Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Integrating Cost Benefit Analysis And Pareto Optimality In Security Concepts: Case Study Using Simplified Metric

Thomas Termin[a], Dustin Witte[a], Daniel Lichte[b], Kai-Dietrich Wolf[a]

[a]*Institute for Security Systems, University of Wuppertal, Germany*
[b]*Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany*

Keywords: cost-benefit analysis, Pareto Optimality, security mesaures, vulnerability, decision-making, simplified metric

In the complex landscape of security decisions, the balance between costs and benefits is of paramount importance (Ioannidis et al., 2009). This is especially true when looking at longer periods such as 30-40 years, which should be considered for careful critical infrastructure planning (Harnser, 2010). While the calculation of security costs often follows a simple path involving intervals or distributions to deal with uncertainties (Stott et al., 1987), the evaluation of benefits is a challenge that requires an objective assessment of risk mitigation (Witte et al., 2022).

To assess risk mitigation, the dependency of the probability of occurrence (threat x vulnerability) and the impact (I) of potential risks in conjunction with the risk reduction achieved in the intended timeframe via specific security measures must be examined. The epistemic nature of threat probability, due to the hidden motivations of malicious actors and a lack of evidence, makes a probabilistic estimation difficult (Witte et al., 2023). Also impact estimation may be subject to severe uncertainty. These challenges can be addressed, for example, by assuming equal probabilities for all scenarios or by the deliberate weighting of scenarios by critical infrastructure operators. In the latter approach, operators carefully assess the probability and impact of threats over a defined period of time and determine specific protection goals in terms of likelihood of successful attack (vulnerability) for given scenarios.

The degree of fulfillment of the protection goals to be defined by the operator can then be determined by calculating the vulnerability for a selected scenario and configuration of security measures. To carry out further analyses, a corresponding cost approach must be defined for the security measures under consideration. The principle of Pareto optimality, which states that the improvement of one criterion (e.g. vulnerability) comes at the expense of another (e.g. cost), introduces an additional level of decision making here that requires operators to find and select preferred solutions considering multiple criteria (Stiglitz, 1981). This work introduces a simplified vulnerability assessment methodology that includes a scoring-based evaluation of security measures, as proposed by Termin et al. (2023). Based on the quantitative intervention capability metric (ICM) according to Lichte et al. (2016) as a reference, it can be shown that even with a simplified methodology, similar Pareto fronts are determined, which may be used as a basis for the operators' decision (see exemplarily Figure 1).

Our investigation seeks to answer fundamental questions: Can scorings be used, instead of quantitative metrics as the contribution submitted by Witte et al. (2024), to effectively optimize security concepts? Is it possible to establish an accurate Pareto-optimal configuration (in the context of mapping vulnerability x impact) when utilizing scoring-based approaches? The use of simplified metrics proposed in this paper has significant potential for practical application in a complex and uncertain environment. This paper extends the conceptual framework outlined in "On Pareto Optimality in Cost-Effectiveness Analysis of Physical Security Concepts" as submitted by Witte et al. (2024) for the ESREL 2024 Special Session entitled “Cost-Benefit Decisions under Uncertainty”. Furthermore, this contribution explains the boundary conditions under which a scoring model can yield similar results to those obtained through a quantitative approach.

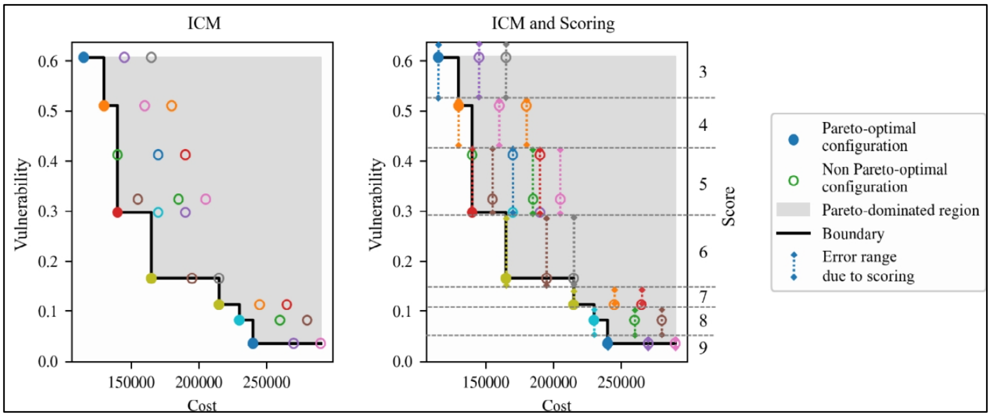

Fig. 1. Cost-vulnerability diagram of security measure configurations according to ICM and a comparison with scoring.

References

Harnser Group. 2010. A Reference Security Management Plan for Energy Infrastructure. European Commission.

Ioannidis, C., Pym, D., Williams J. 2009, February. Investments and trade-offs in the economics of information security. In International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 148-166.

Lichte, D., Marchlewitz, S., Wolf, K.-D. 2016. A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

Stiglitz, J. E. (1981). Pareto optimality and competition. The Journal of Finance, 36(2), 235-251.

Stott, B., Alsac, O., Monticelli, A.J. 1987. Security analysis and optimization. Proceedings of the IEEE, 75(12), 1623-1644.

Termin, T., Lichte, D. Wolf, K.-D. 2023. Risk Adjusting of Scoring-based Metrics in Physical Security Assessment. In: Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023, Southampton, United Kingdom, 03.09. – 08.09.2023).

Witte, D., Lichte, D., Wolf, K.D. 2022. An Approach to the Consideration of Uncertainties in Cost-Benefit Optimal Design of Physical Security Systems.

Witte, D., Lichte, D., Wolf, K.D. 2023. On the Impact of Epistemic Uncertainty in Scenario Likelihood on Security Risk Analysis. In: Proceedings of the 33rd European Safety and Reliability Conference, ESREL 2023, Southampton, United Kingdom, 03-08.09.2023.

Witte, D., Lichte, D., Wolf, K.D. 2024. On Pareto Optimality In Cost-Effectiveness Analysis Of Physical Security Concepts. Extended Abstract Submission. ESREL 2024.