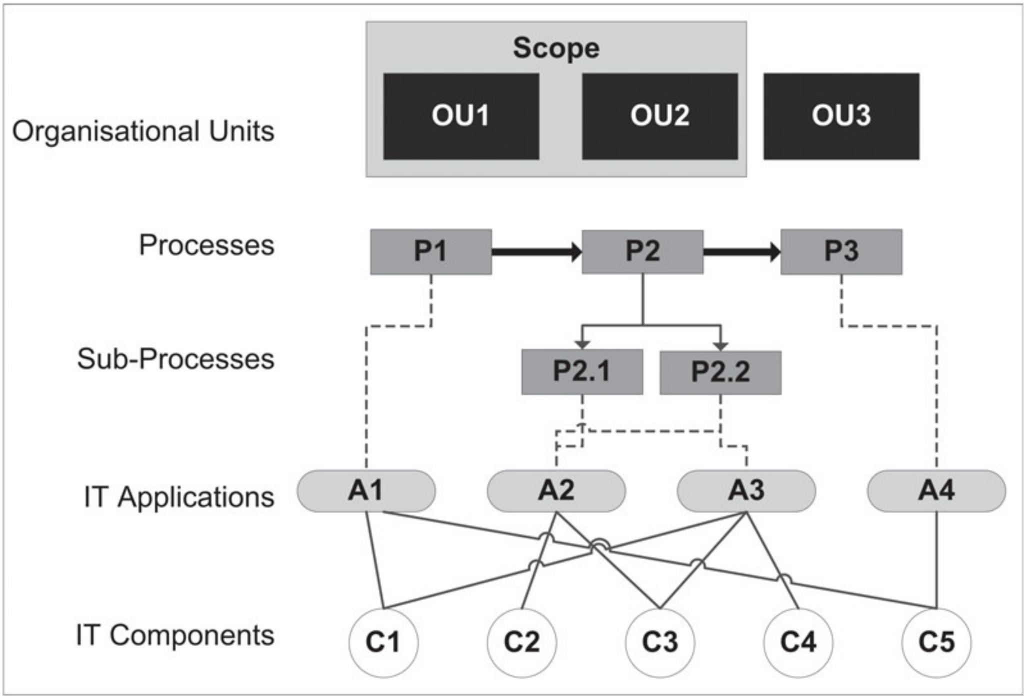


Figure 1: Identification of Critical IT components

5 Risk Identification and Risk Assessment

Risk management includes all activities concerned with the systematic handling of risks in a given organisation. It consists of a cyclic process of identifying, assessing, handling, and controlling those risks that are potentially dangerous for the processes and assets of the organisation. A multitude of methods is available to analyse risks. The available approaches differ in the application field, theoretical background, requirements on precision, or grade of formalisation, for example. Regardless of the differences all approaches operate with similar basic concepts and related tasks like

- Identification of analysis and relevant protection goals' target objects,
- Identification and assessment of threats which can lead to security breaches concerning the protection goals,
- Identification and assessment of vulnerabilities in the protection mechanism of the considered target object,
- Estimation of critical event occurrence probability,
- Estimation of extent and kind of possible damage,
- Assessment of risks based on the results of these tasks.

The risk analysis approach which was developed in the RiKrIT project is compatible with the method proposed in the guide of the Federal Office of Civil Protection and Disaster Assistance [BBK08]. Figure 2 illustrates the key elements of the approach.

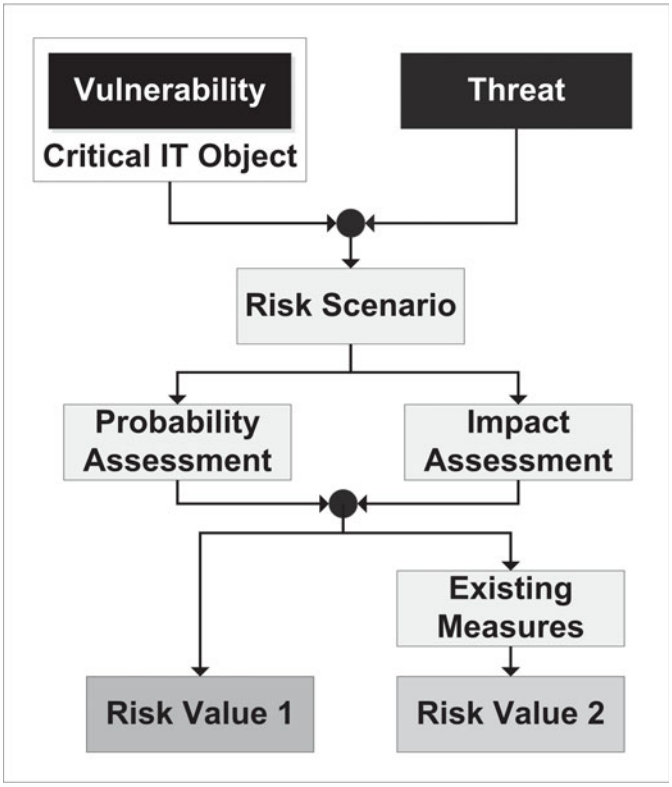


Figure 2: Elements of Risk Analysis

To adopt the method to the characteristics of an IT focused risk analysis, input from different sources has been combined and trimmed to the target group's needs:

- It is based on the theoretical framework which is defined in ISO 27005 [ISO08a] and especially uses the catalogues with examples of vulnerabilities in an annex of this standard.
- Furthermore, BSI-Standard 100-3 and the catalogues of elementary threats, which have been introduced in the last year to simplify the application of this standard [BSI08b] [BSI11a] [BSI11b], are being used.
- To estimate the probabilities of occurrences, ideas from the OWASP testing guide [OWAS08] have been used – the idea is to get comprehensible decisions on these values by regarding factors which facilitate the probability of an attack or the occurrence of other threats like technical failure or natural disasters.

To support the user appropriately, the guidelines includes catalogues of threats and weaknesses as well as a list of criteria to examine the probability of an event.

To reduce the complexity of risk analysis, the catalogues of threats and weaknesses consist of two levels. Level 1 of the threat catalogues lists generic threats like natural events, technical failure (of IT systems, data storage, network, or supply), human failure, deliberate acts, and (internal or external) organizational failures. It should be used as a starting point for the identification of risk scenarios. In level 2, these generic threats are refined further. For example, the level 1 threat of deliberate acts with respect to software, data and information is in level 2 refined into possible attacks denial of acts, spying of information/data, manipulation of software and information/data, misuse of personal data, abuse of privileges, and destruction of data carriers.

The catalogues of weaknesses are organized in a similar way, e.g. is the vulnerability "inadequate security functionality of software" in level 2 refined into vulnerabilities lack of password security, lack if encryption mechanism or lack of access protection.

To allow the probability assessment of a risk scenario, a list of criteria is given. For example, the probability of deliberate acts depends on the degree of publicity of the weakness, the necessary experience of an attacker, and the opportunity of attack detection.

The risk value, which is calculated based on the assessment of a threat's probability and potential impact, serves as an indicator to support the decisions on risk treatment. To allow estimations on the effect of existing or already planned security controls, this value should be calculated both with and without the consideration of these security measures.

6 Risk Treatment

The risk treatment process starts with a decision on how to handle risks that are not appropriately covered by the introduced or planned security measures. As described e.g. in [BBK08] or [BSI08b], principally, one of the following strategic options could be reasonable for the treatment of a given risk:

- Risk avoidance – the risk will be reduced by restructuring the critical process so that the vulnerabilities are minimised, or by completely dispensing with it;
- Risk reduction – the probability of occurrence or the amount of possible damage will be reduced by additional security measures;
- Risk transfer – the shifting of the risks to another institution e.g. by outsourcing a critical process or by taking out insurance policies to avoid or at least decrease financial losses as consequence of an incident;
- Risk acceptance – a reasonable option if sufficient security measures are too ex-pensive or not feasible within the application context.

Usually, whenever the application of IT contributes in a positive manner to a hospital's treatment process or other critical processes, risk avoidance or risk reduction should be the preferred strategic options. Hospitals should therefore be supported in the selection of adequate measures. More or less generic information security frame-works like ISO 27002 [ISO05] – or ISO 27799 [ISO08], the hospital related version of the ISO 27002 controls – and the IT-Grundschutz Catalogues [BSI11a], can give an orientation for this task. To assist the user in the application of these complex rule-sets, the guidelines for IT risk analysis provides the users in hospitals with a subset of relevant security measures, which will fulfil at least baseline security requirements in the protection against threats and vulnerabilities identified and assessed in the previous steps. Furthermore, similar to the IT-Grundschutz Catalogues these measures are linked to typical hospital IT components like

- Clients (client PCs, terminal clients, laptops, and other mobile devices),
- Servers (terminal server, application server, database server, authentication server, communication server, virtualisation server),
- Networks and access control systems (including concepts like demilitarised zones),
- Other devices like printers or storage.

Each group of measures also has references to the threats against which they protect as well as to the corresponding protection goals. For this purpose, cross-reference tables have been developed with a mapping of the elementary threats in the threat catalogue to the corresponding protection measures defined in the IT-Grundschutz Catalogues.

Besides the implementation of proactive measures to reduce the probability and/or the amount of damages, it is essential to keep in mind that IT systems and IT applications can still fail, no matter how well their protection mechanism have been implemented. Thus, it is essential for a hospital to provide alternative measures, in order to be resilient against IT failures and to be able to continue its critical processes, especially those directly related to patient care. In particular, the residual risk of a CIS outage should be minimized by means of the maintenance of a corresponding paper documentation, to be used instead of the IT application in case of such an incident. Moreover, IT-related compensation methods are possible. For example, important information like the electronic health records can be maintained as PDF files on a separate system and updated at short intervals (e.g. every hour). These files can be printed out in case of a CIS outage. For reasons of timely availability, this would require a high-performance printer.

7 Conclusion

As in most other parts of society, information technology has become a crucial resource for the successful performance of a modern hospital's medical and administrative processes. This means new opportunities for such core processes like patient care quality and efficiency, but it carries also new risks if the dangers of the existing IT-dependencies are unknown and adequate measures and concepts for the treatment and mitigation of said risks are missing.

The method described in this paper is targeted at supporting the responsible persons in defining and applying adequate risk management strategies and by developing a guide and an approach that fits

- The application area – hospitals and related institution –,
- The target group – hospital and subordinate agencies' risk managers –,
- And the subordinate concepts – the risk and crisis management guide of the Federal Ministry of the Interior [BMI08] and the guide for risk management in hospitals of the German Federal Office of Civil Protection and Disaster Assistance [BBK08].

The method is described in detail in the documents [BSI13a] and [BSI13b].

References

[BBK08] Federal Office of Civil Protection and Disaster Assistance (BBK): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus (Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens), Langfassung, Bonn 2008. Download: www.kritis.bund.de.

[BMI08] Federal Ministry of the Interior (BMI): Protecting Critical Infrastructures – Risk and Crisis Management – A Guide for Companies and Government Authorities. Berlin 2008. Download: www.kritis.bund.de.

[BSI08a] Federal Office for Information Security (BSI): BSI-Standard 100-2: IT-Grundschutz Methodology, Version 2.0. Bonn 2008. Download: www.bsi.bund.de/Standards.

[BSI08b] Federal Office for Information Security (BSI): BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, Version 2.5. Bonn 2008. Download: www.bsi.bund.de/Standards.

[BSI11a] Federal Office for Information Security (BSI): Threats Catalogue: Elementary Threats, Version 1.0. Bonn 2011. Download: www.bsi.bund.de/Standards.

[BSI11b] Federal Office for Information Security (BSI): Supplement to BSI-Standard 100-3, Version 2.5, Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses, Bonn 2011. Download: www.bsi.bund.de/Standards.

[BSI11c] Federal Office for Information Security (BSI): IT-Grundschutz-Kataloge. 12. Ergänzungslieferung, Bonn 2011. Download: www.bsi.bund.de/IT-Grundschutz-Kataloge.

[BSI13a] Federal Office for Information Security (BSI): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT (Langfassung). Bonn 2013. Download: www.kritis.bund.de.

[BSI13b] Federal Office for Information Security (BSI): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT (Management-Kurzfassung). Bonn 2013. Download: www.kritis.bund.de.

[IEC10] International Electrotechnical Commission: IEC 80001:1: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities, 2010.

[ISO05] International Organization for Standardization: ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, 2005.

[ISO08a] International Organization for Standardization: ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management, 2008.

[ISO08b] International Organization for Standardization: ISO/IEC 27799:2008 Health informatics – Information security management in health using ISO/IEC 27002, 2008.

[OWAS08] OWASP Foundation: OWASP Testing Guide V 3.0, 2008. Download: www.owasp.org.

When does Abuse of Social Media constitute a Crime? – A South African Legal Perspective within a Global Context

Murdoch Watney

University of Johannesburg, South Africa
mwatney@uj.ac.za

Abstract

Each day many millions of communications take place by means of social media. Communication via social media has not created new behaviour but merely facilitates old behaviour, but due to its characteristics such communication may have in some instances devastating consequences which were not possible prior to the availability of social media. The question arises how should social media usage be governed and more specifically, what role if any the criminal law should full-fill in this regard? For example, when does social media usage amount to abuse and if the communication does amount to abuse, should such conduct be criminalized? The effect such criminalization might have on human rights is but one of the relevant factors that should be considered in this regard. The paper also investigates emergent legal developments pertaining to the criminalization of communication. The topic touches on a variety of issues that necessitate a discussion within a global context as socialization and democratisation of information is becoming an integral part of the global society. Although the discussion emanate from a South African perspective, a legal comparative approach is followed as social media abuse is a global phenomenon affecting various countries.

1 Introduction

People are increasingly communicating by means of social media and therefore it is not surprising that social media behaviour is receiving attention on a national and global level.

The discussion covers a wide range of aspects relating to social media communication. Legal discussions have thus far mostly focused on a specific aspect of social media usage. In this paper an overview will be given of the different aspects pertaining to social media communication and the possible legal implications of such communication, specifically within the ambit of criminal law.

Reference is made to the South African position in a legal comparative approach. South Africa has no reported case law that deals specifically with criminal conduct on social media. Quite a number of reported cases in South Africa deal with labour disputes pertaining to social media abuse in the workplace which resulted in the dismissal of an employee. [Misc11] The lack of criminal prosecutions regarding social media communications in South Africa might be ascribed to its' status as a developing country with social media activity only becoming an integral facet

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_20, © Springer Fachmedien Wiesbaden 2013

of society in recent years. In the United States of America (USA) criminal prosecutions on social media activity is still rare [Grigg12], which is note-worthy taking into consideration that the USA ranks as one of the countries with the highest number of social media users. On the other hand, the United Kingdom (UK) has over the years experienced a rise in social media prosecutions (http://www.indexoncensorship.org/2012/12/social-media-pro...).

It will be illustrated in this discussion that, although social media has been used to benefit and improve users' lives, [Qual13] it has the potential to be abused and therefore social media communication cannot be unregulated. The focus will be on when communication constitutes an abuse and whether that abuse might be classified as a crime? It will be argued that communication constitutes an abuse when the limits of free speech are exceeded. If the abuse is not yet classified as a crime, the question arises whether the conduct should be criminalized? It is also of interest to the South African legal system to consider what other countries consider as abuse of social media usage and how it is dealt with.

There are many questions within the ambit of social media communication that necessitate answers. For example, if someone by means of social media

- criticizes the government and/or call for protests against the government;
- posts false information;
- creates a false account on a social networking site, such as MySpace by impersonating another and posting information in the name of the impersonated person;
- spreads propaganda regarding a specific religious or political affiliation;
- makes threats to another person or to people in general;
- makes derogatory remarks about another person;
- posts an unsavoury or even a disturbing opinion or video;

does the conduct amount to merely bad, in some instances even mean behaviour, or is it social media abuse and if abuse, does it constitute a crime? The discussion will not only focus on the user of social media or those affected by the social media usage but also on how a government may deal with communication by means of social media. It is also about the role of the company that provides the social media, for example should Facebook block access to a posting that someone finds offensive or should the aggrieved person directly approach the Facebook user for removal?

Reference is increasingly made to the dangers of cyber bullying and trolling, especially where teenagers and young adults are the victims. Does such behavior amount to a crime and if it does not yet constitute a crime, should it be criminalized? If social media abuse does not constitute a crime, which other legal remedy, if any, is available to the aggrieved party?

It might be argued that the above given examples of communication should be protected by a right to freedom of expression. If this is the correct approach to follow, the question arises whether there should be any limitations to such right to freedom of expression. In this regard it would be relevant to determine when free speech would constitute hate speech. And even further to determine whether a government might block access to social media, for example by requesting YouTube to block access to a certain video in the interest of children?

The dangers of social media communication were highlighted with the 2011 UK riots following the police shooting and killing of a person. The scale of the disorder and the speed with which it spread were attributed to the use of social media such as Twitter, Facebook and Blackberry.

Blackberry in particular was singled out as a major operational factor in the spread of the riots. [ScCo13a]

Social media usage is not only about freedom of expression. The right of privacy of the social media users as well as those affected by the particular communication is also relevant. How should the right to freedom of expression be balanced in relation to the right to privacy of the user and affected or aggrieved party? Similarly in some instances the online social media behaviour may affect the reputation of another and thus impact on the right to dignity and these human rights must be balanced against each other. Concerns about the security of society might arise where social media is employed by terrorists to spread propaganda for their cause in order to recruit and inspire future terrorists.

In *H v W* 2013 (2) SA 530 (GSJ) which is the only South African civil court case pertaining specifically to social media behavior, the court stated: "The law has to take into account changing realities not only technologically, but also socially or else it will lose credibility in the eyes of the people. Without credibility, law loses legitimacy. If law loses legitimacy, it loses acceptance. If it loses acceptance, it loses obedience. It is imperative that the courts respond appropriately to changing times, acting cautiously and with wisdom." This statement of the court is especially relevant in respect of the application of criminal law to social media communication.

2 Defining Online Social Media

There is no universal or even concise definition for social media. A simplistic explanation is provided merely as background to the legal discussion. Nations [Natio13] contrasts traditional media as an instrument of communication to social media as a social instrument of communication. Social media is defined as online technology that people use, not only to share opinions, insights, experiences and perspectives but also to interact with other people. The technology used to interact may take different forms, such as blogs, message boards, bookmarks etc. Examples of social media applications are Wikipedia (used for the purpose of reference), MySpace, Facebook and Twitter (used for social networking), YouTube (used for video-sharing) and Instagram (used for photo-sharing) to name but a few. Although there are many social media websites, they all share a common link, namely that the user is able to interact with the website and interact with other visitors to that website. Social media can therefore be likened to a two-way street in respect of communication unlike traditional media such as television or newspaper in paper format which amounts to a one-way street [Natio13].

The impact of social media websites is best illustrated as follows: if Facebook was a country, it would be the third largest in the world behind only China and India [Qual13] and on YouTube more than four million videos are viewed daily and sixty hours of video loaded every minute. [ScCo13a]

The characteristics of social media contribute to possible abuse as communication by means of interaction takes place in an electronic, public and borderless medium where the information is instantaneous and globally visible at any time to all who can interact with the information anywhere from a computer, smart phone or tablet computer. Although the discussion focuses on abuse and criminalization, it should not diminish the many advantages of social media usage.

3 The Role of Criminal Law in Addressing Social Media Abuse

Criminal law prescribes which human conduct constitutes a crime and the punishment that may be imposed. [Burc11] Crime constitutes conduct that is not only a transgression against the victim but also against the public interests. A delict (tort), unlike a crime, is directed against private interests and unlike criminal law where the state prosecutes, the private (injured or aggrieved) party institutes a civil action. Criminal law affects directly the so-called perpetrator, the affected party (which can be a private person, society in general or the government) and the provider of the social media.

Cohen and Schmidt (CoSc13a) states: "And because what we post, email, text and share online shapes the virtual identities of others, new forms of collective responsibility will have to come into effect." But who will define collective responsibility? Will it be the role of the criminal law? When should a government intervene and criminalize conduct which is not yet criminalized? The role of criminal law is not to prescribe moral behavior to society and it might be that the dilemma confronting social media usage pertains to the grey area between unethical conduct and criminal behavior.

On 19 December 2012 the UK Director of Public Prosecutions issued interim Crown Prosecution Services (CPS) guidelines relating to the institution of criminal prosecutions against people posting offensive or abusive comments on social media websites. The final guidelines came into effect on 20 June 2013. These guidelines may address excessive social media prosecutions which have allegedly become a challenge in the UK ((http://www.indexoncensorship.org/2012/12/social-media-pro...). Before undertaking a brief overview of the guidelines, reference should be made to Paul Chambers v Director of Public Prosecutions [2012] EWHC 2157 (QB) (also referred to as the Twitter Joke trial) as this case served as a catalyst for the guidelines.

The facts are as follow: during late December 2009 and early January 2010 cold weather caused considerable disruption across Northern Ireland. Robin Hood Airport in South Yorkshire was one of many airports which were forced to cancel flights. On 6 January 2010 Paul Chambers, an intending traveler, sent a tweet stating that he would blow Robin Hood airport "sky high" if his flight to Belfast was cancelled due to bad weather. The message on Twitter was discovered a week later by an off-duty airport manager while doing an unrelated computer search. He reported it to the police that led to the arrest, prosecution and conviction of Chambers for sending a "public electronic message that was grossly offensive or of an indecent, obscene or menacing character contrary to the Communications Act 2003." His conviction for sending a menacing tweet drew widespread condemnation. He appealed three times against his conviction and in July 2012 the London High Court upheld the third appeal in his favour. The judgment concluded that "a message which does not create fear or apprehension in those to whom it is communicated or who may reasonably be expected to see it, falls outside this provision (of the 2003 Act)." The court found that the tweet was not of menacing character.

Against the background of the above-given case, the Director Public Prosecutions published final guidelines for prosecutors on the approach they should take in cases involving communications sent via social media. In accordance with the social media guidelines:

1. The content of the communications amount to a credible threat of violence, a targeted campaign of harassment against an individual or the breach court orders. Here the intention of the social media user and context of the communication must be considered. In the following examples the social media behaviour amounted to a crime, such as where a Facebook troll told people to target businesses run by Muslims after the murder of Drummer Lee Rigby early 2013 and where nine people tweeted the name of a woman raped in breach of laws that prevent the victims of sex attacks from being identified. [Webb13] An interesting case that clearly illustrates the relevance of the impact of social media behaviour is that of UK citizen, Reece Elliot, a troll who left messages using a false name on a memorial Facebook page for a US schoolgirl killed in a car crash in 2012. He wrote: "My father has three guns. I'm planning on killing him first and putting him in a dumpster. Then I'm taking the motor and I'm going in fast. I'm gonna kill hopefully at least 200 before I kill myself. So you want to tell the deputy, I'm on my way." Those who accessed the Facebook page were deeply concerned and reasonably believed that this could happen as killing of school children in the US have been rife in the past year. As a result of this posting, approximately 3000 children were kept out off school on that specific day. [BoWi13] The transgressor clearly wanted to elicit some response to his postings. The law enforcement agencies in the US and UK worked together to establish the identity of the transgressor and he was prosecuted and convicted in the UK. It may be asked whether the US and UK law enforcement agencies over-reacted and how this case differs from the Chambers case? Here the strongest competing factors were the aim to protect society on the one hand and freedom of expression on the other hand. As Keevan and McGrath [KeeMc01] states: The courts will have to be alive to the multiplicity of issues, rights and freedoms in attempting to strike the correct balance."
2. Prosecutions will be instituted where the content of the communications is considered grossly offensive, indecent, obscene or false and in the latter instance, a high threshold applies. In determining whether the content is grossly offensive, indecent or false, the context of the communication will have to be taken into consideration. Prosecution should only take place if it is in the public interest, or differently put, if it is both necessary and proportionate. The following factors may negate against the institution of prosecutions, bearing in mind that the list of factors are not exhaustive and that each case will have to be considered on its own facts and its own individual merits:
   - The suspect has expressed genuine remorse;
   - Swift and effective action has been taken by the suspect and/or others for example the service provider, to remove the communication in question or otherwise block access to it;
   - The communication was not intended for a wide audience, nor was that the obvious consequence of sending the communication; particularly where the intended audience did not include the victim or target of the communication in question;
   - The content of the communication did not obviously go beyond what could conceivably be tolerable or acceptable in an open and diverse society which upholds and respects freedom of expression;
   - The age and maturity of suspects should be given significant weight, particularly if they are under the age of 18; and
   - Communications which is in bad taste or controversial or unpopular or cause offence to a specific person.

The purpose of criminal law should be kept in mind. It is to protect the safety of citizens. Photographs of the autopsy of a person who had died mangled in a car accident may be disturbing or shocking, but is the conduct a crime? Over-criminalization of social media usage is a real concern and there must be constraints to criminal liability otherwise society will lose faith in the criminal justice system [Husa08]. Social media usage is not only about striking a balance between competing human rights but also when to prosecute and/or when to criminalize conduct.

4 Protection of Human Rights on Social Media

Reference was made to competing human rights. The examples already discussed and mentioned hereafter will illustrate that balancing the human rights of the user as well as the affected without limiting or abolishing rights is not an easy task.

The Universal Declaration of Human Rights which was adopted in 1948 established the right to freedom of opinion and expression. At the time of its adoption technologies such as social media did not exist. Today human rights protection in respect of an online medium, such as social media usage may come under threat if a country does not commit itself to the recognition and application of human rights protection in cyberspace. The Organization for Security and Co-Operation in Europe (OSCE) which consists of 57 participating states from Europe, Central Asia and North America proposed at the 2010 Astana Summit a Declaration on Fundamental Freedoms in the Digital Age which has not yet been adopted. [The Draft Declaration is available at http://www.osce.org/mc/97986] The purpose of the Declaration is ensuring a free and open Internet and the freedom of people to employ technologies to exercise their human rights and fundamental freedoms in cyberspace.

The European Convention of Human Rights provides in article 10: "Everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority. [The Convention is available at http://www.echr.coe.int/Documents/Convention_Eng.pdf] The European Court of Human Rights has made it clear that it protects not only speech which is well-received and popular, but also speech which is offensive, shocking or disturbing. In *Sunday Times v UK* (no 2) [1992] 14 EHRR 123 the court stated: "Freedom of expression constitutes one of the essential foundations of a democratic society…It is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also as to those that offend, shocking or disturbing…". Freedom of expression and the right to receive and impart information are not absolute rights and it cannot trump above all rights. They may be restricted but only where a restriction can be shown to be both necessary and proportionate. The Sunday Times case (at paragraph 50) emphasises that the restrictions must be narrowly interpreted and the necessity for any restrictions convincingly established.

5 Examples of Social media abuse and whether the Conduct constitutes a Crime

Reference will be made to examples of social media conduct and whether the conduct amounted to abuse and if affirmative, whether this abuse constituted a crime or should be criminalized. These examples may have occurred in different countries, but they address issues that confront all internet-connected nations at present. A distinction is drawn between social media communication that fall within the ambit of

- law enforcement; and
- national security.

5.1 Communications that may affect the Feelings of Others

A discussion on social media abuse will be incomplete without reference to one of the first reported social media abuse cases, namely the US case of *US v Drew* 259 F.R.D. 449 (C.D. Cal.2009). The facts are as follow [Qual13]: In 2006 Lori Drew lived with her teenage daughter in St. Charles County, Missouri. Her daughter had at one time been best friends with Megan Meier who lived down the street from Drew. Drew allegedly became concerned that the one-time friend of her daughter, Megan, was spreading rumours about her daughter. Drew, her daughter and Drew's employee created a MySpace account for a non-existent 16 year old boy under the alias "Josh Evans" and they used this account to discover whether Megan was spreading rumours about Drew's daughter. Drew then used the MySpace account to contact Megan who apparently believed that she was communicating with the 16 year old Josh Evans. Megan came to believe that he was her boyfriend and was completely unaware that he was a fictitious person who had been created by the mother of her one-time friend. She was therefore extremely distraught when this "Josh Evans" started berating her through a series of unfriendly comments and nasty remarks and allegedly a message to the effect that the world would be a better place without her. MySpace members whose profiles reflected links to "Josh Evans" also sent Megan negative messages. Megan, who was an emotionally vulnerable 13 year old girl at the time, committed suicide. The question was whether the conduct of Drew constituted a crime? There was considerable debate on whether she could be prosecuted and the Missouri prosecutors announced that they would not prosecute her. The federal government decided to pursue the case in Los Angeles where MySpace servers are located. She was ultimately prosecuted and convicted for *inter alia* a statutory offence in terms of the Computer Fraud and Abuse Act (CFAA), so-called anti-hacking legislation, whereby she had violated the website terms of service. The federal prosecutors argued that the violation of MySpace's terms of service was the legal equivalent of computer hacking. Her conviction was overturned on the basis that a conviction would have meant the criminalization of what would amount to a breach of a contract, namely the violation of website terms of service. [Zett09] It is clear that Drew abused social media.

Could her conduct have amounted to bullying or harassment? Cyber-bullying may be defined as the repeated harassment of and/or humiliation and/or threats toward a single individual via social media. Trolling is described as anyone who anonymously leaves crude, derisive or sarcastic commentary within an online public forum. Undeniably bullying, especially where children are the target, has become a global problem. In the USA there have been calls for cyber-bullying legislation on a federal level [Kenn13]; similarly calls have been made for specific legislation in the UK (http://www.teachtoday.eu/en/Teacher-advice/Cyberbullying/...). Drew's conduct may have constituted cyber-bullying.

In South Africa the Prevention of Harassment Act 17 of 2011 came into operation in 2013. The act protects a person from behaviour which may not constitute a crime, but which may impact negatively on various rights of an individual. [Maws13] In terms of this legislation, the person (applicant) who is being harassed (bullied) may apply to the court for an interim protection order, in other words the legislation provides for a civil remedy against the person harassing him. This order will be granted as long as the court is satisfied the respondent has harassed or is harassing the applicant and harm has or may be caused. Harassment in terms of the act also includes sexual harassment. Harm is defined in the act as mental, psychological, physical or economic harm. The act also stipulates that service providers may be forced to hand over the name, surname, identity number and addresses of the person to whom the IP address, email or mobile phone number belongs. As soon as the order is made final, the applicant receives a warrant of arrest that may be handed to the police if the respondent fails to abide by the order. A maximum term of 5 years imprisonment might be imposed on a person who contravenes the order. However, if the transgressor makes threats towards the victim with the consequence that the victim feels unsafe the conduct may constitute the crime of assault.

Social media enables so-called "revenge pornography." A former scorned boyfriend may for example post naked and compromising photographs of his ex-partner online with many consequences such as the victim receiving anonymous Facebook messages for sexual intercourse. This social media conduct is an example of stalking and/or harassment and/or defamation. South Africa provides for this situation in the Domestic Violence Act 116 of 1998 which is similar in application to the Prevention of Harassment Act 17 of 2011. The victim may also request the service provider to remove the photographs, although the remedy may not always be effective as the photographs may appear on another website. A shocking example of "revenge porn" was the case where the perpetrator, an ex-marine, posted photos of his former girlfriend on Facebook with a message purportedly written by her requesting a rape fantasy to be fulfilled. Pretending to be her, he arranged a date and time with the rapist (more than 100 men had responded) and she was brutally raped in her home. Both the marine and rapist were sentenced to 60 years imprisonment. [Lasl13] As indicated the victim is not without a legal remedy, but it has been said that the criminal law lags behind with enforcement of the law being ineffective. [Lasl13]

The creation of a false social media account and the impersonation of another should be prosecutable but on the basis of which crime? In South Africa the transgressor may be prosecuted for the common law (unwritten law) crime of fraud, but it might be advisable to consider implementing specific legislation such as identity theft. The problem with this type of fraud is that no monetary value can be established, but the damage to the reputation of the affected party may be considerable. It is therefore doubtful whether the prejudice suffered will be reflected in the sentencing. Although hacking is not under discussion, a person may hack into another's Facebook profile and post communications as if it originates from the registered Facebook user. In the instance of the Drew case, she did not impersonate a real person and that alone, does not constitute a crime. However, posting false information which results in law enforcement agencies wasting resources in the investigation of such information should constitute a crime.

In a first of its kind, a South African civil court had to decide in *H v W* 2013 (2) SA 530 (GSJ), whether the behavior of the respondent on Facebook amounted to social media abuse and more specifically defamation. The remedy the applicant sought was interestingly enough, not criminal and/or civil liability for defamation but the removal of the posting from her Facebook as well as any other social media. The court could only make an order and determine the terms of the order once it had established whether the posting was defamatory to the applicant or not.

The facts are as follow: the applicant was an insurance broker who was separated from his wife. They were engaged in divorce proceedings. They were the parents of three minor children. The respondent had been a close friend of the applicant long before he married his wife. The applicant assisted the respondent in starting a business and the respondent lent the applicant money to tide him over financial difficulties. On 14 January 2012 the applicant's wife left him and moved in with the respondent. This resulted in the severing of the friendship between the applicant and the respondent. The applicant also "defriended" the respondent from his Facebook.

On 27 February 2012 the respondent published the following posting on her Facebook: "Letter to WH (the applicant) – for public consumption. I wonder too what happened to the person who I counted as a best friend for 15 years, and how this behavior is justified. Remember I see the broken hearted faces of your girls every day. Should we blame the alcohol, the drugs, the church or are they more reasons to not have to take responsibility for the consequences for your own behavior? But mostly I wonder whether, when you look in the mirror in your drunken testosterone haze, do you still see a man?"

The applicant took exception to the posting stating that it damaged his reputation and his right to privacy as the posting portrayed him not only as a person who has a problem with drugs and alcohol but also as a father who does not provide financially for his family nor cares about his family.

The respondent saw her behavior, in this instance the posting published on her Facebook, not as abuse within the ambit of defamation. She saw her posting merely as an incentive for the applicant to reflect on his life and the road he had chosen.

To determine whether the posting was defamatory the South African court had to determine whether a reasonable person of ordinary intelligence might reasonably understand the words concerned to convey a meaning defamatory of the applicant. The court found the posting defamatory and Facebook users face civil action if they post defamatory comments about another. [Ajam13]

Once the court had established that the accused had been defamed, the court had to decide on the order. The respondent argued that the applicant could have requested Facebook to block the posting. The court stated that one should focus on the users rather than on Facebook itself.

The court ordered the respondent to remove the posting on her Facebook. The court was not willing to grant an interdict restraining the respondent from posting any information pertaining to the applicant on Facebook or any other social media. The court also did not make an order for her arrest for non-compliance as the court felt that "everyone knows that life can be made uncomfortable for those who do not comply with court orders." The court also felt it could not order the sheriff to remove the posting if the respondent failed to do so.

The applicant may have decided to lay a criminal charge as the conduct of the respondent amounted to criminal defamation. Criminal defamation in South Africa is a common law crime. It is defined as a) publication (verbal and writing – on paper and electronic writing) b) of a defamatory allegation concerning another which is made c) unlawfully and d) intentionally. However, applying the UK prosecutors' guidelines in respect of social media prosecution to the content, the prosecutor may have decided not to institute prosecution as the communication may not be deemed grossly offensive, even though it may be distasteful or painful to those subjected to it. A person does not have a right not to be offended and if offended, then the civil law should be employed. The main role of law enforcement is to protect the safety of society and not feelings. [Grig13]

This case should be contrasted to a case in Sweden where two teenage girls, aged 15 and 16 years respectively, were convicted of criminal defamation for posting insults about their class mates and calling them sluts. The defamation conviction was a result of the girls creating the "sluts of Gothenburg" account on the photo-sharing social media site, Instagram and encouraging people to share photos of teenagers whom they claimed were sexually promiscuous. [Gye13] Was this prosecution justified or should an alternative civil remedy have been used?

The following examples illustrate the problem of determining when communication constitutes hate speech, especially in a diverse and multi-cultural society. Hate speech is a communication that vilifies a person or a group based on discrimination in respect of sexual orientation, gender, religion, ethnicity or race. For example discriminatory comments were elicited when a Romanian student attending a Hungarian school wore a headband with the colours of the Romanian flag on Hungary's National day [Lajm13] and a US soccer player posted on his Facebook profile a racist remark regarding the then newly elected Obama as US president [Qual13]. In 2013 Khumalo, a black South African Facebook user invited his 493 Facebook friends to "celebrate the death of whiteness" with reference to a school bus crash in which 42 white children drowned. Khumalo listed the names of 24 of the 42 victims, noting that their deaths were "much appreciated, my lord." His social media communication offended the victims' family. His conduct was not a crime but an expression of his feelings. Had he promoted violence against a group of people it may have constituted a crime. A charge was laid with the South African Human Rights Commission as his communications were perceived as hate speech and the "punishment" imposed was the cleaning of the gravesites. Khumalo showed remorse by removing the communication and lodging on his Facebook page an apology to those whom he had offended. [Roan13]

The above examples illustrate that social media users are increasingly engaging in social media to express their thoughts and feelings without taking cognizance of the consequences of such communications. By giving publicity to social media conduct and the boundaries of such communication, awareness is created amongst users.

5.2 Communications that may affect the Safety of Society

Examples have been given of communication that threatens the safety of a person or a group of persons. Most of the social media conduct will fall within the ambit of law enforcement.

A more problematic and complex issue is determining when social media communication affects the safety of society as a whole and whether it falls within the ambit of law enforcement or national security? It is important to differentiate in this regard between an individual's right to freedom of expression as manifested in protest action on the one hand and subversive activity amounting to a crime against the state as high treason on the other hand. The 2010 Arab Spring protests were for example organised on Facebook and Twitter. [ScCo13b] However, when the call is made for violence, such conduct may constitute a crime. Extremists may also use social media for propaganda which may result in an increase in terrorist acts, political assassinations and sectarian conflicts. Governments such as China have blocked access to social media and has stated "laws and regulations clearly prohibit the spread of information that contains contents subverting state power, undermining national unity [or] infringing upon national honour and interests." [ScCo13b]

But how far does safety of society extend? May a government request a service provider to remove communications that are deemed harmful? The Russian government has requested social media providers such as Facebook, Twitter and YouTube to remove material that it deemed illegal or harmful to children, for example a video promoting suicide. [Kram13] The communication may originate from outside the Russian borders but even within its borders, such a video may be seen as freedom of expression and such limitation questioned. The UK government has also requested internet providers, such as Google, Facebook and Yahoo as well as phone companies to use filtering technology to limit access to harmful material such as child sexual abuse images. [Chap13] It is submitted that freedom of expression should not extend to child pornography. In South Africa the distribution and accessing of child pornography is a crime and there is a statutory obligation on service providers to make use of filtering technology. In this instance the right to freedom of expression, which includes the right to information, is limited and could be likened to censorship but only in respect of specific communications.

6 Conclusion and the Way Forward pertaining to Criminalization of Social Media Abuse

The reasons why people utilize social media communication which centers on social interaction and networking will not change, although the tools and/or technologies in socialization and democratization of information might change. Social media usage will gain momentum as more users, especially in developing countries, gain access to social media by means of their computers or mobile phones. The advantages of social media use by far outweigh the disadvantages constituted by abuse, but severe consequences are often suffered as a result of these abuses.

A dilemma facing law enforcement is when to institute criminal prosecutions. Social media abuse cannot be down-played, but over-zealous prosecutions will not address these problems related to social media. The UK CSP guidelines for social media prosecutions may serve as a yardstick in preventing excessive prosecutions, as over-criminalization results in an imbalance between human rights protection and law enforcement, the loss of credibility in the legal system and suppress the advantages of social media use.

The purpose of the contribution is to establish the parameters of acceptable social media usage and the legal implications when social media usage moves outside these acceptable standards. Acknowledging the severe consequences abusive use of social media may have, a conservative approach is advocated to the application of criminal law in addressing these ills. However, the discussion is only now beginning. Even if the limits to communication is established, policing of social media and enforcement of the criminal laws pertaining to social media usage within the parameters of human rights and law enforcement and/or national security investigations must be determined. If the criminal laws are not enforced or perceived not to be enforced, the criminal justice system will lose credibility in the eyes of the public whom the criminal law must protect.

References

[Ajam13] Ajam, Kashiefa: „"SA man wins Facebook slander case." In: http://ww.iol.co.za/news/crime=courts/sa-man-wins-faceboo...

[Burc11] Burchell, Jonathan: South African Criminal Law and Procedure. Publisher: Juta & Co Ltd, Cape Town, South Africa, 2011, page 3.

[Chap13] Chapman, James: "Internet Gaints could end up in the dock if there is another horrific case like April Jones". In: http://www.dailymail.co.uk/news/article-2338632/Internet-gi...

[Gye13] Gye, Hugo: "The Instagram 'slut shaming' which sparked a riot: Teenage girls who set-up account are jailed an fined 55, 000 after hundreds took to the streets of Gothenburg in violent protest." In: http://www.dailymail.co.uk/news/article-2348959/Teenbage-g

[Grigg12] Griggs, Brandon: "When is social media use a crime?" In: http://edition.cnn.com/2012/12/18/tech/social-media/newtown-social-media-crime

[Husa08] Husak, Douglas: Overcriminalization. Publisher: Oxford University Press, New York.

[Kenn13] Kennedy, Kerry: "The Time is Now for a Federal Anti-Bullying Law". In: http://www.huffington-post.com/kerry-kenneyd/the-time-is-n...

[KeMc01] Keevan, Tim and McGrath, Paul: Email, the Internal and the Law. Publisher: EMIS Professional Publishing, Hertfordshire, 2001, page 57.

[Kram13] Kramer, Andrew: "Russians selectively blocking Internet." In: http://www.nytimes.com/2013/04/01/technolgy/russia-begi...

[Lasl13] Lasley, Tabita: "Revenge is a dish best served cold." In: Marieclaire, June 2013, pages 65 – 66.

[Maws13] Mawson, Nicola: "Cyber bully Act becomes law." In: http://www.itweb.co.za/index.php?option=com_content&vie...

[Misc11] Mischke, Carl: "Social networking, privacy and dismissal." In: Contemporary Labour Law, vol.21, no. 2 September 2011, pages 11 – 20.

[Natio13] Nations, Daniel: "What is social Media?" In: http://webtrends.about.com/od/web20/a/social-media.htm

[Qual13] Qualman, Erik: Socialnomics. Publisher: John Wiley and Sons, USA, pages xvii, 11, 95, 98, 283, 286.

[Roan13] Roane, Brendan: "Facebook racist: I'm sorry." In: http://ww.iol.co.za/news/south-africa/gauteng/facebook-rac...

[ScCo13a] Schmidt, Eric and Cohen, Jared: The New Digital Age. Publisher: John Murry, London, England, pages 7, 73, 156 – 158, 122, 123,127, 157, 181.

[ScCo13b] Schmidt, Eric and Cohen, Jared: "Web censorship: the net is closing in." In: http://ww.guardian.co.uk/technology/2013/apr/23/web-cens...

[Webb13] Webb, Sam: "Facebook and Twitter Trolls will avoid prosecution if they apologise as new rules impose a 'high threshold' for court action." In: http://www.dailymail.co.uk/news/article-2345048/Offensive-...

[Zett09] Zetter, Kim: "Judge acquits Lori Drew in Cyberbullying Case, Overrules Jury." In: http://www.wired.com/threatlevel/2009/07/drew_court/

Mobile Security & Applications

Protected Software Module Architectures

Raoul Strackx[1] · Job Noorman[1] · Ingrid Verbauwhede[2]
Bart Preneel[2] · Frank Piessens[1]

[1]iMinds-DistriNet, KU Leuven
Celestijnenlaan 200A, 3001 Leuven, Belgium
{Raoul.Strackx | Job.Noorman | Frank.Piessens}@cs.kuleuven.be

[2]iMinds-COSIC, KU Leuven
Kasteelpark Arenberg 10, 3001 Leuven, Belgium
{Ingrid.Verbauwhede | Bart.Preneel}@esat.kuleuven.be

Abstract

A significant fraction of Internet-connected computing devices is infected with malware. With the increased connectivity and software extensibility of embedded and industrial devices, this threat is now also relevant for our industrial infrastructure and our personal environments. Since many of these devices interact with remote parties for security-critical or privacy sensitive transactions, it is important to develop security architectures that allow a stakeholder to assess the trustworthiness of a computing device, and that allow such stakeholders to securely execute software on that device. Over the past decade, the security research community has proposed and evaluated such architectures. Important and promising examples are *protected software module architectures*. These architectures support the secure execution of small protected software modules even on devices that are malware infected. They also make it possible for remote parties to collect *trust evidence* about a device; the remote party can use the security architecture to collect measurements that give assurance that the device is in a trustworthy state.

In this paper we outline the essential ideas behind this promising recent line of security research, and report on our experiences in developing several protected module architectures for different types of devices.

1 Introduction

Any programmable device is at risk of being reprogrammed, exploited, or infected with malware by attackers. This risk goes up significantly for network-connected devices, as exploitation or infection can now be done remotely. Protection against this threat is significantly harder for devices that are *open* in the sense that they support software extensibility, possibly even by several parties that do not necessarily trust each other. Historically, the first such devices were classical computers (desktops and servers), and history has taught us that the threat of malware infection and other software attacks against these devices is very real indeed.

Over the past years, more and more embedded computing devices are being connected to the Internet, and many of these devices are open to some extent to software extensibility. Examples include smartcards that support over-the-air updates, programmable sensor-networks, set-top boxes and internet-connected TV's as well as SCADA (supervisory control and data acquisition) systems that control important components of our critical infrastructure. The increasing connec-

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_21, © Springer Fachmedien Wiesbaden 2013

tivity of all these devices, as well as their increasing impact on our society, gives rise to significant threats. Viega and Thompson [ViTo12] describe several recent incidents and summarize the state of embedded device security as "a mess".

An important research question in this context is: what kind of infrastructural support for security (such as hardware support, or operating system support for security) will make it easier for device manufacturers to construct secure networked and extensible devices? Of course, we have built up a rich body of experience on securing classical computing devices, such as servers or desktops. A first important technique is the use of hardware support for virtual memory, and processor privilege levels. An operating system can build on this support to run software modules in isolated processes, and the operating system can guard the interactions between these various processes. A second important technique is the use of a memory-safe virtual machine (for instance a Java VM) where software modules are deployed in memory-safe bytecode, and a security architecture in the VM guards the interactions between them. While these well-understood techniques could be ported to the new context of networked embedded devices, there are also several important known disadvantages to these techniques. First, there is the cost in terms of required resources such as chip surface, power or performance that might be unacceptable in some embedded device scenarios. Second, these classic solutions all require the presence of a sizable trusted software layer (either the operating system, or the VM implementation). History has shown that it is very difficult to get such a software layer sufficiently secure that it cannot be exploited by software attacks such as buffer overflows or injection attacks [YJP12]. And finally, with these classic solutions it is non-trivial to securely support *remote attestation*, where a stakeholder can remotely check that a specific software module is running untampered on a remote device.

As a consequence, researchers have started investigating alternatives. One important line of research is developing *protected (software) module architectures* [MPP+08, MLQ+10, StPi12]. These are security architectures running independent of a classical operating system, and that can execute security sensitive code in an isolated area of the system. The isolation does not rely on the operating system, thus improving the security guarantees that can be offered. Of course, an important design goal (and design challenge) is to realize this while remaining compatible with current operating systems and hardware. Most of these proposed systems leverage recent hardware extensions for trusted computing or virtualization to execute code. These architectures were originally developed for high-end computing devices such as desktops and servers, to better protect against the malware threat.

A second important line of research is the development of program-counter based memory access control systems for isolation. This is an alternative kind of memory protection that is less expensive than full support for virtual memory, yet it is sufficient to implement strong isolation between software modules, and it is very compatible with remote attestation. Several researchers have independently proposed program-counter based memory access control as a suitable memory protection mechanism for low-end embedded devices [EFPT12, StBP10].

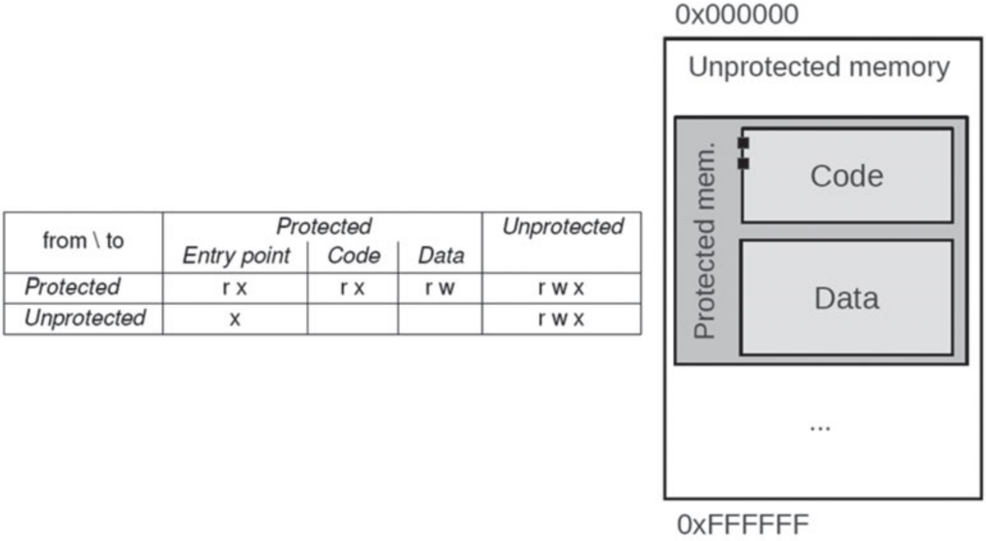
In this paper, we report on our experiences in developing several protected software module architectures that build on the idea of program-counter based memory access control. We show that the combined idea of protected modules using program-counter based access control can be useful for a range of systems, ranging from low-end embedded devices (where memory protection would be built into the hardware) over desktops and servers (where memory protection can be either realized by means of a hypervisor or in an operating system kernel). In general, these new security architectures contribute to increasing the trust that stakeholders can have in a networked computing device, either by providing strong assurance about the state of a device (as in remote attestation), or by supporting measurements of the state of the device that can be used as heuristic evidence of trustworthiness.

2 Program-Counter based Memory Access Control

Program-counter based memory access control is a memory protection technique intended to provide isolation between software modules running on the same device, but that do not necessarily trust each other. As such, it is a low-cost alternative to virtual memory, processor privilege levels and process isolation. We first explain how program-counter based memory access control works, and then we show that it provides a very strong and precise notion of isolation between modules.

2.1 Software Modules and Memory Access Control

Software modules are essentially memory sections. One module consists of two sections: a text (or code) section containing protected code and constants and a protected data section. In addition, the text section has a fixed number of *entry points*. These are addresses of memory locations in the text section where control flow is allowed to enter the module.



from \ to	*Protected*			*Unprotected*
	Entry point	*Code*	*Data*	
Protected	r x	r x	r w	r w x
Unprotected	x			r w x

Fig. 1: A software module and the memory access control rules

Figure 1 shows a memory space with one protected module with two entry points in the code section. The Figure also summarizes the memory access control rules that program-counter based memory access control enforces. While some details of this access control matrix vary in different implementations, the key characteristic is that access rights to memory, depend on where the processor is executing (i.e. on the value of the program counter). If the program counter is in unprotected memory then only unprotected memory can be read or written. Execution can continue to other unprotected memory, or to one of the entry points of a protected module. After jumping to an entry point, the program counter is now in the code section of a protected module, and the protected data section of that module can be read or written, and execution can proceed to any address of the protected code section of that module. In addition, any access to unprotected memory is allowed.

When there is more than one protected module in memory, the rules for accessing the code and data sections of a given module treat all the other modules as if they were unprotected memory. So protected module A can only jump to the entry points of module B; it cannot read or write the data section of module B, or start executing in the code section at any other address than an entry point.

The key underlying idea of this memory access control model is that it ensures that *only the code of a given module can manage the state of that specific module.*

2.2 Isolation Properties

Program-counter based memory access control is a sufficiently strong building block to get all the isolation guarantees that modern programming languages can express at source code level [ASJP12]. Modern high-level programming languages such as Java, C#, ML or Haskell offer protection facilities such as abstract data types, the private field modifier, or module systems. These programming language concepts were designed to enforce software engineering principles such as information hiding and encapsulation. But these can also be used as building blocks to ensure security properties of programs. For instance, declaring a class instance variable private in Java protects the integrity and confidentiality of that field towards instances of other classes.

Unfortunately, these protection features are typically lost when the program is compiled. Suppose for instance that we compile a Java program to native machine code. Then, an attacker that has injected malware in the memory space of the program can read or write any private variable, thus violating that variable's confidentiality and integrity. In other words, the isolation guarantees offered by the source language can be violated.

However, recent research [ASJP12] has shown that it is possible to maintain the security properties of a high-level program even after it is compiled into a lower-level language (such as native code), by relying only on program-counter based memory access control. This is strong evidence that this kind of memory access control is sufficient for all practical purposes. We can get the isolation properties that modern high-level programming languages support.

3 Three Implementations

The idea of program-counter based memory access control can be implemented in different ways. In this Section, we discuss our experience with three implementations, each of these with its own advantages and limitations:

- *Sancus* is a hardware-level implementation, that in addition implements a very strong form of remote attestation

- *Fides* is a hypervisor-level implementation, that shows that the additional isolation offered by program-counter based memory access control can also be efficiently implemented on legacy desktops and servers
- *Salus* is a kernel-level implementation that offers program-counter based memory access control as an additional layer of isolation on top of regular virtual memory

We briefly discuss each of the three implementations.

3.1 Sancus

The Sancus architecture [NAD+13] implements program-counter based access control in hardware in a microprocessor, and in addition implements a remote attestation mechanism.

The architecture targets systems where a single infrastructure provider, IP, owns and administers a (potentially large) set of microprocessor-based systems that we refer to as nodes N_i. A variety of third-party software providers SP_j are interested in using the infrastructure provided by IP. They do so by deploying software modules $SM_{j,k}$ on the nodes administered by IP.

A Sancus node N (Fig. 2) is a low-cost, low-power microcontroller (our implementation is based on the TI MSP430). The processor in the nodes uses a von Neumann architecture with a single address space for instructions and data. The processor is extended with a protected storage area that, for each protected software module loaded in main memory, maintains the following metadata:

- The bounds of the text and data sections of the module. The processor uses these to enforce the memory access control rules.
- A cryptographic module key $K_{N,SP,SM}$ that is used for remote attestation and authenticated communication.

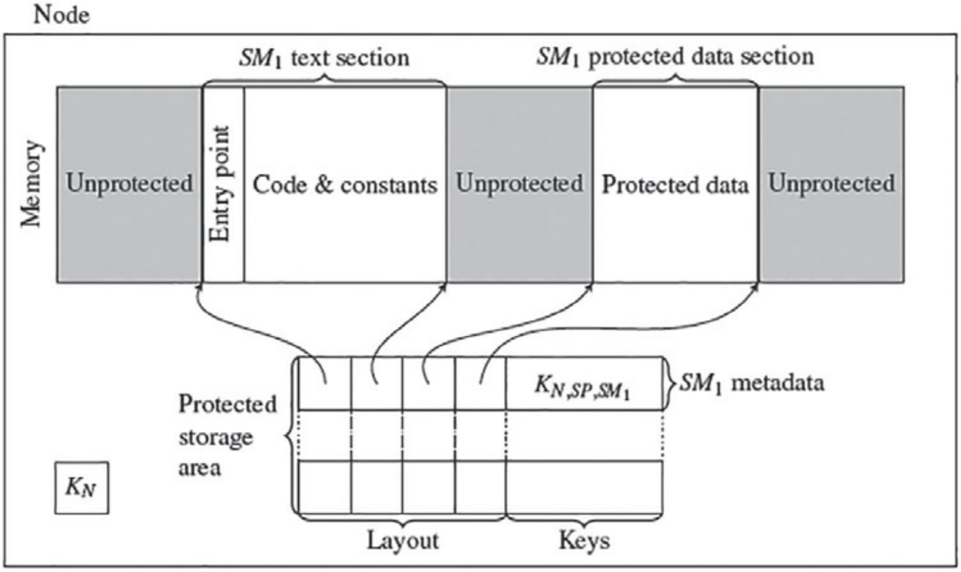


Fig. 2: A Sancus node (from [NAD+13])

The module key $K_{N,SP,SM}$ can only be used by (1) a software module SM running on a specific node N on behalf of the software provider SP, and (2) by the SP itself. The hardware enforces (1) by deriving the key from the hash of the contents of the text section of the module (among other things), thus guaranteeing that any tampering with the module would invalidate the key. This is the basis for remote attestation support and authenticated communication in Sancus.

The essence of the security argument for remote attestation in Sancus is the following: the module key $K_{N,SP,SM}$ can only be used by means of specific processor instructions, and the hardware of node N ensures that the use of key $K_{N,SP,SM}$ is limited to code from module SM. In other words, some form of program-counter based access control to cryptographic operations is enforced to ensure that only the correct module can use a module key. For a detailed description of the system, and a security and performance evaluation, we refer the reader to [NAD+13].

3.2 Fides

The Fides architecture [StPi12] implements program-counter based access control in a hypervisor running on top of a commodity desktop processor. It shows that the idea of program-counter based access control can be used efficiently on modern processors, even if one cannot change the hardware.

Figure 3 sketches the implementation strategy: A hypervisor runs two separate virtual machines that both have the same logical view of physical memory, but with different memory access control rights. The Legacy virtual machine (on the right) runs the legacy operating system and legacy software. The memory belonging to protected software modules (called Self-Protecting Modules or SPM's in Fides) is made inaccessible in this legacy virtual machine, and any attempt to access it will trap to the hypervisor. The hypervisor then verifies the memory access control rules (in this case, it checks if an appropriate entry point was called) and if so switches to the secure virtual machine (on the left). That second virtual machine enables access to the memory regions belonging to the module that was just entered. A small dedicated kernel in the second virtual machine enforces the memory access control rules between modules.

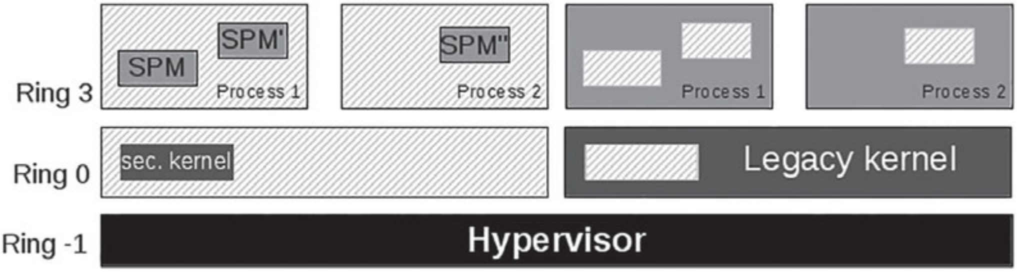


Fig. 3: The implementation strategy behind Fides (from [StPi12])

For a detailed description of the Fides system, and a security and performance evaluation, we refer the reader to [StPi12].

3.3 Salus

Our third and final implementation is Salus, a kernel-based implementation. Salus applies the idea of program-counter based memory access control in the virtual address space of processes running on a Linux operating system. In other words, the isolation offered by program-counter based memory access control is used as *an additional layer of protection* over the isolation offered by the process abstraction in the Linux operating system.

In Salus, the effects of program-counter based access control are obtained by making sure that a trap to the operating system kernel occurs on entering and exiting of a module. On entering, this is ensured by setting memory protection of modules to no-access as long as the module is not active. Hence, attempting to enter will trap with a memory access violation to the kernel that can then check if an entry point is being called and if so change the memory access rights. On exit of a module this is achieved by means of a new system call that resets memory access rights before proceeding with execution outside of the module.

Similar to how Sancus extends the idea of program-counter based access control to cryptographic operations offered by the hardware, Salus extends this to system calls. Protected modules can be configured with a policy that says which system calls are allowed to occur within the module. This opens the possibility to use Salus not only for protecting a module from its environment, but also for enforcing modules to operate under a least-privilege regime.

For a detailed description of the Salus system, we refer the reader to the master thesis of Niels Avonds [Avon13].

4 Application scenarios

Program-counter based access control is a generic software isolation mechanism, and it can be used in a variety of application scenarios. The three different implementations we have discussed have different advantages and limitations, and depending on the application scenario, one implementation might be preferable over the other. In this Section, we list a few possible application scenarios, and discuss what implementation technique fits best with them.

4.1 Trustworthy extensible networked systems

All kinds of computing devices play a crucial role in our society and in our individual lives, both private and professional. On the high-end side, there is the emergence of cloud computing, while on the low-end side there is an explosion of shrinking or disappearing devices: a modern car has over 100 micro-controllers, RFID chips are replacing barcodes, and sensor networks are common in logistics, healthcare and many other application domains.

Many of these networked computing devices are software extensible by a variety of stakeholders. Any system that supports extensibility (through installation of software) by several stakeholders must implement measures to make sure that the different software modules cannot interfere with each other in undesired ways (either because of bugs in the software, or because of malice).

We believe such extensible networked systems are the prime application scenario for the protected module architectures described in this paper. Since both minimization of the trusted software stack, as well as support for remote attestation of the state of a device are important requirements for this application scenario, a hardware-level, Sancus-style implementation seems the most appropriate. In particular for small embedded devices, where hardware heterogeneity is common, customization of the hardware to support Sancus could be a feasible path.

4.2 Isolating security critical components of applications

A more short-term application scenario considers the protection of desktops and servers against the malware threat. Given the prevalence of malware-infections on the Internet, it makes sense to deploy additional protection for security critical components (like cryptographic libraries) running on these systems, to make sure that secret keys cannot be stolen from such a component even if the system is infected.

This scenario was the original motivating scenario for protected module architectures such as Flicker [MPP+08] and TrustVisor [MLQ+10]. By implementing program-counter based memory access control in a hypervisor, as in Fides, one can get such an additional protection with the additional benefit that – because of the shared memory address space between protected modules and the rest of the program – porting legacy programs to such a protected module architecture is made simpler.

4.3 Trust assessment modules

For existing legacy systems, it may be infeasible to redesign and re-implement them with better isolation and/or attestation support. Changing the hardware, or even refactoring the application code to support protected modules, might be too costly. Yet, even for such systems, it is important for remote stakeholders to gather evidence about the trustworthiness of a remote networked system.

In a third application scenario, the protected software module architecture is used to protect modules that are added to the system purely for the purpose of gathering trust evidence. Since these security architectures are designed to give protected modules access to the entire unprotected legacy system state, they can be used to securely execute measurement modules that inspect the state of legacy software while being protected in case that legacy software has been infected by an attacker. In other words, modules have the necessary access to perform measurements, and are protected from tampering by the environment they are measuring.

Such *trust assessment modules* will analyze the state of other software applications and services on the system that they are part of to compute trust evidence, i.e. metrics that give an indication of the likelihood that a software application or service is in a trustworthy state and has not been compromised. They perform a function similar to intrusion detection or virus detection systems.

Since trust assessment modules run on top of a legacy system, it is mainly the Fides and Salus implementations that are useful for this application scenario. Fides is to be preferred, as it has a smaller trusted computing base, but Salus might be applicable and give better performance for cases where the system to be monitored is a single process (e.g. a server process). In that case, the trust assessment module can be made application-specific: it could monitor for instance whether state invariants that are known to be valid in the application are violated.

4.4 Containing application vulnerabilities

Software applications are often built from modules at source code level, but after compilation that modularization is lost. As a final application scenario, we consider the case where compilation maps source-level modules on protected modules. While this kind of compilation is difficult for classic isolation mechanisms (consider for instance the effort involved in refactoring a server program such that its modules run as different processes), this is easier for program-counter based memory access control, as the application still runs in one single address space.

An important advantage of this secure compilation is that vulnerabilities in a single module can now only impact that module. Hence, if we combine this with support for limiting the privileges of individual modules (as for instance in Salus, where the operating system calls available to modules can be limited), then we get an important additional layer of protection. By limiting the privileges of likely vulnerable modules (such as a parsing module, or a network-facing module), the bar is raised significantly for attackers, as exploiting the likely vulnerable module will give the attacker less privileges on the system under attack.

Both for performance reasons, as well as because of its potential to support least-privilege policies, this application scenario is best supported by kernel-level implementations such as Salus.

5 Limitations

While we hope that this paper convinces the reader of the potential value of protected software module architectures based on program-counter based memory access control, no security architecture is perfect, and the architectures described in this paper have limitations that require further research.

An important limitation is that the protection of a module depends on the correct implementation of that module: if a module contains a vulnerability, then protection guarantees can be undermined. For instance, if a module that implements a cryptographic library has a method that returns the key, then running that library inside a protected module offers no additional protection for key secrecy. Moreover, vulnerabilities in protected modules can be subtle and hard to detect. Hence, an important avenue for future work is the development of analysis and verification techniques for protected modules.

A second limitation is that it is difficult to marry protected modules and multi-threading in a secure way, in particular in cases where multiple modules collaborate. Multi-threading can give rise to time-of-check-to-time-of-use vulnerabilities, where one module checks the presence of another module before calling it, but between the check and the actual call another thread intervenes and removes the module that is called. Further research is needed to understand the interactions between multi-threading and program-counter based memory access control.

Finally, some important security concerns are not addressed yet by the protected module architectures described in this paper. In particular, the concern of *state-continuity* [PLD+11], i.e. the guarantee that an attacker cannot roll back a module to an earlier state by crashing and rebooting the system is an important avenue for future work.

6 Conclusion

With the combined trends of more network connectivity and more software extensibility for computing devices comes an increased threat of exploitation and malware infection. In this paper, we have surveyed a recent line of research that is developing countermeasures for this threat. Protected software module architectures provide additional protection against exploitation and can support the secure collection of trust evidence about the state of computing devices.

We have discussed three implementations of such protected software module architectures, and have considered a variety of application scenarios where these implementations might be useful. We also identified remaining limitations in these architectures that should be addressed by future research.

Acknowledgments

This work has been supported in part by the Intel Lab's University Research Office. This research is also partially funded by the Research Fund KU Leuven, and by the EU FP7 project NESSoS. With the financial support from the Prevention of and Fight against Crime Programme of the European Union (B-CCENTRE).

Raoul Strackx holds a PhD grant from the Agency for Innovation by Science and Technology in Flanders (IWT).

References

[ASJP12] Pieter Agten, Raoul Strackx, Bart Jacobs, and Frank Piessens: Secure compilation to modern processors, In: IEEE 25th Computer Security Foundations Symposium (CSF 2012), p. 171-185.

[Avon13] Niels Avonds: Implementation of a State-of-the-Art Security Architecture in the Linux Kernel. Master thesis KU Leuven, 2013.

[EFPT12] Karim El Defrawy, Aurélien Francillon, Daniele Perito, and Gene Tsudik: SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2012).

[MLQ+10] Jonathan M. McCune, Yanlin Li, Ning Qu, Zongwei Zhou, Anupam Datta, Virgil D. Gligor, and Adrian Perrig: TrustVisor: Efficient TCB Reduction and Attestation. In: IEEE Symposium on Security and Privacy 2010, p. 143-158.

[MPP+08] Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki: Flicker: an execution infrastructure for tcb minimization. In: EuroSys 2008, p. 315-328.

[NAD+13] Job Noorman, Pieter Agten, Wilfried Daniels, Raoul Strackx, Anthony Van Herrewege, Christophe Huygens, Bart Preneel, Ingrid Verbauwhede, and Frank Piessens: Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base, In: 22nd USENIX Security symposium, 2013.

[PLD+11] Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens, and Jonathan M. McCune: Memoir: Practical State Continuity for Protected Modules. In: Proceedings of the 2011 IEEE Symposium on Security and Privacy, p. 379-394.

[StBP10] Raoul Strackx, Frank Piessens, and Bart Preneel: Efficient isolation of trusted subsystems in embedded systems, In: SecureComm 2010, Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering: Security and Privacy in Communication Networks, volume 50, p. 1-18, 2010.

[StPi12] Raoul Strackx, Frank Piessens: Fides: Selectively hardening software application components against kernel-level or process-level malware, In: Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), p. 2-13.

[ViTo12] John Viega, and Hugh Thompson: The state of embedded-device security (spoiler alert: It's bad). In: IEEE Security & Privacy Magazine, volume 10, issue 5, 2012, p. 68-70.

[YJP12] Yves Younan, Wouter Joosen, and Frank Piessens: Runtime countermeasures for code injection attacks against C and C++ programs, In: ACM Computing Surveys, volume 44, issue 3, p. 1-28, 2012.

Securing Communication Devices via Physical Unclonable Functions (PUFs)

Nicolas Sklavos

KNOSSOSnet Research Group
Technological Educational Institute of Western Greece, Greece
nsklavos@ieee.org

Abstract

In recent years, it has been more than obvious that electronic hardware devices are more than pervasive parts, in most aspects of everyday life. Although, the increased need for communications and transactions, makes both security and privacy manners a crucial factor, that has to be considered with high attention. New methodologies and approaches are developed, in order the need for high security levels, to be satisfied successfully.

Physical Unclonable Functions (PUFs) have attracted the interest of the research community the last years. PUFs basically support cryptographic primitives, in order to implement security schemes, such as key generation and storage, authentication, as well as identification.

This work carries out operation aspects of PUFs, as well as use cases, which are currently investigated by the researchers. In this paper, design approaches of PUFs are introduced, with detailed aspects of their behaviour. The security properties of the presented designs are given in detail, in order to demonstrate the security properties, introduced by the physical properties, in the most sufficient way. Comparisons of the alternative philosophies of the different designs are given.

1 Introduction

Intrinsic random physical features have been used lately at a great manner, in a great number of applications, as a useful approach for different aims and scopes. Physical(-cally) Unclonable Functions (PUFs) have been developed the last years, and new types are proposed, from time to time, regarding both their operation and construction.

A PUF can be described as a disordered physical system. Such a system can be challenged by the external environment. The PUF operation includes responses to those challenges. The responses depend on the nanoscale structural disorder in the PUFs.

Especially, PUFs have attracted lately the interest of the research community, since they are proven a very promising and trustworthy solution, especially in the areas of cryptographic hardware, since they can be used successfully for a great number of security applications.

This work proposes alternative directions and applied approaches of securing communication devices, via Physical Unclonable Functions (PUFs).

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_22, © Springer Fachmedien Wiesbaden 2013

First, the alternative Physical Unclonable Functions (PUFs) categories are introduced by the construction point of view. The characteristics of each one of them are introduced.

The PUFs operations are presented, regarding alternative approaches of the design. The security application aspects are given in detail, regarding PUFs utilization and usage. Furthermore, the achieved security level of each one of PUFs categories is examined.

Last but not least, different aspects for the efficient implementation of PUFs are introduced. Conclusions are discussed and future directions are given.

2 PUFs from the Construction Point of View

In this section the alternative approaches for the construction of PUFs are given, as well as their certain properties.

Non Electronic PUFs: There is a number of PUFs designs which belong to this category, for which construction or/and operation is not related to electronic aspects. Although, the operation of this category is combined with other electronic parts or digital devices, mainly for the efficiency of storage. The non-electronic nature of these PUFs is related to the nature of random primitives generation. Other electronic parts are involved with the issues of processing and storage purposes.

PUFs based on Optical: Random optical procedures have been used as an alternative direction for the construction of unclonable functions. Such properties have also been used for the integration of functions with one way operation. Detailed test although, have to be performed in order the properties of the optical PUFs to be determined. It has to be mentioned that such a design approach may needs an initialization setup process regarding the laser, and possible other mechanical parts of the positioning system. Integrated designs with such or similar concepts could be found in technical literature.

PUFs and Compact Discs: Compact discs, as a laser technology product, can be used in order to support PUFs operation. In general, pits and lands of a common CD, are used as a random primitive, based on probabilistic options, which are occurred during the stage of manufacture.

PUFs Operation on Papers: Another completely different approach compared with the previous ones, is those PUFs, where their operation are based in the use of papers. They are based on scanning the random structure of a paper, which can be in a normal or in a modified version. Methodologies are introduced, in order to in order to make a connection of the document data with the paper version, based on digital signature techniques, or other methodologies like paper fingerprint.

Intrinsic PUFs: Although it is not efficient enough to define at a formal way the term of an intrinsic PUF, in order a function to belong to this category must meet at least the following specifications:

- The function has to be fully integrated in the hardware module, which may include any equipment which needed for the right operation of it.
- Any components should be fully available during the manufacturing process, of the hardware device.

PUFs and Memory Usage: This category includes PUFs which operation is based on memory elements. Alternative proposals have been published in the technical literature which contain different elements of memory storage like SRAM blocks, storage elements constructed of Flip-Flops , or data latches.

3 PUFs Operation

PUFs operation means different concepts, based on the alternative nature of the proposed designs. The concept of a Physically Obfuscated Key (POK) describes permanently the storage of a key in a physical way, instead of a digital one. Both of them have similarities, and it is efficient POKs to be constructed from PUFs. The combination of PUFs with other cryptographic primitives such as hash functions, results to controlled operation, with a number of advantages. The normal operation of a PUF can be extended to a number of additional operations which are well known are reconfiguration. As a result, the operation of the PUF is changed, concluding to a completely different design.

4 Security Applications Aspects and PUFs

The area of Physical Unclonable Functions (PUFs) has grown up at a great factor, during the last years, and it is expected for additional raise, for the forthcoming ones.

More analytically, Physical Unclonable Functions (PUFs) are widely used in a variety of aspects and especially for security applications and purposes. In this part of the paper, the alternative usages of PUFs regarding application aspects are presented in detail.

4.1 Cryptographic Engineering

One crucial aspect of security applications, where PUFs are used, has to do with the need of the key generation, for several applications of security. In this approach PUFs are used as external component of the Security System, which generates the key, which is extracted to the Security Core, as it is presented in the next Figure 1:

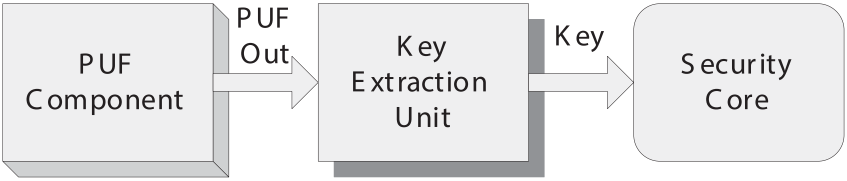


Fig. 1: PUFs Key Generation: Classical Method

Another approach for the key generation, is the integration of the PUF, inside the security primitive, with final result of this design, the hardware entangled security primitive, which is illustrated in the following Figure 2:

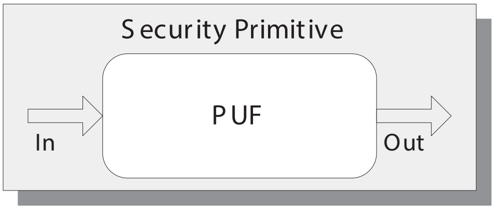


Fig. 2: PUF Integration in Security Primitive

Comparing the above presented approaches, someone can conclude to the fundamental differences between the alternative philosophies of both of them.

A cryptographic algorithm, and especially a block cipher, which operation is based on a PUF, can support cryptographic primitives based on the first approach, for which security issues may arise. The generated key is needed to be stored, as digital information, in general purpose components like memory devices, which can attract the interest of an attack attempt.

On the other hand hardware entangled security primitives are characterized as keyless approach, and fully support security, in the sense that it is not efficient for a possible attacker to gain access on information of the keys, since the data are not stored to any reachable component.

The above comparison makes clear that integrating the PUF as an internal part of the security primitive, meet the requirements of secure cryptographic systems, based on the unique properties of random physical features.

4.2 Authentication

For authentication purposes, PUFs can be alternatively used, as a module of the hardware component of each part of an established communication. Current methodologies are fundamentally based in password usages or other available approaches from software or hardware perspectives of view. Intrinsic PUFs although, can be applied alternatively.

An authentication handshake mechanism is based each time on a challenge and response scenario, which is applied for both client, as well as for server authentication as well. In most of the cases, the server takes the role of the verification part and applies a challenge-response pair, (CRP), to the system's database. This is related to a dedicated PUF component, which is being set up each time during the initialization process. The client responds to a random challenge, which has been caused by the server, which is the verifier party of the handshake protocol. The PUF is usually queried, and the response, which has been measured, is sent back to the verifier. The expected response is compared with the answered one, and in the case that these are the same, the authentication is achieved.

On the other side, server can be authenticated in a similar way of operation. In this case, there is the same initial condition and the PUF device possesses the client, while the server sends a CRP primitive, which has been chosen, in a random way. The client verifies it or not, by using it's PUF, expecting the response to be the same with the provided one.

The above described authentication protocols could be applied with additional security primitives. In such cases, a possible eavesdropper could take gain of the CRPs, which are sent during the communication, and personate a certain part of the communication. This is possible to be taken place, in the case that the challenge is used at least twice or more times, due to the fact that the attacker has the knowledge of the right response. In order to avoid such kind of attack, the CRP is proposed to be used only for one time. In different cases a new one CRP is used, for each case of authentication.

4.3 Identification of the Device

The purposes of authentication issues, analysed in detail in the previous section, make the device behaviour to the identification token. In this case, there is no need for security keys storage, which bypass the possibility an attacker to recover key data, which are stored in hardware components like RAMs. The PUFs devices, generates the cryptographic key on the fly, by making use of the intrinsic physical features of them.

Although typical components and devices could be used as PUFs, this arise security related issues, which could be under the investigation of external attackers of the system. These security issues, is a matter for further research and investigation, regarding the applied PUFs approaches.

4.4 Random Number Generation

Most of the security applications are based on random number generation, in order to ensure security in alternative means. These random generated data are basically used for the key generation or for other purposes such as salt vectors, and must not be predicted, under a possible attack. In most of the cases, pseudo random generators are used, since real random generators are not efficient to be applied.

The input of these pseudo random generators is coming from seeds with high entropy. Alternative approaches have been examined, which make use of general purpose devices, as input for high entropy data. Hardware components which are used for such purposes are GPUs, CPU Cache States, and SRAM Devices. PUFFIN project examines such approaches, for random number generation.

4.5 Safety Generation

For those applications that request keys generation, the last could be produced from any environment that includes a PUF primitive. The crucial factor in this case, has to do with those features of the environment, which could guarantee the secure generation of the keys. Following this approach, the key for the appropriate security application is generated, based on the certain hardware module. In this case, the hardware module is identified. Following that, the key maybe used in order to unlock encrypted data, which are stored on the device, or other applications that may be installed on it.

In order to achieve this, detailed schemes are applied, providing alternatives for devices identification. For example, the storage of a great number of keys and certifications, in dedicated hardware components and also in software parts could be applied. In this direction, such approaches usually need extra hardware modules, which increase the resources and the final cost of the hardware device. Although someone could suggest software solutions, which may be cheaper approaches, in order to reduce the cost. In general, software approaches, could not support strong trust directions, in order to ensure safety platforms.

Finally, today's solutions in most of the cases could attract side-channel attack attempts, or other methodologies, in order someone to gain access to the applied cryptographic data. The use of PUFs gives the benefit of embedding primitives to a hardware module, without storing cryptographic data to a separate module, or external hardware device.

4.6 Protecting IPs

It is obvious from the above section, that the physical properties of the underlying hardware are crucial aspects for the establishment of an identification scheme, which may be used for a device. As a result of this, additional applications and schemes can take place, in order to support other security or cryptographic schemes.

One very important aspect is to ensure security for IPs (Intellectual Property) protection, in software platforms. This can be achieved, by binding applications, based on hardware modules, in software platforms. With this method, illegal or not illegal software versions could be detected.

Furthermore, there are much cases, where software tools or applications have to be configured or controlled, by distance, or configurations options and primitives have to be delivered to other parties. As it has also been mentioned before, software instances, could be bind in hardware modules, and in this case software configuration information could be delivered safety, to the involved parties.

5 PUFs Security Level

Since there are several types and subtypes of PUFs available today, each one of them supports its own applications and security schemes. These different types could be divided to three main categories: a) Strong, b) Controlled and c) Weak, which have obvious differences in the sense of the security level.

5.1 Strong PUFs

With the term Strong PUFs, systems with physical environmental characteristics and with a great number of challenges and also with a complicated challenge and response behaviour are described.

Strong PUFs are widely used for a great number of applications such as key authentication processes, identification procedures and key establishment issues. This category can support cryptographic applications with high level of security, without complex arithmetic computational to be involved in the process. Electrical circuits can be used to construct Strong PUFs. Their main security features are described in the following paragraphs.

A Strong PUF is impossible to be cloned. This means in other words that it is not efficient to construct more than one system that achieves the same behaviour, for example in a challenge and response protocol. This feature, guarantees that each Strong PUF is unique from the begging of the manufacturing line process, and neither a designer nor a manufacturer could produce two PUFs with the same behaviour.

Another feature of Strong PUFs has to do with the challenge and response pairs (CRPs). It is not efficient for someone, even in the case he takes access to a PUF to measure all possible challenges and responses, in a given time period. Even in the case that someone takes full access to all challenges and responses of a PUF device, this is impossible for a long time period of days or weeks.

Finally, it is not efficient for someone to estimate a possible response for a given challenge, even in the case that some CPRs have been well known.

5.2 Controlled PUFs

Strong PUFs could be used as fundamental primitives in combination with control logic circuits. Additional logic could be used in order to control the challenges and the corresponding responses of the PUFs. In this way, challenges could be prevented from being sent to the PUF as well as responses could be read or not from other parts of the module. This strategy ensures defence from attacks or other possible deceptions.

It has to be clear that the possible outputs of a PUF, and especially a strong one, must not be read. In different case, it may be possible the behaviour of the PUF to be predicted, and the Control PUF logic to be broken.

5.3 Weak PUFs

The last category of the PUFs has to do with the weak behaviours of some of them. This means that there are cases where PUFs support a small number of challenges, and in the worst case just only one. For this reason, their response(s) has not to be given directly to the external environment.

Weak PUFs are basically used for cryptographic keys derivation, which is considered as a secret input of a security system. They can also be parts of key storage, in more efficient and secure way compared with other components, like types of ROM, which may be read. Different alternatives could be found today, in this category, like SRAM PUF, Coating and Butterfly PUF.

Strong PUFs can be used in order to construct Weak PUFs, with reducing the used number of challenges, of the available set.

Last but not least, other behaviours of the Weak PUFs have also to be considered such as error correction and stability also. A weak PUF produces and output response, which could be considered a secret key. This amount of information is been processed internal in the device. Error correction process has to been combined with high precision, since it is carried out internally on the chip. In order this to be achieved, it is possibly needed additional parts of data to be stored internally in the chip. The recipients of the produced responses, is possible to establish error correction procedures, which are allowed by Strong PUFs.

6 Implementation Aspects

Today, in technical literature there is a great number of alternative directions, regarding PUFs implementation. In order to prove their superiority and novel aspects of the proposed designs each time, a great number of advantages are figured out each time, in order the proposed design to be proven better to the compared one. Although such comparisons are based on the measurements provide for the proposed one. This concludes to a great number of measurements sets, which practically cannot be applied to all different categories of PUFs.

In order to have a fair and detailed comparison, for all different available designs, a number of parameters have to be applied, in order the security primitives as well as the practical usages of them to be examined and presented. In the following paragraphs, the most important parameters for such a comparison are considered.

- **Sample Size**: One of the basic characteristics is sample size which is considered as: the number of distinct devices, the number of challenges, as well as the number of the corresponding responses to them, as well as the measurements of each one response. Furthermore, statistical analysis has to be performed, regarding samples, in order to conclude to formal analysis each time of the examined PUF.
- **Histograms**: In most of the cases, inter- and intra- distance histograms are basically used for alternative designs comparisons, in order the uniqueness and the noise of a PUF to be determined. These histograms are mainly Gaussian, and their average is basically used. In addition, the standard deviation of each one of them is applied. For these reasons statistical approaches are considered to be used and due to the histograms' nature. Although, these are proven a good estimation for PUFs behaviour, in general, they are not sufficient enough in order to have a point of view for the factor of the entropy.
- **Entropy**: This parameter is presented as an estimation factor, in a number of PUFs responses. Alternative methods have been proposed in order to estimate and measure entropy. Although it has to be clear that these approaches are just an estimation for the factor of entropy, due to the available length of the responses, which not extend to great numbers.
- **Challenge and Response Pairs**: For the CPRs the number of the non-predictable ones is equal to a limited amount, close to a polynomial in the size of the PUF. Actually, each time and for a given size, the length, in term of bits, for the unpredictable response data is a key of great importance.
- **Implementation**: Implementation issues, regarding cost and efficiency are issues that are always related with the practical applications of the PUFs. It is obvious that such modules must have low cost. PUFs which are usually implemented in hardware modules, must also be examined in the implementation parameters by using hardware terms such as performance, speed, size, allocated resources and power consumption.
- **Influences**: PUFs usually response to non-wanted influences of the environment. It possible due to these influences to have failures in the PUFs operation, which are applied to a real application. Such influences should be examined and avoided in the term of possible, each time.
- **Tamper Evidence**: This factor is also considered as one of the important parameters of PUFs. Experimental measurements and validation are needed in order to conclude in a safe way, for a given PUF design, regarding tamper evidence. In this direction, experiments are proven of great importance, in order to result to the behaviour of the Challenge and Response Pairs, regarding PUF behaviour.

7 Conclusions & Outlook

This work proposes alternative directions of securing communication devices via Physical Unclonable Functions (PUFs). PUFs are coming on the market as part of the consumer devices. As a result of this growth, the areas the PUFs applications are introduced and presented in detail. Up today, in the field of PUFs, a great number of constructions have been set up. A comparative study of PUFs properties, for the different types of them, is essential in order to conclude to useful results, regarding the appropriate type, for each application and each time. From the implementation point of view, concrete characteristics have to be introduced and evaluated, in the applied design of PUFs. This will conclude to more advantages of the PUFs research areas. The first results of this state-of-the-art work in progress are more than promising, and the future directions are expected to achieve higher aims and scopes.

Acknowledgement

This work was partially supported by COST Action IC1204: Trustworthy Manufacturing and Utilization Of Secure Devices (TRUDEVICE).

References

[BePo09] Beckmann, N., Potkonjak, M.: Hardware-based public-key cryptography with public physically unclonable functions pp. 206-220, 2009.

[MaVe10] Maes Roel, Verbauwhede Ingrid, Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions, In Towards Hardware-Intrinsic Security, D. Naccache, and A. Sadeghi (eds.), Springer, 36 pages, 2010.

[Puff13] Puffin Project: Physically Unclonable Functions Found in Standard PC Components, "INFSO-ICT-284833", Web: http://puffin.eu.org/, 2013.

[ScLe13] Schaller Andre, Leet van der Vincent, Pkysically Unclonable Functions found in Standard Components of Commercial Devices, First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, Co-located with IEEE European Test Symposium, Avignon, France, May 30-31, 2013.

[SkEf07] Sklavos Nicolas, Efstathiou Costas, SecurID Authenticator: On the Hardware Implementation Efficiency, proceedings of 14th IEEE International Conference on Electronics, Circuits and Systems (IEEE ICECS'07), Morocco, 2007.

[Skla10] Sklavos Nicolas, On the Hardware Implementation Cost of Crypto-Processors Architectures, Information Systems Security, The official journal of (ISC)2, A Taylor & Francis Group Publication, Vol. 19, Issue: 2, pp. 53-60, 2010.

[SkZh07] Sklavos Nicolas, Zhang Xinmiao: Wireless Security and Cryptography: Specifications and Implementations, CRC-Press, A Taylor and Francis Group, ISBN: 084938771X, 2007.

[TGG10] TCG, Mobile Trusted Module Specification, Version 1.0, Revision 7.02, Trusted Computing Group, Tech. Rep., 2010.

Secure Mobile Government and Mobile Banking Systems Based on Android Clients

Milan Marković[1] · Goran Đorđević[2]

[1]Banca Intesa ad Beograd, Bulevar Milutina Milankovića 1c
11070 Novi Beograd, Serbia
milan.z.markovic@bancaintesa.rs

[2] Institute for Manufacturing banknotes and coins NBS, Pionirska 2
11000 Beograd, Serbia
djg_goran@mail.com

Abstract

In this paper, we consider an overview of a possible secure model for m-government and m-banking systems. The proposed model is based on secure mobile application and SOA-Based central platform. The model additionally consists of external entities/servers, such as: PKI, XKMS, Authentication and Time Stamping server. The proposed model could be used in different local and/or cross-border m-government scenarios, as well as in different kind of m-banking systems. As a possible example of described secure mobile application we considered and experimentally evaluated a possible usage of secure Android based Web services application in the proposed model.

1 Introduction

This work is related to the consideration of possible secure m-government and m-banking models and applying a secure Android Web services based application in them. An overview of possible secure m-government and m-banking systems realized according to the similar model based on secure JAVA mobile Web service application and the SOA-Based central platform is given in [MaDj12]. In this paper, a possibility of using the secure Android based mobile application in the proposed model is considered and experimentally evaluated.

First, we consider a possible model of secure SOA-based m-government online systems, i.e. about secure mobile communication between citizens and companies with the small and medium governmental organizations, such as municipalities. This model will be considered in both local and cross-border case. The latter means either crossing borders of municipalities in the same country or crossing borders between countries (e.g. some municipalities in different countries). The work presented related to the m-government systems and examples described have been partially included in the general framework of the EU IST FP6 SWEB project (Secure, interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries, SWEB) [MaDj10], [MaDj08], [MaDj11].

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_23, © Springer Fachmedien Wiesbaden 2013

As a second goal of this paper, we consider a possible usage of similar secure model in the m-banking systems.

As a third goal of this paper, we consider a possible usage of the Android-based secure mobile application in the proposed model of m-government and m-banking systems. A feasibility of using such Android based secure mobile application is experimentally evaluated in the paper.

The paper is organized as follows. The architecture of the proposed model is given in Section 2 while the proposed mobile application is described in the Section 3. A description and some experimental results obtained by the secure Android-based application is given in Section 4 while conclusions are given in Section 5.

2 Possible Secure M-Government and M-Banking Model Architecture

The proposed model for m-government and m-banking systems consists of:

- **Mobile users** (citizen, companies) who send some Web services requests to m-government or m-banking platform for a purpose of receiving some governmental documents (e.g. residence certificate, birth or marriage certificates, etc.) or doing some banking transactions. These users use secure mobile Web service application on their mobile devices (mobile phones, smart phones, tablets, etc.) for such a purpose.
- **SOA based Web service endpoint implementation** on the platform's side that implements a complete set of server based security features. Well processed requests with all security features positively verified, the Web service platform's application proceeds to other application parts of the proposed SOA-Based platform, including the governmental Legacy system for issuing actual governmental certificates requested or to the back office system in the Bank for processing the banking transactions. In fact, the proposed platform could change completely the application platform of some governmental or banking organization or could serve as the Web service „add-on" to the existing Legacy system implementation. In the latter case, the Legacy system (or back office in the Bank) will not be touched and only a corresponding Web service interface should be developped in order to interconnect the proposed SOA-Based platform and the Legacy governmental of Bank's back office system.
- **External entities**, such as: Authentication server (e.g. STS server), PKI server with XKMS server as a front end, and TSA (Time Stamping Authority) server.

Functions of the proposed external entities are following:

- **STS server as the Authentication server** – is responsible for strong user authentication and authorization based on PKI X.509v3 electronic certificate issued to users and other entities in the proposed model. The communication between STS server and the user's mobile Web service application is SOAP-based and secured by using WS-Security features. After the succesful user authentication and authorization, the STS server issues a SAML token to the user which will be subsequently used for the user authentication and authorization to the Web service of the proposed m-government platform. The SAML token is signed by the STS server and could consist of the user role for platform's user authentication and authorization. The alternative is that it could be a general-purpose Au-

thentication server which will authenticate users by using any kind of authentication credentials, such as: user credentials (username/password), OTP, PKI digital certificates, etc.
- **PKI server** – is responsible for issuing PKI X.509v3 electronic certificates for all users/entities in the proposed m-governmental and m-banking model (users, civil servants, administrators, servers, platforms, etc.). Since some certificate processing functions could be too heavy for mobile users, the PKI services are exposed by the XKMS server which could register users, as well as locate or validate certificates on behalf of the mobile user. This is of particular interests in all processes that request signature verification on mobile user side.
- **TSA server** – is responsible for issuing time stamps for user's requests as well as for platform's responses (signed m-documents).

3 Secure Mobile Web Service Client Application

The proposed secure mobile Web service client application comprises of following functionalities:

- **Graphical User Interface (GUI)** for presenting business functionalities to the end user. The GUI object of the proposed mobile Web service application is responsible to show user interface that enable calling of function for authentication of the end user and presenting the core functionalities to the end user. According to this, the GUI object communicates with following modules:
  - User Authentication module for mobile client application of the Security object
  - User PKI Registration module (XKMS module) of the Security object
  - User Authentication and Authorization module for the m-government platform (SAML module) of the Security object
  - Business module of the Business object.
- **Business (core) functionalities** of the application – m-government and m-banking functionalities. Business functionalities have links to Security and Communication objects of the secure mobile Web service application.
- **Security functionalities.** The Security object of the considered secure mobile Web service application is responsible for overall application-level security functionalities.
- **Communication.** The communication module is responsible for establishment of secure communication between citizens and governmental or banking organizations. Similar communications are done between the secure mobile client Web service application and the m-banking platform implemented according to the same proposed model.

The security functionality of the proposed Secure Mobile Client application consists of the following modules:

- **Authentication module** to the secure mobile application. End user could have the proposed secure application installed on his mobile phone/terminal following one of two possible ways:
  - Installing the secure mobile application by using the desktop computer and via wired (corresponding cable) or wireless (e.g. Bluetooth, Infrared, WiFi) transmission path to the mobile terminal – **offline approach**.
  - Installing the secure mobile application through some OTA (Over-The-Air) services – **online approach**.

User authentication for using the secure mobile application should be two-step process:

- The first step would be a combination of username/password for accessing the application (password should be changeable by the user). This should be done immediately after the application starts. These credentials will be generated during the user registration process. During the initial phase of the registration application, the user will obtain the username and default password. The application has to force the user to change the password on the first application start.
- The second step will be in presenting a corresponding PIN code for accessing the asymmetric private key just before digital signing the m-residence certificate request or other requests in the scenarios.

The generation of user asymmetric public/private key pair and corresponding digital certificate should be done through user registration function of the XKMS protocol. The User Authentication module is called from the GUI object.

- **XKMS module.** XML Key Management Specification enables to simplify the use of PKI by mobile client systems.
- **STS module.** The STS module is responsible for the communication with the STS server in order to receive a SAML assertion (token) that will be used afterwards to enable access to the business functionalities by the client. The user first sends a RequestSecurityToken message to the STS (Security Token Service) server by using a SAML protocol. A protection is done by using WS Security mechanisms. After successful authentication of the user based on the client's X.509v3 digital certificate, the STS server issues a SAML token to the user which is digitally signed by the STS server. This token is securely communicated to the end user by using the WS security mechanisms.
- **XML security module.** XML security module is responsible for implementation of standard XML signature and XML encryption components. XML security module consists of:
    - Implementation of the RSA private key operation for creating digital signature, as well as a function for signature verification.
    - Implementation of hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512).
    - Implementation of different symmetrical cryptographic algorithms (3DES, AES).
    - Implementation of the RSA private key operation for decryption of encrypted session symmetric key in digital envelope.
    - Implementation of the RSA public key operation for encryption of session symmetric key in digital envelope.
- **WS-Security module.** Web Service (WS) Security module is implemented as standard security mechanisms for protection of SOAP messages. WS-Security module is very important module of the Security object since it is used for protection:
    - Communication with STS server.
    - Communication with the proposed SOA-Based platform.

This way, the WS-Security module communicates with SAML module of the Security object as well as with Business functionalities object. The SAML module communicates with WS security module of the Security object as well as with the Communication object.

- **Time-Stamping module.** This module is responsible for communication with the TSA. A time-stamping service supports assertions of proof that a datum existed before a particular time. As the first message of this mechanism, the user's application requests a timestamp token by sending a request to the TSA. As the second message, the TSA responds by sending a response, i.e. actual timestamp, to the requesting entity.

The secure mobile Web service application communicates with all mentioned external entities in Section 2, i.e. it has all security functions mentioned implemented:

- Secure mobile Web service application sends Request for Security Tokens to the STS server by using WS-Secured (WS-Signature and WS-Encryption) SOAP communication.
- Secure mobile Web service applications sends digitally signed (XML signature) request for mobile governmental document to the Web service of the proposed governmental platform by using WS-Encrypted SOAP communication. The sent request includes of the SAML token issued and signed by the STS server.
- The request is timestamped by sending a timestamp request and obtaining the corresponding timestamp response (digitally signed by the TSA).
- The secure mobile Web service application also receives the signed and timestamped m-governmental document from the platform through WS-Encrypted communication and performs all necessary signature verifications and certificate validations (by help of the XKMS server) actions.

4 Experimental Analysis

This Section is dedicated to the experimental analysis of the cryptographic operations implemented on Android mobile phone as a possible example of the proposed secure mobile client application. We analysed implementation of different PKI functions that could be main elements of the considered secure Android based web service application on three different test platforms: smart mobile phone, tablet and PC. Namely, we compared experimental results obtained on some mobile devices (smart phone, tablet) with the same experiments obtained on the PC computer in order to test feasibility of the analysed PKI functions implementation on mobile devices.

The presented experimental results are generated using following devices:

1. LG E610 mobile phone that has following characteristics (Mobile Phone):
   - CPU Core: ARM Cortex-A5
   - CPU-Clock: 800 MHz
   - RAM-capacity: 512 MB
   - Embedded_Operating_System: Android 4.0.3 Ice Cream Sandwich
   - NFC Functions.
2. Tablet Ainol Novo 7 Paladin device that has following characteristics (hereafter Tablet):
   - XBurst CPU
   - CPU-Clock: 1 GHz
   - RAM-capacity: 1 GB
   - Embedded_Operating_System: Android 4.0.1
3. PC Desktop Computer that has following characteristics (PC Desktop):
   - Intel Pentium CPU G620
   - CPU-Clock: 2.60 GHz
   - RAM-capacity: 2 GB
   - Operating_System: Windows XP with Service Pack 3
4. PC Laptop computer that has following characteristics (PC Laptop):
   - Intel Celeron CPU P4600
   - CPU-Clock: 2 GHz
   - RAM-capacity: 3 GB
   - Operating_System: Windows 8

The Android platform ships with a cut-down version of Bouncy Castle – as well as being crippled. It also makes installing an updated version of the libraries difficult due to class loader conflicts. The different versions of Android operating system have implemented different versions of Bouncy Castle library releases. In order to avoid lack of interoperability between different devices that have implemented different operating systems and get more flexible code we used Spongy Castle functions (http://rtyley.github.com/spongycastle/). In order to achieve smaller and faster implementation we partly modified Spongy Castle functions. Experimental results that are presented in this Section are based on the modified version of Spongy Castle functions.

We first considered possibility to create asymmetric RSA private/public keypair in a real-time using the standard mobile phone device. During generation of private components of RSA keypair it is used Miller-Rabin big number primality test. It is a probabilistic algorithm for determining whether a number is prime or composite. The number of iteration of Miller-Rabin primality test that we used during private keypair component generation is 25. The error probability of Miller-Rabin's test for T =25 times is 8.88*10^{-14}%. Times (in miliseconds – ms) needed for generation RSA private components and calculation of Chinese Remainder Theorem's parameters are shown in Table 1. Throughout this Section, all presented experimental results are given in miliseconds – ms.

Table 1: RSA private/public key pair generation

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	286.23	1 282.46	7 437.70	23 167.97	62 274.3
Tablet	159.97	822.29	5 727.04	21 612.54	57 545.29
PC Laptop	53.39	367.23	3 552.45	15 964.68	47 630.71
PC Desktop	40.18	273.29	2 647.51	12 038.61	35 593.62

After generation of RSA private/public key pair we stored the private component of the key in PKCS#5 based key store using a mechanism of the Password Based Encryption Scheme 2 (PBE S2). An algorithm used for protection of RSA private component in the created key store is AES. The number of iteration count was 1000. Times needed for creation of key store, encrypting private key component using AES algorithm with two different key lengths (128 and 256 bits) where number of iterations was 1000, are shown in Table 2.

Table 2: RSA private key protecting in AES based keystore

Device	AES key length (bits)	
	128	256
Mobile Phone	167.46	332.94
Tablet	1 116.39	2 217.99
PC Laptop	7.84	15.60
PC Desktop	5.02	10.01

We also measured the time needed for creation X509 v3 self-signed certificate comprising a creation of PKCS#10 certificate request (Table 3). As a signature algorithm we used SHA-1 hash algorithm and RSA asymmetric cryptographic algorithm.

Table 3: Create X509 v3 self-signed certificate

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	18.11	27.41	84.41	216.89	467.95
Tablet	34.49	46.27	116.05	283.22	548.40
PC Laptop	1.78	9.01	58.07	180.97	414.14
PC Desktop	1.33	6.78	43.92	137.36	312.90

In order to evaluate the possibility of using the mobile phone for mobile client application in m-Government/m-Banking systems based on Web service we measured times needed for creation of XML-Signature and Web Service (WS) Signature (Table 4, Table 5), respectively. In all these experiments, we used a file of 1KB and SHA-1 hash function.

Table 4: XML-Signature creation

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	29.64	38.15	95.87	228.20	479.10
Tablet	59.73	73.78	144.08	319.65	586.54
PC Laptop	2.12	9.38	58.50	181.54	414.74
PC Desktop	1.57	7.05	43.85	137.87	312.79

Table 5: WS-Signature creation

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	63.76	74.51	131.00	266.29	507.47
Tablet	126.99	147.68	216.81	384.48	663.93
PC Laptop	2.79	10.07	59.18	182.1	415.19
PC Desktop	2.02	7.50	44.57	138.03	311.66

The time needed for verification of WS-Signed message is shown in Table 6.

Table 6: WS-Signature verification

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	34.67	34.81	34.87	34.94	50.20
Tablet	94.83	95.61	101.27	107.58	111.22
PC Laptop	0.88	1.16	2.42	4.58	7.29
PC Desktop	0.61	0.84	1.74	3.29	5.31

We also analyzed possibility of encryption XML based message using WS Encryption as well as WS Decryption mechanisms (Table 7, 8), respectively. In all these experiments, we used a file of

1KB and SHA-1 hash function, as well as 3DES symmetric cryptographic algorithm with symmetric key length of 168 bits.

Table 7: WS-Encryption mechanism

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	38.03	38.39	38.54	45.36	48.94
Tablet	80.86	85.13	89.96	100.32	109.08
PC Laptop	0.98	1.29	1.78	4.59	6.99
PC Desktop	0.67	0.90	2.63	3.19	5.36

Table 8: WS-Decryption mechanism

Device	RSA private key length (bits)				
	512	1024	2048	3072	4096
Mobile Phone	34.96	44.20	102.48	232.75	486.20
Tablet	80.91	119.74	169.87	339.54	609.42
PC Laptop	2.41	9.67	58.88	181.79	415.98
PC Desktop	1.77	7.28	44.36	138.01	313.88

We also considered possibilities of communication with Timestamp Server in order to obtain the timestamp token (Table 9). During the tests we measured the time needed for the following process:

- Extraction of Signature Element from XML-Signed (or WS-Signed) message;
- Calculating SHA-1 hash value of the content of extracted Signature element;
- Creation of appropriate TimeStamp Request message according to RFC-3161;
- Sending TimeStamp Request message to TimeStamp Server;
- Receiving, processing and extraction of generated TimeStamp Token created by Timestamp Server.

During the experiments, we have used the following publicly published Time Stamp servers:

1. http://tsa.starfieldtech.com
2. http://services.globaltrustfinder.com/adss/tsa
3. http://tsp.iaik.at/tsp/TspRequest
4. https://timestamp.geotrust.com

Table 9: Communication with Time Stamp Server

Device	URL address of TimeStamp Server			
	1	2	3	4
Mobile Phone	508.07	230.98	179.30	906.80
Tablet	487.84	226.49	174.52	876.94
PC Desktop	481.61	196.84	148.22	665.34

In the above experimental analysis we presented experimentally obtained results/times required for implementation of different kind of cryptographic operations that could be main elements of the considered Secure Android Web services application. We compared results obtained on mobile phone with the results obtained from tablet, laptop and PC desktop computer. Some of the observations are:

- The operation of digital signature of XML message (XML-Signature mechanism), using 2048-bit private RSA key, takes 95.87 ms on mobile phone. It means that in one second 10 operations of generation XML-Signature can be implemented by using 2048-bit private key pair component. This fact could lead to the conclusion that mobile phone could be used in real time for implementation of digital signature operations.
- The operation of encryption of RSA private keypair component that have been stored in PKCS#5 based key store (PBE S2 scheme) by using AES algorithm with 1000 iterations takes 167.46 ms on mobile phone. Bearing in mind the above mentioned, we can conclude that protected PKCS#5 based key store, that contains RSA private keypair component could be implemented in Android based mobile phone in a real time.
- The operation of encryption of XML message (WS-Encryption mechanism), using 2048-bit public RSA key, extracted from X509 certificate, takes 38.54 ms on mobile phone. The operation of decryption of WS-Encrypted message using 2048-bit private RSA key, takes 102.48 ms. It means that in one second can be implemented about 10 operations of decryption WS-Encrypted message using 2048-bit RSA private key. Regarding to the above mentioned, we can also conclude that mobile phone could be used in a real time in process encryption/decryption WS messages that are used in secure Web Service communications.
- Operations of creation of appropriate request message, communication with TimeStamp Server and processing its response message takes on mobile phone from 179.30 ms (using HTTP protocol) to 906.80 ms (using SSL over HTTP protocol). Based on the obtained results we could conclude that mobile phone could be used in real time in process of communication with TimeStamp Server in order to get TimeStamps and that the obtained results are pretty similar to results obtained by using tablet or computers.

5 Conclusions

In this paper, we presented an overview of possible secure model of m-government and m-banking systems as well as an analysis of possibility and feasibility of using secure Android-based web service mobile application in it.

First, this work is related to the consideration of some possible SOA-based m-government online systems, i.e. about secure mobile communication between citizens and companies with the small and medium governmental organizations, such as municipalities. Second, the paper refers to the application of the same or similar proposed secure model in m-banking systems. Third, the paper presented a possible example of an Android-based secure mobile client application that could be used in the described m-government and m-banking model.

Presented experimental results justify that security operations related to asymmetric key pair generation, primality tests on the random numbers, X.509v3 digital certificate generation, XML/WS digital signature/verification, XML/WS encryption/decryption and communication with TimeStamping servers are feasible for usage on some current Android based smart phones. Thus, we could conclude that the proposed application could serve as a basis for implementing secure m-government/m-banking systems based on the model described in this paper.

Main contributions of the paper are:

- A proposal of the possible secure model for m-government and m-banking systems based on secure Android based mobile Web service application and SOA-Based platform.
- Usage of secure mobile Web service application in which all modern security techniques are implemented (XML security, WS-Security, Authentication/SAML, Time Stamping, PKI, XKMS).
- Usage of SOA-Based request-response m-government and m-banking platform (Web Services) which is more suitable for usage of secure mobile application compared to the session-based Web application platform [LeLS07].
- Usage of XKMS service which is more suitable for mobile PKI system since it outsources complex operations such as PKI certificate validation services to the external entity, the XKMS server, compared to other techniques [LeLS07].
- Usage of the Android-based mobile client application for which a feasiility of implementing security operations is experimentally presented and verified.

Future researching directions in domain of m-government systems are:

- Full implementation of secure mobile Web service applications for all other mobile platforms (JAVA, iPhone, BlackBerry, Windows Mobile)
- Full implementation of advanced electronic signature formats (e.g. XAdeS, PAdeS)
- Integration of PKI SIM technology in the secure mobile client Web service application
- Application based (Android, JAVA, iPhone, Windows Mobile) digital signature by using the asymmetric private key on the PKI smart cards and usage of the integrated NFC (Near Field Communication) security element as a smart card reader.
- Using the proposed secure model for other PKI based e/m-governmental services (strong user authentication to other e-government web portals, signing documents prepared through some other communication channels, qualified signatures, etc.)

Future researching directions in domain of m-banking systems are:

- PKI SIM cards with asymmetric private key and signature JAVA applet on it
- Application based (Android, JAVA, iPhone, Windows Mobile) digital signature by using the asymmetric private key on the PKI SIM cards
- One single channel for mobile banking – mobile phone with the equivalent security mechanisms as in the case of Internet Banking – Application based Mobile Banking functionalities with PKI SIM card
- Application based (Android, JAVA, iPhone, Windows Mobile) digital signature by using the asymmetric private key on the PKI smart cards and usage of the integrated NFC (Near Field Communication) security element as a smart card reader.

References

[MaDj12] Marković, M., Đorđević, G.: On Secure m-government and m-banking model. In Proc of 6th International Conference on Methodologies, Technologies and Tools Enabling e-Government. Belgrade, Serbia, July 3 – 5, 2012. pp. 100-111.

[MaDj10] Marković, M., Đorđević, G.: On Possible Model of Secure e/m-Government System. Information Systems Management. Taylor & Francis Group, LLC. 2010. 27:320-333,.

[MaDj08] Marković, M., Đorđević, G.: On Secure SOA-Based e/m-Government Online Services. In Handbook "Service Delivery Platforms: Developing and Deploying Converged Multimedia Services". Taylor & Francis, 2011, p. 251 – 278, Chapter 11.

[MaDj11] Marković, M., Đorđević, G.: On Possible Secure Cross-Border M-Government Model. In: Proceedings of the 5th International Conference on Methodologies, Technologies and Tools Enabling e-Government, Camerino, Italy, June 30th – July 1st. 2011. pp. 381 – 394.

[LeLS07] Lee, Y., Lee, J., Song, J.: Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. Computer Communication. 2007. 30 (4): 893-903.

Index

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2, © Springer Fachmedien Wiesbaden 2013