Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Toward web-based information security knowledge sharing

*Daniel Feledi**, *Stefan Fenz*, *Lukas Lechner*

Vienna University of Technology and SBA Research, Vienna, Austria

Keywords:
Information security
Knowledge sharing
Web-Protégé
Security ontology
Web-based collaboration

ABSTRACT

Today IT security professionals are working hard to keep a high security standard for their information systems. In doing so, they often face similar problems, for which they have to create appropriate solutions. An exchange of knowledge between experts would be desirable in order to prevent developing always the same solutions by independent persons. Such an exchange could also lead to solutions of higher quality, as existing approaches could be advanced, instead of always reinventing the security wheel.

This paper examines how information security knowledge can be shared between different organizations on the basis of a web portal utilizing Web-Protégé. It can be shown that through the use of ontologies the domain of information security can be modeled and stored in a human- and a machine-readable format, enabling both human editing and automation (e.g. for risk calculations). The evaluation of the web portal has shown that the most important challenge a tool for knowledge sharing has to face is the aspect of motivating users to participate in a knowledge exchange.

Results from the evaluation have been used to further develop and enhance the web portal by implementing additional facilitating features. These features include a credit system, which rewards users for contributions, as well as the ability to select multiple entities, improving the system's usability.

1. Introduction

Nowadays[1] many organizations and companies rely heavily on information systems and have to ensure that they work properly at any given time. Additionally Information and Communication Technologies (ICTs) have become an important part of everyday life. In some areas, ICT systems and services are an essential part of economy and society, for example as part of critical information infrastructures where "*their disruption or destruction would have a serious impact on vital societal functions* (European Network and Information Security Agency, 2009)"

In a study (McAfee Inc, 2009) conducted in 2008 it was found that information security breaches caused companies worldwide to lose more than $1 trillion (708 billion) within one year. Often, security breaches were performed by insiders, especially by former employees. Cyber criminals are also increasing their efforts to steal sensitive data and information.

The study found that criminals will increase their efforts to create sophisticated schemes which take advantage of employees, new technologies and software vulnerabilities. Criminals will also assemble detailed profiles of executives and other high-level targets in order to utilize more effective spear phishing attacks.

When security breaches can have such dire consequences, both in financial and societal terms, securing the systems is of utmost importance. This applies both for the containment of

* *Corresponding author.*
E-mail addresses: feledi.daniel@gmail.com (D. Feledi), stefan.fenz@tuwien.ac.at (S. Fenz).

[1] Disclaimer: This paper is an extension of a conference paper published at ARES 2012 (Feledi and Fenz, 2012).

1363-4127/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.istr.2013.03.004

everyday risks such as failures of individual components and also for preventing malicious attacks from outside against the systems.

To be able to approach such challenges in a professional manner, experts have to collect knowledge on information security, about potential risks and to create own solutions to reduce them. Information security is usually defined as the protection and preservation of confidentiality, integrity and availability of information, though other properties such as authenticity, reliability etc. are also of concern (Glaser and Pallas, 2007).

Many of these situations occur on a regular basis. For this reason it would be of advantage to allow knowledge sharing between experts, so that the same solutions aren't created over and over again by different individuals. Such a sharing of knowledge could save valuable resources which could be used in more productive ways. Moreover, sharing could lead to solutions of higher quality, due to the fact that existing solutions are enhanced instead of similar solutions being developed all the time. Till now organizations are partly comparing solutions with other organizations, but there is no unifying system with a widespread basis which could support knowledge sharing in a formal and structured way. This paper will present a web portal based on Web-Protégé, aiming to offer a tool for structured sharing of information security knowledge.

1.1. *Motivation*

The research question this paper tries to answer is how web portal can be used to foster sharing of information security knowledge among organizations. The working hypothesis is that a tool can provide a central platform for participating organizations over which a sharing of knowledge can take place. This allows having more efficient and more structured cooperation than would be possible through classic channels like phone calls or e-mails. In the following sections we will discuss the functionality and the evaluation of a web portal based on Web-Protégé that aims to offer such a centralized platform.

2. Related research

The European Network and Information Security Agency (ENISA) has undertaken efforts to build the European Information Sharing and Alerting System (EISAS) (European Network and Information Security Agency, 2009), a pan-European network for information sharing. It was followed by different projects, for example the Framework for Information Sharing and Alerting (FISHA) (Kijewski, 2011). The main goal of these European projects is to raise the information level and the awareness of IT security issues among regular citizens and SMEs, while the shared information comes from different network security organizations. The captured knowledge is then distributed over a web portal that provides information for end users and shares the information with other members of the sharing network. One of the main differences between the FISHA initiative and the web portal presented in this paper is the formalization of the captured knowledge, achieved through the usage of an ontology. This can be advantageous when users want to use the knowledge for other purposes (e.g. risk management calculations), due to the available formal representation.

The advantages of using ontologies to capture the information security knowledge have also been suggested in other papers. Mace et al. (2010) suggest capturing information security knowledge in an ontology. This could be an appropriate mean to summarize different sources that influence security policies. By using an ontology approach to capture knowledge, information is formalized as a set of concepts, thus "*creating an agreed-upon vocabulary of IT-security knowledge. The interdependencies between fragments of such knowledge will be exposed, facilitating navigation across related information concepts.*" (Mace et al., 2010) The authors discuss their approach to create a web-based tool for collaborative ontology development for the domain of information security knowledge. They advocate collaboration as a mean to create a robust body of knowledge. As was described by Mace et al. (2010), collaboration is an integral part of the ontology development, since it allows several information security experts to capture, integrate, publish and share their knowledge with their peers and colleagues. Collaboration in the form of submitting, commenting on, and peer-reviewing the submitted knowledge, allows these domain experts to work toward reaching a consensus The authors identify main features they regard as essential for successful collaborative ontology development. "*These include synchronous/asynchronous communication; proposed content agreement policy; annotation of content and changes; content provenance; concurrency and version control; and personalized views of ontology content.*" (Mace et al., 2010).

Schumacher (2003) explains that the development of an security ontology allows automatization in the processing of security-related information and helps to clarify "inconsistencies" in the used terminology. The developed ontology contains core concepts and relations of the security domain with the primary objective to adopt standard names and definitions of security concepts.

Vorobiev and Bekmamedova (2010) also point to the fact that ontologies can provide the means for a common vocabulary, which would allow the exchange and effective communication of security related information. The motivation for this paper was the increasing number of distributed attacks which require a new kind of countermeasures. They argue that collaborative intrusion detection and defenses in distributed environments are needed to face this new kind of security threat. These security measures should have a common mechanism to share the collected knowledge about attacks and possible countermeasures.

Parkin et al. (2009) develop an information security ontology which aims to further the comprehension of human-behavioral factors as well as to maintain compliance with external standards, which allow organizations to demonstrate that their information is secured. One goal of the authors is to use the created ontology to inform the decision-making process, "*allowing security managers to account for the identifiable effects […] that information security mechanisms have upon individuals […]*" (Parkin et al., 2009) This should allow creating solutions that meet not only technical requirements for certain security problems, but also the usability requirements of employees, since it is necessary to consider both the impact of security mechanisms upon the workforce as well as their

reaction to those mechanisms. Taking the human-behavioral perspective into account can lead to a better acceptance of information security measures within the organization. The developed ontology captures assets, threats and vulnerabilities while including behavioral aspects; for example usability-oriented side effects of certain countermeasures can lead to new vulnerabilities.

Fenz and Ekelhart (2009) developed a security ontology representing domains such as threats, controls, assets and vulnerabilities in order to formalize information security knowledge. In Fenz et al. (2011) an information security knowledge management portal is presented, which uses Web-Protégé to enable collaborative editing of the knowledge captured in the underlying ontology. This web portal is the foundation for the work in this paper.

3. Collaborative web portal solution

The presented web portal is aiming to create a unified and machine-readable platform for information security knowledge sharing, enabling collaboration between users, helping them to understand and extend the underlying security ontology together. The knowledge captured in the ontology is dynamic in nature and should model current threats and vulnerabilities as well as up-to-date control mechanisms.

This approach is not restricted to a certain organization but tries to elevate the collaboration to a global level, crossing organizational and regional borders. Due to the collaborative nature of this approach, a single organization can reduce their costs at knowledge capturing and processing for information security compliance and risk management tasks, since the effort is divided among a larger number of participants.

The security ontology captures different concepts and interrelations within the information security domain. As shown in Fig. 1 above, the security ontology consists of several classes, of which the main classes will be described in the following.

3.1. Security ontology

1) The Asset Class: The term "asset" describes all the objects of an organization that generate some business value for the organization. Assets are endangered by threats and are exposed to vulnerabilities, but can also implement controls that mitigate these vulnerabilities.

"*The asset concept is categorized either as a tangible or an intangible asset. Typical subconcepts of intangible assets are data, role, software, or reputation. The data concept comprises meta-data on the knowledge of an organization. […] The role concept distinguishes between internal and external roles. Every physical person or organization is connected to one or more roles, which enables a flexible handling if those concepts are to be modeled as control implementations or threatened elements. […] In contrast to the data concept, the software concept has been introduced to provide an ontological structure for those virtual elements which only possess processing characteristics such as text editors, cryptosystems, or operating systems.*" (Fenz and Ekelhart, 2009) Tangible assets can be classified as movable (like computers, servers etc.) or immovable elements (like buildings etc.). "*The connections between the asset concepts allow an organization to ontologically map its entire physical infrastructure (including buildings, floors, rooms, computers, alarm systems, etc.).*" (Fenz and Ekelhart, 2009).

2) The Control Class: When implemented correctly, controls can mitigate vulnerabilities and protect the affected assets. Controls can have preventive, corrective, deterrent, recovery or detective measures, depending on the control type. Controls are derived from and correspond to best-practice and information security standard controls (e.g. ISO 27001).

"*Controls are implemented by asset concepts (e.g. fire extinguisher, software firewall, security guard, etc.). Complementary implementations (e.g. the need for smoke detector and a fire extinguishing system) as well as implementation alternatives (e.g. facial scan or fingerprint scan) are incorporated into the knowledge base.*" (Fenz and Ekelhart, 2009).

3) The Threat Class: A threat gives rise to or be a consequence of another threat and potentially endangers an organization's assets. For example the threat "Network attack" can give rise to "Malware affliction". Threats exploit vulnerabilities and are described by potential threat origins (human or natural origin) and threat sources (accidental or deliberate source). To model the threat's damage potential, each threat is connected to asset concepts through the "threatens" relation.

4) The Vulnerability Class: Vulnerabilities are exploited by threats and are in the form of physical, technical or

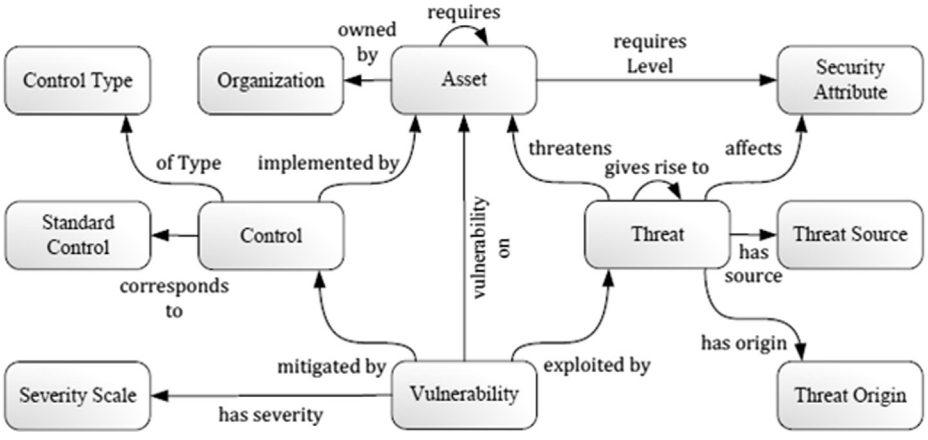

Fig. 1 – Security ontology (Fenz and Ekelhart, 2009, p.2).

administrative weaknesses. How severe an exploit can be is determined by the severity scale (high, medium, and low). This rating enables a machine to interpret the significance of the vulnerability. Vulnerabilities are bound to assets that take damage when a vulnerability is exploited.

3.2. *Web portal*

In order to enable collaborative, web based editing on the security ontology, a web portal based on Web-Protégé was created (see Fig. 2). In the following section a short introduction to the web portal will be given.

The browser based solution was chosen in order to make ontologies more accessible for users without the need to install software. Moreover with the ability to customize the interface it is possible to create useful environments for users who are not ontology experts. A customized version of Web-Protégé was created to enable information security knowledge sharing in the following domains: threats, vulnerabilities, controls, ISO 27001 controls and asset classes.

Web-Protégé was chosen because it offers an accessible and structured way to share knowledge on a high level among users without the requirement to be experts on ontologies. Moreover it enables registered users to edit, discuss and agree on knowledge, thus supporting the creation of a community that steadily develops the collaborative ontology further for common benefit.

The system is based on a client-server architecture. On the server side the ontology is accessed through the Ontology API which contains methods for reading and writing OWL ontologies. Additionally the server part supports collaboration services, such as annotation of ontology components and change tracking. The server keeps track of the changes in the ontology as well as manages conflicts when different clients make changes to the same ontology. The ontology resides on a Collaborative Protg server, which provides support for collaboration such as simultaneous editing, transactions and operation atomicity. The task of the Web-Protg server is to manage the clients.

The server maintains a current version number for each ontology. When a change is made, the ontologys version number is incremented. At a set time interval the clients contact the server to get new changes which are then included in the clients internal model.

Threats are shown in a tab in the user interface. The tab contains several portlets such as the class tree portlet for the class “Threat” and a portlet listing the individual threats. Moreover another portlet shows the details of a selected threat. These details are a user defined label, comments, predecessor/successor threats and exploited vulnerabilities. Web-Protégé supports several collaboration features that allow users to discuss and annotate parts of the knowledge in the ontology. These annotations can also be found in a portlet for attached notes.

The home tab is the first tab that is shown to the user after the application is loaded. It contains a short introduction to the platform, a portlet showing the last changes in the ontology and a portlet showing watched entities for logged-in users.

The other tabs are composed of similar portlets like the threats tab, but adjusted for the respective domain (vulnerability, control etc.)

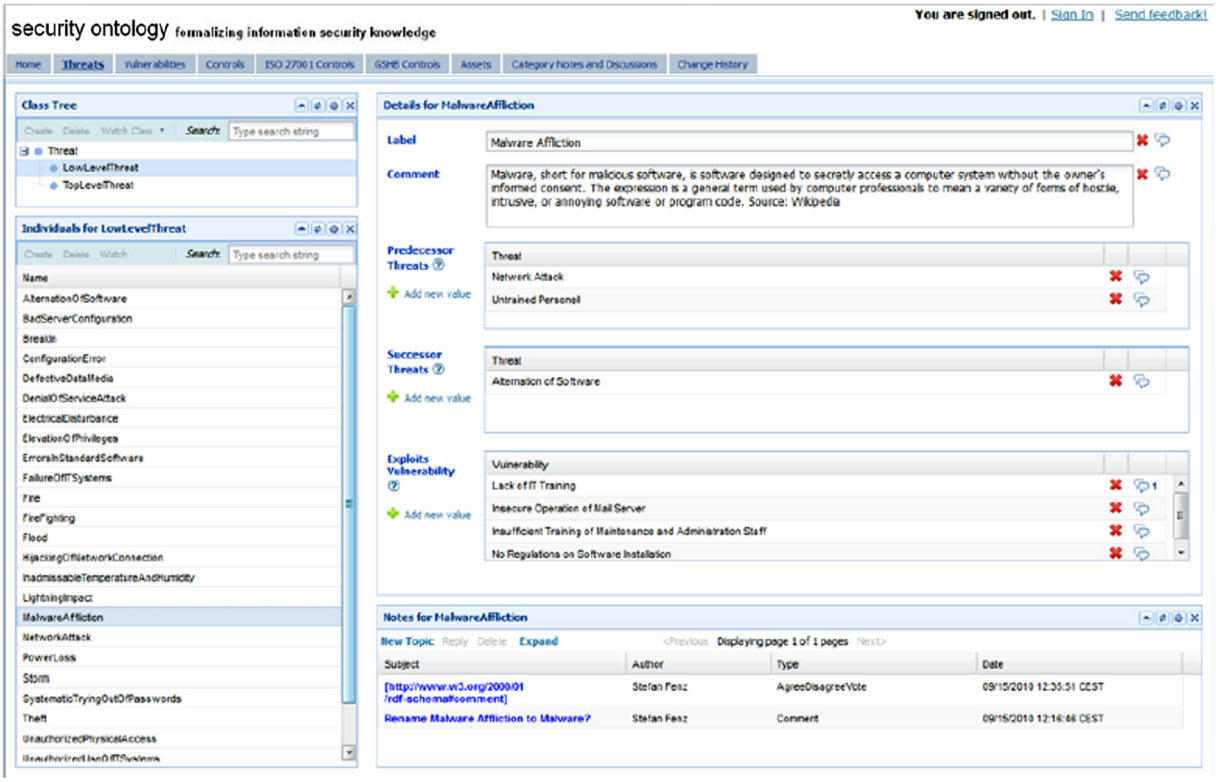

Fig. 2 – Screenshot of the web portal.

3.3. *Identified challenges*

In a preliminary evaluation of the web portal several challenges have been identified that had to be addressed. Among these were the missing possibility to connect existing individuals from the ontology, the lacking support for multiple languages and the limited options to send user feedback. Another missing feature was the definition of the severity of vulnerabilities, which is important in order to assess the impact of a vulnerability.

These challenges were addressed by the implementation of several extensions, which will be described in the following section.

3.4. *Extensions*

The basic extensions include the option to connect threats, connect vulnerabilities with threats and to use user defined labels to describe entities rather than using internal identifiers. These extensions should improve the usability and general functionality of the web portal.

Attributes such as threat source, threat origin, security attribute and control type were incorporated in order to improve the expressiveness of the ontology and to give users more options to describe threats or controls.

A feedback widget was implemented in order to offer the community an opportunity to voice their impressions and opinions, contributing to further development and improvement of the web portal and the security ontology.

The feature to support multiple languages was implemented in order to attract users from different countries and regions, enabling them to capture and discuss information security knowledge in their own languages. Presenting the same content in different languages may support sharing initiatives aligned along national or regional lines, making experts possibly more comfortable at sharing their knowledge.

The export feature was implemented to serve as an incentive for participants, since users expect to receive benefits from participating in a knowledge exchange. Therefore, offering them an option to export the collected knowledge from the web portal can be used as an incentive, allowing them to use the ontology within their own system without causing additional costs. Based on the level of participation of users, they can export the ontology as a file that can be imported into a local installation of Protégé, enabling users to customize the ontology to suit their own needs.

4. Evaluation

4.1. *Methodology*

For the purpose of evaluating the implemented functionality of the security ontology web portal, an evaluation process consisting of multiple phases was conducted. The goal of this process was on the one hand to review the usability of the web portal functions and on the other hand to assess if the tool can support information security knowledge sharing among information security experts.

For the evaluation we selected three experts with at least five years of information security expertise who should complete the evaluation phases independently. The evaluation process had a total duration of about 6 h, during which the execution of the assignments was observed and following their completion a structured interview was conducted to receive feedback.

Expert 1 (IS1) is an IT and security specialist with more than 5 years of professional experience in the field. The organization he is working for is a SME with a special focus on secure software development. Expert 2 (IS2) is a security specialist with 5 years of experience and is working in the IT security consulting sector. Expert 3 (IS3) works as a security specialist at a small-sized Austrian enterprise which is specialized on secure software development and security consulting.

The evaluation process is structured in three phases:

1) Phase 1: Within the first phase we introduced the participants to the security ontology and to the corresponding web portal. This introduction covers (i) the general purpose of the security ontology, (ii) an overview of the captured concepts, (iii) and a general overview of the main functions of the web portal.

2) Phase 2: Within the second phase we gave three assignments to the participants (adding new knowledge, editing existing knowledge, and exporting knowledge). Only a brief introduction to the web portal was given to evaluate how intuitive the interface is. The execution of the assignments was monitored in order to observe the participants' behavior and list any noticeable issues.

a) Assignment 1: The first assignment should help to get familiar with the web portal. As a first step the user should login with a provided test account. Then he should select his preferred language in the user settings. After this is done, the participant should take one threat or vulnerability and add additional knowledge to the existing one by editing the commentaries in his preferred language. Afterward the participant should get familiar with the function to connect threats and vulnerabilities by adding new relations between existing entities.

b) Assignment 2: In the second assignment, the user should create new threats and vulnerabilities. The vulnerabilities should be connected to controls that can mitigate it. The user should define a new control and create a relation between the vulnerability and the control. Threats should also be connected with predecessor and successor threats were applicable (for example "Data Loss" as a successor threat to "Untrained personnel"). Each new entity should be described with a label and describing commentary in the preferred language selected in the user settings.

c) Assignment 3: As the final assignment participants should use the export function on the home tab to export the ontology into an OWL file. Afterward the user should load the OWL file into a local ontology project in Protégé.

3) Phase 3: Within the third phase we gathered user impressions and opinions about the web portal by structured and open questionnaires. Some of the questions were:

- How easy or difficult was it to complete the assignments?
- How long did it take to complete them? Was the time appropriate or do you feel it took too long?

- Do you think that there is a way to complete the assignments more efficiently? If so, what are your suggestions?
- Was the structure of the security ontology clear?
- Could you benefit from using such a tool in your every day work?
- Do you think that the web portal offers you enough functions to express your knowledge on the subject? Or are you missing tools that could enhance the expressiveness?
- Would you contribute your own knowledge to this or a similar web portal? If not, please explain

4.2. *Results*

After performing the given assignments, the participants were asked about their impressions and opinions.

a) On the assignment tasks: On the one hand IS1 felt that the time it took to complete the assignments was appropriate and that the web portal offered the necessary means to complete them. On the other hand IS1 pointed out that ambiguities in the used terminology made it difficult to find the best way to represent the knowledge. Especially defining the predecessor or successor threats was complex, because the direct or indirect dependencies and relations are not visible. IS1 said that it is not clear on what level a relationship should be described, for certain threats can result indirectly from another threat, which makes the modeling process overly complex.

IS2 thought that the assignments given were not too complicated, but entering the required knowledge was too much effort. It takes too much time to enter knowledge and to determine if certain entities already have existing entries.

For IS3 performing the assignments was not too difficult, though he would have liked more tooltips to explain certain functions, for example for the exploitation degree of the threat–vulnerability relation or for the tools buttons of portal widgets.

b) On the ontology: When IS1 tried to select multiple entities from the IndividualsListPortlet in order to add new relations, this was not possible. IS1 thought that it would be very useful to add several entities at once, so that the user does not have to repeat the same steps over and over again.

IS2 criticized that it is possible to define a threat source (e.g. deliberate or accidental) for top level threats, where according to his opinion such a definition is too restricting. The same goes for security attributes (e.g. confidentiality, integrity, …) for the low level threats, because they usually can affect several attributes and cannot be restricted to one.

Another point addressed by IS2 was the possibility to define a low level threat as a successor to a top level threat, which is wrong from a modeling perspective. IS2 also brought up the issue of the clarity of the ontology and its depiction. The ontology is presented as a list of entities, which could become confusing with rising number of entities.

IS2 found that the current system lacks a mechanism that detects double entries, preventing users from adding knowledge and entities that are already present in the ontology. For example some kind of moderator could review the knowledge base, assuring that the represented knowledge meets the quality standards.

IS3 lacked the option to specify fixes to vulnerabilities or threats besides the ability to choose mitigating controls. IS3 said that he could describe those as comments, but this would make the purpose of comments too general. IS3 would have liked to have different options for comments, such as indicating further literature through references, website links etc.

c) On the usefulness of the web portal: When asked about his willingness to contribute his own knowledge to such a web portal, IS1 said that he would only contribute if he saw clear benefits from participating. The benefits of sharing knowledge should be communicated clearly to the users in order to motivate them to participate over a longer period.

IS1 also pointed out that the question of trust between the members is essential. Only if trust is present among the participants, people will contribute their knowledge. If members of the community do not have enough trust toward the other users, they will not share their knowledge in fear of revealing vulnerabilities which could lead to competitive disadvantages. On the other hand, if trust is given and sustained, people could benefit from sharing their knowledge with other experts.

IS2 had several issues with the current state of the web portal. One problem is that the target group is not clearly defined. According to his opinion, CISOs would not use the web portal due to the fact that it takes too much effort and time to add knowledge with no or little visible benefit. Especially the dynamic nature of the web portal makes it impractical for CISOs as a foundation for risk analysis.

A consultant in the field of information security would not use the portal because sharing his knowledge would take away his business foundation.

Another problem is that the benefit of participating is not clear, which is also an aspect of the not yet defined target group. This benefit has to be communicated clearly to motivate users to contribute their knowledge and to give them a justification for investing time and energy.

IS2 brought up the issue of “critical mass” of content which is required to attract users to the web portal and to make it useful for them.

When asked about being able to use a web portal, IS3 said that when he is working in risk management, he could use such a web portal as a reference. Regarding the contribution of his own knowledge, IS3 would require an existing, useful foundation before adding his own knowledge.

IS3 thought that the web portal could support the exchange of security knowledge between experts of different organizations, where these experts contribute and consummate knowledge at the same time. The tool could also be useful as a work of reference where current threats and vulnerabilities can be looked up.

Regarding the question about editing contributions of other users, IS3 said that he would rather not edit knowledge contributed by others, but would want to contact the user and send him suggestions. This would allow discussing a topic before a user could edit and possibly delete knowledge, adding a layer of security, preventing legit knowledge from being deleted. Alternatively IS3 suggested that an additional authority could check the submitted changes and give clearance if the contribution is valuable.

d) On the portal layout and functionality: IS1 had several suggestions regarding the efficiency of the web portal. IS1 missed the visibility of the selected language in the user settings

menu, which made it clear to the user which language was selected.

IS1 also pointed out, that it would be helpful to be able to navigate to different entities by double clicking on them, for example on a vulnerability that is connected to a threat.

IS1 also found that some buttons were unnecessary and distracting and should be removed from certain parts of the user interface. Regarding the layout of the web portal, IS1 thought that it was lucid and clear, but would have wished the export widget on the Home tab to be placed more prominently.

He also pointed out, that there are ambiguities in the terminology used in the web portal and therefore more explanation should be offered to the users. For example the terms "Low Level Threat" and "Top Level Threat" were not clear enough in order to understand what is meant by them. IS1 said that at least some information could be offered in form of tooltips as to explain shortly to the user what is meant by these terms.

Also more explanation about the export functionality would be useful to explain users what can be done with the exported OWL files. The Home tab could for example offer information about Protégé and how an ontology can be imported into the program.

Concerning the structure of the ontology, IS1 thought that the structure was clear, but mentioned that with time it could lose its clarity, when the ontology grows and the number of entities increases.

IS1 also pointed to the fact that no meta data could be represented with the web portal, which would make the captured knowledge more useful. In the current state threats could only be represented through labels, comments and the associated relationships to other entities, but no classification or other meta data can be defined.

IS2 said that in order to enhance the usability, more explanations and definitions are needed. In the current state there were many ambiguities regarding the terminology. Like IS1 before, IS2 also thought that "Low Level Threat" and "Top Level Threat" are not precise enough and should be explained in more detail to the user. Also the "exploitation degree", which describes the weight of the relation between a threat and a vulnerability, should be explained in more detail to the user, because misinterpretations are likely to happen.

Moreover IS2 mentioned several features that in his opinion would improve the usability, such as keyboard shortcuts for often used functions. Also IS2 lacked visible feedback to the user, showing which entities were already in relation to the current subject, in order to prevent double entries while adding relations to existing values. IS2 also said that it would be desirable to have the possibility to add new entities directly from the dialog used to add new relations between entities. This could help if an entity is not yet present in the knowledge base, but should be added and have a relation to the currently edited subject.

Regarding the efficiency of adding knowledge to the web portal, IS3 suggested to add labels automatically when a new entity is created. This removes one working step that is redundant in the creation process.

IS3 felt that the layout was intuitive, but suggested that some widgets could be collapsed when not needed right away. This would save some space on the web page that could be used to enlarge more important functions. For example the widget for notes on the threats tab could be collapsed while the details form could take more space.

IS3 had also suggestions regarding the search feature when adding predecessor or successor threats. He noticed that the search results include entities from the whole ontology and not just from the class tree that is currently being edited. Here it could help if relevant results are marked according to their respective classes. Another suggestion was related to the threat–vulnerability relation, which would be more efficient if the user could select the related entity together with the exploitation degree. This way users would not have to make the additional step of changing the degree separately. Regarding the exploitation degree IS3 also said that a little explanation in the user interface would help to understand the meaning of the degree better, for example built in as a tooltip.

4.3. *Conclusion*

The challenges that were derived from the evaluation are explained in this section, and have additionally been summarized in Table 1 along with their advantages.

It was shown, that especially the aspect of the target group has yet to be mapped out and clearly defined. This is important in order to be able to meet the requirements in a professional and adequate manner. Currently the target audience is too vaguely defined and therefore the actual benefits of using the web portal for information exchange cannot be clearly communicated.

Table 1 – Evaluation results.

Challenges	Advantages
Define clear target group	Tailor portal to suit needs of specific target group, making portal more attractive and useful
Enhance usability	Reduce the time needed to become acquainted with web portal
Address ambiguities in term selection	Helps users to grasp the meaning of ontology and web portal elements more quickly, enhancing the work experience
Rethink threat dependencies	Creating clear hierarchies and dependencies in the ontology reduces the risk of confusion and misunderstandings
Reaching critical mass	Reaching a critical mass of knowledge is crucial to attract new users to the web portal. Until it is reached use of the web portal offers little benefits
Quality assurance	Implementing a quality assurance supports trust building that is essential for knowledge sharing

The evaluation process has shown that there are several possible target groups, which include software vendors, consultants, researchers, modelers and CISOs. As one of the participants pointed out, a CISO could use the system in the process of making a risk analysis. In order to complete such an analysis, the CISO requires a stable and comprehensible basis for the assessment and calculation. The problem here is the collaborative and highly dynamic nature of the web portal, which possibly changes this basis frequently. Therefore the CISO lacks a profound basis for decision making and loses the benefits of a well structured approach. At the same time, if the knowledge base has a stable core that represents certified knowledge contained in best practices and standards, it can be useful as an information source for CISOs.

For example the threat tree could be managed centrally by moderators, so that on the one hand the quality of the represented knowledge is ensured and on the other hand the knowledge does not change as often as the rest of the entities in the ontology. Users could then for example add and edit vulnerabilities, while threats remain mostly stable. This could help CISOs somewhat so that they can rely on the modeled threat structures. It could also help if parts of the ontology are created and edited only by certified experts in order to guarantee the quality found in core parts.

Additionally CISOs would like to model their system environment in more detail than is possible in a collaborative tool, limiting the use of such a web portal further. CISOs especially require additional data about costs and consequences of vulnerabilities and countermeasures to author sound risk analyses.

IT security consultants are also a problematic target group. The problem is that in the context of a collaborative IT security ontology development, they lack the motivation to use such a web portal. Consultants primarily make money with their knowledge and would lose value if they contributed their assets without financial gain.

After successfully identifying the target group, the necessary level of detail has to be researched further so that the depth of knowledge can be adjusted to the final target group. Generally the benefits to the users have to be specified more clearly and a unique selling point has to be defined, so that organizations and individual users are motivated to contribute their knowledge to the ontology. The aspect of motivating users and organizations to participate actively in a knowledge exchange has to be researched further.

During the evaluation it was also indicated, that certain aspects of the ontology are difficult to model and offer too much ambiguity. One of the participants pointed out that the comprehensibility of the dependencies between the different entities is not always given. For instance threats can be predecessors or successors of other threats directly or indirectly, and this makes it difficult for users to clearly define these relations. Here it might be necessary to create clearer definitions in the ontology concept in order to be more precise in the modeling. Also the degree specified for relations between threats and vulnerabilities has to be explained further, as some participants found the meaning unclear. Explanations can be built in as tooltips directly into the user interface or in some kind of user manual that can be offered through the web portal.

The differentiation between low and top level threats has also proven to be difficult for some participants, since the manner of classification was not clear. An explanation should make the classification clearer to the users.

The participants generally thought that at least a small amount of time is needed to become acquainted with the web portal and to be able to use it effectively. Therefore further effort has to be put into the platform to enhance the user friendliness and to make the working experience more intuitive.

It was also pointed out that the representation of the ontology classes mainly in the form of lists is only lucid as long as the number of entities is manageable. With entities increasing in number, this method of presentation could become confusing and unclear. As an alternative, some kind of visual representation was suggested; the practicability of such an approach has yet to be checked. Another approach would be to divide the ontology into smaller parts that focus on certain business sectors in order to maintain the clarity and offer users the knowledge they require.

One of the more important points that have been found during the evaluation was the need to reach a “critical mass” of knowledge in order to attract new users to the web portal. As long as this level of information is not reached, people will not have the motivation to use the tool, because the value gained is lower than the effort that has to be put into it. This means that a certain level has to be reached right from the beginning, so that users immediately benefit from collaborating. Another important point is that a collaborative editing of the ontology is necessary in order to divide the effort of creating a knowledge base between a large number of participants, so that a balance is reached where everyone contributes a little and gains much in return.

In order to maintain the quality of the represented knowledge, it may be necessary to have moderators regularly review the presented knowledge and remove unnecessary or incorrect data. Alternatively the tool could be based on the principle of peer-reviews and the issue of quality assurance could be left in the hands of the user community. However, this would probably only work when the user community represents a trusted environment, else the acceptance of the captured knowledge could diminish.

5. Discussion

5.1. *Conclusion*

It was found that there are a number of incentives and barriers that encourage or hinder organizations to participate in information sharing. The most important incentives were of economic nature. Organizations want to benefit economically from sharing their knowledge with possible competitors. As was shown in a study by ENISA in 2010 (European Network and Information Security Agency, 2010) economic incentives are coming from cost savings, which can result from enhanced reaction times to threats, vulnerabilities and attacks, or from better capabilities at anticipating network failures.

Part of the motivation to share information is the expectation to receive knowledge of equal value. Additionally the

information that is shared must be relevant to participants' concerns to ensure that participants benefit from and maintain participation.

When participants are not convinced that they gain a benefit from sharing, they will not participate. Therefore, a strong emphasis has to be put on highlighting the possible benefits for organizations.

Another major incentive and at the same time one of the most powerful barrier is the matter of trust. Almost all studies observed that trust is a crucial factor in sharing information. Participants have to be able to trust their peers with whom they share crucial and sensitive information about the state of their information security and their knowledge on the subject. This trust has to be built over time and through personal relationships. Trust can also be based on the perception that other participants have similar desires and intentions.

When trust is misused and broken, it is very difficult to rebuild it. Therefore it is most important to ensure that misuse of shared information is as difficult as it can be and that it is penalized. When information sharing between organizations takes place in a structured manner, security measures have to be implemented to keep the information safe.

There is still much space for developing technical solutions for information security knowledge sharing. The web portal presented in this paper represents one approach to offer a collaborative platform for knowledge sharing. It was shown that through the use of ontologies the domain of information security can be modeled and stored in a human- and a machine-readable format, enabling both human editing and automation (e.g. for risk calculations).

Though the approach is useful, several challenges could be pointed out. One such challenge is to define the target group, which might consist for example of CISOs, IT researchers, marketing professionals or a mix of different positions and professions. Depending on which audience is targeted by the tool, different aspects have to be very carefully considered in order to find the most useful solutions for the group.

Another challenge is to find the appropriate degree of detail for modeling the information security domain. While having a low degree of detail may limit the potential use of a tool for experts, modeling too much detail could limit the benefits of a collaborative tool as well, which makes finding the balance a key factor for the usefulness of a tool.

Maintaining the overview of the modeled content was also found to be a challenge. While the presentation in list form is practicable for a small number of entities, the overview is quickly lost when dealing with large numbers, making the aspect of presentation for a growing knowledge base an important factor for maintaining the usefulness of the tool.

The most important challenge a tool for knowledge sharing has to face is the aspect of motivating users to participate in a knowledge exchange. While researchers may enjoy the exchange of knowledge and ideas, organizations expect to benefit from disclosing knowledge. Therefore, as previously mentioned, concrete benefits have to be developed for the target group in order to ensure collaboration and participation in the long term.

In order to encourage participation and to find solutions enabling better cooperation between participants, it will also be necessary to take a look at existing social dilemma research, as was done by Cabrera and Cabrera (2002).

The evaluation showed that a collaborative tool can serve as a reference for experts to look up vulnerabilities, threats and countermeasures, or could be useful to risk management experts when applied together with risk calculations. However, creating a trustful environment is crucial in order to make the collaboration work.

The evaluation also showed that before a tool can prevail, a thorough requirement analysis has to take place which identifies the needs of the target group, and a "critical mass" of knowledge has to be compiled to attract new users.

Once users have been successfully motivated to participate, they can add new entries manually to the platform in order to extend the knowledge base. Depending on the final operation model, the entries can be reviewed by a central authority or by the community to ensure the quality of the captured knowledge.

5.2. *Update on further development*

After the initial publication, further work has been put into the development of the web portal by Lukas Lechner. On the one hand additional theoretical questions have been explored, on the other additional features have been implemented in order to meet some of the deficits identified in the original release.

1) Exploration of additional theoretical questions:

a) How can the individual's perceived benefit be increased?: One possibility would be to offer rewards or incentives to users who contribute a lot. Moreover we could restrict access to some specific knowledge and make it only accessible for users who have already shared a part of their knowledge. Receiving a reward will maximize the individuals gain and so the user takes his time and effort to gain this reward. As a result, the individual and collective interests coincide.

There can be a disadvantage in fact that the quality could suffer at the expense of quantity because the users are forced to contribute to gain their rewards. A system that rates the value of the content of someone's contribution, where users can decide how good, helpful or valuable it is, would be useful in that case.

As a combination of the quantity and quality of ones contribution, the users could get credited with points or credits with which they for instance could buy new content or new functionality.

In our portal it would be fitting, if users would generally have access to all the online knowledge but they would have to earn a certain amount of credits to be able to get access to the export function, which exports the whole knowledge base to an offline file. Each time they want to use the export function and download the actual state of the ontology, they have to pay it for that certain amount of credits. There are many ways to earn credits:

- by adding new threats, vulnerabilities or controls
- by adding a relation between entities
- by adding advice, comments, examples, explanations or reviews to existing threats, vulnerabilities or controls
- by answering an asked question from another user

As mentioned before, the pressure of the users to gain credits might lead to a lack of quality in the content of the

contributions. Hence someone has to decide if the added contribution is of value and if the credits for the user are justified. This could either be accomplished by a moderator or by the community with a rating system. The advantage of a rating system is the reduction of costs that would be incurred for the evaluation work of moderators.

b) How to enhance efficacy and contribution?: Technology is only one of the ingredients for successful knowledge exchange. The other, maybe even more important requisite is a social environment which encourages or even enforces knowledge sharing.

Social dilemma literature says that a strong dependence exists between perceived efficacy and the level of cooperation. When people think that their actions will affect the value of a public good, in our case the existing knowledge, in a positive way, they are more likely to corporate.

Further, efficacy can be divided into information self-efficacy and connective efficacy.

Information self efficacy in our case means, that if someone has the knowledge and thinks he can help the community, he is more likely to contribute. On the other hand, connective efficacy is the belief that other users will actually receive the contributed information.

One way to increase efficacy is to implement a feedback mechanism where contributors can see whenever others had used their contribution or considered it as valuable. If a contributor receives feedback, the perception of connective efficacy increases. The content of someone's feedback also provides an indication of the value and impact of the contribution. Feedback increases the information self efficacy, because the contributor recognizes that his knowledge helps someone else, provided that the feedback was positive. Obviously there is a problem if someone receives a negative feedback. Logically the information self efficacy decreases when that happens and the contributor will most likely not contribute to the knowledge base in the future again. Nevertheless there is also a positive consequence of negative feedback too. It can help to control the quality of contributions and compensate the negative effects of the reduced information self efficacy. However, feedback mechanisms encourage quality rather than quantity.

This would be another advantage of the rating/feedback mechanism we proposed in the section Increasing the benefit. Furthermore feedback could automatically be sent via email to the author of the initial contribution so that he receives the information that someone has assessed his content. This would also increase the users efficacy.

2) Implementation of additional features:

a) Simplified registration process: New users are crucial for a knowledge base to grow. So the registration procedure has to be quick, simple and easy. Until now, users had to send an e-mail with their registration data to the administrator, who activated their account thereafter. The registration process has been simplified by implementing an easy to use registration form.

b) Multiple selection: To increase the usability of the portal, participants of the conducted user study suggested implementing multiple selections in the IndividualsListPortlet. This

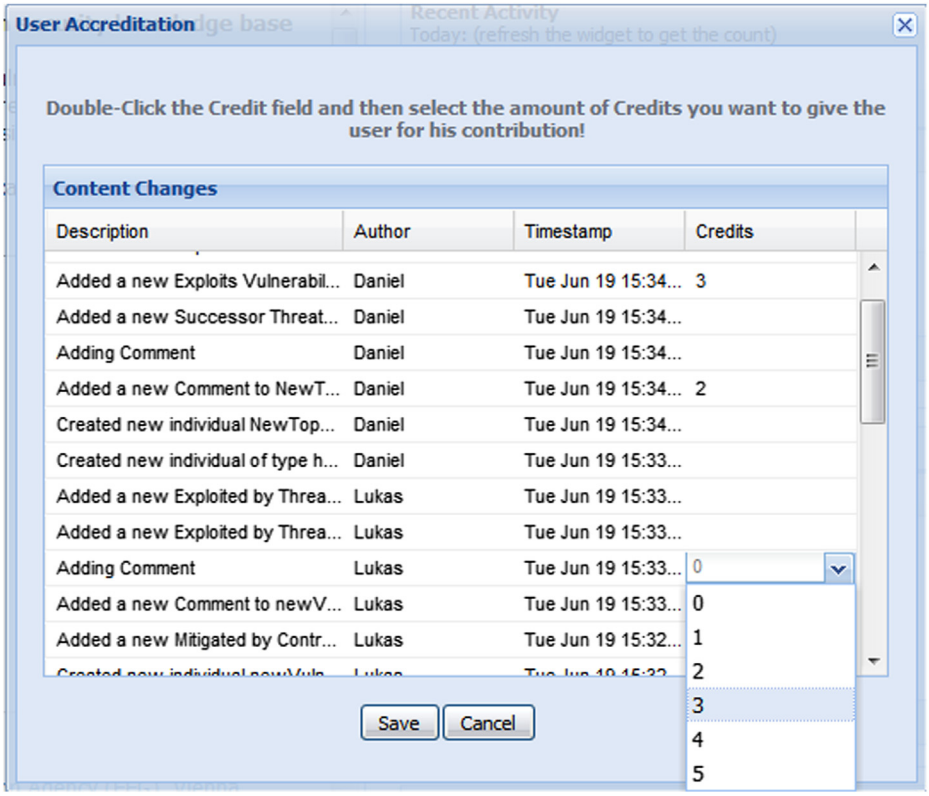

Fig. 3 – Screenshot of the credit system.

is necessary to make the task of adding entities in order to create relations more efficient so the user does not have to do the same steps over and over again.

c) Integration of Google Analytics: Google Analytics has a lot of merits when analyzing the traffic of a website. With Google Analytics we can capture a lot of data of the users on our portal and their behavior. We can see for example:

- demographic characteristics
- the distribution of new visitors and returning visitors
- the average visit duration
- the bounce rate (percentage of single-page visits)
- the source from where the visitors accessed the side (via links, keywords on search engines)

With this information, we can draw some conclusions of how to improve the web presence of the platform and how to conceive better information of our visitors.

d) User rewards: One possibility identified to increase the contribution of users is to raise their perceived benefit. A benefit for users could be some functionality, which gets unlocked only if the user contributes a certain degree of contribution.

To realize that incentive, a credit system was implemented for the platform (see Fig. 3). Each new user has to earn credits by contributing to the portal. The benefit of earning credits is that the user can use the export functionality, which lets him download the full ontology to an offline owl file. The implementation was realized in a way that it is easy to configure and expandable for new functionality to unlock. For each contribution made by a user, an authorized administrator can decide how valuable the contribution is and how many credits the author deserves.

6. Outlook

The web portal presented in this paper has the potential to support information security experts in their everyday work. The evaluation has shown that the interface is easy to handle, though some refinements have still to be implemented. Still there are conceptual challenges that have to be addressed in future work. During the evaluation it was also shown, that certain aspects of the ontology are difficult to model and offer too much ambiguity. For example the comprehensibility of the dependencies between the different entities is not always given. In the process of further developing the web portal, it is important to put a stronger focus on determining the final target group. This will help to concentrate on the needs of this group and to develop a unique selling point, making the web portal more attractive to use. At the same time incentives have to be developed to attract experts and to motivate them to contribute their knowledge.

Acknowledgments

The research was funded by COMET K1, FFG – Austrian Research Promotion Agency.

REFERENCES

Cabrera A, Cabrera EF. Knowledge-sharing dilemmas organization studies, vol. 23 (5). Sage Publications; 2002. p. 687–710.

European Network and Information Security Agency. Good practice guide network security information exchanges. Retrieved January 17, 2012, from, http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide/; June 2009.

European Network and Information Security Agency. Incentives and challenges for information sharing in the context of network and information security September 2010.

Feledi D, Fenz S. Challenges of web-based information security knowledge sharing. In: 2012 Seventh international conference on availability, reliability and security 2012. p. 514–21.

Fenz S, Ekelhart A. Formalizing information security knowledge. ASIACCS. Sydney, Australia: ACM; 2009.

Fenz S, Parkin S, van Moorsel A. A community knowledge base for IT security. IT Professional 2011;13(3):24–30.

Glaser T, Pallas F. Information security and knowledge management: solutions through analogies?. Berlin: Technische UniversitÃ¤t Berlin; 2007.

Kijewski Piotr. A new approach in European awareness raising and alerting February 2011.

Mace JC, Parkin S, van Moorsel A. A collaborative ontology development tool for information security managers. In: Computer-human interaction for management of information technology. San Jose, California: ACM; 2010.

McAfee, Inc. Unsecured economies: protecting vital information. Santa Clara: McAfee, Inc; 2009.

Parkin SE, van Moorsel A, Coles R. An information security ontology incorporating human-behavioural implications. In: International conference on security of information and networks. Gazimaguse, North Cyprus: ACM; 2009. p. 46–55.

Schumacher M. Toward a security core ontology. In: Schumacher M, editor. Security engineering with patterns. Berlin: Springer-Verlag; 2003. p. 87–96.

Vorobiev A, Bekmamedova N. An ontology-driven approach applied to information security. Journal of Research and Practice in Information Technology February 2010;42(1):61–76.