Ontologies for Security Requirements: A Literature Survey and Classification (long version)

Amina Souag, Camille Salinesi, Isabelle Wattiau

Ontologies for Security Requirements: A Literature Survey and Classification

Amina Souag[1] , Camille Salinesi [1], Isabelle Wattiau[2]
[1] CRI ,University Paris 1 , France
{Amina.Souag, Camille.Salinesi}@malix.univ-paris1.fr
[2] CEDRIC ,Conservatoire National des Arts et Métiers , France
isabelle.wattiau@cnam.fr

Abstract. Despite existing methodologies in the field, most requirements engineers are poorly trained to define security requirements. This is due to a considerable lack of security knowledge. Some security ontologies have been proposed, but a gap still exists between the two fields of security requirement engineering and ontologies. This paper is a survey, it proposes an analysis and a typology of existing security ontologies and their use for requirements definition.

Keywords: Security, Ontologies, Security Requirements, Analysis, Classification.

1 Introduction

Security of 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 issues [1]. Recall that security is defined as a discipline [2] which allows one to build reliable systems that can face malice, errors or mischief [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 domain of IS security also encompasses a set of methods, techniques and tools responsible for 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 is characterized by the equation:

Risk = threat * vulnerability / countermeasure.

The countermeasures are sets of actions implemented in prevention of the threat. A requirement prescribes a property judged necessary for the system; security

requirements engineering frameworks derive security requirements using security-specific concepts, borrowed from security engineering paradigm. With the growing need to implement IT security measures in world-wide corporate environments and the growing application scope, a major obstacle, that face ordinary analysts and developers using existing security requirements modeling and analyzing frameworks, is the lack of security knowledge and expertise. It becomes also increasingly difficult for them to understand each other due to a non precisely defined terminology. Problems occur if an Asian employee is drafting a corporate-wide security policy, while his colleague in Russia is misinterpreting the policy, since the terms which were used are not explicitly defined. Some kind of agreed ontology can be used to avoid such inefficiencies [7].

An ontology, in the field of knowledge representation, is most often defined as "a representation of a conceptualization" [8]. A more detailed description of an ontology is that it is a formal representation of the entities and relationships which exist in some domain. It should also represent a shared conceptualization in order to meet any useful purpose [9]. Ontologies are useful for representing and interrelating many types of knowledge. In 2003, Marc Donner urged the necessity of having good security ontologies. He argued that too much security terminology is vaguely defined, thus it becomes difficult to communicate between colleagues and, worse, confusing to deal with the people we try to serve : "What the field needs is an ontology – a set of descriptions of the most important concepts and the relationships among them... A great ontology will help us report incidents more effectively, share data and information across organizations, and discuss issues among ourselves" [10]. The need for a security ontology has been also recognized by the research community in [11].

Recent studies have shown that the 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. In 2006, the European Network and Information Security Agency (ENISIA) rated the establishment of unified information bases for information security risk management and the need for risk measurement methods as high priority issues [12].

Since the awareness about security knowledge has grown in the scientific community, many security ontologies have been proposed during the last decade. But there are still many questions around these works: what are the different security ontologies available nowadays? Do they meet the requirements? Do they cover all or some security aspects? Which ontology can I choose as an analyst seeking for security knowledge for the definition of IS requirements? We faced these questions, and conclude that we definitely need a general survey of existing security ontologies. Because interest in using security ontologies in different fields of research has grown, analysts and researchers may find in this paper a road map, an overview of what exists in terms of security ontologies.

This work is part of a larger project aiming to improve security requirement definition using ontologies. Our main objective in this paper is to review, analyze, select and classify security ontologies, as a scope study but with a particular interest in the field of security requirements engineering.

The rest of the paper is organized as follows: in Section 2 we explain the methodology used in the study, Section 3 includes the survey and classification, and Section 4 recalls related works. Finally, Section 5, the conclusion, raises future perspectives.

2 Methodology of research

To perform this survey, we relied on information retrieval and survey methodologies presented in [13,14,15,16]. We started by gathering, as far as possible, any publication related to ontologies, requirements, security and its various aspects. The search was conducted inside the relevant and known sources of literature such as Google Scholar, ACM libraries, IEEE digital library etc. About 50 papers were gathered. We performed a first read to get a general idea; 21 papers were discarded at this stage when they were found to be far away from our target objective. A second read was carried out for deeper understanding and analysis of concepts and relations between them. Finally, a quality analysis lead us to classify them into different families, and we defined a set of criteria allowing us to compare the approaches. The result of this comparison is synthesized in Table 1. The table illustrates how each proposed ontology deals with security aspects and requirements.

3 Synthesis and Classification

It appears that some researchers intend to cover all security aspects and propose general ontologies while others tackle a specific aspect of security; they sometimes refer to previous security taxonomies. In another context, given the increased importance of the World Wide Web in many fields, while security plays a vital role in the success of the Semantic Web, the web community proposed some security related ontologies helping them to define security aspects of web resources and communication. Back to security analysis, some authors proposed related security ontologies by adapting risk analysis, we grouped them in a specific category. Others tried to develop security ontologies for requirements engineering studies, and later with the advancement of security requirements agent models (Secure i* [17], Secure Tropos [3,18]), related modeling ontologies were proposed describing the concepts and relationships used. In some cases the security ontologies belong simultaneously to two categories. For example, there are taxonomies for requirements [19], or web oriented and fairly generic [20]. In these cases, we assigned the ontology to the more dominant field of research. The result is composed of 8 families of security ontologies (Fig. 1), described as follows.

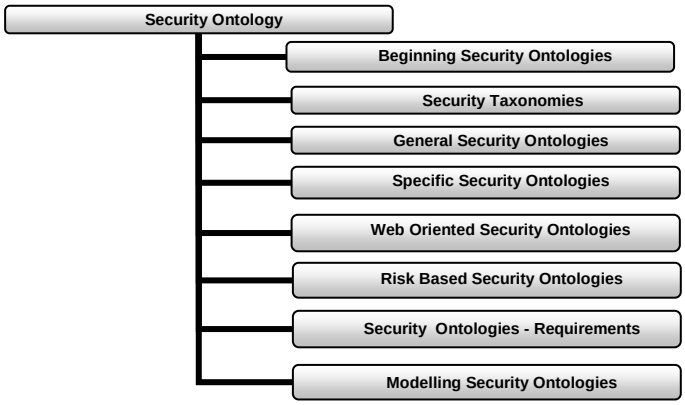

Fig. 1. Classification of Security Ontologies into 8 families.

3.1 Beginning security ontologies

One of the earliest work (back in the nineties) about merging knowledge base and information system management at an early level of development was [21] who proposed a language called Telos for representing knowledge about information systems and illustrates how this language can be applied in developing knowledge bases about software. The knowledge base is divided into four sub-worlds (*subject world, usage world, system world, development world*). Mylopoulos et al. note that Telos users can develop models for the purpose of security specification.

3.2. Security taxonomies

A taxonomy is an ontology in the form of a hierarchy. Whereas ontologies can have any type of relationship between categories, in a taxonomy there can only be generalization hierarchies. Taxonomies of security concepts are a common method for sharing security knowledge. There are some interesting taxonomies, which were used later for developing security ontologies:

- [22] provide a detailed taxonomy that contains classes of *faults*, *fault modes*, classification of *fault tolerance techniques*, and *verification* approaches. In this taxonomy, the main threats to dependability and security are defined as *failures*, *errors*, and *faults*. Avizienis et al. [22] classify the main means to attain security and dependability attributes into *fault prevention*, *fault tolerance*, *fault removal*, and *fault forecasting*.

- Landwehr et al. [23] were particularly interested in security flaws. Their taxonomy is based on three basic questions about each observed flaw: genesis (how

did it enter the system?), time of introduction (when did it enter the system?), and location (where in the system did it manifest?).

3.3. General security ontologies

By general ontologies we mean these ontologies which aim at covering all (or most) security aspects :

- Herzog and colleagues [24] have proposed an OWL-based ontology of information security. They endeavored to deliver an extensible ontology for the information security domain that includes both general concepts and specific vocabulary of the domain, and supports machine reasoning and collaborative development. The proposed ontology is built around the following top-level concepts: *assets*, *threats*, *vulnerabilities* and *countermeasures*. These general concepts together with their relations form the core ontology which presents an overview of the information security domain in a context-independent and application neutral manner. In order to be practically useful, the core ontology is populated with domain-specific and technical vocabulary which constitute the core concepts and implement the core relations. The ontology contains 88 threat classes, 79 asset classes, 133 countermeasure classes, and 34 relations between these classes.

- In the same vein, Fenz and Ekelhart [12] have proposed an ontology (500 concepts) that has a similar goal but attempts to cover a broader spectrum: their ontology models a larger part of the information security domain, including non-core concepts such as the infrastructure of organizations. In the high level concepts of the ontology and their relations we find *threat* which gives rise to follow-up threats, represents a potential danger to organization's *assets* and affects specific security attributes (*confidentiality*, *integrity*, *availability*) as soon as it exploits a *vulnerability* in the form of a physical, technical, or administrative weakness, and it causes damage to certain assets.

3.4. Specific security ontologies

This category gathers the specific domain security ontologies – the ones that describe specified aspects of security such as Session Initial Protocol vulnerabilities, Intrusion detection, etc.

- In [26], the authors propose a data model that characterizes the domain of computer attacks and intrusions as an ontology and implement that data model with an ontology representation language. At the topmost level of the ontology, they define the class *Host*. The *System Component* class is comprised of the subclasses (*Network*, *System*, *Process*). The class *Attack* is described by the properties *Directed to*, *Effected by*, and *Resulting in*. Accordingly, the classes *System Component*, *Input*, and *Consequence* are the corresponding objects. The class *Consequence* is comprised of several subclasses which include (*Denial of Service*, *User Access*, *Probe*). Finally, the

class *Input* is characterized by the predicates *Received from* and *Causing*, where *Causing* defines the relationship between the *Means of attack* and some *input*. *Received from* links *Input* and *Location*. The class *Location* is an instance of *System Component* and is restricted to instances of the *Network* and *Process* classes. *Means of attack* contains the following subclasses: *Input Validation Error, Logic Exploits*.

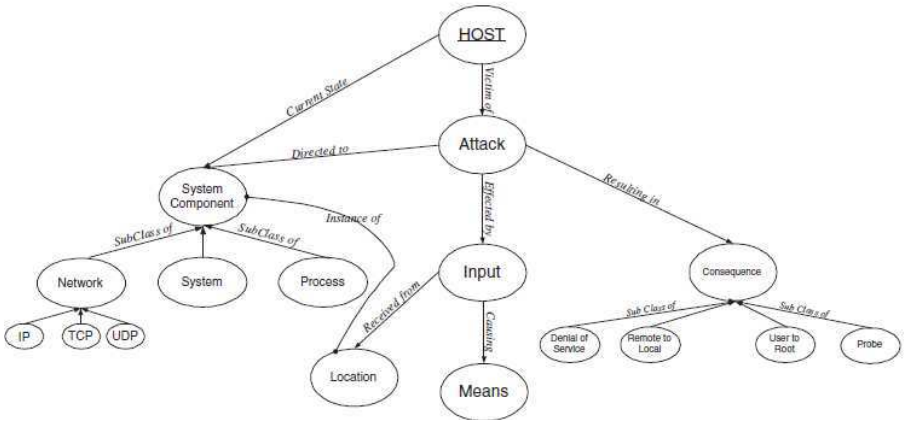

Fig. 2. Part of the ontology proposed by [26].

- [27] analyzed thirteen different computational trust models and derived a common vocabulary for describing facts that are considered for trust calculation in the reviewed trust models. The models can be classified as *identity-aware*, *action-aware*, *business value aware*, *capability-aware*, *competence-aware*, *confidence-aware*, *context-aware*, *history-aware* and *third-party-aware* in their input factors. The trust ontology comprises many ontological structures; *trust* is a relationship between two principals, the subject, *trustor*, and the target, *trustee*.

- Voice over IP (VoIP) telephony services suffer from various types of attacks and vulnerabilities, mainly due to the utilization of an open environment, the Internet. Geneiatakis and Lambrinoudakis [28] propose an ontology for SIP-VoIP based services. This ontology can be applied either to find a countermeasure against attacks on SIP based VoIP services or for testing the security robustness of SIP-VoIP (Session Initial Protocol-VoIP) infrastructure. The ontology contains two main concepts *SIP_attack* and *SIP_message*. Specifically any SIP attack employs a SIP message that is forwarded to a target node trying to cause a specific consequence. The SIP_attack is directed by a target and causes a consequence. It has two subclasses: *malformed* and *flood*.

3.5. Web oriented security ontologies

Some works addressed both the security community and the semantic web community.

- Denker et al in [30], [31], [32] develop several ontologies for security annotations of agents and web services, using DAML (DARPA Agent Markup Language) and later OWL (Web Ontology Language). The defined ontology is composed of two sub-ontologies: "*security mechanisms*" which capture high-level security notations and "*credential*" which defines authentication methods. The goal of these ontologies is to enable high-level markup of Web resources, services, and agents while providing a layer of abstraction on top of various web service security standards. These ontologies represent well-known security concepts and enable their users to interconnect security standards.

- The NRL Security Ontology proposed in [20] is organised around seven separate ontologies (*Main Security Ontology*, *Credential Ontology*, *Security Algorithms Ontology*, *Security Assurance Ontology*, *Service Security Ontology*, *Agent Security Ontology*, *Information Object Ontology*). Three of them are based on existing based ontologies in DAML: firstly, "*Service security ontology*", which describes security annotation of semantic web services; secondly, "*Agent security ontology*", which enables querying of security information; and finally "*Information object ontology*", which describes security of input and output parameters of web services. The four remaining ontologies are as follows: "*Main security ontology*", describes security protocols, mechanisms and policies; "*Credentials ontology*", specifies authentication credentials; "*Security algorithms ontology*", describes various security algorithms; and "*Security assurance ontology*", specifies different assurance standards.

- Artem Vorobiev and Jun Han proposed a security attack ontology for Web service [33]. The ontology brings together a set of attacks (*attacks on Web services*, *probing attacks*, *CDATA Field attacks*, *WS DoS attacks*, *WS DoS attacks*, *Application attacks*, *SOAP attacks*, *XML attacks*, *semantic WS attacks*).

3.6. Risk based security ontologies

Recent trends in security methodologies tends to consider that the best approach of security consists in starting from a risk analysis. It allows the experts to adapt the security solutions to the actual risk, leading to a more effective security plan.

- [7] proposed a security ontology framework based on four parts: the first part is the security and dependability taxonomy from [22], the second part presents the underlying risk analysis methodology, the third part describes concepts of the IT infrastructure domain and the fourth part provides a simulation enabling enterprises to analyze various policy scenarios. The ontology 'knows' which threats endanger which assets and which countermeasures could lower the probability of occurrence, the potential loss or the speed of propagation for cascading failures.

- [29] proposed to develop a knowledge base containing ontologies for the analysis of industrial risks describing concepts used for the achievement of a risk analysis.

3.7. (Security) Ontologies for Security requirements

Some papers refer to ontologies in order to cope with the definition of security requirements:

- Dobson and Sawyer [9] propose an ontology of dependability by merging two conceptualisation models (IFIP model: proposed by the IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance & UMD model: Unified Model of Dependability). Some of the IFIP attributes are themselves goals of security (Availability, Integrity, Maintainability, and Confidentiality). The ontology covers some security aspects such as *Failure*, Dependability Threat (*Error*, *Fault*), Dependability Attributes (*Availability*, *Integrity*, *Confidentiality*…)

- Tsoumas et al. [34] define a security ontology using OWL and propose the security framework of an arbitrary information system which provides security acquisition and knowledge management. Tsoumas et al. have used *Asset*, *Stakeholder*, *Vulnerability*, *Countermeasure* and *Threat* concepts in the construction of the security ontology. The security ontology acts as a container for the IS security requirements ("What" part).

- In [35], the authors use OWL to propose a security ontology with which to develop secure applications. The proposed ontology is formed of "*assets*" (data asset, hardware data,...), "*countermeasures*" (identification and authentication, network management, auditing services, physical protection,...), "*objectives*", "*persons*" (insider stakeholder, attacker,...) and "*threats*" (errors, attacks, technical failures,...). They validate the defined ontology using nRQL queries in order to demonstrate that their ontology can be used in various contexts. They apply it to e-government scenarios: e-tax and e-voting.

- Firesmith [19] presents a taxonomy of safety-related requirements: "*Safety requirements*" are requirements obtained from threats analysis. "*Safety-significant requirements*" includes non-safety requirements that can cause hazards and safety incidents. "*Safety constraints*" are constraints that directly impact safety and are derived from laws, policies, standards, and industrial practices. "*Safety system requirements*" specify aspects of the primary system.

3.8. Security modelling ontologies

Even if authors present them as ontologies, they mainly describe metamodels. They are very close to being a metamodel of security models. While the previous ontologies include security specific concepts such as threat, attack, vulnerability ..,

these ontologies include security related concepts for modelling requirements and the dependencies between them such as relationship, proposition, situation ..

- In [36], first, the concept of *security constraint* is introduced, as a separate concept, next to the existing concepts of Tropos. Secondly, existing concepts such as goals, tasks, resources, are defined with and without security in mind. For example a goal should be differentiated from a secure goal, the latter representing a goal that affects the security of the system. Thirdly, security-engineering concepts such as *security features*, *protection objectives*, *security mechanisms* and *threats*, which are widely used in security engineering, are introduced in the Tropos ontology, in order to make the methodology applicable by software engineers as well as security engineers.

- Massacci et al. [37] propose an extended ontology for security requirements. The very top of the taxonomy is adapted from DOLCE, a foundational ontology intended to account for basic concepts that underlie natural language and human cognition. Lower levels of the taxonomy include concepts from i*, problem frames and argumentation frameworks, with security concepts occupying the lowest strata of the taxonomy. Let's list some of their proposed concepts: Objects (*Proposition*, *Situation*, *Entity*, *Relationship*) – Entities (*Actor*, *Action*, *Process*, *Resources*, *Assets*) – Relationships (*do-dependency*, *can-dependency*, *trust-dependency*) from SI* – Propositions (*Fact*, *Claim*, *Argument*, *Domain-Assumption*, *Quality Proposition*, *Goal*).

Thus many papers propose security ontologies composed of different but related concepts aiming at common or different objectives. The following section compares and evaluate them.

3 Discussion and evaluation

In this section, we compare security ontologies and try to evaluate to which extent they cover security requirements and thus can be used in requirement engineering.

[21] did not literally propose a security ontology nor an ontology, but a basic taxonomy composed of four sub-worlds. The authors note that users of Telos (the proposed language for developing the knowledge base and the sub-worlds) have developed models for the purpose of security specification but did not detail the underlying models.

In the family of security taxonomies, [22] proposed a detailed taxonomy of security and dependability. But this taxonomy fails to cover techniques for protecting confidentiality, establishing authenticity, analysing issues of trust and the allied topic of risk management. Some important security elements are not addressed, such as vulnerabilities and assets. The taxonomy doesn't deal with any use for requirements.

The main limit in the taxonomy of [23] is that it is too basic, focused on some flaws in operating systems only, far from many kinds of security flaws that might occur in

application programs for database management, word processing, electronic mail, and so on. The study needs to be updated with recent work. Flaws in networks and applications are becoming increasingly important, and the distribution of flaws among the categories they have defined may not be stationary. The taxonomy of [23] focused on a special kind of threats and does not address any countermeasure or related vulnerability.

The two general security ontologies [24] and [12] are both interesting contributions but neither of them is complete. While the first one seems simple and clearer, the second is much richer but more complex. Fenz et al. cover better asset concepts, while Herzog et al. cover threat concepts better. Fenz's main contribution consist of the organisation concepts, clearly absent from Herzog. Herzog's countermeasures tend to be technical whereas Fenz's are both business and technical. The advantage of these ontologies of being generic and capturing most security aspects leads also to drawbacks since they lack in specificity that the specific security domain ontologies [26], [27], [28] provide, and vice-versa. Neither [24] nor [12] ontologies were used for requirements definition and analysis, but both, combined with the specific ontologies, can be a very good source of security knowledge for requirements. The general ontologies offer generic concepts of security objectives, assets, vulnerabilities, countermeasures, threats... while the rest offers more specific threats concepts (computer attacks and intrusions in [26], for example).

The security ontologies developed in the semantic web area are not negligible. The ontology of [20] looks like a generic security ontology from a first sight with its seven sub-ontologies. However it does not cover some aspects like vulnerabilities and assets or organisation, or even threats. Nevertheless, in a web sharing community, where both resource requestors and providers have security requirements, [20] proposed a matching algorithm that facilitates mapping of higher level (mission-level) security requirements to lower-level (resource level) capabilities using the ontology. In a very similar previous work by Denker et al. [30][31][32], the proposed ontology fails to consider vulnerabilities, assets and threats; but a reasoning engine matches between the request requirements and the capabilities of the potential web service whose requirements need to be satisfied by the capabilities specified in the request.

The risk based security ontologies we found in [7] and [29] could be useful for a risk based requirement analysis like [38] or [39]. However, to the best of our knowledge, there were no propositions combining both sides.

In the context of requirements engineering some ontologies were proposed, but unfortunately none of them is associated to a methodology describing how to use them for requirement definition. Dobson and Sawyer's ontology [9] concentrates on few threat concepts, and neglects many other aspects of security. Tsoumas et al [34], in addition to their ontology, provided a framework, but don't indicate any detailed mechanism on how to use the ontology for requirement collection. The main lack of Karyda et al. [35] is the absence of vulnerability related concepts, although they propose many examples of queries on the ontology, that provide answers to the developer in an e-government application.

Finally, the security modelling ontologies, which are more security modelling oriented (relationship, entity...) than security concept oriented (assets, threats, ...) might be useful for constructing security requirements models like Secure i* and Tropos. A limitation common to all the ontologies we have been facing is that they are described in papers but are not available on the Internet, which makes their use difficult.

We summarise this analysis and evaluation in Table 1. The rows are the families of security ontologies. The columns list the aspects related to security (objectives, assets, vulnerabilities, threats, countermeasures and organisation). The last column in the table evaluates the link between the ontology and requirements definition. A black dot measures to which extent does the security ontology cover this specific aspect of security, and how does this particular security ontology deals with requirements. We used a dash for absence of use and a black square to indicate that technical aspects of security were addressed, as follows: How does the ontology cover this concept of security? How does this security ontology proposal deal with requirements (last column)?

-: absent ●: very few ●●: few ●●●: much ●●●●: very much ■: Technical

To complete the study we drew up a graph that represent roughly, for each security ontology, how much it deals with requirements (axis of abscissa) and how much it covers security concepts (axis of ordinates). The graph in Figure 3 clearly reveals a gap between the two fields. There is not a perfect ontology that covers lots of security aspects and, at the same time that can be used in the definition for security requirements.

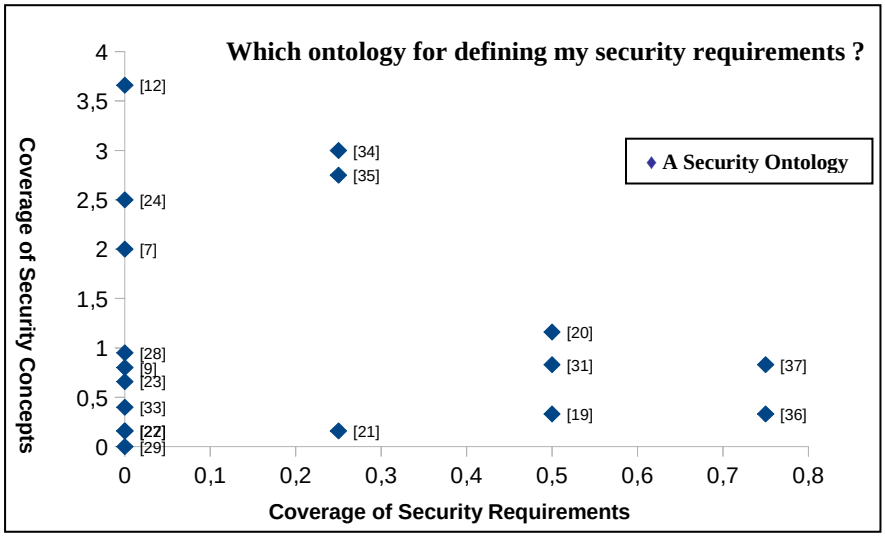

Fig. 3. Using security ontologies for requirement definition

4 Related works

While many security ontologies have been proposed, few surveys have been attempted. The only ones we can cite here are [1], [6] and recently [40]. [6] was not primarily about ontologies, but she mentioned some security ontologies and taxonomies in her state of art of security requirements. [40] proposed a survey of general ontologies for information systems encompassing some few security ontologies. Blanco et al. [1] is an interesting review and comparison of security ontologies that helped us in our study. However, since 2009 other ontologies have been proposed, indicating a need for updating. Moreover, Blanco et al. organized the existing ontologies under four categories (general security ontologies, applied to a specific domain, theoretical works, semantic web-oriented). Our aim was to extend this classification to additional categories and to update their surveys with recent literature contributions.

5 Conclusion and perspectives

Let us come back to our main question: which security ontology for my requirements? This study has shown the existence of considerable work around security ontologies; several ontologies have been proposed. We classified them into eight families (theoretical basis, security taxonomies, general, specific, risk based, web oriented, requirements related, modelling). This classification extends the previous works which were limited to two, three, or four families at best.

Our analysis has also shown that the existing security ontologies vary a lot in the way they cover security aspects; we tried to analyse how each ontology covers each aspect of security (objectives, assets, vulnerabilities, threats, countermeasures, and organisation). Moreover, we studied whether the proposed security ontology can be used for requirements definition and the degree of this use.

The study revealed a real gap between the fields of security requirement engineering and ontologies, and thus a new area of research to explore.

We believe that this work can be improved; the classification needs to be extended. We need sub-categories for each family of security ontologies. We also believe that there are still important issues to be addressed in the adaptation of ontology-based requirements engineering techniques to security requirements Engineering. This paper allows us to assert that the challenges facing software security is the lack of an easily accessible large common body of security knowledge. Although much security ontologies are available, they all fall short in completeness and suitable granularity. It also remains difficult for designers to extract relevant pieces of knowledge to apply to their specific design or requirements related decision making situations.

Our objective for the next steps of the project is to explore the techniques and mechanisms for the best use of these security ontologies for security requirement definition.

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, Reliability 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 – Latvi. (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]: Ekelhart A., Fenz S., Klemen M., Weippl E.: Security Ontologies: Improving Quantitative Risk Analysis", pp.156a, 40th Annual Hawaii International Conference on System Sciences (HICSS'07), (2007).

[8]: Gruber, T. R.: Toward Principles for the Design of Ontologies Used for Knowledge Sharing. International Journal Human-Computer Studies, 43(5-6):907 928, (1995).

[9]: Dobson G., Pete S.. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web." Requirements Engineering , (2006).

[10]: Donner, M.: Toward a Security Ontology. IEEE Security and Privacy, (2003).

[11]: Denker G.: Access Control and Data Integrity for DAML- +OIL and DAML-S, SRI International, USA, (2002).

[12]: Fenz S., Ekelhart A.: Formalizing information security knowledge. In 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09), pp. 183-194, 2009., (2009).

[13]: Levy, Y., and Ellis, T.J.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research, Informing Science Journal (9), pp 181-211. (2006).

[14]: Barnes, S. J.: Assessing the value of IS journals. Communications of the ACM, 48(1), 110-112. (2005).

[15]: Rainer, R. K., & Miller, M. D.: Examining differences across journal rankings. Communications of the ACM, 48(2), 91-94. (2005).

[16]: Metcalfe, M.. Metaphors for literature reviews (responses summary for ISWorld listserv email request). (2002, June 21).

[17]: Liu L., Yu E., and Mylopoulos J.: Security and privacy requirements analysis within a social setting. In Proc. of RE'03, page 151. IEEE Computer Society, (2003).

[18]: Mouratidis H.: Analyzing Security Requirements of Information Systems using Tropos Proceedings 1st Annual Conference on Advances in Computing and Technology (AC&T), London - United Kingdom, pp. 55 – 64. (2006).

[19]: Donald G. Firesmith.: A Taxonomy of Safety-Related Requirements, RE'2004 Requirements for High Assurance Systems (RHAS)Workshop, in Kyoto, Japan, IEEE Computer Society, Washington, D.C., (6 September 2003).

[20]: Kim, A., Luo J., and Kang M.: Security Ontology for Annotating Resources. in 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05). (2005).

[21]: Mylopoulos J., Jarke M., Koubarakis M.. Telos – a language for representing knowledge about information systems. ACM Trans. Information Systems 8(4):327-362, (1990).

[22]: Avizienis A., Laprie J.-C., Randell B., and Landwehr C. E.: Basic concepts and taxonomy of dependable and secure computing. EEE Trans. Dependable Sec. Comput., vol. 1, no. 1, pp. 11–33, (2004).
[23]: C. E. 23, A. Bull R., McDermott J. P., and Choi W. S.: A taxonomy of computer program security flaws," ACM Comput. Surv., vol. 26, no. 3, pp. 211–254, (1994).
[24]: Herzog A., Shahmehri N., and Duma C.: An Ontology of Information Security. International Journal of Information Security 1.4 : 1-23 (2007).
[25]: Bishop M .:Computer security – art and science. Addison Wesley, (2003).
[26]: Undercoffer J., Joshi A., Pinkston A.: Modeling computer attacks: an ontology for intrusion detection . Lecture Notes in Computer Science, pp. 113–135.2820, (2003).
[27]: Viljanen, L.: Towards an ontology of trust. In: Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus'05). (2005).
[28]: Geneiatakis, D. and C. Lambrinoudakis, An ontology description for SIP security flaws. Computer Communications,. In Press, Corrected Proof. (2006).
[29]: Abou Assali A., Lenne D., Debray B.: Ontology development for industrial risk analysis. In: IEEE International Conference on Information & Communication Technologies: from Theory to Applications (ICTTA 2008), Damascus, Syria (April 2008).
[30]: Denker, G., Kagal, L., Finin, T., Paolucci, M., and Sycara K.: Security for DAML Web Services: Annotation and Matchmaking. In Proc. of the 2nd International Semantic Web Conference (ISWC2003): Sanibel Island, Florida (2003).
[31]: Denker, G., Nguyen, S., and Ton, A.: OWL-S Semantics of Security Web Services: a Case Study. In 1st European Semantic Web Symposium: Heraklion, Greece.(2004).
[32]: Denker, G., L. Kagal, and T. Finin.: Security in the Semantic Web using OWL. Information Security Technical Report. 10(1): p. 51-58. , (2005).
[33]: Vorobiev, A. and J. Han, Security Attack Ontology for Web Services. Proccedings of the Second International Conference on Semantics, Knowledge, and Grid SKG '06. IEEE Computer Society, p. 42. (2006).
[34]: Tsoumas B., Gritzalis D.: Towards an ontology-based security management. In 20th International Conference on Advanced Information Networking and Applications, pp. 985-992, (2006).
[35]: Karyda, M., et al.: An ontology for secure e-government applications. First International Conference on Availability, Reliability and Security (ARES'06). IEEE Computer Society: p. 1033-1037. (2006).
[36]: Mouratidis, H., P. Giorgini, and Manson G.: An Ontology for Modeling Security: The Tropos Approach, in Knowledge-Based Intelligent Information and Engineering Systems., Springer Berlin / Heidelberg. p. 1387-1394. (2003).
[37]: Massacci, F., Mylopoulos, J., Paci, F., Tun, Thein and Yu, Yijun.: An extended ontology for security requirements. In: International Workshop on Information Systems Security Engineering, (20-24 June 2011).
[38]: Herrmann A., Morali A., Etalle S., Wieringa R.: RiskREP: Risk-based Security Requirements Elicitation and Prioritization. In BIR 2011, Associated Workshops and Doctorial Consortium, Latvia, 155-162. (2011).
[39]: Meyer N., Rifaut A., and Dubois E.. Towards a Risk-Based Security Requirements Engineering Frame-work. REFSQ-Proc. Of Internet. Workshop on Requirements Engineering for Software Quality, (2005).
[40]: Nguyen V., Ontologies and Information Systems: A Literature Survey, http://hdl.handle.net/1947/10144 , (2011).

Table 1. Summary of security ontologies of the study

Family	Security ontology[1]	Security Objective[1]	Assets[1]	Vulnerabilities[1]	Threats[1]	Counter-measures[1]	Organisation[1]	**Requirements[2]**
Beginning	[21]	-	-	-	-	-	●	●
Security Taxonomies	[22]	●●●	-	-	●●	●●●●	-	-
	[23]	-	-	-	●●●●■	-	-	-
General	[24]	●●	●●●■	●●	●●●■	●●●■	●●	-
	[12]	●●●●	●●	●●●●	●●●●	●●●●	●●●●	-
Specific	[26]	-	●■	●■	●●■	-	-	-
	[27]	●	-	-	-	-	-	-
	[28]	●●	-	-	●●●■	-	-	-
Risk based	[7]	●●	-	-	●●●● ■	●●●	●●●	-
Web oriented	[30] [31] [32]	●●●	-	-	-	●●■	-	●●
	[20]	●●●●	-	-	-	●●●■	-	●●
	[33]	-	-	-	●●●●■	-	-	-
For security requirements	[9]	●●	-	-	●●	-	-	-
	[34]	-	●●●	●●●	●●	●●●	●	●
	[35]	●●	●●●	-	●●●	●	●●	●
	[19]	-	●	-	●	-	-	●●
Modelling	[36]	●	-	-	-	-	●	●●●
	[37]	●●	●●	-	●	-	-	●●●

[1] How does the ontology cover this concept of security ? - : absent ●: very few ●●: few ●●●: much ●●●●: very much ■: Technical

[2] How does this security ontology deal with requirements (last column)