Decision Support for Choice of Security Solution: 

The AORDD Framework

Siv Hilde Houmb
Department of Computer and Information Science, NTNU, Norway
Service Platforms, Telenor R&I, Norway
Information Systems, University of Twente, The Netherlands
S.H.Houmb@utwente.nl
Outline

- Context and Motivation
- Problem space
- One possible solution
  - The Aspect-Oriented Risk Driven Development (AORDD) Framework
- Security Solution Trade-off Analysis
- Trade-off tool BBN topology
- Aggregate information as input to the trade-off tool
  - Trust-Based Information Aggregation Schema (TBIAS)
Context and Motivation

Solution 1?
Solution 2?
Solution 3?
Solution 4?
Solution 5?
Solution 6?
What is 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) on the security risks posed upon a system
  – Insufficient information available (uncertainty) on the effect that the security risks have on the system behaviour
  – Insufficient information available (uncertainty) and therefore difficult to estimate the likelihood, impact and cost of security risks (or actually the misuse)
  – Insufficient information available (uncertainty) related to the actual effect of various alternative security solutions and thus the security level of a future system
  – Cost, TTM and other project or organisational constraints
What is Needed?

• Methodology and tool-support that derive a situation where it is clear which security solution is the better one
  – For the particular security risk
  – For the system as a whole
  – For the end-users
  – “Cost-effective”
  – Easy to evolve
  – Easy to maintain

• In other words… *decision support for choice of security solution*
Focus of This Work

RQ.1: How can alternative security solutions be evaluated against each other to identify the most effective alternative?

RQ.2: How can security risk impact and the effect of security solutions be measured?

RQ.3: Which development, project and financial perspectives are relevant for an information system and how can these be represented in the context of identifying the most effective security solution among alternatives?

RQ.4: How can the disparate information involved in RQ1, RQ2 and RQ3 be combined such that the most effective security solution among alternatives can be identified?
Main Contributions

C.1 A set of security risk variables used to measure the impact, frequency and cost of potential undesired events, which in this work is called misuses.

C.2 A set of security solution variables used to measure the treatment effect and cost of alternative security solutions.

C.3 A set of trade-off parameter variables to represent and measure relevant development, project and financial perspectives.

C.4 Methodology and tool-support for comparing the security solution variables with the security risk variables to identify how effective a security solution is in protecting against the relevant undesired behaviour (misuse).

C.5 Methodology and tool-support for trading off security solutions and identifying the best-fitted one based on security, development, project and financial perspectives.
One Possible Solution: The AORDD Framework

AORDD Framework

- Security aspect repository
- Estimation repository
- RDD annotation rules
- AORDD security solution trade-off analysis
- RDD information input rule set
- Trust-based information aggregation schema

AORDD Process

www.ntnu.no
Security Solution Trade-Off Analysis

Risk-driven analysis

- security risk acceptance criteria
- list of security risks in need of treatment
- alternative security solutions
- trade-off parameters
- best “fitted” security solution or set of security solutions
Phase 2: Trade-Off Analysis

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

Trade-off parameters
- Budget
- TTM
- Business goals
- Business strategy
- Security acceptance criteria
- Law and regulation
- Priorities
- Standards

Security solution variables
- Security solution effect
- Security solution cost

Security Solution Fitness Score
BBN Implementation
Trade-Off Tool BBN Topology
Bayesian Belief Networks (BBN)- Reasoning under Uncertainty

• BBN is a powerful tool for reasoning under uncertainty
• In security solution decisions reasons for uncertainty are
  – Incomplete understanding of a security risk or the behaviour of a software system
  – Incomplete understanding of the system (security) environment
  – Incomplete knowledge of the impact of a security risk
  – Incomplete knowledge of the system’s inherent vulnerabilities
  – Inconsistent information on the behaviour of a system
  – Inconsistent information of the effect that a security solution has on the system behaviour
Trade-Off Tool BBN Topology

- Static Security Level
- Risk Level

AND

- “Current” Security Level
- Solution Treatment Level

AND

- Trade-Off Parameters
- Treatment Effect and Cost

AND

- Security Solution Fitness Score

Level 1

- Static Security Level (SSLE)
- Risk Level (RL)

Level 2

- Security Level
- Security Solution Treatment Level (SSTL)
- Trade-Off Parameters (TOP)
- Treatment Effect and Cost
- BUDget (BJ)
- Time-To-Market (TTM)

Level 3

- Fitness Score Utility

Level 4

- Fitness Score
TOP Sub Net

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

<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>
Risk Level (RL) Sub Net

- Misuse Frequency (MF)
- Misuse Impact (MI)
- Misuse Cost (MC)
- Security risk
- Existing safeguards

- Attacker motivation
- Attacker resources
- Attacker skills
- Attacker abilities
- METM
- MTM
- Operational security level

Risk Level Utility

Risk Level
Treatment Level Sub Net
This is all good but…

…where does the information (data/numbers) come from?

…and how to combine them?
Information Sources

• Two main categories of information sources
  – Empirical, historical, “objective” or directly observable and subjective

• Directly observable information sources
  – Information that represent a direct observation of the world or a phenomenon and which are relatively close in time (this includes information from simulation of the real world, such as experiments)

• Subjective information sources
  – Direct observation done a while back in time, a direct observation of a related phenomenon and information given by a third party (expert)
Directly Observable Information Sources

- Public available prior experience (repository)
- Company confidential prior experience (repository)
- Domain knowledge
- Experiments
- Other empirical information
- 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
TBIAS Overview

Step 1
- Trust Context
  - purpose
  - assumptions

Step 2
- Trust relationship between information sources (A)
- Trust relationship between decision maker and information sources (B)

Step 3
- Trust-based performance weighting schema

Step 4
- Apply B on A
- Trust-based IS performance weights

Step 5
- Aggregate information using TBISP weights
- Trust-based Information aggregation
Evaluation Plan

• Phase 1: Example run-throughs and preliminary discussion of the validity, feasibility and applicability of the approach – This work
• Phase 2: Case scenarios and evaluation of the validity, feasibility and applicability of the approach – Current work
• Phase 3: Industrial field trials and evaluation of the validity, feasibility and applicability of the approach – Future work
Concluding Remarks

• The AORDD Security Solution Trade-Off Analysis helps to find the best fitted security solution to a particular security risk (or set)
• The Trust-Based Information Aggregation Schema is a information source ability weighting aggregation approach that support the Trade-Off Tool
• This work has produced a preliminary version (prototype) of both
Future Work

• Investigate the relationship between the variables in the trade-off tool
  – Currently done using expert judgment and industrial experience

• Combine the BBN topology for the trade-off tool and TBIAS
  – Currently the transfer of information between them is a manual task

• Real Option Analysis

• Evaluate using case scenarios

• Prepare the field trials
  – Ongoing work

• Evaluate using field trials