ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Privacy Requirement Engineering Based on Modified Evidence Combination Approach

Nithya V. P., R. Subha

Abstract: **A major challenge in the field of software engineering is to make users trust the software that they use in their every day professional or recreational activities. Trusting software depends on various elements, one of which is the protection of user privacy. Protecting privacy can be defined as the right to determine when, how and to what information about them extends is communicated to others. The paper introduces the Privacy Safeguard (PriS) method. The method aims to include privacy requirements early in the system development process. Each privacy requirement is treated as a separate goal to be met during the system design process. The PriS method can be extended to address the degree of participation of every privacy requirements. It can be done by fuzzifiying privacy variables that maps degree of participation of each privacy variables to the [0, 1] interval. Dempster Shafer rule of combination is proposed to combine the evidences needed to select the implementation of the privacy requirement. A modified combination rule is proposed based on ambiguity measure (AM). The combination results based on the proposed approach can be more reasonable.**

***Keywords*- Privacy Requirement, Dempster Shafer Rule of Combination, Ambiguity Measure, PriS, Soft Computing**

I. INTRODUCTION

Privacy is a social and legal issue. It can be defined as the ability of an individual to control his own information. Various software applications are used as basic e-services, so additional technology-related requirements for protecting the electronic privacy of individuals are required. Privacy needs to be considered early in the software development process.

Nithya V. P, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore-64 1042, Tamil Nadu, India.

R. Subha, [2]Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore-64 1042, Tamil Nadu, India.

A) Privacy Oriented Requirement Engineering

Privacy protection is described in terms of eight privacy requirements [2] namely identification, authentication, authorization, data protection, anonymity, pseudonymity, unlinkability and unobservability. Authentication is the mechanism whereby the systems may securely identify their users. Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. Anonymity is defined as the ability of a user to use a resource or service without disclosing his/her identity. Pseudonymity is the user's ability to use a resource or service by acting under one or many pseudonyms. unlinkability expresses the inability to link related information. Unobservability protects users from being observed or tracked while browsing the Internet or accessing a service.

The protection of user privacy fall in two main categories: security-oriented requirement engineering methodologies [7] and privacy 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.

The paper presents, PriS conceptual framework for privacy management in requirement engineering. Then uses a soft computing approach that enables the expression of preferences from

independent participants in the system design process and their combined management using fuzzy metrics. PriS provides a methodological framework for representing privacy related issues during system development. It gives a set of concepts for expressing privacy requirements and also provides different ways for translating these requirements in to system models. Dempster Shafer rule of combination is used to combine the evidences from various sources to select the suitable method to implement the privacy requirement. Dempster rule of combination exhibits a counterintuitive behavior when combining conflicted evidences. This limits the use of Dempster shafer rule of combination. It discards all the conflicting mass assignments.

In the remainder we continue as follows. Section 2 details the related work to our paper. Section 3 provides more details about the methodology we used. Section 4 describes the experiments and the result obtained from those experiments. Conclusion is presented in section 5.

I. RELATED WORK

Evangelia Kavakli [9] introduced a unifying view of goal analysis in the context of RE. This allows the identification of similarities and differences between the different conceptions of goal used by different approaches and promote the understanding of the overall role of goal analysis in RE. Based on this understanding the various approaches can be put together thus leading to a stronger goal-driven RE framework that takes advantage of the contributions from the many streams of goal-oriented research. The different goal oriented method used in this paper are the goal-driven change method, the ISAC change analysis, the ***i**** strategic rationale modeling, the NFR framework, the GBRAM goal-based requirements analysis, the goal-scenario coupling method and the KAOS goal directed requirements elaboration method.

The method called PriS [3] describes a security requirements engineering method, which incorporates privacy requirements early in the system development process. PriS considers privacy requirements as organizational goals that need to be satisfied and adopts the use of privacy-process patterns as a way to: (1) describe the effect of privacy requirements on business processes; and (2) facilitate the identification of the system architecture that best supports the privacy-related business processes. 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 [6], is based on the Enterprise Knowledge Development (EKD) framework [13], which is a systematic approach for developing and documenting organizational knowledge. This is achieved through the modeling of: (1) organizational goals, that express the intentional objectives that control and govern its operation, (2) the 'physical' processes, that collaboratively operationalise organizational goals and (3) the software systems that support the above processes. In this way, a connection between system purpose and system structure is established.

Christos Kalloniatis provides an overview of recent requirements engineering approaches which focus on the elicitation and management of privacy requirements. Various privacy oriented requirement engineering methods [4] are described such as NFR (Non-Functional Requirement Framework) method, RBAC (Role-Based Access Control) method, M-N (Mofett-Nuseibeh Framework) method, B-S (Bellotti-Sellen Framework) method**.** The methodology describes the need of analyzing security and privacy requirements early during the system design phase.

Soft Computing is a collection of techniques which uses the human mind as a model and aims at formalizing our cognitive processes. These methods are meant to operate in an environment that is subject to uncertainty and imprecision. The objective is to study, model and analyze complex phenomena for which more conventional methods have not yielded low cost, analytic, and complete solutions. The main components of Soft Computing [10] are Fuzzy Logic [15], Probabilistic Reasoning, Neural Computing and Genetic Algorithms. Fuzzy set theory is an extension of classical set theory, where elements have varying degrees of membership. A fuzzy set is any set that allows its members to have different degree of membership in the interval [0, 1].

The Dempster-Shafer Theory (DST) [16], requires an expert to provide for each plausible model an interval of values, limited by a lower bound, called belief, representing the amount of belief that directly supports a given model and an upper bound, called plausibility and measuring the fact that the model could possibly be true "up to that value". According to the Dempster rule of Combination the measures of Belief and Plausibility are derived from the combined basic assignments. Dempster's rule combines multiple belief functions through their basic probability assignments (*m*).

II. METHODOLOGY

The methodology includes PriS [5] conceptual framework along with a soft computing approach to evaluate privacy requirements. This method uses the Dempster's modified rule of combination based on ambiguity measure (AM).

A) The PriS Conceptual Framework

PriS is a privacy requirements engineering methodology, which 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 is based on the Enterprise Knowledge Development (EKD) framework, which is a systematic approach to developing and documenting enterprise knowledge, helping enterprises to consciously develop schemes for implementing changes. EKD adopts a goal-oriented approach to software engineering.

The first step in PriS concerns the elicitation of the privacy goals [1] that are relevant to the specific organization. This task usually involves a number of stakeholders and decision makers. Therefore elicitation of privacy goals [9] includes the following activities: perform stakeholder analysis and organize stakeholder workshop; identify privacy issues; and agree on a structured set of privacy goals. The second step is to analyze the impact of these privacy goals on processes and related support systems. It involves identify the influence of privacy goals on organizational goals and analyze the impact on processes. The last step is to define the system architecture that best supports the privacy-related process identified in the previous step.

B) Soft Computing approach for privacy requirement evaluation

We can use Fuzzy theory [11] to expand PriS method to increase the flexibility of selecting implementation techniques which satisfy the identified process patterns. Fuzzy measures help interpret vague, imprecise and in general data that may not follow some well expected behavior, for example an evaluation from a human expert. We can use some methods provided by evidence theory to overcome the impreciseness that is the outcome of cooperation between different partners with different needs and experiences in a software project. We can use a combination of fuzzy measures and evidence theory such as Dempster Shaffer theory to determine the degree of support towards a given fact.

Dempster Shaffer theory is a mathematical theory of evidence [12]. It allows one to combine evidence from different sources and arrive at a degree of belief (represented by a belief function) that takes into account all the available evidence. Belief in a hypothesis is constituted by the sum of the masses of all sets enclosed by it (i.e. the sum of the masses of all subsets of the hypothesis). It ranges from 0 (indicating no evidence) to 1 (denoting certainty). Beliefs from different sources can be combined with various fusion operators to model specific situations of belief fusion, e.g. with Dempster's rule of combination [14], which combines belief constraint that are dictated by independent belief sources.

Belief measure is 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. The Belief metric can be represented by a function m: P(X) → [0, 1], such that m (Ø) = 0 and ∑m (A) = 1. Function m (A) expresses the proportion to which available evidence supports the claim that a particular element belongs to A. The belief Bel(A) for a set *A* is defined as the sum of all the masses of subsets of the set of interest:

$$\text{Bel}(A) = \sum_{B|B\subseteq A} m(B) \quad (1)$$

We need to find out the joint estimation $m_{1\,2}$ from independent assignment to values m_{1} and m_{2} from two independent sources. 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:

$$\sum_{B\cap C=A} m1\,(B).m2(C) \quad (2)$$

For all A≠ Ø. Since m1, 2(Ø) should equal to 0, we need to exclude the following sum of products of these subsets who's intersection results in the empty set: $\sum_{B\cap C=\,\emptyset}$ m1 (B) · m2(C). For normalization purposes the final result for the combined evidence is calculated by subtracting the value K= $\sum_{B\cap C=\emptyset} m1(B)m2(C)$ from 1. Where K *represents* basic probability mass associated with conflict. The denominator in Dempster's rule, 1-*K*, is a normalization factor. This has the effect of completely ignoring conflict and attributing any probability mass associated with conflict to the null set.

For normalization purposes the final result for the combined evidence $m_{1,\,2}$ is given by the formula:

$$m_{1,2} = \frac{\sum_{B\cap C=A} m1(B)m2(C)}{1-\sum_{B\cap C=\emptyset} m1(B)m2(C)} \quad (3)$$

The above mentioned metrics can be used in the system design process and can handle uncertainty.

C) Evidence Combination based on Ambiguity measures

In practical applications of evidence combination, there exist conflicts among the different evidences. In Dempster 's rule of combination, the conflicting mass assignments are discarded and it will lead to counterintuitive results. In Ambiguity measure (AM) [8] approach a modified combination rule is proposed. It uses weight factors to handle conflicts. The combination rule is as follows:

$m(A)= \sum_{B\cap C=A} m1(B).m2(C) + \Delta,$

Δ Can be

$$\sum_{A\cap D=\emptyset} w1m1(A)m2(D)+\sum_{A\cap E=\emptyset} w2m1(A)m2(E) \quad (4)$$

Where w1 is the weight for evidence m1 and w2 is the weight for evidence m2. $w1,w2 \in [0,1]$ and $w1 + w2 = 1$. The conflicting mass assignments are reassigned to the two conflicting focal elements with the proportion of (w1, $w2$). In this method the local conflicting mass assignments are redistributed based on the weight factors of different evidence sources. Let Q be a set with n elements $Q= \{\theta_1,\theta_2 \ldots \theta_n\}$, and let m be a basic probability assignment on Q.

$$AM= -\sum_{\theta\in Q} BetPm(\theta)\log_2(BetP_m(\theta)) \quad (5)$$

Where $$BetP_m(A)= \sum_{B\in Q} m(B)\frac{|A\cap B|}{|B|} \quad (6)$$

is the pignistic probability distribution. AM is also called the pignistic entropy. The lower the value of AM is, the less uncertainty the corresponding evidence has. The higher the value of AM is, the more uncertainty the corresponding evidence has.

III. EXPERIMENT AND RESULT

An electronic voting system [17] case study is taken and applied the PriS method on it. The aim of 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.

The four primary organizational goals of e-voting system are Generality, Equality, Freedom and Directness. Generality implies that all citizens above a certain age should have the right to participate in the election process. Equality implies that both political parties - that participate in the election process - and voters do not have equal rights before; during and after the election process and 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 implies that no intermediaries chime in the voting procedure and that each and every ballot is directly recorded and counted.

A goal model is constructed based on these organizational goals using GR Tool. The goal model also represents the relevant processes that satisfy each sub-goal.

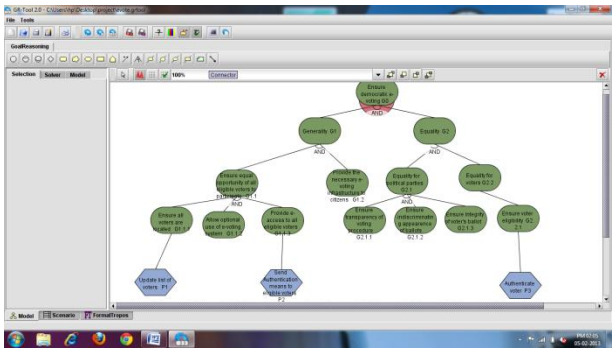

Fig. 1 Goal Model of E-Voting System

Authentication, unlinkability and unobservability are the identified privacy process patterns that affecting goals in E-Voting system. Consider the authentication process pattern, we have to find out the method to implement Authentication pattern. There are different methods to implement authentication process, they are,

- Identity management
- Biometrics
- Smart cards
- Permission management
- Monitoring and auditing tools.

We need to select one among these methods based on the opinion of experts to implement privacy process patterns. The PriS method couldn't suggest a specific implementation method. In most organizations the decision is made by the developers with different capabilities and select suitable methods for their organization. But this method is not flexible. For each of the available technologies the two parties will evaluate based on the three criteria: the necessity of a measure, the cost for its implementation and the complexity for its development. Each one of the experts can assign a value that shows to which degree it belongs to the given set and belief towards this estimation. Then we combine the evidences from the two sources using equation (3). We will get the following tables, Table1 and Table 2 corresponding to the two authentication implementation techniques, biometrics and smart card.

TABLE I
COMBINATION OF EVIDENCES FROM DIFFERENT EXPERTS FOR BIOMETRICS

Elements	Partner 1		Partner 2		Combined Evidence	
	m 1	Bel1	m 2	Bel2	m 1,2	Bel 1, 2
N	0.05	0.05	0.10	0.10	0.20	0.20
A	0.01	0.01	0.02	0.02	0.03	0.03
C	0.04	0.04	0.08	0.08	0.07	0.07
NUA	0.20	0.26	0.10	0.22	0.12	0.35
AUC	0.20	0.25	0.30	0.40	0.24	0.34
NUC	0.20	0.29	0.10	0.28	0.22	0.49
N ∪ A ∪ C	0.30	1	0.30	1	0.12	1

TABLE I
COMBINATION OF EVIDENCES FROM DIFFERENT EXPERTS FOR SMART CARDS

Elements	Partner 1		Partner 2		Combined Evidence	
	m 1	Bel1	m 2	Bel2	m 1,2	Bel 1, 2
N	0.03	0.03	0.05	0.05	0..05	0.08
A	0.04	0.04	0.03	0.03	0.03	0.07
C	0.03	0.03	0.02	0.02	0.2	0.08
NUA	0.1	0.17	0.15	0.23	0.15	0.27
AUC	0.1	0.17	0.18	0.24	0.18	0.24
NUC	0.2	0.26	0.2	0.27	0.21	0.26
N ∪ A ∪ C	0.3	1	0.37	1	0.37	1

From TABLE1 and TABLE II we can see that there is stronger evidence for the values m 1, 2 ($N \cup A \cup C$) in table 2. It means that there is stronger evidence towards implementing the second solution (smart cards) than implementing the first (biometrics).

IV. CONCLUSION

Introduced a privacy requirement engineering methodology, PriS. The aim is to incorporate privacy requirements early in the system development process adopting a goal-oriented approach. A fuzzy approach is used to extend the PriS method to address the degree of participation of every privacy requirements. Fuzzification of privacy variable maps the expression of degree of participation of each variable to the [0, 1] interval. Dempster shafer rule is used to combine the evidences from various sources needed to select the suitable implementation technique for privacy variables. An ambiguity measure based combination rule is proposed to handle conflicts in Dempster shafer rule of combination. Based on the proposed method (AM Based Method), results obtained are more reasonable and agree better with actual situations.

REFERENCES

[1]. Anton A.I Goal Based Requirement Analysis, IEEE Conference Publications. Proceedings of the 2nd IEEE international conference on requirements engineering (ICRE'96).
[2]. Christos Kalloniatis, Petros Belsis , Stefanos Gritzalis, A soft computing approach for privacy requirements engineering: The PriS framework. Applied Soft Computing**.** Volume 11, Issue 7, October 2011, Pages 4341–4348.
[3]. Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis, Addressing privacy requirements in system design: the PriS Method. pp. 133–153.
[4]. Christos Kalloniatis , Evangelia Kavakli, Stefanos Gritzalis, Methods for Designing Privacy Aware Information Systems: A Review, IEEE CPS Conference Publishing Services, Proceedings of the PCI 2009 13th Pan-Hellenic Conference on Informatics, **Page(s):** 185 - 194 .
[5]. C. Kalloniatis, E. Kavakli, E. Kontellis, PriS Tool: A Case Tool for Privacy Oriented Requirement Engineering, Journal of Information System Security, Vol. 6, No. 1, pp. 3-19, AIS SIGSEC
[6]. C. Kalloniatis, E. Kavakli, S. Gritzalis, "PriS Methodology: Incorporating Privacy Requirements into the System Design Process", Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference – Symposium on Requirements Engineering for Information Security, J. Mylopoulos, G. Spafford (Eds.), August 2005, Paris, France, IEEE CPS
[7]. Charles B. Haley, Robin Laney, Jonathan D. Moffett, Bashar Nuseibeh, Security rquirements Engineering: A Framework for Representation and Analysis, IEEE Transactions on Software Engineering (2008)
[8] Deqiang Han, Chongzhao Han, Yi Yang, A Modified Evidence Combination Approach Based on Ambiguity Measure, Information Fusion, 2008 11th International Conference Page(s)**:** 1 – 6
[9]. Evangelia Kavakli Goal Oriented Requirements Engineering: A Unifying Framework, Springer, Requirements Engineering January 2002, Volume 6, Issue 4, pp 237-251
[10]. Inma P. Cabrera, Pablo Cordero, and Manuel Ojeda-Aciego, Fuzzy Logic, Soft Computing, and Applications, Springer(2009), Volume: 5517.
[11]. Klir G., Yuan B, "Fuzzy sets and fuzzy logic", Prentice Hall, 1995
[12]. L.A. Zadeh, Review of books: a mathematical theory of evidence, The AI Magazine 5 (3) (1984) 81–83.
[13].Loucopoulos, P., Kavakli, V., Enterprise Knowledge Management and Conceptual Modelling. LNCS Vol. 1565. Springer (1999) 123-143
[14]. Piero Baraldi, Enrico Zio, A comparison between probabilistic and Dempster-Shafer Theory approaches to Model Uncertainty Analysis in the Performance Assessment of

Radioactive Waste Repositories, Wiley Online Library, Risk Analysis 2010,Volume 30.
[15].Rajwinder Kaur , Manisha Bhardwaj ,Neha Malhotra, Analyzing Imprecise Requirements Using Fuzzy Logic, International Journal of Engineering Research & Technology (2012), Volume 1.
[16]. Sentz, K. and S. Ferson. Combination of Evidence in Dempster-Shafer Theory, Sandia National Laboratories, Technical Report SAND 2002-0835, Albuquerque, New Mexico, 2002.
[17]. 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, 21/11/2003, Samos.