Ontologies for Security Requirements: A Literature Survey and Classification

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-CNAM & ESSEC Business School, 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, Requirements, Analysis, Classification.

1 Introduction

Security of Information Systems (IS) has progressively become a very broad research field [1]. Security is defined as a discipline which allows one to build reliable systems that can face malice, errors or mischief [2]. 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. 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 [3][29]. Ontologies are useful for representing and interrelating many types of knowledge [4],[5]. In 2003, Marc Donner 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 [6]. Since that, many security ontologies have been proposed during the last decade. But there are still 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 concluded that we definitely need a

general survey of existing security ontologies. Analysts and researchers may find in this paper a road map, an overview of what exists in terms of security ontologies. Our main objective 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 [7,8]. We started by gathering 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 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 qualitative 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.

3 Synthesis and Classification

The framework of our classification is composed of 8 families of security ontologies (Fig. 1), described as follows:

- **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 [9] which proposed a language (Telos) and a knowledge base divided into four sub-worlds. Mylopoulos et al. note that Telos users can develop models for the purpose of security specification.

- **Security taxonomies:**

  Taxonomies of security concepts are a common method for sharing security knowledge. Avizienis et al. [10] provide a detailed taxonomy that contains classes of *faults, fault modes, fault tolerance techniques*, and *verification* approaches. McDermott et al. [11] were particularly interested in security flaws.

- **General security ontologies:**

  By general ontologies we mean these ontologies which aim at covering all (or most) security aspects; Herzog and colleagues [12] endeavored to deliver an extensible ontology that includes both general concepts and specific vocabulary of the domain. In the same vein, Fenz and Ekelhart [13] have proposed an ontology that has a similar goal but attempts to cover non-core concepts such as the infrastructure of organizations.

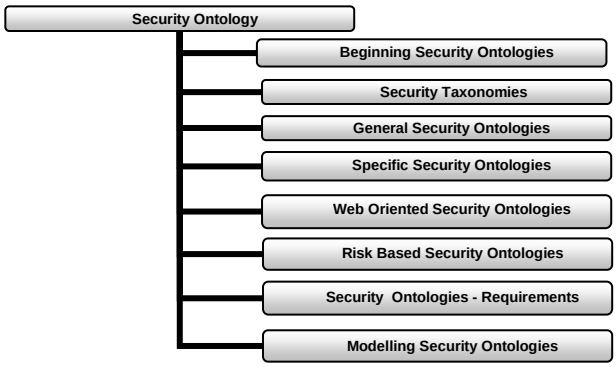

Fig. 1. Classification of Security Ontologies into 8 families.

- **Specific security ontologies:**

This category gathers the security ontologies dedicated to a specific domain. In [14], the authors propose a data model that characterizes the domain of computer attacks and intrusions as an ontology that covers concepts like (*Host, System Component Attack, input, Consequence).* Geneiatakis and Lambrinoudakis [15] 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) infrastructures.

- **Web oriented security ontologies**:

Denker et al in [16,17,18] develop several ontologies for security annotations of agents and web services, using DAML and later OWL. The defined ontology is composed of two sub-ontologies: "*security mechanisms*" and "*credential*". The NRL Security Ontology proposed in [19] is organised around seven separate ontologies. Artem Vorobiev and Jun Han proposed a security attack ontology for Web services [20].

- **Risk based security ontologies**:

Recent trends in security methodologies tend to consider that the best approach of security consists in starting from a risk analysis. Fenz et al. [3] proposed a security ontology framework based on four parts (the security and dependability taxonomy from [10], the underlying risk analysis methodology, the concepts of the IT infrastructure domain, and a simulation enabling enterprises to analyze various policy scenarios). Lenne et al. [21] proposed to develop a knowledge base containing ontologies for the analysis of industrial risks describing concepts used for the achievement of a risk analysis.

- **(Security) Ontologies for Security requirements:**

Some papers refer to ontologies in order to cope with the definition of security requirements: Dobson and Sawyer [5] propose an ontology of dependability by merging two conceptualisation models (IFIP model & UMD model). Tsoumas et al. [22] define a security ontology using *Asset*, *Stakeholder*, *Vulnerability*, *Countermeasure* and *Threat* concepts. In [23] (Karyda et al.), the authors proposed an ontology formed of "*assets*" (data asset, hardware data, etc.),

"*countermeasures*" (identification and authentication, network management, auditing services, physical protection, etc.), "*objectives*", "*persons*" and "*threats*" (errors, attacks, technical failures, etc.). Firesmith [24] presents a taxonomy of security-related requirements (pure security requirements, security-significant requirements, security system requirements, security constraints).

- **Security modelling ontologies:**

Even if authors present them as ontologies, they mainly describe metamodels. 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. Thus Mouratidis et al. [25] and Massacci et al. [26], proposed ontologies respectively associated with Tropos and i*.

4 Discussion and evaluation

In this section, we present the result of our comparison and evaluation of the ontologies by using a set of criteria (security objectives, assets, vulnerabilities, threats, countermeasures and organisation). *Security objective* defines which security objective (accountability, confidentiality, integrity) are wished to be reached and can be affected by a certain threat. A *threat* is anything (manmade or act of nature) that has the potential to cause harm, it exploits a vulnerability. A *vulnerability* is considered as a property of the system or environment which, in conjunction with an attack, can lead to a failure. An *asset* is defined as something valuable in an *organization*. *Assets* are subject to attacks. The *countermeasures* are sets of actions implemented in prevention of the threat [27].

Mylopoulos in [9] did not literally propose a security ontology, but a basic taxonomy composed of four sub-worlds. The authors note that users of Telos have developed models for the purpose of security specification but did not detail the underlying models. Avizienis et al. [10] fail to cover techniques for protecting confidentiality and establishing authenticity. The taxonomy was not used for requirements definition. The main limit in the taxonomy of McDermott et al. [11] 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, electronic mail, and so on. The two general security ontologies of Herzog et al.[12] and Fenz et al. [13] 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. are better focused on threat concepts. 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 criteria leads also to drawbacks since they lack in specificity that the domain dedicated security ontologies provide, and vice-versa. Neither [12] nor [13] ontologies were used for requirements definition and analysis. The general ontologies offer generic concepts of security objectives, assets, vulnerabilities,

countermeasures, threats, etc. while the rest offers more specific threats concepts (computer attacks and intrusions in [14], for example). The web oriented security ontologies do not cover some aspects like vulnerabilities or threats. Nevertheless, Kim et al. [19] 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. [16,17,18], the proposed ontology fails to consider vulnerabilities, assets and threats; but a reasoning engine matches between the request requirements and the capabilities of a potential web service. The risk based security ontologies of Fenz et al. [3] and Lenne et al. [21] could be useful for a risk based requirement analysis. However, to the best of our knowledge, there are 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 [5] concentrates on few threat concepts. Tsoumas et al. [22] don't indicate any detailed mechanism on how to use the ontology for requirement collection. Finally, the security modelling ontologies, which are more security modelling oriented might be useful for constructing security requirements models like Secure i*.

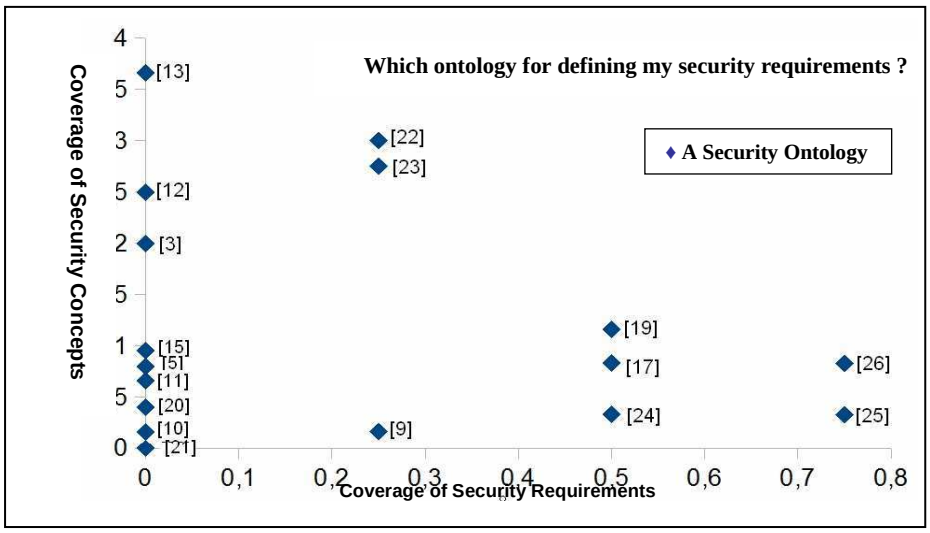

Fig. 2. Using security ontologies for requirement definition.

We summarise this analysis and evaluation in Table 1. The rows are the security ontologies. The columns are the security concepts (criteria of the study: 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 the security ontology covers this specific criterion, and how 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: (-: 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 (x-axis) and how much it covers security concepts (y-axis). The graph in Figure 2 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.

5 Related works

While many security ontologies have been proposed, few surveys have been attempted. The only ones we can cite here are [1], [27], and recently [28] who proposed a survey of general ontologies for information systems encompassing some security ontologies. Blanco et al. [1] contains 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. Our aim was to extend this classification and to update their surveys with recent literature contributions.

6 Conclusion and perspectives

This study has shown the existence of considerable work around security ontologies; We classified the proposed ontologies into eight families. 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 which formed our criteria of the analysis. 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 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. It 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 our research is to explore 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. (ARES). Barcelona, (2008)

[2]. Mouratidis, H; Giorgini, P; Manson, G.: Towards the development of secure information systems: Security Reference Diagram and Security Attack Scenarios. CAiSE, .(2004)

[3]. Ekelhart A., Fenz S., Klemen M., Weippl E.: Security Ontologies: Improving Quantitative Risk Analysis" (HICSS'07), (2007).
[4]. 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).
[5]. Dobson G., Pete S.. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web." Requirements Engineering , (2006).
[6]. Donner, M.: Toward a Security Ontology. IEEE Security and Privacy, (2003).
[7]. Barnes, S. J.: Assessing the value of IS journals. Communications of the ACM, (2005).
[8]. Rainer, R. K., & Miller, M. D.: Examining differences across journal rankings. Communications of the ACM, 48(2), 91-94. (2005).
[9]. Mylopoulos J., Jarke M., Koubarakis M.. Telos – a language for representing knowledge about information systems. ACM Trans. Information Systems 8(4):327-362, (1990).
[10]. Avizienis A., Laprie J.-C., Randell B., and Landwehr C. E.: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Sec. Comput., (2004).
[11]. 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).
[12]. Herzog A., Shahmehri N., and Duma C.: An Ontology of Information Security. International Journal of Information Security 1.4 : 1-23 (2007).
[13]. Fenz S., Ekelhart A.: Formalizing information security knowledge. (ASIACCS '09), pp. 183-194, 2009., (2009).
[14]. Undercoffer J., Joshi A., Pinkston A.: Modeling computer attacks: an ontology for intrusion detection . Lecture Notes in Computer Science, pp. 113–135.2820, (2003).
[15]. Geneiatakis, D. and C. Lambrinoudakis, An ontology description for SIP security flaws. Computer Communications,. In Press, Corrected Proof. (2006).
[16]. Denker, G., Kagal, L., Finin, T., Paolucci, M., and Sycara K.: Security for DAML Web Services: Annotation and Matchmaking. (ISWC2003): Sanibel Island, Florida (2003).
[17]. Denker, G., Nguyen, S., and Ton, A.: OWL-S Semantics of Security Web Services: a
[18]. Denker, G., L. Kagal, and T. Finin.: Security in the Semantic Web using OWL. Information Security Technical Report. 10(1): p. 51-58. , (2005).
[19]. Kim, A., Luo J., and Kang M.: Security Ontology for Annotating Resources. (ODBASE'05). (2005).
[20]. Vorobiev, A. and J. Han, Security Attack Ontology for Web Services. SKG '06. IEEE Computer Society, p. 42. (2006).
[21]. Abou Assali A., Lenne D., Debray B.: Ontology development for industrial risk analysis. (ICTTA 2008), Damascus, Syria (April 2008).
[22]. Tsoumas B., Gritzalis D.: Towards an ontology-based security management. AINA, pp. 985-992, (2006).
[23]. Karyda, M., et al.: An ontology for secure e-government applications (ARES'06). IEEE Computer Society: p. 1033-1037. (2006).
[24]. Donald G. Firesmith. A taxonomy of security-related requirements.(RHAS'05), Paris,05.
[25]. 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).
[26]. Massacci, F., Mylopoulos, J., Paci, F., Tun, Thein and Yu, Yijun.: An extended ontology for security requirements. WEISSE'11, (20-24 June 2011).
Case Study. In 1st European Semantic Web Symposium: Heraklion, Greece.(2004).
[27]. Golnaz Elahi : Security Requirements Engineering: State of the Art and Practice and Challenges , http://www.cs.utoronto.ca/~gelahi/DepthPaper.pdf , (2009).
[28]. Nguyen V., Ontologies and Information Systems: A Literature Survey, http://hdl.handle.net/1947/10144 , (2011)
[29]. Sikora E., Tenbergen B., Pohl K.: Industry needs and research directions in requirements engineering for embedded systems. RE (2012).

Table 1. Summary of security ontologies of the study

Family	Security ontology	Security Objectives[1]	Assets[1]	Vulnerabilities[1]	Threats[1]	Counter-measures[1]	Organisation[1]	**Requirements[2]**
Beginning	Mylopoulos et al. [9]	-	-	-	-	-	●	●
Security Taxonomies	Avizienis et al. [10]	●●●	-	-	●●	●●●●	-	-
	McDermott et al. [11]	-	-	-	●●●●■	-	-	-
General	Herzog et al. [12]	●●	●●●■	●●	●●●■	●●●■	●●	-
	Fenz et al. (a)[13]	●●●●	●●	●●●●	●●●●	●●●●	●●●●	-
Specific	Undercoffer et al. [14]	-	●■	●■	●●■	-	-	-
	Geneiatakis et al. [15]	●●	-	-	●●●■	-	-	-
Risk based	Fenz et al. (b)[3]	●●	-	-	●●●● ■	●●●	●●●	-
Web oriented	Denker et al. [16] [17] [18]	●●●	-	-	-	●●■	-	●●
	Kim et al. [19]	●●●●	-	-	-	●●●■	-	●●
	Han et al. [20]	-	-	-	●●●●■	-	-	-
For security requirements	Dobson et al.[5]	●●	-	-	●●	-	-	-
	Tsoumas et al.[22]	-	●●●	●●●	●●	●●●	●	●
	Karyda et al. [23]	●●	●●●	-	●●●	●	●●	●
	Firesmith [24]	-	●	-	●	-	-	●●●
Modelling	Mouratidis et al.[25]	●	-	-	-	-	●	●●●
	Massacci et al. [26]	●●	●●	-	●	-	-	●●●

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

[2] How does this security ontology deal with requirements (last column)? Does this ontology refer to technical security concepts? ■: Technical