Incorporating Nontechnical Attributes in Multi-attribute Analysis for Security

Shawn A. Butler
Computer Science Department
Carnegie Mellon University
01-412-628-8101
shawnb@cs.cmu.edu

Mary Shaw
Computer Science Department
Carnegie Mellon University
01-412-628-2589
mary.shaw@cs.cmu.edu

Abstract

The most obvious considerations that affect an organization's choice of security technologies are the threats the organization considers significant and the cost-effectiveness of various security technologies against those threats. In practice, however, the choice is also strongly driven by less tangible, more nontechnical, considerations such as ease of implementation and maintenance, fit with organizational culture, or intuitive appeal to security personnel. We originally designed the Security Attribute Evaluation Method (SAEM) to respond to the former considerations. As SAEM has evolved, its multi-attribute risk elicitation and sensitivity analysis also address the latter considerations by helping security engineers make consistent judgements, focus on the highest points of leverage, and understand the implications of potential changes. As a result, the benefit of the method lies not only in its recommendations, but also in its ability to sharpen the security engineers' understanding of their needs and options.

1. Introduction

In previous Economics-Driven Software Engineering Research workshops we presented preliminary ideas on using decision analytical techniques to help security engineers make security architecture design decisions [1][2]. This led to the Security Attribute Evaluation Method (SAEM), which identifies the most effective security technologies for an organization, given its specific risks [3]. SAEM focused on the technical relations among threats, perceived risks, security technologies, and the cost-effectiveness of the technologies as countermeasures against the significant threats.

As SAEM evolved through several case studies in government and industry projects, it became clear that these technical relations only tell part of the story. The real value of a security technology to an organization involves complex interactions between these technical concerns and implicit, even non-tangible attributes of the technology. Maintainability, cultural impact, and ease of implementation are just a few of the factors that a security engineer considers before selecting a specific security technology. Since these implicit attributes can strongly affect the ability to realize expected security benefit, security engineers need a method that allows them to understand how these factors affect their designs. For example, if the adoption of a security technology requires a significant change in system usability, users often develop work-arounds that usually undermine the technologies' expected effectiveness. This may not be evident in the requirements, the risk analysis, or even the first round of technology selection. It may emerge only during later stages of the analysis, when SAEM finds discrepancies between its recommendations and informed judgements of the security analyst.

Since last year's presentation [2], we have expanded SAEM to include decision support for selecting technologies based on general selection criteria, in addition to effectiveness. The *Benefit Analysis* step in SAEM produces a prioritized list of security technologies. When this prioritized list does not represent the security engineer's preferences overall, then we conduct further analysis to determine the basis for the discrepancies between SAEM results and the security engineer's preferences.

1.1 Extending SAEM for Nontechnical Factors

As part of the *Selection Criteria Analysis*, we use the same multi-attribute analysis techniques as in the *Risk Assessment* and *Benefit Analysis* steps to develop a new ranking of security technologies that include other factors that influence the security component selection. Since the security engineer considers effectiveness when selecting a security technology, we use the results of the *Benefit Analysis* for the *effectiveness* attribute values. In essence, the *Selection Criteria Analysis* step is a multi-attribute analysis that partially relies on input from the *Benefit Analysis* step, which also uses a multi-attribute analysis.

The key to *Selection Criteria Analysis* is using sensitivity analysis to explore discrepancies between the security engineer's overall preferences and analysis results. This sensitivity analysis provides insight into the security engineer's decisions. Discrepancies result for a number of reasons, and sensitivity analysis helps show the security engineer possible causes for these differences. These insights may cause the security engineer to revise his overall preference for specific security technologies or re-evaluate the inputs to the *Selection Criteria Analysis*.

Although it is not surprising that nontechnical factors influence design decisions, it is important to understand how much nontechnical factors affect these decisions. Multi-attribute analysis provides such insight and offers a consistent method for comparing alternative designs. This paper presents the expanded multi-attribute analysis technique used in SAEM, with emphasis on the way it brings nontechnical considerations into the analysis.

1.2 Previous Work

The most notable work using decision theory techniques is in software component reuse evaluation. Kontio [4] successfully used Analytical Hierarchical Process (AHP), an alternative decision analysis technique, to recommend commercial off-the-shelf (COTS) components. Kontio used AHP to compare functionally similar software components. In SAEM, we are evaluating functionally dissimilar components and comparing the results to the security engineer's orderings, pre-SAEM. Background

Security engineers can use SAEM to determine which security technologies will provide the greatest risk mitigation given an organization's expectations about threats and the consequences of successful attacks [3]. SAEM relies on information obtained through interviews, multi-attribute analysis, and sensitivity analysis to help security engineers prioritize security technologies based on effectiveness. However, security engineers consider other factors when actually selecting security technologies for the security architecture. SAEM has four steps (Figure 1). We are concerned here with the Selection Criteria Analysis step, in which SAEM helps security engineers identify and consistently evaluate security technologies based on the effectiveness of the technology and other factors that affect the value of the technology within the organization.

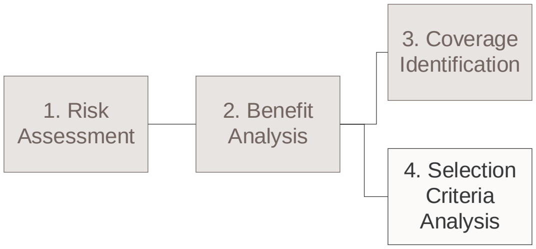

Figure 1 SAEM Steps

Security engineers select specific technologies for different reasons or factors, which vary across organizations. For example, in one of our case studies the security engineer had to ensure that the technology was compatible with the organization's culture and operational processes. The organization was very reluctant to improve security at the cost of changing their business processes. In other case studies, security engineers have been concerned about whether they can adequately maintain the technology, because failure to do so would diminish its effectiveness. An organization may be more willing to adopt a technology that can be maintained using in-house resources rather than out-sourcing support. In fact, the effectiveness of a security technology is often second or third in priority to these other factors. Multi-attribute analysis techniques can show how these other factors influence a security engineer's technology selections.

2. Multi-attribute Analysis for Security Technologies

The *Benefit Analysis* step in SAEM prioritizes security technologies based their expected effectiveness in the organization. At the end of the *Benefit Analysis* step, security engineers use *Selection Criteria Analysis* to evaluate specific security technologies. The *Selection Criteria Analysis* step begins with the security engineer describing which factors he considers when selecting a security technology. Next, the security engineer ranks and weights these factors in relative importance to the organization. The security engineer chooses which security technologies are to be analyzed and assesses each technology a ranking within each selection factor. As in the *Risk Assessment* and *Benefit Analysis* steps in SAEM, this step uses an additive model to rank each technology overall.

2.1 Select Decision Factors

The first step in the selection criteria multi-attribute analysis is to determine which factors the organization considers when deciding whether to adopt a security technology. For example, the security engineer in one case study identified four factors, in addition to effectiveness, which his organization considers when adopting a new security technology into the architecture. These factors were: 1) Purchase Cost, 2) Maintenance, 3) Ease of Implementation, and 4) False Positives.

2.2 Rank Factors

The next step in the multi-attribute analysis is for the security engineer to rank each selection factor. Although security engineers have little difficulty in ranking each selection factor, two interview techniques can facilitate this process. In one, the security engineer places cards annotated with the selection factors on a 0-100 scale drawn out on a large piece of cardboard or whiteboard. In the other, we provide 20 poker chips representing increments of 5 units and ask the security engineer to place the appropriate number of poker chips on each factor. Both methods are cognitively more appealing than simply asked for values, and security mangers are more satisfied with their answers. A security engineer's selection factors, rankings, and weights for one of our case studies are shown in table 1.

Selection Factors	Rank	Weight
Maintenance	100	.31
Purchase Cost	80	.25
Effectiveness	60	.18
Ease of Implementation	30	.09
False Positives	55	.17

Table 1 Selection Factors, Ranks and Weights

In another case study, the organization had information systems in several locations throughout the world and had to be sure that any security technology selected for the architecture was not export restricted and that it could handle the host country's language character set. In addition, the security engineer could not select any security technology that could be perceived to have a significant impact to the organization's business culture. Forcing the organization to change passwords periodically would have a significant impact into how the organization operates on a daily basis. This ability to select which factors are important to each individual organization is one of the advantages of multi-attribute analysis techniques.

2.3 Rate Technologies

The third step in using multi-attribute analysis to prioritize security technologies is to rate each technology in each of the selection factor categories. The best technology in each factor is given 100 points and the other technologies are rated relative to the best. The effectiveness rating is determined using previous steps in SAEM so the 100-point scale is not used, but all ratings are normalized and scaled so that they can be compared. In this example, with the exception of effectiveness, ratings are based on the security engineer's assessment of his organization's ability to maintain and implement the security technologies, and his knowledge about the purchase cost of the technology. Security mangers in other organizations would most likely have different ratings. Table 2 shows the rankings of four security technologies for each selection factor in this case study.

Selection Factors	Host-based IDS	Net-based IDS	Audit Software	Smart Cards
Maintenance	71	80	70	100
Purchase Cost	30	100	100	60
Effectiveness	37	28	35	20
Ease of Implementation	60	100	80	90
False Positives	40	51	40	100

Table 2 Security Technology Ratings

2.4 Overall Ranking

The final step in this multi-attribute analysis is to determine the ranking of each technology using the additive function $Rank_{Security} = \Sigma\, w_f * v(Security_f)$. Although a detailed discussion for using the additive model is beyond the scope of this paper, the additive model allows one to rank each technology (*Security*) based on its normalized rank $v(Security_f)$ weighted w_f by each factor *f*. Table 3 shows the results of each technology and its order.

Security Technology	Overall Rank	Order
Host-based IDS	.293	3
Net-Based IDS	.267	1
Auditing Software	.271	2
Smart Cards	.253	4

Table 3 Overall Rankings and Order

3. Sensitivity Analysis

One of the most important roles for sensitivity analysis is to help explore the discrepancies between the security engineer's pre-SAEM ordering and the ordering produced by the Selection Criteria Analysis. Sensitivity analysis gives the security engineer confidence in the answers, can detect errors made earlier in the process, and uncover actual decision processes. As previously mentioned, before we conduct the Selection Criteria Analysis step, the security engineer orders selected security technologies. We then go through the Selection Criteria Analysis, which also results in an ordering. We compare the ordering and conduct regression analysis to determine which factors are primarily responsible for the SAEM ordering. We review the original input to ensure that the security engineer is confident of the original assessments. If the assessments are revised, the rankings are recalculated. It is through this process that the security engineer gains insight to his decision process.

In this case study, when we first used this multi-attribute analysis technique, the security engineer identified effectiveness as his number one criteria for selecting security technologies. However, the multi-attribute analysis of the selection criteria indicated that effectiveness was not the most important criteria for selecting technologies. The multi-attribute analysis revealed this discrepancy because host-based intrusion detection was the highest rated overall, but the security engineer had prioritized it much lower during his initial preference ordering. After further analysis, the security engineer revised his factor rankings. This ranking change resulted in Host-based IDS falling to number three, which was more consistent with the security engineer's intuitive ranking.

4. Conclusion

Certainly, it is no surprise that security engineers consider implicit factors when actually selecting security technologies. What is noteworthy is the degree to which implicit and nontechnical factors enter into, and may even dominate, a subtle and complex decision about the value of a security technology to an organization.

To provide practical decision guidance, software engineers need systematic ways to evaluate their designs against the rich fabric of an organization's needs and values. Multi-attribute analysis techniques are useful to tease out the factors that matter and provide a mechanism for consistent evaluation of alternatives. The extended SAEM shows how a method that engages the analyst in refining an analysis can elicit and accommodate some of the considerations that may inaccessible to a purely analytic technique.

Acknowledgements

The research reported here has been supported by the Software Engineering Institute, by the National Science Foundation under Grant CCR-0086003 and by the Sloan Software Industry Center at Carnegie Mellon.

5. References

[1] Shawn Butler, Somesh Jha, and Mary Shaw. When Good Models Meet Bad Data: Applying Quantitative Economic Models to Qualitative Engineering Judgments. *Second Workshop on Economics-Driven Software Engineering Research* (EDSER-2), 2000.

[2] Shawn A. Butler. Improving Security Technology Selections with Decision Theory. *Third Workshop on Economics-Driven Software Engineering Research* (EDSER-3), 2001 .

[3] Shawn A. Butler. Security Attribute Evaluation Method, *Proc International Conference on Software Engineering*, May 2002.

[4] Jyrki Kontio. A Case Study in Applying a Systematic Method for COTS Selection. Proc *Eighteenth International Conference on Software Engineering*. 1996