Multiobjective Decision Support for defining Secure Business Processes

Thomas Neubauer [1)], *Johannes Heurix* [2)]

Abstract:
As business processes gain more importance in todays business environment, their unimpeded execution is crucial for a company's success. Corporate decision makers are faced with a wide spectrum of potential risks on the one hand and a plenitude of security safeguards on the other hand. This paper gives an overview of a new approach for the elicitation of security requirements of business processes, for the analysis of threats and vulnerabilities and for the interactive selection of an optimal security level according to the given business processes as well as multiple objectives. It provides decision makers with an instrument for interactively defining Secure Business Processes that are economically and technically efficient.

1 Introduction

As business processes play a major role in todays companies, Business Process Management (BPM) is applied to "analyze and continually improve business activities [6], or in other words, to engineer lean and streamlined business processes. By introducing BPM, companies can gain several benefits such as cost reduction, quality improvements and error reduction, visibility gain or process automation. While BPM aims at efficiently creating business value, security hazards such as viruses, hacker attacks or data theft pose major threats to the reliable execution of business processes. Given the importance of business process and the fact that they are permanently exposed to numerous threats, the security of business processes is crucial for the business success of an enterprise, because skepticism about the security of a company would nullify the potential advantages of BPM. However, although security is considered being one of the most important issues in corporate environments, many companies are not aware of their level of spending on security and even more important if the investments into security are effective. As security does not directly generate business value and does not directly improve the net profit, investing in security can only prevent negative events or reduce related adverse effects. Dealing with security is often seen as a technical problem and the main focus in literature lies in giving technical solutions to specific security issues. Economic approaches use aggregated values as the Annualized Loss Expectancy (ALE) or Return on Investment (ROI) for choosing security improving measures. Relying solely on a single value for the measurement

[1)]Secure Business Austria, Vienna, Austria, neubauer@securityresearch.ac.at
[2)]Secure Business Austria, Vienna, Austria, heurix@securityresearch.ac.at

of security is inappropriate, because typically there are multiple - often conflicting or mutually affecting - factors that need to be considered, e.g., installation costs and running expenditures, manpower as well as an unimpeded execution of the business process itself (cf. [1, 2] for security specific criteria). By selecting the most appropriate set of measures and, thus, setting the right level of security-investments, decision makers have to take into consideration not only multiple objectives, but different and changing preferences of several stakeholders, the necessity of considering existing business processes, and a cost-efficient usage of the available resources [4]. As a result, decision makers and security experts need to revise methods to secure them against external or internal threats. This paper proposes a new methodology that combines elements of risk assessment for a structured process to measure security requirements with the multiobjective decision making to address multiple relevant factors, workshop techniques to deal with different opinions of different stakeholders, and that uses business process models for eliciting security requirements to account for the process-centered view of todays business activities.

2 A Model-driven Risk-based Decision Making Process

The proposed approach is separated into three phases and incorporates elements of different disciplines and their strengths: (i) a Model-based elicitation process for deriving security relevant entities, such as assets and related vulnerabilities, and threats they are exposed to, (ii) a risk assessment process that provides a structured method for measuring information security risks, (iii) a workshop environment that ensures the consideration of the different opinions and expertise of different participating domain experts, such as security experts, process owners and other stakeholders, and (iv) an interactive decision making process that takes multiple criteria into consideration and provides solutions that represent the best trade-offs of opposed factors.

2.1 Phase 1: Modeling and Identification

The Modeling and Identification phase is tasked with the modeling of business processes and identification and modeling of the entities needed for the risk assessment: Assets, threats, vulnerabilities and possible safeguards. The substeps of this phase can be conducted iteratively, e.g., the Chief Process Officer and the Process Manager devise the process model, identify the assets and figure out the threats, then the security expert adds vulnerabilities and further threats, the CPO adds further assets and the security expert adds corresponding vulnerabilities and so on.

Business Process Modeling: At first, a model (diagram) of the business process under evaluation is defined. The model is either newly constructed or, if already existing, simply imported (e.g., from business process management tools such as Aris or Adonis). As the result

of a minor process improvement or a full scale business process reengineering (BPR) effort, a revised process model can then be analyzed for required safeguards.

Asset Modeling: The next step consists of identifying and modeling all relevant assets that are part of the process represented by the model developed in the previous step. Assets may be tangible or intangible e.g., servers and confidential data. Therefore it may help to develop a hierarchy to display the assets, e.g., categorization into tangible and intangible assets, or external/internal information.

Vulnerability Identification: In this step, all the assets identified in the previous step are analyzed for any possible vulnerabilities. The same vulnerability may apply to multiple assets, e.g., customer data and stock information residing on the same server. Additionally, security properties (CIA) may be assigned to vulnerabilities, if they are needed for the decision process.

Threat Modeling/Identification: After the identification of all applicable vulnerabilities, all possible threats are identified. Existing threat listings may be conferred for a complete and accurate threat list. For modeling, the concepts of Misuse and Abuse Case models (cf. [3, 5]) are adapted: Misuse Case models represent all threats that are the result of misuse of the system by legitimate and authorized persons, e.g., not intended faults, such as mistyped characters, or accidental deletion of important data. Additionally, negative events, that are not directly caused by humans, such as fire or hardware failure, are modeled here as well. Abuse Case models represent all threats that are generated through possible attacks of threat agents, e.g., intended abuse of the system, such as hacker attacks, viruses, worms and others.

Safeguard Identification: The final step of the first phase is the Safeguard Identification process, where all safeguards at disposal are identified. Again, the resulting list may be checked against available safeguard checklists in order to generate a complete enumeration of available security measures.

2.2 Phase 2: Workshop-based Risk Assessment

The aim of this phase is the composition of risks as asset/threat/vulnerability-tuples, the definition of cost/benefit-categories and the assigning of values to the risks and safeguards for each defined category. A difficulty of this step is the often missing quantitative data about risks and/or safeguards, such as rate of occurrence. Therefore, the main source of information is the knowledge of the participating members of this assessment process (e.g., IT/Security Expert, (Chief) Process Owner, members of the upper and lower management).

Composition of Risks: This phase begins with the composition of risks by assigning the previously identified threats to applicable vulnerabilities. As vulnerabilities are related to assets, risks are finally defined as asset/threat/vulnerability-tuples. The next task is to define,

which safeguards address which particular vulnerabilities, and subsequently which risks. Another goal of this substep is to check the list of assets, threats, vulnerabilities and safeguards for completeness. Any additional relevant entity is appended to the list and included in the risk composition. This substep terminates when the participants agree on the completeness and correctness of the risk-tuples and assigned safeguards.

Definition of Cost/Benefit-Categories: This step involves the definition of the cost- and benefit-categories the safeguards are rated against. The careful specification of these categories is of vital importance as these categories should reflect the corporate strategy and security policy of the company. The criteria are company specific and individually customizable, and they can range from monetary quantities (e.g., minimizing the reduction of monetary loss, monetary costs) to intangible values (e.g., user acceptance, implementation hours, loss of reputation).

Quantification of Risks and Safeguards: After defining the cost/benefit-categories, the risks and safeguards are assigned to appropriate quantitative values. As accurate quantitative data is often lacking or incomplete, this methodology relies on the expertise of different stakeholders and their experience to accurately estimate data. Other possible sources of information are any available logs, surveys, standards or other either publicly available or company-owned documents.

Specification of Safeguard Dependencies: The final step of the risk assessment phase includes the specification of any safeguard dependencies and their prerequisites (cannibalism and synergy effects), the definition of any safeguards that must be included (must-haves) and the specification of any already implemented safeguards that have to be kept.

2.3 Phase 3: Multiobjective Decision Support for Safeguard Selection

The third and final phase of the proposed methodology comprises the interactive selection process using the pre-defined cost/benefit-categories as objectives and the information about risks and safeguards, gathered in the preceding phases, as input data.

The first step lies in determining efficient safeguard portfolios by identifying all Pareto-efficient combinations of safeguards (i.e., there is no other solution with equally good or better values in all K objectives and a strictly better value in at least one objective) where the binary variables $x_i \in \{0, 1\}$ indicate whether or not a safeguard i is selected ($x_i = 1$ if so, and $x_i = 0$ otherwise). Of course, all solutions taken into consideration have to be feasible with respect to two sets of constraints. The first set relates to limited resources (e.g., development costs or maintenance costs). The second set ensures that at most a maximum – or at least a minimum – number of safeguards from given subsets (e.g., from a certain type of safeguards

such as firewalls) is included in the feasible solutions. In the second phase, the approach supports decision makers in finally determining the solution that best fits his/her notions out of the possibly several thousand Pareto-efficient alternatives identified in the first step. The approach is based on interactive modifications of lower and upper bounds for one or more objectives. To this end, the decision support system (DSS) starts with displaying K bars. For each objective the system provides information on what can be achieved by (i) the efficient safeguard solutions from solution space and (ii) the subset of solutions that have remained after the decision maker has entered some aspiration levels. After initializing the bars with minimum and maximum objective values taken from the alternative safeguards in solution space, they are intended for restricting the set of remaining solutions in a step-by-step manner (e.g., by raising the minimum bound in one of the objectives) or for expanding it (e.g., by once again relaxing some bounds) according to the decision makers preferences. In all cases, the system provides immediate feedback about the consequences of such choices in terms of intervals for values achievable with the remaining alternatives. Because this setting has filtered primarily those solutions that come with relatively high consumptions of resource category A (such as costs) and high benefits in category A, the options in the other objectives have been reduced as well and the position and size of the "flying" bars representing the updated span for the achievable objective values have changed accordingly (cf. Figure 1). In

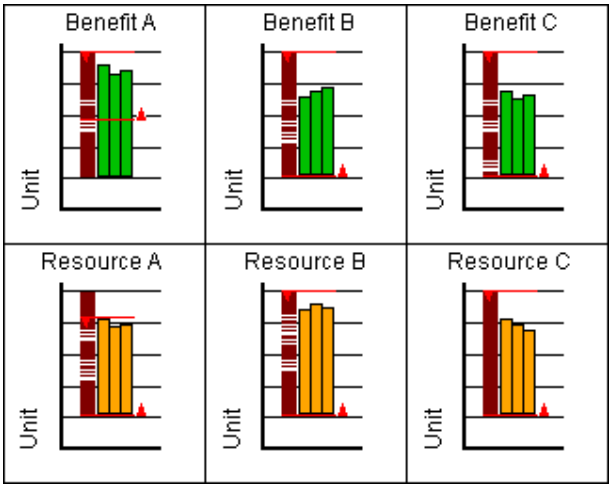

Figure 1: Status of the DSS after two settings

further iterations, the decision maker continues playing with minimum and maximum bounds and by doing so learns about the consequences of his/her decisions and, thus, will get a much better "feeling" for the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives. Ample information on the specific selection problem is provided to him/her and the DSS ensures that the final solution will be an optimal one with no other feasible solution available.

3 Conclusions

This paper proposed a new methodology for the security management of business processes, including the elicitation of security requirements of business process, the analysis of threats and vulnerabilities and the interactive selection of a portfolio of pareto-efficient security safeguards. By using process models as a starting point for a security analysis of business activities, companies may focus on the core processes that are vital for generating business value. The explicit graphical modeling of assets, threats and vulnerabilities supports decision makers in getting an overview of relevant entities. A structured security risk assessment process ensures the consideration of all possible threats and vulnerabilities, as well as the valuable assets. The definition of the risk assessment phase as a workshop allows for multiple persons to participate in the process. This is especially important due to the lack of required data for a formal risk assessment and often the experience and knowledge of domain experts are the only sources of information. The use of a multiobjective decision support method allows to address the multidisciplinary nature of the safeguard selection problem. The whole process can be conducted on a regular basis to reevaluate the current situation of business process security. The tight connection to processes allows the framework to be included in any Business Process Improvement efforts, resulting in an improvement of both economic and security related aspects. As this paper focused on the introduction of this novel approach, further work will concentrate on refining this approach and on conducting case studies.

References

[1] M. D. Abrams and S. Jajodia. *Information Security: An Integrated Collection of Essays*. IEEE Computer Society Press, 1995.

[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 01(1):11–33, 2004.

[3] J. McDermott and C. Fox. Using abuse case models for security requirements analysis. In *Proceedings of the 15th Annual Computer Security Applications Conference, 1999. (ACSAC '99)*, pages 55–64, 6-10 Dec. 1999.

[4] T. Neubauer, M. Klemen, and S. Biffl. Secure Business Process Management: A Roadmap. In *Procs. The First International Conference on Availability, Reliability and Security, 2006. ARES 2006.*, 20-22 April 2006.

[5] G. Sindre and A.L. Opdahl. Eliciting security requirements by misuse cases. In *Proceedings of the 37th International Conference on Technology of Object-Oriented Languages and Systems, 2000. TOOLS-Pacific 2000.*, pp. 120–131, 20-23 Nov. 2000.

[6] M. Zairi. Business process management: a boundaryless approach to modern competitiveness. *Business Process Management*, 3(1):64–80, 1997.