SREBP: Security Requirement Elicitation from Business Processes

Naved Ahmed and Raimundas Matulevičius

Institute of Computer Science, University of Tartu
J. Liivi 2, 50409 Tartu, Estonia
{naved, rma}@ut.ee

In today's fast and dynamic environment, business processes play a crucial role for enterprises to gain competitiveness. The traditional approaches in business process domain tend to focus on business processes execution and their improvement. At the same time business process modelling maturity towards expressing the enterprise's organisational perspective (business values and stakeholders interests) proves huge potential to perform early security analysis in capturing the enterprise' security needs. The phenomenon has been over sighted in business processes and several attempts made to engage the relatively matured security requirements engineering in business processes, either focus on the graphical representation of security aspects in business process models or enforces the security mechanisms or both. However, the security requirement elicitation methods contain a number of limitations [4]. Firstly, security requirements are specified in terms of security architectural design (i.e., security control) and, thus, miss the rationale about the trade-offs of the security decision. Secondly, requirement elicitation is either missing or haphazard. This results in a miss of critical security requirements. And finally, due to the dynamic and complicated nature of business processes the studies only address varying aspects (i.e., authorization, access control, separation of duty or binding of duty) but not the overall security of business processes. These limitations can overcome by eliciting security objectives from the organizational business processes and transform them to security requirements in operational business processes where technology supports the business processes execution.

We propose a two-stage method – Security Requirement Elicitation from Business Processes (SREBP) [1], illustrated in Fig. 1. The method has two-fold advantage: firstly, the security objectives are aligned with the business as they are defined from business processes. They are translated to security requirements that characterise how to execute the business process securely. Secondly, the method has adapted the concepts and activities from existing mature domain of security requirement engineering. This enables an early security analysis and helps elicit security requirements from business processes.

The first stage starts with the analysis of the *value chain*. It helps (*i*) understanding of organisational processes and, thus, (*ii*) determining the business assets. Next, we define the security objectives that must protect these assets against security risks. At the second stage, the information system is divided in to five contextual areas [2]: access control, communication channel, input interface, business service and data store. We define a set of activities to perform

the security assessment with in each contextual area. These activities analyse the business context against an available threat catalogue. The catalogue helps identify the potential vulnerabilities in business processes. Following the domain model of the information system security risk management [3], we elicit the security requirements within each contextual area.

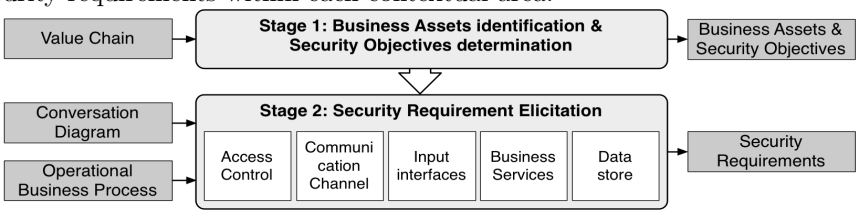

Fig. 1: Security Requirement Elicitation from Business Processes (SREBP)

The contextual area of *Access control* is related to inter- and intra-organisational concerns and specifies the access control policy where roles (individuals, applications or their groups) perform operations and access business asset in the system, to change the state of protected asset. In case of *Communication channel*, one considers how data are exchanged between business partners and system. Here, data need to be protected when they are transmitted over the (untrusted) communication channel. In case of *Input interfaces*, one analyses how input data are treated before accepting them for processing. Here, we identify the input interfaces of the system that receives data from business partners. In case of *Business services*, one needs to protect the enterprise's services, for their availability. Here, we secure the server infrastructure supports the business services. Finally, the *Data store* contextual area concerns data protection when storing or/and retrieving to/from the data store, in case, if the threat agent is capable of accessing the data files directly.

The strength of the SREBP method lies in its general description of security goals, the targeted and systematic analysis of the system contextual areas. In comparison to the other works where the focus is, in majority, placed on representing security requirements, our proposal suggests a novel approach to elicit these requirements and define them as the business rules. The initial validation has shown that the method should be improved with new security risk-oriented patterns. We also plan to extent the method with the requirements prioritisation to support the trade-off analysis.

References

1. Ahmed, N., Matulevičius, R.: A Method for Eliciting Security Requirements from the Business Process Models. In: CAiSE forum (2014), accepted
2. Ahmed, N., Matulevičius, R.: Securing Business Processes using Security Risk-oriented Patterns. Computer Standards & Interfaces 36(4), 723–733 (2014)
3. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Eng., pp. 289–306. Springer (2010)
4. Tøndel, I.A., Jaatun, M.G., Meland, P.H.: Security Requirements for the Rest of Us: A Survey. IEEE Softw. 25(1), 20–27 (2008)