Ontology- and Bayesian-based Threat Probability Determination

Stefan Fenz and A Min Tjoa (Faculty Mentor)
Institute of Software Technology and Interactive Systems
Vienna University of Technology
Vienna, Austria
Email: {fenz,tjoa}@ifs.tuwien.ac.at

Abstract — *Information security risk management is crucial for ensuring long-term business success and thus numerous approaches to implementing an adequate information security risk management strategy have been proposed. The subjective threat probability determination is one of the main reasons for an inadequate information security strategy endangering the organization in performing its mission. To address the problem this research project proposes an ontology- and Bayesian-based approach for determining asset-specific and comprehensible threat probabilities. The elaborated concepts enable risk managers to comprehensibly quantify the current security status of their organization.*

I. The Security Ontology

A conceptual and formal model of information security is required for supporting the threat probability determination in the information security risk management process. Ontologies are one possibility for modeling the information security domain in order to make it accessible to machines. Therefore, the security ontology [1, 2, 3] was proposed based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12. Figure 1 shows the high-level concepts and corresponding relations of our 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, and it causes damage to certain assets. 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, corrective, deterrent, recovery, or detective measures (control type). Each control is implemented as asset concept, or as combinations thereof. Controls are derived from and correspond to best-practice and information security standard controls. To enrich the knowledge model with concrete information security knowledge the German IT Grundschutz Manual is superimposed on the security ontology and more than 500 information security concepts and 600 corresponding formal axioms are integrated into the ontological knowledge base. 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) standard and ensures that the knowledge is represented in a standardized, formal, and therefore machine-interpretable form.

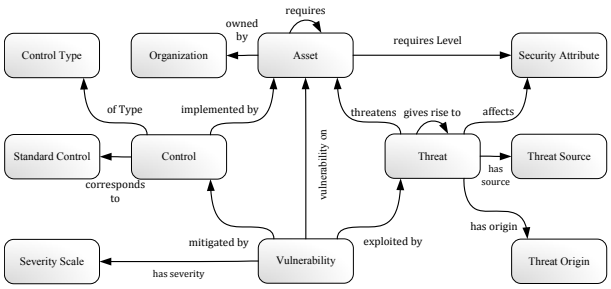

Figure 1: Security relationships

II. Bayesian Threat Probability Determination

This section aims at describing the connection to the security ontology framework, which provides a foundation to enrich the Bayesian network with concrete knowledge. Since the security ontology provides detailed knowledge about threat, vulnerability, and control dependencies, this knowledge could be utilized to build up the Bayesian network for the threat probability determination. Figure 2 gives an overview of the connections between the proposed Bayesian threat probability determination and the security ontology. It is assumed that each node has exactly one of a finite set of probability states (expressed as a vector, representing the probability distribution among distinct states, e.g. high, medium, and low). Since the threat probability or influencing factors cannot be determined quantitatively, a qualitative rating is used in this approach. For each variable a three-point Likert scale was defined to capture the subjective impressions on the input variables and to represent the results on the intermediate and output variables.

First of all, the approach has to set up a threat net, in-

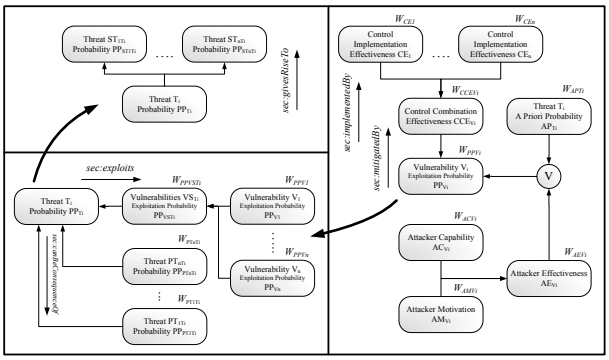

Figure 2: Utilizing the security ontology for the Bayesian threat probability determination

cluding the relations between the threats and their a priori threat probability. Since each threat modeled in the security ontology is connected by the relation *sec:givesRiseTo* to follow-up threats (see Figure 2) the corresponding threat net can easily be created. The a priori threat probability vector $\vec{AP}_{T_i}$ for each threat T_i is also derived from the security ontology, depending on the actual physical location of the organization. The *sec:Probability* concept and the *sec:probabilityDistribution* property of the security ontology connect each threat of a given physical location with its a priori probability. Weights for all threat probability influencing factors (influencing threats and vulnerabilities) are distributed equally.

For each threat the approach has to determine the corresponding vulnerabilities. In the security ontology this relationship is modeled by the *sec:exploits* relation which allows revealing the vulnerabilities of a given threat. As the vulnerabilities vector $\vec{PP_{VS_{T_i}}}$ is determined by single vulnerabilities and their weights, the weight of each vulnerability which influences the intermediate vulnerabilities vector $\vec{PP_{VS_{T_i}}}$ was determined. Since the security ontology provides a severity rating S_{V_i} for each vulnerability (high (3), medium (2), and low(1)), a numerical weight $W_{PP_{V_i}}$ for each vulnerability can be determined by dividing the severity of the considered vulnerability by the severity sum of all vulnerabilities relevant to the threat: $W_{PP_{V_i}} = \frac{S_{V_i}}{\sum_{j=1}^{n} S_{V_j}}$

The exploitation probability of each vulnerability variable is determined by (1) the effectiveness of the implemented control combination $\vec{CCE}_{V_i}$, (2) the attacker's effectiveness $\vec{AE}_{V_i}$ in the case of a deliberate threat source or by the a priori threat probability $\vec{AP}_{T_i}$ in the case of an accidental threat source. By default all components, namely $\vec{CCE}_{V_i}$, $\vec{AE}_{V_i}$, and $\vec{AP}_{T_i}$, are weighted equally. While the attacker's effectiveness $\vec{AE}_{V_i}$ and the a priori threat probability $\vec{AP}_{T_i}$ are not rated on an asset-specific level, the control combination effectiveness $\vec{CCE}_{V_i}$ is determined specifically for the considered asset. Therefore, reasoning algorithms query the security ontology regarding those control implementations effectiveness values which are relevant for the considered asset/vulnerability combination.

With the security ontology relation *sec:mitigatedBy* (see Figure 2) the required control implementation combination which is necessary to mitigate the given vulnerability can be derived. Since each implementation in the recommended control combination has a different effectiveness $\vec{CE}_i$, the weight W_{CE_i} differs dependently on the implementation's importance for the current control combination. The security ontology concept *sec:ControlImplementation* represents the effectiveness for each control/implementation combination $\vec{CE}_i$ by a three-point Likert scale (high, medium, low).

III. Results

The question is if the proposed Bayesian threat probability determination is the solution to the fundamental information security risk management problem, namely disposing of realistic probability values. The answer is neither yes nor no. The advantage of the proposed Bayesian threat probability determination is that it gives the risk manager a methodology to determine the threat probability in a structured and, by incorporating the security ontology, comprehensible way. The calculation schema is fully documented and each state of the Bayesian network can be explained and justified mathematically and formally taking the given input factors into consideration. However, the high dependence on realistic input values requires further research on sound methods to gather, store, and provide these crucial threat probability calculation components.

References

[1] Andreas Ekelhart, Stefan Fenz, Markus Klemen, and Edgar R. Weippl. Security ontology: Simulating threats to corporate assets. In A. Bagchi and V. Atluri, editors, *Information Systems Security, Second International Conference, ICISS 2006*, volume 4332/2006 of *Lecture Notes in Computer Science*, pages 249–259, Kolkata, India, December 2006. Springer Berlin / Heidelberg. 978-3-540-68962-1.

[2] Andreas Ekelhart, Stefan Fenz, Gernot Goluch, and Edgar Weippl. Ontological mapping of common criteria's security assurance requirements. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, editors, *Proceedings of the IFIP TC 11 22nd International Information Security Conference, IFIPSec 2007*, pages 85–95, Sandton, South Africa, May 2007. IFIP. 978-0-387-72366-2.

[3] Thomas Neubauer, Andreas Ekelhart, and Stefan Fenz. Interactive selection of ISO 27001 controls under multiple objectives. In *Proceedings of the IFIP TC 11 23rd International Information Security Conference, IFIPSec 2008*, pages 477–492, Boston, July 2008. Springer.