Decision Support for Cost-Effective Choice of Security Solution: The AORDD Security Solution Trade-Off Analysis

Siv Hilde Houmb

Department of Computer and Information Science
Norwegian University of Science and Technology, Norway
Service Platforms, Telenor R&I, Norway
(Information Systems, University of Twente, The Netherlands)
sivhoumb@yahoo.com
Outline

• Motivation and context
• Aspect-Oriented Risk Driven Development (AORDD) Framework
• What is a security solution and what is meant by trading off?
• AORDD Security Solution Trade-Off Analysis
• BBN implementation of Security Solution Trade-Off Analysis
• Evaluation plan
Context and Motivation (1)
Context and Motivation (2)

The problem:
• **Balancing** system stakeholders’ goals, end-users’ expectations and contracted level (or expected level) of security is not straightforward
  – Conflicting goals
  – Insufficient information available (uncertainty) related to the security of a future system and the actual effect of various alternative security solutions
  – Cost, TTM and other project or organisational issues directly or indirectly involved

The “solution”:
• Decision **support for choice of security solution** that takes multiple concerns into mind
• Combine disparate information
  – Be able to use **whatever information available** to aid decisions
AORDD Framework

- Aspect repository
- Estimation repository
- BBN-based cost-benefit trade-off analysis
- Rules for how to annotate UML models
- Rules for transferring info to the BBN topology

Security Solution Trade-Off Analysis using BBN for AORDD
What is a security solution?

A security solution is any construct that increases the level of confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and/or reliability of a system or system design. Examples of security solutions are security requirements, security protocols, security procedures, security processes, cryptographic algorithms etc.
What is meant by trading off?

Trade-off is making decisions when each choice has both advantages and disadvantages. In a simple trade-off it may be enough to list each alternative and the pros and cons. For more complicated decisions, list the decision criteria and weight them. Determine how each option rates on each of the decision score and compute a weighted total score for each option. The option with the best score is the preferred option. Decision trees may be used when options have uncertain outcomes.
Security Solution Trade-Off Analysis

Risk level variables
- Misuse impact
- Misuse frequency
- METM
- MTTM

Security solution variables
- Security solution effect
- Security solution cost

Trade-off parameters
- Budget
- Time-To-Market (TTM)
- Security acceptance criteria
- Priorities

Trade-Off Analysis

Security Solution Fitness Score

Security Solution Trade-Off Analysis using BBN for AORDD
BBN Implementation
Bayesian Belief Networks/Nets

• BBN is a powerful tool for reasoning under uncertainty
• In security evaluation reasons for uncertainty could be such as
  – Incomplete understanding of a security problem or the behaviour of a software system (interrelated problems)
  – Incomplete understanding of the system environment
  – Incomplete knowledge of the effect of a security incident
  – Incomplete knowledge of the system’s inherent vulnerabilities
  – Inconsistent information on the behaviour of a system
  – Inconsistent information of the effect that some security mechanism has on the system behaviour
BBN topology
Trade-Off Parameters (TOP) Sub Net

Law and Regulations (LR)
BUSiness Strategy (BS)
STAndards (STA)
Business Goals (BG)
BUudget (BU)
Time-To-Market (TTM)
POLicies (POL)
Sec. risk Accept. Crit. (SAC)

TCP Priorities Utility

<table>
<thead>
<tr>
<th>Node/Variable</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP</td>
<td>BU, TTM, Conf, Integr, Avail, NonR, Accnt, Auth and Relia</td>
</tr>
<tr>
<td>PRI</td>
<td>BU, BG, BS, LR, TTM, SAC, POL</td>
</tr>
<tr>
<td>BU</td>
<td>[min, max]</td>
</tr>
<tr>
<td>TTM</td>
<td>[mindate, maxdate]</td>
</tr>
<tr>
<td>SAC, STA, BG, BS and POL</td>
<td>Conf, Integr, Avail, NonR, Accnt, Auth and Relia</td>
</tr>
</tbody>
</table>
Static Security Level Sub Net
Risk Level (RL) Sub Net

Diagram showing the relationship between Risk Level and other factors such as Misuse Cost (MC), METM, MTTM, Misuse Frequency (MF), and Misuse Impact (MI).
MI and MC Sub Nets
Security Solution TL Sub Net

Security Solution Trade-Off Analysis using BBN for AORDD
SC Sub Net

SC1-Procurement  SC2-Employment  SC3-Maintenance  SC4-Productivity

Solution Cost Utility

Security Solution Cost
Trade-Off Procedure

Security Solution Trade-Off Analysis using BBN for AORDD
Trade-Off Procedure (1)

1. Estimate the input parameters in the set
   \( I=\{MI, MF, MC, SE, SC\} \), where \( MI \) is misuse impact, \( MF \) is misuse frequency, \( MC \) is misuse cost, \( SE \) is security solution effect and \( SC \) is security solution cost

2. Estimate the static security level by combing Asset Value (AS) for the set of assets in the system \( A \) with development related information according to Part 3 of Common Criteria; the security assurance components

3. Estimate the risk level using the prediction model described in Houmb et al. (2005)
4. Estimate the treatment level of the security solution using the prediction model in Houmb et al. (2005)

5. Estimate the trade-off parameters in the set $T = \{SAC, POL, STA, LR, BG, BS, TTM, BU\}$, where $SAC$ is security acceptance criteria, $POL$ is policies, $STA$ is standards, $LR$ is law and regulation, $BG$ is business goal, $BS$ is business strategy, $TTM$ is time-to-market and $BU$ is budget
6. Compute RoSI by
   a) Evaluate “current” security level by combining static security level and risk level
   b) Evaluate the treatment effect of a security solution by looking at how good it treats the risk(s) and by considering the security solution effect and the security solution cost
   c) Compute RoSI by evaluating the result of a) and b) using the trade-off parameters

7. Find the fittest security solution by evaluating RoSI for a particular security solution against the other potential security solutions in the security solution set $S$
Where does the information come from?

• Two main categories of information sources
  – Empirical/Objective/Observable …
  – Subjective

• Two types of information sources
  – Directly observable information sources
    • Information that represent a direct observation of the world and which are relatively close in time
  – Indirectly observable information sources
    • Information from observations done though a simulation of the real world (e.g. experiments), an direct observation done a while back in time, a direct observation of a related phenomenon and information given by a third party
Empirical information sources

- Public available prior experience (repository)
- Company confidential prior experience (repository)
- Domain knowledge
- Recommendation (best practices)
- Standards
- Real-time information sources
  - Honeypots
  - IDS
  - Log-files
Subjective information sources

- Expert judgments
- Expert judgments on prior experience from similar systems
Specify trust context (define the problem in question)

Determine trust hierarchy

Determine IS trustworthiness weight

Compute IS trust score

Derive BBN utilities by combining trust score with evidence
Evaluation Plan

• Evaluation done in two phases

• Phase 1: Example run-throughs and preliminary discussion of scalability, performance, efficiency, feasibility and applicability of the approach

• Phase 2: Case study and evaluation of scalability, performance, efficiency, feasibility and applicability of the approach