

Ontology based IT-security planning

Stefan Fenz

Secure Business Austria - Security Research
Favoritenstr. 16
1040 Vienna, Austria
sfenz@securityresearch.at

Edgar Weippl

Secure Business Austria - Security Research
Favoritenstr. 16
1040 Vienna, Austria
eweippl@securityresearch.at

Abstract

IT-security has become a much diversified field and small and medium sized enterprises (SMEs), in particular, do not have the financial ability to implement a holistic IT-security approach. We thus propose a security ontology, to provide a solid base for an applicable and holistic IT-security approach for SMEs, enabling low-cost risk management and threat analysis.

1. Introduction

With the need to implement IT-security measures in almost every environment and faced with the growing scope of applications, it is becoming increasingly difficult for experts in different domains to understand each other and use precisely defined terminology. [4], [9] and [8] have already proposed security-related ontologies but a holistic security ontology is still missing. Such an ontology can help to clarify the meaning and interdependence of IT-security relevant terms [5] and can, furthermore, integrate the interdependencies of threats, countermeasures, and resources. The integration of these interdependencies is necessary to model the events that threaten existing resources. Subsequently, for each threat we have to model proper countermeasures capable of protecting the resources. The ontology proposed in the current paper combined with an user interface will enable SMEs to perform low cost risk management and threat analysis without requiring the purchase of extensive consulting services in order to implement standards such as COBIT [3] or ISO17799 [7].

2. The Security Ontology

The security ontology consists of five sub-ontologies: (1) Attribute, (2) Threat, (3) Infrastructure, (4) Role, and (5) Person.

Attribute We derived the *Attribute* sub-ontology from [2], unifying the security- and dependability-relevant attributes: *Availability, Confidentiality, Integrity, Maintainability, Reliability and Safety*. These attributes are necessary to model the impact of threats and each instance in the *Threat* ontology impacts n security attributes. The ontology shows which threats influence certain security attributes and enables the company to prioritize the IT-security strategy with regard to specific attributes.

Threat Figure 1 shows an excerpt of the most important parts and relations of the *Threat* ontology. We derived the fundamental structure from [2] and extended it with our own concepts and relations. The *Threat* ontology with its various relations represents a central part of the entire security ontology and enables the mapping of threats including proper countermeasures, threatened infrastructure, and proper evaluation methods. The most important relations in a nutshell: Any instance of concept *sec:Threat* or one of its sub-concepts affects n instances of class *Attribute* and with *sec:preventedBy* and its inverse relation it is possible to map mitigating countermeasures to a certain threat. To enable the mapping of a threatened infrastructure to a defined threat, the relation *sec:threatens* was introduced, where each threat threatens n infrastructure elements. Last but not least, the *sec:evaluatedBy* relation enables the user to map certain evaluation methods (e.g., qualitative methods, quantitative methods) to a defined threat class to support the user in risk analysis.

Infrastructure This sub-ontology describes infrastructure elements such as buildings, rooms, electronic devices, networks, etc. and the United Nations Standard Products and Services Code [10] along with the ITAndTelecommunication branch provide a large part of the security ontology. A complete listing of all infrastructure elements and their relationships goes beyond the scope of this paper and we recommend extending the infrastructure ontology dynamically to satisfy the actual requirements.

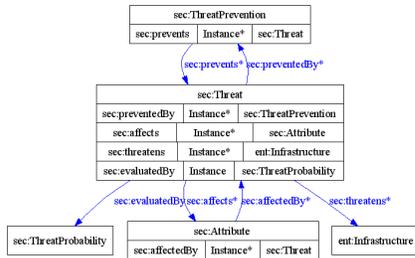


Figure 1. Threat ontology - concept relations

Role and Person The integration of the role-ontology is used to map enterprise hierarchies to the security ontology. The person-ontology represents a simple listing of natural persons who are relevant for the modeling of certain security issues. Every person holds n roles.

2.1. Proof of Concept

To evaluate the security ontology, we created a prototype implementation for a common threat scenario where the simulation shows the financial damage caused by a spreading fire. We have to define the starting point for the fire and since the company's entire building is mapped to the ontology we can then simulate the fire's spread. The *Fire* instance itself is equipped with the attribute *spreadTime*, which allows us to specify the spread time in minutes. Each room and the contained IT-infrastructure elements are entirely burned when the fire spreads to the next room and together with the *assetCost* and *outageCost* attributes, which are stored at each infrastructure element, it is possible to calculate the damage accrued over a specified period of time. Beside the outage costs of machines, we also consider possible personnel outage costs and therefore employees are associated with the infrastructure elements necessary for their work. If this infrastructure is destroyed, the outage costs are accumulated by adding the outage costs of the infrastructure and the outage costs of the associated employee. Of course we also have to consider detection (i.e. smoke detector), preventive (i.e. fire resistant materials) and corrective (i.e. preaction pipe) controls. Each corrective control is specified by the time it takes to extinguish one room and is also associated with a detection control, which specifies the reaction time. For instance: The automatic fire extinguishing system is connected with a smoke detector. In the case of fire, the smoke detector reacts within 5 seconds and activates the automatic extinguishing system. Without an automatic detector someone has to activate the extinguishing system manually resulting in the fire spreading to a bigger radius. More technical details about the simulation and the damage calculation can be found in [1].

3. Conclusion

We presented a security ontology that allows small and medium sized enterprises to implement a holistic IT-security approach and we see two potential application areas for such an ontology. First, it can be used to define a precise terminology of the IT-security sector. Second, the ontology provides a framework to store machine-readable knowledge about the security domain and relevant infrastructure elements. The framework proposed in this paper represents the ontological integration of best practices ([10], [2]), which are enhanced with new concepts and additional attributes. Furthermore, we modeled an example of a threat to evaluate the ontology. To use the ontology with further threats or for a completely different security-related purpose it can be extended with additional concepts and/or subontologies. Further research activities focus on the formulation of a program-controlled mapping of standards such as [10] or [6] and the integration of additional threats. An enhanced prototype with a user interface for the ontology management and advanced risk analysis support will take failure probability into account.

4. Acknowledgements

This work 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 federal province of Vienna.

References

- [1] M. K. Andreas Ekelhart, Stefan Fenz and E. Weippl. Security ontology: Simulating threats to corporate assets. Vienna University of Technology, 2006.
- [2] A. Avizienis, J.-C. Laprie, B. Randell, and C. E. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Sec. Comput.*, 1(1):11–33, 2004.
- [3] Cobit. <http://www.isaca.org/>, 2006.
- [4] G. Denker, L. Kagal, T. W. Finin, M. Paolucci, and K. P. Sycara. Security for daml web services: Annotation and matchmaking. In *International Semantic Web Conference*, pages 335–350, 2003.
- [5] M. Donner. Toward a security ontology. *IEEE Security and Privacy*, 1(3):6–7, May/June 2003.
- [6] eclass. <http://www.eclass.de/>, 2006.
- [7] Iso17799. <http://www.iso.org/>, 2006.
- [8] A. Kim, J. Luo, and M. Kang. Security ontology for annotating resources. In *OTM Conferences (2)*, pages 1483–1499, 2005.
- [9] L. A. F. Martimiano and E. dos Santos Moreira. An owl-based security incident ontology, 2005.
- [10] United nations standard products and services code. <http://www.unspsc.org/>, 2006.