Visualization of Mapped Security Standards for Analysis and Use Optimisation

Simona Ramanauskaitė, Dmitrij Olifer, Nikolaj Goranin, Antanas Čenys, and Lukas Radvilavičius

***Abstract*—There are many security standards which the company can use. 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 while implementing these security requirements.**

In this paper we analyze existing solutions for standard harmonization, describe concepts of adaptive mapping and present new ideas for visualization of mapped security standards. These ideas were integrated into developed tool to visualize mapped security standards.

***Index Terms*—Chord diagram, graph, mapping standard, visualization.**

I. 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.

Manuscript received December 9, 2013; revised February 2, 2014. 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.

S. Ramanauskaitė, D. Olifer, N. Goranin, A. Čenys, and L. Radvilavičius are with the Vilnius Gediminas Technical University, Vilnius, LT-10223 Lithuania (e-mail: {simona.ramanauskaite, dmitrif.olifer, nikolaj.goranin, antanas.cenys, lukas.radvilavicius}@vgtu.lt).

II. Harmonization of Security 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 [1]. 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 [2]:

- 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.
- 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.
- Adaptive mapping integrates selected standards automatically by using mapping documents for the selected standard. To reduce the complexity and necessity of many mapping documents one base ontology is used to map all the other standards. This would require just as many mapping documents as there are standards that have to be integrated.
- 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 mentioned harmonization techniques have different properties and usage area (see Table I). However adaptive mapping solution combines all other harmonization techniques and allows using of all the benefits it gives:

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

TABLE I: COMPARISON OF PROPERTIES OF DIFFERENT STANDARD HARMONIZATION TECHNIQUES

Technique	Number of documents for harmonizing n standards	Number of records for harmonizing n standards in one document	Usage examples
Semantic compatibility	From 1 to $n(n\text{-}1)/2$	Same as number of synonyms in these standards	ISO standard family
Mapping	From 1 to $n(n\text{-}1)$	Up to m_1+m_2, where m_1 is a number of controls in first standard and m_2 – in second	[3], [4]
Adaptive mapping	n	Up to m, where m is a number of controls in the standard	[5]
Integration	1	Up to $\sum m_i$, where m_i is a number of controls in i-th standard	[6], [7]

Therefore for developement of interactive security standards mapping tool we use an adaptive mapping. We mapped ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621 security standards to the proposed security ontology. Mapping between two or more standards can be generated automatically according to the similarity of link in standard-ontology mapping. For example in Fig. 1 a control in ISO 27001 (A.8.3.3 Removal of access righ...) and control in PCI DSS (PCI DSS 8 5 4) standards have identical links with security ontology, therefore the full match relation exists between these two controls of different standards. 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 defines situations, where vulnerability of no deactivation of 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 in certain level, therefore a weeker link exists between these controls.

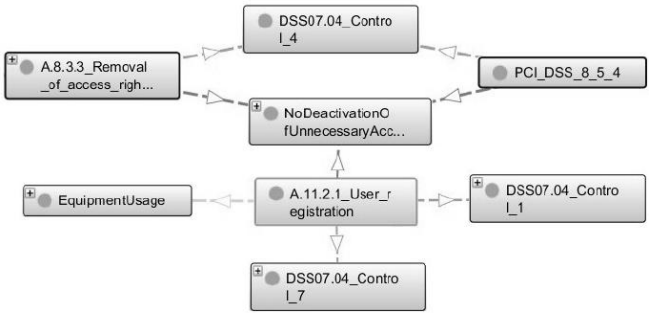

Fig. 1. Example of standard mapping trough ontology.

Full adaptive mapping is possible when all controls and concepts of these standards are mapped to the security standard.

III. VISUALIZATION OF MAPPPED SECURITY STANDARDS

A. Visualization of Overlapping or Simillar Networks

A usage of mapped security standards can be simplified, if intuitive and informative graphical user interface is designed to analyze mapped standards. Visualizations are tools used to express both the structure of the data and cognitive mapping of the user observing and interacting with this data [8]. By default one security standard is ussually presented as graph or tree structure and in some cases, cliques are derived from these graphs (networks or subnetworks). While mapping information between two or more standards is presented as table, where controls of one standard are presented in one collumn, while controls of other standard are rpesented in another collumn. The mapping information is obtained by identifieing rows with controls in both standards, collumns.

We could not found any methods or tools for graphical presentation of mapped security standards, however some visualization ideas for overlapping or simillar networks in other areas than standard mapping exists, which can be adopted for visualization of standard mapping.

David CY Fung *et al.* proposed to use 2.5D visualisation of overlapping biological networks [9] where three parallel two dimensional planes are placed in three dimensions to represent overlapping networks: one for each network (the top and the bottom planes) and one for the overlapping part (in the middle plane) see Fig. 2. This aproach allowe identifying overlapped nodes very visually, but has some limitations as more than two networks or standards would be difficult to visualize as links from one standards to another can cross other standards and be confused with standard nodes between these two.

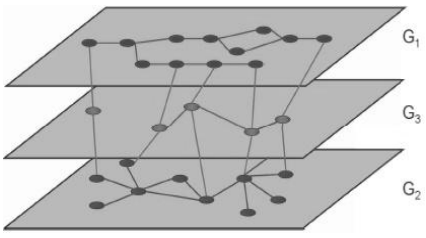

Fig. 2. Idea of 2.5D visualisation of overlapping biological networks [9].

Patrick M. Dudas *et al.* proposes a semi-supervised approach for visualizing and manipulating overlapping communities, where 3D model is used [10]. This model takes into account the potential number of edges between nodes, therefore they reduced overlap and the number of connections by creating a single vertex for each clique as a marker for the entire clique. Using this idea for visualization of mapped security standards, mapped nodes would be presented in smaller clique as one, combined node. This solution helps to observe simillar controls in different standards, however standard node hierarchy is not presented in this solution (see Fig. 3).

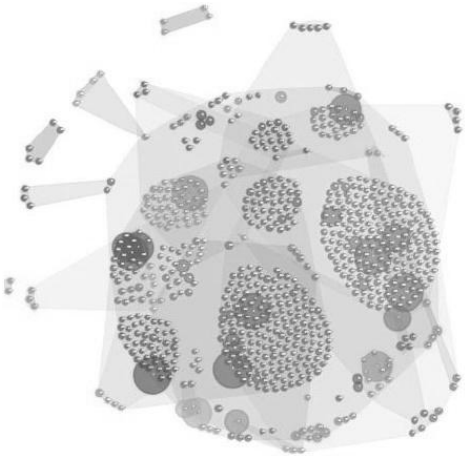

Fig. 3. Example of 3D visualization of overlapping communities by reducing the number of connections between standard nodes [10].

There are some examples, where overlapping in network is presented by other structures rather than graph or tree. Steve Horvath and Peter Langfelder for visualization of gene networks uses heatmap plot of the topological overlap matrix [11]. In the heatmap, rows and columns correspond to nodes, light colors represent low topological overlap, and progressively darker orange and red colors represent higher topological overlap (see Fig. 4).

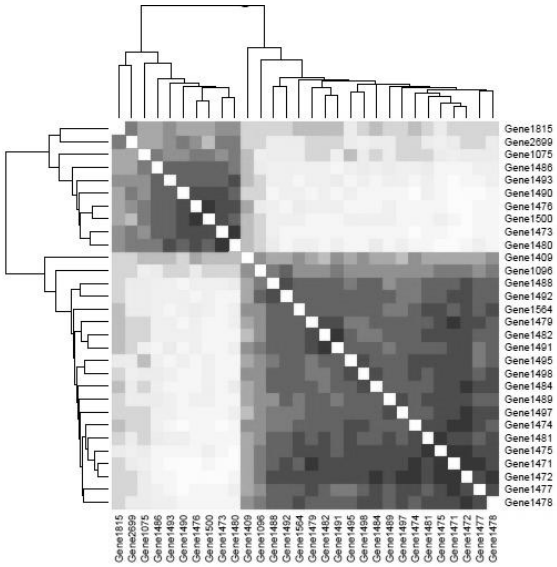

Fig. 4. Example of the heatmap plot usage for overlapping matrix [11].

This visualization method can be used to present mapping information of security standards, however the heatmap plot can visualize only overlapping of two standards.

Other idea, which could be adopted for more than 2 standard visualization is described in A. Telea and O. Ersoy paper "Image-Based Edge Bundles: Simplified Visualization of Large Graphs" [12]. These authors combine the advantages of edge bundles with a bundle-centric simplified visual representation of a graph's structure. In Fig. 5 a simple list of nodes is presented, however a needed number of standards can be placed around the circle with all the nodes.

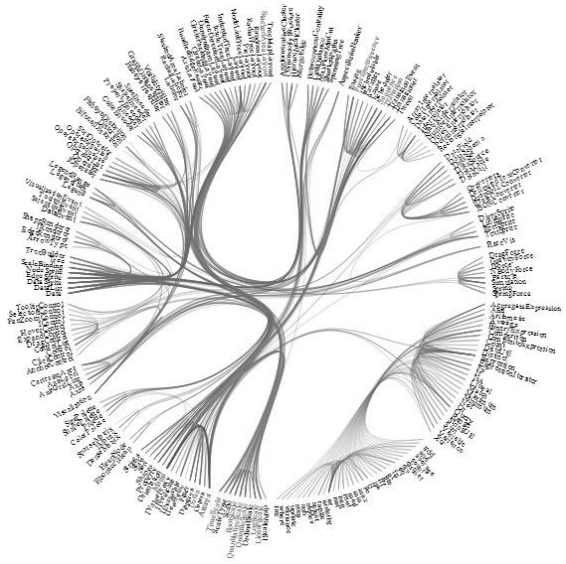

Fig. 5. Example of Chord diagram [12].

B. Our Solutions for Visualization of Mapped Standards

If standard structure have to be presented we suggest using the tree (specific kind of graph) structure for representation of concepts of standard and to display inheritance links to represent only the main structure. Other links could be presented trough node notation and analyzed by viewing detailed information of certain node.

Some node notation modifications are proposed to make the standard tree more representative for viewing mapped standards:

- The width of stoke 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).
- 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):

1) The length of dash defines the maximum match value.
2) 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 Fig. 6. 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.

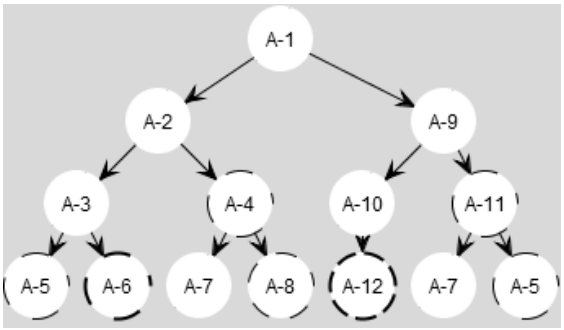

Fig. 6. Example of proposed standard mapping visualization, using graph structure.

As security standards has many controlls (nodes in the tree) and this type of visualization of mapped standards requires big viewing area to present all the structure of the standard. As well other disadvangate of this visualization is that only one standard structure can be viewed at once (user chooses which standard should be viewed). Therefore only mapping of one standard to other standards can be viewed and there will be no full information how other standards are mapped to each other.

To visualize the full mapping information with Chord, centric diagrams are more appropriate, as all standard nodes can be viewed at once. A big number of links between nodes are grouped to increase the abstraction level, however more detailed information can be extracted including interactive explanations, highlights, etc. The biggest disadvantage of this type of mapped standard visualization is the lack of standard structure presentation. However we do improve the visualization by adding the standard structures in the outer border of the circle. This increases the size of the diagram, however both full mapping information and standard structures can be visualized as the same time see Fig 7.

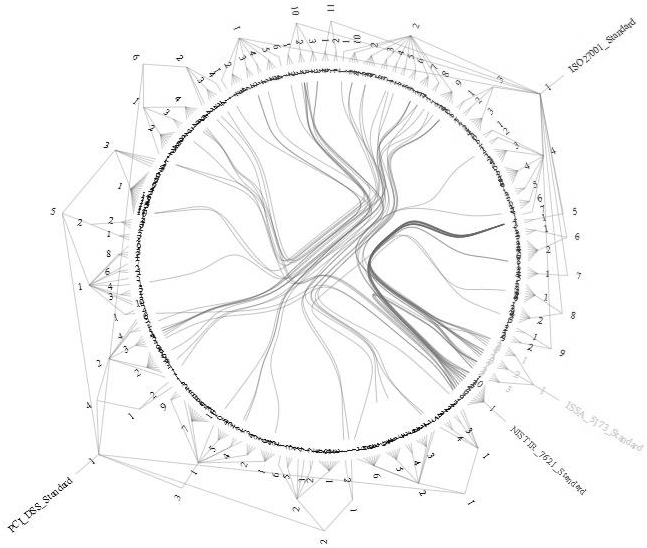

Fig. 7. Example of the Chord diagram for standard mapping visualization.

IV. Conclutions

Both of proposed visualization methods were implemented in our adaptive mapping of security standard (AMSS) tool where 4 standards (ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621) were mapped using proposed security ontology. The usage of both of these standards mapping visualization methods showed that:

1) Chord diagram is very helpfull when main trends in standard similarities have to be esmitated or summarized as the width of mapping links ilustrates how ofted certain control is mapped to other controls. As well this visualization method helps to identify unmapped controls as "blank areas" with no mapping connections are seen.
2) The improvement of Chord diagram to add the hierachy of standard nodes was usefull, as now the Chord diagram can provide all most the same information as graph structure diagram.
3) Graph structure visualization is more suitable when one security standard have to be analyzed and information is needed on how controls of this standard maches controls in another standards, what type of maching exists between those two nodes etc.

References

[1] J. Siviy, P. Kirwan, L. Marino, and J. Morley, "The value of harmonization multiple improvement technologies: A process improvement professional's view," Software Engineering Institute, March 2008.
[2] A. Souag, C. Salinesi, and I. Comyn-Wattiau, "Ontologies for security requirements: A literature survey and classification," in *Advanced Information Systems Engineering Workshops Lecture Notes in Business Information Processing*, vol. 112, 2012, pp. 61-69.
[3] M. Hofherr. Mapping ISO 27001 <> PCI?DSS 2.0. [Online]. Available: http://www.forinsect.com/downloads/Mapping-ISO27001-PCI_public.pdf
[4] C. Pardo, F. J. Pino, F. Garcia, M. Piattini, and M. T. Baldassarre, "An ontology for the harmonization of multiple standards and models," *Computer Standards & Interfaces*, vol. 34, issue 1, pp. 48-59, January 2012.
[5] S. Ramanauskaite, D. Olifer, N. Goranin, and A. Cenys, "Security ontology for adaptive mapping of security standards," *International Journal of Computers, Communications & Control*, ISSN 1841-9844; ISSN-L 1841-9836, 2013.
[6] S. Ahuja. (2009). Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework. [Online]. Available: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-21.pdf
[7] IT Governance Institute, Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, 2008.
[8] A. Tversky and I. Simonson, "Context-dependent preferences," *Management Science*, vol. 39, pp. 1179-1189, 1993.
[9] D. C. Y. Fung, S. H. Hong, D. Koschutzki, F. Schreiber, and K. Xu, 2.5D "Visualisation of overlapping biological networks," *Journal of Integrative Bioinformatics*, vol. 5, no. 1, pp. 90, 2008
[10] P. M. Dudas, M. de Jongh, and P. Brusilovsky, "A semi-supervised approach to visualizing and manipulating overlapping communities," in *Proc. 17th International Conference on Information Visualisation*, 2013.
[11] S. Horvat and P. Langfelder, Visualization of gene networks, Tutorial for the WGCNA package for R: III. Using simulated data to evaluate different module detection methods and gene screening approaches, 2011.
[12] A. Telea and O. Ersoy, "Image-based edge bundles: Simplified visualization of large graphs," in *Proc. Eurographics/ IEEE-VGTC Symposium on Visualization 2010*, vol. 29, no. 3, 2010.

Simona Ramanauskaitė was born on December 18, 1983. She received her M.Sc. in Informatics in 2008 and PhD in Informatics Engineering in 2012 from Vilnius Gediminas Technical University. Currently she is working as an assoc. prof. at Siauliai University, Department of Information Technology and as a researcher at Vilnius Gediminas Technical University, Information System Security Laboratory. Her current research interests include different aspects of Information Security.

Dmitrij Olifer was born on October 7, 1982. He received master degree in engineering informatics in 2006. From 2010, He was a member of ISACA organization and during 2012, he was approved as a certified information security manager. Dmitrij Olifer has job experience as a system administrator, information security specialist in Lithuanian Police department. He participates in Europol Security meetings as a lithuanian police member. Currently he works as Security and Compliance specialist in Barclays Lithuanian Technology Centre, and as a researcher at Vilnius Gediminas Technical University, Information System Security Laboratory.

Nikolaj Goranin was born on November 26, 1981. He received master degree in engineering informatics in 2006, performed training at Joint Research Center IPSC Cyber Security laboratory in 2004 and received a PhD degree at Vilnius Gediminas Technical University (VGTU) in 2010. Nikolaj Goranin has a job experience as a system administrator, FP6 and EU structural funds project coordinator. Currently works as an Assoc. Prof. at VGTU IT security laboratory and as a Chief Information Security Officer at level 1 (according to VISA classification) service provider (responsible for PCI DSS compliance and certification).

Antanas Čenys was born on December 7, 1955. In 1978, he graduated from Department of Physics at Vilnius University. He defended Ph.D. thesis on semiconductor physics in 1983 and habilitation thesis on nonlinear dynamics in 1999. Antanas Čenys started his research career at Semiconductor Physics Institute (SPI) in 1978 and became chief research associate and chairman of the Senate of SPI in 2001. Now Antanas Čenys is a professor at Information Systems Department at Vilnius Gediminas Technical University (VGTU). In 2006 he established and leading IT security laboratory at VGTU. From 2008 he was Dean of Faculty of Fundamental Sciences and in 2011 became vice-rector for research.

Prof. Antanas Čenys worked as visiting researcher at NORDITA (Denmark), KFA Julich (Germany), Ecole Normale Superrieur in (France), EU JRC Institute of Perspective Technological Studies. He participated and coordinated more than 10 EC and NATO research projects and published more than 150 scientific publications. In 1999 he received Lithuanian National Award of Science.

Lukas Radvilavičius was born on January 3, 1982. He received master degree in engineering informatics in 2006, received a PhD degree at Vilnius Gediminas Technical University (VGTU) in 2013. Lukas Radvilavicius has a job experience as a system administrator, EU structural funds project coordinator. Currently he works as a researcher at VGTU Information System Security Laboratory. and as a chief executive officer at information technology development company.