Ontology- and Bayesian-based Information Security Risk Management

Stefan Fenz
sfenz@securityresearch.at

4th ETSI Security Workshop
13 – 14 January 2009 – ETSI, Sophia Antipolis, France
Motivation

- Almost every business decision is based on electronically stored information
- Information security is crucial for ensuring long-term business success
- Information security risk management is an issue since the 1970s, but still linked to several problems
Abstracting the assessed approaches

- System Characterization
  - Inventory and determination of acceptable risk levels
- Threat and Vulnerability Assessment
  - Determination of potential threats and corresponding vulnerabilities
- Risk Determination
  - Threat Probability x Impact
- Control Identification
  - Identification of risk-reducing controls
- Control Evaluation and Implementation
  - Cost/Benefit analysis
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
RQ: To what extent can the information security domain knowledge, including concepts and relations which are required by common information security risk management methodologies, be modeled formally? Which source can be used to enrich the knowledge model with concrete and widely accepted information security knowledge?
The Security Ontology
top-level concepts and relations

Establishing the Knowledge Base

- Evaluation of common information security standards and best-practice guidelines regarding their acceptance, completeness, availability, and knowledge representation

- Incorporation of the German IT Grundschutz Manual into the security ontology

- Creation of more than 500 concepts and 600 formal axioms

- Reasoning algorithms are used to exploit the formal knowledge base
Reasoning Algorithms - Example

- Up to what extent protect existing control implementations a given asset?

- Protects(x, y) = true if control implementation x protects asset y.

- Therefore, the function reveals concept z which is connected via the sec:vulnerabilityOn relation to the corresponding vulnerability of control implementation x.

- To protect asset y, control implementation x has to be implemented at concept z which is connected depending on the vulnerability type to asset y.

```plaintext
1: A ← given asset
2: IC ← null
3: NC ← null
4: TL ← GetThreats(A)
5: for i ← 0 to TL.Length do
6:   VL ← GetRelated(TL[i], sec:exploits)
7:     for j ← 0 to VL.Length do
8:       CL ← GetRelated(VL[j], sec:mitigatedBy)
9:    for k ← 0 to CL.Length do
10:      IL ← GetRelated(CL[k], sec:implementedBy)
11:        for l ← 0 to IL.Length do
12:          CI ← GetInstances(IL[l])
13:            if CI != null then
14:              for m ← 0 to CL.Length do
15:                if Protects(CI[m], A) == true then
16:                  IC.Add(IL[l], "implemented by: ", CI[m])
17:                else
18:                  NC.Add(IL[l], "not implemented")
19:                end if
20:              end for
21:            else
22:              NC.Add(IL[l], "not implemented")
23:           end if
24:       end for
25:    end for
26: end for
27: PTL ← GetRelated(TL[i], sec:canBeConsequenceOf)
28: for n ← 0 to PTL.Length do
29:   Line 6 to Line 30 with PTL[n] for TL[i]
30: end for
31: end for
32: return IC
33: return NC
```
RQ: To what extent can a formal information security knowledge base be used to calculate threat probabilities, taking the individual security status of the considered organization into account?
Bayesian Threat Probability Determination
Prototypical Implementation
AURUM – Prototype
AURUM – Prototype III
Conclusion

- Incomplete knowledge is one of the main problems in information security risk management

- AURUM enables organizations
  - To automatically map general information security knowledge to their infrastructure
  - To comprehensibly quantify the current security status of their organization
  - To automatically check the organization’s compliance with existing best-practice guidelines and information security standards

- The developed concepts are not limited to the information security domain
Limitations

- We measure what is in fact not measurable
- Bayesian threat probability determination depends on realistic input values which are not always available
- Completeness of the information security knowledge base is not guaranteed
- Inventory of organizational control implementations has not been addressed
Further Research

- Business process integration
- Impact rating
- Usability
- Visualization
- Certification support
- Evaluation methodology
Thank you for your attention

Contact: sfenz@securityresearch.at