An Approach to Select Cost-Effective Risk Countermeasures

Le Minh Sang Tran[1], Bjørnar Solhaug[2], and Ketil Stølen[2,3]

[1] University of Trento, Italy
[2] SINTEF ICT, Norway
[3] Department of Informatics, University of Oslo, Norway
tran@disi.unitn.it, {bjornar.solhaug,ketil.stolen}@sintef.no

Abstract. Security risk analysis should be conducted regularly to maintain an acceptable level of security. In principle, all risks that are unacceptable according to the predefined criteria should be mitigated. However, risk mitigation comes at a cost, and only the countermeasures that cost-efficiently mitigate risks should be implemented. This paper presents an approach to integrate the countermeasure cost-benefit assessment into the risk analysis and to provide decision makers with the necessary decision support. The approach comes with the necessary modeling support, a calculus for reasoning about the countermeasure cost and effect, as well as means for visualization of the results to aid decision makers.

1 Introduction

Security risk analysis concludes with a set of recommended options for mitigating unacceptable risks [8]. The required level of security and the acceptable level of risk should be defined by the risk criteria. However, deciding which countermeasures to eventually implement depends also on the trade-off between benefit and spending. No matter the criteria and the mitigating effect of the countermeasures, risk mitigation should ensure return on investment in security [2]. Currently there exists little methodic support for systematically capturing and analyzing the necessary information for such decision making as an integrated part of the security risk analysis process.

The contribution of this paper is an approach to integrate the assessment of countermeasures and their cost and effect into the risk analysis process. The approach comes with the necessary modeling support, a calculus for reasoning about risks, countermeasures, costs and effects within the risk models, as well as support for decision making. A formal foundation is provided to ensure rigorous analysis and to prove the soundness of the calculus. The approach is generic in the sense that it can be instantiated by several established risk modeling techniques. The reader is referred to the full technical report [12] for the formal foundation, the soundness proofs and other details. The report demonstrates the instantiation in CORAS [9] with an example from the eHealth domain.

In Section 2 we present our approach, including the method, the modeling support and the analysis techniques. Section 3 gives a small example. Related work is presented in Section 4, before we conclude in Section 5.

L. Wang and B. Shafiq (Eds.): DBSec 2013, LNCS 7964, pp. 266–273, 2013.

2 Our Approach

Our approach (see Fig. 1) takes a risk model resulting from a risk assessment and the associated risk acceptance criteria as input, and delivers a recommended countermeasure alternative as output. Hence, the approach assumes that the risk assessment has already been conducted, *i.e.* that risks have been identified, estimated and evaluated and that the overall risk analysis process is ready to proceed with the risk treatment phase. We moreover assume that the risk analysis process complies with the ISO 31000 risk management standard [8], in which risk countermeasure is the final phase. Our process consists of three main steps.

In Step 1, the risk model is annotated with relevant information including the countermeasures, their cost, their reduction effect (*i.e.* effect on risk value), as well as possible effect dependencies (*i.e.* countervailing effects among countermeasures). In Step 2, we perform countermeasure analysis by enumerating all countermeasure alternatives (*i.e.* combinations of countermeasures to address risks) and reevaluating the risk picture for each alternative. This analysis makes use of the annotated risk model and a calculus for propagating and aggregating the reduction effect and effect dependency along the risk paths of the model. Step 3 performs synergy analysis for selected risks based on decision diagrams. The output is a recommended countermeasure alternative.

Fig. 2 presents the underlying concepts of our approach. A *Risk Model* is a structured way of representing unwanted incidents, their causes and consequences using graphs, trees or block diagrams. An unwanted incident is an event that harms or reduces the value of an asset, and a risk is the likelihood of an unwanted incident and its consequence for a specific asset [8]. A *Countermeasure* mitigates risk by reducing its likelihood and/or consequence. The *Expenditure* includes the expenditure of countermeasure implementation, maintenance and so on for a defined period of time. The *Effects Relation* captures the extent to which a countermeasure mitigates risks. The *Effects Relation* could be the reduction of likelihood, and/or the reduction of consequence of a risk. The *Dependency relation* captures the countervailing effect among countermeasures that must be taken into account in order to understand the combined effect of identified countermeasures. The *Calculus* provides a mechanism to reason about the annotated risk model. Using the *Calculus*, we can perform countermeasure analysis on annotated risk models to calculate the residual risk value for each individual risk. A *Decision Diagram* facilitates the decision making process based on the countermeasure analysis.

As already explained, the input required by our approach is the result of a risk assessment in the form of a risk model, and the corresponding risk

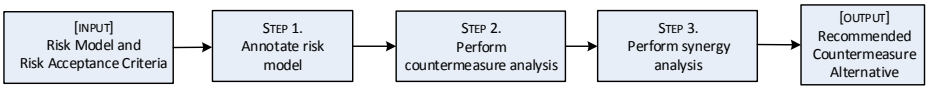


Fig. 1. Three-steps approach

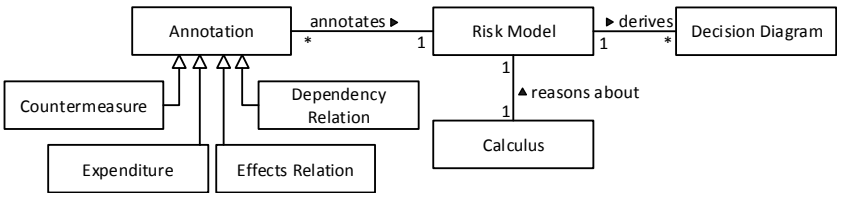


Fig. 2. Conceptual model

acceptance criteria. To ensure that our approach is compatible with established risk modeling techniques, we only require that the risk model can be understood as a risk graph. A risk graph [3] is a common abstraction of several established risk modeling techniques such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Attack Trees, Cause-Consequence Diagrams, Bayesian networks, and CORAS risk diagrams. Hence, our approach complies with these risk modeling techniques, and can be instantiated by them.

A risk graph is a finite set of vertices and relations (see Fig. 3(a)). Each vertex v represents a threat scenario, *i.e.* a sequence of events that may lead to an unwanted incident, and can be assigned a likelihood f, and a consequence co. The likelihood can be either probabilities or frequencies, but here we use only the latter. A *leads-to* relation from v_1 to v_2 means that the former threat scenario may lead to the latter. The positive real numbers decorating the relations capture statistical dependencies between scenarios, such as conditional probabilities.

2.1 Detailing of Step 1 – Annotate Risk Model

This step is to annotate the input risk model with required information for further analysis. There are four types of annotation as follows.

Countermeasures are represented as rectangles. In Fig. 3(b) there is one countermeasure, namely *cm*. An *expenditure* is expressed within square brackets following the countermeasure name (e in Fig. 3(b)). This is an estimation of the expense to ensure the mitigation of countermeasure including the expense of implementation, maintenance, and so on. An *effects relation* is represented by

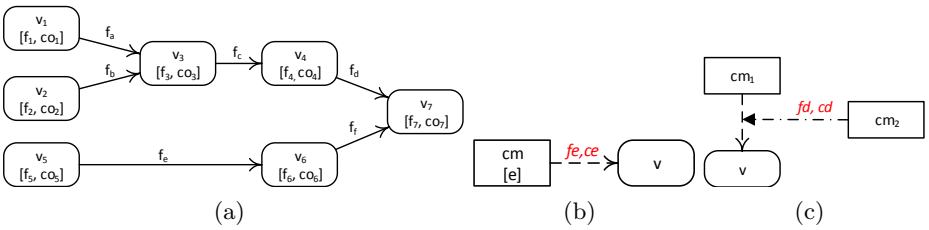


Fig. 3. A risk graph (a) and its extended annotations: Effect relation (b), and Dependency relation (c)

a dashed arrow decorated by two numbers (*fe* and *ce* in Fig. 3(b)). It captures the mitigating effect of a countermeasure in terms of reduced frequency (*i.e. frequency effect - fe*), reduced consequence (*i.e. consequence effect - ce*), or both. Both fe and *ce* are relative percentage values, *i.e.* $fe, ce \in [0, 1]$. A *dependency relation* is represented by a dash-dot arrow with solid arrowhead decorated by two numbers, namely a *frequency dependency - fd* and a *consequence dependency - cd* as illustrated in Fig. 3(c). A dependency relation captures the impact of a countermeasure on the effect of another when both are implemented. In Fig. 3(c) the *fd* impacts *fe* while the *cd* impacts *ce*. Both *fd* and *cd* are relative percentage values, *i.e.* $fd, cd \in [0, 1]$.

2.2 Detailing of Step 2 – Countermeasure Analysis

The countermeasure analysis is conducted for every risk of the annotated risk model. The analysis enumerates all possible countermeasure combinations, called *countermeasure alternatives* (or *alternatives* shortly), and evaluates the residual risk value (*i.e.* residual frequency and consequence value) with respect to each alternative to determine the most effective one. The residual risk value is obtained by propagating the reduction effect along the risk model.

From the leftmost threat scenarios (*i.e.* scenarios that have only outgoing *leads-to* relations), frequencies assigned to threat scenarios are propagated to the right using the formal calculus. The reader is referred to [12] for the full formal calculus and for the soundness proofs. During the propagation, frequencies assigned to *leads-to* relations, reduction effects, and effect dependencies are taken into account. Finally, the propagation stops at the rightmost threat scenarios (*i.e.* scenarios that have only incoming *leads-to* relations). Based on the results from the propagation, the residual risk value is computed.

A *Decision Diagram*, as depicted in Fig. 4 for two different risks, is a directed graph used to visualize the outcome of a countermeasure analysis. A node in the diagram represents a *risk state* which is a triplet of a likelihood, a consequence, and a countermeasure alternative for the risk being analyzed. The frequency and consequence are the X and Y coordinates, respectively, of the node. The countermeasure alternative is annotated on the path from the *initial state* S_0 (representing the situation where no countermeasure has yet been applied). Notice that we ignore all states whose residual risks are greater than those of S_0 since it is useless to implement such countermeasures.

2.3 Detailing of Step 3 – Synergy Analysis

The synergy analysis aims to recommend a cost-effective countermeasure alternative for mitigating all risks. It is based on the decision diagrams of individual risks (generated in Step 2), the risk acceptance criteria, and the overall cost (OC) of each countermeasure alternative. The OC is calculated as follows:

$$\mathrm{OC}(ca) = \sum_{r \in R} \mathrm{rc}(r) + \sum_{cm \in ca} \mathrm{cost}(cm) \tag{1}$$

Here, *ca* is a countermeasure alternative; R is the set of risks; rc() is a function that yields the loss (in monetary value) due to the risk taken as argument (based on its likelihood and consequence); cost() is a function that yields the expenditure of the countermeasure taken as argument.

The synergy analysis is decomposed into the following three substeps:

STEP 3A *Identify countermeasure alternatives:* Identify the set of countermeasure alternatives CA for which all risks are acceptable with respect to the risk acceptance criteria. CA could be identified by exploiting decision diagrams.

STEP 3B *Evaluate countermeasure alternatives:* If there is no countermeasure alternative for which all risks fulfill the risk acceptance criteria ($CA = \emptyset$), do either of the following:

- identify new countermeasures and go to STEP 1, or
- adjust the risk acceptance criteria and go to STEP 3A.

Otherwise, if there is at least one such countermeasure alternative ($CA \neq \emptyset$), calculate the overall cost of each $ca \in CA$.

STEP 3C *Select cost-effective countermeasure alternative:* If there is at least one countermeasure $ca \in CA$ for which OC(ca) is acceptable (for the customer company in question) select the cheapest and terminate the analysis. Otherwise, identify more (cheaper and/or more effective) countermeasures and go to STEP 1.

The above procedure may of course be detailed further based on various heuristics. For example, in many situations, with respect to STEP 3A, if we already know that countermeasure alternative *ca* is contained in CA then we do not have to consider other countermeasure alternatives ca' such that $ca \subseteq ca'$. However, we do not go into these issues here.

3 Example

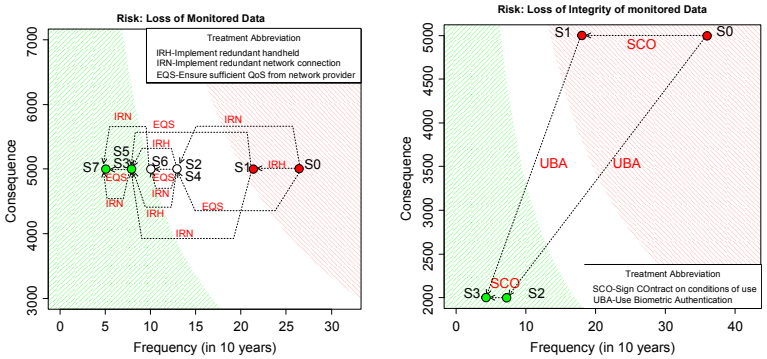
In the following we give a small example of the synergy analysis based on our eHealth assessment [12]. The scenario is on remote patient monitoring, where one of the identified risks is *loss of monitored data* (LMD). Table 1 is input from STEP 2, namely the result of the analysis of seven treatment alternatives given three identified treatments. The corresponding decision diagram is depicted in Fig. 4(a). The shaded area to the lower left are the acceptable risks levels, whereas the upper right are the unacceptable levels. Notice that while the treatment alternatives for LMD reduce only the consequence, some of the alternatives for *loss of integrity of monitored data* (LID) also reduce the frequency.

The results of the synergy analysis of three risks are depicted in Table 2. Their respective treatment alternatives that yield acceptable risk levels are shown in the middle, whereas their combinations are shown in the first column. The third column shows the overall costs as calculated in STEP 3. If also the costs are acceptable, the cheapest alternative should be selected.

Table 1. Analysis for the risk *Loss of monitored data*

Each treatment alternative S is shown in the first column (*Risk State*) followed by its combination of treatments. The *Frequency* column is the number of occurrences in ten years. Both *Frequency* and *Consequence* columns are valued after considering the treatments.

Risk State	Ensure sufficient QoS from network provider	Implement Redundant Network connection	Implement Redundant Handheld	Frequency	Consequence
S0				26.4	5000
S1	•			21.36	5000
S2		•		12.96	5000
S3	•	•		7.92	5000
S4			•	12.96	5000
S5	•		•	7.92	5000
S6		•	•	10.08	5000
S7	•	•	•	5.04	5000



(a) (b)

Fig. 4. Decision diagrams of two risks in the eHealth scenario

4 Related Work

In risk management, decision on different risk mitigation alternatives has been emphasized in many studies [6,10,11]. The guideline in [11] proposes cost-benefit analysis to optimally allocate resources and implement cost-effective controls after identifying all possible countermeasures. This encompasses the determination of the impact of implementing (and not implementing) the mitigations, and the estimated costs of them. Another guideline [6] provides a semi-quantitative risk assessment. The probability and impact of risks are put into categories which are assigned scores. The differences between the total score for all risks before and after any proposed risk reduction strategy relatively show the efficiency among strategies, and effectiveness of their costs. It also suggests that the economic costs for baseline risks should be evaluated. However, the proposed methods for conducting the evaluation have not been designed to assess cost of treatments, but rather cost of risks.

Table 2. Results from synergy analysis of three risks

	Individual Risk			
Treatment Alternative	LID	LMD	DAS	Overall Cost
{UBA,SCO,IRH,IRN,USW}	S3	S3	S3	101740
{UBA,SCO,IRH,IRN,EQS,USW}	S3	S7	S3	102340
{UBA,IRH,IRN,USW}	S2	S3	S3	104500
{UBA,IRH,IRN,EQS,USW}	S2	S7	S3	105100
{UBA,SCO,IRH,IRN}	S3	S3	S2	108740
{UBA,SCO,IRH,IRN,EQS}	S3	S7	S2	109340
{UBA,IRH,IRN}	S2	S3	S2	111500
{UBA,IRH,IRN,EQS}	S2	S7	S2	112100

Norman [10] advocates the use of Decision Matrix to agree on countermeasure alternative. A Decision Matrix is a simple spreadsheet consisting of countermeasures and their mitigated risks. The approach, however, is not clearly defined, and the spreadsheets are complicated to implement and follow. Meanwhile, our proposal is graphical and backed up with a formal definition and reasoning. Butler [4] proposes the Security Attribute Evaluation Method (SAEM) to evaluate alternative security designs in four steps: benefit assessment, threat index evaluation, coverage assessment, and cost analysis. This approach, however, focuses mostly on the consequence of risks rather than cost of countermeasures, whereas our approach captures both.

Chapman and Leng [5] describe a decision methodology to measure the economic performance of risk mitigation alternatives. It focuses on the cost-difference aspect, but does not consider the benefit-difference (*i.e.* level of risks reduced) among alternatives.

Houmb et al. [7] introduce SecInvest, a security investment support framework which derives a security solution fitness score to compare alternatives and decide whether to invest or to take the associated risk. SecInvest relies on a trade-off analysis which employs existing risk assessment techniques. SecInvest ranks alternatives with respect to their cost and effect, trade-off parameters, and investment opportunities. However, this approach does not provide a systematic way to assess the effects of alternatives on risks, and does not take into account the dependency among countermeasures in an alternative.

Beresnevichiene et al. [1] propose a methodology incorporating a multi-attribute utility evaluation and mathematical system modeling to assist decision makers in the investment on security measures. It can be employed in existing risk assessment methods, including ours, to evaluate the residual risk.

5 Conclusion

We have presented an approach to select a cost-effective countermeasure alternative to mitigate risks. The approach requires input in the form of risk models represented as risk graphs. The approach analyses risk countermeasures with respect to different aspects such as the mitigating effect, how countermeasures affect others, and how much countermeasures cost. We have developed a formal

calculus extending the existing calculus for risk graphs. The extended calculus can be used to propagate likelihoods and consequences along risk graphs, thereby facilitating a quantitative countermeasure analysis on individual risks, and a synergy analysis on all the risks. The outcome is a list of countermeasure alternatives quantitatively ranked according to the their overall cost. These alternatives are represented not only in tabular format, but also graphically in the form of decision diagrams. The approach is generic in the sense that it can be instantiated by several existing risk assessment techniques.

Acknowledgments. This work has received funding from the European Commission via the NESSoS NoE (256980) and the RASEN project (316853), and from the Research Council of Norway via the DIAMONDS project (201579/S10).

References

1. Beresnevichiene, Y., Pym, D., Shiu, S.: Decision support for systems security investment. In: Network Operations and Management Symposium Workshops (NOMS 2010), pp. 118–125. IEEE/IFIP (2010)
2. Birch, D.G., McEvoy, N.A.: Risk analysis for information systems. Journal of Information Technology 7, 44–53 (1992)
3. Brændeland, G., Refsdal, A., Stølen, K.: Modular analysis and modelling of risk scenarios with dependencies. J. Syst. Softw. 83(10), 1995–2013 (2010)
4. Butler, S.A.: Security attribute evaluation method: a cost-benefit approach. In: Proceedings of the 24th International Conference on Software Engineering (ICSE 2002), pp. 232–240. ACM (2002)
5. Chapman, R.E., Leng, C.J.: Cost-effective responses to terrorist risks in constructed facilities. Technical report, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (2004)
6. Risk Characterization of Microbiological Hazards in Food: Guidelines. Microbiological Risk Assessment Series No. 17. Food and Agriculture Organization of the United Nations (FAO)/World Health Organization (WHO) (2009)
7. Houmb, S.H., Ray, I., Ray, I.: SecInvest: Balancing security needs with financial and business constraints. In: Dependability and Computer Engineering, pp. 306–328. IGI Global (2012)
8. International Organization for Standardization. ISO 31000 Risk management – Principles and guidelines (2009)
9. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer (2011)
10. Norman, T.L.: Risk Analysis and Security Countermeasure Selection. CRC Press (2010)
11. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, pp. 800–830. NIST Special Publication 800-30 (2002)
12. Tran, L.M.S., Solhaug, B., Stølen, K.: An approach to select cost-effective risk countermeasures exemplified in CORAS. Technical Report A24343, SINTEF ICT (2013)