Applying Soft Computing Technologies for Implementing Privacy-Aware Systems

Christos Kalloniatis[1], Petros Belsis[2], Evangelia Kavakli[1], and Stefanos Gritzalis[3]

[1] Department of Cultural Technology and Communication, University of the Aegean, Harilaou Trikoupi & Faonos Str., 81100 Mytilene, Greece
chkallon@aegean.gr, kavakli@ct.aegean.gr
[2] Technological Education Institute of Athens, Department of Marketing, Agiou Spyridonos Street, 12210 Aigaleo, Athens, Greece
pbelsis@aegean.gr
[3] Information and Communication Systems Security Laboratory
Department of Information and Communications Systems Engineering
University of the Aegean, 83200, Samos, Greece
sgritz@aegean.gr

Abstract. Designing privacy-aware systems gains much attention in recent years. One of the main issues for the protection of users' privacy is the proper selection and realization of the respective Privacy Enhancing Technologies for the realization of the privacy requirements identified in the design phase. The selection of PETs must be conducted in a way that best fits the organization's needs as well as other organization's criteria like cost, complexity etc. In this paper the PriS method, which is used for incorporating security and privacy requirements early in the system development process, is extended by combining knowledge from a soft computing approach in order to improve the way that respective PETs are selected for the realization of the respective requirements incorporated during the design phase.

1 Introduction

A major challenge in the field of software engineering is to make users trust the software that they use in their everyday activities for professional or recreational reasons. Trusting software depends on various elements, one of which is the protection of user privacy. Protecting privacy is about complying with user's desires when it comes to handling personal information. Users' privacy can also be defined as the right to determine when, how and to what extend information about them is communicated to others.

Nowadays, protecting privacy is focused on reducing the information collected and stored to a minimum, and deleting the information as soon as it has served its purpose. Most of today's e-services are relying on stored data, identifying the customer, his preferences and previous record of transactions. However, combining such data will in many cases constitute an invasion of privacy.

Research efforts aiming to the protection of user privacy fall in two main categories: security-oriented requirement engineering methodologies and privacy

M. Bajec and J. Eder (Eds.): CAiSE 2012 Workshops, LNBIP 112, pp. 31–45, 2012.

enhancing technologies. The former focus on methods and techniques for considering security issues (including privacy) during the early stages of system development and the latter describe technological solutions for assuring user privacy during system implementation. The main limitation of security requirement engineering methodologies is that they do not link the identified requirements with implementation solutions. Understanding the relationship between user needs and the capabilities of the supporting software systems is of critical importance. Privacy enhancing technologies, on the other hand, focus on the software implementation alone, irrespective of the organizational context in which the system will be incorporated. This lack of knowledge makes it difficult to determine which software solution best fits the organizational needs. A review on a number of well-known security and privacy requirements engineering methods can be found in [1]. Due to limited space the comparison results are excluded from this paper but can be found in our previous work conducted in [1].

To this end, PriS, a new security requirements engineering method, has been introduced aiming to incorporate privacy requirements early in the system development process. PriS models privacy requirements in terms of business goals and uses the concept of privacy process patterns for describing the impact of privacy goals onto the business processes and the associated software systems supporting these processes.

The conceptual model of PriS uses a goal hierarchy structure. Every privacy requirement is either applied or not on every goal. The representation of a privacy requirement that constraints a goal is achieved by the use of a variable which can take two values, zero and one. If one of the privacy requirements is applied on a specific goal the respective privacy variable will be assigned with the value of one otherwise will remain zero which was also its initial value. Thus, on every privacy-related goal seven privacy variables are applied and representing which privacy requirements constraint the goal and which not (Since pseudonymity can be considered as part of anonymity, they are both addressed in one pattern). Following this way of working PriS ends up suggesting a number of implementation techniques based on the privacy requirements constraining the respective goals. While PriS successfully guides the developers through the implementation phase by suggesting a number of implementation techniques it fails to address the degree of participation of every privacy requirement for achieving the generic goal of privacy.

This paper applies the extended PriS (along with the soft computing approach) on an e-voting case study. Specifically, in section 2 the case study is presented. Section 3 presents a brief description of PriS along with its way of working. Section 4 presents the application of fuzzy PriS on the specific case study. Finally, section 5 concludes with pointers to future work.

2 PriS Conceptual Framework and Way of Working

As mentioned earlier, privacy enhancing technologies focus on the software implementation alone. In other words, there is no obvious link between the

organizational processes that are constrained by the privacy requirements and the supporting software systems. This lack of knowledge makes it difficult not only to determine which software solution best fits the organizational needs but also to evaluate alternatives.

To this end, PriS provides a set of concepts for modeling privacy requirements in the organization domain and a systematic way-of-working for translating these requirements into system models. The conceptual model used in PriS, shown in figure 1, is based on the Enterprise Knowledge Development (EKD) framework [2,3], which is a systematic approach to developing and documenting organizational knowledge. This is achieved through the modeling of: (a) organizational goals, that express the intentional objectives that control and govern its operation, (b) the 'physical' processes, that collaboratively operationalise organizational goals and (c)

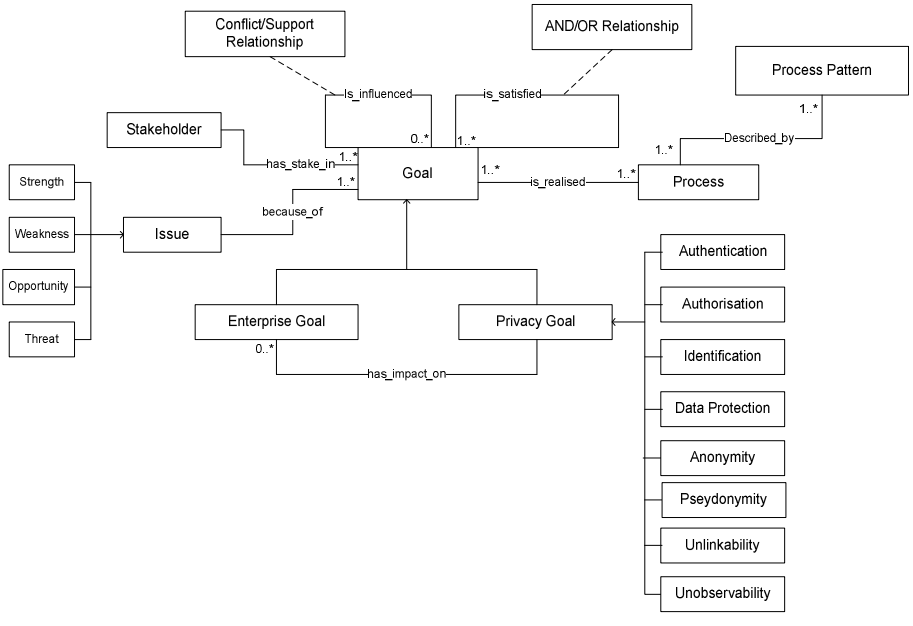

Fig. 1. PriS Conceptual Framework

the software systems that support the above processes. In this way, a connection between system purpose and system structure is established.

PriS models privacy requirements as a special type of goal (privacy goals) which constraint the causal transformation of organizational goals into processes. From a methodological perspective reasoning about privacy goals comprises of the following activities: (a) Elicit privacy-related goals, (b) Analyze the impact of privacy goals on business processes (c) Model affected processes using privacy process patterns and (d) Identify the technique(s) that best support/implement the above processes.

The first step concerns the elicitation of the privacy goals that are relevant to the specific organization. This task usually involves a number of stakeholders and

decision makers who aim to identify the basic privacy concerns and interpret the general privacy requirements with respect to the specific application context into consideration. In addition, existing privacy requirements already forming part of the organization's goals are identified. The second step consists of two stages. In the first stage the impact of privacy goals on the organizational goals is identified and analyzed. In the second stage, the impact of the privacy goals on the relevant processes that realize these goals is examined and the processes that realize the privacy-related goals are identified and characterized as privacy-related processes. Having identified the privacy-related processes the next step is to model them, based on the relevant privacy process patterns. Business process patterns are usually generalized process models, which include activities and flows connecting them, presenting how a business should be run in a specific domain [4]. The last step is to define the system architecture that best supports the privacy-related process identified in the previous step. Once again, process pattern are used to identify the proper implementation technique(s) that best support/implement corresponding processes.

PriS assists in the application of privacy requirements in the organizational context as well as in providing a systematic way of locating a number of system architectures that can realize these requirements. PriS way of working assumes that privacy goals are generic-strategic organizational goals thus being mentioned high in the goal model hierarchy.

A formal expression of PriS can be found in [5]. A software tool for supporting PriS way of working has also been constructed and a detailed description can be found in [6].

3 The e-Voting case

PriS method is demonstrated through an e-voting case study, regarding the transformation of an Internet based electronic voting system in order to accommodate the new legal framework regarding privacy protection. The specific case study has been used for evaluation of previous versions of PriS as well. However, we consider the same case study in this paper as well in order to be able to test and validate the progress and effectiveness of our method by applying the proposed soft computing approach in comparison to our previously suggested versions of PriS.

The initial design of the electronic voting system was developed in the context of the European Project "E-Vote" by the University of Regensburg, in cooperation with the University of the Aegean, the Cryptomatic company, the Quality and Reliability company and the Athens University of Economics and Business and is described in [7]. According to this description, the main objective of the e-voting system is to provide eligible citizens the right to cast a vote over the Internet rather than visiting an election district, aiming to simplify the election processes thus increasing the degree of citizens' participation during elections. It is described by four main principles that form the four primary organizational goals namely: a) Generality, b) Equality, c) Freedom and d) Directness. Generality implies that all citizens above a certain age should have the right to participate in the election process. Equality signifies that both

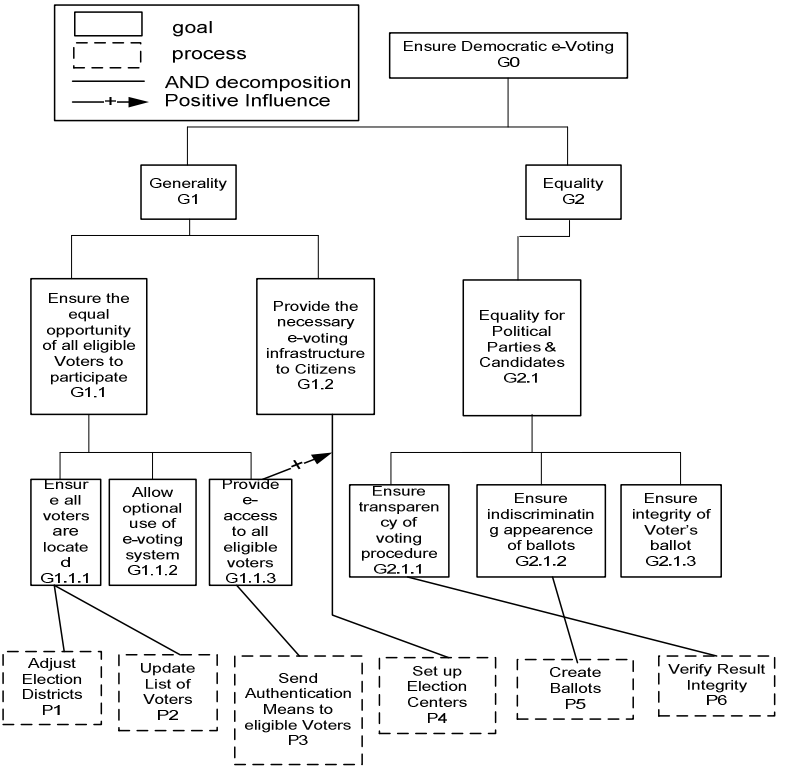

Fig. 2. Partial View of the e-Voting System Goal-Model

political parties - that participate in the election process - and voters have equal rights before; during and after the election process and neither the system nor any other third party is able to alternate this issue. Freedom implies that the entire election process is conducted without any violence, coercion, pressure, manipulative interference or other influences, exercised either by the state or by one or more individuals. Finally, directness means that no intermediaries chime in the voting procedure and that each and every ballot is directly recorded and counted.

A partial view of the system's current goal model is presented in Figure 2. In the last line the doted boxes are the relevant processes that satisfy organizational goals.

As mentioned earlier, the system has to be re-designed in order to guarantee that user's privacy is not violated. To this end, PriS was applied by two teams of postgraduate students of the University of the Aegean that worked in parallel in order to:

(a) to analyze the impact of privacy issues on the system's goals and processes and propose alternative system implementations (first team)

(b) formally describe the above process and its deliverables (second team)

(c) provide feedback regarding both difficulties encountered and recommendations or incorporation into the PriS method (both teams)

The students were computer science graduates and had knowledge of requirements engineering principles but no experience with the particular method. Work from this case study is reported in [4, 8]. The findings of this case study were cross checked with the ones of a second case study regarding the University of the Aegean Career Office System [9] which was conducted by two similar groups during the same period.

In the following section the application of the extended version of PriS (including the proposed fuzzy extension) is presented.

4 Applying Fuzzy PriS

In this section the PriS method is applied according to the four basic steps mentioned before. Through this case study the application of the new extension of PriS is also presented. Our main goal is to prove that the knowledge combination from a soft computing approach improves the way that PriS selects the respective PETs for the realization of the privacy requirements incorporated during the design phase, thus overcoming the drawback between design and implementation phases in a more robust and constructive way.

4.1 Elicitation of Privacy Related Goals

The first step concerns the elicitation of the privacy goals that are relevant to the specific organization. This task usually involves a number of stakeholders and decision makers (managers, policy makers, system developers, system users, etc). Identifying privacy concerns is guided by the eight privacy goal types shown in Figure 2. The aim is to interpret the general privacy requirements with respect to the specific application context into consideration. In the e-voting case two privacy goals were identified, namely: unlinkability and unobservability. The former refers to the voters' right to receive the respective authentication means (username and password) without others being able to reveal to whom the data are sent. Thus, even when a malicious third party is able to steal these data he/she won't be able to know neither the user nor the system where these data can be used. The latter concerns the voters' right to ensure the transparency of the e-voting procedure by verifying the results' integrity without other parties (either system users or malicious third parties which do not belong to the system) being able to observe the whole verification process.

It should be noted, that PriS assumes the existence of the organization's current goal model. If not, a goal modeling method should be used for constructing the goal model prior to PriS's application [10].

4.2 Analyze the Impact of Privacy Goals on Organizational Processes

The second step is to analyze the impact of privacy goals on processes and related support systems.

To answer this question, the first task is to identify the impact it may have on other organizational goals. This impact may lead to the introduction of new goals or to the improvement / adaptation of existing goals. Introduction of new goals may lead to the introduction of new processes while improvement / adaptation of goals may lead to

the adaptation of associated processes accordingly. Repeating this process for every privacy goal and its associated organizational goals leads to the identification of alternative ways for resolving privacy requirements. The result of this process modeled in the spirit of an extended AND/OR goal hierarchy [8].

Let us consider the privacy goal of unlinkability in the e-voting case. Guaranteeing voters' unlinkability will clearly impact the way that goal '$G_{1.1}$: *Ensure the participation of all eligible voters'* is realized. In particular, by applying unlinkability goal on $G_{1.1}$, this will have an impact on all subgoals that realize goal $G_{1.1}$. For every subgoal it is analyzed which are the modifications that need to be done in order to satisfy the unlinkability goal. In the specific example, subgoals '$G_{1.1.1}$: *Ensure all Voters are located'* and '$G_{1.1.2}$: *Update List of Voters'* are maintained while goal '$G_{1.1.3}$: *Provide e-access to all eligible Voters'* needs to be adapted. Specifically, two new subgoals are introduced namely '$G_{1.1.3.1}$: *Provide e-access*' and '$G_{1.1.3.2}$: *Prevent others to reveal to whom the data are sent*' as the result of the impact analysis. Finally, the process that realizes these new subgoals is also adapted for accomplishing the realization of the new privacy goal [8]. The result of this analysis is graphically illustrated in Figure 3.

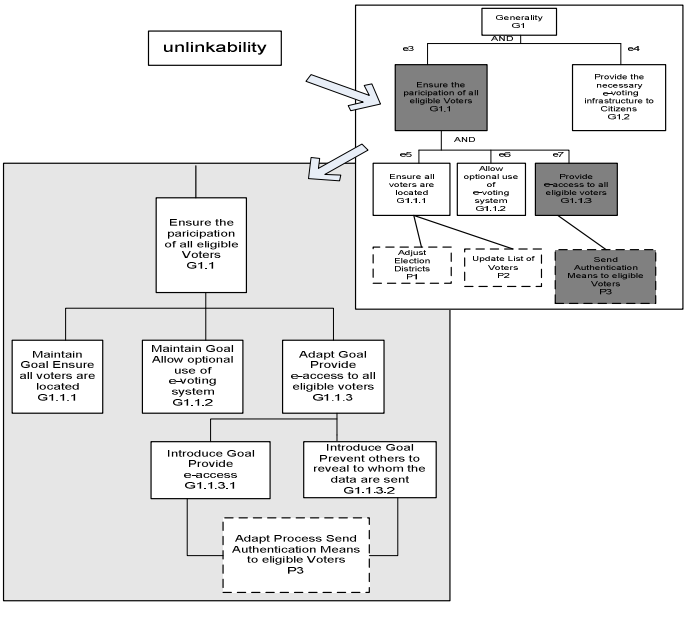

Fig. 3. Analyze the impact of unlinkability goal

4.3 Model Affected Processes Using Privacy Process Patterns

Having identified the privacy-related processes the next step is to model them, based on the relevant privacy process patterns. A detailed description of the seven privacy process patterns can be found in [8,11].

Figure 4 presents the process pattern for addressing the unlinkability requirement, which describes the relevant activities needed to realize that process. The application

of the unlinkability pattern on process 'P3: *Send Authentication Means to eligible voters*', which realizes goals $G_{1.1.3.1}$ and $G_{1.1.3.2}$ as shown in Figure 4, is presented next to the general pattern.

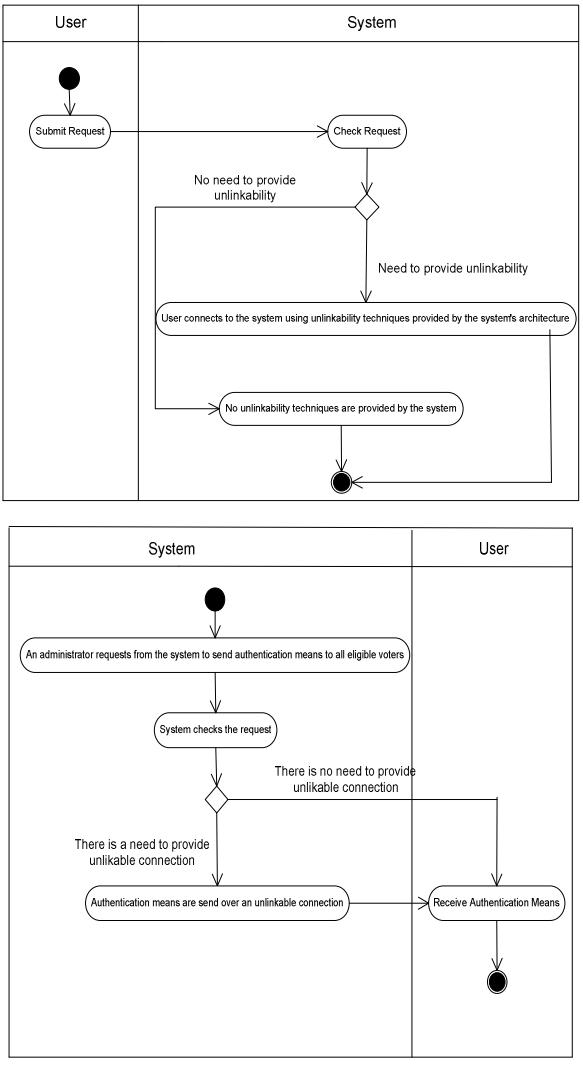

Fig. 4. Unlinkability Pattern & its Specialization on the e-voting case

4.4 Identify the Technique(s) that Best Support/Implement the Above Processes

For assisting the process of selecting the proper PETs for the realization of the respective privacy processes a table that matches the process patterns with a number of PETs is constructed and presented in a Table 1.

Table 1. Matching privacy patterns with implementation techniques

	Administrative Tools					Information Tools			Anonymizer Products, Services and Architectures											Pseudonymizer Tools		Track and Evidence Erasers				Encryption Tools		
	Identity Management	Biometrics	Smart Cards	Permission Management	Monitoring and Audit tools	Privacy Policy Generators	Privacy Policy Readers	Privacy Compliance Scanning	Browsing Pseudonyms	Virtual Email Addresses	Trusted Third Parties	Surrogate Keys	Crowds	Onion Routing	DC-Nets	Mix-Nets	Hordes	GAP	Tor	CRM Personalization	Application Data Management	Spyware Detection and Removal	Browser Cleaning Tools	Activity Traces eraser	Harddisk data eraser	Encrypting Email	Encrypting Transactions	Encrypting Documents
Authentication	X	X	X	X	X																							
Authorization	X	X	X	X	X																							
Identification	X	X	X	X	X																							
Data Protection	X	X	X	X	X	X	X	X																				X
Anonymity and/or pseudonymity	X	X	X	X					X	X	X		X	X	X	X	X	X	X	X	X	X			X			
Unlinkability											X	X		X		X	X	X	X	X	X	X	X	X	X			
Unobservability			X	X	X												X	X	X			X	X	X	X	X	X	X

Different tools in each category implement specific privacy process patterns. So far, using Table 1, a developer could choose for every process pattern which is/are the best implementation technique(s) among the ones available, always based on the privacy requirement(s) that needs to be realized, as well as the specific business context in which it will be implemented. However, this is not always the case since most organizations have a number of developers with different capabilities and opinions as well as various criteria with different weights that form the final decisions regarding which is the best technology that fits their organization.

Requirements engineering is a complex task that is affected by various factors. Among else, prioritization is a process that aims to determine which requirements should be given relative priority to the implementation process. When many project partners participate, often their personal experiences affect the way that they consider different requirements should be implemented first; in such a case, there is a need to establish a way to evaluate the different experiences and expertise and make a decision based on estimating all the participants' opinions. We describe methodological tools that provide a framework for decision support over conflicting evidence. We attempt to tackle with the issue of combining evidence from different experts in order to reach consensus in respect to the implementation of specific technique. The expert's opinion plays an important role in several parts of the development process; especially when decisions like the selection of tools for privacy and security come into focus. Instead of adopting a rigid process that demands consensus about the validity of a certain choice in respect to its evaluation for a number of factors, such as the cost or complexity, we prefer to utilize a method that lets the experts express on a scale their opinion about a specific choice and then combine the evidence from different sources.

Fuzzy theory provides solutions in the presence of vague or imprecise knowledge. Most of the cases people face decisions which cannot be made on a clear selection

with a yes or no answer. Binary decisions are rare. In most of the cases, evidence that comes from different sources is hard to be managed. Fuzzy measures may be well suited in these cases; among else they provide a framework to treat variables that are spreading in the [0,1] interval. Evidence theory [12] is a branch of decision theory that utilizes fuzzy measures to handle uncertainty.

In evidence theory, and more specifically the branch which is acknowledfged as Dempster-Schafer of major importance are belief measures, which can be defined as a function mapping a given set to the [0,1] interval: Bel:P(X) → [0,1]. The belief measure may be interpreted as the degree of confidence that a fact is true or that a given element belongs to a set. It is obvious that if X is the set for which its subjects are considered, then the following relations stand: ($Bel(\varnothing)=0$, Bel(X)=1,

$$Bel(A_1 \cup A_2 \cup .. \cup A_n) \geq \sum_i Bel(A_i) - \sum_{i<k} Bel(A_i \cap A_k) + .. + (-1)^{n+1} Bel(A_i \cap A_2 \cap .. \cap A_n)$$

(1), for all subsets A of X.

Considering the facts A1, A2,.., An, are pair-wise disjoint, the inequality (1) requires that the belief required with the union of the sub-sets is no smaller than the sum of belief pertaining to each individual set.

The Belief metric can be represented by a function m: P(X) → [0,1], such that $m(\varnothing)=0$ and $\sum m(A)=1$. Function m(A) expresses the proportion to which available evidence supports the claim that a particular element belongs to A. In other words the relation between the metric and the supporting function can be expressed as: $Bel(A) = \sum_{B|B\subseteq A} m(B)$ (2).

The utility of the aforementioned measures is considerable in case that the evidence comes from independent sources for example from independent evaluators.

Therefore in order to calculate $m_{1,2}$ for the set A considering the evidence that focuses on subset B∈ P(X) and on the subset C∈ P(X) the following sum of products needs to be calculated: $\sum_{B\cap C=A} m_1(B)\bullet m_2(C)$ (3) for all $A \neq \varnothing$. Since $m_{1,2}(\varnothing)$ should equal to 0, we need to exclude the following sum of products of these subsets who's intersection results in the empty set: $\sum_{B\cap C=\varnothing} m_1(B)\bullet m_2(C)$. Since $\sum_{A\in P(X)} m(A) = 1$, the combined evidence we are seeking is calculated if we subtract the value from 1 resulting in: 1- $\sum_{B\cap C=\varnothing} m_1(B)\bullet m_2(C)$. For normalization purposes the final result for the combined evidence $m_{1,2}(A)$ is given by the formula[14][16]:

$$m_{1,2} = \frac{\sum_{B\cap C=A} m_1(B)\bullet m_2(C)}{1-\sum_{B\cap C=\varnothing} m_1(B)\bullet m_2(C)} \quad (4).$$

Another issue worth noting is that by introducing, in our approach, the normalization factor $(1 - K)$ at the denominator we normalize the values and consider the appearance of strongly conflicting evidence as unlikely, associating thus such conflicts with the null set; in relevant literature there has been a lot of discussion on managing conflicts in evidence theory. In [13], Zadeh presents an example with a medical scenario in presence of conflicting evidence from different medical experts; it is shown that the combined evidence for unlikely events with high degrees of belief towards this unlikelihood, may result in a case where these not so probable events are given priority (due to the high support values on this unlikelihood). We need to clarify that in our examples, due to the nature of the software development process and due also to the fact that the variables have been specified from the beginning and are not assigned ad hoc by the evaluators, we do not consider that two different experts in the field will give conflicting evidence while examining the same parameters for the same technology.

Let's get back to the e-voting case. We consider independent experts who evaluate different solutions for a given privacy requirement. Considering that independent opinions may give different priorities to the existing requirements, we need to find an analysis tool that will enable us to reach a conclusion by incorporating these different evaluations. Traditional methods, and PriS so far, decide on a yes-no basis; this binary logic is hard to resolve conflicts in case when two different opinions lean differently, for example one is in favor of a specific technology while the other is less supportive. With traditional methods it would be hard to decide; fuzzy logic provides support to express intermediate opinions for example on the [0,1] interval.

Evidence theory [12][13][15] provides a methodological tool that considering the opinion of each member as well as an expressed support for this opinion, to make combined calculations and express the overall opinion of the group. In a given project we consider that a given set of requirements is achieved by implementing a given number of measures. As X we may consider the universal set of measures that implement a specific requirement. We consider next the subsets N, A and C that: a) the first subset N includes the measures that are by presumptive evidence essential in implementing a specific requirement, b) the set A includes the measures that are cost-efficient (affordable) and provide a value for money and c) is the set of measures that their complexity is such that allows their integration into a given software project. In our case study we had two different partner organizations that were responsible to select the appropriate technologies for the implementation of specific requirements.

In the specific case now we need to find the most appropriate technologies for realizing process P3 on which unlinkability process pattern is applied. According to table 1 a subset of candidate technologies (all available technologies are shown in the respective table) for realizing unlinkability in P3 is:

- Trusted Third Parties
- Onion Routing
- DC-Nets
- Mix Nets
- GAP
- Hordes
- Tor

The aim is to apply for the list of available solutions the ones that are considered by both parties as more appropriate, in terms of satisfaction of the given parameters that affect the decision:

a) the necessity of a measure,
b) the cost for its implementation, and
c) the complexity for its development.

We asked from the two parties to assign a value for each of the three parameters for two of the available solutions. Then we combine the evidence from the two sources according to equation (4) so that the outcome produces the combined evidence. The same process can be applied iteratively when more factors are considered for a given project. Initially, we examined the case Tor. The two parties assigned a value for the three parameters (necessary, affordable and complex, independently, as well as for their combination, for example necessary and affordable at the same time). The Bel metric shows the belief and is calculated using equation 2. Table 2 presents the values m_1 assigned by the first partner, while column 3 represents the respective values from the second partner. The 2nd and 4th columns are calculated and finally we extract the combined values for the combined evidence $m_{1,2}$ and Belief: $Bel_{1,2}$. Fig. 5 shows the values from Table 2.

From what is apparent, both parties give more value to the necessity and cost of the solution, as they have assigned in general higher values to these two metrics. The combined value for N and A are considerably high, which means that both parties consider that this solution should be implemented and also that it would not cost enough. We also see that they still consider it as complex in respect to other potential solutions.

We also considered the case for Hordes presented in Table 3 and figure 6 respectively. This time we see that both parties grade very low the cost of the solution. This results to very low combined values for the parameter A. But the combined values give to the project managers a tool to estimate the trend from the participants.

Table 2. m_1 assigned from the two developers regarding Tor

	m_1	Bel_1	m_2	Bel_2	$m_{1,2}$	$Bel_{1,2}$
N	0.03	0.03	0.15	0.15	0.20	0.20
A	0.03	0.03	0.22	0.22	0.22	0.22
C	0.02	0.02	0.06	0.06	0.08	0.08
N∪A	0.2	0.26	0.07	0.44	0.12	0.54
A∪C	0.2	0.25	0.12	0.4	0.16	0.46
N∪C	0.1	0.15	0.05	0.26	0.07	0.35
N∪A∪C	0.42	1	0.33	1	0.15	1.00

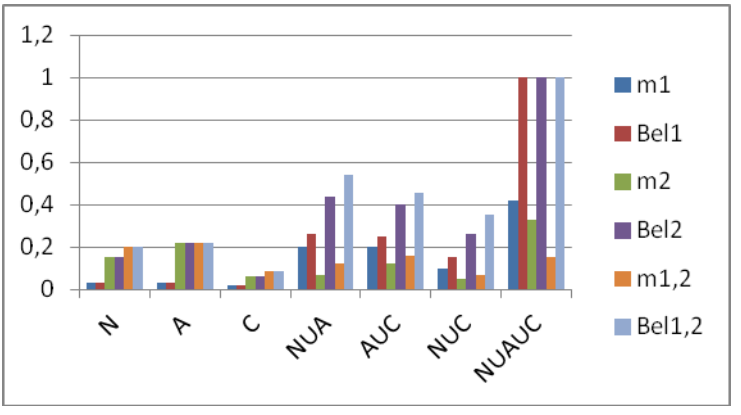

Fig. 5. Graphical representation of the values of Table 2

Table 3. m_1 assigned from the two developers regarding Hordes

	m_1	Bel_1	m_2	Bel_2	$M_{1,2}$	$Bel_{1,2}$
N	0.04	0.04	0.15	0.15	0.21	0.21
A	0.01	0.01	0	0	0.02	0.02
C	0.03	0.03	0.05	0.05	0.08	0.08
NUA	0.17	0.22	0.05	0.2	0.13	0.36
AUC	0.09	0.13	0.2	0.25	0.19	0.29
NUC	0.06	0.13	0.05	0.25	0.07	0.36
NUAUC	0.6	1	0.5	1	0.31	1.00

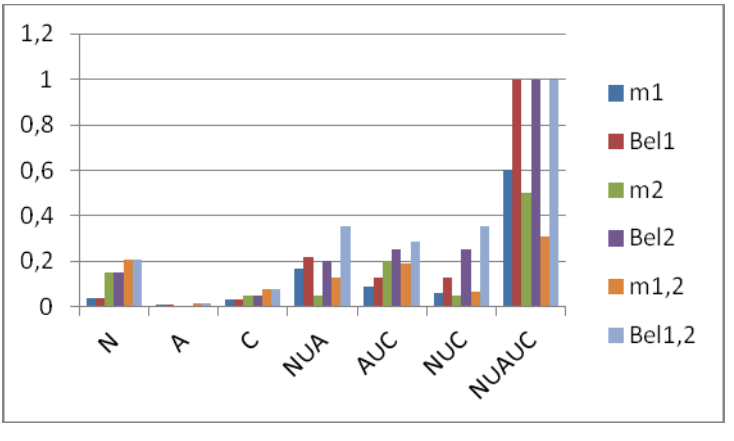

Fig. 6. Graphical representation of the values of Table 3

5 Conclusions

Decision making in software design process is not always straightforward; often the implementation of specific privacy related countermeasures depends on the evaluation of different factors for which often opinions vary among the project partners. In this paper an extension of PriS method is presented. On the main drawbacks of PriS was on the selection of proper PETs for the realization of the privacy process patterns identified during system design. While PriS bridges the gap between design and implementation it fails on the way of suggesting the implementation techniques. Specifically, the selection was conducted without any criteria rather than a yes/no criterion based on Table 1.

Thus, we have extended PriS by providing methodological tools that help the developers estimate the most appropriate solutions by considering combined opinions from independent sources while developing privacy measures in the software design process. The aforementioned method enables also to tackle a serious problem of estimating the combined opinions in a formal manner. It is important also to note that the method also is by no means limited by the number of independent evaluations nor by the number of subsets (factors) considered prior to making the decision.

References

[1] Kalloniatis, C., Kavakli, E., Gritzalis, S.: Methods for Designing Privacy Aware Information Systems: A review. In: Alexandris, N., Chryssikopoulos, V., Douligeris, C., Kanellopoulos, N. (eds.) Proceedings of the PCI 2009 13th Pan-Hellenic Conference on Informatics (with International Participation). IEEE CPS Conference Publishing Services, Corfu (2009)

[2] Loucopoulos, P., Kavakli, V.: Enterprise Knowledge Management and Conceptual Modelling. In: Chen, P.P., Akoka, J., Kangassalu, H., Thalheim, B. (eds.) Conceptual Modeling. LNCS, vol. 1565, pp. 123–143. Springer, Heidelberg (1999)

[3] Loucopoulos, P.: From Information Modelling to Enterprise Modelling. In: Information Systems Engineering: State of the Art and Research Themes, pp. 67–78. Springer, Berlin (2000)

[4] Kavakli, E., Gritzalis, S., Kalloniatis, C.: Protecting Privacy in System Design: The Electronic Voting Case. Transforming Government People Process and Policy 1(4), 307–332 (2007)

[5] Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: The PriS method. Requirements Engineering 13(3), 241–255 (2008)

[6] Kalloniatis, C., Kavakli, E., Kontellis, E.: PRIS tool: A case tool for privacy-oriented Requirements Engineering. Journal of Information Systems Security 6(1), 3–19 (2010); AIS SIGSEC

[7] University of the Aegean, E-Vote: An Internet-based electronic voting system. University of the Aegean, Project Deliverable D 7.6, IST Programme 2000#29518, Samos (November 21, 2003)

[8] Kavakli, E., Kalloniatis, C., Loucopoulos, P., Gritzalis, S.: Incorporating Privacy Requirements into the System Design Process: The PriS Conceptual Framework. Internet Research, Special issue on Privacy and Anonymity in the Digital Era: Theory, Technologies and Practice 16(2), 140–158 (2006)

[9] Kalloniats, C., Kavakli, E., Gritzalis, S.: Dealing with Privacy Issues during the System Design Process. In: 5th IEEE International Symposium on Signal Processing and Information Technology, Athens, Greece, December 18–21 (2005)
[10] Kavakli, V.: Goal Oriented Requirements Engineering: A Unifying Framework. Requirements Engineering Journal 6(4), 237–251 (2002)
[11] Kalloniatis, C., Kavakli, E., Gritzalis, S.: PriS Methodology: Incorporating Privacy Requirements into the System Design Process. In: Mylopoulos, J., Spafford, G. (eds.) Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference – Symposium on Requirements Engineering for Information Security. IEEE CPS, Paris (2005)
[12] Klir, G., Yuan, B.: Fuzzy sets and fuzzy logic. Prentice-Hall (1995)
[13] Zadeh, L.A.: Review of Books: A Mathematical Theory of Evidence. The AI Magazine 5(3), 81–83 (1984)
[14] Yager, R.: Quasi-Associative Operations in the Combination of Evidence. Kybernetes 16, 37–41 (1987)
[15] Sentz, K., Ferson, S.: Combination of Evidence in Dempster-Shafer Theory, Sandia National Laboratories, Technical Report SAND 2002-0835, Albuquerque, New Mexico (2002)
[16] Inagaki, T.: Interdependence between Safety-Control Policy and Multiple-Sensor, Schemes Via Dempster-Shafer Theory. IEEE Transactions on Reliability 40(2), 182–188 (1991)