University of Tartu

Faculty of Mathematics and Computer Sciences

Computer Sciences Institute

Information Technology

Olga Altuhhova

Developing System Security through Business Process Modelling

Bachelor's thesis

Supervisor: Raimundas Matulevičius

Author: ..... "....." June 2012

Supervisor: ..... "....." June 2012

Allow to defence

Professor: ..... "....." June 2012

Tartu 2012

Abstract

Business process modelling is one of the major aspects in the modern system development. Recently business process model and notation (BPMN) has become a standard technique to support this activity. Although BPMN is a good approach to understand business processes, there is a limited work to understand how it could deal with business security and security risk management. This is a problem, since both business processes and security concerns should be understood in parallel to support a development of the secure systems. In this paper we analyse BPMN with respect to the domain model of the IS security risk management (ISSRM). We apply a structured approach to understand key aspects of BPMN and how modeller could express secure assets, risks and risk treatment using BPMN. We align the main BPMN constructs with the key concepts of the ISSRM domain model. We show applicability of our approach on a running example related to the Internet store. Our proposal would allow system analysts to understand how to develop security requirements to secure important assets defined through business processes. In addition we open a possibility for the business and security model interoperability and the model transformation between several modelling approaches (if these both are aligned to the ISSRM domain model).

Content

Content of Figures

Content of Tables

Chapter 1. Introduction

1.1 Motivation

Security is a major aspect of Information System development that affects each component of the system very closely. We can claim that the process of security integration into the information systems is not completely and appropriately understood, otherwise there won't exist a necessity in analysing and designing new methodologies and tools. The concept of security itself refers to the capability of a product, information system in our case, to protect information and data in order to avoid the accessibility of it by unauthorized persons or systems that are able to read or modify it. One of the important component of IS development is Business process understanding and modelling. It helps us effectively analysing the needs of providing software and services that become considerable and practical for the demands of any kind of business nowadays. So the actual challenge remains to create business processes with respect to security of the system being described.

1.2 Scope

The great variety of business process modelling approaches was developed in order to optimize business processes and to meet its business goals. Some of them are EPC, YAWL, and UML activity diagrams. The short description of each is presented below.

An Event-driven Process Chain (EPC) is a type of flowchart that is used for business process improvement and also for laying out business process work flows, originally in conjunction with SAP R/3 modelling. The EPC is a base of the ARIS-framework and combines the different views towards the description of enterprises and information systems in the control view on the conceptual level (Seel et al., 2005).

Another representative of the business process modelling tools is YAWL, Yet Another Workflow Language, which is java-based open-source workflow system. Funded on a concise and powerful modelling language, YAWL is able to support complex data, integration with organizational resources and external applications, process verification and process configuration. It has open interfaces based on Web standards that enable to plug-in existing applications and to extend the system. It also provides a graphical editor with built-in verification functionality that helps to detect errors automatically on early stages (Aalst et al., 2005).

The most common and typical tool for business process modelling is UML activity diagrams. The standardized general-purpose modelling language, UML, uses activity diagrams to model the workflow behind the system being designed. An activity diagram is a flowchart which shows the flow of control between the sequential activities of a process (Börger et al., 2000).

For this analytical work we choose quite young modelling notation BPMN, which is becoming a standard that has been developed by Business Process Management Initiative in year 2004 (White, 2004). Although the BPMN, which stands for Business Process Modelling Notation, is a comparatively new methodology, it gained a respectable place among the business process

modelling languages. Because BPMN is a standard and thanks to it's similarity to flowcharting notations, it is friendly and familiar to business users. Each shape has a defined meaning, confined with rules that precisely dictate what can be connected to what. That means diagrams that you create will be completely understandable to other users from any business companies. Moreover, BPMN specifies the technical details that can be attached to any shape, details that make the model executive as an automated workflow. Nowadays BPMN provides language that describes process behaviour, shareable by business and IT; "We've never had that before" (Silver, 2009).

1.3 Problem Description

Identification of the security requirements is typically performed only after the business process has been defined. Furthermore, it is observed that security considerations often arise most usually during *implementation* or *maintenance* stages (Jürjens, 2005). 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, for example Menzel et al., (2009), Rodríguez et al., (2007a), Rodríguez et al., (2007b), or to relate business process and security requirements modelling, for example 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.

1.4 Purpose and Research Question

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. In this work our goal is *not* to develop new modelling approach for security, but rather to understand (*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. In this paper we specifically address the second (*ii*) and third (*iii*) aspect.

1.5 Short Overview of Contribution

To achieve our goal we have selected a domain model (Dubois et al., 2010; Mayer, 2009) for IS security risk management (ISSRM) and have aligned the BPMN constructs to the concepts of this domain model.

During the analysis we apply a structures approach to understand key aspects of BPMN and how modeller could express secured assets, risks and risk treatment using BPMN. Thus in this way we align the main constructs of the BPMN language with the key concepts of the ISSRM domain model. We result in a grounded and fine-grained reasoning for extensions of BPMN toward secure business processes. In addition we extend BPMN with the principles to model and manage security risks. We show applicability of our approach on few illustrate examples (e.g., Internet store). We believe that our proposal will allow system analysts to understand both business processes and security concerns using the same modelling language (thus removing the necessity of learning several modelling languages). In addition we open the possibility for the business and security model interoperability and the model transformation between several modelling approaches (if these are also considered using the ISSRM domain model).

1.6 Structure of the Thesis

Current work consists of five logical parts, divided into six chapters. Chapter 1 is introductive, it makes a short overview of a thesis, scope of our work and problem domain. Chapters 2 and 3 is a background of a thesis; it consist of description of Information System Security Risk Management, or ISSRM, and the latter is dedicated to Business process modelling notation or BPMN, which is taken as a basis for current work. In Chapter 4 we make an analysis of adopting the BPMN to ISSRM, using the running example. Chapter 5 is mapping and the summary of the results into. Chapter 6 represents problems that we faced with during the modelling of the example with a focus on security, and some proposals for language extensions.

Chapter 2. Information System Security Risk Management

Information System Security Risk Management (ISSRM) is practitioner-oriented methodological tool that helps organizations make decisions related to the security of Information Systems (Dubois et al., 2010). Today there exists hundreds of ISSRM methods and standards, which mainly consist of process guidelines to identify vulnerable assets, determine security objects, risks, define and implement security requirements for risk treatment.

2.1 Scope and Basic Definitions

The ISSRM approach used in this work focuses on security risk management. The goal of using the ISSRM approach is to protect organization's assets. *Asset* is defined as anything that has value to the organization, and has a need in protection. Assets, related to the organization information system, such as people, machines, processes, data, software and similar will be taken into account as well. All the risks that threaten to above-mentioned subjects have to be evaluated with respect to three main properties: *confidentiality* – means that information can't be or become available to any unauthorized individuals or processes, *integrity* – the property of protection the accuracy and completeness of secure assets, *availability* – corresponds for accessibility in usage upon demand of authorized individual or entity. Other criteria like accountability, authenticity can be added according to the context requirements.

2.2 Domain Model

Since the ISSRM domain model (Dubois et al., 2010; Mayer, 2009) (shown in Fig. 1) is an important artefact to analyse BPMN in this paper, we will briefly introduce its major concepts.

Assets-related concepts describe organisation's assets and their security criteria. Here, an *asset* is anything that is valuable and plays a vital role to accomplish organisation's objectives. A *business asset* describes the information, processes, capabilities and skills essential to the business and its core mission. An *IS asset* is the IS component, valuable to the organisation since it supports business assets. A *security criterion* is the property or constraint on business assets describing their security needs, which are, typically, expressed through *confidentiality*, *integrity* and *availability.*

Risk-related concepts introduce a risk definition. A *risk* is composed of a threat with one or more vulnerabilities that leads to a negative impact on one or more assets by harming them. An *impact* is the consequences of an event that negates the security criterion defined for business assets in order to harm assets. An *event* is an aggregation of threat and one or more vulnerabilities. A *vulnerability* is the characteristics of IS assets that expose weakness or flaw. A *threat* is an incident initiated by a threat agent using attack method to target one or more IS assets by exploiting their vulnerabilities. A *threat agent* is an agent who has means to harm intentionally IS assets. An *attack method* is a standard means by which a threat agent executes threat.

Risk-treatment related concepts describe the concepts to treat risk. A *risk treatment* is a decision (e.g., *avoidance*, *reduction*, *retention*, or *transfer*) to treat the identified risk. A *security*

requirement is the refinement of a risk treatment decision to mitigate the risks. A *control* designates a means to improve the security by implementing the security requirements.

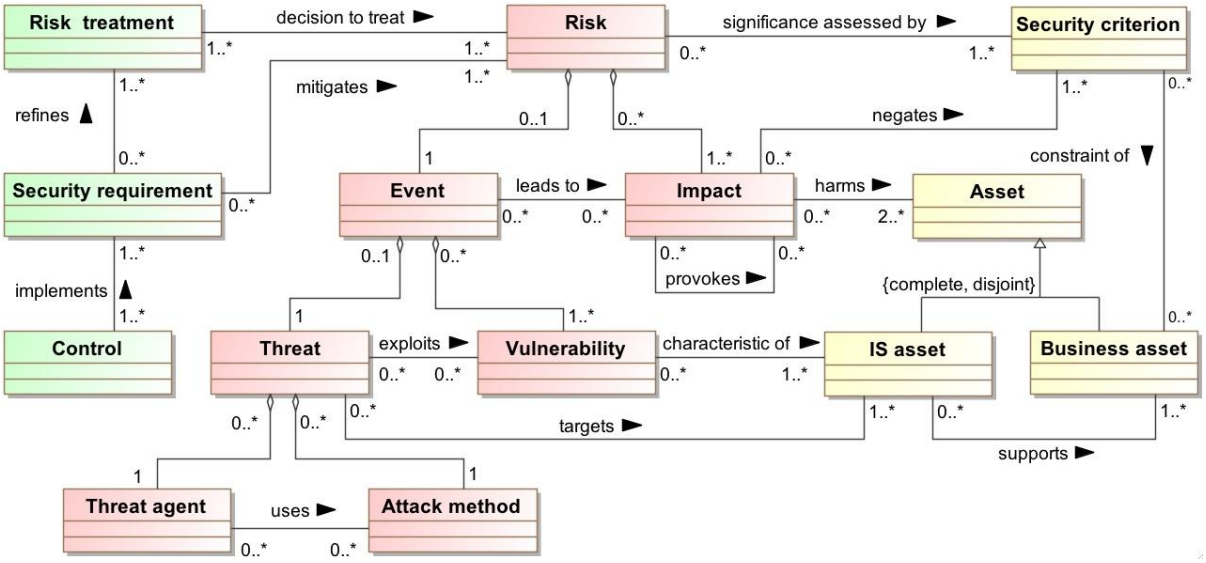

Fig. 1 The ISSRM Domain Model; adapted from (Dubois et al., 2010)

2.3 Application Guidelines

The ISSRM application follows the general risk management process (See Fig. 2). It is an iterative process consisting six steps. Firstly, a developer needs to *define the organisational context and assets* that needs to be secured. Then, one *determines security objectives* (e.g., *confidentia-lity*, *integrity*, and *availability*) based on the level of protection required for the identified assets. Next, *risk analysis and assessment* help identify potential risks and their impacts. Once risk assessment is performed *risk treatment decision* should be taken. This would result in *security requirements definition*. Security requirements are *implemented* into *security controls*. The risk management process is iterative, because new security controls might open the possibility for new (not yet determined) security risks.

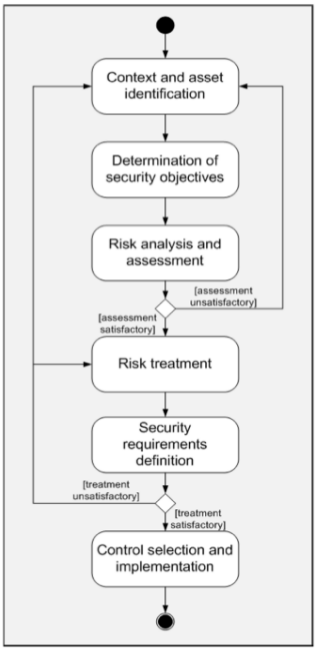

Fig. 2 ISSRM Process, adapted from (Matulevičius et al., 2008a)

2.4 Summary

In this chapter we make an overview of basic definitions of the ISSRM approach, its domain model and the process of risk management. We defined the scope of ISSRM application, and the fact that we are focusing only on security risk management. With the help of conceptual model we present three principal groups of ISSRM concepts: *asset-related* concepts, *risk-related* concepts and *risk-treatment related* concepts. And we also introduce the ISSRM process that describes steps to be taken to manage the security risks. This process includes context and asset identification, determination of security objectives, risk analysis and assessment, risk treatment, security requirements engineering and implementation of selected control measures.

Chapter 3. Business Process Modelling Notation

Business Process Modelling Notation (BPMN) is a language for constructing business process models (White, 2004). It considered being business-friendly, because it is based on notions familiar from traditional flowcharting. At the same time, the notations are linked to a semantic model, which means that each shape used in the notation has a specific meaning, with defined rules and connections between objects. The key element of BPMN application is the Business Process Diagram. It is constructed of a set of graphical elements that were chosen to be distinguishable from each other and to utilize shapes that are familiar to most modellers. It describes a typical order of activities and what role or organizational unit performs or is responsible for the process.

As a part of pedagogical approach, BPMN is classified to three levels, based on how the model is used (Silver, 2009). *Descriptive modelling* describes the typical order of activities and what role or organizational unit each one performs, or responsible for. *Analytical modelling* describes the activity flow precisely, including the exception paths significant to key performance indicators. *Executable modelling* targeted to the system developing, not business architecture or analysis. The scope of this work is limited with the *Descriptive modelling*. It concentrates on business-oriented process mapping by simply documenting what the flow is.

3.1 Introduction to BPMN through Example

We make the short introduction into BPMN through the order making, execution, and product delivery process in the Internet store (See Fig.3) as an example. There are four participants involved in this communication, they are represented with a help of *pools* User, Internet store, Factory and Bank. The reader can also notice that the pool named Internet Store, which is a main container of a process, is divided into three *lanes*: it is done in order to organize flow elements belonging to different store departments. The process starts with a *message triggered start event*, and continues the flow with a *task* Receive request. The next *task* represents the action of user identification (*task* Identify user), which requires the connection to the system Database in order to check necessary information. The check is performed with a *gateway* Identified?: if the user identification failed, the process is leaded to the *end event* with a sign of *terminal signal* inside, which doesn't mean the end of a *parent process*, but the end of a *sub-process.* If the user is successfully identified, process continues with a *sequence flow* and leads to the entering of order data into the system (see *task* Enter order). It is a point where main process flow forks into two parallel going sub-processes: checking the product availability and the finance control. The system checks the product availability in-store (see *task* Check product availability), if it is not available (see *gateway* In-store available?), it offers User to order needed product from factory (see *task* Order from factory), sending a request for confirmation. This activity uses a *message flow* (see Confirmation request and Response), which helps to organize the communication between participants. If the product is not in the store (see the BPMN *gateway* In-store available?), it is ordered from the factory (*task* Order from factory); otherwise the product is prepared for delivery (*task* Prepare product for delivery) and waiting for confirmation from finance control. If the answer is positive, order can be closed and product -

delivered (task Close and deliver). The second flow from the finance control leads to failure and process ends with order cancellation (end event Financing failed)

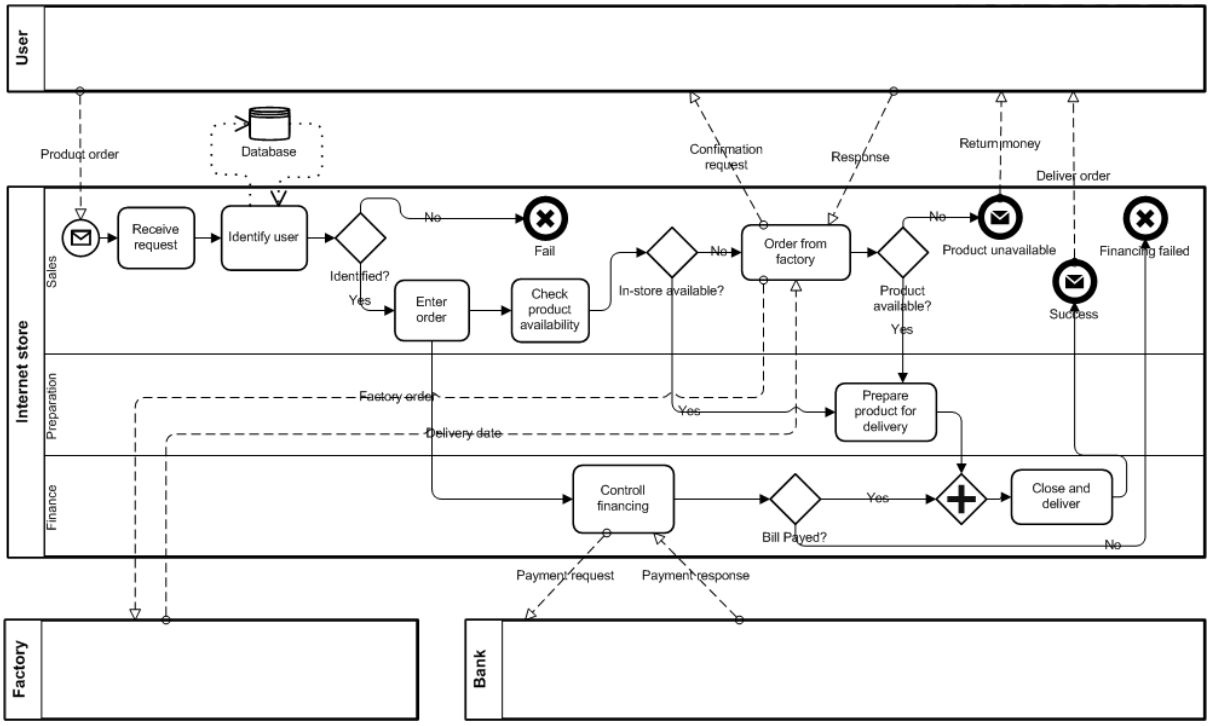

Fig. 3 The BPMN Example: Internet Store

3.2 Major Constructs and Concepts

The four basic categories of objects are *flow objects*, *containers*, *flows* and *artefacts* (See concrete syntax of basic constructs in Fig.4). The *flow objects,* used to describe the atomic units of a process, are *events*, *tasks* and *gateways*. An *event* indicates *start* or *end* of a process path; it can be *triggered* or *non-triggered* (it means an activity that executes or finishes the event; e.g. message, timer, error etc). A *task* is an atomic activity that has no internal sub-parts defined by the model. In some cases, task can also represent the *sub-process*, a compound activity with sub-parts then the task figure is labelled with a small plus on the bottom, which identifies collapsed process. The control of the divergence and convergence of sequence flow is realised by the *gateways*. The *gateway* determines traditional decisions, as well as forking, merging, and joining of paths. We can define some types of *gateways*. An *exclusive gateway* or *XOR gateway* represents an exclusive decision, which means only one of the output *sequence flows* to be followed, based on some condition; *parallel gateway* signifies a parallel split or AND-split, means that all of the outgoing *sequence flows* are to be followed in parallel, unconditionally.

The BPMN *containers* are *pools* and *lanes*. They both play roles of object holders. However, the *pool* shows the message flow between the process and external participants. The *lane* is a subdivision of a process, used to organize flow elements belonging to different categories, also represent performer roles or organizational units.

Relationships between different BPMN constructs are defined with *flows*, which include *sequence flow*, *message flow* and *associations*. The *sequence flow* links *activities*, *gateways*, and *events* within a single *pool*; it is represented by a solid line connector. The *message flow* is a dashed connector representing a signal sent between two *pools*. *Association* is used to associate *data*, *text*, and other *artefacts* with *flow objects*, represented with the help of dotted line connector.

The last group of graphical objects in BP diagrams is *artefacts*. The BPMN *artefacts* contain concepts of *data objects*, which are defined as mechanism to show how data is required or produced by *activities*, data stores and *annotations*. *Data stores* describe the way data could be stored. *Annotations* suggest mechanism to provide additional text information for the user of a *BP Diagram*.

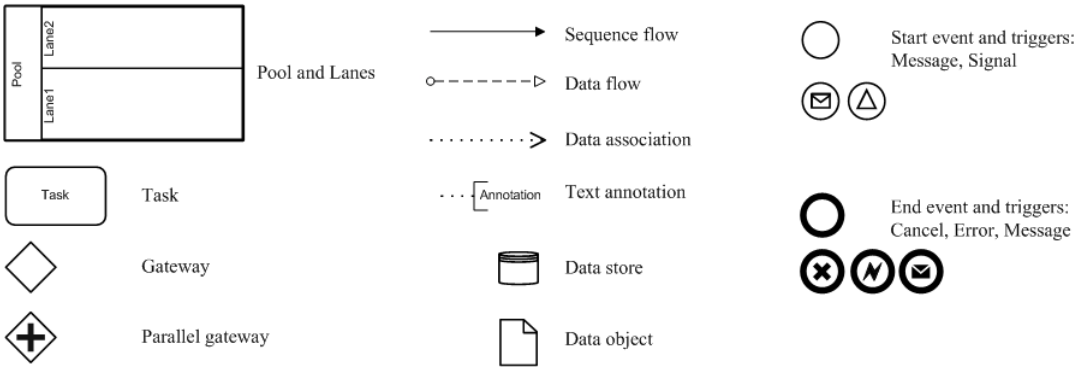

Fig. 4 BPMN Concrete Syntax (*Descriptive Modelling*)

3.3 BPMN Meta-model

Figures below (See Fig.5 and Fig.6) represent BPMN conceptual meta-model. As it was mentioned in previous paragraph, BPMN includes four major categories of constructs (Fig. 5): *flow objects*, *containers*, *flows* and *artefacts*. The *flow objects* describe the atomic units of a process using *events*, *tasks* and *gateways*. An *event* indicates *start* or *end* of a process path; it can be *triggered* or *non-triggered*. A *task* is an atomic activity that has no internal sub-parts defined by the model. In some cases, the *task* can also represent the sub-process, a compound activity with sub-parts. The control of the divergence and convergence of sequence flows is realised by the *gateways*. The BPMN *containers* are *pools* and *lanes*. They both play a role of object holders. However, the *pool* shows the message flow between the process and external participants. The *lane* is a subdivision of a process used to organise flow elements belonging to different categories, and also represents a performer role or an organisational unit. The BPMN *artefacts* include such constructs as *data objects*, *data stores* and *annotations*. *Data objects* define what data is required or produced by activities. *Data stores* describe how data are stored.

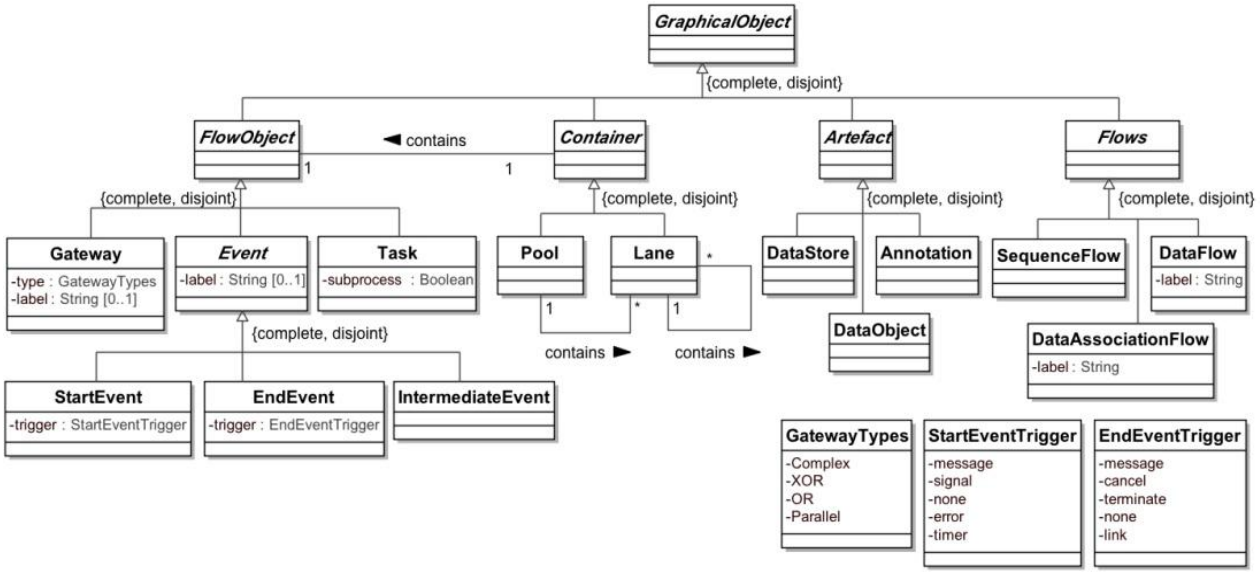

Fig. 5 The BPMN Abstract Syntax: Concept Classification

Relationships (Fig. 6) between different BPMN constructs are defined using *flows*, which include *sequence flows*, *data flows*, and *data association flows*. For instance, the *sequence flows* link together the BPMN activities, gateways, and events within a single pool. The *data flows* show the input/output between pools. Finally, the *data association flows* link together the BPMN tasks and artefacts (i.e., data objects, data stores, and annotations).

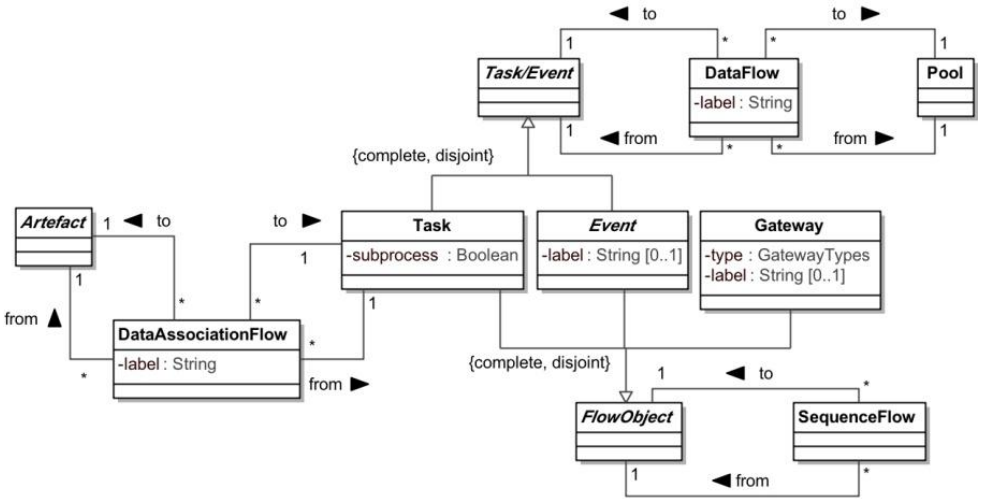

Fig. 6 The BPMN Abstract Syntax: Relationships[1]

[1] Here we do not define the explicit integrity constraints of the abstract syntax. But these exist, especially, to strengthen the flow relationships. For instance, the data association flow could only be defines between the artefacts and task; the data flow could only be defined between the pool and task/event, and similar.

3.4 Summary

This chapter is dedicated to Business Process Modelling Notation, language for constructing business process models. We defined the scope of analysis, concentrating on *Descriptive models*, the first level of BPMN modelling. We made the short introduction to BPMN using example, created with BPMN version 2.0, which represents the main activities in the Internet store: order making, order execution, product delivery. In paragraph 3.2 we collected together major BPMN concepts and constructs. The connections and relationships between them are represented in Fig.5 and Fig.6, in BPMN meta-model.

Chapter 4. Analysis

In this section we will follow the ISSRM process to investigate security risks in a running example modelled using BPMN. We will show which BPMN constructs could be used to address concepts of the ISSRM domain model. Our running example is an *online registration process of the Internet store*.

4.1 Context and Asset Identification

Let's consider the following situation where the potential User (*pool* User in Fig. 7) wishes to start using the Internet store system (*pool* System). In order to get registration details, user sends a message with an inquiry to the system administrator. After the message is accepted (*task* Accept message) and read (*task* Read message) by the administrator, the guidelines (*data flow* Demand for registration) are sent (*task* Send answer) back to the user.

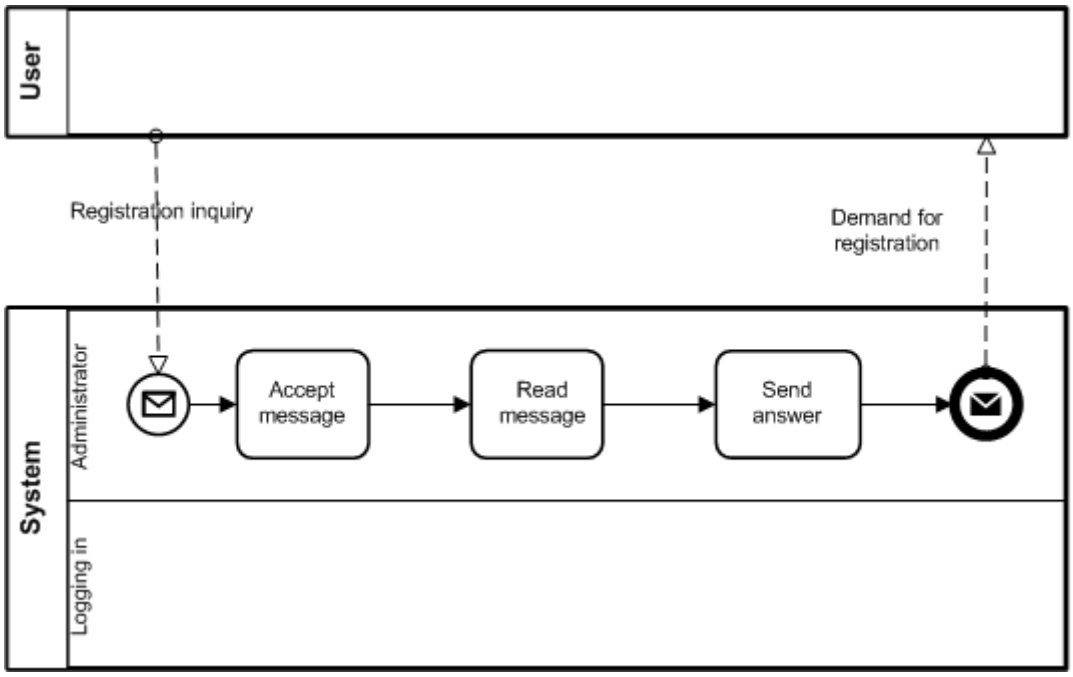

Fig. 7 Message Handling Process

In Fig. 8 we present a user registration process. After receiving the guidelines, the user registers to the Internet store by submitting his data (*data flow* User info). The system, then, accepts registration information (which includes data on the preferred Username and Password) and includes it into the database (*task* Insert data to DB). After registering the valid Username and Password, the user is able to login to the system. The system checks the username and the password. If these match, the user gets the acknowledgement about registration success and is able to use the Internet store system. Otherwise the user gets a notification about the failure.

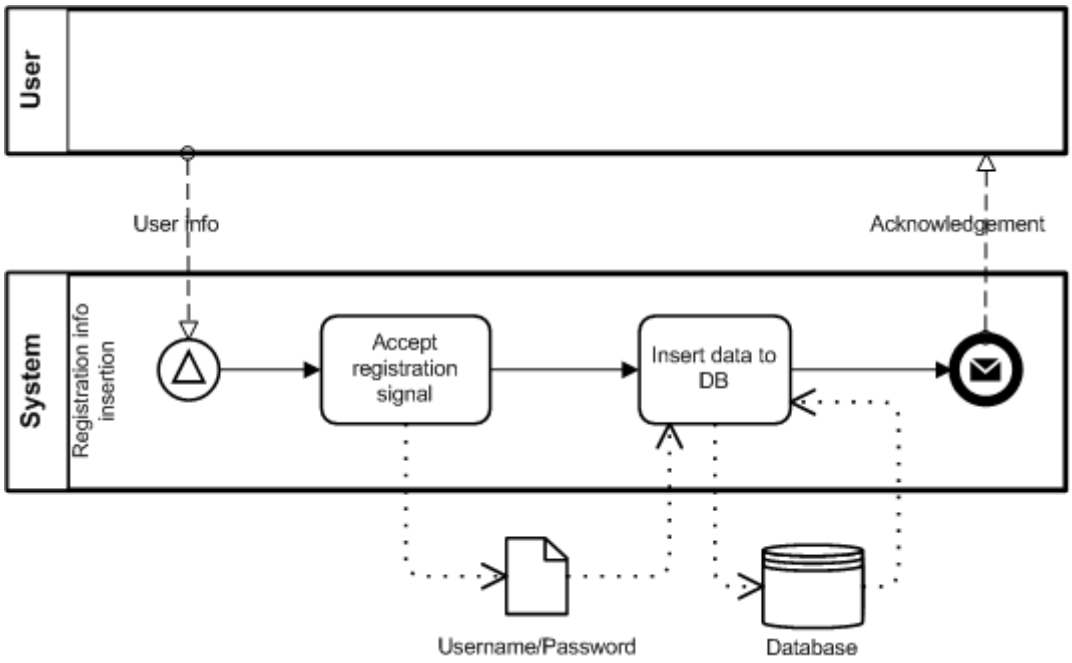

Fig. 8 User Registration Process

4.2 Determination of Security Objectives

In this scenario we can identify several major assets that need protection against security risks. Firstly, we need to ensure *confidentiality of username and password*. If confidentiality is revealed the system violators could use the user's personal data for not intended purposes. In addition we need to ensure *integrity of all the business processes*. If integrity is broken the system might be used not according to its purpose.

4.3 Risk Analysis and Assessment

In Fig.9 we model a potential security risk scenario. Let's say, that there exists a violator (presented as the BPMN *pool* Violator) who would like to login to the system without registering his personal user account (skipping process defined in Fig.8). Similarly as illustrated in Fig.7, the violator sends a message to the system. But this time the message includes a spy program (*data flow* Registration inquiry + spy malicious code), which is started after the message is accepted (*task* Accept message) and read (*task* Read message). The spy program initialises a new task (e.g., Extract data from database), which sends an inquiry to the database and extracts the Usernames and Passwords of existing users. These data are then attached to a reply message, which is sent to the violator (*task* Send answer and *data flow* Demand for registration + data copied from database).

In this analysis we are able to identify the ISSRM *threat agent* (e.g., Violator) and the ISSRM *attack method* (e.g., Registration inquiry + spy malicious code and Extract data from DB). Combination of these elements forms a security *threat*. The direct impact of this threat is that the *confidentiality* of the Usernames and Passwords is broken. On the other hand, this ISSRM *impact* provokes another *impact*, which negates the *integrity of the business processes*; i.e., the Violator is able now to access the system without registering, and, thus, change the business processes according to his needs.

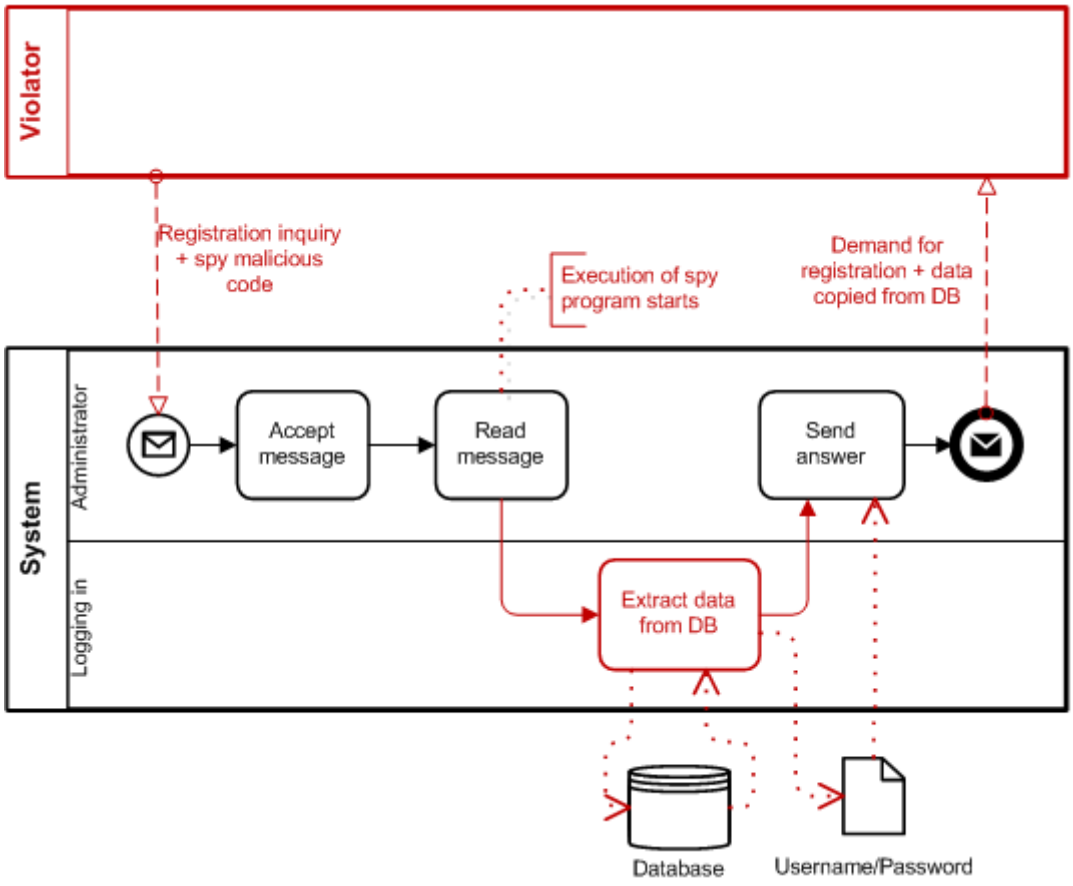

Fig. 9 Message Handling Process Including Security Risk Attack

4.4 Risk Treatment

Risk treatment involves deciding how the identified security flows could be mitigated. In our example we will take a *risk reduction* – i.e., actions to lessen the probability of the negative consequences – decision.

4.5 Security Requirements Definition

To reduce the probability of accepting the message, which contains a spy program, firstly, we introduce a *task* for Scan message, as defined in Fig.10. If scanning of the message reports a problem, the message is deleted and the message sender is blocked (*task* Block user/Delete message). Secondly, another security requirement includes the *task* Control activity of DB access. If there is a try to access the Database during the message handling process, it is blocked (*task* Block DB access). The final security requirement includes control of the outgoing/sent information (*task* Control outgoing traffic). This investigates if the response message is of the same length as initially defined. If this check reports a problem, the system stops the message sending (*cancel end event* Operation stopped).

4.6 Control Implementation

The BPMN application is typically performed at the system analysis stages. Thus, implementation of the security requirements remains postponed for the later system

development stages. On the other hand the iteration of the ISSRM process is needed where the current security requirements (e.g., ones introduced in Fig.10) would be investigated for the new security risks.

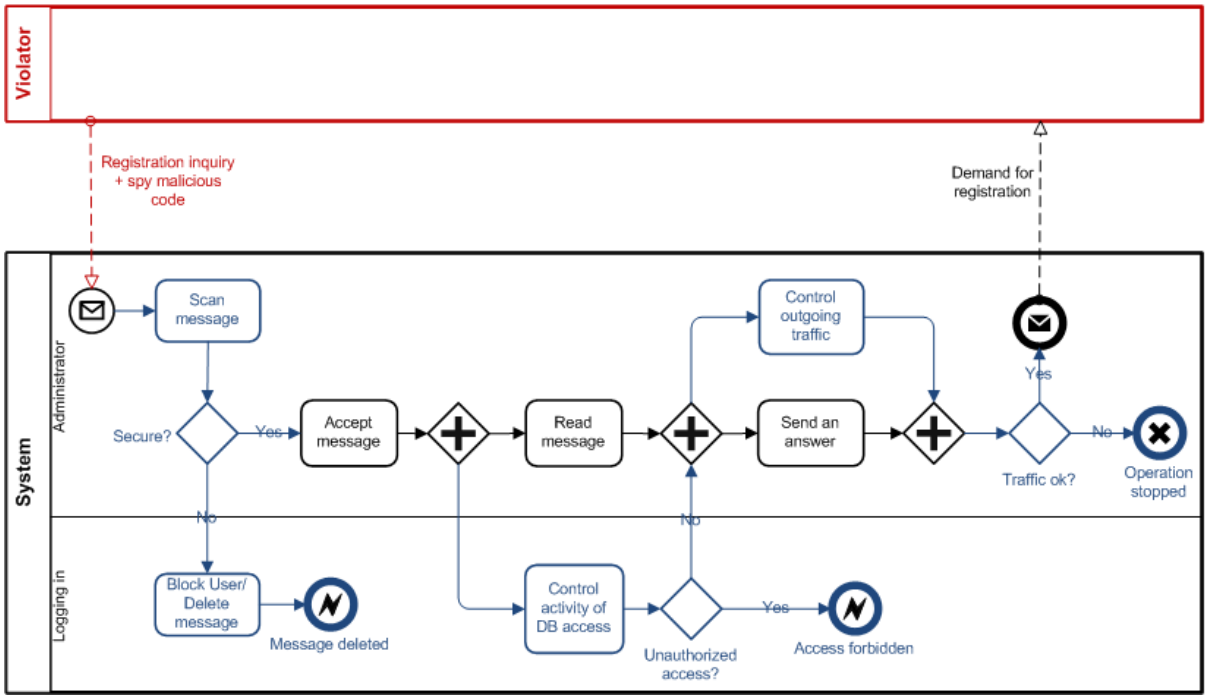

Fig. 10 Message Handling Process Including Security Requirements

4.7 Summary

In Chapter 4 we have performed an analysis of how BPMN can be applied to ISSRM process according to its six steps. We identified context and assets that has any value to the system described in running example, determinate security objectives. We also analysed and made an assessment of risk with the help of created potential security risk scenario. Moreover, we made decision about risk treatment method and according to that we defined the security requirements and opportunity of control implementation.

Chapter 5. Mapping

The running example illustrates a semantic alignment between ISSRM and BPMN. We show how BPMN is applied to consider possible attack scenarios and how countermeasures are defined. We summarise this discussion in table (see Table 1).

5.1 Asset-related Concepts

As described in Chapter 3, the ISSRM *business asset* could include valuable processes and information. In the first place the BPMN approach is meant for describing business processes within organisation. Thus, we can observe its constructs, such as *task, gateway*, *event* and their connecting link, i.e., *sequence flow*, that they help describing valuable processes. In the BPMN model the *flow objects* (i.e., *task, gateway* and *event*) are contained in the BPMN *containers*; i.e., *pools* and *lanes*. In other words the *container* constructs support definition and execution of the *business processes*. In terms of ISSRM, we align the *pool* and *lane* constructs to the ISSRM *information system assets*. The BPMN *data object*, which describes the required or produced data, is aligned to the ISSRM *business asset*, and BPMN *data store* is defined as ISSRM *IS asset*

The BPMN approach does not contain any constructs for explicit definition of the ISSRM *security criterion*. However, the created model can suggest the implicit expression (e.g., *Confidentiality of username and password*; *Integrity of the process*).

5.2 Risk-related Concepts

Risk-related concepts present what major principles should be taken into account when defining the potential risks. In principle the BMPN does not have the direct means to model security risks. However, in our example we have applied BPMN to model the negative and harmful processes. We have observed that the BPMN *pool*, when represents a negative/not intended actor, could be characterised as the ISSRM *threat agent*. Thus, the means that the *threat agent* is capable to use, are considered as the ISSRM *attack method*. For example, the BPMN *task*, as an atomic activity, when initialised by the "non-intended" actor, should be understood as the "means by which a threat agent executes threat"; such a *task* is aligned to the ISSRM *attack method*. Similar argumentation could be done about the BPMN *flow* and *data association flow*, which are also aligned to the ISSRM *attack method*.

We have not identified any explicit BPMN constructs to model the ISSRM *risk*, *impact, event*, or *vulnerability*. But we have observed that some of these concerns could be identified implicitly from the analysed problem. For instance, we can describe the ISSRM *threat* as the combination of the *threat agent* and *attack method* (see Table 1). Furthermore, two system *vulnerabilities* (namely, *Message is being handled without any scanning* and *the outgoing traffic is not monitored*) are identified. The third *vulnerability* (i.e., *the access to database is not controlled*) is found regarding the *database*. Finally, we can also define implicitly the ISSRM *impact*, which constitutes the negation of the identified *security criteria* and harm to the corresponding *assets*. These implicitly identified examples could not be expressed with the BPMN constructs.

Table 1 Alignment of the ISSRM Concepts and the BPMN Constructs

The ISSRM Concepts		BPMN Constructs	Example
Asset-related concepts	Asset	–	–
	Business asset	*Data object*; *Task*, *Gateway*, *Event*, *Sequence flow*	Username and Password; Processes of Message handling, User registration, and User login to the system
	IS asset	*Data store* *Pool*, *Lane*	Database; System, Registration info insertion, Message
	Security criterion	–	*Confidentiality* of Usernames and Password; *Integrity* of processes for Message handling, User registration and User login to the system
Risk-related concepts	Risk	–	–
	Impact	–	Confidentiality of Usernames and Password is broken; Integrity of processes is negated
	Event	–	–
	Threat	A combination of constructs for *Threat agent* and *Attack method*	A violator sends a message containing a spy program, which extract info from database and sends it back to the violator.
	Vulnerability	–	Message is being handled without any scanning; The outgoing traffic is not monitored; The access to database is not controlled
	Threat agent	*Pool*	Violator
	Attack method	*Task*; *Flows (e.g., Data flow* with the label describing attack method; *Data association flow* with the label describing attack method);	Extract data from DB; *Data flow* Registration Inquiry + spy malicious code; *Data association flows* Sends a request and Gets data
Risk treatment-related concepts	Risk treatment	–	Reduction (but other decision are also possible)
	Security requirement	*Task*, *Gateway*, *Event*, *Sequence flow*	*Tasks* Message scanning; Block user/Delete message; Control activity of DB access; Block DB access; Stop operation; Outgoing traffic control *Gateways* Secure?; Unauthorized access?; Traffic ok? *Events* Message deleted; Access forbidden; Operation stopped
	Control	–	–

5.3 Risk Treatment-related Concepts

Risk treatment-related concepts describe the decisions that should be taken, and controls to be implemented in order to mitigate the identified risks. In our example we select the *risk reduction*. However, other types of ISSRM *risk treatment decision* could also be taken depending on the level of risks mitigation.

The ISSRM *security requirements* are presented using the BPMN *task*, *gateway*, and *event* constructs connected using *sequence flow* links. For instance, the *security requirement* to mitigate the vulnerability *Message is being handled without any scanning*, starts with the BPMN *task* Scan message, followed by the *gateway* Secure?. If the problem is found the *task* Block user/Delete message, and the process finishes with the *event* Message deleted. We do not align any BPMN construct to the ISSRM *controls*. However, we should note that in late system development stages the combination of the BPMN *task*, *gateway*, and *event* constructs (as illustrated above) might result in different security control modules.

5.4 Summary

This chapter makes an overview of mapping the BPMN to ISSRM with respect to security risk analysis. We analysed how BPMN can be applied in order to follow the risk management process. We summarize results of our analysis into a table (Table 1); it introduces the major ISSRM concepts and corresponding BPMN concepts, and also provides the examples of BMN language use. The analysis shows that mapping can be realised partially; not all but the great part of risk related concepts can be represented with BPMN. Missing part can be described according to the problem context.

Chapter 6. Discussion and Conclusion

In this work we have performed an analysis of the BPMN approach following the ISSRM domain model. Our major contribution is the semantic alignment of the BPMN constructs to the ISSRM concepts. In this chapter we discuss the validity threats, conclude the study with the potential extensions and improvements of the BPMN approach towards security risk management and also present the related and future work.

6.1 Threats to Validity

The following threats to the validity of this study have been identified. Firstly, our results contain a certain degree of subjectivity. On the one hand, only two researchers have performed this study. Thus, it might mean that some aspects of the BPMN approach or its application could be interpreted and aligned to the ISSRM concepts differently. On the other hand, the running example also involves the subjective decisions on how to model the selected problem. For instance, in Fig.10 we have selected to take the risk reduction decision. However, the security requirements would be different if one would take the risk avoidance (or other) decision. Secondly, the scope of the current work is limited to the BPMN descriptive modelling. We acknowledge the importance to investigate the analytical and executable modelling, but this remains for the future research. Finally, in this work we analyse only a simple example of the Internet store. Although this example is realistic, we have not applied it in the practical settings. Thus, our analysis remains based on the selected BPMN literature (Remco et al., 2007; Seel et al., 2005; White, 2004).

6.2 Potential Improvements

In general., the BPMN approach is not specifically dedicated to the security modelling but to the business process modelling. On one hand we argue that the major version of the language should not lose its original purpose, and it should remain relatively simple. On the other hand we illustrate that BPMN provided the major set of constructs that help understanding important business assets, their security risks, and potential security requirements. Certainly this requires some potential language extensions:

- Using BPMN we are able to address only a part of the ISSRM domain model. For example, we were not able to express the ISSRM *security criterion*, *risk*, *impact*, *vulnerability*, *risk treatment*, and *control* constructs. This situation suggests potential extensions of the BPMN approach (at the concrete syntax, abstract syntax and semantic levels) and this is a potential direction for future research.
- The same constructs used for different ISSRM concepts. This could be noticed for the BPMN *task*, which is used to express the ISSRM *business asset*, *attack method*, and *security requirement* constructs; the BPMN *pool*, which helps modelling the ISSRM *threat agent* and *IS asset* constructs; and also some other constructs and links. This situation might provoke a readability and comprehensibility problem.
  There might be few solutions. The modellers could apply meta-labelling to identify different ISSRM-related concepts (e.g., [Business asset], [Attack method], or [Security requirement])

or introduce differentiating variables (e.g., *white* for the *asset-related*, *red* for the *risk-related*, and *blue* for the *treatment-related* constructs) between the same BPMN constructs aligned to different ISSRM constructs.

During our analysis we faced with a problem when one ISSRM concept could be presented using several BPMN constructs. For example, the ISSRM *security requirement* is modelled using the combination of the ISSRM *task*, *gateway*, *event* constructs and *sequence flow* links. This makes it difficult to understand the heuristics of the modelling process. Thus, it could be helpful to define rules and/or patterns to guide the use of the (security) modelling constructs.

6.3 Related Work

Rodríguez *et al.* (2007a) proposes the BPMN extensions for modelling secure business processes through understanding the security requirements. Firstly, their proposal illustrates the extension of the BPMN abstract syntax with the security-related concepts such as non-reputation, attack harm detection, integrity, privacy, access control, security role and security permission. Secondly, the concrete BPMN syntax is extended through the stereotypes introduced to the ordinary constructs of BPMN. The study does not include any consideration of the extension semantics. Further, some extensions of BPMN (called *BPSec*) are proposed towards the graphical representation of security requirements (Rodríguez et al., 2007b). They present a symbol of *padlock* to express security requirements and a *padlock with twisted corner* for audit register.

Menzel *et al.* (2009) proposes the BPMN enhancements towards trust modelling. They focus on the outline the metric that describes the value of enterprise assets and pay attention to the level of security or so called trust level of each participant of the process. Here, enterprise assets are presented using BPMN tasks, data objects, and communication links between tasks and participants. Authors define how to enable trustworthy interactions, organisational trust, and security intensions through BPMN. Other proposed extension is a security policy model used to define specific security patterns for authorisation, authentication, integrity, and confidentiality.

The limitations of these works (Menzel et al., 2009; Rodríguez et al., 2007a; Rodríguez et al., 2007b) are that they focus either on a coarse-grained level, or target only some security aspects in business processes. In comparison our study does not propose any BPMN extensions. However, we present a semantically grounded fine-grained analysis based on the well-established ISSRM domain model (Dubois et al., 2010; Mayer, 2009). As a result we present the alignment between ISSRM concepts and the BPMN constructs, which allows developers to understand current BPMN means to deal with security. Also we identify potential BPMN extensions towards security both at the (concrete and abstract) syntax and at the security risk-oriented semantics levels. In other words we explore the reasons *why* and *how* BPMN needs to be extended to consider security at the business process modelling.

Paja *et al*. (2012) introduce a method to understand *security needs* through participants' objectives and interactions. *Security requirements* are captured in terms of social commitments between the actors of the system. Then these security requirements are used to annotate business processes modelled in BPMN. Similarly, in our proposal we argue that security annotated BPMN models could be further analysed using the same modelling language, namely BPMN.

The advantage is that the business analyst would not be required to learn yet another modelling notations, but would be able systematically reason for the return on security investment in business processes.

BPMN is not the only language assessed for the IS security risk management: ISSRM has been used to evaluated Secure Tropos (Matulevičius et al., 2008b), misuse cases (Matulevičius et al., 2008a), KAOS extensions to security (Mayer, 2009), and Mal-activity diagrams (Chowdhury et al., 2012). But BPMN is the language to define the business process modelling. We have not found any business modelling language, which would support security analysis; thus the recent standard (White, 2004) for business process modelling was our natural choice. We envision that after analyzing a number of languages for security modelling it will be possible to facilitate model transformation and interoperability between them, thus introducing the security analysis from the early development stages to design and implementation, also resulting in a sustainable and secured system. Such a model transformation would be supported by transformation rules, developed on the semantic alignment of the (*business* and *security*) modelling approaches to the common base, i.e., the ISSRM domain model. However, definition of these transformation rules also remains a future study.

6.4 Future Work

The major task of our future work remains the performance of validity test. One opportunity to validate our analysis results is to create an illustrative example with proposed improvements in BPMN – to realise a performance test. That will show if proposed improvements allow using language in earlier mentioned directions with respect to security and risk management. On the other hand, to achieve more objective view, more people can be involved in validation process to conduct usability testing; providing participants with ability for using improved syntax and language semantics, ask them to create an example. That practise will discover if the language mapping and proposed improvements are available and understandable for users and are easy to use in practise. For efficiency testing, we can compare BPMN with other approaches in order to find out if it proposes a reasonable and worth method to model business process security. By reason of scope limitations, we addressed our analysis only for the first level of BPMN modelling – descriptive modelling. But we also acknowledge the importance to investigate two other level - the analytical and executable modelling, so this remains for the future research. On the other hand, our contribution should be also understood in a broader sense. For instance, in some cases application of the BPMN security extensions would not be applicable because of the language nature to model organisation's business processes, i.e., leading to the weak expressive power to address security concerns. This would result in translation of the BPMN model to the security modelling languages, such as Secure Tropos or misuse cases. Such a model translation would be supported by transformation rules, developed on the semantic alignment of the (business and security) modelling approaches to the common base, i.e., the ISSRM domain model. However, definition of the transformation rules remains a future work.

Süsteemide turvalisuse arendamine kasutades äriprotsesside modelleerimist

Resümee

Äriprotsesside arusaam ja modelleerimine on üks olulisematest aspektidesttänapäevases süsteemiarenduses. Infosüsteemide modeleerimiseks on loodud erinevaid käsitlusi ning äriprotsesside modeleerimisnotatsioon on üks nendest. On teada, et BPMN aitab äriprotsesse kirjeldada, modelleerida ja optimeerida. Keerulisem on mõista kuidas saab selle käsitluse raames juhtida äriprotsesside turvalisust ning analüüüsida infosüsteemi turvariske. See aspekt muutub kaasaegsetes infosüsteemides veel komplitseeritumaks, kuna turvatud süsteemi loomiseks peavad nii äriprotsessid kui ka selle turvalisuse küsimused olema vaadeldud parallellselt, see tähendab koostoimes. Käesoleva uurimistöö eesmärgiks on analüüsida BPMN ja infosüsteemi turvariskide juhtimise vastastikkust koosmõju. BPMN'i võtmeaspektide väljaselgitamiseks ja antud modelleerimissüsteemi turvanäitajate, riskide ja riskide juhtimise mõistmiseks on antud töös kasutatud struktureeritud lähenemist. Töös uuritakse kuidas modelleerija saab BPMN'i abil väljastada turvatud süsteemi komponente, riske või riskide juhtimist. Töös ühtlustatakse BPMN keele põhikonstruktsioonid ISSRM mudeli kontseptiga. Antud uurimistöös on BPMN-i käsitluse rakendausvõimalusi vaadeldud ühe internetikaupluse näitel.

Meie uurimistöö pakkub infosüsteemi analüütikule või arhitektile võimalust mõista äriprotsesse ja turvakomponente ühe modelleerimiskeele abil. Analüüs on tehtud ainult esimese keele, *Descriptive modelling,* tasemel. Sellega avatakse uurijale võimalus tuua paralelle erinevate modeleerimiskeelte vahel, et uurida mustreid ISSRM perekonda kuuluvate mudelite loomises .

References

1. van der Aalst, W.M.P., ter Hofstede, A.H.M. (2005) : YAWL: Yet Another Workflow Language. Information Systems, 30(4), pp 245–275

2. Backes, M., Pfitzmann, B., Waidner, M. (2003): Security in Business Process Engineering. In: van der Aalst W. M. P. (eds.) BPM 2003, pp 168-183. Springer Heidelberg

3. Börger, E., Cavarra, A., Riccobene, E. (2000): An ASM Semantics for UML Activity Diagrams. In: Proceedings of the 8th AMAST 2000, pp. 293-308. Springer, Heidelberg

4. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R (2010).: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering. pp. 289-306. Springer

5. Jürjens J. (2005): Secure Systems Development with UML, Springer-Verlag Berlin Heidelberg

6. Matulevičius, R., Mayer, N., Heymans, P. (2008a): Alignment of Misuse Cases with Security Risk Management. In: Proceedings of ARES'08, pp. 1397-1404. IEEE Computer Society

7. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N. (2008b): Adapting Secure Tropos for Security Risk Management during Early Phases of the Information Systems Development. In Proceedings of CAiSE'08, pp. 541-555. Springer Heidelberg

8. Mayer, N. (2009): Model-based Management of Information System Security Risk. Doctoral Thesis, University of Namur

9. Menzel M., Thomas I., Meinel C. (2009): Security Requirements Specification in Service-oriented Business Process Management. ARES 2009, 41-49

10. Paja, E., Giorgini, P., Paul, S., Meland P. H. (2012): Security Requirements Engineering for Secure Business Processes. In Proceedings of the Selected Papers from Workshops and Doctoral Consortium of the 10th International Conference BIR 2011, LNBIP (in press)

11. Remco, M., Dijkman, R.M., Dumas, M., Ouyang, C. (2007): Formal Semantics and Analysis of BPMN Process Models using Petri Nets. Queensland University of Technology, Tech. Rep.,

12. Rodriguez, A., Fernandez-Medina, E., Piattini, M. (2007a): A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE – Transactions on Information and Systems, vol E90-D (4), pp. 745-752

13. Rodríguez, A., Fernández-Medina, E., Piattini, M. (2007b): Towards CIM to PIM Transformation: From Secure Business Processes Defined in BPMN to Use-Cases, LNCS, vol. 4717, 408-415

14. Seel, C., Vanderhaeghen, D. (2005): Meta-Model Based Extensions of the EPC for Inter-Organisational Process Modelling. In: Proceedings of the 4th GI-Workshop EPK 2005 – Geschaftsprozessmanagement

15. Silver, B. (2009): BPMN Method and Style: A Levels-based Methodology for BPMN Process Modeling and Improvement using BPMN 2.0, Cody-Cassidy Press

16. Sindre, G. (2007): Mal-activity Diagrams for Capturing Attacks on Business Processes. In Proceedings of REFSQ 2007, pp. 355-366, Springer Heidelberg

17. Stephen A. White. (2004): Introduction to BPMN, article, BP Trends, IBM Corporation

18. Stoneburner G, Goguen A, Feringa A. (2002): NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Gaithersburg

19. White, S.A.: Introduction to BPMN, IBM, (2004), http://www.bpmn.org/Documents/Introduction_to_BPMN.pdf

Appendix

Altuhhova O., Matulevičius R., Ahmed N., (2012): Towards Definition of Secure Business Processes. M. Bajec and J. Eder (Eds.): CAiSE 2012 Workshops, LNBIP 112, pp. 1-15, Springer-Verlag Berlin Heidelberg