IGI PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

ITJ3908

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 1, Issue 4
edited by **Hamid R. Nemati © 2007, IGI Global**

An Ontology of Information Security

Almut Herzog, Linköpings Universitet, Sweden

Nahid Shahmehri, Linköpings Universitet, Sweden

Claudiu Duma, Linköpings Universitet, Sweden

ABSTRACT

We present a publicly available, OWL-based ontology of information security which models assets, threats, vulnerabilities, countermeasures and their relations. The ontology can be used as a general vocabulary, roadmap, and extensible dictionary of the domain of information security. With its help, users can agree on a common language and definition of terms and relationships. In addition to browsing for information, the ontology is also useful for reasoning about relationships between its entities, for example, threats and countermeasures. The ontology helps answer questions like: Which countermeasures detect or prevent the violation of integrity of data? Which assets are protected by SSH? Which countermeasures thwart buffer overflow attacks? At the moment, the ontology comprises 88 threat classes, 79 asset classes, 133 countermeasure classes and 34 relations between those classes. We provide the means for extending the ontology, and provide examples of the extendibility with the countermeasure classes 'memory protection' and 'source code analysis'. This article describes the content of the ontology as well as its usages, potential for extension, technical implementation and tools for working with it.

Keywords: *computer science; information systems; is security; ontologies; software*

INTRODUCTION

Agreeing on the meaning of concepts and their relations is useful in all domains because the consequences of a misunderstanding can be time-consuming and costly. In the domain of information security many concepts are vaguely defined, even for security professionals. Is a password "a unique character string held by each user, a copy of which is stored within the system" (Oxford University Press, 2004) or "an example of an authentication mechanism based on what people know" (Bishop, 2003, p. 310)? Such ambiguities could be mitigated by a common repository of domain knowledge for the security domain. In this article, we present such a repository by means of an ontology. An ontology "defines the basic terms and relations comprising the vocabulary of a topic area, as well as the rules for combining terms and relations to define extensions to the vocabulary" (Neches, Fikes, Finin, Gruber, Patil, Senator, & Swartout, 1991).

The need for an ontology of information security has also been clearly verbalised by Donner (2003):

> *What the field needs is an ontology—a set of descriptions of the most important concepts and the relationship among them. ... Maybe we [the community of security professionals] can set the example by building our ontology in a machine-usable form in using XML and developing it collaboratively.*

Previous work, such as Schumacher (2003); Kim, Luo, and Kang (2005); Jutla and Bodorik (2005); Squicciarini, Bertino, Ferrari, and Ray (2006); Nejdl, Olmedilla, Winslett, and Zhang (2005); Undercoffer, Joshi, Finin, and Pinkston (2004); Tsoumas, Dritsas, and Gritzalis (2005); Takahashi, Abiko, Negishi, Itabashi, Kato, Takahashi, and Shiratori (2005), has only partly addressed these needs, and, so far, an ontology of information security that provides general and specific concepts, is machine-usable, and can be developed collaboratively is still missing.

In this article we present an ontology that (1) provides a general overview over the domain of information security, (2) contains detailed domain vocabulary and is thus capable of answering queries about specific, technical security problems and solutions, and (3) supports machine reasoning. As a step towards an ontology that is collaboratively developed and acceptable by the security and ontology community, we have designed our ontology according to established ontology design principles (Gruber, 1995) and best practices (obofoundry.org1) and make our ontology available online. Consequently, users can browse the ontology online. They can extend it either by downloading and modifying it or by importing the ontology from the Web and extending it with new concepts.

Our security ontology builds upon the classic components of risk analysis (Whitman & Mattord, 2005, p. 110ff): assets, threats, vulnerabilities and countermeasures. By modeling these four basic building blocks of information security and their relations, and refining each block with technical concepts, we arrive at an ontology that provides the "big picture" of the domain of information security as well as a classification and definition of specific domain vocabulary.

Our ontology provides natural language definitions for general terms such as 'asset', as well as domain-specific, technical terms, such as 'SSH'. By implementing high-level relations for specific, technical concepts, one can also find answers to questions such as "What and how does SSH protect?". Other examples of questions that our ontology helps answer are: Which threats threaten user authentication? Which countermeasures protect the confidentiality of data? Which vulnerabilities enable a buffer overflow attack? Which countermeasures protect against buffer overflow attacks? Which countermeasures use encryption?

Users may find our ontology useful, (1) as a reference book or hypertext learning material on information security, (2) as a template for classifying and comparing security products, security attacks or security vulnerabilities, (3) as a framework for plugging in new or existing detailed security taxonomies and (4) as a knowledge base for reasoning with semantic Web applications. We have implemented our ontology in OWL (Web Ontology Language) (Bechhofer, van Harmelen, Hendler, Horrocks, McGuinness, Patel-Schneider, & Stein, 2004), a markup language based on RDF/XML (Resource Description Framework/Extensible Markup Language) (Powers, 2003), specifically devised for creating extensible ontologies for the semantic Web. Thus, our ontology uses a commonly accepted notation for describing ontologies and supports querying and acquisition of new knowledge through inference and rule-based reasoning using OWL reasoners and OWL query languages.

The remainder of the article is structured as follows. An overview of our ontology is given in the following section. Then we present refinements of the core concepts. Afterward, we provide examples that demonstrate the power of inference and querying. We also describe useful tools for creating and working with ontologies.