How to determine threat probabilities using ontologies and Bayesian networks

[Extended Abstract]

Stefan Fenz
Vienna University of Technology
Vienna, Austria
fenz@ifs.tuwien.ac.at

Thomas Neubauer
Secure Business Austria
Vienna, Austria
neubauer@securityresearch.ac.at

ABSTRACT

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.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous

General Terms

Security

Keywords

threat probability determination, risk management, information security

1. INTRODUCTION

Information security risk management was defined, e.g., by the National Institute of Standards and Technology (NIST) in Special Publication 800-30 as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' mission. As the security measures which are necessary to lower the risk are mostly associated with costs, organizations strive for those measures which are capable to reduce the risk to an acceptable level at the lowest possible costs. Risk is defined as the probability per time unit of the occurrence of a unit cost burden [6]. In the information security context risk is defined as a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [7]. Typically decision makers (e.g., asset owners according to [4]) have to (i) define and (ii) value their assets, (iii) identify threats and vulnerabilities affecting the asset, (iv) identify controls that are currently used for protecting the asset, (v) assess the assets' risk level and (vi) identify alternative or additional controls in order to meet the demanded risk level.

The approach presented in this paper supports decision makers at determining asset-specific threat probabilities by using a security ontology in combination with a Bayesian threat probability calculation model. The security ontology framework provides a foundation to enrich the Bayesian network with concrete knowledge and to enable automatic processing by machines. Since the security ontology provides detailed knowledge about threat, vulnerability, and control dependencies, this knowledge is utilized to build up the Bayesian network for the threat probability determination. The objective of the Bayesian network is to determine asset-specific threat probabilities by taking asset-specific influence factors into account. The research question discussed in this paper is, if the proposed Bayesian threat probability determination is the solution to the disposing of realistic threat probability values and, thus the risk calculation.

2. OVERVIEW

The majority of business processes in today's world are supported by (IT) assets. Therefore, the success of a business strategy is linked to the availability of appropriate (IT) assets and its protection by safeguards. Figure 1 shows our overall risk determination methodology (see [1] and [2] for further details). The risk associated with each corporate asset is the product of:

- Asset Importance: we use business process models as a basis for identifying corporate risks by estimating the importance of the assets needed for executing a certain business process.
- Asset-specific Threat Probability: the security ontology (cf. Chapter 3) and the Bayesian threat probability determination (cf. Chapter 4) have been developed to calculate asset-specific threat probabilities.

This extended abstract focuses on describing the concepts we have developed to determine asset-specific threat probabilities.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
CSIIRW '09, April 13-15, Oak Ridge, Tennessee, USA
Copyright 2009 ACM 978-1-60558-098-2 ...$5.00.

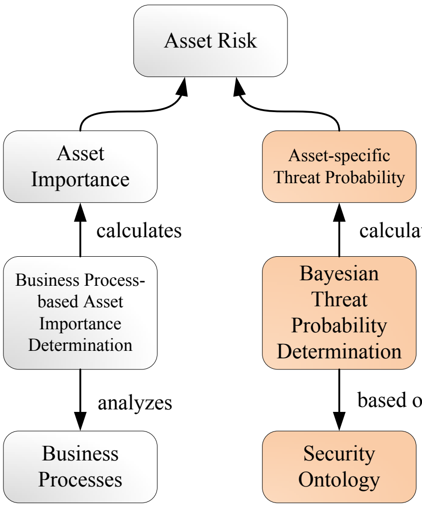

Asset Risk
Asset Importance
Asset-specific Threat Probability
calculates
calculates
Business Process-based Asset Importance Determination
Bayesian Threat Probability Determination
analyzes
based on
Business Processes
Security Ontology

Figure 1: Overview (the extended abstract focuses on the colored concepts)

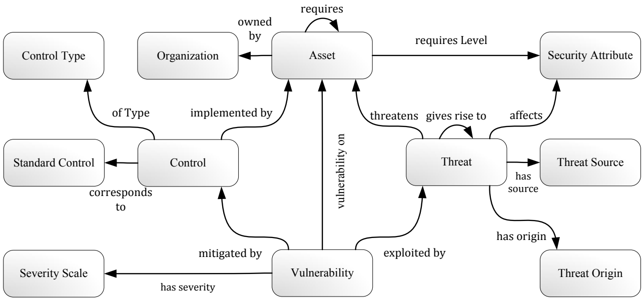


Figure 2: Security relationships

3. THE SECURITY ONTOLOGY

Figure 2 shows the high-level concepts and corresponding relations of our security ontology [3], based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12.

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, 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.

4. BAYESIAN THREAT PROBABILITY DETERMINATION

Figure 3 gives an overview of the connections between the proposed Bayesian threat probability determination and the security ontology. T is assumed to be the set of variables $\{T_1, ..., T_n\}$ representing the threats which probabilities have to be determined. It is assumed that each threat 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. In contrast to a quantitative rating with which it is hardly possible to determine the occurrence of a certain threat with a 67% and not with a 68% chance, a qualitative rating (e.g. high, medium, and low) is a more human way of estimating or handling a probability. To enable humans to provide the necessary input and to understand the corresponding output respectively, clear definitions for every possible variable state in the Bayesian network were provided. For each variable a three-point Likert scale is defined to capture the subjective impressions on the input variables and to represent the results on the intermediate and output variables.

As already mentioned, the objective of the Bayesian network is to determine the probability of threats taking various influence factors into account. Therefore, the following factors have been identified: (1) predecessor threats $(PT_{1_{T_i}}, ..., PT_{n_{T_i}})$ influence the considered threat (T_i) which influences its successor threats $(ST_{1_{T_i}}, ..., ST_{n_{T_i}})$; therefore dependencies amongst a given threat set T had to be considered (see the upper left section in Figure 3), (2) according to [7], each threat (T_i) requires one or more vulnerabilities $(V_1, ..., V_n)$ to become effective; thus the existence of unmitigated vulnerabilities significantly influences the threat probability (see the lower left section in Figure 3), (3) controls can be used to mitigate identified vulnerabilities, while the mitigation depends on the effectiveness of a potential control combination (CCE_{V_i}) which again depends on the actual effectiveness of the controls which are used in this combination $(CE_1, ..., CE_n)$, and (4) (a) in the case of deliberate threat sources, the vulnerability exploitation probability (PP_{V_i}) is determined by the effectiveness of a potential attacker (AE_{V_i}) which is again determined by the motivation (AM_{V_i}) and the capabilities (AC_{V_i}) of the attacker as stated in [5], (b) in the case of accidental threat sources and/or natural threat origins, the vulnerability exploitation probability (PP_{V_i}) is determined by the a priori probability (AP_{T_i}) of the corresponding threat (T_i) (see the right section of Figure 3). Figure 3 shows the proposed model for determining threat probabilities by taking the aforementioned factors into consideration. Note that the risk manager merely has to rate the nodes for the attacker's motivation AM_{V_i} and the attacker's capabilities AC_{V_i}. Further input, such as poten-

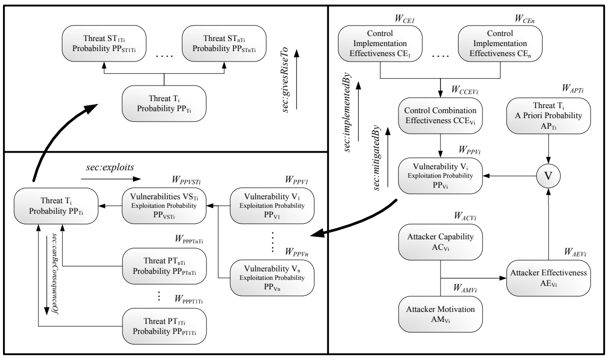


Figure 3: Utilizing the security ontology for the Bayesian threat probability determination

tial control implementations, their effectiveness CE_i and the calculation schemes for every intermediate node, is derived from the security ontology. The result for each threat probability is represented as a distribution of the chosen rating scale (e.g. high, medium, and low).

First of all, the approach sets up a threat net, including 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 3) 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 3) 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).

5. CONCLUSIONS

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.

6. REFERENCES

[1] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for supporting information security risk management. In *Proceedings of the 42nd Hawaii International Conference on System Sciences*. IEEE Computer Society, 2009.

[2] A. Ekelhart, T. Neubauer, and S. Fenz. Automated risk and utility management. In *Proceedings of the Sixth International Conference on Information Technology: New Generations*, 2009.

[3] S. Fenz and A. Ekelhart. Formalizing information security knowledge. In *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security*. ACM, 2009.

[4] ISO/IEC. ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, 2005.

[5] ISO/IEC. ISO/IEC 27005:2007, Information technology - Security techniques - Information security risk management, November 2007.

[6] A. Sage and E. White. Methodologies for risk and hazard assessment: A survey and status report. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-10(8):425–446, August 1980.

[7] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, July 2002.

AURUM

© 2004-2008 Secure Business Austria

Motivation 1/2

- Security breaches pose major threats
  - to the reliable execution of corporate strategies and
  - may have negative effects on business value, e.g., on profit, shareholder value, or reputation.
- As a consequence, companies are steadily increasing the amount of resources for protecting corporate assets.
- Although companies consider security as one of the most important issues on their agenda, many companies are not aware
  - how much they spend on security and
  - if their investments in security are effective.

© 2004-2008 Secure Business Austria

Motivation 2/2

- Risk management provides an effective approach for measuring the security through risk assessment, risk mitigation and evaluation:
  - CRAMM,
  - NIST SP 800-30,
  - CORAS,
  - OCTAVE,
  - EBIOS, and recently
  - ISO 27005.
- Well established concepts.

© 2004-2008 Secure Business Austria

Problem Statement

- Best-practice guidelines provide excellent knowledge about potential threats, vulnerabilities, and controls, but organizations are not always able to consider all the complex relationships between relevant information security concepts
- Error-prone manual application of general information security knowledge to the infrastructure of the organization
- Subjective threat probability determination
- Lack of knowledge regarding appropriate control implementations

→ results in inadequate information security strategies

© 2004-2008 Secure Business Austria

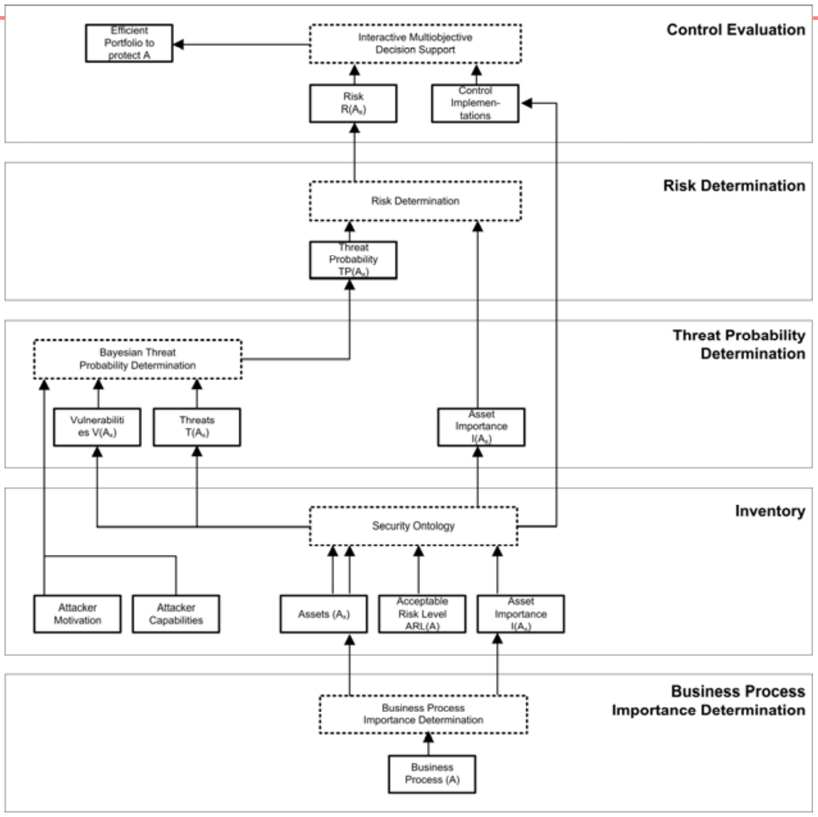
Solution Approach

- Goals:
  - –minimize the interaction necessary between user and system;
  - –provide decision makers with an intuitive solution;
  - –use without extensive knowledge about the information security domain.

- Methodology (AURUM) for supporting the entire NIST SP 800-30 risk management standard.
  - –(I) Inventory of the Organization
  - –(II) System Characterization
  - –(III) Threat and Vulnerability Assessment
  - –(IV) Risk Determination
  - –(V) Control Evaluation and Implementation

© 2004-2008 Secure Business Austria

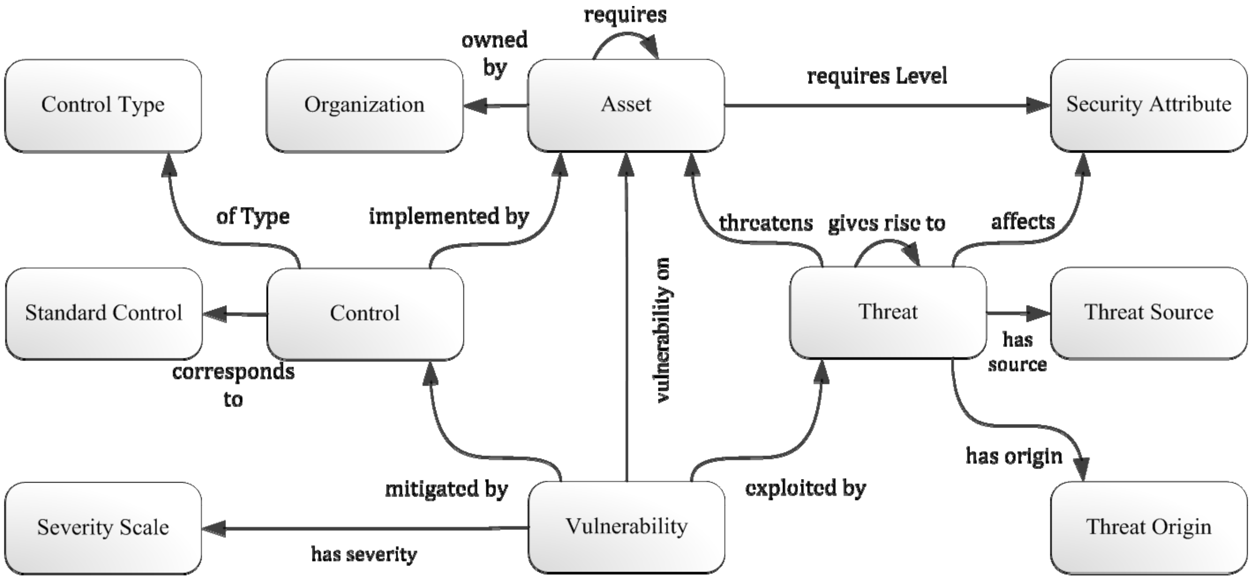
AURUM Methodology


Control Evaluation
Efficient Portfolio to protect A
Interactive Multiobjective Decision Support
Risk R(A$_x$)
Control Implemen-tations
Risk Determination
Risk Determination
Threat Probability TP(A$_x$)
Threat Probability Determination
Bayesian Threat Probability Determination
Vulnerabiliti es V(A$_x$)
Threats T(A$_x$)
Asset Importance I(A$_x$)
Inventory
Security Ontology
Attacker Motivation
Attacker Capabilities
Assets (A$_x$)
Acceptable Risk Level ARL(A)
Asset Importance I(A$_x$)
Business Process Importance Determination
Business Process Importance Determination
Business Process (A)

© 2004-2008 Secure Business Austria

The Security Ontology
top-level concepts and relations

www.securityresearch.at



Further details: Fenz, S. & Ekelhart, A.: “Formalizing information security knowledge” *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security, ACM,* **2009**

© 2004-2008 Secure Business Austria

(II) Inventory 1/2

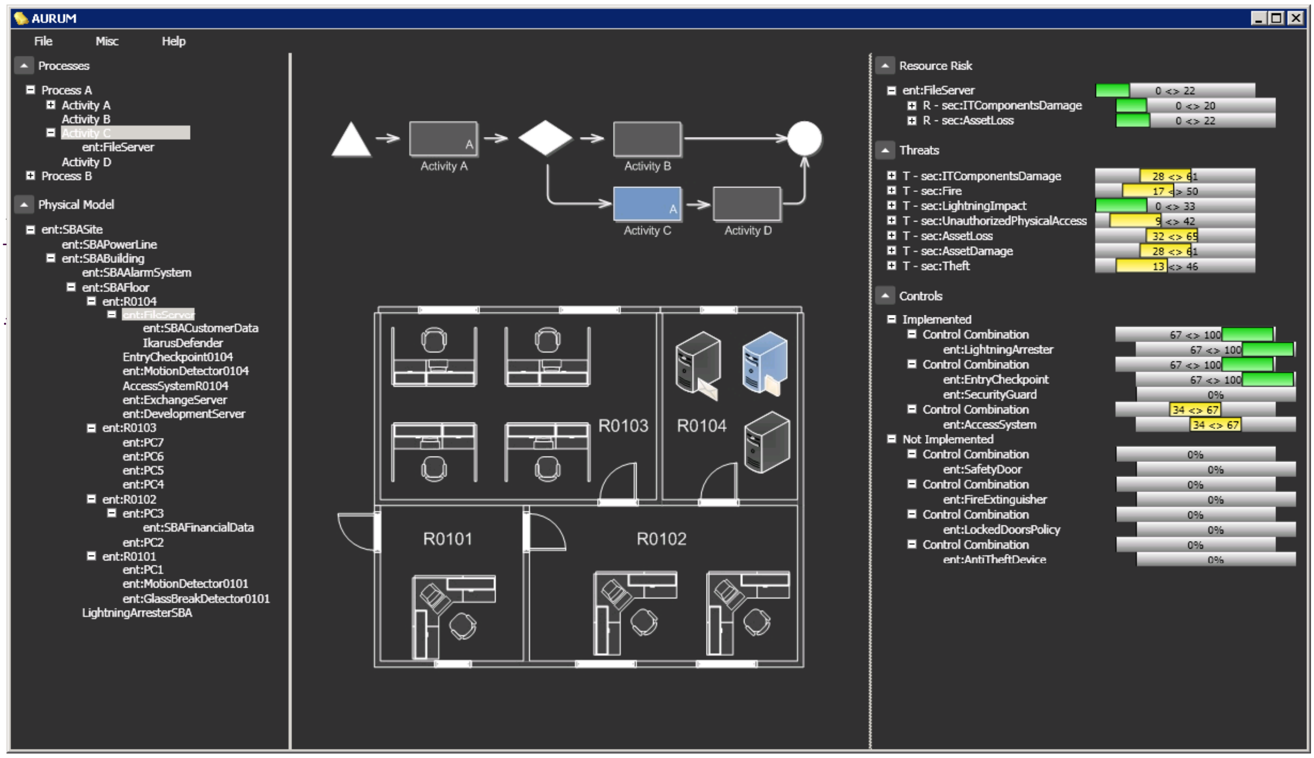
www.securityresearch.at

- Refinement of the system boundaries, of the assets and information used and/or required by the defined system
  - systematic inventory of hardware, software, existing physical and organizational controls, system interfaces, data, information, and persons.
  - determination of the acceptable risk level for each inventoried asset.

- Process Model: use of business process models as a basis for identifying corporate risks; import from business process management tools such as Adonis, Aris.
- Location Model: AURUM allows to generate a building map including the location of all assets.

© 2004-2008 Secure Business Austria

(II) Inventory 2/2



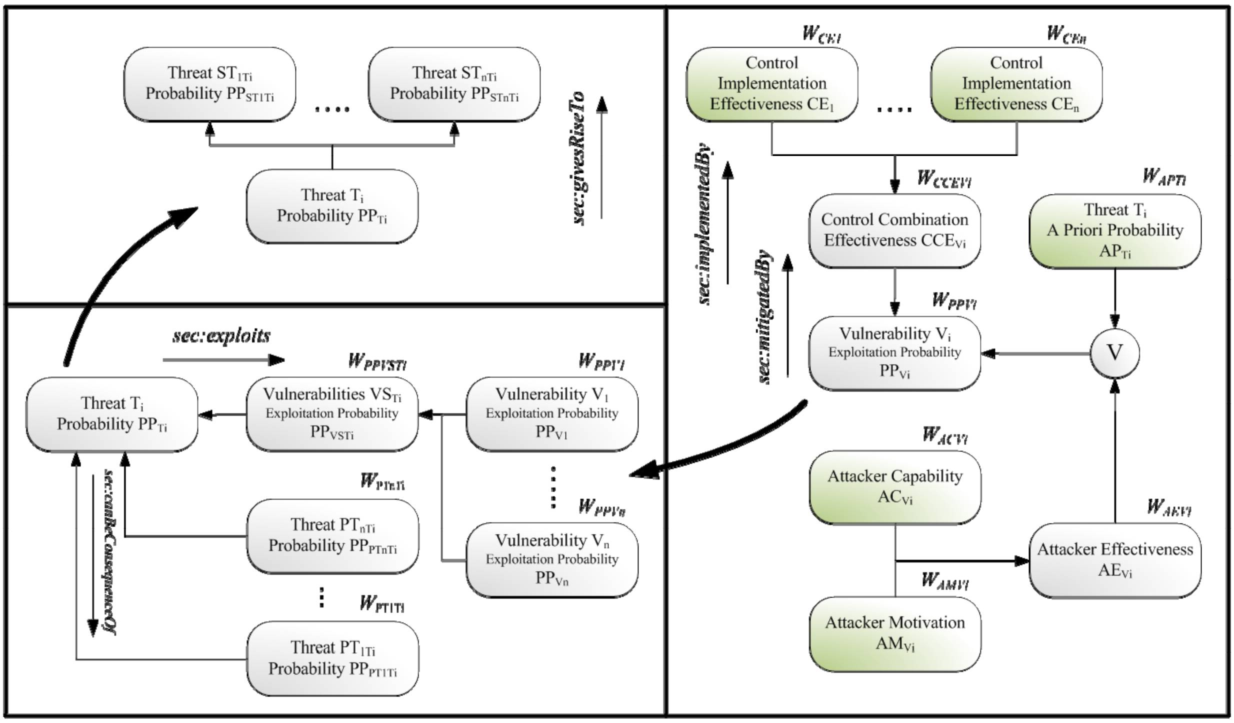
```
Processes
  ⊟ Process A
      ⊞ Activity A
        Activity B
      ⊟ Activity C
          ent:FileServer
        Activity D
  ⊞ Process B

Physical Model
  ⊟ ent:SBASite
        ent:SBAPowerLine
      ⊟ ent:SBABuilding
          ent:SBAAlarmSystem
          ⊟ ent:SBAFloor
              ⊟ ent:R0104
                  ⊟ ent:FileServer
                        ent:SBACustomerData
                        IkarusDefender
                    EntryCheckpoint0104
                    ent:MotionDetector0104
                    AccessSystemR0104
                    ent:ExchangeServer
                    ent:DevelopmentServer
              ⊟ ent:R0103
                    ent:PC7
                    ent:PC6
                    ent:PC5
                    ent:PC4
              ⊟ ent:R0102
                  ⊟ ent:PC3
                        ent:SBAFinancialData
                    ent:PC2
              ⊟ ent:R0101
                    ent:PC1
                    ent:MotionDetector0101
                    ent:GlassBreakDetector0101
          LightningArresterSBA
```

```
Resource Risk
  ⊟ ent:FileServer                               0 <> 22
      ⊞ R - sec:ITComponentsDamage                 0 <> 20
      ⊞ R - sec:AssetLoss                          0 <> 22

Threats
  ⊞ T - sec:ITComponentsDamage                   28 <> 61
  ⊞ T - sec:Fire                                 17 <> 50
  ⊞ T - sec:LightningImpact                      0 <> 33
  ⊞ T - sec:UnauthorizedPhysicalAccess           9 <> 42
  ⊞ T - sec:AssetLoss                            32 <> 65
  ⊞ T - sec:AssetDamage                          28 <> 61
  ⊞ T - sec:Theft                                13 <> 46

Controls
  ⊟ Implemented
      ⊟ Control Combination                        67 <> 100
            ent:LightningArrester                    67 <> 100
      ⊟ Control Combination                        67 <> 100
            ent:EntryCheckpoint                      67 <> 100
            ent:SecurityGuard                        0%
      ⊟ Control Combination                        34 <> 67
            ent:AccessSystem                         34 <> 67
  ⊟ Not Implemented
      ⊟ Control Combination                        0%
            ent:SafetyDoor                           0%
      ⊟ Control Combination                        0%
            ent:FireExtinguisher                     0%
      ⊟ Control Combination                        0%
            ent:LockedDoorsPolicy                    0%
      ⊟ Control Combination                        0%
            ent:AntiTheftDevice                      0%
```

(III) Threat Probability Determination 1/2

- The goal of the threat identification step is to determine potential threats and their corresponding threat sources.
- AURUM supports the decision maker to answer the following questions:
  - Which threats threaten critical assets?
  - Which threat is a multiplier (i.e. which threat gives rise to other threats)?
  - Which vulnerabilities have to be exploited by a threat to become effective?

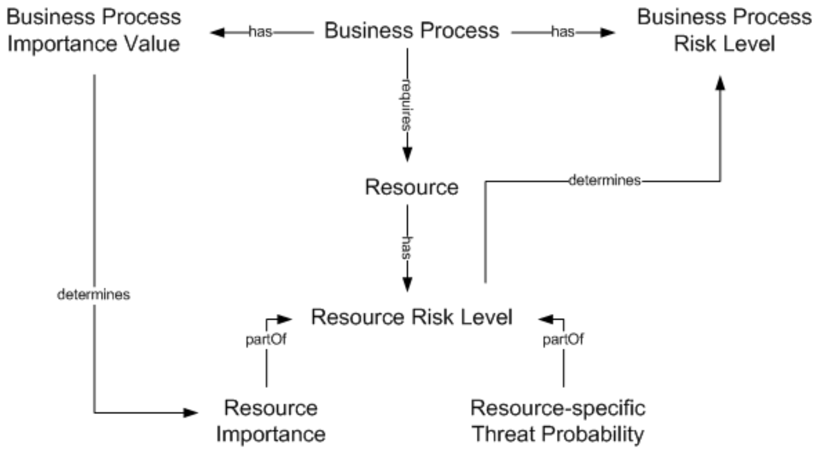
(III) Threat Probability Determination 2/2


Threat ST_{1Ti} Probability PP_{ST1Ti}
....
Threat ST_{nTi} Probability PP_{STnTi}
Threat T_i Probability PP_{Ti}
sec:givesRiseTo
sec:exploits
W_{PPVSTi}
W_{PPVi}
Threat T_i Probability PP_{Ti}
Vulnerabilities VS_{Ti} Exploitation Probability PP_{VSTi}
Vulnerability V_1 Exploitation Probability PP_{V1}
W_{PTnTi}
W_{PPVn}
Threat PT_{nTi} Probability PP_{PTnTi}
Vulnerability V_n Exploitation Probability PP_{Vn}
W_{PT1Ti}
Threat PT_{1Ti} Probability PP_{PT1Ti}
sec:canBeConsequenceOf
W_{CE1}
W_{CEn}
Control Implementation Effectiveness CE_1
....
Control Implementation Effectiveness CE_n
sec:implementedBy
W_{CCEVi}
W_{APTi}
Control Combination Effectiveness CCE_{Vi}
Threat T_i A Priori Probability AP_{Ti}
sec:mitigatedBy
W_{PPVi}
Vulnerability V_i Exploitation Probability PP_{Vi}
V
W_{ACVi}
Attacker Capability AC_{Vi}
W_{AEVi}
Attacker Effectiveness AE_{Vi}
W_{AMVi}
Attacker Motivation AM_{Vi}

© 2004-2008 Secure Business Austria

(IV) Risk Determination

- Determination of the probability of a threat exploiting a certain vulnerability.
- Risk Level: combining the threat probability with the magnitude of the impact.



© 2004-2008 Secure Business Austria

(IV) Control Evaluation and Implementation 1/2

www.securityresearch.at

- The first phase involves determining solution alternatives that are (i) feasible with respect to given constraints and (ii) Pareto-efficient with respect to a number of objectives.

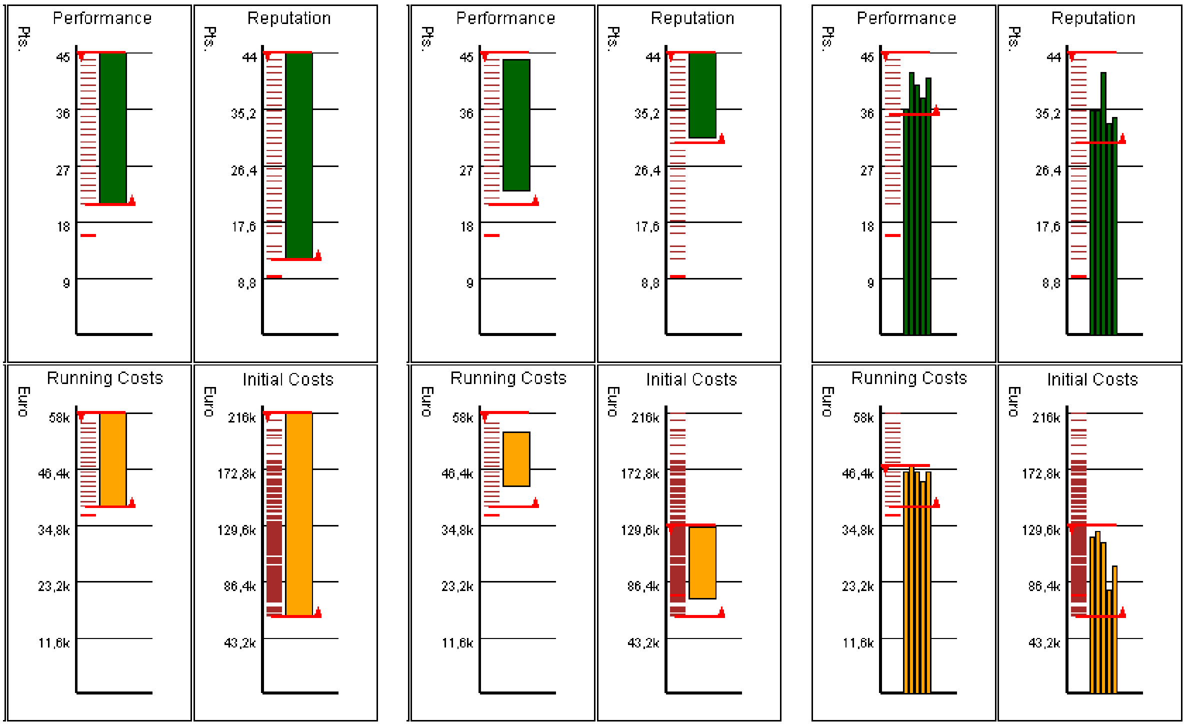
- In the second phase the decision maker is supported in interactively selecting the "best" portfolio.

- The system provides information for each objective on
  - –resource/benefit categories
  - –the efficient solutions from solution space,
  - –on the subset of solutions from the solution space that have remained after the decision maker has entered some aspiration levels.
  - –The red controller represent lower and upper bounds.

© 2004-2008 Secure Business Austria

(IV) Control Evaluation and Implementation 2/2

www.securityresearch.at



© 2004-2008 Secure Business Austria

Conclusions

- AURUM enables organizations
  - – to automatically map general information security knowledge to their infrastructure,
  - – to quantify the current security status of their organization,
  - – to automatically check the organization's compliance, e.g., according to information security standards (GGSM, CC),
  - – to support the entire information security risk management process.

- Further Work
  - – Case Studies with our partner companies.

© 2004-2008 Secure Business Austria