A Community Knowledge Base for IT Security

Stefan Fenz

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Motivation and Problem

- Corporate IT security managers have a difficult time staying on top of the endless tide of new technologies and security threats.
- IT security managers in different organizations face many of the same threats and establish similar solutions, which is clearly inefficient.

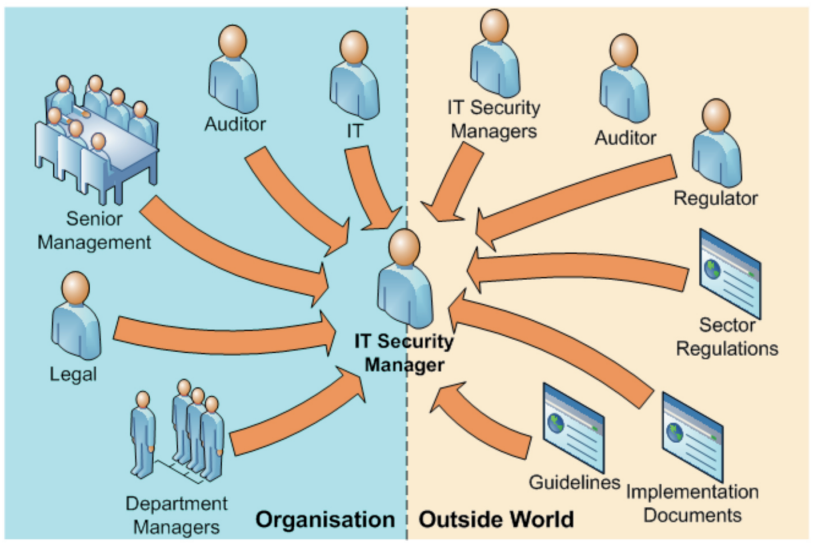

Figure 1: Motivation and Problem

Creating a community knowledge base

- We propose taking an open, shared approach to creating and managing information security knowledge by pooling our efforts to formalize a user-community knowledge base.
- Using consistent, unambiguous classification for the underlying knowledge systematizes the addition and subsequent communication of new and disparate sources of advice and their inherent vocabularies.
- A formalized knowledge base can inform many aspects of information security management, such as risk management, IT security investment trade-offs, compliance checks, and awareness training in an automated way.

The security ontology web portal (sec.sba-research.org)

- Supports role-based user access control, so editing is restricted to defined roles and the corresponding users.
- On the left-hand side, the user selects the entity of interest in the context of the ontological knowledge model (for example, "Malware" threat).
- The right-hand side shows detailed knowledge such as natural-language labels, definitions and comments, entity relationships (such as vulnerabilities that are exploited by the malware threat), and community notes regarding the entity.
- The portal enables structured knowledge sharing by
  - providing a fixed high-level knowledge structure (threats, vulnerabilities, controls, etc.)
  - enabling registered users to edit, discuss, and agree on the knowledge;
  - annotating each change with metadata such as username and time stamp; and
  - providing the knowledge in a standardized form to other applications (for example, for risk or compliance management).

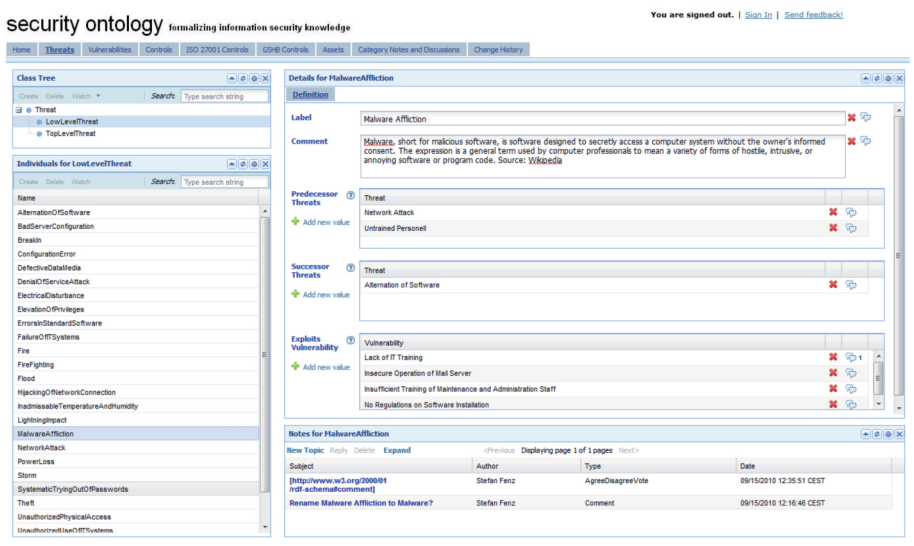

Figure 2: The security ontology portal: sec.sba-research.org

Upcoming Challenges

- Reaching critical mass of users
- All users edit the same ontology and its concepts, so moderators have to decide which knowledge fragments are – according to the majority of users – more accurate and which aren't broadly accepted by the community.
- The knowledge base serves to address shared problems that arise and change. Potential inconsistencies must be addressed by the community, moderators, and (on a logical level) reasoning engines, but despite being perpetually incomplete, a knowledge base can empower the community to address shared challenges.

S. Fenz, S. Parkin, A. van Moorsel: "A Community Knowledge Base for IT Security," in IT Professional, Vol. 13/3, 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.