

Security Ontologies: How to Improve Understanding of Complex Relationships

Edgar R. Weippl, Stefan Fenz, Andreas Ekelhart
Secure Business Austria &
Vienna University of Technology
Vienna, Austria
weippl@securityresearch.at

Key words: E-learning, Security, Ontology

Abstract: It is commonly accepted that simulation can provide a valuable tool in improving learning. Building on a complex knowledge base of IT security related concepts we offer our students a simulation to experience how different safeguards can influence the outcome of security incidents. The goal is to teach students that countermeasures have to cost-effective, that is, the cost of installing and operating safeguards should not exceed the anticipated benefit.

1 Introduction

In the past years, security education has become increasingly important. Many universities created Master programs in IT security either with a bias towards business issues such as corporate governance or with focus on technical skills such as ethical hacking. Moreover, security classes are offered also for students in computer science or business courses.

Our experience with various security classes has shown that students are usually skilled in the technical tasks that we teach. They know, for instance, details of router vulnerabilities (technical focus) or can perform the required steps for a security risks analysis (business focus) reasonably well. However, they usually lack—just like most professionals in industry and many academics—the understanding of how vulnerabilities and security measures may interact.

In this paper we propose to use a simulation tool (Fenz et al 2006, Ekelhart et al 2006) to show students how security measures influence the total damage that a threat can cause. The rationale is straight-forward. We model the location of IT infrastructure (such as servers, PCs, network equipment), the applications that run on this infrastructure, the business processes that require the applications, and the users who work in the business processes.

Simulation tools will be the next step in improving e-learning (Chapman 2004). According to Lee's (2006) taxonomy, we created a cognitive, learner-to-interface, contextual simulation (C3C). While our simulation is no real game-based simulation, we do share most requirements with Bagley-Woodward's (2006) work on game-based simulation and – not surprisingly – many the interaction mechanisms we will provide are similar. Some common requirements are “Predict the impact of specific errors on the total [...] experience”, “Predict the impact of a specific error [...]”. Bulger (2006) reports that in-class use of simulation helps to improve attention spans of students and may thus impact learning outcome.

2 Security Ontologies

We created a security ontology to improve the planning and validation of security policies and safeguards. After initially using this ontology in consulting projects, we discovered that we often used this tool to educate decisions makers in companies. Therefore, we decided to extend the use of the tools to the teaching of security at our university. In the ontology there are three different regions that can be distinguished.

1. One part is based on taxonomy on security and dependability by Landwehr (Avizienis 2004),
2. The second region contains concepts related to IT infrastructure, and
3. Personnel and internal role may be modeled in the third region.

The taxonomy is designed in a very general way to facilitate easy maintenance and encourage companies to adapt the knowledge base to their specific needs. Technically, the ontology is encoded in OWL (Web Ontology Language (Owl 2004)).

A *Threat* (such as virus outbreak or fire) impacts *security attributes* such as data integrity or availability. Fundamental concepts and the most common threats are derived from Avizienis (2004) and Peltier (2001). The strength of semantically enriched knowledge representation is that concepts are linked with typed links. The most important relationships can be summarized as follows. Any instance of concept *Threat* or one of its sub-concepts affects one or more instances of concept *Security Attribute* (e.g. Availability, Integrity, Maintainability). The relationship *preventedBy* and its inverse relationship are used to map mitigating countermeasures to a certain threat. We defined the relationship *threatens* to link a threatened element of the infrastructure to a defined threat. Finally, *evaluatedBy* is a relationship that was created to map evaluation methods (e.g. probabilistic methods, qualitative methods, and quantitative methods) to a defined class of threats. The rationale is that this will support the user and the ontology-based application in a risk analysis. In fact the ontology shows which threats influence certain security attributes, and is thus useful if a company wants to prioritize the IT-Security strategy regarding specific attributes.

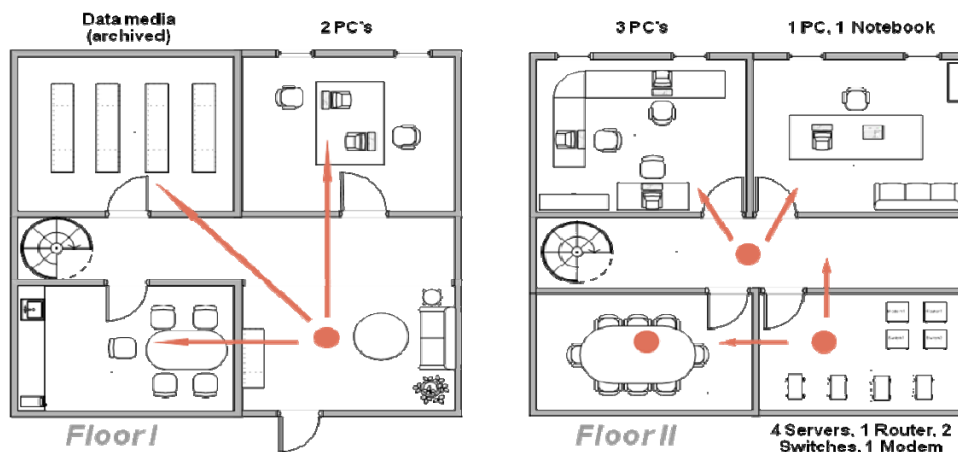


Figure 1: The ontology describes relationships of physical objects such as the location of servers, PCs and rooms.

3 Simulations

In this section we provide an example of how advanced students would model a company's IT infrastructure using the aforementioned security ontology. In introductory courses, we will provide students with the ontology. A specification could be as follows: The company is an SME with six employees. Their main business is software sales and custom programming to modify their standard software. The company rents two floors (1st and 2nd floor) of a 5-floor building in the center of a small town. The following listing shows the allocation of relevant (IT) infrastructure elements: (1) First floor - Office room (R0103): 2 PC's, (2) First floor - Storage room (R0104): data media (archived), (3) Second floor - Server room (R0202): 4 Servers, 1 Router, 2 Switches, 1 Modem, (4) Second floor - Office room (R0203): 1 PC, 1 Notebook, and (5) Second floor - Office room (R0204): 3 PC's.

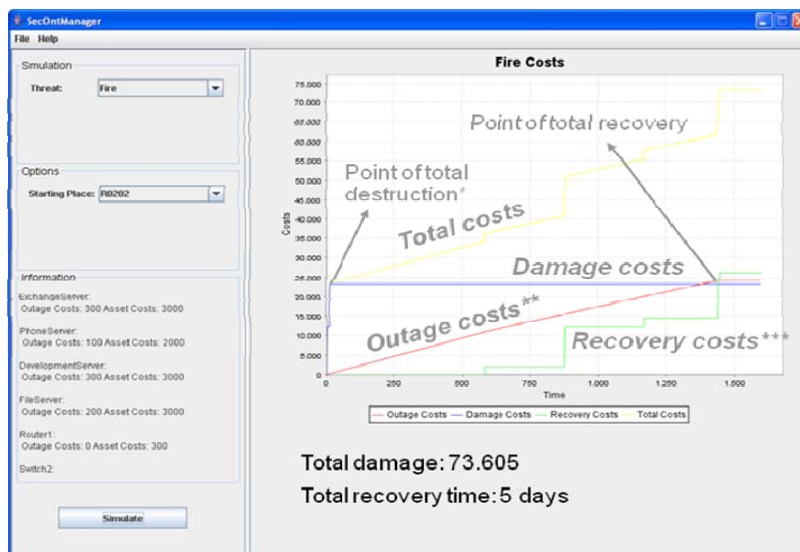
Using the well known ontology tool Protégé, advanced students would model the company and be able to run the simulation. In introductory courses the teacher would prepare the ontology and students would simply run simulations and make minor modifications such as adding or removing countermeasures.

After describing the company with its infrastructure, we specify the disaster which will hit our software company. Due to its simplicity we chose the threat of fire, as a physical threat. The simulation shows the damage in the course of time; a certain room can be defined as the fire source; the speed of propagation without any countermeasures will be, for instance, 5 minutes per floor and 5 minutes per room. Every infrastructure element is assigned to a certain room. In the case of fire all infrastructure elements within a room will be destroyed completely. The outage costs per room correspond to the outage costs sum of all destroyed elements, which are located in the room.

It is possible to assign countermeasures to any of the rooms. These safeguards will lower either the probability of occurrence or the speed of propagation in the case of fire. For instance, the fire extinguisher is located in room R0102 and will start, when switched on, immediately; it will extinguish the room within one minute, before it can propagate to other rooms.

A threat and a corresponding starting point have to be chosen before a simulation can be started. We decide for fire as threat and the server room (Room0202) as origin of fire. The program run produces a detailed log file which shows how the fire spreads from room to room and what damage it causes.

The simulation tool processes each room completely. Within each room all IT infrastructure elements, the corresponding business process, and the people impacted by failing business processes are calculated. Currently the tools cannot deal with redundant hardware that is located in different rooms that fail at different times. Redundant hardware at an unaffected location, however, is no problem. At the end of the simulation all accrued costs are visualized (see Figures 2 and 3).



' All rooms are burned down – sum of all asset values

'' Unproductive personnel costs due to destroyed infrastructure

''' Increase by restoring infrastructure elements → outage costs line flattens

Figure 2: Simulation run (fire) without any countermeasures installed.

The second figure (Figure 3) shows how damage can be reduced by installing safeguards. We chose to install a fire suppression system in the building. We decide for pre-action pipes in the entire building. Necessary detectors and fire extinguishers amount to 7200 Euros. Running the simulation shows how much the total costs of the failure have decreased. Nevertheless costs and recovery times are still very high. The reason is that water extinguishers damage electric devices. We might also opt for the more expensive CO₂ fire extinguishers for locations where no people work. We can then see whether the higher cost of installing such a system make sense.



Figure 3: With countermeasures the damage is lower.

4 Conclusion

In this paper we present a simulation of how security safeguards can influence the damage caused by threats. We can use this tool to improve the teaching process to show students the complex interactions of physical properties of buildings, IT infrastructure located in buildings, applications that require IT infrastructure and users who need applications to work in their business processes. The simulation uses an ontology as a knowledge base. We store all relevant concepts and relationships in this knowledge base. Advanced students can modify this knowledge base to experiment with the simulation and gain deeper insight into the interdependencies of security safeguards.

5 References

- Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl E. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Sec. Comput.*, 1(1):11–33, 2004.
- Elizabeth Bagley-Woodward, Micah White, Karen Orenstein, Kevin Lane, Tom Warner, John M. Crotty, Patricia Kanode, Strategy for a Game-based Simulation to Transform Global Business Processes, *Proceedings of EDMEDIA 2006*, Orlando, 977 – 983, 2006.
- Bryan, Chapman. (2004). *E-Learning Simulation Products and Services*. Brandon-hall report. www.prisim.com/News/execsum_sim2004.pdf
- Stefan Fenz, Andreas Ekelhart, Markus Klemen, and Edgar R. Weippl. Security ontology: Simulating threats to corporate assets. In *Proceedings of the 2nd International Conference on Information Systems Security (ICISS 2006)*, Calcutta, India, December 2006. Springer LNCS
- Andreas Ekelhart, Stefan Fenz, , Markus Klemen, A Min Tjoa, and Edgar R. Weippl. Ontology-based business knowledge. In *Proceedings of the 6th International Conference on Practical Aspects of Knowledge Management (PAKM)*, Vienna, December 2006. Springer LNCS,
- Jeong Min Lee, Theoretical Framework of Instructional Simulation Taxonomy, *Proceedings of EDMEDIA 2006*, Orlando, 2948 – 2953, 2006.
- Owl web ontology language. <http://www.w3.org/TR/owl-features/>, 2004.
- T. R. Peltier. *Information Security Risk Analysis* Boca Raton. Auerbach Publications, Boca Raton, Florida, 2001.
- Monica Bulger Richard E. Mayer Kevin C. Almeroth, Engaged by Design: Using Simulations to Promote Active Learning, *Proceedings of EDMEDIA 2006*, Orlando, 1770 -1777, 2006.