An Overview of Security Ontologies

Helder Gomes[1], André Zúquete[2], Gonçalo Paiva Dias[3]

1) Escola Superior de Tecnologia e Gestão de Águeda – Universidade de Aveiro, Águeda, Portugal

helder.gomes@ua.pt

2) Departamento de Electrónica, Telecomunicações e Informática – Universidade de Aveiro, Aveiro, Portugal

andre.zuquete@ua.pt

1) Escola Superior de Tecnologia e Gestão de Águeda – Universidade de Aveiro, Águeda, Portugal

gpd@ua.pt

Abstract

This paper presents an overview of ontologies in Information Systems Security. Information Systems Security is a broad and dynamic area that clearly benefits from the formalizations of concepts provided by ontologies. After a very short presentation of ontologies and Semantic Web, several works in Security Ontologies targeting different aspects of security engineering are presented together with another study that compares several publicly available security ontologies.

Keywords: Security Ontologies

1. Introduction

Information Systems today spread almost everywhere in our society. Governments, public organizations, private companies (and at the very end, all of us) all critically depend on Information Systems. One consequence of this is that Information Systems security becomes an increasingly important area and must be considered at every stages of Information Systems lifecycle, from conception to maintenance [Mouratidis, et al. 2005].

However, security is a very active field, were too much terminology is vaguely defined [Donner 2003]. This leads to difficulties for security experts to communicate clearly about security incidents, not only with non-expert people but also between experts. A solution for this situation is the development of an ontology for Information Systems security that includes the most important concepts in the field, and the relations among them. Such ontology will greatly help the organization and communication in the field [Donner 2003].

Ontologies in computer science aroused from the field of Artificial Intelligence, and allow us to represent knowledge about a given domain in a structured, formal and machine processable form. For this knowledge to be representative, it must be agreed (shared) by community members. This formalization of shareable concepts delivered by ontologies provide us better communication, reusability and organization of knowledge, as well as a better computational inference [Blanco, et al. 2008].

In 2001, Tim Berners-Lee proposed a new Web concept: a Semantic Web [Berners-Lee, et al. 2001]. "The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation". Information on the Semantic Web is represented in such a way that computers can understand it. It can be used by computers not only for display purposes, as in current Web, but also for interoperability and integration between systems and applications. This brought a renewed interest to ontologies, as they provide a formal framework for supporting explicit machine processable semantics definition, and they enable the derivation of implicit knowledge through automated inference. This emerging semantic Web, with all its revolutionary potential, brings new challenges to computer interactions, both with humans and between computers, and security plays a vital role in its success. Security semantics are used to provide better communication of security concepts and to allow better support to security based decisions.

In this paper, we present an overview of the use of ontologies in Information Systems Security. After this short introduction, ontologies (what are ontologies) are briefly presented in section II and Semantic Web and Semantic Web Services, as huge application field for security ontologies, are presented in Section III. In section IV we present some applications using security ontologies and, finally, in Section V we conclude by making a summary of this paper and pointing some open issues in the use of security ontologies.

2. Ontologies

Ontologies, whose name was borrowed from philosophy, became very popular in computer science and information systems. This popularity comes from its promise of a shared and common understanding of a domain that can be communicated between humans and applications.

An ontology defines the terms used to describe and represent an area of knowledge. It is a conceptual model, yet executable, that contains a description of important concepts in a domain, relations among them, crucial properties of each concept and restrictions on properties. By using knowledge representation techniques, based in first order logical formalisms, this model is interpretable by computers and, therefore, can be used by Information Systems to make better decisions supported in domain knowledge.

To make ontologies available to information systems, various ontology languages have been developed and proposed for standardization. The most popular is OWL[1] – Web Ontology Language, which has been standardized by W3C consortium[2].

3. Semantic Web

The Semantic Web [Berners-Lee, et al. 2001] is the vision of a Web with meaning, in which information is processed both by computers and by humans. This is achieved through the use of computer processable semantically rich metadata for Web resources, describing their meaning, which is expressed in ontologies. This is in opposition with the current Web, were computers are not able to give meaning to data.

In the field of Semantic Web, Semantic Web Services are of particular interest due to the power and flexibility they promise. Semantic Web Services are Web Services that are self-described and amenable to automated discovery, composition and invocation [Cabral, et al. 2004]. They bring the technology from Semantic Web to the area of Web Services.

---

[1] http://www.w3.org/2004/OWL

[2] http://www.w3.org

Web services are well-defined, reusable, software components that perform specific, encapsulated tasks via standardized Web-oriented mechanisms. They can be discovered, invoked, and the composition of several services can be choreographed, using well-defined workflow modeling frameworks. Current Web Services' technology mainly uses open standards (like UDDI[3], XML[4], SOAP[5], etc.) that provide no semantic description about their functionalities. This lack of semantics implies human intervention for tasks like service discovery and composition, which complicates their usage in complex systems.

Semantic Web Services are Web services with formal descriptions of their properties, capabilities, interfaces and effects. These formal descriptions, described using ontological languages, provide semantics to the Web services, and will play an important role in automatic service discovery, composition, invocation and monitoring without human intervention (from [Studer, et al. 2007]):

- When searching for a service providing a specific functionality, ontologies and associated thesauri can provide synonyms of words, the taxonomic structure of service capabilities, relationships between service capabilities, etc.
- When trying to harmonize different data formats for two services which have to exchange messages, ontologies can provide elaborated conceptual data models for message descriptions, which facilitate automated translation.
- When mediating different communication protocols of services to work together, highly expressive Semantic Web languages can provide well-founded means to describe interaction patterns in communication protocols.
- When trying to compose complex business processes from given partial processes implemented by a number of Web Services, automated planning algorithms can be employed, provided the semantics of the input services is formally defined.

Semantic Web Services have the potential to change the way knowledge and business services are consumed and provided on the Web [Cabral, et al. 2004].

The ontological languages currently used are OWL-S[6], WSMO[7], WSDL-S[8] and SWSA/SWSL[9].

4. Security Ontologies

Security ontologies are ontologies applied to the domain of information systems security. In this section, we present some relevant work on security ontologies.

Application Development

One of the stages in a Software Engineering process is Requirements Engineering that aims to produce models to assist in the development of applications. Since an ontology is based in a logical formalism and explicitly models domain knowledge in a machine interpretable way, it

---

[3] http://uddi.org/pubs/uddi_v3.html

[4] http://www.w3.org/XML

[5] http://www.w3.org/TR/soap

[6] http://www.w3.org/Submission/2004/SUBM-OWL-S-20041122

[7] http://www.w3.org/Submission/WSMO

[8] http://www.w3.org/Submission/2005/10

[9] http://www.daml.org/services/swsl

has long been recognized the benefits of their use in the field of Requirements Engineering. This is the reason for numerous works addressing the use of ontologies in the Requirements Engineering field. However, in [Dobson and Sawyer 2006] the specific area of Dependability Requirements Engineering is identified as one on which little effort has been made to define an ontology, even though dependability is a very important area for many systems. Contrary to what occurs in many other domains, a consensus exists in the field of dependability, thanks to the works from IEEE Computer Society Technical Committee on Fault Tolerant Computing and IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance[10]. Based on that works, authors created an ontology compliant with the IFIP Working Group 10.4 taxonomy [Dobson and Sawyer 2006]. This ontology can be used, together with requirements' ontologies and domain ontologies, to form the basis of a dependability requirements engineering process with strong tool support.

Despite the fact that nowadays security is a concern for most applications, for some applications security is of critical importance, not only in terms of functionality, but also in terms of a trust environment with increased security and privacy features required for user confidence, as is the case of e-government applications. In [Karyda, et al. 2006] the issue of accommodating security requirements in the development of secure applications is addressed by the use of a security ontology. That ontology captures and formalizes security knowledge from security experts and aims to support and improve communication between security experts, users and developers. Furthermore, it is intended to facilitate software developers to address security requirements at an early stage in the software development process and to support security related design choices.

Inter-organizational Database Access

Ontologies are also used in preserving privacy of databases belonging to different organizations that must provide access to users from the other organizations. The Privacy Access Control Toolkit (PACTS) was presented in [Mitra, et al. 2006]. It proposes a solution for privacy of an organization database schema, not data privacy, when delivering access to a partner organization. This schema privacy is achieved with Organization Ontologies (one from each organization), which are generated to include the organization database terms and some term synonyms. These ontologies are sent to a mediator system where they are compared to generate an ontology-mapping table. Ontologies act here simply as a way of obfuscating database schemas, since these never leave the owner organization. Additionally, access control can be delivered by using a similar process to create a role-mapping table that maps one organization role hierarchy into the other organization role hierarchy. A more detailed work on this role mapping for the purposes of authentication can be found in [Pan, et al. 2006]. This solution has the drawback that ontology and role hierarchy mappings must always be created between all the organizations that share accesses to their internal databases.

Security Attacks

Another use of security ontologies is in the characterization of security attacks on information systems. Since systems become highly distributed and increasingly complicated, application components have to collaborate to achieve system goals, and have to face new types of attacks, specially distributed attacks which are difficult to identify and mitigate [Vorobiev, et al. 2008]. In this scenario, communication between applications, or between distributed application components, regarding security attacks and countermeasures must be encouraged, because it can improve the detection and resistance to such attacks. Since application components may have different proveniences (developed by different companies), collaboration is at risk if a common

[10] http://www.dependability.org/

basis vocabulary lacks. To fulfill this lack, in [Vorobiev, et al. 2008] is proposed a set of security ontologies which specify information security issues, allowing the sharing of a common understanding of information about attacks and defenses among humans and computers.

Semantic Web Services

Security plays an important role in Semantic Web Services, as in Web Services, since they can operate across the boundaries of independent organizations. Issues related to service protection and security, reliability of results, or validity of source and cost become important. One crucial issue is the dynamic nature of many transactions, where service requesters and service providers interact without any prior direct trust relationship. In these situations, trust relationships must be established on the fly and for a limited purpose and time. To facilitate such establishment of trust, in [Denker, et al. 2003] is proposed the annotation of service descriptions with information relating their security requirements and capabilities. Two security ontologies are proposed: Credential ontology, which summarizes various ways in which authentication using credentials take place, and Security ontology, which summarizes at a very high abstraction level many of the commonly used security-related notations that can be used to describe user, agent or security service policies. This information can then be used during matchmaking processes to ensure that clients and service providers meets each other security requirements.

In further work, [Kagal, et al. 2004] and [Denker, et al. 2005] added security and privacy policies to the above mentioned proposal. They claim that policies should be part of the representation of the Web service, because they provide the specification of who can use a service under which conditions, how information should be provided to the service and how provided information will be used later. Consequently, they propose the extension of OWL-S to include policies and suggest the inclusion of a property for describing the different policies that must be enforced for the correct execution of a service. In their work, they address three kinds of policies: authorization, privacy and confidentiality. An authorization policy is a set of rules that restrict access to a service. Authorization policies constrain the provider to only accept requests for service from certain clients. Privacy policies specify what information can be exchanged, the legitimate uses of that information and the condition under which this exchange is possible. Privacy policies are interpreted as an obligation from its publisher and can then act as a contract. Confidentiality policies describe the cryptographic characteristics of the input and output parameters of a service, e.g., all communication must be encrypted. To describe policies they use Rei[11], a logic-based language for policy specifications based in RDF[12] and RDFS[13]. Associated with a policy language is a policy engine that interprets and reasons over the policies and domain information to make decisions about applicable permissions and prohibitions.

Web service security was further extended in [Ashri, et al. 2004], which investigates security implications that arise due to interactions between service providers and clients that operate from within different domains where different security policies may hold and different security capabilities exist. They propose a Semantic Firewall, a security device that makes use of Semantic Web technology, to reason about where the interacting entities are able to support the required security policies and whether the interactions that take place are those expected given the aims of the interaction. In order to perform such reasoning, the device requires knowledge of what are the security policies of the secured site (site policies), and what are the expected interactions for a given task (user-defined workflow or process policies). The main challenge is describing the appropriate workflows. The semantic Firewall needs to have access to workflows

[11] http://rei.umbc.edu

[12] http://www.w3.org/RDF

[13] http://www.w3.org/TR/rdf-schema

describing the associated parties, the expected series of interactions and the temporal, data and causal dependencies between them. Workflows can also be annotated with security related requirements. The candidate technologies for describing workflows are the Process Model Ontology, defined by OWL-S, and conversational policies [Smith, et al. 1998].

Security ontologies developed by Denker et al and Kagal et al [Denker, et al. 2003, Kagal, et al. 2004], named as DAML security ontology, serves as a basis for the security ontology presented by Kim et al [Kim, et al. 2005]. This work, that comes from the military area, points some problems in the DAML security ontology, namely for not being intuitive to understand, and refines and extends it to include additional security information, namely to represent security devices (military and commercial), firewall or military security policy instances and algorithms supported by a protocol. The reasoning algorithm from [Denker, et al. 2003] is also enhanced to take into account property attributes. This allows supporting cases where both the requirement and the capability point to the same concept, but the concepts are annotated with different properties, e.g., both requestor and provider use SSH (Secure Shell) but one requires SSH with TripleDES encryption and the other SSH with AES encryption, these two should not match.

An Ontology for Information Systems Security domain

The security ontologies presented in all previous sections were defined and used for particular fields or domains of interest. The Security Ontology reclaimed by Donner [Donner 2003] to be used as a global reference to the Information Systems Security discipline is still missing.

An approach to this security ontology was made in [Tsoumas and Gritzalis 2006]. They made an attempt to assist in the security management of today organizations, where security experts deal with a variety of diverse security related information knowledge sources, ranging from security standards, security tools, security policies, management which formulates the organization security objectives, etc. They propose a framework for security knowledge acquisition and management to support the process leading from informal, high-level statements found in policy and risk assessment documents to deployable technical controls. This framework is based in a security ontology that extends the DMTF CIM model[14] with ontological semantics, in order to use it as a container for information systems security related information, based on widely accepted security management standards.

A comparison of security ontologies is made in Blanco et al. [Blanco, et al. 2008] and they conclude that a complete security ontology has not yet been accomplished by the scientific community: most of the work in security ontologies has been focused in specific domains or in the semantic web. They recognize that the goal of a complete ontology for the security field cannot be an isolated task, since it is impossible to formalize all the existing concepts; it can only be achieved with the collaboration of all the security community by joining and improving the developed ontologies for the specific domains. Their main conclusion, after reviewing a set of selected ontologies, is that the analyzed security ontologies are still in early stages of development, therefore not mature enough for being reused and extended to accomplish the complete security ontology goal.

5. Summary

This paper presents an overview of recent work in the field of security ontologies. Security ontologies are an important topic due to the increasing importance of security in Information Systems and the need of a common language for the Information Systems security area. Presented works come from areas like application development, inter-organizational database

[14] Distributed Management Task Force, Inc. (DMTF) Common Information Model (CIM) Standards. http://www.dmtf.org/standards/cim

access, management of security attacks in distributed environments, semantic web services and information systems security management. We also summarized a study that analyses several publicly available security ontologies and concludes that the use of ontologies in Information Systems security is an emerging subject still in its infancy [Blanco, et al. 2008] and still open to new contributions, both with new applications using security ontologies and for the achievement of a Security Ontology to organize the thinking and discussion of concepts in information systems security domain, as reclaimed in [Donner 2003].

6. References

Ashri, R., T. Payne, D. Marvin, M. Surridge, and S. Taylor. "Towards a Semantic Web Security Infrastructure." In *Semantic Web Services 2004 Spring Symposium Series*. Stanford University, Stanford California, 2004.

Berners-Lee, Tim, James Hendler, and Ora Lassila. "The Semantic Web." *Scientific American* (2001).

Blanco, Carlos, J. Lasheras, R. Valencia-Garcia, E. Fernandez-Medina, A. Toval, and M. Piattini. "A Systematic Review and Comparison of Security Ontologies." In *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security - Volume 00*: IEEE Computer Society, 2008.

Cabral, Liliana, John Domingue, Enrico Motta, Terry Payne, and Farshad Hakimpour. "Approaches to Semantic Web Services: An Overview and Comparisons." In *The Semantic Web: Research and Applications*, 225-39, 2004.

Denker, G., L. Kagal, and T. Finin. "Security in the Semantic Web Using Owl." *Information Security Technical Report* 10, no. 1 (2005): 51-58.

Denker, Grit, Lalana Kagal, Tim Finin, Massimo Paolucci, and Katia Sycara. "Security for Daml Web Services: Annotation and Matchmaking." In *The Semanticweb - Iswc 2003*, 335-50, 2003.

Dobson, G., and P. Sawyer. "Revisiting Ontology-Based Requirements Engineering in the Age of the Semantic Web." 2006.

Donner, Marc. "Toward a Security Ontology." *IEEE Security and Privacy* 1, no. 3 (2003): 6-7.

Kagal, Lalana, Massimo Paolucci, Naveen Srinivasan, Grit Denker, Tim Finin, and Katia Sycara. "Authorization and Privacy for Semantic Web Services." *IEEE Intelligent Systems* 19, no. 4 (2004): 50-56.

Karyda, M., T. Balopoulos, L. Gymnopoulos, S. Kokolakis, C. Lambrinoudakis, S. Gritzalis, and S. Dritsas. "An Ontology for Secure E-Government Applications." In *Proceedings of the First International Conference on Availability, Reliability and Security*: IEEE Computer Society, 2006.

Kim, Anya, Jim Luo, and Myong Kang. "Security Ontology for Annotating Resources." In *On the Move to Meaningful Internet Systems 2005: Coopis, Doa, and Odbase*, 1483-99, 2005.

Mitra, Prasenjit, Chi-Chun Pan, Peng Liu, and Vijayalakshmi Atluri. "Privacy-Preserving Semantic Interoperation and Access Control of Heterogeneous Databases." In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. Taipei, Taiwan: ACM, 2006.

Mouratidis, Haralambos, Paolo Giorgini, and Gordon Manson. "When Security Meets Software Engineering: A Case of Modelling Secure Information Systems." *Information Systems* 30, no. 8 (2005): 609-29.

Pan, Chi-Chun, Prasenjit Mitra, and Peng Liu. "Semantic Access Control for Information Interoperation." In *Proceedings of the eleventh ACM symposium on Access control models and technologies*. Lake Tahoe, California, USA: ACM, 2006.

Smith, I. A., P. R. Cohen, J. M. Bradshaw, M. Greaves, and H. Holmback. "Designing Conversation Policies Using Joint Intention Theory." Paper presented at the Multi Agent Systems, 1998. Proceedings. International Conference on 1998.

Studer, Rudi, Stephan Grimm, and Andreas Abecker, eds. *Semantic Web Services, Concepts, Technologies and Applications*: Springer, 2007.

Tsoumas, B., and D. Gritzalis. "Towards an Ontology-Based Security Management." Paper presented at the Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on 2006.

Vorobiev, A., Han Jun, and N. Bekmamedova. "An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems." Paper presented at the Software Engineering, 2008. ASWEC 2008. 19th Australian Conference on 2008.