INT J COMPUT COMMUN, ISSN 1841-9836
8(6):878-890, December, 2013.

Security Ontology for Adaptive Mapping of Security Standards

S. Ramanauskaitė, D. Olifer, N. Goranin, A. Čenys

Simona Ramanauskaitė*, **Dmitrij Olifer**,
Nikolaj Goranin, **Antanas Čenys**
Vilnius Gediminas Technical University
simona.ramanauskaite,dmitrij.olifer, nikolaj.goranin, antanas.cenys@vgtu.lt
Lithuania, LT-10223 Vilnius, Sauletekio al. 11
*Corresponding author: simona.ramanauskaite@vgtu.lt

Abstract: Adoption of security standards has the capability of improving the security level in an organization as well as to provide additional benefits and possibilities to the organization. However mapping of used standards has to be done when more than one security standard is employed in order to prevent redundant activities, not optimal resource management and unnecessary outlays. Employment of security ontology to map different standards can reduce the mapping complexity however the choice of security ontology is of high importance and there are no analyses on security ontology suitability for adaptive standards mapping.
In this paper we analyze existing security ontologies by comparing their general properties, OntoMetric factors and ability to cover different security standards. As none of the analysed security ontologies were able to cover more than 1/3 of security standards, we proposed a new security ontology, which increased coverage of security standards compared to the existing ontologies and has a better branching and depth properties for ontology visualization purposes. During this research we mapped 4 security standards (ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621) to the new security ontology, therefore this ontology and mapping data can be used for adaptive mapping of any set of these security standards to optimize usage of multiple security standards in an organization.
Keywords: security ontology, security standards, adaptive mapping.

1 Introduction

An ontology defines the basic terms and relations compromising the vocabulary of a topic area as well as the rules for combining terms and relations to define extensions to the vocabulary [9]. The ontology provides a better communication, reusability and organization of knowledge by decreasing language ambiguity and structuring transferred data [1], [2], [3], [4].

Security becomes fundamental in our society and the survival of organizations depends on the correct management of up-to-date security elements [6]. As the security area is very broad and has many relations between its concepts, usage of security ontology could improve security knowledge description unambiguity in information systems. The necessity of security ontology can be noticed in various security communities and considered as an important challenge and a research branch [5], [7], [8].

In small and medium enterprises the knowledge database of security area and its unambiguity is very important in formal/legal activities, such as certification, standard compliance, etc. In many cases organizations have to meet certain security requirements from different sources, which may be redundant or overlapping by simultaneous usage. Therefore standard mapping should be put into practice in cases where more than one security standard has to be met. The mapping of security standards allows the optimization of resources by indicating matching elements of standards and by eliminating duplicated activities and security measures to meet it. However mapping of security standards can be complicated if more than two standards have to be mapped.

Security ontology can be used to simplify the mapping of more than two security standards [10]. This solution suggests mapping all security standards under one security ontology. This ontology would act as a basis for standard knowledge formalization and would allow adaptive mapping of any standards, mapped to the ontology. Therefore the security ontology plays a large role in adaptive mapping and covers a wide area and should be detailed to meet all security standards.

The aim of this paper is to analyse suitability of existing security ontologies to be used for adaptive mapping of security standards and to propose a new one, more suitable for the purpose.

2 Security Ontology

Existing security ontologies vary according to described area and level of detail. One of the first works mentioning information system knowledge concepts concerning security was published in 1990 by J. Mylopoulos et al. The paper "Telos: Representing Knowledge about Information Systems" [12] describes a Telos language to describe the knowledge about information systems and suggests it can be employed for security specification as well. C. E. Landwehr et al. on 1994 published a paper called "A taxonomy of computer program security flaws " [13] where types of computer program security flaws were summarized and claimed it can be used for introduction to the characteristics of security flaws and their origins. A. Avizienis et al. also proposed a taxonomy, concerning security concepts [14]. This taxonomy describes more abstract and wide concepts than C. E. Landwehr et al. provided however clear relationships between categories of taxonomy are missing too.

The need of ontology rather than taxonomy was indicated in a paper "Toward a Security Ontology" by M. Donner on 2003 [7]. On the same year G. Denker et. al. presented security related ontologies for web services and published it in paper "Security in the Semantic Web using OWL" [15] while H. Mouratidis el al. published work "An Ontology for Modelling Security: The Tropos Approach" [16] where presented ontology for security modelling in agent-based information systems. H. Mouratidis provided more works concerning security ontologies [17], [5] where clear orientation to usage of security ontologies in software developments is noticed, therefore these ontologies are meant more for system requirement representation rather than for basic security concepts.

There are ontologies concentrated specifically on security requirements only. One of such ontologies is presented by F. Massacci [18]. Other specific security ontologies are proposed by D. Geneiatakis et al. [19] (designed for describing Session Initiation Protocol security flaws), by M. Karyda et al. [20] (dedicated for describing applications of e-government), by J. Undercoffer et al. [21] (designed for describing computer attacks), by A. Souag [22] (designed for requirements engineering process) and by other authors. A. Kim extended specific ontologies and created one which can be applied to any electronic resource [23]. However this ontology does not overlay all the concepts of information security. More detailed general security ontologies were proposed by A. Herzog et al. [24] and S. Fenz et al. [25].

Security ontology, proposed by Herzog et al. represents information security domain that includes both general concepts and specific vocabulary of the domain. The proposed ontology has 4 top level concepts: assets, threats, vulnerabilities and countermeasures. The ontology overviews the information security domain in a context-independent and application neutral manner. Similar properties apply to security ontology proposed by S. Fenz et al. however it has more concepts in it including non-core concepts such as the infrastructure of organizations. The main top level concepts in this ontology are: asset, control, organization, threat and vulnerability.

Table 1: Data of general comparison of security ontologies

Property	Ontology			
	G. Denker	A. Herzog	S. Fenz	S. Fenz (raw)
Total number of classes	39	460	641	311
Total number of data types properties	0	7	16	14
Total number of object properties	12	30	58	58
Total number of annotation properties	2	4	10	10
Total number of individuals	117	211	486	478
Number of sub-classes	11	571	1051	409
Max. depth of class tree	4	8	6	6
Min. depth of class tree	1	1	1	1
Avg. depth of class tree	1,4	4,1	3,0	3,2
Max. branching factor of class tree	27	83	199	114
Min. branching factor of class tree	1	1	1	1
Avg. branching factor of class tree	7,6	3,2	3,9	14,5

3 Analysis of Security Ontologies

Three security ontologies were chosen for deeper analysis because of its particularity: security ontology created by G. Denker; Security ontology, created by A. Herzog et al.; Security ontology, created by S. Fenz.

While S. Fenz security ontology includes concepts of several security standards (ISO 27001, Grundschutz) in it, one more version of S. Fenz's security ontology will be analyzed in this study (hereinafter S. Fenz (raw)). All classes and elements of security standards will be excluded from S. Fenz's ontology, relying solely on raw concepts of ontology security.

3.1 General Comparison

In general comparison of security ontologies the total number of different ontology elements, the depth and branching metric of the ontology tree are put into comparison. To get these metrics an OWL ontology editor SWOOP was used. Data obtained by this tool are presented in Table 1.

As results of general ontology comparison reveal, G. Denker's ontologies have the least number of concepts, while security ontologies, created by S. Fenz and A. Herzog have the largest number of concepts. G. Denker's ontology is intended to interface between various notations of security standards while ontologies of S. Fenz and A. Herzog represent the whole area of security, therefore have more concepts.

The purpose of ontology usage inflicts on the number of individuals as well - wider range ontologies have more individuals to allow user to chose from; specific purpose ontologies have less or no individuals as all individuals should be known or unnecessary to the user.

Another important metric is the depth and branching factor of ontology class tree. It defines the main properties of tree structure of the ontology and can be exercised to define how intuitive the ontology should be for individual users. Our analysis displays the security ontology of A. Herzog has the deepest class structure and has the most substantial detailing level. However the maximum branching factor of class tree is equal to 83, which may result in human users facing difficulties while viewing the ontology. Ontology of S. Fenz should be difficult to visualize as well, because of its branching factor.

Table 2: OntoMetric analysis data of the ontologies content and the contents organization

Characteristic	**Ontology**			
	G. Denker	A. Herzog	S. Fenz	S. Fenz (raw)
Concepts (factor)	2	4	4	4
Relations (factor)	3	3	3	3
Taxonomy (factor)	2	3	3	3
Axioms (factor)	2	4	4	4

3.2 OntoMetric Analysis of Security Ontologies

General comparison of security ontologies gives just a few main quantitative metrics, while the quality of ontology is not taken into account. OntoMetric [26] is a method for ontology quality measurement. This method compares ontologies in five dimensions (the ontologies content and the contents organization; the language in which it is implemented; the methodology that has been followed to develop it; the software tools used to build and edit the ontology; the costs that the ontology will require in a certain project) and measures all the characteristics from 1 to 5 according to their low or high degree of accomplishment.

While all ontologies we are analyzing are written in the same file format, we are analyzing the content metrics alone (metric of language, tools and costs should be equal, because all analyzed ontologies are written in OWL files, while the development process of ontology do not have significant influence on its usage and are unknown to us). According to OntoMetric, the content of ontology can be defined by 4 factors: concepts, relations, taxonomy and axioms.

As evaluation of OntoMetric is qualitative, we will evaluate all of them as all security ontologies are meant for presenting the broadest security area possible and should be able to present any situation in area of information security. The imagination of ideal security ontology is important in order to evaluate the concept factor in OntoMetric analysis as this measurement should provide information on how well the security area is covered by the ontology.

Other factors in OntoMetric analysis are more relative and describes how well the relations, taxonomy and axioms are described in the ontology, not the whole security area.

All data of our OntoMetrix analysis are presented in Table 2.

The OntoMetrix analysis shows the G. Danker ontology has the lowest scores, while S. Fenz and A. Herzog ontologies have similar scores, the level of detail and provides wide range of security concepts. However the data of OntoMetric analysis does not show differences between S. Fenz and A. Herzog.

While comparing the differences in S. Fenz's and A. Herzog's ontologies, it can be noticed that ontology, created by A. Herzog has more of a theoretical approach rather than the ontology of S. Fenz and describes more definitions, formal concepts of information security area. S. Fenz's ontology provides more information on practical side of information security, by listing basic controls as a guide for security administrators for system security assurance however does not mention concepts, related to organizational security.

3.3 Research of Security Ontology Usage for Mapping of Security Standards

As security ontologies, proposed by A. Herzog and S. Fenz have similar ontology comparison results, a deeper analysis has to be performed to select the best one for usage in adaptive mapping of security standards.

Adaptive Mapping of Security Standards

To ensure security in an organization, security standards or best practices can be employed. In some cases compliance to a certain security standard is even required to obtain privileges to supply or to get different services. However when organization uses more than one security standard, mapping or integration of security standard usage should be done in order to avoid redundant activities, not optimal resource management, unnecessary outlays etc. Integration or direct mapping of security standards are time and knowledge consuming as well as very static (everything has to be redone when a standard has to be removed or added), while adaptive mapping of security standards provides more flexibility to change the list of used standards as well as requires less work to map a larger number of standards as each standard have to be mapped to ontology only. Therefore n mapping activities have to be done to map n standards in stead of n*(n-1) mappings for direct mapping. The process of adaptive mapping and integrated standard generation is presented in Fig. 1

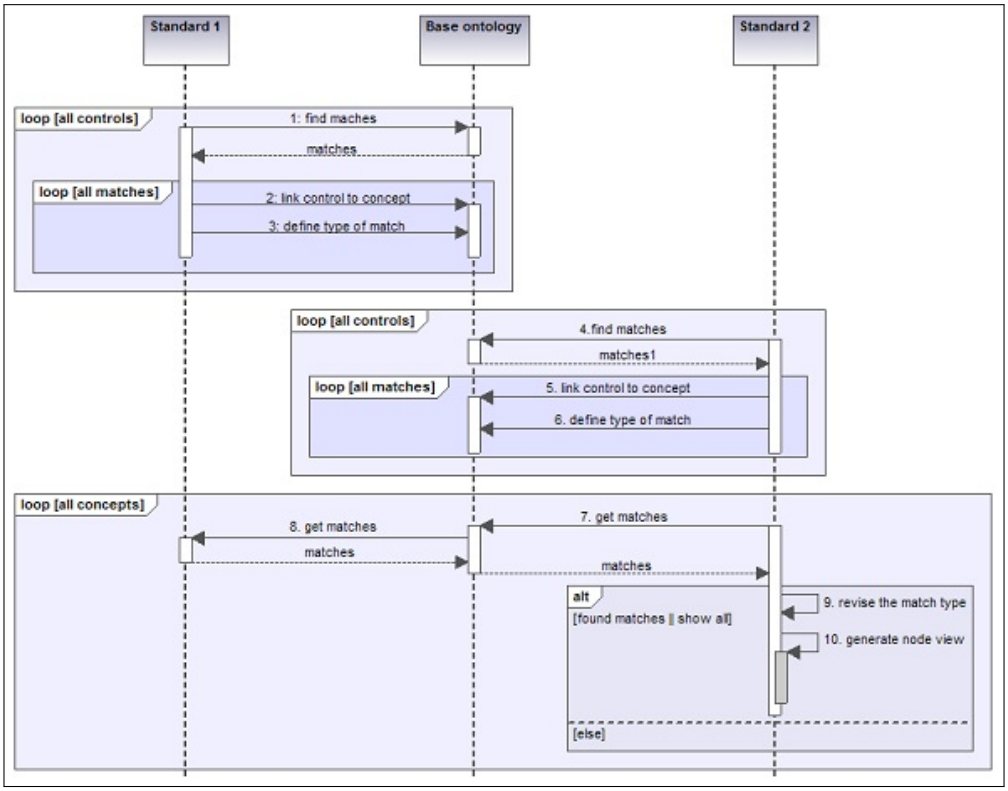

Figure 1: Sequence of mapping two standards and generating the mapped standard in relation to the structure of ontology

When a standard is mapped to the base ontology, all matching controls and concepts between ontology and standards have to be linked. This has to be done once for all standards which have to be mapped together. The generation of standard maps or integrated standards is dynamic and can be done on demand by changing standards which have to be mapped or integrated, properties for relation type estimation etc. The map generation process finds similar controls in selected standards by comparing its linking to the base ontology. An example of relation type estimation in adaptive mapping is provided in Fig. 2.

In this example a control in ISO 27001 (A.8.3.3_Removal_of_access_righ...) and control in PCI DSS (PCI_DSS_8_5_4) standards are mapped with the same links to the security ontology (control in one standard has the same relations to concepts of security standard as control in

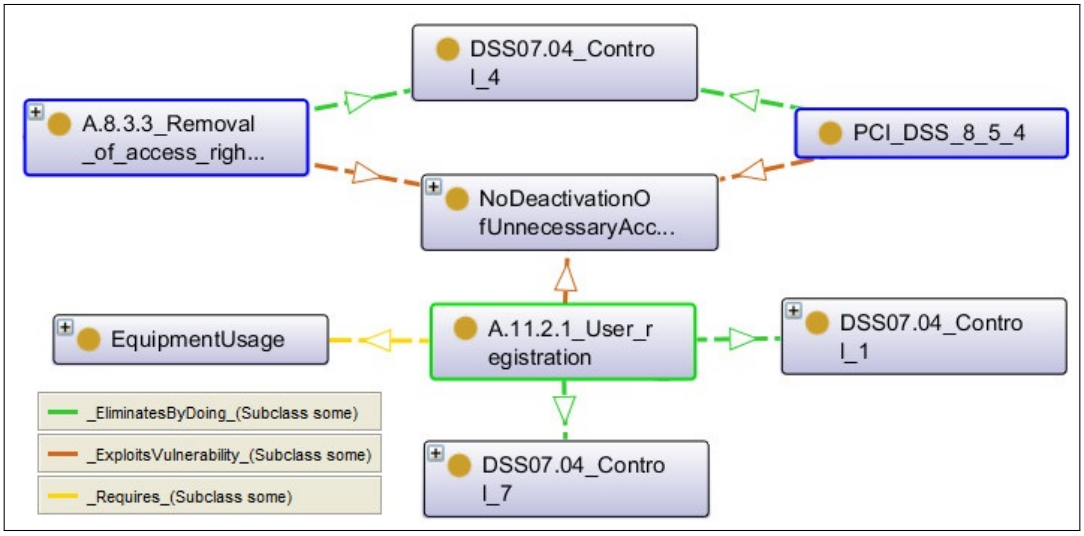

Figure 2: Example of standard mapping trough ontology

another standard). As these two controls have no differences in mapping, the full match relation between these two controls of different standards can be generated. One more control of ISO 27001 standard (A.11.2.1_User_registration) is presented in this example to illustrate relevant (not matching) controls. These two controls of ISO 27001 security standard define situations, where vulnerability of nonblocked unnecessary accounts or terminals can be exploited. However both of ISO 27001 controls have more links to different concepts of security ontology, therefore these two ISO 27001 controls can not be treated as equal, however are relevant on certain levels. This kind of information can be used to analyse security standards and to optimize the resource usage when multiple security standards have to be met in an organization.

For visualization and analysis of overlapping of multiple security standards a tool for adaptive mapping of security standards was created (see Fig. 3). This tool uses security ontology and maps security standards data to generated tree structure hierarchies, representing a chosen security standard or integration of few security standards as well as providing additional data trough node notation and explanation boxes on similarities of controls in chosen security standards.

Research of Security Standards Coverage by Security Ontologies

To compare which security ontology is more suitable for adaptive security standards mapping and adaptive mapping, ontology and standard concept coverage were analyzed. A. Herzog's and S. Fenz's ontologies were mapped with:

- ISO27001 - the most popular security standard, which was created according to British Security standard BS7799. This standard covers practically all security areas, provides certification opportunity and is widely recognized.
- PCI DSS - security standard developed by such worldwide organizations as Visa, MasterCard, American Express, Discover and JCB. Standard developed to ensure cardholder information protection. This standard is a "Must-have" for all organizations who handle debit, credit, prepaid and other cards. Otherwise these organizations are forbidden to use Visa, MasterCard, American Express and other cards.
- ISSA 5173 - security standard for SME (Small Medium Enterprise). This standard has not been approved or officially recognized, however describes main security requirements,

which need to be implemented in any organization.

- NISTIR 7621 - security standard, developed by national institute of Standards and technology. Document clearly defines which actions are "absolutely necessary" for information, systems and networks protection. It also provides best practices on needed security level implementation.

Data on links between these security standards are presented in static form for 2 specific standards (as a table with matching controls between two security standards [28]) mostly. S. Fenz was the first who mapped ISO 27001 and Grundschutz security standards to his ontology. He used this mapping for purposes of automated risk and utility management [11], however this information can be also used for adaptive standard mapping. S. Fenz mapped two standards only, therefore links can only be generated between ISO 27001 and Grundschutz security.

We analyzed all controls in all 4 chosen standards and mapped them to related concepts in S. Fenz and A. Herzog security ontologies. The mapping of security standards was performed by mapping the lowest level concepts (usually it's a certain control, requirement for the organization), while the classes in security standards, used for presentation of class hierarchy were not accounted as mapping objects.

The process of security standard mapping to security ontologies revealed differences between analyzed ontologies as well. Biggest part of mapping links in S. Fenz's ontology are very direct - one requirement of the standard has an equal or very similar control in S. Fenz's ontology. This type of mapping links are very direct, easy to understand for individual users, however the controls have to be detailed by other links between different concepts of the ontology, otherwise it will be difficult to define relations between standards controls, clustering, etc. Meanwhile mapping security standards according to A. Herzog's ontology was done from logical structure standpoint - one requirement of security standard is to have several links to ontology, by describing which concepts of ontology are related to this requirement (by defining what and how one has to do or use to protect against certain threat or vulnerability). This type of mapping requires more mapping links and has a potential to be easier to cluster controls of security standards into relevant groups. This type of mapping would be more understandable to information systems however would require more analysis or visualizing tools for people to understand links between two security standards, mapped through ontology this way.

Summarizing the security standard mapping process to security ontologies - S. Fenz's ontology can be used to simplify the mapping of security standards because all the most important concepts for mapping are described as list of classes, while in ontology of A. Herzog's mapped classes have more links to ontology and provide more analysis and application possibilities after the mapping is done.

In table 3 data on ontology coverage by standard (covered) and standard coverage by ontology (covers) are provided. Column "covered" defines what part of security ontology was used to map certain standard while column "covers" defines what percentage of security standard was mapped to the security ontology. The property "covers" is more important in this research as it provides information on how well the ontology is capable to present certain security standards in the knowledge database.

The analysis of security ontology and standard coverage revealed that ontologies of A. Herzog and S. Fenz are not capable to fully cover none of analyzed security standards: only security standards with small number of controls or requirements can be mapped with security ontology to cover more than 50% of standard controls; security standards with more than 100 controls or requirements can not be mapped to A. Herzog's and S. Fenz's security ontologies to cover more then 30% of standard controls or requirements. This shows the fact that these two security ontologies do not have all necessary concepts to be fully mapped to security standards.

Analysis of concepts of security ontologies to be employed to map security standard revealed that just a small part (5-18%) of classes from A. Herzog's and S. Fenz's ontologies are mapped directly to security standards. This number could be improved by providing more detailed concept of relationship, however it allows defining what part of ontology is directly related to concepts, mentioned in security standards.

Security ontology, created by S. Fenz was able to cover a larger part of analyzed security standards than A. Harz's ontology. The biggest difference (29% and 19%) was noticed in PCI DSS standard. This could be an argument to chose S. Fenz's security ontology if a company is working with PSI DSS standards, while coverage differences for other analyzed standards are minor. However to cover 29% of PSI DSS standard is not enough to represent it. A new security ontology with more security concepts could help to improve the situation and would allow mapping of bigger parts of security standards.

4 New Security Ontology

As S. Fenz's and A. Herzog's ontologies have low security standard coverage and are not the excellent choice for adaptive mapping of security standards we have created a new general purpose security ontology, which would extend these two ontologies and would be more suitable for adaptive mapping of security standards.

Our ontology has 5 top level classes (see. Fig. 3): asset, countermeasure, organization, threat and vulnerability. These 5 classes are the most basic in security area and are detailed in lower levels.

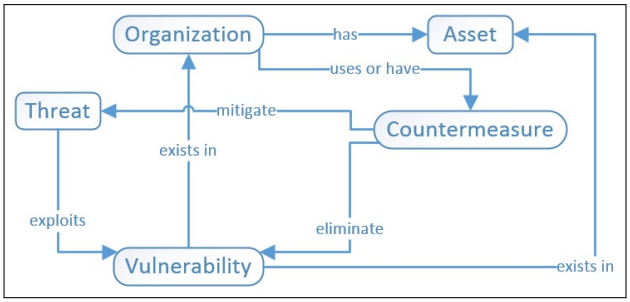

Figure 3: Top level structure of proposed Security ontology

Asset class describes both tangible and intangible asset an organization can have. We describe this class more appropriately than other security ontologies do with the addition of more knowledge on used data by the organization, location and other equipment, owned or used in the company and related to organization's security. The intangible asset is divided into Data and Software (see Fig. 4), while inner structure describes various types of data and software. The tangible assets are structured to subclasses of Movable and Unmovable asset (see Fig. 4). Immovable asset describes location and building concepts and main elements which can be found in it. We structured movable assets into 4 subclasses: alarm systems and detectors; furniture; IT components; utilities. These 4 categories allows the creation of more links to security standards by defining what kind of assets are involved into certain controls (who is at risk, who has a vulnerability etc.).

Countermeasure and Threat classes are described pretty well in A. Herzog's ontology, therefore we made minor changes to it and use similar structure and components as A. Herzog did.

The need for more organizational concepts arose during the mapping of security standards to A. Herzog's and S. Fenz's security ontologies. These two ontologies have a poor description

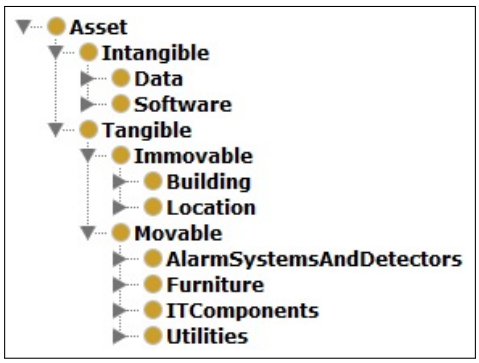

Figure 4: Basic hierarchy of asset concept

of organization structure and policies, while the companies' information security policy is the most important to ensure its security. As subclasses of organization Department, Personnel and Policy concepts were distinguished (see Fig. 5). Precise control description of security standards can be achieved if links to certain executor can be made. Therefore Department and Personnel classes were added and detailed to distinguish plausible types of departments and positions in it.

COBIT is a framework [27], which describes the best ideas for information technology management, quality, evaluation and improvement. Therefore we adopted COBIT 5 framework into our ontology, by defining IT policy class as organization policy subclass, where all COBIT 5 ideas are detailed (see Fig. 5). The COBIT 5 framework was exercised as it is in IT policies class. This guaranties the intuit of ontology usage to those, who is familiar with COBIT framework. Meanwhile in order to propose multiple views and ways to find necessary concepts in the ontology, more subclasses were added to Policy class (see Fig. 5). These classes should present more general policies of the organization however most of them have relations to classes of IT policies class (COBIT 5 framework).

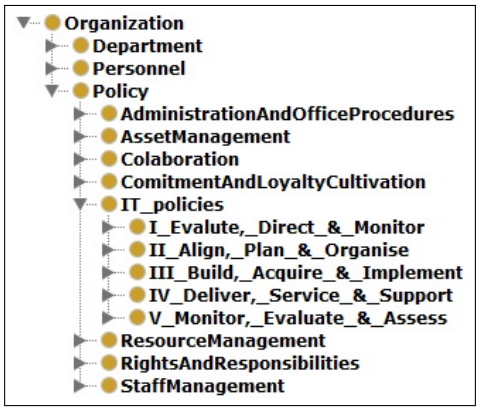

Figure 5: Basic hierarchy of organization concept

Vulnerability class was not detailed properly in A. Herzog's and S. Fenz's ontologies as well. S. Fenz provides a list of vulnerabilities describing individuals with no structure, while A. Herzog describes simply basic types of vulnerabilities. Therefore we extended vulnerability class by dividing it into Code vulnerabilities, Configuration vulnerabilities, Design vulnerabilities, Policy vulnerabilities and Transfer vulnerabilities (see Fig. 6). Those classes are detailed to reflect the basic security vulnerabilities, however they are more structured than in S. Fenz's ontology, to make it more intuitive and simpler to visualize.

To use this ontology as a base for adaptive mapping of security standards a clear and intuitive

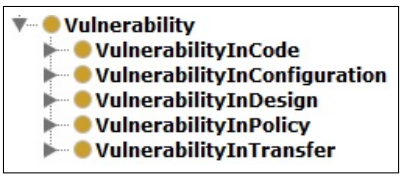

Figure 6: Basic hierarchy of vulnerability concept

ontology structure has to be maintained. We optimized the tree structure of the ontology, therefore now it has 1795 classes, average depth of class tree is 6,5 (has maximum up to 9 depth of class tree) and average branching factor of class tree is 4,8 (has from 1 to 18 subclasses). Such a structure is more viewable in tree structure and should be more intuitive for ontology users (see Fig. 7).

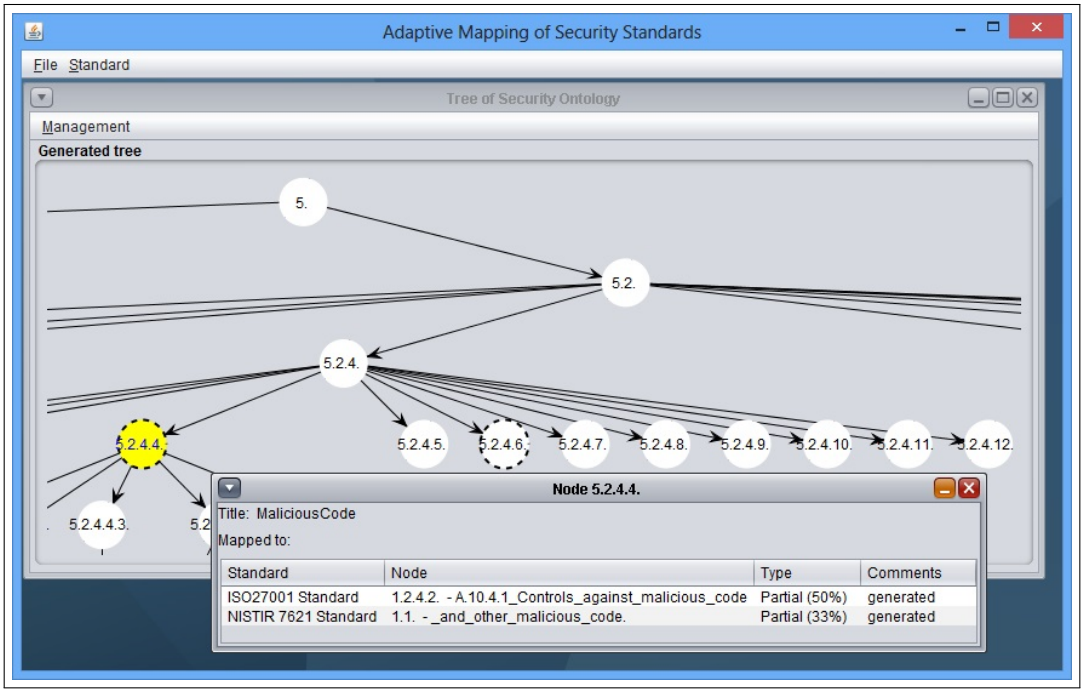

Figure 7: Structure fragment of proposed security ontology and adaptive mapping data in AMSS (created tool for adaptive mapping of security standard)

While structure optimization of new security ontology is more important to ensure user friendly usage and understanding, new concepts allowed a better coverage of security standards. We do not provide direct list of controls and use similar ontology structure for standard mapping as A. Herzog therefore security standard mapping to this ontology has to be done by defining more than one relation to ontology. This mapping property is useful to analyze and to map security concepts in different standards.

ISO27001, PCI DSS, ISSA 5173 and NISTIR 7621 security standards were specified and mapped to it in order to evaluate its suitability to map security standards. Using this ontology as a base for adaptive mapping, 80% of ISO27001, 100% of PCI DSS, ISSA 5173 and NISTIR 7621 standards were mapped to the ontology (see Table 3).

The 100% mapping of ISO27001 standard was not achieved because we did not mapped very specific requirements in security standard (like security properties of used operating system etc.) to more abstract in our ontology.

Table 3: Coverage of ontology to standard and standard to ontology

Standard	Ontology/Standard coverage					
	S. Fenz		A. Herzog		Proposed ontology	
	Covered	Covers	Covered	Covers	Covered	Covers
ISO27001	35/311 (11%)	23/133 (17%)	26/460 (6%)	19/133 (14%)	130/1795 (7%)	107/133 (80%)
PCI DSS	42/311 (14%)	48/165 (29%)	25/460 (5%)	32/165 (19%)	132/1795 (7%)	165/165 (100%)
ISSA 5173	31/311 (10%)	7/12 (58%)	29/460 (6%)	6/12 (50%)	15/1795 (1%)	12/12 (100%)
NISTIR 7621	14/311 (5%)	8/10 (80%)	21/460 (5%)	8/10 (80%)	19/1795 (1%)	10/10 (100%)

This ontology and mapping of these 4 security standards to it can be used to generate adaptive maps between any of the two mapped security standards or integrated standard can be created with the usage of any set of mapped security standards without the necessity to map two security standards directly. As our proposed security ontology can cover a larger part of concepts in analysed security standards (the average coverage of these 4 security standards is 92%, while S. Fenz's average coverage of these security standards is 27%, A. Herzog - 20%) the adaptive mapping of security standards will be more precise by applying it as a base ontology. However the ontology does not cover all standards by 100%, therefore should be improved to get even bigger precision of adaptive mapping.

5 Conclusions and Future Works

General comparison of G. Denker's, A. Herzog's and S. Fenz's security ontologies has shown the necessity of user friendly ontology structure - all three ontologies have classes, with more than 25 subclasses in them. Such ontology could be difficult to use for visual presentation or quick knowledge search.

OntoMetric methodology allows a more precise judgment on security ontologies rather than general comparison, because it enables an evaluation of the content of compared ontologies. However the evaluation marks are very dependable on the evaluator's opinion and requirements for the ontology. Evaluation of ontologies' ability to be mapped to security standards is a more suitable measurement to choose the base ontology for adaptive mapping of security standards comparing to OntoMetric.

In order to evaluate ontologies' suitability to map different security standards we compared percentage of concepts in security standard (ISO 27001, PCI DSS, ISSA 5173 and NISTR 7621) which can be mapped to security ontology. This research revealed there are no security ontologies, that would be able to map at least 50% of any security standards we have analyzed. This fact implies the necessity of new or modified ontology, which could be used to present larger parts of knowledge, used in security standards.

We proposed a new security ontology, by integrating concepts of COBIT framework, part of classes of A. Herzog's and S. Fenz's ontologies. This new ontology increased the coverage of security standards. Using this security ontology, from 80% to 100% of analyzed security standards (ISO 27001, PCI DSS, ISSA 5173 and NISTR 7621) can be mapped to it. This percentage can be increased even more with the addition of more specific (related to payment cards, law and standard requirements etc.) concepts to this ontology. The proposed security ontology has a more balanced tree structure as well, which increases its visualization possibilities.

Acknowledgements

The study was carried out within the framework of the National Project No.VP1-3.1-MM-08-K-01-012: "Virtualisation, visualization and e-services security technologies and research", supported by the EU Social Fund.

Bibliography

[1] Gruber, T (1995). Towards Principles for the Design of Ontologies used for Knowledge Sharing, *International Journal of Human-Computer Studies*, ISSN 1071-5819, 43(5-6): 907-928.

[2] Dobson, G.; Sawyer P. (2006). Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web, *In: Dependable Requirements Engineering of Computerised Systems at NPPs*, Institute for Energy Technology (IFE), Halden, 2006.

[3] Fernandez-Breis, J. T.; Martiinez-Bejar R (2002). A cooperative framework for integrating ontologies, *International Journal of Human-Computer Studies*, ISSN 1071-5819, 56(6): 665-720.

[4] Gruninger, M.; Lee J. (2002). Ontology Applications and Design, *Communications of the ACM*, ISSN 0001-0782, 45(2): 39- 41.

[5] Mouratidis, H.; Giorgini P. (2006). *Integrating Security and Software Engineering: Advances and Future Visions*, IGI Global.

[6] Dhillon, G.; Backhouse J. (2000). Information system security management in the new millennium, *Communications of the ACM*, ISSN 0001-078, 43(7): 125-128.

[7] Donner, M. (2003). Toward a Security Ontology, *IEEE Security and Privacy*, ISSN 1540-7993, 1(3): 6-7.

[8] Tsoumas, B.; Gritzalis D. (2006). Towards an Ontology-based Security Management, *Advanced Information Networking and Applications*, ISSN 1550-445X, 1: 985 - 992.

[9] Gomez-Perez A.; Fernandez-Lopez M.; Corcho O. (2004). *Ontological Engineering*, Springer.

[10] Ramanauskaite, S.; Goranin, N.; Cenys, A.; Olifer, D. (2013) Ontology-based security standards mapping pptimization by the means of Graph theory, *Proceesings of International congress on engineering and technology ICET 2013*, ISBN 978-80-87670-08-8: 74-83.

[11] Fenz S. (2010). Ontology-based Generation of IT-Security Metrics, *Proceedings of the 2010 ACM Symposium on Applied Computing*, ISBN 978-1-60558-639-7: 1833-1839.

[12] Mylopoulos J.; Borgida A.; Jarke M.; Koubarakis M. (1990). Telos: Representing Knowledge About Information Systems, *ACM Transactions on Information Systems*, ISSN 1046-8188: 325-362.

[13] Landwehr C. E.; Bull A. R.; McDermott J. P.; Choi W. S. (1994). A taxonomy of computer program security flaws, *ACM Computing Surveys*, ISSN 0360-0300, 26(3): 211-254.

[14] Avizienis A.; Laprie J. C.; Randell B.; Landwehr C. (2004). Basic concepts and taxonomy of dependable and secure computing,emphIEEE Transactions on Dependable and Secure Computing, ISSN 1545-5971, 1(1): 11-33.

[15] Denker G.; Kagalb L.; Finin T. (2005). Security in the Semantic Web using OWL, *Information Security Technical Report*, ISSN 2214-2126, 10(1): 51-58.

[16] Mouratidis H.; Giorgini P.; Manson G. (2003). An Ontology for Modelling Security: The Tropos Approach, *Proceedings of the KES 2003 Invited Session Ontology and Multiagent Systems Desing.*

[17] Giorgini P.; Manson G.; Mouratidis H. (2004). Towards the Development of Secure Information Systems: Security Reference Diagrams and Security Attack Scenarios, *Proceeding of 16th Conference On Advanced Information Systems Engineering.*

[18] Massacci F.; Mylopoulos J.; Paci F.; Tun T. T.; Yu Y. (2011). An Extended Ontology for Security Requirements, *Advanced Information Systems Engineering Workshops*, ISSN 1865-1348, 83: 622-636.

[19] Geneiatakis D.; Lambrinoudakis C. (2007). An ontology description for SIP security flaw, *Computer Communications*, ISSN 0140-3664, 30(6): 1367-1374.

[20] Karyda M.; Balopoulos T.; Gymnopoulos L.; Kokolakis S.; Lambrinoudakis C.; Gritzalis S.; Dritsas S. (2006). An ontology for secure e-government applications, *Proceedings of the The First International Conference on Availability, Reliability and Security, ARES 2006.*

[21] Undercoffer J.; Joshi A.; Pinkston J. (2003). Modeling Computer Attacks: An Ontology for Intrusion Detection, *The Sixth International Symposium on Recent Advances in Intrusion Detection.*

[22] Souag A. (2012). Towards a new generation of security requirements definition methodology using ontologies, *Proceedings of 24th International Conference on Advanced Information Systems Engineering*: 1-8.

[23] Kim A.; Lou J.; Kang M. H. (2005). Security Ontology for Annotating Resources, *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE* ISSN 0302-9743, 3761: 1483-1499.

[24] Herzog A.; Shahmehri N.; Duma C. (2007). An Ontology of Information Securit, *International Journl of nformation Security and Privacy*, ISSN 1930-1650, 1(4): 1-23.

[25] Fenz S.; Ekelhart A. (2009). Formalizing information security knowledge, *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ISBN 978-1-60558-394-5: 183-194.

[26] Lozano-Tello A; Gomez-Perez A. (2004). ONTOMETRIC: A method to choose the appropriate ontology, *Journal of database management*, ISSN 1063-8016, 15(2): 1-18.

[27] ISACA (2013). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.

[28] Hofherr M. (2011). Mapping ISO27001 <>PCI DSS 2.0, *ForInSecT*, http://www.forinsect.com/downloads/Mapping-ISO27001-PCI_public.pdf.