Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory

Simona RAMANAUSKAITĖ1 – Nikolaj GORANIN1 – Antanas ČENYS1 – Dmitrij OLIFER1

1 Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius, Lithuania

Abstract:
There are many security standards which a company can use. Sometimes usage of security standards can be required by regulating institutions. While security standards can differ in purpose and covered area, more than one standard can be used at the same time which leads to overlap and potential conflicts in requirements of different standards. In such cases, deep analysis of used standards has to be done to ensure optimal usage of company’s resources implementing these security requirements.

In this paper we analyze existing solutions for standard harmonization and security ontologies to design an adaptive mapping of security standards by using ontology to map standards and graph theory to visualize mapped standards. We present the architecture of prototype and use it to map ISO27001 standard and Grundschutz best practice. The experiment shows the proposed model can reduce the need of standard mapping documents. Proposed solution can be useful for detailing certain controls of security standards in wider domain; nevertheless, it depends on the description of security standards in the base ontology.

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.

Keywords: security standards, security ontology, standard mapping, standard visualization.

1 Introduction
Increasing popularity of information and telecommunications solutions requires bigger attention to security issues. Usage of security standards is one way to increase the security level in a company. Some standards must be met in the company to be certified and acquire additional possibilities (for example, if company wants to work with payment cards it has to be compliant with PCI-DSS standard) while the other standards can be used as advisory to improve the security level in the company. However, using more than one standard at the same time (which becomes very common at present) there can be duplication or even conflicts between requirements of the different standards. Such a situation in the company can cause an inefficient usage of company’s resources implementing security requirements, while used components of information security management system can be redundant as well. Therefore clear understanding of requirement relations in the used standards must be ensured to optimize the process of its implementation and maintenance.

The purpose of this work is to increase the understanding of consolidated usage of different standards by visualizing security standard and relations to controls of other standards. Consequently, the object of this research is security standards. In section 2, we analyze existing solutions for harmonizing controls of different standards. Section 3 presents our proposal for the adaptive standard mapping. In section 4, information about existing security ontologies is provided and our choice to map security standard is explained. Section 5 is dedicated to define notation of the mapped standard visualization.
section 6, we revise analysis results of S. Fenz’s Security Ontology [1] and visualization of two standards mapped in this ontology. Last section concludes the work and provides future directions.

2 Harmonization of Different Standards

Optimizing the usage of multiple security standards at the same time, harmonization of these standards has to be done. Harmonization is an activity that seeks to define and configure the most suitable harmonization strategy for achieving the strategic goals of an organization where two or more models are involved [2]. However, it is noticeable that different terminology is used to address the harmonization of different standards in analyzed related works: harmonization, synergy, compatibility, etc. All these terms are related, nevertheless, they have specific meaning in this context. Basically there can be separated 3 different techniques to associate controls of different standards, which imply the usage of different terms [3]:

1) Semantic compatibility means achieving of standard harmonization through the same terminology. These methods attempt to unify the terminology in different standards eliminating any misunderstanding and establishing the relations between different controls by the same terms. It can be difficult task to associate controls of standards by terminology, because the analysis must take into account both terminology and context it is used in, while different standard structure and other properties in standards require more advantaged technologies to do it in a right way.

2) Standard mapping is one of the most popular techniques used to harmonize different standards. It attempts to compare different standards and make links between different concepts, controls, structures, etc. The result of mapping two standards usually is shown in a table of matches between these standards, which indicates which parts of these standards match and which parts are unique just in a certain standard. However, to map more than 2 standards at the same time can be tricky and sometimes ineffective.

3) Integration technique is used to combine a few standards into one. While mapping document supplies just links between standards, integration creates a new document, which combines all information from used standards making no difference which parts match between standards and which are unique for one of the standards. A User simply gets one combined document, which matches usage of few standards in conjunction. However, this solution requires additional work to create it comparing to the standard mapping. This is because elements of different standards must be identified as in the standard mapping, while a new document structure and control formulations must be reasonably created as well. Removal or addition of the new standard is difficult using this technique and requires overall revision of the document.

All 3 mentioned techniques have different properties and usage area (see Tab. 1).

<table>
<thead>
<tr>
<th>Technique</th>
<th>Related terms</th>
<th>Number of documents for harmonizing n standards</th>
<th>Number of records for harmonizing n standards in one document</th>
<th>Usage examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semantic compatibility</td>
<td>Syntactic analysis, Homogenization</td>
<td>From 1 to n(n-1)/2</td>
<td>Same as number of synonyms in these standards</td>
<td>ISO standard family</td>
</tr>
<tr>
<td>Mapping</td>
<td>Comparison, Alignment, Coverage</td>
<td>From 1 to n(n-1)</td>
<td>Up to m1+m2, where m1 is a number of controls in first standard and m2 is in second</td>
<td>[4, 5]</td>
</tr>
<tr>
<td>Integration</td>
<td>Unification, Synergy, Complementation</td>
<td>1</td>
<td>Up to  ( \sum m_i ), where m_i is a number of controls in i-th standard</td>
<td>[6, 7]</td>
</tr>
</tbody>
</table>

The integration of many standards into one is very simple when it is used for the end user. However, additional information allowing to distinguish belonging of specific controls to the specific standard is useful [8], and sometimes it is missing in the integration technique. Other disadvantage of standard integration is its inflexibility because none of the standards can be easily added or removed.
from the integrated document (new integration for different combination of standards).

Mapping technique solves these problems; however, what is missing is better representation of the integrated standards. The solution for designing technique allowing to combine the best parts of both techniques and to eliminate their disadvantages is to use adaptive standard integration.

3 Ontology-based Standard Mapping

The main principle of proposed adaptive standard mapping is to integrate selected standards automatically by using mapping documents for the selected standard. However, to reduce the complexity and necessity of many mapping documents one base standard could be used to map all the other standards. This would require just as many mapping documents as there are standards that have to be integrated.

To implement this solution, the base standard for mapping other standard to has to be complete and detailed. However, it is difficult to find a suitable standard because of required ability to expand it easily and cover all necessary areas. There are some works on representation of security standards included into security ontology [8—11]. Therefore, we suggest using ontology as a basis for mapping different standards. The ontology could be supplemented if certain concepts are missing, and also it can serve as a basis for semantic mapping of standards.

The main algorithm of adaptive standard integration can be divided into several simple steps:

1) Choosing/creating of the overall and detailed ontology.
2) Creating of the mapping of ontology with all of the selected standards.
3) Mapping of the selected standards according to related elements in the ontology and standard.

Fig. 1 Sequence of mapping two standards and generating the mapped standard in relation to the structure of ontology or chosen standard

The adaptive standard mapping can be generated and represented by chosen standard structure. Figure 1 shows the main principle of mapping 2 standards using ontology as the mapping basis, and how the adaptive standard mapping can be generated according to structure of chosen standard.
The generation of adaptive standard mapping requires getting matches for all standard nodes from the base standard and matches to the controls of base standard in another standard. Additionally, the mapping type should be revised considering these two standards in such a situation where representation of the match type should be more accurate.

This solution combines all 3 harmonization techniques and allows using of all the benefits it gives:

1) harmonizing n standards exactly n mapping documents have to be created (less than in mapping technique);
2) integrated standard can be regenerated automatically changing the list of harmonizing standards and the base of view (more flexible than integration technique);
3) mapping standard to ontology context of the class can be represented (this task for semantic analysis can be more difficult to achieve).

4 Security Ontologies for Adaptive Mapping of Security Standards

There are plenty of security ontologies at present. One of the first works mentioning information system knowledge concepts concerning security was published in 1990 by J. Mylopoulos et al. [12]. The paper “Telos: Representing Knowledge about Information Systems” describes the Telos language to review the knowledge about information systems and mentions that it can be used for security specification as well. In 1994, there was published paper by C. E. Landwehr et al. “A taxonomy of computer program security flaws” [13] which summarized types of computer program security flaws and claimed it can be used for introduction to the characteristics of security flaws and how they can arise. A. Avizienis et al. [14] also proposed a taxonomy concerning security concepts. This taxonomy describes more abstract and wide concepts than provided by C. E. Landwehr et al. [13]; nevertheless, clear relations between categories of taxonomy are missing as well.

The need of ontology rather than taxonomy rise, and it is proved by M. Donner’s paper “Toward a Security Ontology” [15]. In the same year, G. Denker et al. represented security related ontologies for web services [16] and introduced improvement in the paper “Security in the Semantic Web using OWL” [17], while H. Mouratidis et al. published work “An Ontology for Modelling Security: The Tropos Approach” [18] where presented ontology for security modeling in agent-based information systems. H. Mouratidis provided more works concerning security ontologies [19, 20] where clear orientation to usage of security ontologies in software developments is noticed, therefore these ontologies are meant more for system requirement representation than basic security concepts.

There are ontologies concentrated only specifically on the security requirements. One of such ontologies is presented by F. Massacci [21]. Other specific security ontologies are proposed by D. Geneiatakis et al. [22] (meant for describing of the Session Initiation Protocol security flaws), by M. Karyda et al. [23] (meant for describing of the applications of e-government), by J. Undercoffer et al. [24] (meant for describing of the computer attack), by A. Souag [25] (meant for requirements engineering process), and by other authors. In addition, A. Kim et al. [26] extended specific ontologies and created one which can be applied to any electronic resource. However, this ontology does not comprise all the concepts of information security. More detailed general security ontologies were proposed by A. Herzog et al. [27] and S. Fenz et al. [28].

Security ontology proposed by Herzog et al. [27] 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. [28]; however it embraces more concepts 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.

A choice of ontology can vary depending on situation, and standards which have to be mapped. We recommend to choose as wide domain ontology as possible to ensure ability to map security standards of different type and purpose. According to research results of A. Souag et al. [3], the ontology proposed by S. Fenz has the biggest coverage of security concepts. In addition, S. Fenz et al. published a series of works [1, 10, 28—34] where the ontology is extended by adding concepts of ISO 27001 standard, the French EBIOS (Expression des Besoins et Identification des
Objectifs de Securite) standard, the German IT-Grundschutz Manual, and other concepts for improvement of this ontology usage for risk management. Because of all these facts, for further research we will use the security ontology proposed by S. Fenz et al. providing ability to add more concepts or different standards.

5 Adaptive Mapping and Visualization of Security Standards

All security standards, best practices or ontologies have their structure which could be visualized for better understanding. While there are proposals how ontology can be visualized [35—39] works on visualization of mapped standards are missing. Actually, visualization of mapped security standards could improve the identification of duplicated elements of standard; it could be used as a tool for progress analysis implementing the standards, etc. Therefore we suggest method for visualizing of mapped standards using graph theory. The most intuitive method for standard visualization is usage of graphs. The concept of standard can be represented as graph node, while relations between concepts can be displayed as edges. Thus, existing security standards have sufficient number of concepts and relationships between them to make the graph hard to read to the end users. Therefore, we suggest using the tree structure for representation of the concepts of standard and to display inheritance links to represent only the main structure. Other links could be analyzed by viewing detailed information in relation to certain node.

Some node notation modifications are proposed to make the standard tree more representative for viewing mapped standards:
1) In the middle of a node, a code or an abbreviation of the standard node is represented.
2) The width of stroke for a node defines how many standards have an analogue for this control (the number of mapped standards, and not the number of mapped nodes in other standards).
3) The pattern of stroke for a node defines what type of match the node has with nodes of other standards (if node of other standard matches the node partially – the value is 1; if node of other standard matches the node fully – the value is 2; if node of other standard is redundant – the value is 3):
   a) The length of dash defines the maximum match value.
   b) The length of space defines the minimum match value.

Additional information, such as full description of the node, details of controls matching etc. should be represented separately for each of the nodes. A small example of integrated standard tree notation usage is presented in figure 2. It can be noticed that nodes A-1, A-2, A-9, A-3, A-10 and A-7 have no matches in other standards while nodes A-4, A-11, A-5 and A-8 have one match, and nodes A-6 and A-12 have two matches with other standards. This information can be retrieved by the width of node stroke.

By the pattern on stroke we can find out what type of matches these nodes have. For example, node A-12 matches two other standards, while the explanation window of this node shows that there are 3 relations to controls of other standards, where one of them is redundant and two of them match the node. The pattern of stroke for this node summarizes the information and shows that there
are at least one redundant node and one matching node in the mapping list of this node. If there were no ability to view detailed list of matches of specific node notation legend, it would be necessary to provide using the software.

One problem can come up creating the standard tree because of concepts ability to belong to more than one parent node in standard (For example, in figure 2, nodes A-5 and A-7 are listed in multiple places of the standard). Such situation is acceptable in relation to graph; however, the tree structure does not allow it. For solving this problem, we use copies of node making association links between the copy and real node. This solves the problem of multiple parents, while information of the copied node can be replaced by information of the original node in rendering of the standard tree.

To map standard to ontology two different techniques can be used:
1) To map the same nodes in standard and ontology. If the same node is used both in class hierarchy of standard and ontology, there is a full match between them.
2) To map nodes in standard and ontology by matching node properties. If a node in standard has the same properties as different node in ontology, these nodes can be mapped together. There can be three types of matches in this situation:
   a) Partial mapping if standard node has just some of the properties of standard node.
   b) Full mapping if standard node has all the same properties as standard node.
   c) Redundant mapping if standard node has all the same properties as standard node, and some more.

To define standard or ontology tree, all nodes should have a short code for representation, full description of a list of the properties it has, a list of links to copies of the node, and other useful fields for tracing relations between nodes and standards as well as for visualization. The data structure for storage of security standard or ontology tree that we used is represented in figure 3.

![Diagram](image)

**Fig. 3 Main data structure for storage of mapped security standard**

Proposed a data structure can be used for graphical standard tree generation and management. Developing a prototype for adaptive mapping of security standards (see Fig. 2), we used Java programming language, Apache Jena framework for building class hierarchy from OWL file of The Security Ontology and Java Universal

79
Network/Graph (JUNG) framework for graphical standard of the tree generation and management. The software has 3 main functions:


2) To map ISO27001 and Grundschutz controls to Security Ontology automatically by the same subclasses and properties used in it.

3) To visualize the standard class hierarchy representing the mapping information.

However, the software can be extended to map different security standards, as well as to provide additional information on the used ontology and mapped standards.

6 Analysis of Security Standards using Adaptive Mapping of Security Ontologies

S. Fenz extended Security Ontology by adding ISO27001 standard and Grundschutz Manual concepts to it. However, there is no deep analysis on the mapping that S. Fenz did in the Security Ontology. Therefore, we used created tool for adaptive mapping of security standards to analyze properties of Security Ontology and ISO27001 and Grundschutz mapping for the purpose.

Flat structure of ISO27001 and Grundschutz in the Security Ontology was observed during the development of owl file parsing code to represent its class hierarchy. All controls of ISO27001 are presented as subclasses of one class called “ISO27001 Controls” while links to certain objectives are realized through restrictions on property isoControl_has_ISOObjective (relation between ISO categories and objectives is similarly comprehended). Meanwhile, Grundschutz Manual has only one level class hierarchy. Therefore we parsed the class hierarchy according to names of classes, for example, class named “M_3_5” was separated into parent class “M_3” and child class M_3_5”.

The analysis of Security Ontology proposed by S. Fenz showed that ontology can be a little bit uncomfortable to view as tree because some of nodes have up to 114 sub nodes. Therefore, in the future the structure of the ontology could be improved for graphical viewing.

The ISO27001 and Grundschutz standards have more representative class hierarchy but S. Fenz added additional nodes to the original structure of ISO27001 and Grundschutz standard to realize the mapping to ontology using sub nodes. Therefore, for mapping ISO27001 and Grundschutz standards to Security Ontology there were parsed 307 mapping links between ontology and certain standard. 278 (64 in ISO27001 standard, and 214 in Grundschutz standard) mapping links were realized by using sub classes of ontology, and 29 (11 in ISO27001 standard, and 18 in Grundschutz standard) by assigning the same properties to classes as ontology classes have. Therefore, the mapping is done on the deepest level, and only categories of standards are not mapped.
Analyzing which parts of Security Ontology are mapped to ISO27001 and Grundschutz security standards, it was noted that all deepest level categories were mapped in Control (117 out of 117) and Organization (96 out of 96) classes; and small part of the deepest level Asset classes were mapped (3 out of 148), and none of Vulnerability and Threat classes were mapped using the chosen security standards. This shows that ISO27001 and Grundschutz standards are concentrated on organization structure and used controls, while no deep analysis on how these controls relate to the organization assets, potential vulnerabilities and threats is done by S. Fenz in the extension of Security Ontology.

Mapping ISO27001 standard, some categories, objectives and controls were not detailed by adding appropriate sub classes of Security ontologies; however, these which were detailed have matches both in ontology and Grundschutz Manual. Grundschutz Manual has 47 classes used both in ISO27001 standard and security ontology, while 84 of them were linked only to the security ontology. This shows that Grundschutz Manual is mapped in a wider domain to present different content of its controls.

7 Conclusions and Future Work

In this paper, we presented an adaptive mapping of security standards where ontology is used for mapping multiple security standards, which can reduce the need of standard mapping documents between different security standards. This solution can be useful for detailing certain controls of security standards in wider domain; nevertheless, it depends on the description of security standards in the base ontology.

Visual representation of the security standard can be useful to understand of the structure of standard, therefore, we suggest using tree structure for representation of standard nodes and adding additional node notation to present more information about the mapping to other standards as well. The notation allows easier tracing of related nodes in different standard; however, in the future it can be improved by adding node colors or other notation to represent conflicts between some nodes, node importance to organization, etc.

A tool for adaptive mapping of security standards was developed to implement the model of ontology-based standard mapping and visualization of mapped standards. It allows visualization of chosen security standard where relations between security standards are visualized and generated automatically by the mapping information in S. Fenz’s Security Ontology. This proves the practical usage of proposed model, and can be extended including new security standards in S. Fenz’s Security Ontology.

Security Ontology proposed by S. Fenz et al. allows mapping of different security standards. ISO27001 and Grundschutz standards are represented in this ontology, and can be used for adaptive mapping of the security standards. However, the base view for the adaptive mapping should be chosen as ISO27001 and Grundschutz standard as the class structure of Security Ontology is not very representative because of the big number of sub classes in it. In the future, these classes could be restructured to make the ontology more representative for adaptive mapping.

References


