TOMASZ BOIŃSKI, PIOTR ORŁOWSKI, HENRYK KRAWCZYK
Faculty of Electronics, Telecommunications and Informatics,
Gdańsk University of Technology

EXTENDABLE SAFETY AND SECURITY ONTOLOGY

SUMMARY

Security plays an increasingly important role in our everyday life, and researchers and users of computer systems point out that the need arises for a common, formalised model capable of integrating different solutions. In this paper we show that an ontology can be designed and created in a way that will make it suitable for interoperability and integration. A security and safety ontology and the methodology for creating a common model allowing future expandability and reuse are considered. Such interoperable ontologies can be easily integrated with current and future solutions and provide principles for increasing system interoperability.

Keywords: Security Ontology, ontology development

1. Introduction

Security plays an increasingly important role in our everyday life. Researchers and organisations point out that any misunderstandings within the field of security and safety can lead to serious expenses and their amendment can be time consuming. Unfortunately many terms from this domain have ambiguous and unclear definitions. Because of that Donner, in 2003 [6] and later in 2006 ENISA (the European Network and information Security Agency) [7], called for the creation of common safety and security ontology for the need of describing resources available in the World Wide Web.

This paper is a response to that appeal. It describes proposed safety and security ontology that covers the domain of computer security as described in taxonomies created by different parties, thus allowing the capture of different approaches to security and safety.

The ontology was also created for the purpose of testing and extending the OCS[1] system and lexical algorithm for the merging and alignment of ontologies [3].

The ontology was constructed with interoperability and extendibility in mind, so future adaptations and integration with other ontologies should be possible. To ease future works on the ontology, the paper presents both the ontology itself and the methodology used during ontology creation.

2. The Methodology

Ontology construction was divided into four steps:

1. Creation of Ontology Requirement Specification Document (Section 3),
2. Establishing a set of core concepts (Section 4),
3. Specification of ontology modules (Section 5),
4. Ontology implementation and integration (Section 6).

The ontology was meant to be implemented as three separate modules, which in the final stage would be merged into one monolithic ontology. Each intermediate as well as the final ontology were implemented in an iterative manner.

The Risk Core Concepts module [4] was created by integration of three small ontologies com-

1 http://ocs.kask.eti.pg.gda.pl

posed of less than 100 classes each. During creation of those ontologies the set of core concepts was also established. Then those three ontologies were combined into a single OWL ontology. Two other modules (Basic Security Concepts module and Safety and Security Requirements module) were created from single, average-sized ontologies (based on Avižienis taxonomy [2] and Firesmith taxonomy [10, 11], respectively).

The procedure for developing each of the ontologies was based on methodology provided by Noy and McGuiness [21]. That methodology was also based on the elements of NeOn [27] and UPON [5] methodologies and extended with regards to teamwork [3] and better core concepts selection procedures [3].

The methodology consists of the following steps [4]:

- Lexicon creation – in this step selection of concepts from chosen knowledge sources have been made (both glossaries and taxonomies), concept selection – each subject included into the lexicon automatically becomes a member of a concept set. This set is further expanded by proper names and significant nouns from the definition of previously selected concepts. Each concept in the final set is then converted into an OWL class. Wherever possible, those classes were annotated with their description taken from the glossary or taxonomy,
- Concept hierarchy creation – each occurrence in the glossary or taxonomy of statements similar to "expression A is of type B" was converted into the OWL subclassOf relation. All inheritance relations defined within Avizenis and Firesmith taxonomies were directly converted into this relation,
- Selection of disjointed concepts and synonyms – classes which names are clearly disjointed, such as AccidentalBreakdown and NonAccidentalBreakdown were connected by the disjointWith relation. In other cases, wherever possible, disjointedness was added manually based on human judgment. The same procedure was applied in the case of synonyms,
- Relations identification and selection – verbs were selected from concept definitions as the basis for relations between ontology elements. If a verb connects any two selected concepts then it is transformed into a relation between those concepts. In case of taxonomies, aggregation was converted into has part relation,
- Creation of relationship hierarchy – relationships were grouped based on the similarity of verbs in their names,
- Refining of the relations – the ontology was supplemented by domains and counter domains of all relations added to it earlier. Wherever possible, relations were marked as (non)functional, (non)transitive etc.,
- Ontology integration – the intermediate ontologies were combined into a single one creating either the Risk Core Concepts module or final Security and Safety Ontology.

3. Ontology Requirement Specification Document

The Ontology Requirement Specification Document [4] was based on a template proposed for the NeOn project [26]. It was extended by elements from [5] and the second edition of the Handbook on Ontologies [28]. Its refined and updated content is briefly described in the following sections.

3.1. The reason for creating the ontology

The goal of the ontology is the creation of a common, unambiguous, widely available semantic model of terms from the security and safety domain. Such ontology should provide the means for

MOST WIEDZY Downloaded from mostwiedzy.pl

easy extension and usability in research projects.

3.2. Boundaries of the ontology

To be extendable and usable in different projects the ontology should contain subjects from the areas of general meaning of security and safety and domains closely related with security but in limited scope.

It was decided that the final ontology should contain:

- basic and general concepts in the domain of security,
- terminology from the domain of information safety and security,
- the most important concepts from other fields of security to allow integration with other solutions:
    - road traffic,
    - national and international,
    - energetic.

The main scope of the ontology will be general security and safety terminology as well as detailed terminology describing the security and reliability of computer systems. Information security is close to other fields of security and is generally understood by people from the field of computer science. Concepts from other fields mentioned earlier will be provided to allow easy integration and extension of the ontology.

As mentioned in the introduction to this paper, the ontology is based on sources from different parties related to computer security. The following knowledge bases were selected as fundamentals for the ontology:

- NIST Glossary [12],
- ENISA risk management glossary [8],
- Ian Sommerville's book "Software Engineering" [25].

Such selection of knowledge sources incorporates points of view on the safety and security represented by the institutions from the U.S. and EU and by software engineers.

It was also decided to extend the ontology with knowledge contained within by the following taxonomies:

- IEEE computer security taxonomy [2],
- Firesmith security requirements taxonomy [10, 11].

The aforementioned taxonomies are well formalised and established in the community. The creation of ontologies based on them was necessary as unfortunately there are no publicly available ones based on those sources.

3.3. End Users

The ontology is intended to be used by:

1. Groups of people interested in topics regarding safety and security or the ontology itself, both in the fields of research and commercial applications,
2. Software engineers needing formalised structures for describing semantic annotations in their software,
3. Developers of agent systems, Internet services, search engines etc. for knowledge exchange and communication.

3.4. Intended usage

The intended usages of the ontology include, but are not limited to:

1. Applications created with ubiquitous programming in mind,
2. Search engines and agent systems,
3. Applications aimed to be components of the Semantic Web,
4. Creation of teaching materials regarding topics from the domain of safety and security,

MOST WIEDZY Downloaded from mostwiedzy.pl

5. Research and development, including testing and extending of the OCS system.

To be usable in general the created ontology should be general purpose ontology so that its adaptation is easier than a specific ontology, and thus it should be usable in external applications.

3.5. Nonfunctional requirements

The expected nonfunctional requirements are:

1. Both the Polish and English languages should be supported.
2. Concept and properties definitions should come from renowned sources or standards.
3. Knowledge sources should be clearly provided allowing for the verification and adaptation of the ontology by external parties.
4. Concepts and properties should be described in human and machine readable form to allow them to be both easy to understand by the ontology users and able to be processed by machines.
5. The ontology should be consistent, thus allowing reasoning.
6. The ontology should be portable and therefore usable in mobile applications such as agent systems.
7. The ontology should work with OCS system.
8. Classification operation should be doable in finite time.

3.6. Functional requirements

Functional requirements, as suggested by [26], were presented in the form of competency questions (Table 1).

Table 1. ***Functional requirements.***

Question	**Expected answer**
What is a risk?	Probability of a loss.
What type of attacks can be performed against computer systems?	DoS, unauthorised access
What is internal safety?	State of internal threats.
What are attributes of external security?	Accessibility, integrity, confidentiality.
What is an attack?	Violent usage of force against someone.

3.7. Implementation language and ontology portability

This model should be widely available and easily usable by the community; thus, it should be created using common and well-understood language. OWL was selected as such a language due to its wide usage in tools like Protégé [18] or OCS [3]. Recently OWL was introduced in its 2.0 version; however, due to popularity reasons it was decided that it would be used to support the DL dialect of OWL 1.1. For file representation, rdf/owl was selected as it will ensure its portability. Furthermore, based on Web Ontology Working Group recommendations [30], it was decided that individuals will not be used in the ontology and all concepts will be represented as classes.

3.8. Ontology architecture

Following recommendations from Ontology Design Patterns [22] it was decided that the ontology should be divided into modules. Three modules are planned: the Risk Core Concepts module, Basic Security Concepts module and Safety and Security Requirements module (Fig. 1).

MOST WIEDZY Downloaded from mostwiedzy.pl

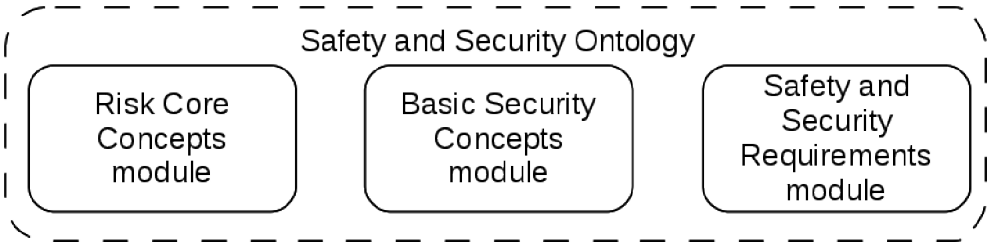

Figure 1. *Safety and Security ontology modules*

3.9. Language, localisation and naming convention

The basic language of the ontology is English. The nonfunctional requirement stating that the ontology should be available both in English and Polish can be easily accommodated by adding additional annotations and labels combined with proper country code (”pl” for Polish). Switching between languages is done by the solution utilising the ontology and has no influence on its construction or behaviour of the reasoner.

Schober’s naming convention [23] was applied to the ontology. It advocates the usage of context free and human readable names and discourages usage of names in the form of negations. Additionally it was decided to use camel case for multi-word labels with names of classes starting with uppercase (e.g. SampleClassName) and names of properties starting with lowercase (e.g. samplePropertyName).

3.10. Evaluation and verification of the ontology

Consistency, completeness and adaptability of the created ontology were checked using Protégé Ontology Tests, included in version 3.4.4 of Protégé editor [19]. Tests were performed both for intermediate ontologies and for the final ontology and were based on questions defined in Table 1. Results of the test were compared with the expected ones. Completeness tests were performed manually by domain experts as there are currently no means of automatic coverage checks [20, 29].

4. Defining the Set of Core Concepts

Establishing the set of core concepts is crucial for future ontology integration [3, 4]. To guarantee compatibility with existing ontologies and taxonomies and not to introduce heterogeneity for future solutions, analysis of existing sources was conducted. Three groups of solutions were analyzed:

- Norms and standards defining security and safety - ISO 13335-1 norm and IAEA lexicon,
- Existing ontologies - Fenz Herzog ontologies,
- Literature regarding security and safety from different points of view.

4.1. Norms and standards

4.1.1. ISO 13335-1 Norm

ISO 13335-1 norm [15], also in Poland known as Polish Norm PN-I-13335-1, defines risk management in ICT security. Basing concepts this norm defines are: *risk*, *asset*, *loss*, *vulnerability*, *threat*, *safeguard* and *security requirement*. It also defines relations between those concepts.

4.1.2. IAEA Glossary

IAEA (International Atomic Energy Agency) has created a glossary [14] that binds security and safety directly with: *safeguard*, *risk*, *threat*, and *protective measures*.

4.2. Existing Ontologies

4.2.1. Fernz Ontology

Fenz created an expanded ontology [9] based on the following core concepts: *control*, *control type*, *standard control*, *organization asset*, *organization*, *security attribute*, *threat*, *threat source*,

MOST WIEDZY Downloaded from mostwiedzy.pl

vulnerability and *threat origin*. Those concepts were gathered based on extensive analysis of literature, including "An introduction to computer security: the NIST handbook" by Guttman and Roback [12]. Furthermore, the risk management model is very similar to that represented by the ISO 13335-1 norm.

4.2.2. Herzog Ontology

Herzog ontology [13] was based primarily on Schumacher's book entitled "Security engineering with patterns: origins, theoretical model, and new applications" [24] and Kim's ontology [17]. As a core, the following concepts were selected: *organization asset*, *protective measure*, *defense strategy*, *security goal*, *threat* and *vulnerability*.

4.3. Literature

4.3.1. Security engineering

Anderson describing security [1] concentrates on its targets and attributes: *confidentiality*, *integrity* and *availability*. For describing security itself the following concepts were used: *system*, *subject*, *participant*, *identity*, *trusted*, *reliable*, *privacy*, *secrecy*, *anonymity*, *authenticity*, *vulnerability*, *threat*, *security breach*, *security*, and *security profile*.

4.1.2. Software engineering

Sommerville [25] connects internal safety with: *incident*, *threat*, *harm*, *level of threat*, *probability of risk* and *risk*. External security is connected with: *exposure*, *vulnerability*, *threat* and *surveillance*. Additionally, according to the author, security is connected with *reliability*, *availability* and *credibility*.

4.4. Selection of Core Concepts

Table 2 presents the combination of occurrences of selected concepts in analyzed sources. Only concepts occurring in two or more sources were presented. Whenever possible, the concepts were generalized. As a result, words such as *availability*, *reliability*, *confidentiality* and *integrity* were treated as security attributes rather than basic concepts; *system* and *participant* are treated as *assets* and *supervision* as a form of *safeguard*.

Table 2. ***Concepts occurrence in different publications***

Concept	ISO	IAEA	Fenz	Herzog	Anderson	Sommerville
Security attributes			X	X	X	X
Vulnerability	X		X	X		X
Risk	X	X				
Loss	X					X
Security measure (safeguard, supervision)	X	X	X	X		X
Threat	X	X		X		X
Object of protection (asset, property)	X		X	X	X	

Based on the aforementioned analysis the following concepts were selected as core concepts for created ontologies: *attack*, *threat*, *protection*, *security*, *safety*, *safeguard*, *risk*, *asset*, *harm*, *vulnerability*, *threat*, *security feature*, *availability*, *integrity*, and *confidentiality*.

During construction of actual ontologies definitions of those concepts were taken directly from the appropriate knowledge source on which given ontology is based.

5. Construction of ontology's base model

MOST WIEDZY Downloaded from mostwiedzy.pl

The base model was constructed upon previously selected core concepts. Usage of OWL DL requires the use of *SHOIN* logic for ontology modeling. This section presents base concepts that are described using this model.

Security: Earlier in this paper security was described as state where there are no threats. It can be expressed using Expression 1:

$$\texttt{Security} \equiv \texttt{State} \sqcap \neg\exists \texttt{occurrs.Threat} \tag{1}$$

Furthermore, security can be divided into internal and external security. The boundary between those two types is not clear, so no new relationships will be introduced (Expression 2).

$$\begin{aligned} \texttt{InternalSecurity} &\sqsubseteq \texttt{Security} \\ \texttt{ExternalSecurity} &\sqsubseteq \texttt{Security} \end{aligned} \tag{2}$$

Security attributes: Security has a given set of attributes (Expression 3).

$$\texttt{hasAttribute}(\texttt{SecurityAttribute}) \sqsubseteq \texttt{Security} \tag{3}$$

The set of attributes depends on the domain of the model. ISO 13335-1 norm defines: confidentiality, authenticity, availability, integrity, accountability and reliability (Expression 4).

$$\begin{aligned} \texttt{InformationSecurityAttributeISO13335} \equiv \{&\texttt{Confidentiality},\\ &\texttt{Authenticity, Availability, Integrity, Accountability,}\\ &\texttt{Reliability}\} \sqsubseteq \texttt{AtrybutBezpieczeństwa} \end{aligned} \tag{4}$$

Vulnerability WordNet dictionary combines vulnerability directly with exposure by stating "the state of being vulnerable or exposed" (Expression 5).

$$\texttt{Exposure} \equiv \texttt{State} \sqcap \exists \texttt{exists.Vulnerability} \tag{5}$$

Vulnerability also exists when a subject has no protection against harm or threat (Expression 6).

$$\begin{aligned} \texttt{Vulnerability} \equiv &\neg\exists \texttt{existsResistance.Harm}\\ &\sqcup \neg\exists \texttt{existsResistance.Threat} \end{aligned} \tag{6}$$

Security policy: The meaning of security policy can be different depending on the context. In the target domain of the constructed ontology, organization security policy and information security policy can be distinguished. ISO 13335-1 defines security policy as "a set of general rules and basic requirements defining how material and intellectual assets of an organization should be managed, shared and protected from unauthorized use, destruction or modification" [15] (Expression 7).

MOST WIEDZY Downloaded from mostwiedzy.pl

$$\begin{aligned}\texttt{contains}(&\texttt{SetOfSecurityPolicyRules}\\ &\sqcup \texttt{SetOfSecurityPolicyRequirements})\\ &\sqsubseteq \texttt{SecurityPolicy}\end{aligned} \tag{7}$$

Risk: Risk is defined in many different ways which makes its meaning vague. In such case it is recommended to choose the most commonly used definitions and model them as inseparable subclasses of the defined concept. Following this rule, we define information risk as a type of risk (Expression 8).

$$\texttt{InformationRisk} \sqsubseteq \texttt{Risk} \tag{8}$$

ISO 13335-1 also defines risk as a probability of a loss (Expression 9).

$$\texttt{isProbabilityOfOccurance.Loss} \sqsubseteq \texttt{Risk} \tag{9}$$

Harm: WordNet defines harm as a material loss, moral loss or injury (Expression 10).

$$\texttt{Harm} \equiv \texttt{MaterialLoss} \sqcup \texttt{MoralLoss} \sqcup \texttt{Injury} \tag{10}$$

Safeguard: In conjunction with security, the literature often mentions concepts of safeguard, protective measures and supervision [14]. In WordNet "safeguard is something that protects". It is also a "a protective measure against threat" (Expression 11).

$$\begin{aligned}\texttt{Safeguard} \equiv\ &\texttt{protects.SubjectOfProtection} \sqcup \texttt{ProtectiveMeasure}\\ &\sqcap \texttt{counteracts.Threat}\end{aligned} \tag{11}$$

A protective measure in turn is something that counteracts other activity or an event (Expression 12).

$$\begin{aligned}\texttt{ProtectiveMeasure} \equiv\ &\texttt{Activity}\\ &\sqcap (\exists\texttt{counteracts.Activity} \sqcup \exists\texttt{counteracts.Event})\end{aligned} \tag{12}$$

Threat and danger: WordNet defines threat as something that is a source of danger (Expression 13), and danger as a state of being vulnerable to harm (Expression 14).

$$\texttt{Threat} \equiv \texttt{isSourceOf.Danger} \tag{13}$$

$$\texttt{Danger} \equiv \texttt{State} \sqcap \exists\texttt{exists.Vulnerability} \tag{14}$$

Both WordNet and Fenz ontology state that threat can be a source of another threat (Expression 15).

$$\exists\texttt{isSourceOf.Threat} \sqsubseteq \texttt{Threat} \tag{15}$$

MOST WIEDZY Downloaded from mostwiedzy.pl

Subject of protection: Subject of protection is a concept with its meaning dependent on the described domain. ISO 13335-1 defines organization assets as being the primary subject of protection in terms of information security (Expression 16).

$$\texttt{OrganizationAsset} \sqsubseteq \texttt{SubjectOfProtection} \tag{16}$$

6. Ontology implementation

The model defined in the previous section was fundamental to the construction of the final ontology. As mentioned before, it was divided into 3 modules, one consisting of three ontologies and two consisting of one ontology each[2].

6.1. Risk Core Concepts module

This module was based upon core concepts selected to match the domain of risk analysis: *risk*, *asset*, *vulnerability*, *threat* and *safeguard*. This set was then extended by concepts derived from the appropriate knowledge sources and their definitions according to methodology described in Section 2.

Three ontologies were constructed based on the sources listed in Section 3.2. ENISA-based ontology consists of 43 classes and 28 properties, NIST-based consists of 70 classes and 23 properties and the one based on Sommerville's book is composed of 40 classes and 22 properties.

The ontologies were then merged manually with support from Falcon-AO [16]. The tool was used to compare ontology elements, and the results were introduced into the merged ontology manually by usage of *subClassOf*, *subPropertyOf*, *equivalentClass* and *equivalentProperty* OWL relations using Protégé editor. The following rules were applied:

- When the label or definition of concept or property pointed out that one of the analysed elements had a broader meaning than the other, then *subClassOf* or *subPropertyOf* relation was used,
- When the label or definition of concept or property pointed out that the analysed concepts or properties are equal, then they were connected with *equivalentClass* or *equivalentProperty* relation,
- When the meaning of the concepts was different, the common parent node was created (if needed) and the concepts were connected with subclass relation with that parent.

After the merge, namespaces of all ontologies were unified (with the names of concepts left unchanged) and the ontology was verified for consistency. The final ontology creating Risk Core Concepts module consists of 122 classes and 66 properties.

6.2. Basic Security Concepts module and Safety and Security Requirements module

The two remaining modules consist of a single ontology each and were created using the same methodology as each ontology is composed of the Risk Core Concepts module. The Basic Security Concepts module consists of 269 classes and 91 properties; the Safety and Security Requirements module is composed of 195 classes and 56 properties.

6.3. Security and Safety Ontology

The three modules were integrated using the same procedure that was used during the creation of the Risk Core Concepts module. The concepts belonging to each ontology module were compared using Falcon-AO and then manually moved to the final ontology. The resulting general pur-

2 Each intermediate ontology, the modules, and the final ontology are available in OCS Portal and at http://kask.eti.pg.gda.pl/projekty/#Ontologia_bezpieczestwa in OWL format.

MOST WIEDZY Downloaded from mostwiedzy.pl

pose ontology consists of 566 classes and 193 properties.

7. Conclusions

Security plays an increasingly important role in our everyday life. More and more complex solutions are being developed, thus increasing heterogeneity of the environment in which they are applied.

The proposed ontology tries to address that issue by providing a means for system interoperability in the domain of computer security. The proposed solution tries to unify knowledge gathered from different sources, and by being a general-purpose ontology it introduces a means for combining different ontologies used in different systems.

According to Gruber's definition ontologies need to be shared. The proposed methodology aims at increasing the possibility of ontology exchange. Constructing ontologies having existing solutions in mind greatly improves its usefulness for other researches and increases possibility of its reuse. The presented results show that both the process itself and even the selection of basic concepts can influence how and even if the ontology will be usable outside its primary application or whether it be suitable for integration with other ontologies.

The proposed ontology aims at being easily extendable providing a common platform for future projects that will be able to interoperate with each other. By incorporating knowledge gathered from current glossaries, taxonomies and ontologies those future projects will be able to integrate easily with current solutions, thus reducing divergence among computer systems.

Acknowledgements

This work was funded by the National Science Center under the grant N N516 476440.

8. Literature

[1] Anderson R. *Security engineering*, Wydawnictwo Naukowo Techniczne, 2005.
[2] Avizienis, A., Laprie, J.C., Randell, B., and Landwehr, C. *Basic concepts and taxonomy of dependable and secure computing*. Dependable and Secure Computing, IEEE Transactions on, 1(1):11–33, 2004.
[3] Boiński, T. *Procedures for merging and alignment of domain ontologies*, PhD Thesis [in Polish]. Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, 2012.
[4] Boiński, T., Orłowski, P., Szymański, J., and Krawczyk, H. *Security ontology construction and integration*. In Proceedings of KEOD2011 of the 3nd International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 369–374. INSTICC, 2011.
[5] De Nicola, A., Missikoff, M., and Navigli, R. *A software engineering approach to ontology building. Information Systems*, 34(2): 258–275, 2009.
[6] Donner, M. *Toward a security ontology*. IEEE Security & Privacy, pp. 6–7, 2003.
[7] ENISA. *Risk management: implementation principles and inventories for risk management/risk assessment methods and tools*. Technical report, 2006.
[8] Enisa. *Enisa: a European Union Agency - Glossary of Risk Management*. 2010.
[9] Fenz, S., Pruckner, T., and Manutscheri, A. *Ontological mapping of information security best-practice guidelines. In Business Information Systems*, pp. 49–60. Springer, 2009.
[10] Firesmith, D.G. *A Taxonomy of safety-related requirements*. In International Workshop on High Assurance Systems (RHAS'05), 2005.
[11] Firesmith, D.G. *A taxonomy of security-related requirements. In International Workshop on High Assurance Systems* (RHAS'05). Citeseer, 2005.
[12] Guttman, B. and Roback, E.A. *An introduction to computer security: the NIST handbook*. DIANE Publishing, 1995.

MOST WIEDZY Downloaded from mostwiedzy.pl

[13] Herzog, A., Shahmehri, N., and Duma, C. *An ontology of information security*. 2009.
[14] International Atomic Energy Agency (2007). *IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection* [Online]. Available at: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1290_web.pdf.
[15] ISO/IEC (2004). *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management* [Online]. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066.
[16] Jian, N., Hu, W., Cheng, G., and Qu, Q. *Falcon-AO: Aligning ontologies with Falcon*. In *Integrating Ontologies Workshop Proceedings*, p. 85. Citeseer, 2005.
[17] Kim, A., Luo, J., and Kang, M. *Security ontology for annotating resources*. On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, pp. 1483–1499, 2005.
[18] Knublauch, H. *Protégé-owl api programmer's guide*. 2009.
[19] Knublauch, H., Fergerson, R.W., Noy, N.F., and Musen, M.A. *The Protégé OWL plugin: An open development environment for semantic web applications*. The Semantic Web–ISWC 2004, pp. 229–243, 2004.
[20] Krawczyk, H. *Ontology engineering and its applications*. Department of Computer System Architecture, ETI Faculty, Gdańsk University of Technology, 2007.
[21] Noy, N.F., McGuinness, D.L., et al. *Ontology development 101: A guide to creating your first ontology*, 2001.
[22] ontologydesignpatterns.org (2011). Ontology Design Patterns [Online]. Available at: http://ontologydesignpatterns.org/wiki/Main_Page.
[23] Schober, D., et al. *Towards naming conventions for use in controlled vocabulary and ontology engineering*. Proceedings of BioOntologies SIG, ISMB07, pp. 29–32, 2007.
[24] Schuemacher, M. *Security engineering with patterns: origins, theoretical model, and new applications*. Springer-Verlag, 2003.
[25] Sommerville, I. *Software Engineering*. 8th. Harlow, UK: Addison-Wesley, 2006.
[26] Suárez-Figueroa, M., Gómez-Pérez, A., and Villazón-Terrazas, B. *How to write and use the Ontology Requirements Specification Document*. On the Move to Meaningful Internet Systems: OTM 2009, pp. 966–982, 2009.
[27] Suárez-Figueroa, M.C. et al. (2009), *D5. 4.2: Revision and extension of the neon methodology for building contextualized ontology networks*. [Online]. Available at: http://www.neon-project. org
[28] Sure, Y., Staab, S. and Studer, R. *Handbook on Ontologies*. 2009.
[29] Tartir, S. *Ontology-driven question answering and ontology quality evaluation*. 2009.
[30] W3C, Heflin, J. (2004), *OWL Web Ontology Language Use Cases and Requirements* [Online]. Available at: http://www.w3.org/TR/webont-req/.

UNIWERSALNA ONTOLOGIA BEZPIECZEŃSTWA

STRESZCZENIE

Bezpieczeństwo odgrywa coraz bardziej istotną rolę w naszym codziennym życiu. Użytkownicy systemów komputerowych wskazują więc na potrzebę utworzenia jednego, wspólnego i sformalizowanego modelu integrujących wiele opisów i defini-

MOST WIEDZY Downloaded from mostwiedzy.pl

cji bezpieczeństwa. Celem artykułu jest zaprezentowanie ontologii bezpieczeństwa zaprojektowanej i zaimplementowanej w sposób umożliwiający jej przyszłą rozbudowę i integrację z innymi rozwiązaniami. Zaprezentowano zarówno samą ontologię bezpieczeństwa jak i metodologię jej wytwarzania. Zaprezentowana metodlogia bazuje na pryncypiach uniwersalności, co pozwala na jej zastosowanie w celu integracji i rozbudowy zarówno obecnych jak i przyszłych systemów.

Słowa kluczowe: ontologią bezpieczeństwa, inżynieria ontologii

Tomasz Boiński, Piotr Orłowski and Henryk Krawczyk
Politechnika Gdańska
Wydział Elektroniki, Telekomunikacji i Informatyki
Katedra Architektury Systemów Komputerowych
ul. Gabriela Narutowicza 11/12, 80-233 Gdańsk
tobo@eti.pg.gda.pl

MOST WIEDZY Downloaded from mostwiedzy.pl