Ontological Mapping of Information Security Best-Practice Guidelines

Stefan Fenz, Thomas Pruckner, and Arman Manutscheri

Vienna University of Technology and Secure Business Austria, Vienna, Austria
fenz@ifs.tuwien.ac.at

Abstract. Due to a rapid growth in the use of electronic data processing and networking, an information security management system with a holistic and widespread view becomes more and more important for any kind of organization. The fundamental challenge for such systems is the representation and management of information security knowledge. While information security ontologies already exist, no methods have been proposed to map existing best-practice guidelines or information security standards to an existing ontology. Therefore, this paper presents a method for mapping the information security knowledge of the French EBIOS standard and the German IT Grundschutz Manual to a OWL-DL security ontology. Applying the introduced method allows to reuse existing information security knowledge bases and to map them to open and standardized data structures which can be easily reused by organizations and developers to support their existing information security management systems.

Keywords: Ontological mapping, information security best-practice guidelines, security ontology, EBIOS, IT Grundschutz Manual.

1 Introduction

In recent years a rapid growth in the use of electronic data processing and networking took place. By now almost all kind of organizations are depending on IT systems in large parts of their business activity. With the extensive use of information technologies and the increasing networking in all business areas the requirements on IT security widened dramatically [11,1]. The large quantity of potential threats and the growing complexity of IT systems led to the conclusion that the holistic perspective of IT security and the implementation of IT security management systems is absolutely essential [10]. The fundamental challenge for such systems is the representation and management of information security knowledge. The characteristics of an ontology allow to address this challenge. While ontologies in the information security domain exist (cf. [6,7,12]) no methodology has been proposed to map information security knowledge from existing information security standards or best-practice guidelines to these knowledge models. In this paper we propose a methodology for mapping information security best-practice guidelines to existing information security ontologies. Applying the introduced method allows to reuse existing information

W. Abramowicz (Ed.): BIS 2009, LNBIP 21, pp. 49–60, 2009.

security knowledge bases and to map them to open and standardized data structures which can be easily reused by organizations and developers to support their existing information security management systems. The proposed methodology is demonstrated by mapping the French EBIOS [5] and the German IT Grundschutz Manual [4] to the security ontology by [6].

2 Ontological Mapping of Information Security Best-Practice Guidelines

An essential requirement for mapping existing information security best-practice guidelines to an ontological structure is that the selected best-practice guideline is available in a machine-readable form. A survey among existing information security standards and best-practice guidelines has shown that national guidelines such as the German IT Grundschutz Manual [4] and the French EBIOS [5] are available in a machine-readable form. While EBIOS provides its knowledge base in form of structured XML-documents, the IT Grundschutz Manual provides a proprietary but still readable database structure. We propose the following methodology to map machine-readable information security best-practice guidelines to existing ontological structures:

- **Ontology analysis:** Before starting the actual mapping process, the ontological structure of the selected security ontology has to be analyzed. Especially the analysis of existing concepts and corresponding relations is crucial for relating them to the knowledge base structure identified in the next phase.
- **Knowledge base analysis:** This phase identifies entities and relations which are semantically similar to the ontological concepts and relations identified in the previous phase.
- **Mapping concepts and relations:** Based on the results of the previous two phases, this phase maps entities and relations of the machine-readable best-practice guideline representation to the ontological model.
- **Mapping the knowledge:** The mapping schema of the previous phase is used to map the actual knowledge from the best-practice guideline to the ontological information security model.
- **Evaluation:** Since the mapping of the knowledge may be conducted semi - automatically, the evaluation phase requires the manual evaluation of the mapped knowledge by human beings.

In the following sections we describe the application of the proposed mapping methodology and the difficulties which arise in the mapping process. We used the machine-readable knowledge bases of EBIOS and the IT Grundschutz Manual to map them to the security ontology by [6].

3 Ontology Analysis – Security Ontology

Figure 1 shows the high-level concepts (boxes) and corresponding relations (arrows represent at their start the domain and at their end the range of the corresponding relation) of the used security ontology (cf. [6] for further details on the used security ontology). A threat gives rise to follow-up threats, represents a potential danger to the organization's assets and affects specific security attributes (e.g. confidentiality, integrity, and/or availability) as soon as it exploits a vulnerability in the form of a physical, technical, or administrative weakness. Additionally each threat is described by potential threat origins (human or natural origin) and threat sources (accidental or deliberate source). For each vulnerability a severity value and the asset on which the vulnerability could be exploited is assigned. Controls have to be implemented to mitigate an identified vulnerability and to protect the respective assets by preventive, deterrent, recovery, or detective measures (control type). Each control is implemented as asset concept, or as combinations thereof. The controls are modeled on a highly granular level and are thus reusable for different standards. When implementing the controls, a compliance with various information security standards is implicit. The coded ontology follows the OWL-DL (W3C Web Ontology Language) [14] standard and ensures that the knowledge is represented in a standardized and formal form.

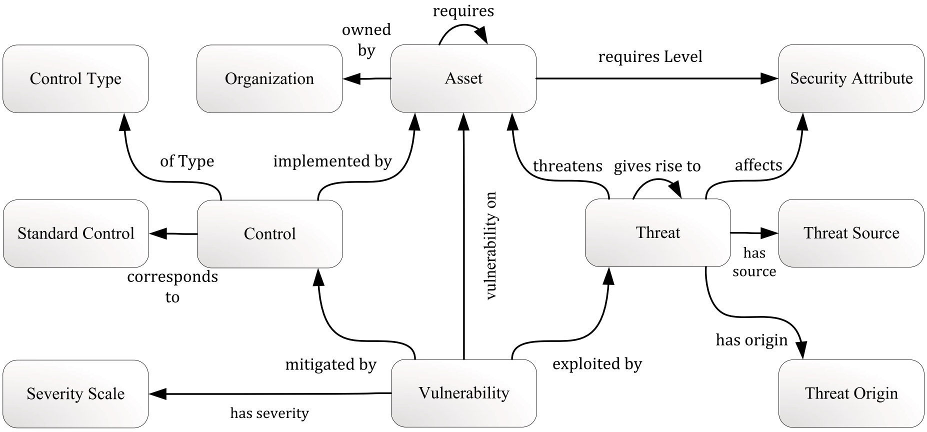

Fig. 1. Security ontology top-level concepts and relationships

4 Mapping EBIOS to the Security Ontology

According to the proposed methodology, this section shows how we mapped the knowledge represented by EBIOS to the security ontology.

4.1 Knowledge Base Analysis

EBIOS [5] was created by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information - a department of the French Ministry of Defense) and represents a method for the assessment and treatment of IT security risks. For the definition of a certain level of security, EBIOS specifies generic security objectives that are used for the protection of entity types (assets) and the mitigation of vulnerabilities. The implementation of these objectives is carried out by predefined functional security requirements derived from standards like ISO 17799. The data-sets offered by the EBIOS method include descriptions of entity types, threats, vulnerabilities, and security objectives which can be achieved by the implementation of corresponding measures. See the EBIOS documentation [5] for further details.

4.2 Mapping Concepts and Relations

Figure 2 gives an idea of the relations between EBIOS and the security ontology but it is insufficient in order to map the provided information exactly. Therefore, Table 1 lists all mappable XML-elements and attributes defined by EBIOS and quotes their corresponding OWL-concepts and relations in the security ontology. The creation of such a table requires the semantic analysis of concepts and relations located in the source (best-practice guideline) and the target (security ontology). Although dictionary-based approaches can be used to map common keywords, this phase has to be conducted mainly by manual means. Especially the analysis of the concepts' and relations' natural language descriptions is important for an appropriate mapping between source and target.

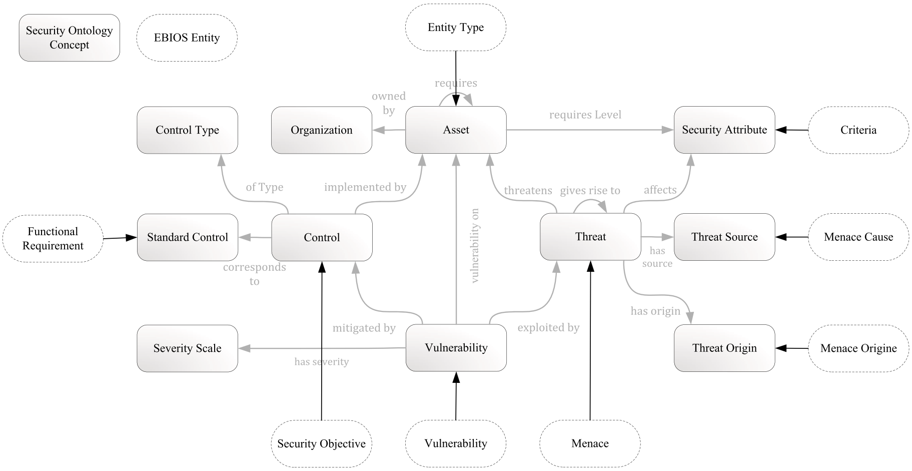

Fig. 2. Relationships among EBIOS entities and security ontology concepts

4.3 Mapping the Knowledge

In this section we show, by using the example of the fire threat, how we have mapped information security knowledge from EBIOS to the security ontology. As listed in Table 1, a menace in EBIOS is equivalent to a threat in the security ontology. The following code snippet shows the EBIOS XML representation of the fire threat[1].

```
<Menace ID=”Menace.1050382052535” label=”01−FIRE” selected=”” description=”Type:
    Natural/Human/Environmental  Accidental cause: Concentration of flammable or
    explosive...” justification=”” descriptionMenaceElement=”” potentiel=””>
  <MenaceThemeList ID=”MenaceThemeList.1050973114465” >
    <Theme id=”Theme.1013467459833” comments=””/>
  </MenaceThemeList>
```

[1] To enhance the readability we shortened the description text.

Table 1. EBIOS entities and attributes and their corresponding security ontology concepts and relations

EBIOS XML-elements and attributes	**Security ontology concepts and relations**
<EntityType>	ent:Asset
type	subclasses of ent:Asset
description	ent:description of abstract instances of subclasses of ent:Asset
<Vulnerability>	sec:Vulnerability
label	subclasses of sec:Vulnerability
menace	sec:exploitedBy of sec:Vulnerability
<EntityTypeList>	sec:threatens of sec:Threat
<Menace>	sec:Threat
label	subclasses of sec:Threat
description	sec:description of abstract instances of subclasses of sec:Threat
<SeverityScale>	sec:affects of sec:Threat
<Criteria>	sec:SecurityAttribute
label	instances of sec:SecurityAttribute
description	sec:description of abstract instances of subclasses of sec:SecurityAttribute
<MenaceCauseList>	sec:hasSource of sec:Threat
<MenaceCause>	sec:ThreatSource
label	subclasses of sec:ThreatSource
description	sec:description of abstract instances of subclasses of sec:ThreatSource
<MenaceOrigineList>	sec:hasOrigin of sec:Threat
<MenaceOrigine>	sec:ThreatOrigin
label	subclasses of sec:ThreatOrigin
description	sec:description of abstract instances of subclasses of sec:ThreatOrigin
<SecurityObjective>	sec:Control
label	subclasses of sec:Control
content	sec:description of abstract instances of subclasses of sec:Control
<SecurityObjectiveCovers>	sec:mitigatedBy of sec:Vulnerability
<FunctionnalRequirement>	iso:Control
abbreviation	iso:controlTitle of abstract instances of iso:Control
description	iso:controlDescription of abstract instances of iso:Control
<Objective>	sec:correspondsTo of iso:Control

```
  <SeverityScale ID=”SeverityScale.1050973114465”>
    <MenaceSeverity ID=”MenaceSeverity.1109436174044” criteria=”Criteria
        .1013307741641” severity=”” violation=”true”/>
    <MenaceSeverity ID=”MenaceSeverity.1109108597320” criteria=”Criteria
        .1011680648037” severity=”” violation=”true”/>
  </SeverityScale>
  <MenaceCauseList ID=”MenaceCauseList.1050973114465”/>
    <MenaceCause id=”MenaceCause.1012606157332” comments=””/>
    <MenaceCause id=”MenaceCause.1011656568285” comments=””/>
  </MenaceCauseList>
  <MenaceOrigineList ID=”MenaceOrigineList.1050973114465”/>
    <MenaceOrigine id=”MenaceOrigine.1051413282991” comments=””/>
    <MenaceOrigine id=”MenaceOrigine.1052902060343” comments=””/>
    <MenaceOrigine id=”MenaceOrigine.1050514650356” comments=””/>
  </MenaceOrigineList>
</Menace>
```

The menaces' attribute *Label* and *Description* correspond to the threat sub-concepts and their descriptions. The element *SeverityScale* lists all affected *Criteria* which comply with *sec:SecurityAttribute* in the security ontology. The elements *MenaceCauseList* and *MenaceOrigineList* provide information about the sources and the origin of a threat. In the given example the attribute *Label* of the fire menace corresponds to the sub-concept *sec:Fire* in the security ontology. The element *SeverityScale* corresponds to the relation *sec:affects*. It lists the affected *Criteria* which correspond to *sec:SecurityAttribute* in the security ontology. The affected criteria in this example are 'Criteria.1013307741641' which is defined as availability and 'Criteria.1011680648037' which is defined as integrity. The element *MenaceCauseList* lists possible causes of a fire and is equivalent to the relation *sec:hasSource*. It is listing all possible *MenaceCause* elements which comply to the sub-concepts of *sec:ThreatSource* in the security ontology. In this example 'MenaceCause.1012606157332' stands for an accidental threat source and 'MenaceCause.1011656568285' stands for a deliberate threat source of a fire. The element *MenaceOrigineList* is equivalent to the relation *sec:hasOrigin*. It is listing all possible *MenaceOrigine* elements which comply with the subclasses of *sec:ThreatOrigin* in the ontology. The menace origins listed are 'MenaceOrigine.1051413282991', 'MenaceOrigine.1052902060343' and 'MenaceOrigine.1050514650356' which stand for environmental, human and natural threat origins. In the ontology the natural and environmental origins are summarized under the term natural origin. On the brief example of the fire threat we showed how to map EBIOS elements such as entity types, vulnerabilities, security objectives, and criteria to the security ontology. The structured XML knowledge representation and the developed mapping table (see Table 1) allowed us the semi-automatic mapping of the knowledge.

5 Mapping the IT Grundschutz Manual to the Security Ontology

According to the proposed methodology, this section shows how we mapped the IT Grundschutz knowledge to the security ontology. In contrast to the EBIOS mapping, the IT Grundschutz mapping requires substantial manual intervention.

5.1 Knowledge Base Analysis

IT Grundschutz is a holistic concept, helping SMEs to create an IT security level that is adequate to satisfy average protection requirements. It has been developed and published by the German Federal Office for Information Security (BSI). The IT Grundschutz Manual contains 3 main catalogs: (i) the modules-catalogs describe the typical aspects and applications for IT security, (ii) the threat-catalogs consist of five sub-catalogs which present numerous threat scenarios, and (iii) the safeguard-catalogs provide detailed safeguard implementation guidelines.

5.2 Mapping Concepts and Relations

Figure 3 shows the relations between IT Grundschutz and the security ontology. Since IT Grundschutz provides its very broad knowledge in a very flat structure (only three catalogs are used), only four Grundschutz entities have been mapped to the security ontology concepts. While entities 'Safeguard' and 'Threat' are mapped directly to the security ontology concepts 'Control' and 'Threat', the entities 'Module' and 'ISO 27001' have been mapped indirectly via support documents (e.g. BSI cross-reference tables). For each module (Generic Aspects, Infrastructure, IT Systems, Networks, etc.) a cross-reference table exists. Each cross-reference table lists threats relevant to the module and shows which safeguards can be used to mitigate the given threat. This enables us to establish the required links between Asset (Module), Control (Safeguard), and Threat (Threat). Since the structure of the IT Grundschutz does not exactly fit the structure of the security ontology, numerous manual actions have to ensure that the knowledge is appropriately incorporated into the security ontology:

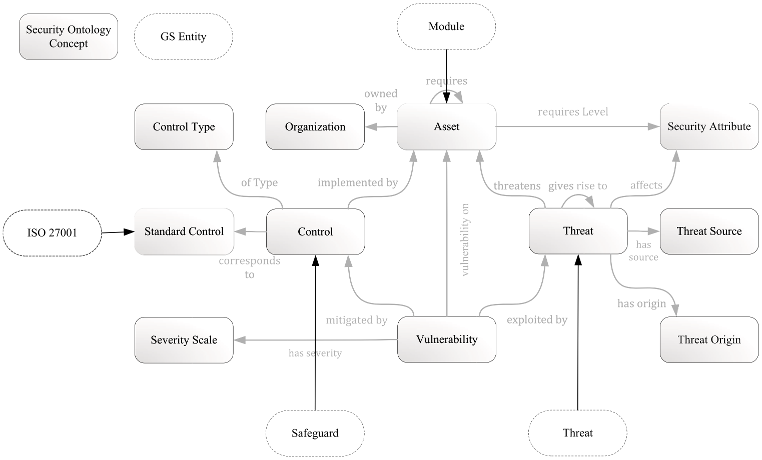

Fig. 3. Relationships among Grundschutz entities and security ontology concepts

1. The BSI cross-reference tables for each IT Grundschutz module are the starting point for the knowledge mapping process: threats and safeguards relevant to the considered module (asset) are identified.
2. IT Grundschutz safeguards are incorporated into the security ontology as controls and the natural language safeguard implementation description is manually transformed into a formal description (relation *sec:implementedBy*). Each control is connected by relation *sec:ofType* to an appropriate control type and the newly created control is related to an ontological representation of its original IT Grundschutz safeguard (relation *sec:correspondsTo*).
3. IT Grundschutz threats are incorporated into the security ontology. Related threats are connected by the *sec:giveRiseTo* relation. Threats directly threatening the considered asset are connected by the *sec:threatens* relation to the considered asset concept. Affected security attributes (e.g. confidentiality) are modeled by the *sec:affects* relation. Threat origin and source are modeled by the relations *sec:threatOrigin* and *sec:threatSource*. Since the IT Grundschutz does not provide structured information on these issues, we had to derive and incorporate them manually.
4. As IT Grundschutz does not provide knowledge on vulnerabilities, we had to derive them and their severity from the corresponding controls. The newly created vulnerability is connected by *sec:mitigatedBy* to corresponding controls and by *sec:exploitedBy* to corresponding threats. Depending on the considered module, relation *sec:vulnerabilityOn* connects the vulnerability to its 'sphere of action'.
5. At last, we have used the BSI ISO27001 - IT Grundschutz mapping tables to link the established controls to ISO 27001 controls.

5.3 Mapping the Knowledge

In this section we show, by using the example of the common server module (B 3.101), how we have mapped the information security knowledge from IT

Grundschutz to the security ontology. The subsequent steps correspond to the mapping process of the previous section.

1. Considered module: common server module (B 3.101) which is equivalent to the *ent:ComputerServer* security ontology concept (ent:ComputerServer $\sqsubseteq$ ent:Asset). Potential IT Grundschutz threat and safeguard: *Disruption of power supply (G 4.1)* and *Local uninterruptible power supply (M 1.28).*
2. The IT Grundschutz safeguard *Local uninterruptible power supply (M 1.28)* has been mapped to the control *sec:UninterruptiblePowerSupplyControl.* The *sec:implementedBy* relation connects the control to the implementation concept *ent:UninterruptedPowerSupplyUnit* → the control is implemented if an uninterrupted power supply unit exists in the considered context. Furthermore, the control has been connected by *sec:controlType* to the *sec:PreventiveControlType* concept. Relation *sec:correspondsTo* connects it to the ontological representation of the original IT Grundschutz control (*gshb:M_1_28*).
3. Threat *Disruption of power supply (G 4.1)* has been mapped to the security ontology concept *sec:PowerLoss* (*sec:PowerLoss* $\sqsubseteq$ *sec:Threat*). The power loss threat is connected by the *sec:givesRiseTo* relation to the already existing *sec:ITComponentsDamage* threat. Based on the natural language threat description the power loss threat has been classified as a threat with a human or natural threat origin, and deliberate or accidental threat source respectively.
4. The vulnerability *sec:NoUninterruptiblePowerSupply* has been created. The *sec:exploitedBy* relation connects it to the *sec:PowerLoss* threat. The relation *sec:mitigatedBy* connects it to the *sec:UninterruptiblePowerSupplyControl* control. The relation *sec:vulnerabilityOn* restricts the vulnerability's sphere of action to the *ent:ComputerEquipmentAndAccessories* concept.
5. By using the BSI ISO 27001 - IT Grundschutz Mapping tables we were able to correspond the *sec:UninterruptiblePowerSupplyControl* control to the ISO 27001 controls *iso:A.9.2.1* and *iso:A.9.2.2.*

6 Difficulties in the Mapping Process

The following problems and incompatibilities had to be solved and compensated during the process of mapping EBIOS and the IT Grundschutz Manual to the security ontology:

Identification of Already Existing Concepts in the Ontology: The main problem when mapping several information security best-practice guidelines is the identification of already existing concepts in the ontology. One approach is to automatically search for terms existing in both, the considered best-practice guideline and the security ontology. However, the found items must be considered in detail if they really correspond to the respective counterpart. If the search results return no corresponding terms, existing concepts of the security ontology must be scanned for analogies by manual means.

No Concept for Vulnerabilities: The IT Grundschutz Manual does not work with the concept of vulnerabilities, unlike the NIST Handbook [8] on which the security ontology structure has been built. Therefore, vulnerabilities had to be created artificially from the scratch. Our approach is based on the NIST Handbook which states: *vulnerabilities are often analyzed in terms of missing safeguards.* Therefore, vulnerabilities were derived from the existing IT Grundschutz controls by implication. For example, interpreting the control *fire doors* as *fire doors should be in place*, the derived vulnerability would be *no fire doors.* This mapping mechanism enables the incorporation of the IT Grundschutz Manual knowledge in the security ontology while keeping its knowledge model consistent.

Vague Connections between Threats and Controls: The problem was to create clear relations between a threat and the corresponding control, which initially was not possible due to the structure of the IT Grundschutz Manual. As a solution 72 cross-reference tables, one for each IT Grundschutz Manual module, were used to identify the connections between threats and corresponding controls to get a more structured access to the relations.

No Relations between Threats: Unfortunately, EBIOS and the IT Grundschutz Manual do not describe connections between individual threats. Therefore, further information security standards, best-practice guidelines and expert knowledge had to be used to model them. To simplify this process a few top-level threats were identified (e.g. data disclosure, data tampering, and data loss) affecting certain security attributes (confidentiality, integrity, and availability).

Inconsistent Granularity of Information: Since the production of a consistent knowledge base with a similar grade of information detail is aimed for, the information of the IT Grundschutz Manual had to be filtered and changed, and topics covering very specific topics were left out in the mapping process. The mapping of topics mentioned in the BSI ISO 27001 - IT Grundschutz Mapping tables were defined as the minimum for the mapping process.

7 Evaluation

According to [13], informal and formal competency questions have been used to evaluate our ontology with the help of a team of experienced information security professionals. Since most ontology evaluation approaches, as described in [2], [9], or [3], are concerned with selecting the most appropriate ontology from a set of existing ontologies, the approach by [13] has been adopted to create an evaluation methodology which is able to check an ontology against its initial requirements. Therefore, the following evaluation phases have been conducted: (i) identification of informal competency questions based on best-practice guidelines and domain expert interviews, (ii) creation of formal competency questions based on the informal competency questions identified in the previous step, and (iii) evaluation (conducted by domain experts) of the formal competency question result sets. As domain experts are central to the ontology evaluation methodology, a team of eight information security professionals was put together. Although this is neither a significant nor representative group of experts, it helped improving the modeled information security knowledge. The following subsections show by an exemplary competency question how the evaluation has been conducted. For a full description of the evaluation process see [6].

7.1 Informal Competency Question

Since the security ontology has been designed to support the information security risk management process the domain expert team developed competency questions according to the generically defined information security risk management phases. The following exemplary competency question is used to show the conducted evaluation process:

Which vulnerabilities are exploited by a given threat and which controls can be used to mitigate the vulnerabilities?

7.2 Formal Competency Question

If a threat is threatening crucial assets of the considered organization, it has to be known which of the existing vulnerabilities the threat exploits and how these vulnerabilities can be mitigated by appropriate controls to reduce the risk to an acceptable level. First of all, the subsequent SPARQL statement queries the vulnerabilities which are associated by relation *sec:exploits* with the power loss threat. Note that the power loss threat is just an example and that the vulnerabilities of each threat can be revealed in the same way.

```
SELECT ?vulnerability
WHERE {sec:PowerLoss sec:exploits ?vulnerability}
```

Since one vulnerability of power loss is the unavailability of an uninterruptible power supply unit, the following query reveals the associated controls.

```
SELECT ?control
WHERE {sec:NoUninterruptiblePowerSupply sec:mitigatedBy ?control}
```

With the appropriate control concept on hand, the organization is now able to derive the control implementation descriptions to mitigate the corresponding vulnerability in the context of a given asset.

7.3 Result Set

By the implementation and the subsequent execution of the formal competency question set, each competency question resulted in a data set, which is evaluated by the security professional expert team in this evaluation step. The formal competency questions return formalized knowledge fragments (e.g., sec:UninterruptiblePowerSupplyUnit to mitigate the no uninterruptible power supply vulnerability and the corresponding power loss threat). Due to the high degree of complexity, not all formal competency questions have been answered with simple ontology queries. Nevertheless, it could be shown that the enriched ontology is able to answer such complex questions, even if an external calculation is required.

8 Conclusion

The more and more comprehensive use of electronic data processing and networking demands for giving particular attention to an IT security management solution capable of providing and dealing with information security knowledge regarding potential threats, vulnerabilities, and controls. We proposed a method for mapping information security best-practice guidelines to existing security ontologies. The method has been demonstrated by mapping EBIOS and the IT Grundschutz Manual to the security ontology: entities and their attributes defined in both knowledge bases have been assigned to corresponding concepts and relations defined in the security ontology. By means of this mapping schema the knowledge provided by EBIOS and the IT Grundschutz Manual can be transformed into OWL-code used by the security ontology. The introduced method for mapping information security knowledge is a guideline trying to equip existing security ontologies with widely accepted information security knowledge. The limitations of the developed method are: (i) in the case of unstructured knowledge sources (e.g. IT Grundschutz) it requires a lot of manual intervention and does not provide a satisfactory degree of automation, (ii) the attempt of incorporating more than one best-practice guideline has shown the limits of the methodology → even if one knowledge source can be semi-automatically incorporated it requires substantial manual intervention to map a further knowledge base on an existing body of knowledge. Further work focuses on addressing these issues and includes the mapping of further information security best-practice guidelines and standards to provide the community with a wide ontological information security knowledge base. Potential applications of such a knowledge base include but are not limited to risk management and automated compliance checks regarding information security standards such as ISO 27001.

Acknowledgments

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 813701 and was performed at the Research Center Secure Business Austria funded by the Federal Ministry of Economics and Labor of the Republic of Austria (BMWA) and the City of Vienna.

References

1. BERR. 2008 information security breaches survey. Technical report, Department for Business Enterprise and Regulatory Reform (BERR) (April 2008)
2. Brank, J., Grobelnik, M., Mladenić, D.: A survey of ontology evaluation techniques. In: SIKDD 2005 at Multiconference IS 2005 (2005)
3. Brewster, C., Alani, H., Dasmahapatra, S., Wilks, Y.: Data driven ontology evaluation. In: International Conference on Language Resources and Evaluation (2004)
4. BSI. IT Grundschutz Manual (2004)

5. DCSSI. Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Section 2 - Approach. General Secretariat of National Defence Central Information Systems Security Division (DCSSI) (February 2004)
6. Fenz, S., Ekelhart, A.: Formalizing information security knowledge. In: ASIACCS 2009: Proceedings of the 2009 ACM symposium on Information, computer and communications security. ACM, New York (2009)
7. Herzog, A., Shahmehri, N., Duma, C.: An ontology of information security. International Journal of Information Security and Privacy 1(4), 1–23 (2007)
8. NIST. An Introduction to Computer Security - The NIST Handbook. Technical report, NIST (National Institute of Standards and Technology), Special Publication 800-12 (October 1995)
9. Patel, C., Supekar, K., Lee, Y., Park, E.: Ontokhoj: a semantic web portal for ontology searching, ranking and classification. In: WIDM 2003: Proceedings of the 5th ACM international workshop on Web information and data management, pp. 58–61. ACM Press, New York (2003)
10. PITAC. Cyber security: A crisis of prioritization - report to the president. Technical report, President's Information Technology Advisory Committee (February 2005)
11. PWC. 2006 information security breaches survey 2006. Technical report, PriceWaterhouseCoopers (2006)
12. Schumacher, M.: Security Engineering with Patterns - Origins, Theoretical Model, and New Applications. Springer, Heidelberg (2003)
13. Uschold, M., Grüninger, M.: Ontologies: Principles, methods and applications. Knowledge Engineering Review 11(2), 93–155 (1996)
14. W3C. OWL - web ontology language (February 2004)