Chapter 42
An Extension of Business Process Model and Notation for Security Risk Management

Olga Altuhhov
University of Tartu, Estonia

Raimundas Matulevičius
University of Tartu, Estonia

Naved Ahmed
University of Tartu, Estonia

ABSTRACT

Business process modelling is one of the major aspects in the modern information system development. Recently business process model and notation (BPMN) has become a standard technique to support this activity. Typically the BPMN notations are used to understand enterprise's business processes. However, limited work exists regarding how security concerns are addressed during the management of the business processes. This is a problem, since both business processes and security should be understood in parallel to support a development of the secure information systems. In the previous work we have analysed BPMN with respect to the domain model of the IS security risk management (ISSRM) and showed how the language constructs could be aligned to the concepts of the ISSRM domain model. In this paper the authors propose the BPMN extensions for security risk management based on the BPMN alignment to the ISSRM concepts. We illustrate how the extended BPMN could express assets, risks and risk treatment on few running examples related to the Internet store regarding the asset confidentiality, integrity and availability. Our proposal would allow system analysts to understand how to develop security requirements to secure important assets defined through business processes. The paper opens the possibility for business and security model interoperability and the model transformation between several modelling approaches (if these both are aligned to the ISSRM domain model).

DOI: 10.4018/978-1-4666-8111-8.ch042

INTRODUCTION

Business process modelling takes an important part when developing Information Systems (IS). It helps specify standard and optimised workflows of organisation. The business processes that involve many participants, their communications, necessary resources and their usage not only extend organisational competiveness but also increase business vulnerabilities. Thus, understanding and modelling of IS security becomes an important activity during IS development. Security refers to the capability of a product, i.e., IS, to protect data and information against the unauthorised access by persons or systems that have intention to harm it.

Identification of the security requirements is typically performed only after the business process has been defined. Furthermore, Jurjens (2005) observes that security considerations often arise most usually during *implementation* or *maintenance* stages. Firstly, this means that security engineers get little feedback about the need for system security. Secondly, security risks are very hard to calculate: security-critical systems are characterised by the fact that the occurrence of a successful attack at one point in time on a given system increases the likelihood that the attack will be launched subsequently at another system point. This is a serious hindrance to secure system development, since the early consideration of security (e.g., when defining the business processes) allows engineers to envisage threats, their consequences and design countermeasures. Then the system design and architecture alternatives, that do not offer a sufficient security level, could be discarded.

Although there exists few attempts to introduce notations to address security at the business process modelling (Menzel *et al.*, 2009; Rodríguez *et al.,* 2007a, 2007b), information assurance and security (Cherdantseva *et al.*, 2012) or to relate business process and security requirements modelling (Paja *et al.,* 2012), these are rather at the coarse-grained level. In principle, the approaches do not illustrate guidelines on how to advance from one security aspect to another, or how to understand security concerns and define security requirements.

In this work we consider Business Process Model and Notation (BPMN, version 2.0) (Remco *et al.*, 2007; Silver, 2009), a multi-vendor standard controlled by the Object Management Group (White, 2004). The primary purpose of BPMN is modelling of the business processes. Like in other modelling languages, BPMN notations are linked to a semantic model, which means that each shape has a specific meaning, and defined rules to connect objects. This paper is an extension of our previous report (Altuhhova *et al*., 2012), where we have selected a domain model (Mayer, 2009; Dubois *et al.*, 2010) for IS Security Risk Management (ISSRM) and aligned the BPMN constructs to the concepts of this domain model. We have resulted in a grounded and fine-grained reasoning for extensions of BPMN toward secure business processes. Based on this alignment, in this paper we introduce a set of security risk-oriented extensions for BPMN. In this paper our goal is to illustrate (*i*) how business activities expressed using BPMN could be annotated with the security concerns; (*ii*) how BPMN could be used to define security requirements; and (*iii*) how the BPMN language itself could be used to reason for the security requirements through illustration of the potential security risks. We result in the security risk-aware BPMN, which could be used to express secure business assets, potential security risks, and their countermeasures. We illustrate our analysis and proposal through few running examples regarding the asset *confidentiality*, *integrity* and *availability*. In this way we end up with guidelines for the BPMN application to analyse security risks.

The paper structure is as follows: firstly, we give the background to our study. Next, we present concrete and abstract syntax of the proposed BPMN security extensions, and illustrate them through confidentiality, integrity and availability analysis in the Internet store example. Then we discuss threats to validity, overview the related work, and conclude the study.