# Information Security Ontology for Dummies

Wan Nor Azura bt. Kamarudin
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
Email: azurawn@yahoo.com
Matrix No: P47925

## Abstract

*The research community realize the need for a standard and formal specification of the domain Information Security in order to ensure a clear understanding amongst the researchers in different areas of the domain Information Security. Thus, the need for Information Security Ontology which has over the years evolved from merely providing domain definitions and classifications to enabling sophisticated decision-making and automation. This paper is a review of some of the work done in developing and supporting the ontology for the domain of Information Security. The review highlights the definitions, concepts, relationships, methodologies, tools, applications and issues related to Information Security Ontology.*

Keywords: Information security, ontology

## 1. Introduction

The most basic concept in Information Security can be stated as safeguarding of information as an asset and its confidentiality, integrity and availability. This concept and more can be specified in detail and their relations shown with the use of an ontology for Information Security. Information Security is an interesting, albeit a vast domain which include the areas of incident handling, risk assessment, cryptography and disaster recovery to name a few. These areas can be detailed further which include terms such as threats, vulnerabilities, attacks, encryption, denial of service, rootkits, virus, malicious code and many more. As is clear with these examples, their existence is acknowledged but without any relationships or classifications between them.

Why develop an ontology for the domain of Information Security? An ontology recognizes and classifies areas and terms as concepts or classes as well as the relationships between them, thus it defines a common vocabulary for researchers to share information in a domain. The detailed description of a concept is known as its properties or slots. Some of the reasons for developing an ontology as stated in [2] are to share common understanding of the structure of information among people, to enable reuse of domain knowledge, to make domain assumptions explicit, to separate domain knowledge from operational knowledge and to analyse domain knowledge. With the use of reasoning tools and an ontology, inferences can be made to automatically discover knowledge or solutions to support decision-making and problem-solving tasks. The Web Ontology Language (OWL) is available for developing the ontology and there are also tools available for reasoning and querying. Interestingly, ontology also has its application in e-learning [3, 7], which is related to the author's current work, Learning Content Management System (LCMS) for Information Security.

This paper is organised as follows. The first section covers the definitions of ontology from previous works, what ontology is made up of and why it is needed in the domain of Information Security. Section two is about the methodologies used in previous works in developing an Information Security Ontology. The tools used in previous works are the focus of section three, be it tools for developing, querying or reasoning an Information Security Ontology. Section four goes further in covering the applications of ontology related to the domain of Information Security. Lastly and as a conclusion, benefits and issues related to Information Security Ontology are covered in this paper.

wna
October 11, 2009

### 1.1. What is an ontology?

An ontology can be defined as an explicit ”specification of a conceptualization”, or in other words, it is explicit formal specifications of the terms in the domain and relations among them [12]. In [10] ontology is described as a highly structured system of concepts covering the processes, objects and attributes of a domain in all their pertinent complex relations. Furthermore in [3], ontology is also described as a combination of concepts, definitions and attributes organized in taxonomies [1] and extended with axioms and rules for reasoning. Ontologies can be categorized into several types

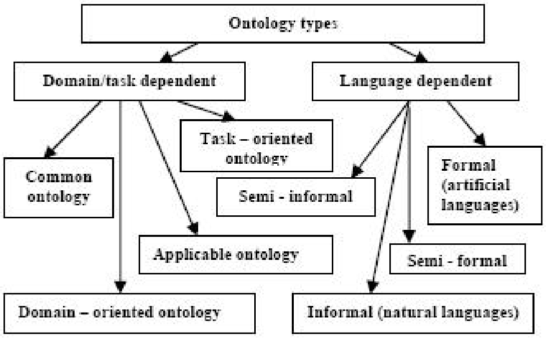


Figure 1. Types of Ontologies

as illustrated in [3] and shown in Figure 1. Nevertheless, the ultimate goal is in the way the ontology is applied to other uses in a domain, not the ontology itself [2]. For example, ontology can be applied as an enabler of automated risk assessment in the domain of Information Security.

## 1.2. The architecture of an ontology

An ontology comprises of three major building blocks namely concepts (classes), relationships and constraints (axioms). A concept is described in detail by its properties. A concept can have sub-concepts. A concept can be linked to other concepts with ”is-a” or ”has-a” relationship. Properties (attributes) provide more information about a concept. They describe the internal structure and terms of a concept. Constraints are rules that model all the possible and meaningful interpretations of the concept [2, 5]. An ontology can have ontology views, as emphasised in [4] or sub-ontologies from different perspectives depending on the needs of the ontology user. Another important feature of an ontology is inheritance. Inheritance is the down-propagation of properties, with their values filled, from parents to children and further descendants [10].

The architecture of an ontology involves sub-ontologies. Logically, over time an ontology will grow larger with usage. Therefore, a need exists to extract a portion of the larger ontology in order to cater to the specific requirements of a user for a given task [4]. Additionally, the use of these localized sub-ontologies are able to minimize processing time involved in executing semantic queries over larger-scale ontologies. Sub-ontologies are also known as ontology views, as in [4].

## 1.3. Ontology for Information Security

Ontologies are significant in the domain of Information Security due to their role in enabling a modular approach and predicting new phenomena [10]. Ontologies represent knowledge in a standardized and formal form to enable its utilization by automated systems [6]. For example, being able to predict the types of attacks is vital in computer security incident handling. ”A common language for computer security incident information” was found to be a necessity to structure the incident reports in order to enhance rapid responses [10]. Figure 2 shows the security relationships [6] in an Information Security Ontology.

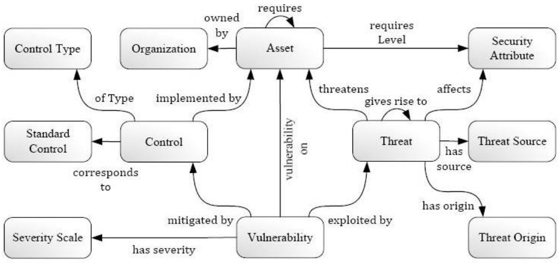


Figure 2. Security relationships

The use of ontologies can find its way in other areas of Information Security such as the four high-level security issues which were identified in [11]: access to Information Systems, secure communication, security management and development of secure Information Systems. The need for ontologies in the domain of Information Security is further emphasised in [13]: ”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. ... Maybe we can set the example by building our ontology in a machine-usable form in using XML and developing it collaboratively.”

## 1.4. Methodologies for Developing Ontologies in the Domain of Information Security

Basic approaches for developing ontologies are top-down, bottom-up and combination [2, 3, 7,]. There is no ”correct” or standard method for developing ontologies [2, 7]. However, the rule-of-thumb approach can be used as a fundamental guide in the methodology for developing ontologies. [2] also stated that ontology development is an iterative process and concepts in the ontology should be close to objects and relationships in the domain of interest. [3] made comparisons and analysed the existing methodologies used and proposed a new methodology for creating an ontology in the domain of e-learning. As for the domain of Information Security, [5] duly illustrated the possible sources of Information Security knowledge and their relevance in populating the Information Security Ontology, as shown in Figure 3. Some of the methodologies

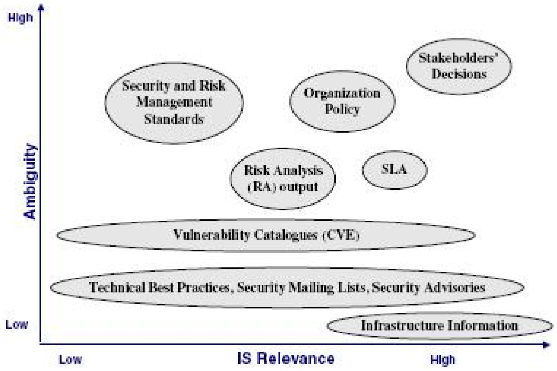


Figure 3. A Classification of Information Security knowledge sources

used in previous works to develop Information Security Ontologies are as follows.

In [5], the collaborative approach is used in the methodology for developing a Security Ontology. The idea used in this methodology is to build an ontology by a group of people in an iterative way, improving the ontology in every iteration. In [7], the ontology was constructed using the Description Logic (DL) knowledge engineering methodology as well as the ontology design criteria as proposed in [12]. The criteria proposed by [12] are clarity, coherence, extendibility, minimal encoding bias and minimal ontological commitment. [6] cited the ontology design criteria by [12] and stated the use of best-practice guidelines and information security standards in developing their ontology. The same ontology design criteria by [12] is also used by [9] together with the application of best practices. It is interesting to note that [9] goes a step further in contributing to the development of Information Security Ontologies by making their ontology publicly available online, downloadable and extendible.

## 1.5. Tools for Information Security Ontology

There are many tools available for developing the ontology. Tools that have been used or proposed in previous works related to the development of Information Security Ontologies are covered next. The author has categorised the tools into three groups in this paper according to their functions for the sake of clarity.

**1.5.1. Developing and Editing the Ontology.** An OWL-based ontology was developed in [9] which uses a commonly accepted notation for describing ontologies and supports querying and acquisition of new knowledge through inference and rule-based reasoning. OWL which stands for Web Ontology Language is specifically devised for creating standard and extensible ontologies for the semantic Web. [2] described their experience in using Protege 2000, Ontolingua and Chimaera to edit their ontology. [5] proposed the use of Protege to populate the instances of the concepts in an ontology from the data collected. [9] used Protege and Swoop editors for their ontology. As stated in [9], Swoop is useful for finding the sources of inconsistencies in a knowledge-base.

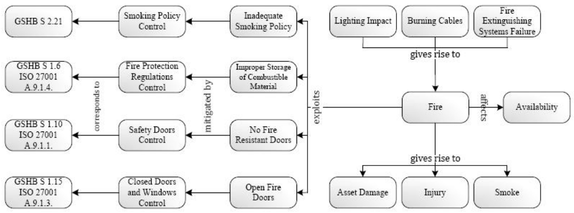

GSHB S 2.21
Smoking Policy Control
Inadequate Smoking Policy
Lighting Impact
Burning Cables
Fire Extinguishing Systems Failure
gives rise to
GSHB S 1.6 ISO 27001 A.9.1.4.
Fire Protection Regulations Control
Improper Storage of Combustible Material
corresponds to
mitigated by
exploits
Fire
affects
Availability
GSHB S 1.10 ISO 27001 A.9.1.1.
Safety Doors Control
No Fire Resistant Doors
gives rise to
GSHB S 1.15 ISO 27001 A.9.1.3.
Closed Doors and Windows Control
Open Fire Doors
Asset Damage
Injury
Smoke

Figure 4. Fire threat

**1.5.2. Querying the Ontology.** In [6], the SPARQL query language was used together with OWL API. [9] also used SPARQL to query and retrieve data from the ontology that they have developed. Additionally, [9] stated the advantages of using SPARQL in that it supports postprocessing, yes/no questions, sorting, filtering and string-matching.

**1.5.3. Reasoning the Ontology.** Reasoners are used to make inferences against the ontology. The Pellet reasoner is used by [6] and [9] for their ontologies. As described in [6], the reasoner is used together with an editor to extract corresponding concepts and to explicitly classify them. Other reasoners as stated by [9] are FaCT and Racer.

## 1.6. Applications of Information Security Ontology

As mentioned previously, Information Security Ontology has many uses in its domain. Noticeably, ontology is synonym with the use of knowledge base and semantic web [4, 6] thus this makes it more significant for ontology to be applied in the domain of Information Security.

A few examples of the applications of Information Security Ontology are as follows. In [5], the Security Ontology is used together with a database of technical controls to provide customised and focused solutions in a technical level which addresses the given security requirements of a system. [5] also refers to the conceptual information model known as the Common Information Model (CIM) in their work as the model can be mapped to structured specifications such as OWL. Information Security knowledge in the area of risk management is formalized in [6] through the use of an Information Security Ontology. As stated in [6], the ontology has been found to support

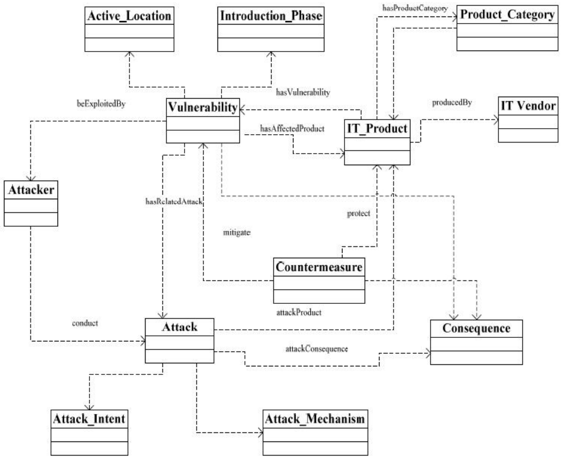
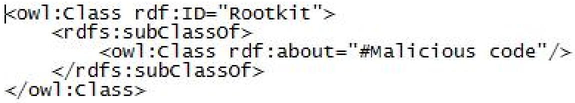


Figure 5. The conceptual model of the vulnerability ontology



```
<owl:Class rdf:ID="Rootkit">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Malicious code"/>
    </rdfs:subClassOf>
</owl:Class>
```

Figure 6. Example of the OWL code for Rootkit

a broad area of information security risk assessment. Figure 4 conceptually shows an example of the ontology from [6] applied in the risk management of a fire threat. In [8], the Information Security Ontology is applied in vulnerability analysis and management. The ontology in [8] represents knowledge for vulnerability classifications and vulnerability metrics and in a formal and structured form. As stated in [8], the ontology also enables the building of automated tools for system security. Figure 5 illustrates the vulnerability ontology in [8]. [9] comprehensively discussed the applications of their Information Security Ontology which can be used as online learning content, as a knowledge base for rule-based reasoning with semantic web applications, as a framework for further extensions and lastly as a framework to compare security products, attacks and vulnerabilities.

To further illustrate the use of an ontology for the domain of Information Security, Figure 6 as shown above is an example in the Appendix of the OWL code for the term or class known as ”Rootkit” which is a form of or a sub-class of ”Malicious code”.

## 1.7. Significance of Information Security Ontology

Why is Information Security Ontology important? As illustrated in Figure 7, ontology is closely related to technologies such as Extensible Markup Language (XML), Semantic Web and Metadata. XML is markup language

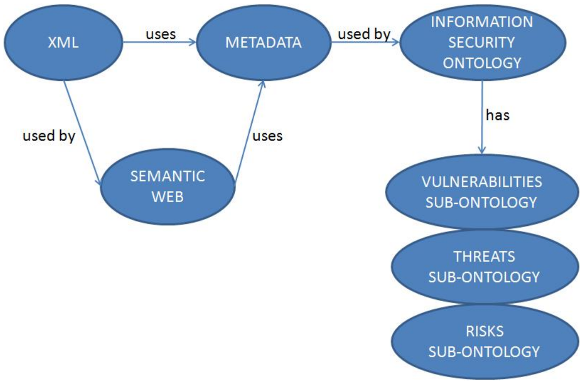


Figure 7. Information Security Ontology and related technologies

with semantics which is used to add more meaning to data. Semantic Web uses XML to create better and intelligent search engines. Metadata is meaningful data that is used to describe data, as used in ontologies. Figure 6 also shows the relationship between the Information Security Ontology and its sub-ontologies such as the vulnerabilities sub-ontology, threats sub-ontology and risks ontology. These sub-ontologies have specific uses in the area of incident handling, disaster recovery and risk assessment. Thus, Information Security Ontology in relation to the related technologies, has significant contribution to the domain of Information Security in the aspects of meaning, understanding and learning of the terms, concepts, principles and practices of Information Security.

What does an ontology have to offer that XML have not already offered? First and foremost, an ontology is different from an XML schema in that it is a knowledge representation, not a message format. The specification offered by an XML schema is not designed to support reasoning outside the specified context. Secondly, the advantage of using an ontology is that there are many tools available to reason the ontology. These tools provide generic support that is not specific to a particular subject domain, as opposed to building an XML-based system to reason a specific industry.

## 1.8. Issues in Information Security Ontology

As described earlier in the examples, some of the issues and challenges that can be highlighted here in Information Security Ontology include the availability, standardization and scalability of the ontologies that are developed for the domain. For example, Information Security Ontology that is made available, extractable and downloadable from the internet would enable the domain community to make optimal use of the ontology in their applications. Different ontologies or sub-ontologies in the domain may have different meanings of the same terms used, therefore the domain community have to collaborate on this issue to ensure a degree of uniformity in ontologies. The issue of scalability involves managing the versions of Information Security Ontologies that are developed and enabling the extension of an ontology through plug-ins from taxonomies and sub-ontologies.

## 2. Conclusion

The use of ontology in the domain of Information Security provides a standard and structured form to define and classify the terms, concepts and relationships between them in the domain. Information Security Ontology has many uses such as in the area of incident handling, risk assessment, disaster recovery and vulnerability management. Previous works on Information Security Ontology resulted in the development of improved and practical ontologies. However, more research is needed as the domain of Information Security is vast therefore there is always room for improvement and refinement of the ontologies. For example, as related with the current work of the author, there exists an opportunity for an ontological view of the domain of Information Security which can be applied in the form of a refined learning content on Information Security.

## Acknowledgment

This review paper is submitted as partial requirement for the TS6234 course under the Masters of Information Technology (Management Information System) at the National University of Malaysia.

## References

[1] Savola, R.M., *Towards a Taxonomy for Information Security Metrics*, pp. 28–30. Proceedings of the 2007 ACM workshop on Quality of protection, ACM New York, NY, USA, 2007.

[2] Noy, N.F. and McGuinness, D.L., *Ontology Development 101: A Guide to Creating Your First Ontology*, pp. 01–05. Knowledge Systems Laboratory, 2001.

[3] Todorova, K., *Towards A Methodology For Ontology Development*, pp. 205. Innovations in E-Learning, Instruction Technology, Assessment and Engineering Education, Springer, 2007.

[4] Rajugan, R. and Chang, E. and Dillon, T.S., *Ontology Views: A Theoretical Perspective*, pp. 1814. Lecture Notes in Computer Science, Springer, 2006.

[5] Tsoumas, B. and Dritsas, S. and Gritzalis, D., *An Ontology-Based Approach to Information Systems Security Management*, pp. 151. Lecture Notes in Computer Science, Springer, 2005.

[6] Fenz, S. and Ekelhart, A., *Formalizing Information Security Knowledge*, pp. 183–194. Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ACM New York, NY, USA, 2009.

[7] Abel, M.H. and Benayache, A. and Lenne, D. and Moulin, C. and Barry, C. and Chaput, B., *Ontology-based Organizational Memory for e-learning*, pp. 98–111. Educational Technology & Society, 2004.

[8] Wang, J.A. and Guo, M., *OVM: An Ontology for Vulnerability Management*.

[9] Herzog, A. and Shahmehri, N. and Duma, C., *An Ontology of Information Security*, pp. 278. Techniques and Applications for Advanced Information Privacy and Security: Emerging Organizational, Ethical, and Human Issues, Information Science Reference, 2009.

[10] Raskin, V. and Hempelmann, C.F. and Triezenberg, K.E. and Nirenburg, S., *Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool*, pp. 53–59. Proceedings of the 2001 workshop on New security paradigms, ACM New York, NY, USA, 2001.

[11] Siponen, M.T. and Oinas-Kukkonen, H., *A Review of Information Security Issues and Respective Research Contributions*, pp. 60–80. ACM SIGMIS Database, ACM New York, NY, USA, 2007.

[12] Gruber, T.R., *Toward Principles for the Design of Ontologies Used for Knowledge Sharing*, pp. 907–928. International Journal of Human Computer Studies, 1995.

[13] Donner, M., *Toward a Security Ontology*, pp. 6–7. IEEE Security and Privacy Magazine, 2003.

[14] *Security Attacks and Intrusion Detection*, University of York, 2005. http://www-users.cs.york.ac.uk/~aservin/docs/attacks_ids.pdf

[15] *Glossary of Terms Used in Security and Intrusion Detection*, The SANS Institute. http://www.sans.org/security-resources/glossary.php

[16] *Security Management Definitions*, Praxiom Research Group Limited. http://www.praxiom.com/iso-27001-definitions.htm

[17] *Definition of Disaster Recovery*, About.com. http://operationstech.about.com/od/glossary/g/GlsDisastRecovy.htm

## Appendix

### Glossary

**Attack**
An attack is the exploit of vulnerabilities on a system by a human or program.

**Cryptography**
Cryptographic transformation of data (called ”plaintext”) into a form (called ”cipher text”) that conceals the data’s original meaning to prevent it from being known or used.

**Denial of service**
The prevention of authorized access to a system resource or the delaying of system operations and functions.

**Disaster recovery**
Disaster recovery is the process in which a business or organization implements a disaster recovery plan that allows it to continue to function after a catastrophic event.

**Encryption**
Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.

**Incident Handling**
Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

**Information security**
Information security is all about protecting and preserving information. It is all about protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.

**Malicious code**
Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

**Risk assessment**
A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

**Rootkit**
A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

**Threat**
A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system.

**Virus**
A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

**Vulnerability**
A vulnerability is a weakness in an asset or group of assets. An assets weakness could allow it to be exploited and harmed by one or more threats.