Towards a new generation of security requirements definition methodology using ontologies

Amina Souag

Towards a new generation of security requirements definition methodology using ontologies

Amina Souag
CRI , Sorbonne University Paris 1 , France
ISID-CEDRIC, Consérvatoire National des Arts et Metiers, France
Amina.Souag@malix.univ-paris1.fr

Abstract. In recent years, security in Information Systems (IS) has become an important issue, and needs to be taken into account in all stages of IS development, including the early phase of Requirement Engineering (RE). Recent studies proposed some useful approaches for security requirements definition but analysts still suffer from a considerable lack of knowledge about security and domain field. Ontologies are known to be wide sources of knowledge. We propose in this research to include ontologies into the requirements engineering process. Ontologies are factors in achieving success in requirements elicitation of high quality.

Keywords: requirements, ontologies, security, elicitation, analysis.

1 Introduction

Security for Information Systems (IS) has progressively become a very broad research field. It is no longer limited to classical virus attacks. Information assurance, security and privacy have moved from being considered by IS designers as technical topics of interest to become critical management issues [1]. Recall that security is defined as a discipline [2] which allows one to build reliable systems that can face malices, errors or mischiefs [3]. The British Standards Institution defined it as the protection of assets from a wide range of threats [4] which are of various origins: accidental or intentional, natural, human or technical [5]. The concept of IS security also encompasses a set of methods, techniques and tools in charge of protecting the resources of an IS to ensure information availability, confidentiality, integrity, and traceability. Elahi [6] provides a set of concepts that security includes: an attacker performs intentional actions without justification to break a system by exploiting a vulnerability. A vulnerability (flaw) is considered as a property of the system or environment which, in conjunction with an attack, can lead to a safety failure. An asset is defined as something valuable in an organization. Assets are subject to attacks. Risk equals threat times vulnerability divided by countermeasures. The countermeasures are sets of actions implemented in prevention of the threat.

A requirement prescribes a property judged necessary for the system; requirements engineering verifies that the requirements for a system are defined, managed and tested systematically [7]. Security RE frameworks derive security requirements using security specific concepts, borrowed from security engineering paradigm.

Despite existing methodologies in the field [8],[9],[10] most requirements engineers are poorly trained to define security requirements. This is due to a considerable lack of knowledge about security on one hand and about the field of business activity on the other hand.

An ontology, in the field of knowledge representation, is most often defined as "a representation of a conceptualization" [11]. It should represent a shared conceptualization in order to have any useful purpose [12]. Ontologies are useful for representing and interrelating many types of knowledge. Several security ontologies have been proposed [13], [14], [12]. Domain ontologies are formal descriptions of classes of concepts and relationships between these concepts that describe a given domain. The question we ask, is about the usefulness of ontologies for defining security requirements?

The rest of the paper is organized as follows: the second section addresses the problem of our research. Section 3 presents our proposal: the approach, related work and expected results. Finally Section 4 provides an update on the work progress and future work.

2 Problem statement

Security requirements are known to be difficult to identify, to express, to elicit, and to manage. Surveying security-related modeling notations and security requirements frameworks (Secure Tropos [9], Secure i* [10], abuse cases [15], misuse cases [16], UMLSec [17], SecureUML [18], reveals challenges for developing secure software systems. Some of them (UMLSec and SecureUML) address security in system-oriented terms, and do not support the modeling and analysis of security at an organizational level. They are designed to model computer systems and access control mechanisms and not for security requirements. Sometimes they turn out to be partial and do not model all security aspects like in [18]. Some others (Secure i* and Secure Tropos) seem to treat general issues of security and do not cover the security for a particular domain. The process proposed for the definition of requirements is incomplete or does not exist. Elahi pointed out in [6] that existing proposals do not consider potential conflicts between security and other functional and non-functional requirements. In current practice, the interaction of security requirements with other design objectives and goals of stakeholders are not analyzed, if any security requirement is gathered at all.

Moreover, it appears that with the growing need to implement IT security measures in world-wide corporate environments and the growing application scope, a major obstacle facing ordinary analysts and developers using existing security requirements modeling and analyzing frameworks is the lack of security and domain knowledge and expertise. Recent studies have shown that their lack of information security knowledge at the management level is one reason for inadequate or non-existing information security management strategies and that raising management information security awareness and knowledge level leads to more effective strategies.

To fill this gap, a major portion of research and practical development in security software engineering is dedicated to developing security ontologies and knowledge

bases. However, it still remains difficult for designers to extract relevant pieces of knowledge and apply it to their specific analysis design of security requirements. Several security ontologies have been proposed [27]. They vary in their degree of generality (business level) and specificity (technical level). They also vary in their coverage of security aspects. Some focus more on vulnerabilities, while others are dedicated to threats, or counter-measures, etc.. In addition, some domain ontologies exist in the literature, eg for medical, banking, aviation and maritime.

We propose to explore the use of security and domain ontologies to define a new guiding approach in the elicitation, analysis and validation of security requirements for a specific domain. How ? Will this be an interesting solution to cover lacks in the definition of security requirements complete, consistent and unambiguous? are the research questions we face. We want to test three main hypotheses: that (H1) the definition of security requirements can be performed using a phased approach in analogy to the definition of functional requirements, that (H2) security and domain ontologies are useful at each stage of the process, and (H3) the defined method will be better than existing methods, especially through the use of ontologies.

3 Proposed theory

As noted in Section 2, some efforts have already been started in the security requirement engineering domain, particularly with analysis and modeling methodologies, but important issues remain open and must be considered. In particular, a real lack of knowledge about security and domain at different development levels leaves these proposals useless. Our goal is to take advantage of the existing security and domain ontologies, and propose mechanisms and techniques to use them in an approach that guides the definition and analysis of security requirements for a particular domain of activity.

3.1 The proposed approach

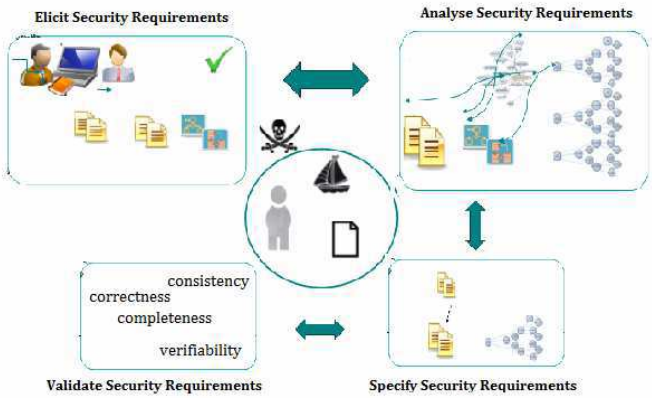

Figure 1. The proposed framework for the definition of security requirements.

The proposed approach is based on the steps in [19] for the development of requirements, but adapts them for the definition of security requirements. We explores the use of security and domain ontologies in each steps. Figure 1 gives a general view of the proposed approach. In the core, we find the Information Systems (IS) of a given organization, characterized by its human, physical and informational elements (Assets). It is exposed to various threats that exploit vulnerabilities in the system. The figure represents around the IS the four steps (elicit, analyze, specify, and validate) to follow for the elaboration of the target security requirement document.

- ***Security requirements elicitation:***

During the elicitation step, security problems are figured out, investigations about stakeholders needs and objectives in terms of security are obtained.
In this step, we suggest to rely on questionnaires, interviews and workshops with stakeholders, to inspect security documents of the field (nomenclature, regulations, etc..), and even to conduct direct observations on-site. Identify actors and potential malicious actors, vulnerabilities, potential threats, assets of the organization, and imagine some countermeasures for them.
The output should be a first set of textual security requirements and corresponding business models (using i* for example).

- ***Security requirements analysis:***

The analysis step aims to refine and restructure security requirements collected during the previous step. Here we plan to introduce security and domain ontologies to enrich, by defining a set of rules and use of mechanisms of ontological mapping, reasoning mechanisms, and queries on the ontologies, the set of textual security requirements and corresponding models. In this step the ontologies will be very helpful to the analyst who lacks knowledge about security and domain.

- Example of an enrichment rule of the security requirements model through the use of a security ontology:

Given a security ontology (SO), controls (Cont) in the security ontology are sets of actions implemented in prevention of a threat that exploits a vulnerability (Vul). Thus, if a control is implemented, the security attributes (SA) (confidentiality, integrity or availability) are maintained and the assets are protected from different threats (Threat). In an i* model, a task (T) is an activity that will accomplish a security softgoal (SG).
In Fig 2., a partial of an i* model shows that a *company* has as a goal to provide *maritime materials* to the *master* of a ship, and has as a security softgoal to ensure the integrity these materials. On the left a partial of a security ontology describes that a security attribute (*integrity*) is affected by the threat (*Damage_Asset*) which exploits a vulnerability (*InsufficientTrainingOfMaintenanceAndAdministrativeStaff*), this vulnerability is mitigated by the control (*TrainingOfMaintenanceAndAdministrativeStaff*).
Thus the security softgoal *Integrity* is mapped to the corresponding ontological element, here the security attribute *Integrity* in the i* model. (We consider that lexical

matching and keyword matching using thesauruses in the area of information retrieval are some of the techniques).
We verify if the security attribute is affected by a threat, thanks the property ***IsAffectedBy***(Integrity,Damage_Asset), and that the threat exploits a vulnerability: ***Exploits***(Damage_Asset,InsufficuentTrainingOfMaintenanceAndAdministrativeStaff) ,and that the vulnerability is mitigated by a control: ***MitigatedBy(***InsufficientTrainingOfMaintenanceAndAdministrativeStaff, TrainingOfMaintenanceAndAdministrativeStaff**)** exists in the security ontology.

The control in the security ontology can therefore be added as a task in the i* model and linked by means end link to the softgoal.

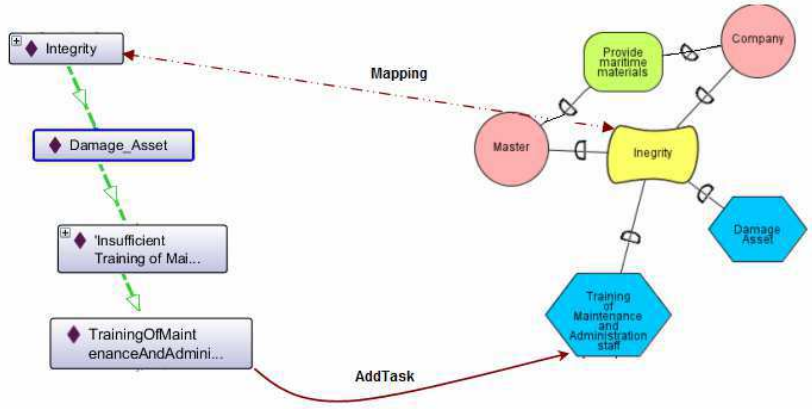

Figure 2. Example of the use of the security ontology in the analysis of security requirements

As an illustration, the `ControltoTask` rule is defined bellow:

```
If   IsAffectedBy (SA, Threat)
AND  Exploits(Threat,Vul)
AND  MitigatedBy(Vul,Cont)
AND  Mapped_element(SA,SG)
THEN Create Task (Cont)
     Create Link (MeansEnd,Cont,SG)
endif;
```

- ***Security requirements specification:***

This step consist in documenting the requirements in a sustainable and effective way for all project stakeholders (developers, testers, customers, etc...)
Once more, we suggest that this step rely on the use of ontologies: generic security ontologies for the problem domain requirements, and technical ones for the solution domain security requirements.

- ***Security requirements validation:***

Finally, during the last step, stakeholders review the defined security requirements. Then they are tested with a prototype. Then a validation is conducted of the quality attributes of the defined security requirements (consistency, correctness, completeness, verifiability) based on the security requirement document.

3.2 Related work

The RE community has started to be aware of the problem of security in the last years and a lot of security RE approaches have been developed:

• Object oriented approaches: or UML extensions, such as UML profiles (SecureUML [18], UMLSec[17]), Usecases (MisuseCases [16], AbuseCases [15], Security Use Cases [20]).
• Goal and agent approaches: such as extended i* [10], extended KAOS [8] and extended Tropos [9].
• Risk analysis based approaches [21] and [22].

To the best of our knowledge, none of these approaches considered the use of security ontologies in the development process. In a closely related context, some approaches used ontologies in the definition of requirements in [23] and [24], [25],[26]. However, these propositions don't deal with security at all, or deal with it in a general way, and do not cover security aspects such as threats, vulnerabilities or countermeasures, moreover, none of them was dedicated to use ontologies for definition of security requirements for a specific domain.

3.3 Expected outcome

This research aims to propose a new evolutionary and equipped approach, for guidance in the definition of security requirements. The principal feature lies in the use of extracted knowledge, of security and domain ontologies. The approach will guide the analyst designer by providing ontologies, a tool and mechanisms to extract relevant knowledge to apply it to his analysis of security requirements. The desired outcome is a better definition of security requirements. Thus, we strive to define 1) the steps of the method 2) the elements required to complete each step well 3), deliverables associated with each step 4) the rules guiding the analyst in charge of the step 5) elements of validation of the end of each step. Then we specify the specification document of the tool that supports the method for which we will build a prototype. The method and the tool will be validated through the maritime case study.

4 Progress

This project research is located at the intersection of three major scientific domains: requirement engineering, knowledge engineering and security engineering.

The first step was to understand the security domain (the target of our research) by gathering related definitions. Then we built a state of the art of different researches and proposals of the two domains requirements and ontologies for security requirement definition. We studied most of the security requirement approaches (12 approaches) and classified them into three families (object-oriented, agent and goal oriented, risk analysis oriented), and how each approach models security requirements (concepts, process, advantages and limitations). We also studied the quality of a lot of existing security ontologies (23 security ontologies) and classified them into eight families (theoretical basis, taxonomies, general, specific, risk based, web oriented, for security requirements, modeling). Moreover, we examined how each ontology of security covers security aspects (security objectives, assets, vulnerabilities, threats, counter-measures, organization), and whether it is used for requirements engineering [27]. This work of literature review is still in progress. As discussed in Section 3.2, some contributions deal with similar problems, but the bibliography indicates that no current approach is able to tackle every part of our problem.

Since the RE domain is very large and varied, we have tried to focus only on our main interests. We investigated mainly the goal-oriented and security driven modeling RE approaches, and up to now mainly the generic security ontologies.

We have extensively explored a case study associated with the maritime domain. We conducted interviews with stakeholders in this domain. A first draft of security requirements has been collected, requirements models were developed based on interviews and analysis of certain documents on maritime security. We are currently testing the incorporation of security ontologies in the process of defining requirements by relying on this case study which is rich in terms of security issues. We plan to validate our methodology by a contolled experience, and validate the resulting requirements with experts from security, domain and methods fields.

5 Acknowledgment

Thanks to my advisors Isabelle Comyn Wattiau and Camillle Selinesi for their guidance in this project. The work is supported by a research grant from the University Paris 1 Pantheon Sorbonne, and supervised jointly by the ISID-CEDRIC (CNAM) and the CRI (Paris 1) research teams.

References

1. Blanco, C., Lasheras, J., Valencia-Garcia, R., Fernandez Medina, E., Toval, A. and Piattini, M : A systematic review and comparison of security ontologies. International Conference on Availability, Relability and Security (ARES). Barcelona, IEEE Computer Society 813-820. (2008)
2. Patrick B. : Management de la sécurité des SI , Paris : Lavoisier, (2007).

3. Mouratidis, H; Giorgini, P; Manson, G.: Towards the development of secure information systems: Security Reference Diagram and Security Attack Scenarios. Proceedings of the FORUM at International Conference on Advanced Information Systems, Riga – Latvia. (2004)
4. BS799-1:1999 Information Security Management - Part 1: Code of Practice for Information Security. British Standards Institution, London. (1999).
5. Jacques Claviez: Sécurité informatique, Paris, J.C.i. inc, (2002).
6. Golnaz Elahi : Security Requirements Engineering: State of the Art and Practice and Challenges , http://www.cs.utoronto.ca/~gelahi/DepthPaper.pdf , (2009).
7. Kauppinen M., Kujala S., Aaltio T. and Lehtola L., "Introducing Requirements Engineering: How to Make a Cultural Change Happen in Practice", RE' (2002).
8. Lamsweerde . "Engineering Requirements for System Reliability and Security", Vol. 9. IOS Press, (2007), 196-238.
9. Mouratidis H., 'Analysing Security Requirements of information systems using Tropos', on Enterprise Information Systems, (2006).
10. Liu, L., Yu, E., Mylopoulos, J.,"Security and Privacy Requirements Analysis within a Social Setting", RE', Proceedings. 11th IEEE International, (2003).
11. Gruber, T. R., 'Toward Principles for the Design of Ontologies Used for Knowledge Sharing', International Journal Human-Computer Studies, 1995.
12. Dobson, Glen, Pete Sawyer. “Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web.” ReqE, (2006).
13. Fenz S., Ekelhart A.. "Formalizing information security knowledge". Information, Computer, and Communications Security, (2009).
14. Herzog, Almut, Nahid Shahmehri, and Claudiu Duma. “An Ontology of Information Security.” International Journal of Information Security , 2007.
15. McDermott J., Fox C., "Using Abuse Case Models for Security Requirements Analysis". In Proc. of ACSAC’99, pages 55–66. IEEE Press, (1999).
16. Sindre, Guttorm, and Andreas L Opdahl. “Eliciting security requirements with misuse cases.” RE' ,(2004).
17. Jürjens Jan, "UMLsec: Extending UML for Secure Systems Development", Proceedings of the 5th International Conference on The Unified Modeling Language,2002.
18. Lodderstedt T., Basin D. Jürgen D., "SecureUML: A UML-Based Modeling Language for Model-Driven Security", Proceedings of the 5th International Conference on The Unified Modeling Language, (2002).
19. Wiegers K. Software Requirements, Microsoft Press, (2003).
20. Firesmith Donald: "Security Use Cases", in Journal of Object Technology, May-June 2003.
21. Herrmann, Andrea and Morali, Ayse, RiskREP: Risk-Based Security Requirements Elicitation and Prioritization, (2010).
22. Mayer N., Rifaut A., Dubois E., "Towards a Risk-Based Security Requirements Engineering Framework", (REFSQ'05), Porto, Portugal, June (2005).
23. Saeki Motoshi, Kaiya Haruhiko, "Using Domain Ontology as Domain Knowledge for Requirements Elicitation". RE' (2006).
24. Liu Wei; He Ke-Qing; Wang Jiang; Peng Rong; "Heavyweight Semantic Inducement for Requirement Elicitation and analysis", Third International Conference on Semantics, Knowledge and Grid, (2007).
25. Castañeda1 V., Ballejos L., Caliusco L., Galli R. "The Use of Ontologies in Requirements Engineering" ,Global Journal of Researches in Engineering, (2010).
26. Dzung D., Ohnishi A., "Ontology-based Reasoning in Requirements Elicitation", 7th IEEE International Conference on Software Engineering and Formal Methods, (2009).
27. Souag A., Salinesi C., Wattiau I.; “Ontologies for Security Requirements: A Litterature Survey And Classification”. 2nd International Workshop on Information Systems Security Engineering WISSE’12, (2012).