To Invest or Not to Invest?
Assessing the Economic Viability of a Policy and Security Configuration Management Tool

11th Annual Workshop on the Economics of Information Security (WEIS 2012)
Berlin, Germany

Lukas Demetz and Daniel Bachlechner
University of Innsbruck
Austria
Policy and security configuration management

- Organizations face numerous regulatory and contractual requirements they need to comply with
- Expenditures for compliance are increasing, especially for service providers offering services to multiple customers
- Managing requirements and the configuration of IT landscape components is cumbersome and error-prone
- A tool partially automating policy and security configuration management may help to
  - reduce the costs associated with policy and security configuration management
  - increase the trustworthiness through higher levels of security and compliance
PoSecCo – A policy and security configuration management tool

• Aims at policy and security configuration management
• Aims to support reducing costs and increasing trustworthiness
• Establishes link between business requirements and security configuration of IT landscape components
• Can be operated in two modes:
  – Planning mode
  – Running mode
• Offered as a whole
• Ideally run not only at one organization but also at its suppliers and customers to increase overall benefits
Requirements for investment approaches for such a tool

The approach

• *must* support investment decisions regarding security products bought as a whole
• *must* consider financial measures
• *should* consider non-financial measures
• *must* support one-time costs and benefits
• *should* support running costs and benefits
• *must* be applicable without explicitly considering attacks
• *should* consider network effects
Identification of approaches

Unsystematic search using Google Scholar

30 articles

Extract, group, and order keywords

List of keywords

Systematic search using Google Scholar

83 articles

Filtering of articles

11 approaches
## Results

<table>
<thead>
<tr>
<th>Authors</th>
<th>Bought as a whole</th>
<th>Financial</th>
<th>Non-financial</th>
<th>One-time costs</th>
<th>Running costs</th>
<th>Attacks</th>
<th>Network effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gordon &amp; Loeb [1]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mizzi [2]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>~</td>
<td></td>
</tr>
<tr>
<td>Sonnenreich et al. [4]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cremonini &amp; Martini [5]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td></td>
</tr>
<tr>
<td>Huang et al. [6]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tallau et al. [7]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td>~</td>
</tr>
<tr>
<td>Wang et al. [8]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Gordon et al. [9]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Bodin et al. [10]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td>~</td>
</tr>
</tbody>
</table>
Findings and conclusion

• The approaches by Bodin et al. [10] and Tallau et al. [7] at least partially fulfill all requirements defined for a policy and security configuration management tool
• Both are not completely suitable as both are primarily suited for comparative analyses
• These two approaches could be combined with useful features of the other approaches
THANK YOU!
Contact

Lukas Demetz
Lukas.Demetz@uibk.ac.at

University of Innsbruck
School of Management
Information Systems
Universitätsstraße 15
A-6020 Innsbruck
Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129).

http://www.posecco.eu
References


