Die approbierte Originalversion dieser Diplom-/Masterarbeit ist an der Hauptbibliothek der Technischen Universität Wien aufgestellt (http://www.ub.tuwien.ac.at).

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology (http://www.ub.tuwien.ac.at/englweb/).

FAKULTÄT FÜR !NFORMATIK

Mapping Security Frameworks Into SecOnt

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Arman Manutscheri
Matrikelnummer 0026170

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer/Betreuerin: o.Univ.Prof. Dr. A Min Tjoa
Mitwirkung: Univ. Ass. Dr. Edgar Weippl
Dipl. Ing. Mag. Stefan Fenz
Dipl. Ing. Mag. Andreas Ekelhart

Wien, 29.08.2008 _____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Abstract

The complexity of IT-Security is growing every day; at the same time the protection of business information has become an indispensable element in every company's business duties. Often small and medium sized enterprises, in particular, do not have the resources to implement a holistic IT-Security approach. My work builds on SecOnt, a security ontology by Stefan Fenz and Andreas Ekelhart, which enables low-cost risk management and threat analysis.

I have extended the ontological model with best practice knowledge from the German BSI's IT-Grundschutz-Catalogues. Therefore, I have analyzed and altered relevant concepts from the domains "threat, vulnerability and countermeasure" and have mapped them into the SecOnt structure. Initial incompatibility, inconsistency and redundancy problems of the IT-Grundschutz-Catalogues have been reduced and eliminated. Furthermore, to allow simulation of threat scenarios and chain reactions the relations between the concepts and also threat interrelations have been derived and modeled into SecOnt.

Acknowledgements

I would like to thank all the people who supported me during my work on this thesis.

I want to thank Prof. Dr. A Min Tjoa for the supervision of my thesis.

I'm grateful to Dr. Edgar Weippl who offered me the issue to this thesis and who made the cooperation with Secure Business Austria possible.

I want to extend special thanks to my consultants Stefan Fenz and Andreas Ekelhart, who supported me with their knowledge and advice. Thank you for your patience!

Last but definitely not least I want to thank my parents not only for supporting me during my thesis but also for supporting me with everything else I do.

Table of Contents

1 Introduction

With the shift of the ages from the Industrial Age to the Information Age, a lot of things have changed. Nowadays information is often more valuable than physical goods. Completely new business opportunities have evolved. Everyday news headlines such as “Google rises to the top of the BRANDZ™ Ranking with a brand value of $66,434 Million” [1] or reports about internet phenomena like Facebook Inc.[1] being valued at $15 billion [2] illustrate constantly that we are right in the middle of the information age and that information has become an essential part of today’s economy.

With information being such a valuable good, its protection has become an indispensable element in every company’s business duties. However, at the same time we regularly read articles that report about incidents where IT-Security vulnerabilities have caused companies massive financial loss. Not only irretrievable data loss and downtime are types of damage the victims have to suffer, also the loss of confidence of customers, suppliers and other miscellaneous business partners are a huge problem those companies have to face. Confidentiality, integrity, reliability, accountability, availability and authenticity [3] are the key factors in the domain of information security.

IT-systems are the key to dealing with huge amounts of data, so very high requirements regarding their security have to be put in place. On the other hand information technology is getting more and more complex, IT systems and networks are growing continuously and IT-Security requirements keep getting more difficult to be met.

A wide variety of dangers pose a threat to a company’s information system, ranging from malicious action such as industrial espionage, hacking or virus attacks to events of force majeure such as fire, power outages or hard disk crashes. To oppose those threats changes in processes and policies, as well as a companywide security culture and awareness are often much more effective than various technical controls. Security infrastructure, i.e. hardware as well as software tools, can only help if applied correctly. Therefore a proper security strategy has to cover a broad

[1] Facebook: www.facebook.com, last access: July 8 2008 – is a social networking platform that allows people to communicate with friends and share social contacts. According to their own site they have around 55 million active members. [16]

spectrum of approaches. Especially small and medium sized enterprises (SME) often do not have the financial potential to implement a holistic IT-Security approach that is able to cover all those aspects.

Another reason why companies must have full control over risks concerning business information are laws such as Basel II [4] or the Sarbanes-Oxley Act (SOX) [5]. Those laws are intended to protect investors against accounting manipulation and the consequential corporate scandals. SOX, amongst other things, regulates how financial information has to be secured. Therefore SOX has a very big influence on how every U.S. publicly owned company's information system, and all processes which are linked to it, have to be organized. Thus, IT-Security cannot longer be ignored by a company's management. It has become a business duty and publicly owned companies and their subsidiaries are even bound by law to implement a proper information security management system.

To help organizations secure their IT systems, various "best practice" frameworks and standards have been created. One of the first of these documents was published by the OECD (Organization for Economic Cooperation and Development) in the year 2002 with the "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [6]. Various other organizations like the ISO (International Standards Organization) or the BSI (Bundesamt für Sicherheit in der Informationstechnik) have seized on the idea of a holistic information security management system (ISMS) and have published detailed guidelines on how to implement such a system in companies of various sizes. Organizations can be certified against those international standards (ISO 27001 [7] and BSI IT-Grundschutz Catalogues [8]) so that they can prove a certain level of trustworthiness and reliability to their business partners.

However, even with the help of certain frameworks and international standards it is difficult to obtain a sustainable level of IT-Security. Companies' structures, personnel, IT hard- and software change with time. Experience shows that IT-Security managers are having a hard time keeping up with those changes.

That is why in my thesis I will filter information about the domains threat, vulnerability and countermeasure out of suitable IT-Security frameworks and create an ontological mapping of these domains. This ontology will help organizations …

- to clarify the meaning and coherence of IT-Security related terms

- identify threats and rate their security risks
- implement countermeasures against vulnerabilities in their system
- manage the continuously growing complexity of security requirements
- accomplish the certification process (e.g. ISO 27001/17799, BSI IT-Grundschutz Catalogues)

I'm building on previous work by Stefan Fenz and Andreas Ekelhart from "Secure Business Austria"[2], who developed an initial security ontology which is called "SecOnt" [9, 10, 11]. They have set up the basic structure of the security ontology and have also introduced a draft of the domains threats, vulnerabilities and controls with exemplary data to demonstrate a proof of concept. My work focuses on extending this draft with established best practice knowledge.

Note:The security ontology is much more complex and has a lot more features than those mentioned above, but the detailed structure and characteristics of SecOnt will be explained later in chapter 5.2.

1.1 Social Relevance of this Topic

The monetary value of information is higher than ever and the need for a protection of critical business data and the importance of fail-safe, reliable IT system are obvious to every company's management. In a survey by PricewaterhouseCoopers conducted in the UK in 2006 [12], 43% of interviewed top managers classified information security as a very high priority business duty [Figure 1].

Nevertheless, IT-Security management is still in the early stages of development.

The average UK Company spends 4-5% of its IT budget on information security. This figure alone does not look so bad, but on the other hand we have a 40 % of the interviewed companies that spent less than 1% of their IT budget on securing their data [Figure 2]. These companies obviously run into danger of being victims of security threats.

[2] Verein zur Förderung der IT-Sicherheit in Österreich: www.securityresearch.at, last acces: July 8 2008

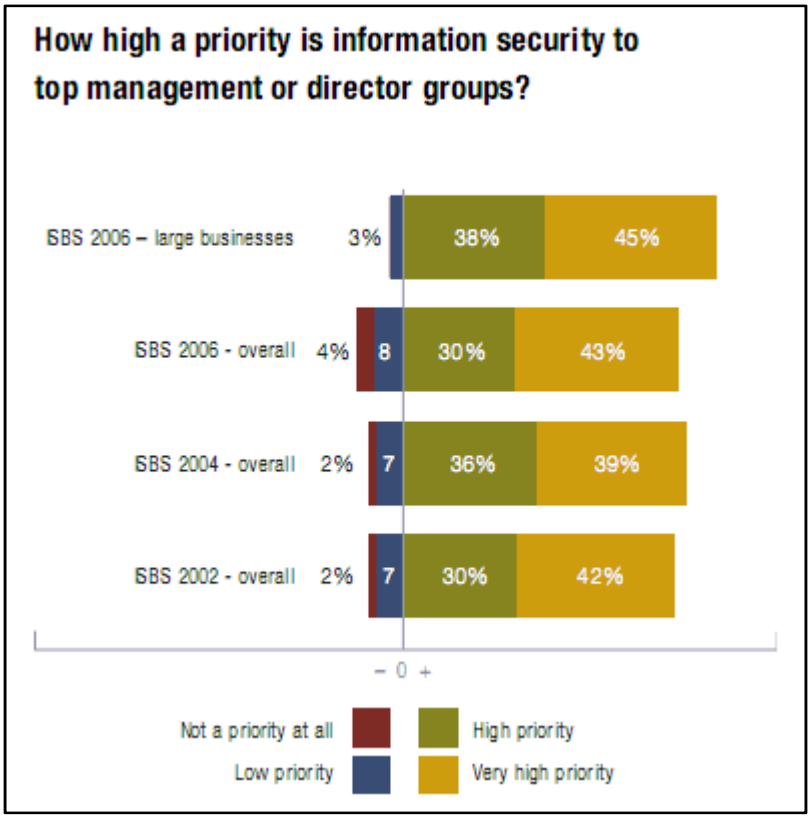


Figure 1: Importance of Information Security **[12]**

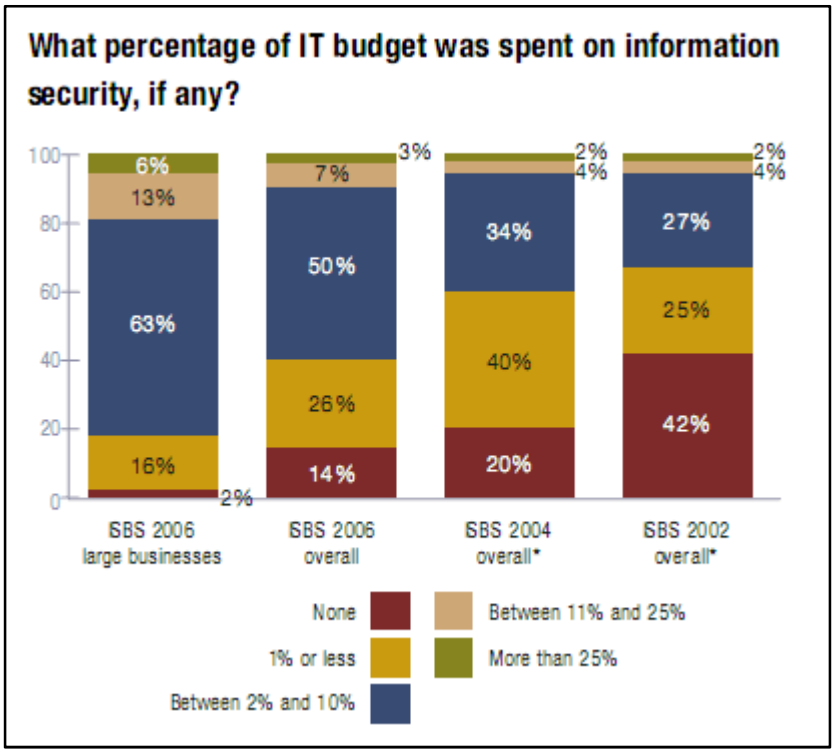


Figure 2: IT Budget spent on Information Security **[12]**

Figure 1 and Figure 2 show that there is a positive trend concerning managements' attitudes towards information security. This also correlates with the positive trend that over the last years the average monetary loss resulting from IT-Security incidents has been declining drastically. The Computer Crime and Security Survey 2006 published by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) reports that the average loss per respondent has declined from $526.010 in 2004 to $203.606 in 2005 and to $167.713 in 2006 [13]. The most relevant categories of losses are Virus infections, followed by unauthorized access to information, theft of mobile hardware and information theft. As shown in Figure 3 those threats sum up to almost three quarters of the total losses.

Due to the difficulty to measure exact amounts of losses resulting from various types of security incidents, e.g. amounts resulting from loss of trust from customers, those figures unquestionably can only be seen as a vague estimation. Nevertheless they show conclusively that there still is a lot of potential for improvement in this domain.

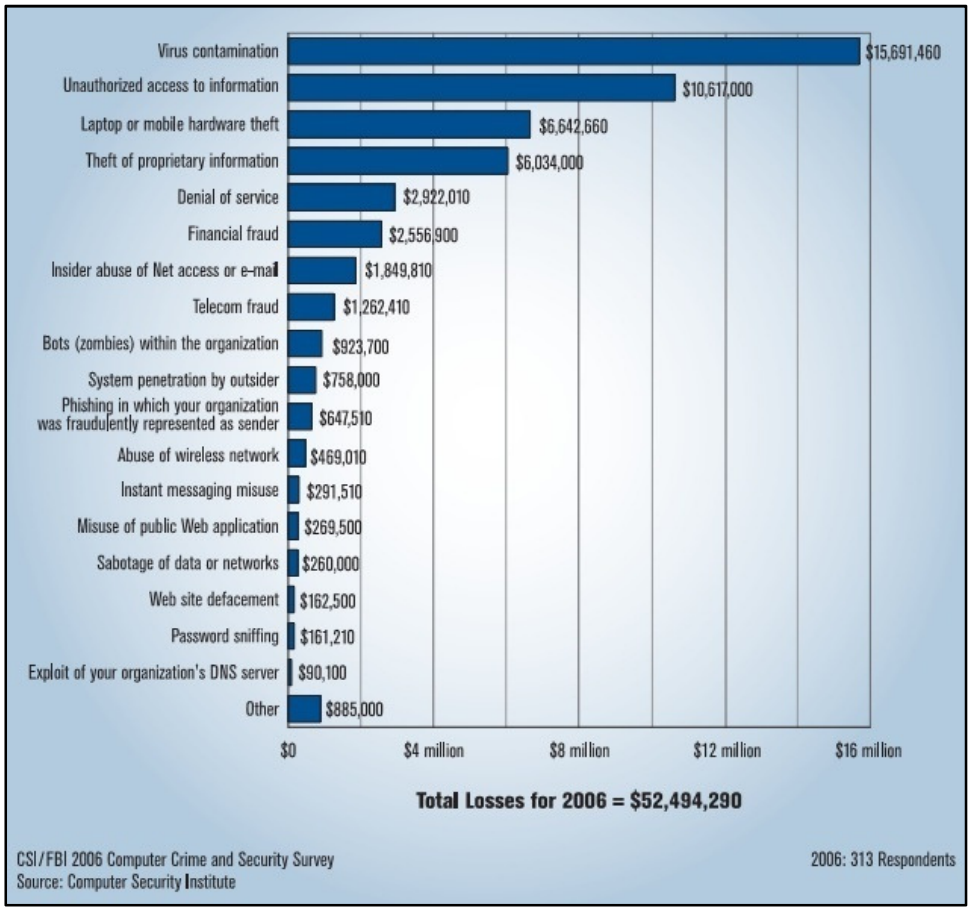


Figure 3: Dollar Amount Losses by Type **[13]**

1.2 Personal Affiliation to the Topic

Working at the IT department in the systems and network management team of a multinational company, which also is subject to SOX, I'm confronted with the complexity and confusion of inhomogeneous, steadily changing computer networks every day. Security at my company is a big issue - mainly because of legal obligations such as the frequently mentioned SOX or the standard for PCI-Compliance (Payment Card Industry Data Security Standard) [14] which every company providing credit card payment has to follow. In some cases, mainly when network structures and applications have grown over time, which I'm sure is the case in a lot of companies, far-reaching and costly changes have had to be made, not only concerning the technical aspects, but also operational processes have had to be adapted to fulfill the legal requirements.

As our company does not have an Information Security Management System implemented and does not use any software application to support information security management, it is very hard to keep up with the ever changing security requirements.

With SecOnt a company's infrastructure and already implemented security controls can be virtually modeled, security requirements can be analyzed and security gaps can be illustrated. Furthermore SecOnt suggests established best practice approaches to close these gaps. Based on this model many more features like cost/benefit analysis of various security implementations or automated aid with the certification process of the ISO 27001 [7] standard or the BSI Grundschutz Manual can be used [8]. On the whole SecOnt can assist me and other system administrators, as well as other personnel responsible for security in protecting business data and information against various threats.

1.3 Organization of this Thesis

After this brief introductory chapter in chapter 2 I am going to discuss the initial problem statement and the approach I have followed during my work.

Afterwards, in chapter 3 I will discuss different approaches presented in related work dealing with the creation of Information Technology Security Ontologies. Further I will compare the used methods with our approach.

Chapter 4 will focus on theory. First I will give a theoretical overview of the most common Information Security Standards and Best Practice collection. In addition I will analyze them with regard to suitability for being the information source for our knowledge base. Then I will present an overview of ontologies and OWL ontologies in particular.

Building on the previous chapters, chapter 5 contains the information related to the practical part of my work – the mapping of the information from the IT-Grundschutz Catalogues to the OWL ontology “SecOnt”. First I introduce “SecOnt”, on which my work is based on. Then I will discuss the problems and solutions we have encountered during the mapping. Finally I will give a step-by-step tutorial of how the mapping was done.

Finally, in the last chapter, I will give a summary of my work and discuss possible future work and examples of application.

2 Problem Statement and Analysis

This chapter contains the analysis of the problem statement and an overview of the approach that led to the final solution of the problem.

2.1 The Problem

The initial assignment was to create an ontological mapping of established information security knowledge, including

- potential threats to a company's data and information system,
- vulnerabilities that these threats can exploit,
- countermeasures that mitigate these vulnerabilities.

This knowledge should be embedded into an existing IT-Security ontology, called SecOnt, which will be explained in detail in chapter 5 of this document.

The ontological database should cover all Information security relevant threats that might affect an average small or medium sized company together with their related vulnerabilities and countermeasures, which would be a very broad range. It would range from natural threats such as a lightning strike to deliberate, malicious attacks, such as hacking attempts to steal information.

Furthermore it should be possible to link threats together to model chain reactions. For example a lightning strike could cause electronical disturbances, those electronical disturbances again could give rise to a power loss, a power loss could lead to a malfunctioning security system. Failure in the security system in turn could allow unauthorized access to the building, and so on. Figure 4 illustrates the idea of connected threats.

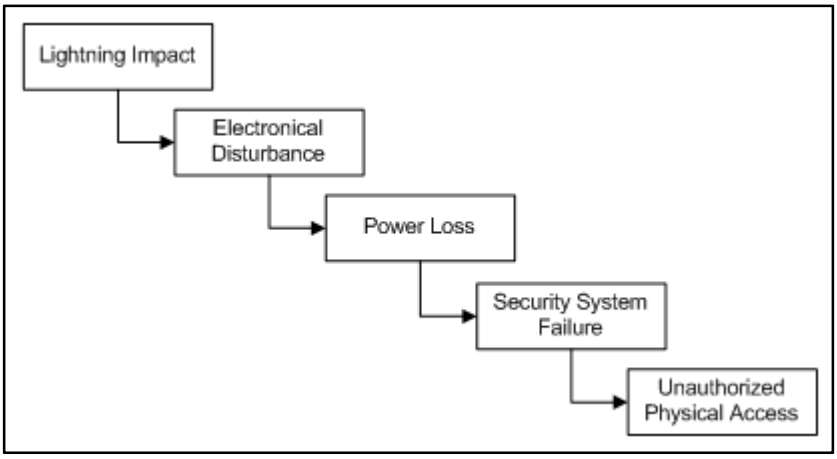


Figure 4: Example of connected threats

The modeling of threat interrelations will provide the essential information for further risk analysis and substantial security planning.

Due to this assignment the following research questions are posed:

- What should be the knowledge source for the mapping to the ontology? Which international standard, respectively best practice knowledge collection covers our requirements best?
- How does the scope and the content of the knowledge source need to be altered to fit the requirements of SecOnt? How can threat interrelations be modeled?
- Which incompatibilities between the knowledge source and the structure of SecOnt are there and how can they be corrected? How can inconsistencies in the knowledge source and in SecOnt be corrected? Which methods are applicable?

2.2 The Approach

First we had to find an established Information Security knowledge base which then should be our source for the mapping. Therefore we have had to analyze the most commonly used standards and best practice collections related to this topic and rate them under the aspect of suitability for our purpose. The most important criteria for the selection would be:

- **Scope**: We want to map information related to Information Security from a small and medium sized enterprise's point of view so the source needs to cover all aspects that are relevant for this target group.
- **Comprehensiveness**: The information has to be in a specific granularity. It must not be too superficial but at the same time it must be detached from specific technology.
- **Compatibility**: The structure should be compatible with SecOnt. If this initially is not the case it has to be possible to convert the information to use it within SecOnt with reasonable expenditure.
- **Acceptance**: The information has to be established and widely accepted.

The following knowledge bases (i.e. standards or best practice collections) have been preselected and afterwards analyzed due to their high level of awareness in the domain:

- The ISO 27000 Standard family
- The Standard of Good Practice [15]
- The IT-Grundschutz Catalogues [8]

The next step is to compare the results of the analysis and choose the source which covers our requirements best. This process is described in chapter 4.1.

After selecting the most suitable knowledge source we have to analyze and overcome incompatibilities and problems that prevent us from mapping logically correct and efficiently. Therefore we have to find solutions for structural and contentual weaknesses and incompatibilities. Chapters 5.3.1 and 5.3.3 are dedicated to these topics.

Only now, after ironing out the problems, we can start to go through the selected knowledge source concept by concept, and map the filtered and trimmed content to the Security Ontology. A step-by-step tutorial in chapter 5.3.4 shows the process of the mapping.

Note: This document is a description of the methods and approaches I have used to map established IT-Security knowledge to SecOnt, an existing security ontology. At this point I want to emphasize that the practical part and also the most time consuming part of my thesis was the mapping itself. The complete IT-Grundschutz-Catalogues, which at the moment contain over 3600 pages, had to be processed and the approaches and methods which I have presented in this document had to be applied on their content.

The practical results of my work, respectively the latest version of the SecOnt security ontology, are available on the website of Secure Business Austria at the following url: http://securityontology.securityresearch.at/downloads/.

3 Related Work

In this chapter I am going to present similar research in the field of security ontologies published by researchers who are not related to our working group.

3.1 Raskin: Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool

Raskin et al. [16] were among the first who introduced the idea of an ontological mapping of information security terms. Their approach pursues the goals of

- inclusion of natural language data sources as an integral part of the overall data sources in information security applications,
- a formal specification of the information security community know-how for the support of routine and time-efficient measures to prevent and counteract computer attacks.
- They also have created an initial ontological lexicon for security terms.

In their work they presented the generic concept of ontologies and discussed their needs in the context of Information Security. In their research they mainly focused on how natural language and information security know-how can be combined into an ontology.

Raskin et al. did not discuss further possibilities that an ontological mapping would bring in detail but they started a lively discussion and set the ball rolling for further security ontology related research.

3.2 Tsoumas: Towards an Ontology-based Security Management

Tsoumas et al. present in [17] a similar approach to an ontology-based framework for information security management. They have built an OWL-Ontology on top of the DMTF Common Information Model (CIM) and introduced a generic approach which is able to use security knowledge from various sources. However, building the actual security knowledge database was listed on their to-do-list, which is exactly where our work continues.

They have created a conceptual model very similar to ours, which is shown in Figure 5, and can be explained as follows:

"…, a *Stakeholder* possesses an *Asset*, which in turn can be compromised by a *Vulnerability*. In addition, a *Threat* initiated by a *Threat Agent* targets an *Asset* and exploits a *Vulnerability* of the *asset* in order to achieve its goal. Exploitation of a *Vulnerability* leads to the realization of an *Unwanted Incident*, which has a certain *Impact*. Furthermore, *Countermeasures* reduce the impact of the *threat* by using *Controls*. Finally, *Security Policy* formulates the *Controls* into a manageable security framework possessed by *Stakeholders*." [17]

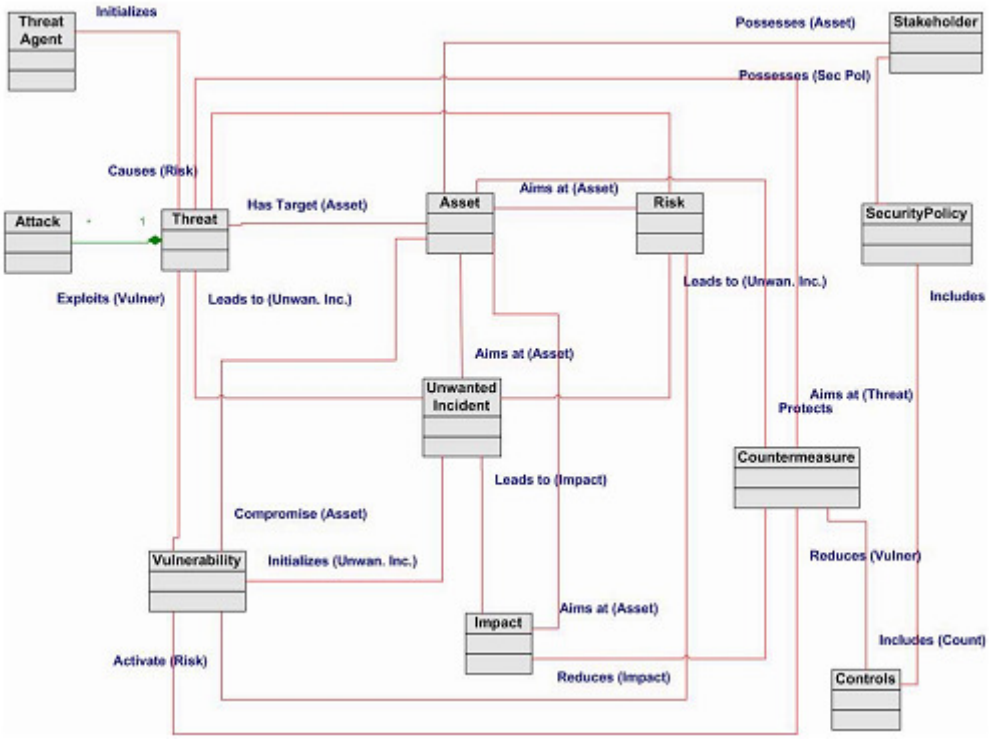


Figure 5: Model of Security Ontology by Tsoumas et al.

They then presented a process for building a security ontology in an organization. This process consists of the following 4 phases:

Phase 1: Building of Security Ontology

In this phase the organization's Information System infrastructure should be mapped into the ontology.

Phase 2: Security Requirements Collection

In this phase the organization's security requirements are extracted from various sources and are mapped into the ontology.

Phase 3: Security Actions Definition

The purpose of phase 3 is to associate the security requirements from phase 2 with specific security controls, which are proposed by the "Database of Technical Controls". Those controls should then be transformed into a Ponder[3]-compatible input.

Phase 4: Security Actions Deployment and Monitoring

Finally the Ponder rules created in phase 3 should be applied on the Information System infrastructure to fulfill the security requirements.

This process should then be repeated over certain periods of time, to keep up with the changing requirements of the organization.

Comparison to our approach

The idea and the structure of Tsoumas' work are very similar to ours, although the approach is different in the following aspects. What it lacks in comparison to SecOnt, our approach, is the possibility to create links between single threats. With SecOnt it is possible to create complex threat scenarios and furthermore it is possible to mitigate threats on different levels of origin. In addition, SecOnt offers the possibility to map entire business-locations, including buildings, infrastructure, hardware, etc and can thus build the foundation for much more complex risk analysis. More detailed information on all features of SecOnt will be provided in chapter 4.

[3] "The Ponder language provides a common means of specifying security policies that map onto various access control implementation mechanisms for firewalls, operating systems, databases and Java. It supports obligation policies that are event triggered condition-action rules for policy based management of networks and distributed systems.." [18]

I once more want to point out that the actual knowledge base - Tsoumas names it “Database of Technical Controls” - has not been created. The creation of such a knowledge base is the main focus of my work in this thesis.

3.3 Herzog: An Ontology of Information Security

During my work on this thesis another group of researchers has published a very similar approach to creating an “Information Security” ontology: Almut Herzog, Nahid Shahmehri and Claudiu Duma of the “Department of Computer and Information Science” of the Swedish “Linköpings universitet” have published their paper on “An Ontology of Information Security” [18] 2007 in the “International Journal of Information Security and Privacy 1”.

They have created a publicly available, OWL-based ontology of information security which like our approach also builds upon the classic components of risk analysis: assets, threats, vulnerabilities and countermeasures. At the time of publishing the ontology contained 88 threat classes, 79 asset classes, 133 countermeasure classes, 13 vulnerability classes and 34 relations between those classes. Figure 6 shows an extended entity-relation diagram of their security ontology model.

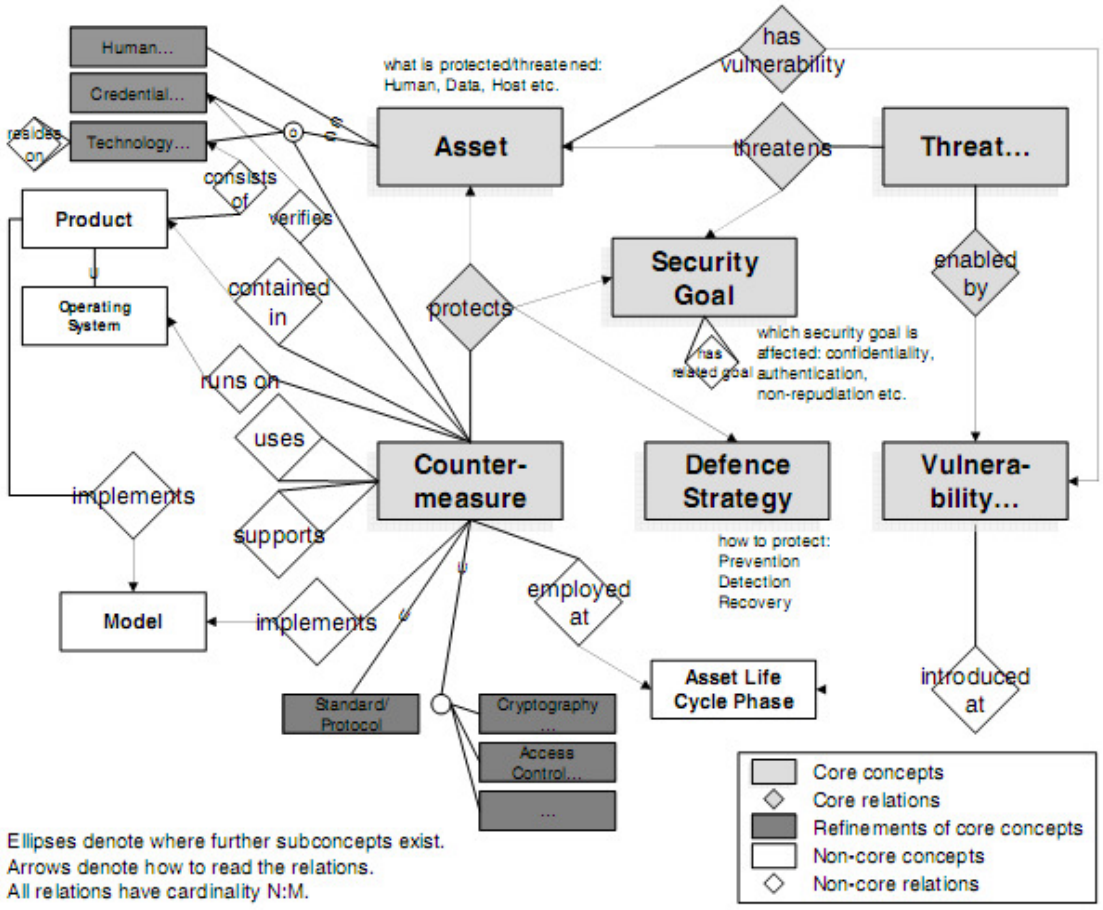


Figure 6: A. Herzog’s security ontology overview

The ideas and the motivation behind A. Herzog's approach is very similar to ours, but the implementation differs in the following aspects:

Comparison to our approach

• Herzog's approach only focuses on specific attacks as a form of threats • Countermeasures contain only hardware, software and technical methods, but no controls or guidelines • Assets contain only IT security related concepts. • No threat interrelations, instead every threat is treated on its own. • Only 13 vulnerabilities	• The SecOnt approach covers every threat that is relevant to secure the data of a small or medium enterprise (including high level threats). • Countermeasures also contain instructions and guidelines. • Assets contain organization-wide concepts. • Threat interrelations are modeled; therefore we are able to map complex risk analysis scenarios. • Integration of the ISO 27001/27002 standard • Approximately 90 vulnerabilities

The table shows that on the first look the concepts of our work are very similar, but on the second look many refined distinctions emerge. To summarize, the Herzog approach is much more detailed and comprehensive in terms of specific attacks and countermeasures related to those attacks, whereas SecOnt covers all aspects (threats, vulnerabilities, assets, countermeasures) which are relevant to an organizations IT-Security in the broadest sense .To use the individual strengths of both approaches it would be a good idea to merge the two ontologies.

4 Theoretical Background

In this chapter I will give a theoretical overview of related topics. First I will introduce the most common Information Security Standards and Best Practice collection which in addition are analyzed with regard to suitability for being the information source for our knowledge base. Then I will present a theoretical introduction to ontologies and OWL ontologies in particular.

4.1 Overview of existing Information Security Standards and Best Practice Collections

Various institutions and organizations have collected IT-Security knowledge over the last couple of years and have created various documents with different approaches to help other organizations, companies and individuals to secure their IT infrastructure and data. These approaches range from a very generic, management point of view to very technical step-by-step implementation guides in very specific security domains. Some even provide international certification to guarantee a certain level, respectively a certain management approach to IT-Security [7, 8, 15, 19]

A standardized IT-Security System provides many benefits to the organization:

- It is always more efficient to use widely approved methods and approaches. As most IT systems are built on similar foundations (hardware, software, infrastructure, protocols) it is really not necessary to reinvent the wheel for every company. Rather, every organization has to analyze their specific risks and implement an adequate security level to protect their critical applications, data and information systems. To reach this goal established knowledge and best practice should be used.
- Companies possessing established certification for their information security management system (e.g. ISO27001/ISO17799) can prove a high level of information security to their suppliers, customers and other business partners, resulting in an increasing market value. Therefore certified companies would prefer to do business with other certified companies.
- There are two main benefits with using ISMSs (Information Security Management Systems) that ensure a company's IT-Security to be up-to-date. Firstly most standards for Information Security Management Systems propose

a process that regularly reviews and improves a company's security implementations. Secondly most standards and best practice collections are updated and published at regular intervals. Furthermore, these features make the IT-Security system less dependent on up-to-date security knowledge of the IT employees.

- Under normal conditions organizations that use an established Information Security Management System have a good chance to be compliant with various financial laws such as SOX and Basel II. At least the effort to reach this compliance with the help of ISMS is minimal compared to the scenario where no ISMS is in place.

In the following chapter I will present an overview of existing Information Security Standards and Best Practice Collections that cover a broad range of security topics from a management's point of view. I will furthermore rate the selected standards and collections under the perspective of suitability for mapping parts of them into our ontology. I want to point out that this rating does not in the least imply that one standard is more valuable than another in general; the different standards rather have different aims and they were developed from different points of view.

4.1.1 The Standard of Good Practice (for Information Security)

The Standard of Good Practice [15] is a very comprehensive best practice framework for information security published by the Information Security Forum (ISF)[4]. First released in 1996 and revised at least every other year, it is one of the oldest and best maintained documents containing information related to information security from an average business' point of view. To provide a versatile approach the development of the standard has been based on the contributions of three different groups of activities as shown in Figure 7.

[4] Information Security Forum: http://www.securityforum.org/, last access: July 8 2008 - the Information Security Forum (ISF) is an international non-profit organization dedicated to information security, with hundreds of members, including 50% of the "Fortune 100" companies.

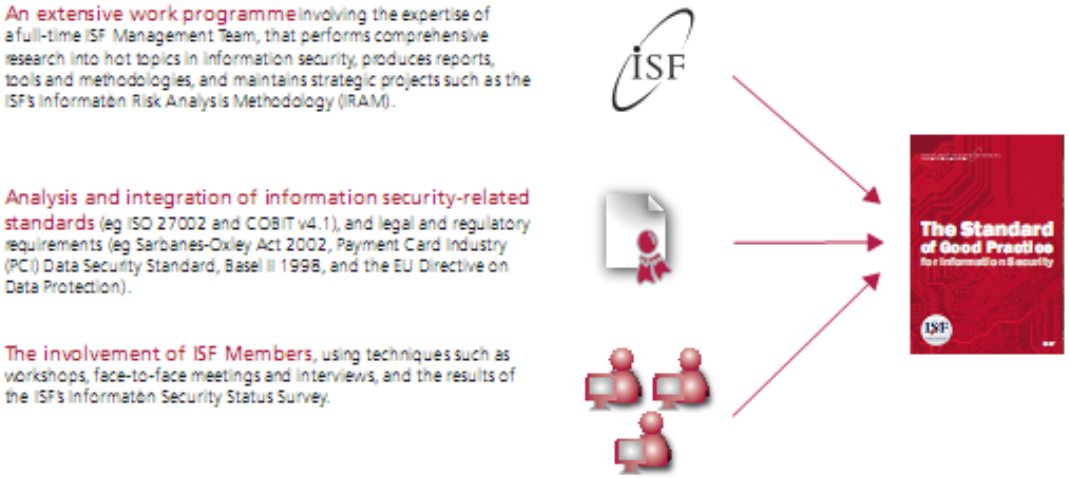


Figure 7: Contributions to the Standard of Good Practice

The standard itself covers six general aspects of information security. The following table shows the main topics and the probed issues:

Security Management: The commitment provided by top management to promoting good information security practices across the enterprise, along with the allocation of appropriate resources.

Critical Business Applications: The security requirements of the application and the arrangements made for identifying risks and keeping them within acceptable levels.

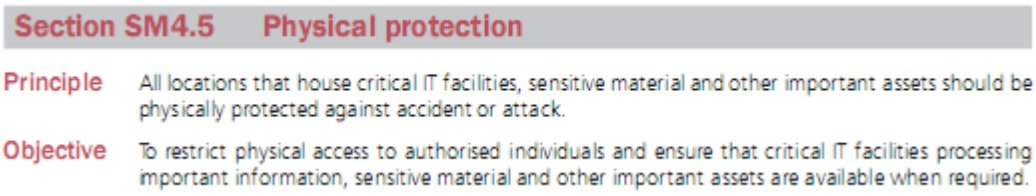
Computer Installations: How requirements for computer services are identified; and how the computers are set up and run in order to meet those requirements.

Networks: How requirements for network services are identified; and how the networks are set up and run in order to meet those requirements.

Systems Development: How business requirements (including information security requirements) are identified; and how systems are designed and built to meet those requirements.

End User Environment: The arrangements for user education and awareness; use of corporate business applications and critical desktop applications; and the protection of information associated with portable computing.

Those main chapters are broken down into areas and sections which contain the actual statements. A typical entry in the Standard of Good Practice (SoGP) would look like this:



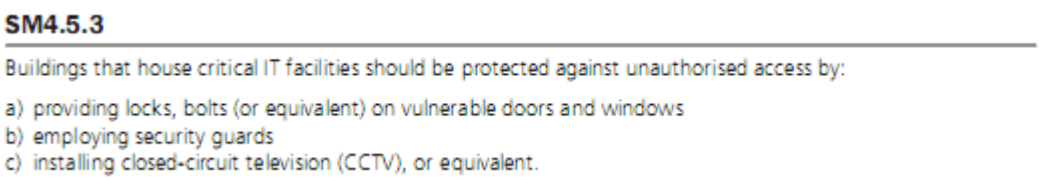
Section SM4.5 Physical protection

Principle All locations that house critical IT facilities, sensitive material and other important assets should be physically protected against accident or attack.

Objective To restrict physical access to authorised individuals and ensure that critical IT facilities processing important information, sensitive material and other important assets are available when required.

Figure 8: Example of a section in the Standard of Good Practice

…



SM4.5.3

Buildings that house critical IT facilities should be protected against unauthorised access by:

a) providing locks, bolts (or equivalent) on vulnerable doors and windows
b) employing security guards
c) installing closed-circuit television (CCTV), or equivalent.

Figure 9: Example of a statement in the Standard of Good Practice

Together with the provided Topics Matrix, which groups similar topics in alphabetical order, the SoGP provides an excellent reference book to the reader who wants to get an overview of a specific security related topic.

In addition to the Standard of Good Practice the ISF provides a reference document, the Information Security Status Survey, which allows to measure the effectiveness of information security across the organisation.

Rating

Pros:

- It covers a very broad range of information security related best practices
- It covers organisational aspects (controls) as well as technical aspects (infrastructure, software) to mitigate security vulnerabilities in an organisation
- It includes a management aspect with the aim to improve the level of security sustainably.

Cons:

- With about 263 pages of actual statements to IT-security related topics, the knowledge is very imprecise. Very few hard facts are proposed so that expert knowledge would still be necessary to implement most of the statements.
- It is not clearly communicated which threats are mitigated, respectively which benefits will occur by implementing a specific statement.

Suitability for our Security Ontology:

The Standard of Good Practice is a good overview for small- and medium-sized enterprises to check their organisations IT-Security on a very broad spectrum.

For our approach it could be used as a resource of countermeasures / controls against threats. Unfortunately the SoGP does not establish a relation between the proposed countermeasures and the thereby mitigated vulnerabilities and threats. Apart from this, statements presented in some domains (e.g. physical threats) are too superficial to be used in our context.

4.1.2 The ISO 27000 Series

The ISO 27000 Series labels a family of standards which are being published by the International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Commission (IEC), covering various topics related to information security management. The following listing shows the individual standards which are members of the ISO 27000 Series, their titling and their status:

ISO/IEC 27001:2005

Information technology -- Security techniques -- Information security management systems – Requirements

Status: Published in October 2005

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. More detailed information on this standard will be given in the following chapter.

ISO/IEC 27002:2005 (formerly ISO/IEC 17799:2005)

Information technology - Security techniques - Code of practice for information security management

Status: Published in July 2007

ISO/IEC 27002:2005 is simply a renaming of the former standard ISO/IEC 17799:2005. It establishes guidelines, general principles and best practices to accomplish the specifications defined in the ISO/IEC 27001:2005. More detailed information on this standard will be given in the following chapter.

ISO/IEC 27006:2007

IT-Security techniques: Requirements for bodies providing audit and certification of Information Security Management Systems (ISMS)

Status: Published in February 2007

ISO/IEC 27006:2007 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

"The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by anybody providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for anybody providing ISMS certification."[20]

ISO/IEC CD 27000

Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

Status: under development

The ISO/IEC 27000 will provide an overview and a standard vocabulary for the ISMS standards in the ISO/IEC 27000 family.

ISO/IEC 27003

Information Technology - Security techniques - Information security management system implementation guidance

Status: under development

The ISO/IEC 27003 will provide help with the implementation of an Information Security Management System in an organization.

ISO/IEC 27004

Information technology -- Security techniques -- Information security management measurements

Status: under development

ISO/IEC 27004 will be a new standard for measuring the effectiveness of an organizations information security management.

ISO/IEC 27005

Information technology -- Security techniques -- Information security risk management

Status: under development

The ISO/IEC 27005 standard will provide techniques for information security risk management.

ISO/IEC 27007

Information technology -- Security techniques -- Guidelines for Information security management systems auditing

Status: under development

ISO/IEC 27007 is going to be a guideline for audit and accredited certification bodies auditing Information Security Management Systems against ISO/IEC 27001.

4.1.2.1 ISO 27001

The "ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements" is an international official standard for information security management systems published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Originating from the British Standard BS 7799-2, it was the first document which was published under the new ISO-series 27000 dealing with information security. It is probably the most important, commonly accepted standard to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's Information Security Management System.

The ISO 27001 standard promotes IT-security management as a continuing process and therefore adopts the PDCA-model ("Plan-Do-Check-Act"), also known as Deming Cycle, which is typically used for quality control. This PDCA-cycle guarantees a consistent monitoring, improvement and the necessary adaptation of the ISMS to the changing requirements of the organization. Figure 10 shows the PDCA-model applied to the ISO 27001 ISMS processes:

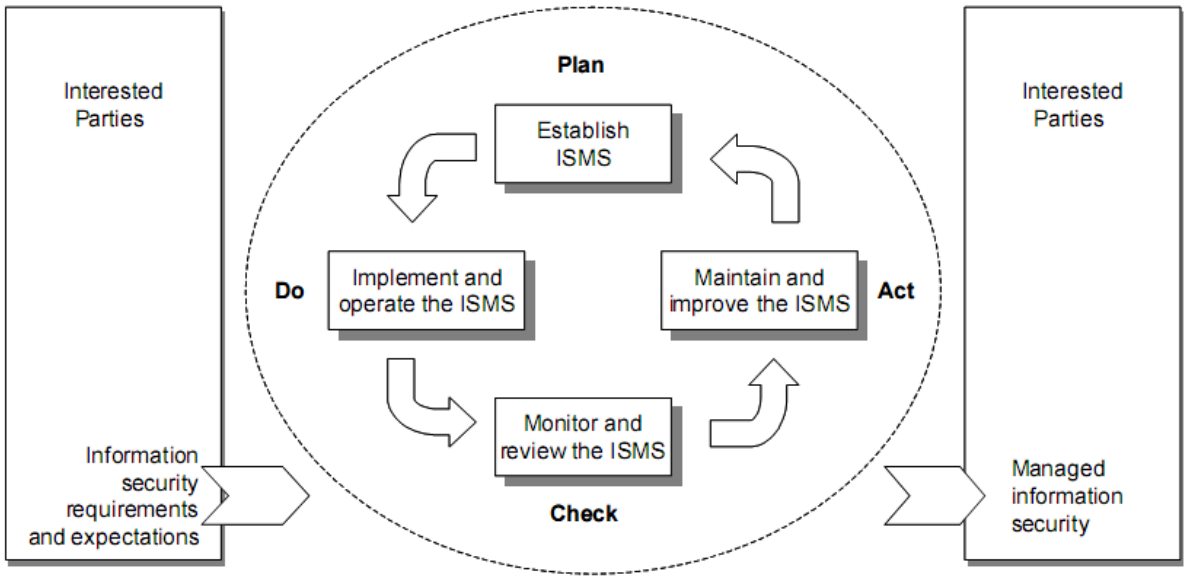


Figure 10: "Plan-Do-Check-Act"-model applied to ISO 27001

The four stages of the circle are explained in the following table:

Plan: Analyze the objectives, processes and policies relevant to managing risk and improving information security. Establish an ISMS policy in accordance with the organizations general strategic business goals.

Do: Implement and operate the policies, controls, processes and procedures defined in the planning phase.

Check: Monitor and review the process performance and analyze if improvements can be made. Results must be reviewed by the management.

Act: If necessary apply corrections or/and preventive actions based on the result of the internal ISMS audit or management review.

Then the circle restarts, the goal is to achieve continual improvement of the ISMS.

ISO 27001 mainly focuses on the process of building and maintaining an Information Security Management System. It is not going into details on how to implement certain controls. Therefore it works hand in hand with the ISO 27002 standard which gives more specific instructions.

The main topics of the ISO 27001 are:

- Information security management system
- Management responsibility
- Internal ISMS audits
- Management review of the ISMS
- ISMS improvement

To give an idea of the information content of the ISO 27001 standards, the following figure shows a sample:

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;

b) ensuring that ISMS objectives and plans are established;

c) establishing roles and responsibilities for information security;

Figure 11: Sample of ISO 27001

Rating

Pros:

- The standard is widely accepted.
- Certifications are available.

Cons:

- It only focuses on how to introduce Information management processes into an organization rather than giving detailed instructions on how to secure the organization's information.

Suitability for our Security Ontology:

Although the information of the ISO Standard 27001 is widely accepted, for our purpose it is not suitable at all. We are looking for a knowledge base that gives detailed information on specific threats and corresponding countermeasures, and for that purpose the ISO Standard 27001 alone is clearly the wrong source.

4.1.2.2 ISO 27002

The ISO 27002:2005[5] - "Information technology – Security techniques – Code of practice for information security management" originates from the BS 7799:1995 and has been revised and republished under different names many times since.

ISO 27002 continues where ISO 27001 stops. Whereas the ISO 27001 formally describes the requirements for an Information Security Management System and therefore focuses on implementing and maintaining the management system itself, ISO 27002 presents a collection of established controls which organizations can implement to achieve compliance to ISO 27001.

Therefore certifications are only against ISO 27001. However, implementation of both standards is somehow a pre-requisite of the former.

Structure of the ISO 27002

After the first three introductory chapters, chapters 4 to 15 contain the main content. ISO 27002 contains 11 security control clauses with a total of 39 main security categories. The main security categories contain one ore usually more controls that can be applied to achieve the objective of the security category. The controls again contain one or more actions or tasks which have to be performed for the control to be effective. All together ISO 27002 contains about 140 controls which are described in approximately 100 pages. Figure 12 shows a mind map of the controls and the categories of the ISO 27002.

[5] The ISO/IEC 17799:2005 has been renamed to ISO/IEC 27002:2005 in the year 2007 to better express its affiliation to the ISO 27000 standards family.

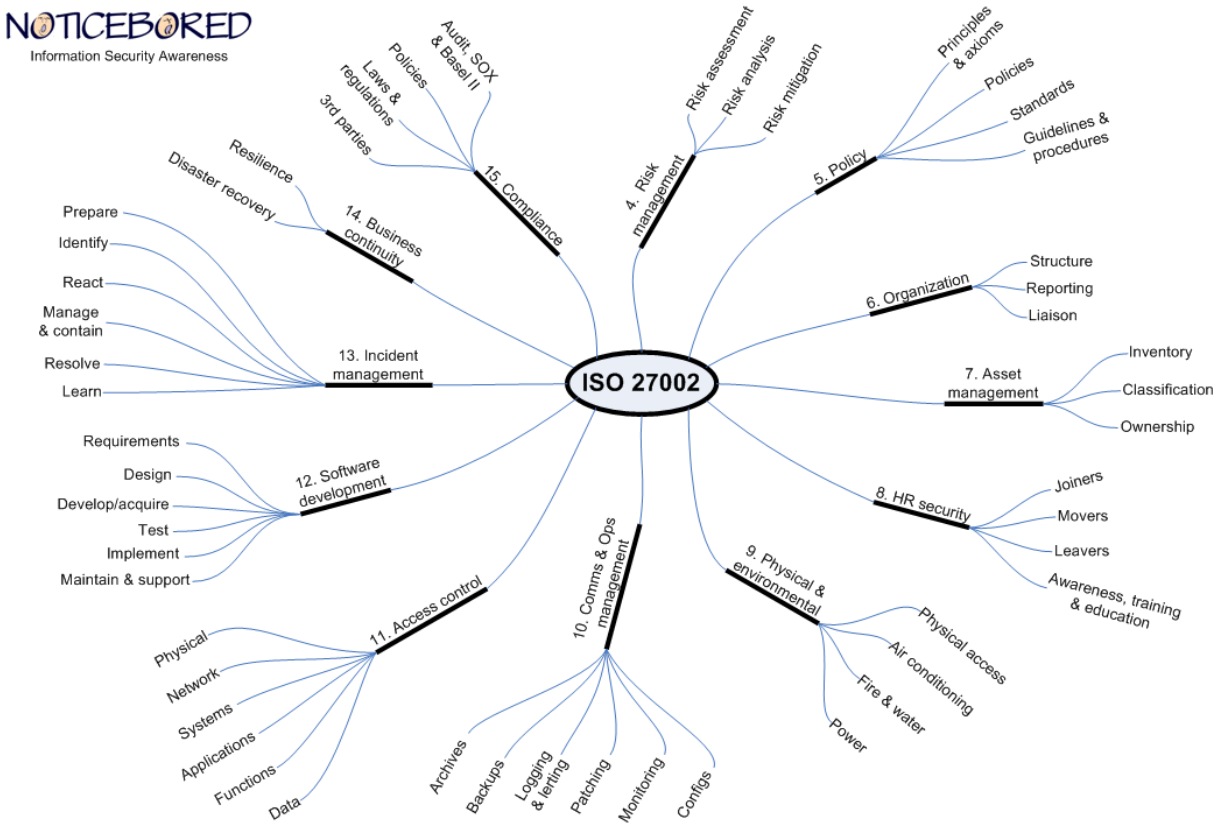


Figure 12: ISO/IEC 27002:2005 Mindmap
(http://iso27001security.com/ISO_27002_mind_map.gif)

Rating

Pros:

- ISO 27002 covers a very general scope and is therefore usable for a very large target audience.
- It is an absolutely necessary guideline for organizations which want to undergo a certification against ISO 27001.
- Due to the close relation to ISO 27001 it is widely accepted and established.
- The descriptions of the controls give a good overview of not only IT-Security related knowledge, but also propagates knowledge on (IT) management topics.

Cons:

- It is not immediately obvious how some controls should be used and how they help protect information.
- The controls in ISO 27002 in general are very generic and in some parts not specific enough. In the end the organization will still need some kind of expert advisory to identify and implement the individually relevant controls.

Suitability for our Security Ontology:

The ISO 27002 is a good guideline for implementing the controls that are necessary to implement ISO 27001's requirements and therefore to secure the information of an organization. However, it is lacking the characteristics of the knowledge base we are looking for. In fact it only focuses on the controls. Therefore the two most important concepts that are missing are:

- No threat concept and therefore no explanation of which control is used against what kind of threats.
- No vulnerability concept

Therefore the ISO 27002 is not suitable as a source knowledge base. However, Stefan Fenz and Andreas Ekelhart have included the controls from the ISO 27002 into SecOnt as a standard reference for our controls and also to allow SecOnt to assist in the ISO 27001 certification process [21].

4.1.3 IT-Grundschutz

4.1.3.1 IT-Grundschutz Overview

IT-Grundschutz is a holistic concept that is aimed at small and medium enterprises and has the goal to help them create an IT-Security level that is adequate to satisfy average protection requirements. It is developed and published by the German "Bundesamt für Sicherheit in der Informationstechnik" (Federal Office for Information Security). The first version has been released 1995 under the name IT-Grundschutzhandbuch (IT-Baseline Protection Manual) and consisted of only 150 pages.

Nowadays IT-Grundschutz consists of four main documents which together count almost 4000 pages. In addition the BSI provides a number of guidelines, example scenarios and software tools to help analyze the individual organizations needs and to implement the relevant concepts.

We want to focus on the largest of those documents - the IT-Grundschutz Catalogues, but first I want to give an overview of the three remaining main documents:

BSI Standard 100-1 Information Security Management Systems (ISMS)

This document describes the general requirements that have to be fulfilled to implement and maintain an information security management system. It follows the concept of the ISO 27001 and therefore is completely compatible with the latter.

BSI-Standard 100-2: IT-Grundschutz Methodology

The BSI-Standard 100-2 describes more practice oriented how an information security management system can be implemented and operated with the IT-Grundschutz approach. The IT-Grundschutz Methodology explains how to create an IT-Security concept, how to select appropriate security measures and with the help of the IT-Grundschutz-Catalogues it also describes how to implement those measures – even at a technical level. It naturally follows the more theoretical concepts described

in the BSI Standard 100-1 and therefore also is also compatible with ISO 27001 standard.

BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz

With the standard approach of IT-Grundschutz it is not absolutely necessary to do risk analysis before implementing the security measures, as the standard "package" is designed to mitigate the average risks and vulnerabilities of an average small or medium sized enterprise. For the target audience that does not fit into this scheme or which needs additional security the BSI-Standard 100-3 provides a method for risk analysis that is specially designed to work with the IT-Grundschutz concept.

4.1.3.2 The IT-Grundschutz Catalogues

After an overview of the various components of IT-Grundschutz we now want to focus on the largest part of the "package" - the IT-Grundschutz Catalogues, which contain the specific information about threats and safeguards.

Structure

The IT-Grundschutz Catalogues, which where called the IT-Grundschutz Manual until 2005, starts with some introductory chapters and continues with its 3 main chapters:

- The Modules-Catalogues
- The Threat-Catalogues
- The Safeguards-Catalogues

The Modules-Catalogues

The Modules-Catalogues describe the typical aspects and applications for IT-Security. Additionally they give an overview of related threat scenarios and a brief listing of applicable safeguards. The main groups are:

- B 1: Generic aspects of IT

  - Contains overlapping topics such as: IT-Security Management, Personnel or Data Backup Policy
- B 2: Security of the Infrastructure
  - This section contains infrastructure related topics such as: Building security, Server Room security, Office security
- B 3: Security of the IT systems
  - In this chapter various (more or less specific) IT systems are discussed. Examples are: General (and operating system specific) server and client machines, network components such as routers and switches, etc
- B 4: Security in the network
  - This chapter contains information about network security and management.
- B 5: Security of applications
  - This section focuses on the security issues of main IT applications such as: Email, Web Servers, Databases, etc. The newer contributions also deal with more specific applications such as Apache Webserver or Exchange 2000 security issues.

Each module comes with a short introduction to the topic and then presents the related threat scenarios and safeguards. The threat scenarios are additionally broken down into the following threat types, which also represent the subgroups in the threat-catalogues: force majeure, organizational shortcomings, human errors, deliberate acts and technical failures. The safeguards are categorized into the appropriate phase of the lifecycle of the module. For example the phases for the building module are: planning and design, implementation, operation, disposal and contingency planning. Those lifecycle phases are not consistent for every module. Unfortunately there are no links between the threat scenario and the related safeguard from the module description.

The Threat-Catalogues

The Threat-Catalogues consist of five sub-catalogues which present various threat scenarios categorized after their threat type. The five threat catalogues are:

- Force Majeure
- Organizational Shortcomings
- Human Failure
- Technical Failure
- Deliberate Acts

The latest version of the threat-catalogues contains more than 400 threat scenarios. The individual threats are first explained and additionally real life examples are given.

The Safeguard-Catalogues

The Safeguard-Catalogues consist of the following 6 catalogues:

- S1 Safeguard Catalogue Infrastructure
- S2 Safeguard Catalogue Organization
- S1 Safeguard Catalogue Personnel
- S1 Safeguard Catalogue Hardware & Software
- S1 Safeguard Catalogue Communication
- S1 Safeguard Catalogue Contingency Planning

The latest version of the safeguard-catalogues includes around 1000 individual safeguards. Besides an overview and a more or less detailed implementation guideline the description of the safeguards also include recommendations concerning who should be the responsible person/role for initiation and implementation.

Rating

Pros:

- Comprehensiveness: With around 4000 pages the IT-Grundschutz Catalogues are the most comprehensive collection of generic IT-Security related best practice knowledge.
- Scope: IT-Grundschutz looks at IT-Security from the perspective of an average sized company with average security requirements. Therefore

it can be used to build a solid IT-Security foundation for a lot of different organizations.

- Compatibility to ISO 27001: Due to the compatibility to the ISO 27001 standard, its content is established, accepted and widely used.

Cons:

- Inconsistency and redundancy: Due to its huge size and the fact that the IT-Grundschutz Catalogues have evolved over time and many different authors have worked on it, the information is not always presented on the same consistency and granularity level.

Suitability for our Security Ontology:

The IT-Grundschutz Catalogues cover IT-Security from the same point of view like SecOnt does. Additionally it contains the biggest number of threat scenarios and safeguards compared to other standards and best practice collections. On the other hand when it comes to logical structuring the IT-Grundschutz has some weaknesses we will need to cope with. More about the incompatibilities and problems is discussed in chapter 5.3.1.

All in all, due to the fact that the cornerstones of the IT-Grundschutz Catalogues meet our requirements best, we have chosen them to be our source of knowledge for the mapping to SecOnt. The process of the mapping and a step-by-step tutorial can be found in chapter 5.3.4.

4.2 OWL Web Ontology Language

This chapter is intended to give a very brief overview of the capabilities, structure and syntax of the OWL Web Ontology Language.

4.2.1 Introduction to OWL

Ontologies provide the functionality to capture and present the knowledge of some domain of interest. To do so they basically describe the concepts of some domain and also the relationships between those concepts. The most popular language for implementing ontologies is OWL [22] which was developed by the Web Ontology Working Group as part of the W3C Semantic Web Activity and was published on 10th February, 2004. The OWL Web Ontology Language has been designed and optimized for machine readability rather than for presenting information to humans. It is a revision of the DAML + OIL web ontology language [23] and therefore also builds on RDF and RDF Schema, which again is a XML dialect.

4.2.2 The Sublanguages of OWL

OWL provides three sublanguages which differ from each other in terms of expressiveness.

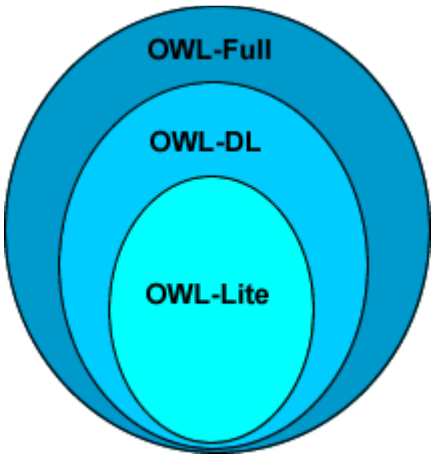


Figure 13: Owl sublanguages

4.2.2.1 OWL-Lite

As we can tell from the name, OWL-Lite is the most lightweight version. It is intended to be used for basic ontologies which only require classification hierarchy

and simple constraints. Its features are very limited, but therefore it also has a lower formal complexity and is hence easier to be used.

4.2.2.2 OWL-DL

"DL" stands for description logics, which implicates that this sublanguage has been optimized for machine readability. It includes all OWL language constructs but they can only be used in a logically correct way to provide computational completeness and decidability. SecOnt uses OWL-DL.

4.2.2.3 OWL-Full

OWL-Full is the most expressive OWL sublanguage. It is intended to be used in situations where syntactic freedom is more important than logical correctness. As computational completeness and decidability are not guaranteed with this sublanguage, it is not possible to perform automated reasoning with OWL-Full ontologies.

4.2.3 Basic Elements of OWL Ontologies

The basic components of OWL ontologies are

- Classes – which represent the abstract concepts of the knowledge domain
- Individuals – which are concrete instances of classes
- Properties – which represent the relations between and attributes of individuals

4.2.3.1 Classes

Classes define the basic characteristics and restrictions of all individuals belonging. Furthermore we can use classes to build hierarchies – so called taxonomies. Sub-classes inherit all characteristics of their super-class and thus information can be broken up into different granularity levels. Every class in OWL is a sub-class of the root class "owl:Thing".

The OWL syntax to create a class is:

```
<owl:Class rdf:ID=”HereGoesTheClassName”>
```

The constructor for creating a subclass is rdfs:subClassOf and is used like this:

```
<owl:Class rdf:ID=”Cat”>
  <rdfs:subClassOf rdf:resource=”#Animal”>
      …
</owl:Class>
```

These are the very basic constructors of the OWL classes. Presenting all features of OWL would go beyond the scope of this document. A complete listing can be found in the OWL Web Ontology Language Reference [24].

4.2.3.2 Individuals

Individuals are the concrete instances of classes and therefore their members. They represent the objects in the domain of interest.

To continue our example, we now want to add an individual to our “Cat” class. This is done with the following statement:

```
<Cat rdf:ID=”Garfield”>
```

4.2.3.3 Properties

Two types of properties can be distinguished:

- Datatype properties are what we would call attributes. They can contain RDF literals and XML Schema datatypes which cover many standard datatypes such as string, integer, etc.
- Object properties are relations between two individuals.

The syntax for properties is:

```
<owl:ObjectProperty rdf:ID="likes">
  <rdfs:domain rdf:resource="#Cat" />
  <rdfs:range rdf:resource="#Food" />
</owl:ObjectProperty>
```

If we wanted to express that our cat Garfield likes the Food Lasagne (we assume that we have already created the class Food and the individual Lasagne) we would use the following statement:

```
<Cat rdf:ID="Garfield">
  <likes rdf:resource="#Lasagne" />
</Cat>
```

Properties can be further specified by characteristics. They can be:

- Transitive
- Symmetric
- Functional
- Inverse
- Inverse and Functional

Further details about properties can be found in the OWL Web Ontology Language Reference [24].

4.2.3.4 Restrictions

It is possible to define constraints on the use of properties in a variety of ways. The following restrictions of properties are possible:

- allValuesFrom – also called the universal quantifier, which can be read as "only"
- someValuesFrom – also called the existential quantifier, which can be read as "at least one, some"
- Cardinality – defines the set of individuals that have a minimum, maximum or the exact number of relationships with other individuals
- hasValue – describes the set of individuals that have a (at least one) relation

Further details about OWL can be found on the website of the OWL Web Ontology Language Guide [25]. How SecOnt uses the various features and components of OWL will be explained in chapter “5.3.4 The Process of Mapping”.

5 SecOnt – Generating Data for an Information Security Ontology

In this chapter I will first give a brief introduction to SecOnt – our security ontology. Afterwards I will explain the concepts and the structure of the ontological model and the porting into the machine-readable OWL-DL standard. The last part of this chapter focuses on how the data was mapped from the IT-Grundschutz Catalogues into the SecOnt structure and describes how the actual knowledge base was built.

5.1 Introduction

SecOnt evolved from research work done by Andreas Ekelhart and Stefan Fenz at the Austrian security research center "Secure Business Austria". In their papers [9, 10, 11] they have introduced an IT-Security related ontological framework with the following capabilities:

- SecOnt can help to clarify the meaning and interdependence of IT-security relevant terms [26].
- SecOnt can improve quantitative risk analysis. Building on established best practices knowledge and a mapping of a company's infrastructure, SecOnt is able to compute the outcome of disaster scenarios.
- Basing on disaster simulation SecOnt can help decision makers to choose the most effective countermeasures to mitigate individual vulnerabilities.
- Due to the addition of an Ontological Mapping of the ISO/IEC Standard to SecOnt [21] the framework is also able to support organizations in the process of the ISO/IEC 27001 certification.

On top of this ontology Ekelhart and Fenz have implemented an application which acts as a graphical user interface for accessing, visualizing and reasoning the knowledge base. The next chapter is describing the architecture of the ontology.

5.2 Structure

The foundation classes of SecOnt - asset, control (=safeguard), vulnerability and threat - are concepts which are well known from the field of classic risk analysis. The SecOnt structure is based on the security relationship model presented in the National Institute of Standards and Technology Special Publication 800-12 [27] which is shown in Figure 14. The NIST Handbook explains the figure as follows: „Safeguards prevent threats from harming assets. However, if an appropriate safeguard is not present, a vulnerability exists which can be exploited by a threat, thereby putting assets at risk.“

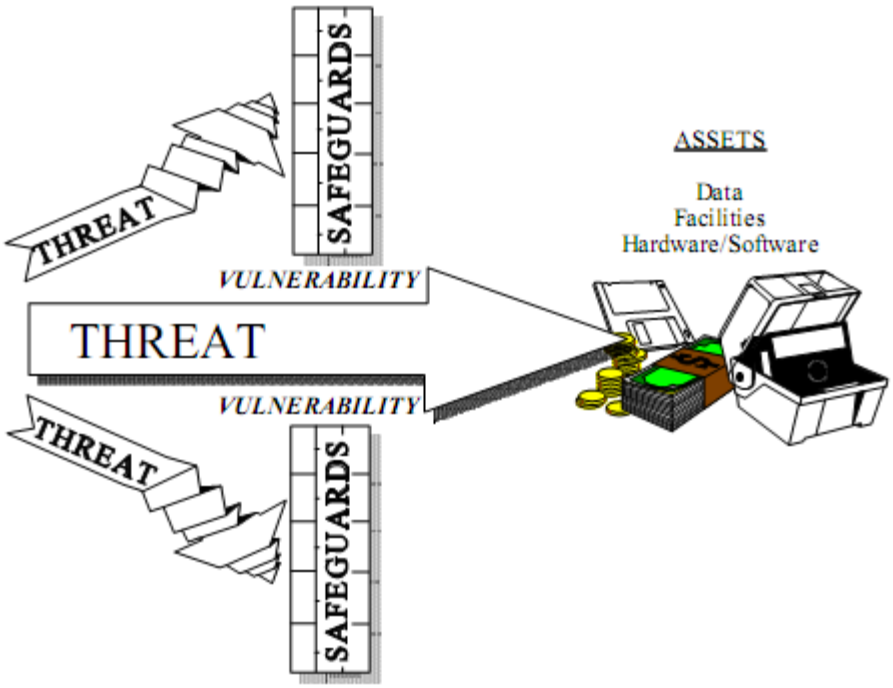


Figure 14: NIST security relationship model [27]

Figure 15 shows a very basic overview of the main concepts of the security ontology and the relations between them. This overview shows only the parts of SecOnt which are relevant for my work – the mapping of information from the IT-Grundschutz Catalogues.

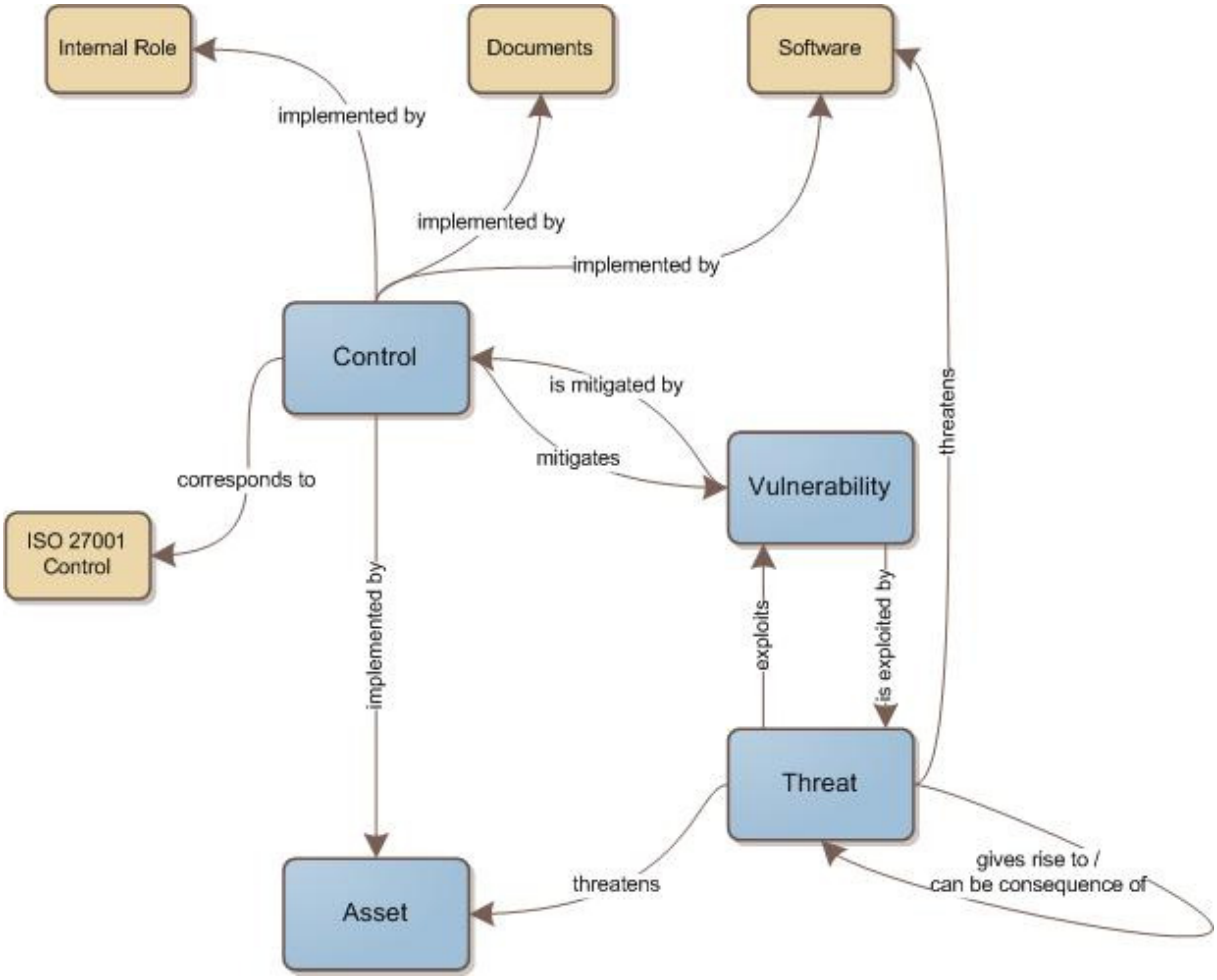


Figure 15: Overview of the security ontology

The core elements and the relations between them are described in the following pages.

5.2.1 Namespaces

As OWL is based on XML we can use xml namespaces to provide the possibility to build unique and reusable vocabularies. For that reason SecOnt introduces various namespaces:

sec: We use the sec: namespace to cover all the security related information. The sec: vocabulary contains the main concepts *Threat*, *Vulnerability*, *Control* and the connections and interrelations between them. To provide additional information SecOnt uses the security related helping concepts *Security Attribute*, *Threat Type* and *Security Rating.* This is the core part of

SecOnt. As a standalone the sec: namespace could be used as a generic Information Security knowledge base. The other namespaces introduced provide additional functionality, but the logic mostly builds on the information from the sec: namespace.

ent: The ent: namespace has been introduced to model an organization together with all its physical and logical connections. It contains *Assets* and relations between them, *Persons* and their *Roles* in the organization, *Data* (Information) and *Documents.*

sof: The sof: namespace is a classified information container for all kinds of software including patches. Dependent on the type of software, the classes in the sof: namespace and their instances have different types of attributes. In SecOnt the classes within this namespace are mainly used as a Control (e.g. software patches, firewall software, etc) or as "Victim" of potential Threats (e.g. Ping of Death attacks Windows NT systems).

iso: S. Fenz et al. have introduced the iso: namespace in order to map the ISO/IEC 27001 standard to SecOnt [21]. Due to the flat hierarchy of the standard they were able to build the structure with only three classes – Categories, Objectives and Controls. SecOnt uses the classes of the iso: namespace to link SecOnt controls to ISO 27001 controls.

abs: We use the abs: namespace to model abstract classes. We wanted to be able to differentiate between concrete and abstract instances. OWL originally didn't work with abstract classes, so we had to build the functionality of abstract classes manually with "tagged" classes. This "tag" is provided through the abs: namespace.

5.2.2 Concepts

As the ontology is coded in the Web Ontology Language OWL the concepts and their sub-concepts are implemented as OWL-classes. The OWL class concept works similarly to the class concept in object oriented programming languages; OWL-classes can have sub-classes which inherit the characteristics and attributes of their super-classes. In this chapter I am going to present the core super-classes of SecOnt

and their attributes. Each super-class acts as a container for similar types of concepts. For clarity reasons we have introduced additional intermediate classes in some class sub-hierarchies, even if the class-attributes wouldn't have required extra classes. Figure 16 shows how we have used the structure of the ISO/IEC 27002 as a basis to create the intermediate sub-classes of sec:Control as an example.

Figure 16: sec:Control class hierarchy

The core super-classes and the relations among them are described in the following listing:

sec:Threat: The threat ontology tries to cover all threats that can possibly harm a small or medium-sized organization. This means not only specifically IT related threats (e.g. virus, denial of service attack, etc), but also natural and environmental threats are implemented.

The sec:Threat class has a **sec:description** property that holds detailed information to the threat topic. This information was collected from the IT-Grundschutz Catalogues.

The **sec:threatType** property holds the type of the threat which can be either of *environmental*, *human* or *natural* origin.

With the **sec:givesRiseTo** and the **sec:canBeConsequenceOf** properties interrelations between threats can be modeled.

The **sec:affects** attribute holds the endangered security objectives following the security- and dependability taxonomy referring to Avizienis et al. [3], which are *confidentiality*, *integrity*, *availability*,

accountability, *authenticity*, *reliability* and *safety*. Thus an organization can build their IT-Security strategic decisions considering specific security attributes.

The threat is connected to one or more *vulnerabilities* it can exploit through the **sec:exploits** property.

If a threat manages to exploit a vulnerability it threatens either one or more *assets*, *data*, *people* (=role) or *software* (or combinations of those). This connection is described with the **sec:threatens** attribute. Due to the high granularity of the threat knowledge base, these attributes are only applied to the threat, which explicitly poses a threat, e.g. an earthquake (= threat) does not directly threaten a company's asset (data, role or software). Instead, for reasons of flexibility and reusability, we have introduced subsequent threats, such as Asset Damage and Injury, which are connected to the threat "earthquake" through the sec:givesRiseTo attribute. Asset Damage directly affects an asset, just like Injury would directly affect an instance of the class ent:Role.

Figure 17 shows an overview of the class sec:Threat.

sec:Threat		
sec:description	String	
sec:threatType	Instance*	sec:ThreatType
sec:givesRiseTo	Instance*	sec:Threat
sec:canBeConsequenceOf	Instance*	sec:Threat
sec:affects	Instance*	sec:SecurityAttribute
sec:exploits	Instance*	sec:Vulnerability
sec:threatens	Instance*	sof:Software
		ent:Data
		ent:Role
		ent:Asset

Figure 17: Owl-Class sec:Threat

sec:Vulnerability: According to the NIST-Handbook [27] and the security relationship model shown in Figure 14 a vulnerability exists if an

appropriate safeguard to stop a threat is absent. We have categorized vulnerabilities into three subclasses: administrative, physical and technical vulnerabilities.

The **sec:description** attribute holds a short description of the vulnerability in natural, human readable language. The description is derived from the corresponding safeguard.

Furthermore it is possible to rate the severity of the vulnerability through the **sec:vulnerabilitySeverityRating** property. This can help management to prioritize strategic options.

Each vulnerability can be exploited by one or more threats, which is implemented by the **sec:exploitedBy** attribute, and can be mitigated by one or more controls, which is represented by the **sec:mitigatedBy** attribute.

Figure 18 shows an overview of the OWL class sec:Vulernability.

sec:Vulnerability		
sec:description	String	
sec:vulnerabilitySeverityRating	String	
sec:exploitedBy	Instance*	sec:Threat
sec:mitigatedBy	Instance	sec:Control

Figure 18: OWL-Class sec:Vulnerability

sec:Control: A Control (or Safeguard) defines instructions on how to mitigate certain vulnerabilities. They can be implemented either by installing infrastructure resources, using organizational controls and policies, employing special personnel or by installing and/or configuring appropriate security software. These connections are modeled as relations to the classes asset (e.g. lightning arrester), documents (e.g. non smoking policy), internal or external roles (e.g. security guard) and software (e.g. anti-virus software). Complementary implementations (e.g. an automatic fire extinguishing system consists of smoke detectors and fire extinguishers) or implementation alternatives (e.g. fingerprint scan or iris scan) can be distinguished in the knowledge

base. Each control consists of a very detailed description which gives the instructions on how to implement the control, a list of the associated vulnerabilities, a connection to the classes that actually implement the control and a link to the appropriate ISO 27001 Control that is covered by it.

Figure 19 shows an overview of the OWL class sec:Control.

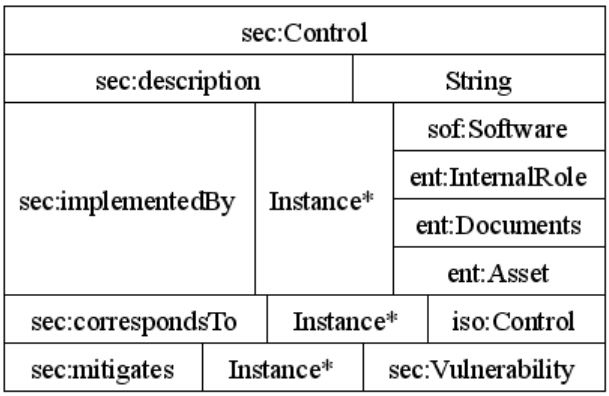


Figure 19: Owl-Class sec:Control

ent:Asset: Assets are a company's belongings. This includes everything from the building it is located in to the secretary's phone. SecOnt distinguishes between movable and immovable assets. Immovable assets are modeled on a highly granular level (e.g. Wall, Room, Door, Water Pipe, etc.) to provide the possibility to map an organizations entire physical infrastructure as exactly as possible, so we can answer questions like: Which room is located next to room A? What is above this room? etc..

Immovable assets have the property **ent:locatedIn** which stores the information in which room the asset is placed.

With this information available it is possible to run special threat scenarios (provided we have necessary additional data) and to calculate the damage those threats would cause. For example: What damage would a fire cause if it broke out in room B and it took 27 minutes to extinguish?

ent:Documents: The Documents class represents an organizations policies, guidelines, contracts etc. A control can be linked to an instance of the document class. For example if the control says that a certain agreement has to be signed, it can point to the related instance of the document class. The document class has a property (**ent:storedOn**) which links to the storage site (server, filename path). That way it is possible to tell if a particular document has been affected by a specific infrastructure failure (e.g. server crash).

ent:Data: The Data class represents an organization's business Data as well as administrative Data. It has a relation (**ent:storedOn**) to the infrastructure class (storage site, server, filename) to model if specific data have been affected by an infrastructure failure. Furthermore Data can be classified to improve decision making (**ent:classification**).

ent:Role: A role is a person who has been assigned a specific function. One person can be assigned more than one roles. We distinguish between internal and external roles. Real persons relevant for the organization are modeled with an instance of the class **ent:Person** and are connected to one or more roles.

sof:Software: The class sof:Software and its subclasses provide a categorized repository for all kinds of software, starting with sec:BusinessFunctionSpecificSoftware and going to sec:SoftwarePatch. Software can be directly targeted by threats (e.g. DDoS attack on WinNT) and can also be used as an implementation of a control (e.g. Patch for WinNT, Anti-Virus Program).

ISO 27001 Control: The ISO 27001 standard has been mapped to SecOnt in a previous work by Stefan Fenz et al [21]. It has been split and mapped into its three hierarchy levels – **iso:Category**, **iso:Objective** and **iso:Control**. SecOnt controls can be connected to the corresponding

iso:Control. The aim is to guarantee a certain level of credibility and to provide support with the ISO 27001 certification process.

5.2.3 Relations

A potential **Threat** first has to *exploit* a **Vulnerability** to be able to actually *threaten* an **Asset** and thereby affect specific security attributes (e.g. confidentiality, integrity, availability,…): e.g. a Lightning flash (Threat) can be destructive for a building if no lightning arrester is installed (Vulnerability)

According to the NIST Handbook [27] a **Threat** is no danger to an organization's assets without a matching **Vulnerability**: e.g. if an organization's building is located in Egypt it is not vulnerable for Blizzards so Blizzards pose no Threat.

A **Control** is put in place to *mitigate* one or more **Vulnerabilities**: Preventive, corrective or detective actions are used to neutralize or minimize a potential threat's impact. For instance a Secure Password Policy (Control) mitigates the Vulnerability "Insecure Passwords" which could be exploited by systematically trying out passwords (Threat).

A **Threat** itself *can give rise to* another **Threat**. This interrelation modeling provides the essential information for further risk analysis and substantial security planning: e.g. the failure of the security system, which is a threat itself, could lead to Unauthorized Access, which also is a threat.

Controls can be *implemented by* different means. They can be implemented by **Assets** (e.g. Lightning Arrester), by **Documents** that define a specific process or obligation (Policy), by employees, i.e. **Internal Roles** (e.g. Security Guards), by Software (e.g. Anti-Virus-Software) or of course by combinations thereof.

Controls *correspond to* a Standard Control to guarantee a certain level of credibility. As our controls are highly granular they can correspond to several Standards or best practice frameworks at the same time. At this time the **ISO 27001 Controls** are included into SecOnt but the structure can easily be expanded to hold more references.

5.2.4 Abstract/Concrete Instances

As mentioned above we distinguish between abstract and concrete instances of classes. Naturally ontologies are not intended to work with the concept of abstract classes, but we want to be able to explicitly tell the difference between concrete instances and abstract concepts.

Here is an example why we want to use abstract instances:

Within the ent: namespace of SecOnt we provide a knowledge pool of infrastructure that can be used as countermeasures against certain threats. Those are only concepts and are clearly not really existent. They can be used to answer questions like “What would company A need to implement as a countermeasure against lightning damage?” The answer would be “a lightning arrester”. We have implemented such cases with an abstract object within the corresponding class, in this case it would be abs:LightningArrester as an object of the ent:LightningArrester class within the infrastructure container.

Every class therefore initially contains only an abstract class!

Here is an example why we want to use concrete instances:

On the other hand, for risk analysis we need to be able to map entire company buildings including the infrastructure inside them and relations among them. For example: in ent:Room1 we have the PCs ent:PC1, ent:PC2 and ent:PC3. On an abstract level the concept “fire” threatens abstract assets. In this concrete case the concrete fire sec:fireA breaks out in the concrete Room ent:Room1. As PCs are assets the fire threatens and finally damages the concrete PCs ent:PC1, ent:PC2 and ent:PC3.

Concrete instances are used for risk analysis and are filled in by the “end-user”!

5.3 Mapping the IT-Grundschutz Catalogues to SecOnt

After the process of analyzing various available standards and best practice collections related to the field of IT-Security, which has been described in chapter 3 of this document, we have found the BSI's IT-Grundschutz Catalogues to be the best suitable for our needs and have chosen them to be our source of information for the security ontology.

The next step was to extract information out of the over 3000 pages of text, to alter it in a way to fit the SecOnt structure and to extend the SecOnt knowledge base by the newly generated information.

In this chapter I am going to subsume the problems we faced during this process, the approach we followed to overcome them and the result which has been generated.

5.3.1 Problems/Incompatibilities

Unfortunately we were not lucky enough to find the IT-Grundschutz Catalogues to be designed to fit the SecOnt structure originally, so we first had to overcome some incompatibility problems.

The IT-Grundschutz Catalogues are very good when used by the human reader. They are probably the most comprehensive accumulation of generic IT-Security related knowledge from an SME's perspective worldwide, but due to the immense coverage and complexity of information, for the authors it is naturally very hard to present the results on a consistent granularity level. The IT-Grundschutz Catalogues have grown over time and many different authors have worked on its content, so the perspectives and specificity of the various topics vary – tremendously in some parts – resulting in incompatibilities on a logical level.

In the following paragraphs I am going to explain the problems and incompatibilities we had to solve during the process of mapping the IT-Grundschutz Catalogues to SecOnt:

5.3.1.1 No concept for Vulnerabilities in the IT-Grundschutz Catalogues

The IT-Grundschutz Catalogues do not use the concept of vulnerabilities, unlike the NIST Handbook [27], on which the structure for SecOnt is built. Instead the IT-Grundschutz Catalogues mix up the concepts of Threats and Vulnerabilities, e.g. the threat "T 2.30 Inadequate domain planning" is not a threat from the NIST Handbook's point of view. When we take a look at the definition of a threat in the NIST Handbook "*A threat is an entity or event with the potential to harm the system. …"* and the definition of a vulnerability "*A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. …*" we can see that "Inadequate domain planning" can clearly be identified as a "weakness in technical controls" and therefore would be a vulnerability after NIST Handbook criteria.

Due to this confusing categorization we had to extract the vulnerabilities from the threats, respectively we had to create the missing vulnerabilities by implication from related controls.

5.3.1.2 Vague connections between Threats and Safeguards

As mentioned before the IT-Grundschutz Catalogues are intended to be used by the human reader. It is a 3000 pages strong reference book for system administrators, IT Managers and other people dealing with IT-Security.

Unfortunately, on a logical level it is inconsistent. Connections between threats and safeguards (=countermeasures, controls) are not clearly evident, only some, but not all, are described in the scrolling text. Threats and safeguards are listed together with the object they relate to, but no connection between a threat and the corresponding safeguard is presented. On the other hand the safeguards are distinguished on the basis of the phase in which they should be applied. This may be useful for introducing and implementing an Information Security Management System according to IT-Grundschutz, but for our purpose it is inapplicable and therefore confusing.

To sum it up, the problem was to produce clear relations between a threat and the corresponding safeguard, which initially was not possible due to the structure of the main document of the IT-Grundschutz Catalogues. Fortunately the BSI provides

additional tools and documents that helped us to overcome this problem. Those are discussed in chapter 5.3.2.2 and 5.3.3.2.

5.3.1.3 No relations between threats

The last paragraph describes some structural problems of the IT-Grundschutz Catalogues concerning logical inconsistency. Those problems also affect incompatibility No. 3.

As mentioned before we want to be able to model potential “chain reactions” in order to make a better risk assessment. Unfortunately the IT-Grundschutz Catalogues do not describe connections between individual threats. Therefore we have to model them ourselves. The problems of varying information depth (No. 4), redundant and overlapping information and concepts (No. 5.) make this task very complex.

5.3.1.4 Inconsistent granularity of information

As the IT-Grundschutz Catalogues have grown over time and many different authors have worked on it, the extent of information with which a topic has been treated, and the perspective under which certain concepts have been described are inconsistent.

For example on the one hand the IT-Grundschutz Catalogues propose the threat “Improper IT system administration” which objectively examined is a very vague description of a threat and can mean anything. On the other hand they cover threats like “Poor planning of the migration of Exchange 5.5 to Exchange 2000” which is a very specific case and is not important for most of the readers.

As we aim to produce a consistent knowledge base with a similar grade of information detail, we have had to filter and transform the information of the IT-Grundschutz Catalogues.

5.3.1.5 Redundancy and overlapping of information

The problem of information redundancy and overlapping is actually very much related to the problem previously stated. Due to the same reasons which were mentioned above, namely a number of different authors, a big scope, a complex domain and a certain timeframe in which the document has grown, only to name a few, many topics have redundant information, respectively cover an overlapping scope. As furthermore there is no connection to other threats, every threat has to be described individually, isolated from all the other (related) threats.

Examples for redundant information would be the threats “Computer Viruses” and “Macro Viruses”. The description of the threat “Computer Viruses” already covers the topic “Macro Viruses”, therefore there is no need for an extra listing, at least not on the same hierarchy level.

This kind of information presentation is confusing and inconsistent on a logical level. Therefore we had to adapt the flat hierarchy of the IT-Grundschutz Catalogues to support a class-based information container.

5.3.1.6 Scope not fully congruent

The scope of the IT-Grundschutz Catalogues includes some domains, which we have decided are not relevant for the SecOnt knowledge base.

The IT-Grundschutz Catalogues, similar to the ISO 27001 standard, cover topics which help to implement a sustainable IT-Security management system. As we intend to model “hard facts” with SecOnt, these types of management and organizational directions are out of scope for SecOnt.

On the other hand some topics that are important for the SecOnt knowledge base are only described superficially or are not mentioned at all.

Therefore we have had to correct the scope by excluding some sections and including others from other sources.

5.3.2 Tools

This chapter presents the tools which were used to solve the incompatibility problems presented in the previous chapter. Furthermore I am going to give a brief introduction to Protégé-OWL, a free, open source ontology editor, which we have used to create and edit SecOnt.

Fortunately the publishers of the IT-Grundschutz Catalogues, the German "Bundesamt für Sicherheit in der Informationstechnik" (BSI), have created a number of useful tools and documents to facilitate the handling and use of the standard. Two of those tools which were especially useful and important in the process of solving the problems and creating the mapping are the "Allocation Table ISO 27001/27002 to IT-Grundschutz Catalogues" and the "Cross-reference table", which are presented in the following paragraphs.

5.3.2.1 Allocation Table ISO 27001/27002 to IT-Grundschutz Catalogues

(OT: Zuordnungstabelle ISO 27001 sowie 27002 und IT-Grundschutz) [28]

As described earlier the IT-Grundschutz Catalogues together with its 3 complementing standards – the BSI Standard 100-1, the BSI Standard 100-2 and the BSI Standard 100-3 – describes a standard approach to plan, build and maintain an Information Security Management System. ISMS built with the help of the BSI approach also meet the requirements of the ISO Standards 27001 and 27002.

The allocation table shows the relationship and the correlations between the requirements of the ISO 27001 and ISO 27002 standards on the one hand and the BSI documents on the other.

Figure 20 shows a snippet of the allocation table ISO 27002 to the IT-Grundschutz Catalogues. The first two columns show the section and the name of the ISO 27002 control. Corresponding content in the BSI documents is listed in the third column. Due to the reason that the BSI documents are much more detailed than the ISO standards, most of the time more than one BSI chapter are related to one ISO control. In those cases the primary source of information is shown in bold letters. The sample shows some of the ISO 27002 controls dealing with Operating system access control. Unfortunately the allocation table is only available in German.

	11.5	Operating system access control	
	11.5.1	Secure log-on procedures	**M 4.15 Gesichertes Login** M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.321 Planung des Einsatzes von Client-Server-Netzen M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz M 4.133 Geeignete Auswahl von Authentikations-Mechanismen
	11.5.2	User identification and authentication	**M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen** M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
	11.5.3	Password management system	**M 2.11 Regelung des Passwortgebrauchs** M 4.133 Geeignete Auswahl von Authentikations-Mechanismen
	11.5.4	Use of system utilities	**M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien**

Figure 20: Allocation table ISO 27002 to IT-Grundschutz

This allocation table helped us tremendously with building our iso: namespace and linking ISO 27001/27002 controls to SecOnt controls. The iso: namespace was described in detail in chapter 5.2.1 Namespaces.

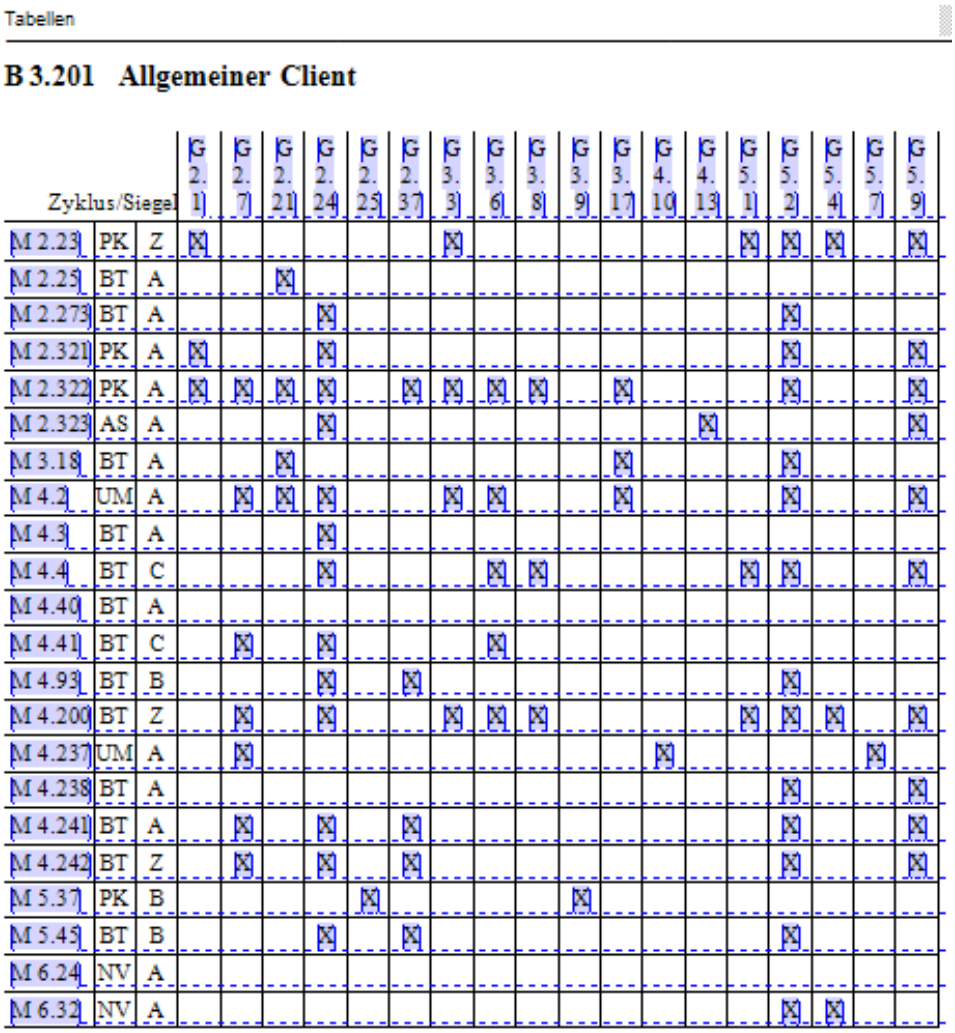
5.3.2.2 Cross-reference tables

(OT: Kreuzreferenztabellen der IT-Grundschutz-Kataloge) [29]

A total of 72 cross-reference tables, one for each module of the IT-Grundschutz Catalogues, describe the connections between the related threats and safeguards. Unfortunately the cross-reference tables are again only available in German.

Figure 21 shows the example cross-reference table related to the module B 3.201 General Client. The rows of the table describe the safeguards which are related to the module (in the German version of the document labeled M, in the English version S) and the columns describe the threats which are related to the module (German = G, English = T). If a connection exists between a threat and a safeguard the point of intersection is marked “X”.

Looking at the example in Figure 21 we see a connection between G 2.7 and M 4.2 which in the English version would be *T 2.7 Unauthorized use of rights* and *S 4.2 Screen Lock,* meaning that the threat “Unauthorized use of rights” can be mitigated by implementing an automatic “Screen Lock” safeguard. Basically we took the information from these cross-reference tables and tried to transfer it directly to the SecOnt mapping. However, due to the previously discussed problems, in a lot of cases we could not use those direct relations.



Tabellen

B 3.201 Allgemeiner Client

Zyklus/Siegel			G 2. 1	G 2. 7	G 2. 21	G 2. 24	G 2. 25	G 2. 37	G 3. 3	G 3. 6	G 3. 8	G 3. 9	G 3. 17	G 4. 10	G 4. 13	G 5. 1	G 5. 2	G 5. 4	G 5. 7	G 5. 9
M 2.23	PK	Z	X						X							X	X	X		X
M 2.25	BT	A			X															
M 2.273	BT	A				X											X			
M 2.321	PK	A	X			X											X			X
M 2.322	PK	A	X	X	X	X		X	X	X	X		X				X			X
M 2.323	AS	A				X									X					X
M 3.18	BT	A			X								X				X			
M 4.2	UM	A		X	X	X			X	X			X				X			X
M 4.3	BT	A				X														
M 4.4	BT	C				X				X	X					X	X			X
M 4.40	BT	A																		
M 4.41	BT	C		X		X				X										
M 4.93	BT	B				X		X									X			
M 4.200	BT	Z		X		X			X	X	X					X	X	X		X
M 4.237	UM	A		X										X					X	
M 4.238	BT	A															X			X
M 4.241	BT	A		X		X		X									X			X
M 4.242	BT	Z		X		X		X									X			X
M 5.37	PK	B					X					X								
M 5.45	BT	B				X		X									X			
M 6.24	NV	A																		
M 6.32	NV	A															X	X		

Figure 21: IT-Grundschutz cross-reference table

To discuss one of those cases let's take a look at the intersection point of "T 2.24 Loss of confidentiality of sensitive data of the network to be protected" and "S 4.3 Periodic runs of a virus detection program". In fact, there is no direct relation between those two concepts. We have to introduce a third concept to connect those two – the Threat "Computer virus". Now the scenario looks like this:

Periodic runs of a virus detection program (S 4.3) would mitigate the chance of a computer virus (T 5.23) infection of a PC (B 3.201 general client). An active computer virus could give rise to the possibility of loss of confidentiality of sensitive data of the network to be protected (T 2.24).

Only at this point, with the concept "Computer virus" in place, has the scenario become conclusive.

Another problem is the lack of differentiation between vulnerabilities and threats. The threat "T 2.1 Lack of, or insufficient, rules" – which, by the way, affects almost every module in the IT-Grundschutz Catalogues, simply because it is too superficial – would, according to our classification from the NIST-Handbook [27] – be a classic vulnerability, the absence of sufficient countermeasures, respectively controls.

To sum up, the cross reference tables have helped us to get a more structured access to the information and the relations between the various concepts. However, due to the missing feature of interrelated threats and the lack of differentiation between vulnerabilities and threats the cross-reference tables could only be used as a guiding principle.

5.3.2.3 Protégé-OWL

The Web Ontology Language (OWL), as described in chapter 4.2, is technically based on RDF / RDF-Schema and thus is an XML dialect. It would be impossible to build such a complex ontology like SecOnt only by using a text editor to edit some thousand lines of plain-text XML code. Therefore we have used a graphical development environment to assist us with the implementation of the SecOnt knowledge base.

The market leading products in this field are "Altova SemanticWorks®"[6] and "Protégé-OWL"[7]. Because the latter is free, open source, extensible and has a big community, we have decided to use Protégé-OWL. Protégé-OWL provides a clear graphical user interface with widgets and plug-ins for all the features of the Web Ontology Language and even more. For visualization we have used the Ontoviz[8] plug-in, which is able to automatically create a graphical illustration from Protégé ontologies.

Chapter "5.3.4 The Process of Mapping" contains screenshots showing Protégé-OWLs user interface of program parts we have used to create SecOnt. To

[6] Semantic Web Tool: http://www.altova.com/products/semanticworks/semantic_web_rdf_owl_editor.html, last access: July 8 2008
[7] what is protégé-owl?: http://protege.stanford.edu/overview/protege-owl.html, last access: July 8 2008
[8] OntoViz: http://protegewiki.stanford.edu/index.php/OntoViz, last access: July 8 2008

learn more about Protégé-Owl and how to build ontologies with it I would like to refer to [30] and [31].

5.3.3 Methods

This chapter presents the methods that have led to the solutions to the previously discussed problems. The numbering of the following subchapters correlates to the related subchapters under 5.3.1 Problems/Incompatibilities.

5.3.3.1 Deriving vulnerabilities

As mentioned before, the IT-Grundschutz Catalogues do not use the concept for vulnerabilities. Instead, they mix up threats and vulnerabilities. Because SecOnt is built on the NIST security relationship model as shown in Figure 14, which differentiates between threats and vulnerabilities, we have had to derive the vulnerabilities ourselves.

In those cases where the German Protection Baseline Manual has mixed classic vulnerabilities into their list of threats, we have used the following approach:

We first had to clarify if the threat was really a threat or if it was – evaluated after the NIST Handbook definition – a vulnerability. If it was a vulnerability, we had to classify it as such in our SecOnt Ontology and had to link it to the corresponding threats and controls.

An example would be the vulnerability “sec:FailureOfExistingSafetyDevices” which has been derived from the threat T 4.3 and has been linked to the threat “sec:Fire” through the property “sec:canBeExploitedBy” and to the control “sec:InhouseMaintenanceAndRepairRegulationControl” through the property “sec:canBeMitigatedBy”.

In the cases where the IT-Grundschutz Catalogues didn’t hold a corresponding vulnerability to a threat at all, we had to create one ourselves. Here the approach was as follows:

As we were aiming to create an easily comprehensible solution, we derived the vulnerabilities from the controls by implication. Our approach is again based on the NIST Handbook which says “*Vulnerabilities are often analyzed in terms of missing safeguards*”. The following paragraph shows a typical example:

If we take a look at the control “sec:FireDoor” – meaning that fire doors should be in place - the derived vulnerability would be “sec:NoFireDoors”, which implicates that no fire doors are in place and that this is a vulnerability which can be exploited by a spreading fire.

Every vulnerability can only be mitigated by one control. But one control can mitigate one or more vulnerabilities. Therefore there is a 1:n relation between vulnerabilities and controls.

5.3.3.2 Creating direct relations between Threats and Safeguards

In chapter “5.3.1.2 Vague connections between Threats and Safeguards” I have explained that we initially had the problem, that the IT-Grundschutz Catalogues do not give structured information about which threat is linked to which safeguard.

As described in the chapter “5.3.2.2 Cross-reference tables”, we have used the BSI provided cross-reference tables for the IT-Grundschutz Catalogues to get a more structured access to the relations between threats and safeguards.

Thus basically we used the information from the cross-reference tables as a guideline to transferring the relations to the concepts we used with SecOnt. However, because of other problems, which were discussed in chapter “5.3.1 Problems/Incompatibilities” and “5.3.2.2 Cross-reference tables”, we had to be very careful and selective with this information.

The biggest problem was that, due to the missing interrelations between threats, a lot of threat-safeguard relations from those tables were not direct relations – as already shown in an example in chapter 5.3.2.2. It was necessary to interpose one or more other threats to create a consistent threat-safeguard scenario. In the following chapter I am going to explain how we created those interrelations.

5.3.3.3 Creating relations between Threats

Due to the lack of connections between threats in the IT-Grundschutz Catalogues and the requirement for SecOnt to be able to model chain reactions we had to manually create interrelations between threats.

Therefore we had to analyze the relevant threats contentswise and build appropriate links. At the beginning of this process the hardest part was to identify a hierarchy of threats. We have tried not to build generic sub-classes which are used only for categorization purposes (i.e. “active attack” – “passive attack”), because we wanted every class to be a concrete threat itself. However, some threat classes have subclasses, which constitute specific forms of the mother-threat.

During this process a handful of top-hierarchy threats have emerged. The most important are:

- Data Disclosure
- Data Tampering
- Data Loss

Most of the other threats show a probability to eventually lead to one of the above threats. Figure 22 illustrates an example of how a Lightning Impact can lead to Theft and end in Data Loss.

After the creation of a solid basis of categories it has become getting a lot easier to classify the threats out of the IT-Grundschutz Catalogues and integrate them into the appropriate SecOnt Threats.

To convey an idea of how complex the final network of interrelations has got, I would like to point to a illustration, which, due to its large size, cannot be integrated into this document but instead can be found at http://securityontology.securityresearch.at/img/Threat_Interrelations.gif.

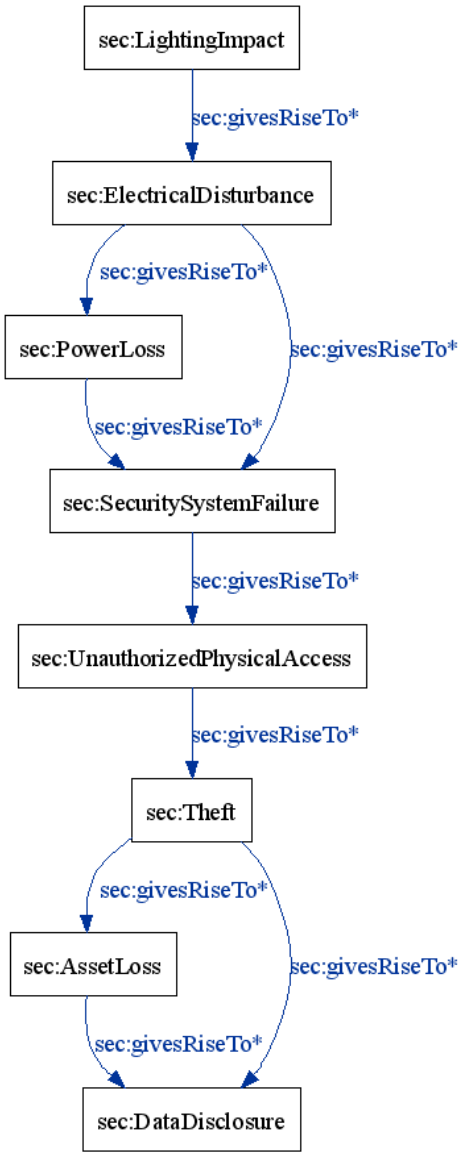


Figure 22: Threat interrelations between Lightning Impact and Data Loss

5.3.3.4 Creating a consistent and appropriate level of granularity

As already mentioned in 5.3.1.4 the IT-Grundschutz Catalogues contain some topics which cover very general areas in IT-Security while others are dealing with very specific problems, which are not relevant for most of the readers.

We basically left out those topics and didn't map them to the SecOnt knowledge base. Unfortunately there is no general rule for what information is too generic and what is too specific, so our rule of thumb was to try to maintain a solid basis of IT-Security knowledge without getting bogged down in details.

As a minimum requirement for what to apply from the IT-Grundschutz Catalogues to SecOnt we have used the Allocation Table ISO 27001/27002 to IT-Grundschutz Catalogues which was discussed in chapter 5.3.2.1.

On the other hand, whenever we felt that a certain module was described as being to superficial we either completed the initial description with the information we felt was missing, or we created a more specialized version of the module additionally.

5.3.3.5 Filtering redundant and overlapping information

As already discussed in "5.3.1.5 Redundancy and overlapping of information" the IT-Grundschutz Catalogues's problem with redundancy is that they do not support different levels of hierarchy.

SecOnt is using the Web Ontology Language (OWL) and therefore is able to use the concept of classes and subclasses. OWL classes have similar characteristics as classes in object-oriented programming languages, which amongst others are that subclasses inherit the properties of their superclass. That function allows us to model characteristics that are similar for every subclass on the superclass level. Only the specific properties which are not shared with all the other subclasses on the same level, have to be modeled individually.

Hence in SecOnt we have modeled topics which contain redundant concepts and information with the help of subclasses. Figure 23 shows an example for the concept "Computer Virus". The superclass would be "sec:ComputerVirus" which then can be further categorized and described in its subcategories "sec:BootSectorVirus" and "sec:MarcoVirus".

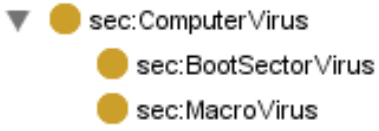


Figure 23: Subclasses against redundancy

The properties which would apply on the superclass (sec:ComputerVirus) level, and therefore are also valid for its subclasses, would be:

- sec:canBeConsequenceOf only (sec:UnauthorizedUseOfITSystems or sec:NonComplianceWithITSecurityMeasures or sec:ActiveWebContent)

- sec:exploits only (sec:InsecureInvocationOfExecutableFiles or sec:NoVirusScanner or sec:NoRegularPatching or sec:NoRegulatedProcedureInTheEventOfMalwareInfection or sec:NoRegularUpdatesOfAntiVirusSoftware)
- sec:givesRiseTo only (sec:DataLoss or sec:DataTampering or sec:ITandTelecommunicationInfrastructureFailure)
- sec:threatens only ent:Computer

In this case the inherited properties of the superclass do not have to be altered at all to fit the properties of both of the subclasses.

This way we were able to create a class-based knowledge base which can easily be improved and extended. At the same time we could eliminate the redundancy problem of the information source – the IT-Grundschutz Catalogues.

5.3.3.6 Altering the scope

Due to the reasons discussed in 5.3.1.6 we had to adjust the scope of the IT-Grundschutz Catalogues to fit the requirements of SecOnt. Therefore we had to exclude certain topics from the original source.

Generally, the IT-Grundschutz Catalogues contain many topics which are too specific to be transferred to SecOnt. But apart from the correction of the scope which was already discussed in “5.3.3.4 Creating a consistent and appropriate level of granularity” we wanted to filter out topics which do not contain “hard facts”. This problem mainly affects the safeguards in the IT-Grundschutz Catalogues.

Generally speaking we simply did not include safeguards which were related to the processes around the topic “How to build, implement and maintain an Information Security Management System”. As already discussed in “4.1.2.1 ISO 27001” this is the domain which is dealt with in the ISO 27001 standard. We have also determined in this chapter, that the information in the ISO 27001 standard does not cover the domain we want to map with SecOnt.

Note: The IT-Grundschutz Catalogues includes these domains to be compatible with the ISO 27001 Standard, but for our purpose at this time it is not required to be included in SecOnt.

Unfortunately those topics are more or less scattered through the IT-Grundschutz Catalogues, but most of them can be found at the end of chapter “S2 Safeguard Catalogue Organization”.

Some examples of safeguards we have not mapped to SecOnt because of the reasons discussed above are:

- S 2.335 Defining the IT-Security objectives and strategy
- S 2.337 Integration of IT-Security in organization-wide workflows and processes
- S 2.199 Maintaining IT-Security
- S 2.200 Preparation of management reports on IT-Security

There were also topics which we wanted to be included in SecOnt that, despite the immense coverage, were not covered by the IT-Grundschutz Catalogues at all. In such cases where we felt an aspect was missing, we have created the class on our own. The description of the concept was mostly taken from third party resources (e.g. Wikipedia[9]). In all cases, whether the source was the IT-Grundschutz Catalogues or something else, the rdfs:comment property of the instance in the SecOnt knowledge base contains a reference to the original source.

[9] www.wikipedia.org – is a multilingual, open content encyclopedia. It is the largest, fastest-growing and most popular general reference work currently available on the Internet.

5.3.4 The Process of Mapping

This chapter shows the process of filtering and altering the information from the IT-Grundschutz Catalogues and mapping it to SecOnt with the use of the Protégé Tool.

Therefore I want to present a step-by-step tutorial by showing the mapping of the threat-scenario “Break in” including all the connected changes and additions to complete the scenario. For the demonstration I will start with the threat as the initial situation. From my point of view this is the most natural and logical approach. In reality, due to the complex network of connections the process of mapping was not always as linear as presented in the example. The screenshots in this chapter show the corresponding parts of the GUI of Protégé.

5.3.4.1 Selecting the Source

The need for including the threat “Break in” into SecOnt originates from the IT-Grundschutz Catalogues’s threat T 5.3 “Unauthorized entry into a building”. This is a good example of a case, where we thought the IT-Grundschutz Catalogues was too imprecise in its description of a module and therefore we have had to create a more specific version.

5.3.4.2 Altering the Source

From our point of view the definition of the threat “Break in” is as follows:

A Break in is an active overcoming of physical barriers either through manipulation or destruction with the intention of getting access to a building or an area.

Furthermore the threat “Break in” can lead to the threat “unauthorized entry into a building”.

Therefore we have had to create the threat sec:BreakIn and connect it to the threat “sec:UnauthorizedPhysicalAccess” which for the example we’ll assume we have already created before.

5.3.4.3 Creating the Threat

First of all we have to create a subclass of sec:Threat and call it sec:BreakIn, which is shown in Figure 24 and Figure 25.

Figure 24: Creating a subclass

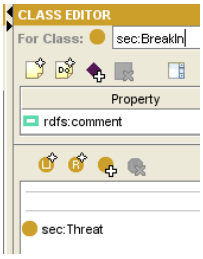


Figure 25: Empty class "sec:BreakIn"

As already mentioned, every subclass initially contains an abstract instance, so the next step would be to create an abstract instance of the threat sec:BreakIn and name it “abs:BreakIn”. We can do this in the “Individuals” tab of Protégé as shown in Figure 26.

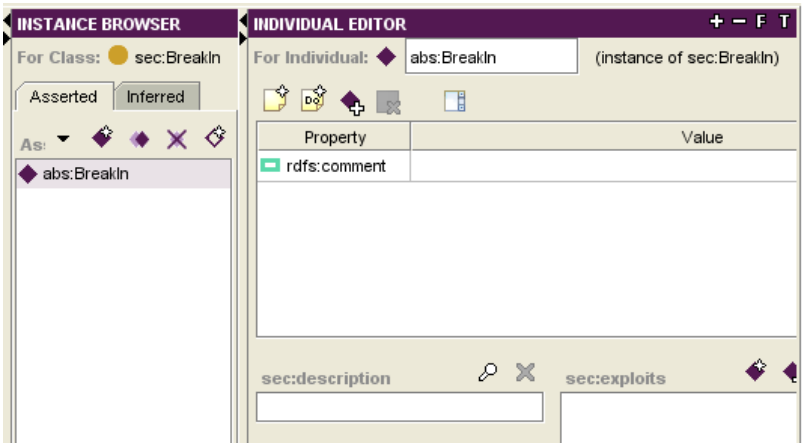


Figure 26: Instance of abs:BreakIn

Here we only insert the description (and the source of the description as an rdfs:comment). The other properties will be filled in later automatically by using an OWL reasoner, based on the class restrictions we are about to define.

5.3.4.4 Analyzing the threat and creating the class restrictions

The first step in analyzing a threat is to create connections between the threat and the related vulnerabilities. As described in chapter 5.3.2.2 we did this with the help of the cross reference tables. In this case the threat “Break In” is not contained in the IT-Grundschutz Catalogues, but as it is based on the threat T 5.3 “Unauthorized entry into a building”, we will take a look if we find useful information in the related cross reference table. The module “B 2.1 Buildings” contains all the threat connections for our threat, so we have to use the cross reference table B02001.

The following table shows the filtered and translated information from the cross reference table B02001 related to the threat T 5.3:

Safeguard No.	Safeguard Title
S 1.10	Use of safety doors and windows
S 1.12	Avoidance of references to the location of building parts requiring protection
S 1.13	Layout of building parts requiring protection
S 1.15	Closed windows and doors
S 1.19	Protection against break-in
S 2.14	Key management
S 2.334	Selection of an appropriate building

Here is a quick overview of the rating of the information:

Safeguard No.	Rating / Comment
S 1.10	Applicable, but due to granularity reasons we want to separate security doors and security windows.
S 1.12	Does not mitigate the threat “Break In”
S 1.13	Does not mitigate the threat “Break In”
S 1.15	If a window/door is open, the intruder does not need to break in. Applicable to “Unauthorized entry into a building”, but not to “Break In”.
S 1.19	Needs further analysis of the description. Definitely too generic.
S 2.14	Applicable to “Unauthorized entry into a building”, but not to “Break In”.
S 2.334	Needs further analysis of the description. Definitely too generic.

After further analysis of the information contained in the descriptions, and also after taking into account the vulnerabilities already existing in SecOnt, we came to the conclusion that we wanted to connect the threat “Break In” to the following vulnerabilities:

BreakIn exploits:

- NoSecureWindows
- NoSecureDoors
- NoEntranceControl
- NoRaisedLocation
- NoIntrusionAlarmSystem

After defining the related vulnerabilities, we have to find the interrelations to other threats. In this case we already know that a “Break In” usually will lead to an “Unauthorized entry into a building”. We also know that per definition a “Break In” can trigger the damage of some asset. So the following two other threats can be the consequences of a “Break In”:

BreakIn givesRiseTo:

- UnauthorizedPhysicalAccess
- AssetDamage

We can also define what entity is threatened by a “Break In”. An entity can be a subclass of the classes Software, Data, Role and/or Asset. In our case a “Break In” directly threatens the following entities:

BreakIn threatens:

- Building
- Doors
- Windows

Two more restrictions have to be defined on class hierarchy level. Those are the security attribute and the threat type. For the threat “Break In” we have chosen the following values:

BreakIn affects Integrity (security attribute)

BreakIn hasThreatType HumanThreat (type of threat)

As already mentioned those restrictions have to be applied on the class level, so that an OWL-reasoner later can fill in the appropriate values automatically. To create these definitions with Protégé we had to use the class editor as shown in Figure 27.

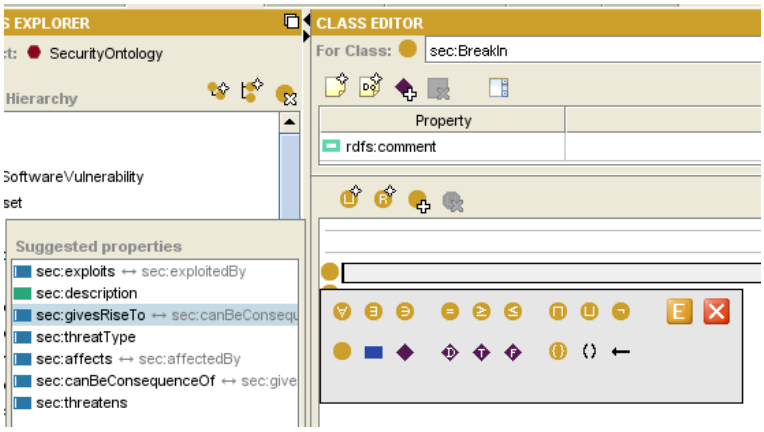


Figure 27: Defining class restrictions in Protégé

Figure 28 shows the final class sec:BreakIn after adding all the previously discussed class restrictions.

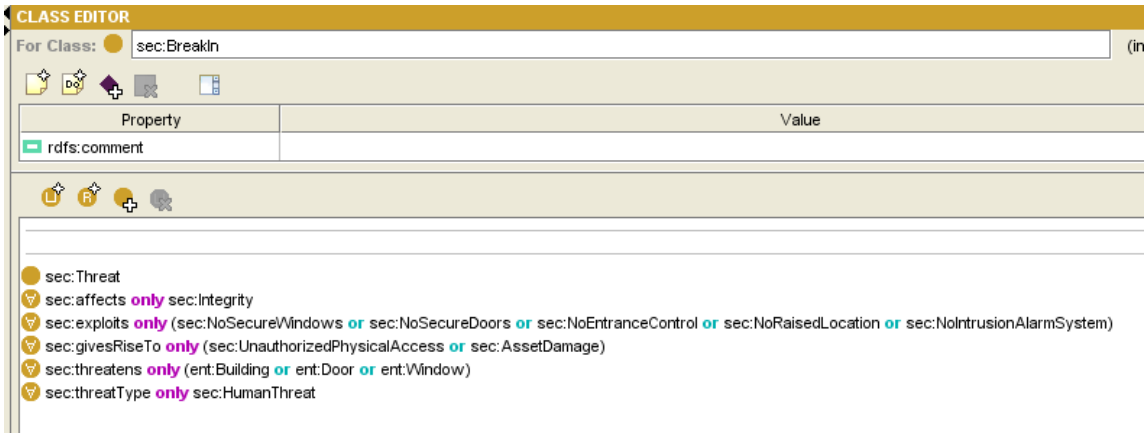


Figure 28: Final class sec:BreakIn

Of course we need all those linked concepts also modeled in the ontology. For this example let's assume only the concept of the vulnerability "sec:NoIntrusionAlarmSystem" is missing at this point. All the other classes have already been modeled.

Nevertheless we need to edit every single connected vulnerability and threat and add the inverse relation. Unfortunately Protégé cannot do this automatically on class level, so we have had to do this manually. The inverse relations for threats and vulnerabilities are:

- [sec:Threat] sec:givesRiseTo [sec:Threat] --
  [sec:Threat] sec:canBeConsequenceOf [sec:Threat]
- [sec:Threat] sec:exploits [sec:Vulnerability] --
  [sec:Vulnerability] sec:exploitedBy [sec:Threat]

An example of one of the inverse relations mentioned – the inverse relation between the vulnerability "sec:NoSecureDoors" and the threat "sec:BreakIn" is shown in Figure 29.

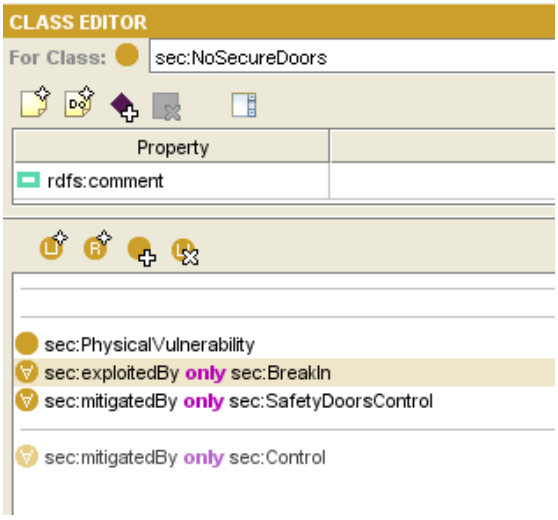


Figure 29: Inverse Relation sec:BreakIn - sec:NoSecureDoors

5.3.4.5 Creating missing vulnerabilities

The next step in completing the mapping of the threat "BreakIn" would be to make sure that all connected concepts are also modeled in SecOnt. For this example

we will assume that we have already created all connected concepts but one, which is the vulnerability “NoIntrusionAlarmSystem”.

We classify vulnerabilities into one of three categories:

- Administrative vulnerability
- Physical vulnerability
- Technical vulnerability

In this case we can clearly identify that the vulnerability of not having an intrusion alarm system installed is a physical vulnerability.

Consequently, we have to create a class named sec:NoIntrusionAlarmSystem as a subclass of sec:Vulnerability/sec:PhysicalVulnerability. Here we also have to create an abstract instance with the prefix abs: and as with the threats we also have to define the description directly on the instance. The other properties are also filled in automatically with an OWL-reasoner based on the class restrictions. The final class including the class restrictions is shown in Figure 30.

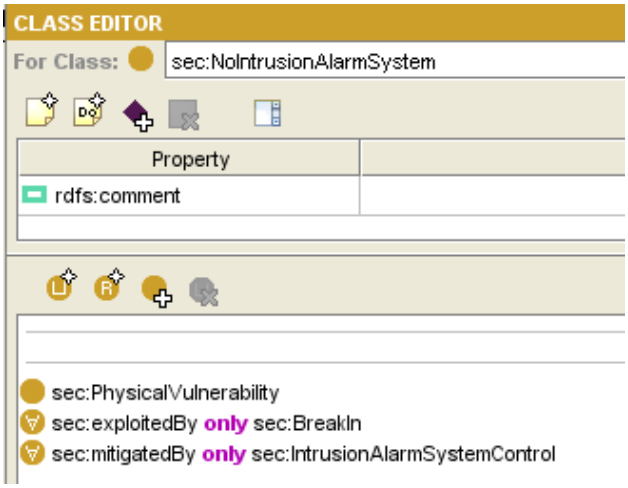


Figure 30: Final class sec:NoIntrusionAlarmSystem

Apart from the inverse connection to sec:BreakIn, which was already mentioned previously, we have defined a new property:

sec:mitigatedBy only sec:IntrusionAlarmSystemControl

As described in chapter 5.3.1.1 we created the vulnerabilities mostly by implication based on the related control. Naturally, this approach also works in the

opposite direction. Therefore the appropriate control for the vulnerability "NoIntrusionAlarmSystem" is the "IntrusionAlarmSystemControl".

5.3.4.6 Creating the missing controls

After having created all the vulnerabilities which are connected to the threat we need to make sure that those vulnerabilities have related controls that are able to mitigate them. In our case, since we are assuming that the other vulnerabilities have already been completely modeled we therefore only have to create the control "IntrusionAlarmSystemControl".

As shown in chapter 5.2.2, Figure 16 for the class hierarchy of the controls we have used a similar structure as it is used in the ISO/IEC 27002 standard. Therefore we have to classify the appropriate category for the current control. In this case the appropriate category would be "sec:PhysicalAndEnvironmentalSecurityControl".

The process of creating an empty class for the controls and the related abstract instance is similar to threat and vulnerability creation as described above.

In this case we have had to create the class "sec:IntrusionAlarmSystemControl" and the corresponding abstract instance "abs:IntrusionAlarmSystemControl". The description for this abstract class was taken from the IT-Grundschutz Catalogues "S 1.18 Alarm Systems" which contentwise is closely related to the safeguard S 1.19 which was proposed in the cross reference table. This is a good example of how we could not blindly rely on the information from the cross reference tables as it is imprecise, inconsistent and incomplete.

Similarly to the description of the safeguard we also have modeled the attribute that holds the relation to the corresponding ISO 27001 control directly on the abstract instance level. Therefore we have consulted the allocation table discussed in chapter 5.3.2.1, which says that the safeguard S 1.18 is corresponding to the chapters 9.1.3 and 9.1.4 in the ISO 27001 standard. Figure 31 shows the abstract instance and the corresponding chapters of the ISO 27001 standard in the Individuals-View of Protégé.

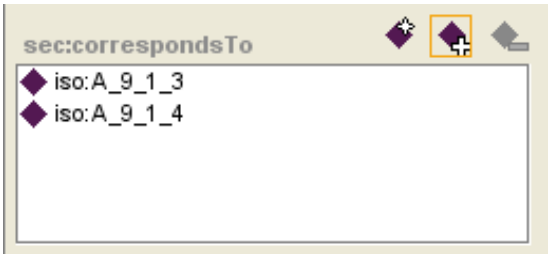


Figure 31: abs:IntrusionAlarmSystemControl and corresponding ISO 27001 chapters

The next step would be to create the remaining properties on the class level.

On the one hand we need to set the inverse property to "*sec:mitigatedBy only sec:IntrusionAlarmSystemControl"* which we have defined on the related vulnerability in the previous chapter. What we want to express is the following statement:

"the control sec:IntrusionAlarmSystem Control mitigates the vulnerability sec:NoIntrusionAlarmSystem".

With protégé we can do this by defining the following class restriction:

(sec:IntrusionAlarmSystemControl) sec:mitigates only sec:NoIntrusionAlarmSystem

Now that we have modeled what vulnerability is mitigated by our control, we have to define the objects which the control consists of.

Controls that consist of only operational tasks, such as "sec:ClosedDoorsControl" which specifies that doors have to be closed, do not have to be implemented by a special asset. The tasks that need to be performed to implement the control are described in the description of the policy. However, we provide the possibility to use the sec:implementedBy attribute to point to a document, which can also be modeled within SecOnt. The document object holds, amongst others, the location of a document which specifies the control, or which contains a certain contract, agreement, etc. Anyhow, the attribute "sec:implementedBy" is non-mandatory.

In our case an intrusion alarm system clearly consists of hardware and therefore we can use the sec:implementedBy attribute to define the assets which are connected to it.

Generally speaking an alarm system consists of a basis alarm system and connected detectors. In our case we want to implement an intrusion alarm system so we need some sort of intrusion detectors.

On the class level of sec:IntrusionAlarmSystemControl we now want to express the following statements:

- An intrusion alarm system consists of an alarm system and of some sort of intrusion detectors.
- There must be at least one alarm system.
- There must be at least one intrusion detector.

In Protégé these statements are equivalent to the following class restrictions:

(sec:IntrusionAlarmSystemControl) …

- sec:implementedBy only (ent:AlarmSystem or ent:IntrusionDetectors)
- sec:implementedBy some ent:AlarmSystem
- sec:implementedBy some ent:IntrusionDetectors

Figure 32 shows the final class sec:IntrusionAlarmSystemControl including all class restrictions.

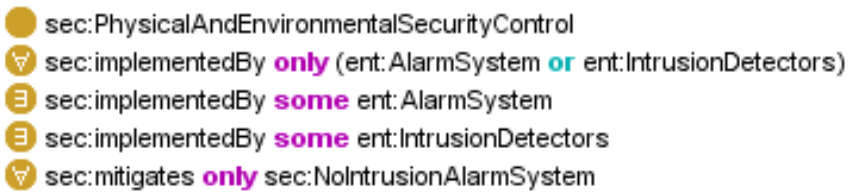


Figure 32: Final class sec:IntrusionAlarmSystemControl

Now that we have finished modeling the control, we have to focus on the integration of the previously mentioned assets.

5.3.4.7 Creating the related assets

As already introduced in chapter 5.2.1 we use the ent: namespace to provide a possibility to model assets. Those assets can either be concrete assets of an

organization, or abstract assets that propose a way of implementing a certain control. In this chapter we focus on the latter ones.

As discussed in the previous chapter we need to create certain assets related to an intrusion alarm system. These are the following:

- (Core) Alarm System
- Intrusion Detectors

To provide a selection of the most commonly used systems, we have chosen the following intrusion detectors to be integrated in SecOnt:

- Glass break detector
- Motion detector
- Normally closed circuits detector

All the detectors listed above are specializations of “intrusion detectors”. So they can be modeled as sub-classes of the class “sec:IntrusionDetectors”.

Therefore we have to create subclasses of the concept “ent:Asset”. For modeling reasons “ent:Asset” is split into “ent:ImmovableAsset” - e.g. walls, rooms, etc – and “ent:MovableAsset” – e.g. computer, fire extinguisher, etc. In our case all parts are movable, so we need to find the appropriate subclass to create our concepts. Once the class has been created we only need to add a corresponding abstract instance and define a brief description of the concept. Further functionality of the classes within the ent: namespace is not relevant for my work and therefore out of scope. Figure 33 shows the class ent:IntrusionDetectors and its subclasses.

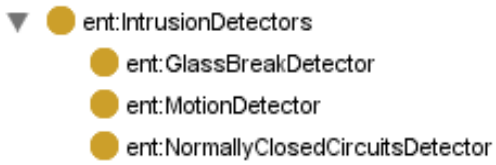


Figure 33: ent:IntrusionDetectors and subclasses

Once we have successfully created all the classes and instances of the related assets we have finally completed the last step of the mapping of the threat-scenario “Break In”.

To summarize, in this chapter I have shown how the initial creation of one threat concept leads to a number of creations of associated vulnerability, control and assets concepts. Each creation of such a concept brings up the question of how and where it has to be integrated within SecOnt. I have also demonstrated some examples of the different approaches we have used to provide answers to these questions.

6 Conclusions

The value of information is steadily increasing, that is why organizations have to protect data as it does with all valuable assets. Therefore information technology security has become inevitable.

Stefan Fenz' and Andreas Ekelhart's [9, 10, 11, 21] contribution in the field of research of IT-security - amongst others - is SecOnt, a security ontological framework with the following capabilities:

- SecOnt can help to clarify the meaning and interdependence of IT-security relevant terms [26].
- SecOnt can improve quantitative risk analysis. Building on established best practices knowledge and a mapping of a company's infrastructure SecOnt is able to compute the outcome of disaster scenarios.
- Basing on disaster simulation SecOnt can help decision makers to choose the most effective countermeasures to mitigate individual vulnerabilities.
- Due to the addition of an Ontological Mapping of the ISO/IEC Standard to SecOnt [21] the framework is also able to support organizations in the process of the ISO/IEC 27001 certification.

My thesis is building on this previous work by Fenz and Ekelhart on SecOnt. With my work – the creation of the security knowledge base – it has become possible to use the features of the SecOnt framework not only with demo data but with real world, well established best practice knowledge.

The initial assignment was to create the core security knowledge base and fill it with best practice knowledge related to the topics threats, vulnerabilities, controls and the relations between them.

At this point I want to refer to the first research question from chapter 2.1:

- *What should be the knowledge source for the mapping to the ontology? Which international standard, respectively best practice knowledge collection covers our requirements best?*

To answer this question I had to make the following considerations:

To ensure that the knowledge is established and well accepted I had to create a mapping from a popular and widely used source, i.e. a best practice collection or an IT-Security related standard. Therefore I had to start with an analysis of qualified sources, which is described in chapter 4.1. The outcome of this analysis has shown that the IT-Grundschutz Manual [8] fits our requirements best and therefore will be the basis for the mapping to SecOnt.

The other two research questions

- *How does the scope and the content of the knowledge source need to be altered to fit the requirements of SecOnt? How can threat interrelations be modeled?*
- *Which incompatibilities between the knowledge source and the structure of SecOnt are there and how can they be corrected? How can inconsistencies in the knowledge source and in SecOnt be corrected? Which methods are applicable?*

… can be answered by the following paragraphs:

Before the mapping could be started some incompatibility and inconsistency problems had to be solved. Dealing with inconsistent knowledge bases is a well known topic in logics and AI [32, 33, 34]. Anyhow, it is only possible to repair inconsistent ontologies with the use of algorithms or special logics when the problems originate from structural or logical inconsistency. In our case, where the inconsistency problem is related to the content, a domain specialist with deep knowledge has to manually adjust the content. Chapter 5.3.1 shows the problems we have had to overcome and chapter 5.3.3 describes the methods we have used to solve them.

Chapter 5.3.4 finally illustrates how the process of the mapping was carried out. Therefore I have created a tutorial which exemplarily shows the steps which were necessary to map one threat-vulnerability-control scenario.

At the moment the ontology contains approximately 80 threats, 90 vulnerabilities, 90 controls and numerous relations between those concepts. Due to limited space it is not possible to insert a visualization of the whole ontology. To get

an idea of the complexity I would like to refer to http://securityontology.securityresearch.at/img/Threat_Interrelations.gif which shows a diagram of the threat interrelations subontology only.

Besides the impact of my work to the SecOnt project, my thesis can help knowledge engineers with the mapping of knowledge from inconsistent sources. They can learn which methods I have used for inconsistency correction, content filtering and knowledge mapping.

6.1 Outlook

Further research activities could address the integration of other best practice collections and standards. Thus the knowledge base could be extended in depth and breadth.

As already mentioned in chapter 3.3, from my point of view it would be a good opportunity to create synergies with other already existing security ontologies. Due to the nature of OWL-Ontologies they can be easily merged and extended.

Now that a solid basis has been created, it would also be possible to create a Wiki-like collaborative tool that allows all interested members of the IT-security community to enhance and improve our security knowledge base.

Apart from the improvement of the knowledge base itself a number of possibilities for applications that can build upon the ontology arise. Secure Business Austria are continuing their research on combining SecOnt with Risk Management and Risk Analysis as well as improving the support in the ISO/IEC 27001 certification process. However, other fields of application are easily conceivable. The ontology could for example be used as a knowledge base for educational purpose for IT security personnel or students. With further extension of SecOnt and the development of appropriate interfaces SecOnt could be integrated in monitoring systems such as Nagios[10] or MOM[11] (Microsoft Operations Manager). Depending on the incident, which would be tracked by the monitoring system, SecOnt could automatically decide what countermeasure would be appropriate and could initiate the necessary actions.

[10] Nagios: http://www.nagios.org/, last access: July 8 2008
[11] Microsoft Operations Manager 2005: http://www.microsoft.com/germany/mom/default.mspx, last access: July 8 2008

To summarize, this document contains the methods and approaches I have used to create an ontological mapping of the IT-Grundschutz-Catalogues to SecOnt, an IT-Security ontology. The practical results of this mapping are contained in the latest version of SecOnt, which can be downloaded from the website of Secure Business Austria under the following link:

http://securityontology.securityresearch.at/downloads/.

In this thesis I have analyzed, adjusted and mapped the concepts “threat, vulnerability and control” from the BSI’s IT-Grundschutz-Catalogues to SecOnt, an ontological IT-security framework. Furthermore I have derived relations between those concepts and I have created threat interrelations which make the modeling of chain reactions possible. To my knowledge at this time this feature is unique and distinguishes our knowledge base from third party research.

APPENDIX A: References

[1] **Millward Brown.** [Online] April 23, 2007. [Cited: November 22, 2007.] http://www.millwardbrown.com/sites/Optimor/Media/Pdfs/en/BrandZ/BrandZ-2007-Top100PressRelease.pdf.

[2] **Stone, Brad.** Microsoft to Pay $240 Million for Stake in Facebook. *The New York Times.* [Online] October 25, 2007. [Cited: November 22, 2007.] http://www.nytimes.com/2007/10/25/technology/24cnd-facebook.html?_r=1&oref=slogin&pagewanted=print.

[3] **Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl E. Landwehr.** Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable Secure Computing. Vol 1, No. 1,.* 2004.

[4] **Basel Committee on Banking Supervision.** Basel II. *International Convergence of Capital Measurement and Capital Standards.* June 2004.

[5] **The Senate and House of Representatives of the United States of America.** One Hundred Seventh Congress of the United States of America. *Sarbanes Oxley Act of 2002.* January 23, 2002.

[6] **OECD.** www.oecd.org. [Online] 2002. [Cited: November 23, 2007.] http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[7] **International Organization for Standardization.** *ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements.* 2005.

[8] **Bundesamt für Sicherheit in der Informationstechnik.** www.bsi.de. *IT-Grundschutz-Kataloge 2006.* [Online] 2006. [Cited: November 30, 2007.] http://www.bsi.de/gshb/deutsch/download/it-grundschutz-kataloge_2006_de.pdf.

[9] **Stefan Fenz, Edgar Weippl.** Ontology based IT-security planning. *12th Pacific Rim International Symposium on Dependable Computing.* Dec. 2006, pp. 389-390.

[10] **Andreas Ekelhart, Stefan Fenz, Markus D. Klemen, and Edgar R. Weippl.** Security Ontology: Simulating Threats to Corporate Assets. [ed.] A. Bagchi and V. Alturi. *Information Systems Security.* 2006, Vol. 4332 of Lecture Notes in Computer Science, pp. 249-259.

[11] **Andreas Ekelhart, Stefan Fenz, Markus Klemen and Edgar Weippl.** Security Ontologies: Improving Quantitative Risk Analysis. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences.* 2007, pp. 156-162.

[12] **PricewaterhouseCoopers.** information security breaches survey 2006. technical report. [Online] 2006. [Cited: november 27, 2007.] http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf.

[13] **Gordon et al., Lawrence.** *computer crime and security survey.* s.l. : Computer Security Institute Publications, 2006.

[14] **PCI Security Standards Council.** Payment Card Industry (PCI) Data Security Standard, Version 1.1. [Online] September 2006. [Cited: November 30, 2007.] https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

[15] **The Information Security Forum.** The Standard of Good Practice. [Online] 2007. [Cited: March 2, 2008.] http://www.isfstandard.com/.

[16] **Raskin et al.** Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool. *Proceedings of the New Security Paradigms Workshop, ACM.* 2001.

[17] **Tsoumas et al.** Towards an Ontology-based Security Management. *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA '06).* 2006.

[18] **A. Herzog, N. Shahmehri, C. Duma.** An Ontology of Information Security. *International Journal of Information Security and Privacy 1.* 2007.

[19] **Frederick Gallegos, Sandra Senft, Daniel P. Manson, Carol Gonzales.** *(COBIT) Information Technology Control and Audit.* New York : Auerbach Publications, 2004. ISBN: 0-8493-2032-1.

[20] **Standardization, International Organization for.** ISO/IEC 27006:2007. *www.iso.org.* [Online] [Cited: March 10, 2008.] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42505.

[21] **Stefan Fenz, Gernot Goluch, Andreas Ekelhart, Edgar Weippl.** Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. *Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing.* 2007.

[22] **Deborah L. McGuinness, Frank van Harmelen.** OWL Web Ontology Language. *W3C Recommendation.* [Online] February 10, 2004. [Cited: June 7, 2008.] http://www.w3.org/TR/owl-features/.

[23] **Dan Connolly, et al.** DAML+OIL (March 2001) Reference Description. *W3C Note.* [Online] December 18, 2001. [Cited: June 7, 2008.] http://www.w3.org/TR/daml+oil-reference.

[24] **Sean Bechhofer, et al.** OWL Web Ontology Language Reference. *W3C Recommendation.* [Online] February 10, 2004. [Cited: June 7, 2008.] http://www.w3.org/TR/owl-ref/.

[25] **Michael K. Smith, et al.** OWL Web Ontology Language Guide. *W3C Recommendation.* [Online] February 10, 2004. [Cited: June 7, 2008.] http://www.w3.org/TR/owl-guide/.

[26] **M. Donner.** Toward a security ontology. *IEEE Security and Privacy.* May/June 2003, Vol. 1, 3, pp. 6-7.

[27] **National Institute of Standards and Technology.** *An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.* 2006.

[28] **Bundesamt für Sicherheit in der Informationstechnik.** www.bsi.de. [Online] 2007. [Cited: March 16, 2008.] http://www.bsi.bund.de/gshb/deutsch/hilfmi/isovergleich/Vergleich_ISO27001_GS.pdf.

[29] —. www.bsi.de. [Online] 2007. [Cited: March 16, 2008.] http://www.bsi.de/gshb/deutsch/download/kreuzreferenz_tabellen.zip.

[30] **Matthew Horridge, et al.** *A Practical Guide To Building OWL Ontologies Using The Protege-OWL Plugin and CO-ODE Tools.* s.l. : The University Of Manchester, 2004.

[31] *Editing description logics ontologies with the Prot eg e OWL plugin.* **Holger Knublauch, Mark A. Musen, and Alan L. Rector.** 2004.

[32] **Peter Haase, Johanna Völker.** Ontology Learning and Reasoning - Dealing with Uncertainty and Inconsistency. *International Semantic Web Conference.* November 7, 2005, pp. 45-55.

[33] **F. Bacchus.** *Representing and Reasoning with Probabilistic Knowledge.* s.l. : MIT Press, 1990.

[34] **Zhisheng Huang, Frank van Harmelen, and Annette ten Teije.** Reasoning with Inconsistent Ontologies. *In Proceedings of IJCAI'05.* August 2005.

[35] **Facebook Inc.** www.facebook.com. [Online] 2007. [Cited: november 22, 2007.] http://www.facebook.com/press/info.php?factsheet.

[36] **Nicodemos Damianou, Naranker Dulay, Emil Lupu, Morris Sloman.** The Ponder Policy Specification Language. *Lecture Notes In Computer Science; Vol. 1995;*

Proceedings of the International Workshop on Policies for Distributed Systems and Networks. 2001.

APPENDIX B: Index of Figures