

Security Risk Management using Business Process Modelling Notations

Olga Altuhhova and Raimundas Matulevičius

¹ Institute of Computer Science, University of Tartu
J. Liivi 2, 50409 Tartu, Estonia
olgaaltuhhova@hotmail.com, rma@ut.ee

Abstract. Business process understanding and modelling is one of the major aspects in the modern information system (IS) development. Thus, there exist several modelling approaches to support this activity, and one of them is the business process modelling notations (BPMN). Although BPMN is a good approach to understand business processes, there is a limited work to understand how this language could deal with business security and security risk management for IS. This is a problem, since both business processes and security concerns should be understood in parallel to support a development of the secure IS. 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 secured assets, risks and risk treatment using BPMN. Thus we align the main constructs of the BPMN language with the key concepts of the ISSRM domain model. We show applicability of our approach on a running example related to the Internet store. We believe that our proposal would 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 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).

Keywords: Business process modelling notations (BPMN), Security risk management, Alignment of modelling languages, Information systems.

1 Introduction

On the one hand, one of the important aspects of the IS development is the understanding and *modelling of business process* supported by the developed IS. This means we need to have an efficient and effectively way to analyse the needs for the software and services that arise from the demands of today's businesses. On the other hand, *security engineering* is another important concern. The concept of security itself refers to the capability of a product, i.e., information system, to protect data and information against the unauthorised access by persons or systems that have intention

to harm it. Nowadays, it becomes a challenge to create secure business processes that would be protected against the different security risks.

The great variety of business process modelling approaches was developed in the recent decade; for example, event process chains (EPC) [16], yet another workflow language (YAWL) [1], UML activity diagrams [4] and business process modelling notations (BPMN) [14] [17] [19]. For instance, the EPC approach [16] combines the different views towards the description of enterprises and ISs in the control view on the conceptual level. It 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 the SAP R/3 modelling. The YAWL approach is able to support complex data, integration with organisational resources and external applications, process verification and process configuration [1]. One of the most common approaches for business process modelling is the UML activity diagram [4]. Currently the *de facto* industrial standard, the UML uses activity diagrams to model the workflow behind the designed system. In this paper we have selected the BPMN [14] [17], which currently is becoming a standard developed by the Business Process Management Initiative community [19]. Using BPMN developers can specify technical details processes. Because of its intuitiveness the BPMN model can be comprehended by various IS stakeholders [17].

Although BPMN is a good approach to model business processes, there is a limited work [15] done to understand how this language could deal with business security and security risk management for IS. In this paper we investigate how BPMN could be used to determine the security risks. More specifically, we analyse this language with respect to the domain model of the information systems security risk management (ISSRM) [7] [11]. Our analysis allows us to determine the BPMN constructs, which could be used to express secure business and IS assets, their risks and security requirements in order to mitigate these risks.

2 Information Systems Security Risk Management

In order to understand how modelling approach could help consider security concerns, one could utilise different security risk management approaches. For instance, the CORAS approach [5] provides a systematic guidance for security risk analysis. The Tropos Goal-Risk framework [2] supports modelling, assessing and treating risks on the basis of the likelihood and severity of failures. However both these approach are dedicated to the general consideration of security risks. A more specific viewpoint on the *IS development* is suggested by the domain model for ISSRM [7] [11].

2.1 Domain Model

The ISSRM domain model [7] [11] shown in Fig. 1, is inspired by, and compliant with the existing security standards, e.g., [6] [8] [10]. It supports definition of security for the key IS constituents and addresses the IS security risk management process at three different conceptual levels, *i.e.*, *asset-related*, *risk-related*, and *risk treatment-related 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* of business assets.

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.

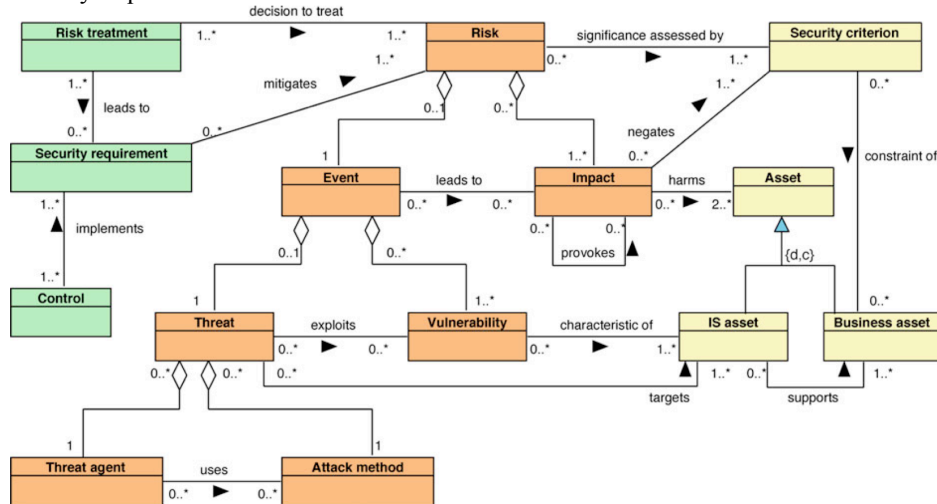


Fig. 1. The ISSRM Domain Model (adapted from [7] [11])

2.2 Application Process

The ISSRM application follows the general risk management process it is based on the existing security standards, e.g. [5] [6] [8] [10]. 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., confidentiality, 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*. Finally, security requirements are *implemented* into *security controls*. The risk management process is iterative, because new security controls might also open the possibility for new (not yet determined) security risks. In Section 4 we will explicitly illustrate how the BPMN approach could be used following the ISSRM process.

3 BPMN

Business Process Modelling Notation (BPMN), a multi-vendor standard controlled by the Object Management Group [19], is a language for constructing business process models. BPMN is considered business-friendly, because it is based on notions familiar from the traditional flowcharting. At the same time, the notation is linked to a semantic model, which means that each shape used in the notation has a specific meaning, with defined rules of connections between objects.

The application of BPMN is classified at three levels, based on how the model is used [17]. *Analytical modelling* describes the activity flow, including the exception paths significant to key performance indicators. *Executable modelling* is targeted to the system developing, not business architecture or analysis. In this paper our scope is on the initial level, i.e., the *descriptive modelling*, which concentrates on business oriented process by documenting the major businesses flows.

3.1 Concrete Syntax

We will introduce the concrete syntax of BPMN through the *Internet store* example. In Fig. 2 we present an order making, execution, and product delivery process. The major stakeholders (e.g., User, Internet store, Factory and Bank) of our example are presented using the BPMN *lanes*. In this diagram the emphasis is placed on the Internet store, which is divided into three BPMN *pools*; i.e., Finance, Preparation and Sales.

The process begins with a message, which *triggers* a *start event* (see Request for product order) and the first *task* Receive request. The next task is an identification of the user (see the BPMN *task* Identify user), which requires a connection with a Database (expressed using BPMN *data store*) in order to check the information on user existence. If the user is not identified (see the BPMN *gateway* Identified?), the process is led to the *end event* with a terminal *trigger*. Otherwise the process continues with the order entering into the system (*task* Enter order), and two parallel tasks start: one for checking the product availability (*task* Check product availability), another for controlling the financing (*task* Control financing). In the first parallel, 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). In the second parallel the payment for the product is checked with the Bank. Both parallels are joined with a *gateway*, after which the order is closed and delivered (*task* Close and deliver) to the user. The process finishes with an *end event* (Success), which sends a message to the User (see BPMN *data flow* Deliver order).

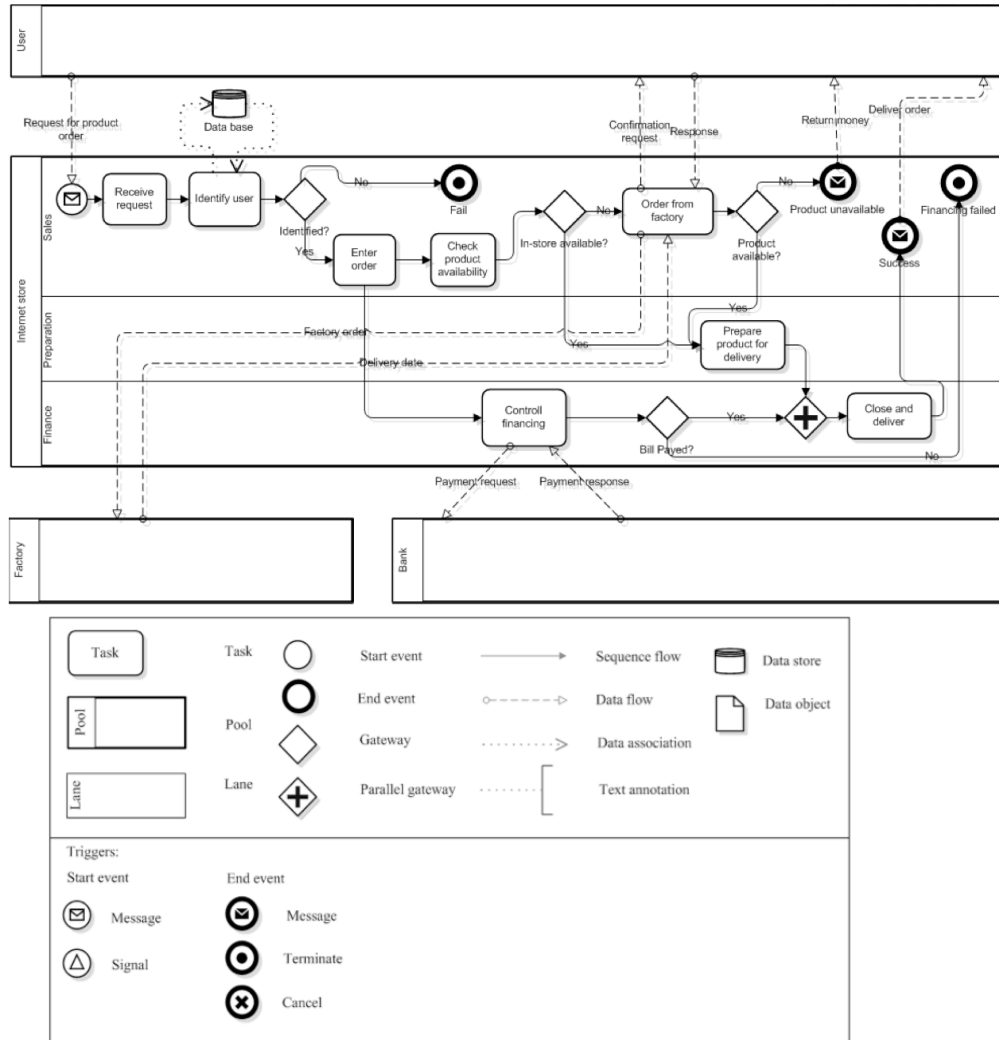


Fig. 2. The Internet Store: Order Making, Execution and Product Delivery Process

3.2 Abstract Syntax and Construct Description

In this paper we focus on the BPMN subset – *descriptive modelling*. The extract of the BPMN abstract syntax (based on [14]) is shown in Fig. 3 and 4. As illustrated in Fig. 3, BPMN includes four major categories of constructs: *flow objects*, *containers*, *flows* and *artefacts*.

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* (i.e., it means an activity that executes or finishes the event; e.g., message, timer, error,

etc.) 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 gateway determines decisions, as well as forking, merging, and joining of the process paths. We can define some types of gateways. An *exclusive* gateway (i.e., XOR) represents an exclusive decision, which means only one of the output sequence flows to be followed, based on some condition. The *parallel* gateway signifies a parallel split or AND-split. It means that all of the outgoing sequence flows are to be followed in parallel, unconditionally.

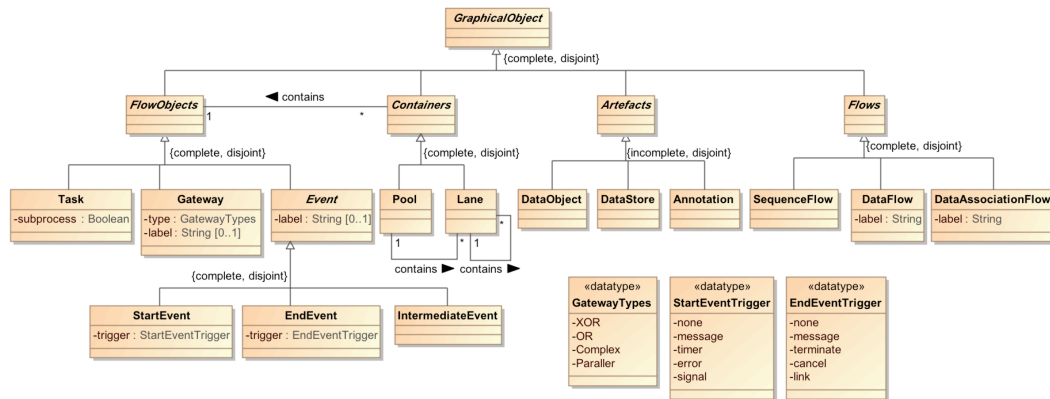


Fig. 3. The BPMN Abstract Syntax: Concept Classification

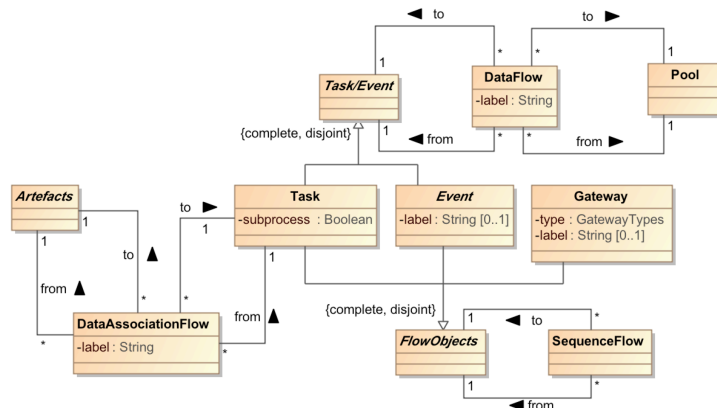


Fig. 4. The BPMN Abstract Syntax: Relationships

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 a mechanism to show what data is required or

produced by activities. *Data stores* describe the way data could be stored. *Annotations* suggest a mechanism to provide additional textual information on the diagram content.

Relationships between different BPMN constructs are defined using *flows*, which include *sequence flows*, *data flows*, and *data association flows*. In Fig. 4 we define what elements could connect together using different flows. For instance, the *sequence flows* link together the BPMN activities, gateways, and events within a single pool. The *data flows* are used to link together the BPMN pools; typically, this relationship defines the input to or output from one pool from/to a task/event executed in another pool. Finally, the *data association flows* link together the BPMN tasks and artefacts (i.e., data objects, data stores, and annotations).¹

4 Analysis and Alignment

In this section we will consider how the BPMN approach could be applied according to ISSRM. We will use the method applied to analyse the security modelling languages, such as Secure Tropos in [13] and misuse cases in [12]. More specifically, we will follow the six steps of the ISSRM process to investigate security risks in a running example modelled using the BPMN approach. Next, we will summarise our observation to the alignment of BPMN to ISSRM.

4.1 Security Risk Modelling with BPMN

Our running example is an *online registration process of the Internet store*. When following the ISSRM process, first, we identify the content and valuable assets.

Context and asset identification. Let's consider the following situation where the potential User (in Fig. 5 presented as the BPMN *pool* User) wishes to start using the Internet store system (*pool* System). In order to get details about the registration, user sends a message with an inquiry to the system administrator. The process of the message handling is presented in Fig. 5. Here, the system accepts the message (*task* Accept message), the message is read by the system administrator (*task* Read message) and a reply with guidelines (*data flow* Demand for registration) is sent (*task* Send answer) back to the user.

In Fig. 6 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 Internet store system as illustrated in Fig. 7. Hence the system, first, checks the username (*task* Check the username existence), and, then, the password (*task* Checks password). If these data matches, the user gets the "Success" signal and is able to use

¹ In this paper we do not define the explicit integrity constraints of the BPMN abstract syntax. However, these exist to strengthen the *flows*. For example, the *data association flow* could only be defined between the BPMN *artefact* and the BPMN *task*; the *data flow* could only be defined between the BPMN *pool* and the BPMN *task/event*, and similar.

the Internet store system. Otherwise he gets a notification about the failure (*data flow* No such user or password).

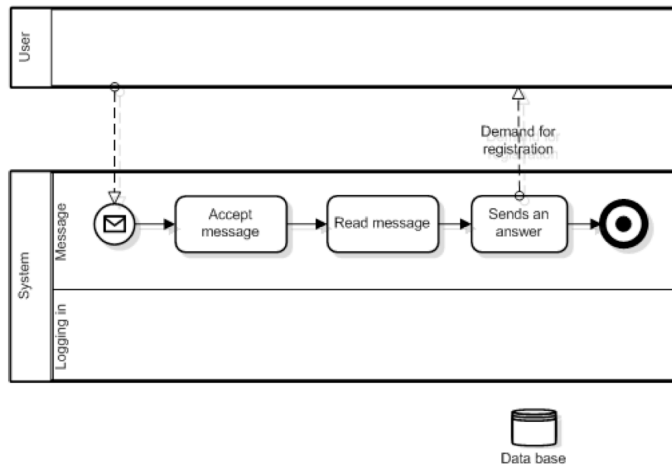


Fig. 5 Message Handling Process

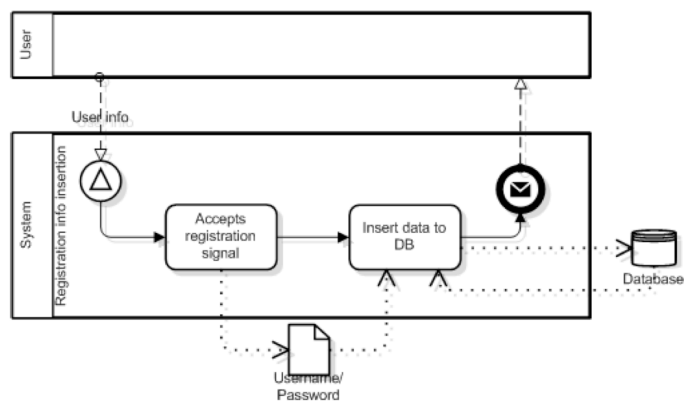


Fig. 6 User Registration Process

Determination of security objectives. In this scenario we can identify several major assets that needs 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 the not intended purposes.

In addition we need to ensure *integrity of all the business processes* (e.g., including the ones described in Fig. 5, 6 and 7). If integrity is broken the system might be used not according to its purpose.

Risk analysis and assessment. In Fig. 8 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. Similarly as illustrated in Fig. 5, the violator sends a message to the system. However this time, the message includes a spy program (*data flow* Message containing a spy

program), 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 DB), 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* Sends an answer and *data flow* Demand for registration).

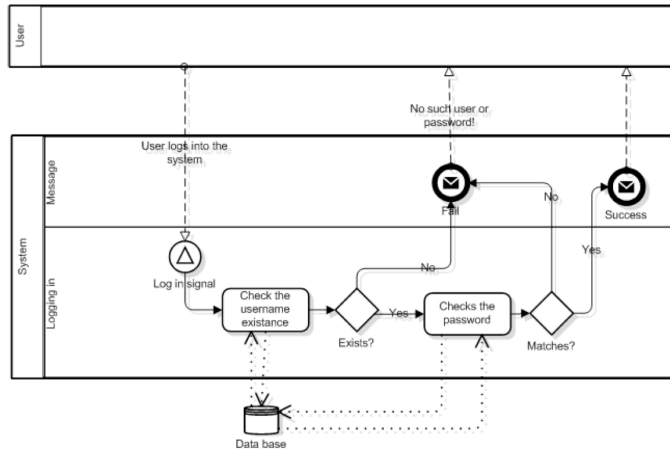


Fig. 7 User Login Process

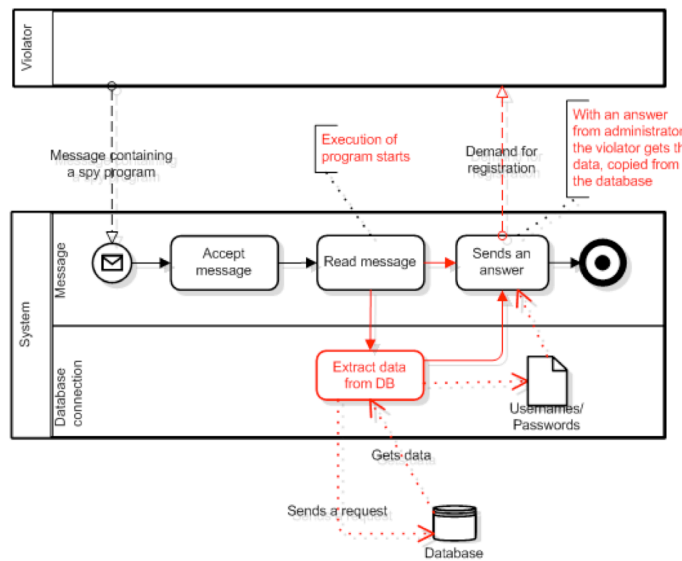


Fig. 8 Message Handling Process Including Security Risk Attack

In this analysis we are able to identify the ISSRM *threat agent* (e.g., Violator) and the ISSRM *attack method* (e.g., Message containing a spy program and Extraction of data from the database). 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 (e.g., using the process described in Fig. 7), and, thus, change the business processes according to his needs.

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.

Security requirements definition. To reduce the probability of accepting the message, which contains a spy program, firstly, we introduce a *task* for Message scanning, as defined in Fig. 9. 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* Outcoming traffic control). This investigates if the response message is of the same length as it was initially defined by the system administrator. If this check reports a problem, the system stops the message sending (*task* Stop the operation).

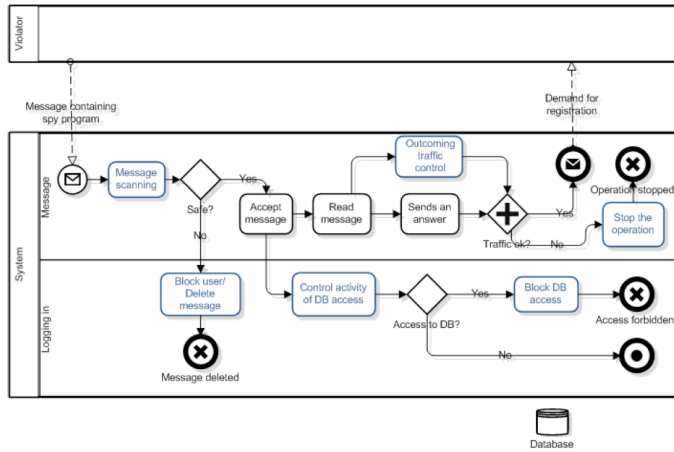


Fig. 9 Message Handling Process Including Security Requirements

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. 9) would be investigated for the new security risks.

4.2 ISSRM and BPMN Alignment

The result of this analysis is the semantic alignment between the ISSRM and BPMN. We illustrate how we can use the BPMN approach to analyse possible attack scenarios and how to derive countermeasures from them. We summarise the discussion on alignment in Table 1.

Table 1. Alignment of the ISSRM Concepts and the BPMN Constructs

The ISSRM domain model		BPMN constructs	Example
Asset-related concepts	Asset	-	-
	Business asset	<i>Data object; Task, Gateway, Event, Sequence flow</i>	Username and Password; Processes described in Fig. 5, 6, and 7
	IS asset	<i>Data store Pool, Lane</i>	Database; System, Database connection, Message
	Security criterion	-	<i>Confidentiality</i> of Usernames and Password; <i>Integrity</i> of processes described in Fig. 5, 6, and 7
Risk-related concepts	Risk	-	-
	Impact	-	Confidentiality of Usernames and Password is broken; Integrity of processes (e.g., Fig. 5, 6, and 7) is <i>negated</i>
	Event	-	-
	Threat	-	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	<i>Pool</i>	Violator
	Attack method	<i>Task; Flows (e.g., Data flow with the label describing attack method; Data association flow with the label describing attack method);</i>	Extract info from database; <i>Data flow</i> Message containing a spy program; <i>Data association flows</i> Sends a request and Gets data
Risk treatment related concepts	Risk treatment	-	Reduction (but other decision are also possible)
	Security requirement	<i>Task, Gateway, Event, Sequence flow</i>	<i>Tasks</i> Message scanning; Block user/Delete message; Control activity of DB access; Block DB access; Stop operation; Outgoing traffic control <i>Gateways</i> Safe?; Access to DB?; Traffic ok? <i>Events</i> Message deleted; Access forbidden; Operation stopped
	Control	-	-

Asset-related concepts. As described in Section 2, 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* regarding the valuable business information. We align together the ISSRM *asset* and the BPMN *data store* (how data should be stored).

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*), which could be recorded using other security modelling means.

Risk-related concepts present how the risk itself can be defined and what major principles should be taken into account when defining the potential risks [7] [11]. In principle the BPMN 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; thus modeller needs to look for other security modelling means.

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* Message scanning, followed by the *gateway* Safe?. 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 Discussion and Conclusion

In this paper 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 section we discuss the validity

threats, then conclude the study with the potential extensions of the BPMN approach towards security risk management. Finally, we present the related and future work.

5.1 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. 9 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 [14] [16] [19].

5.2 BPMN Extensions towards Security Risk Management

In general, the BPMN approach is not specifically dedicated to the security modelling. Thus, it is not a surprise that our study has revealed the potential BPMN extensions and improvements towards the security risk management:

- Using BPMN we were 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*, *threat*, *vulnerability*, *risk treatment*, and *control* constructs. This situation suggests potential extensions of the BPMN approach (at the concrete syntax, abstract syntax and semantic levels) by introducing additional security and security risk constructs.
- 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 BPMN constructs and links. This situation might provoke a readability and comprehensibility problem.

There might be few solutions. Firstly, the modellers could apply meta-labelling to identify different ISSRM-related concepts. For example, the label of the BPMN *task* could be equipped with additional meta-label (e.g., [Business asset], [Attack method], or [Security requirement]), which would identify to which ISSRM concept this construct is aligned. Secondly, the developers could introduce differentiating variables between the same BPMN constructs aligned to different ISSRM constructs. These variables, for instance, might be the construct background or borderline colour; i.e., *white* for the *asset-related* concepts, *red* for the *risk-related* concepts, and *blue* for the *risk treatment-related* 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.

5.3 Related work

In the literature we found few studies on the extension of the business process modelling languages towards security. For instance Sindre introduces an extension of the UML activity diagrams, called mal-activities [18]. Gaaloul *et al.* present a model to ensure integrity, confidentiality and availability when tasks are delegated among business actors [9]. In [3] security requirements (expressed through the cryptographic primitives) are incorporated in the development of the business processes. The limitations of these works are that they focus either on a coarse-grained level, or target only some specific security aspects (e.g., security requirements) in business processes.

In [15] Rodriguez *et al.* propose 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. In comparison to [15] in this work we do not propose any concrete extensions of the BPMN. However, we present a semantically grounded analysis based on the well-established domain model for the IS security risk management [7, 11]. This allows us (i) to understand current BPMN means to deal with security-related problems; (ii) to identify the potential BPMN extensions towards security analysis both at the (concrete and abstract) syntax level and at the security-oriented semantics level.

5.4 Future work

On the one hand, the major tasks of our study remain implementation of identified extensions and performance of the validity test. 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 [13] or misuse case [12]. 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.

References

1. van der Aalst, W.M.P., ter Hofstede, A.H.M.: YAWL: Yet Another Workflow Language. *Information Systems*, 30(4), pp 245–275 (2005)
2. Asnar, Y., Giorgini, P., Massacci, F., Zannone, N.: From Trust to Dependability through Risk Analysis. In: *Proceedings of ARES 2007*, pp. 19-26. IEEE Computer Society (2007)
3. Backes, M., Pfitzmann, B., Waidner, M.: Security in Business Process Engineering. In: van der Aalst W. M. P. (eds.) *BPM 2003*, pp 168-183. Springer Heidelberg (2003)
4. Börger, E., Cavarra, A., Riccobene, E.: An ASM Semantics for UML Activity Diagrams. In: *Proceedings of the 8th AMAST 2000*, pp. 293-308. Springer, Heidelberg (2000)
5. Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., Vraalsen, F.: Model-based Security Analysis in Seven Steps—a Guided Tour to the CORAS Method. *BT Technology Journal*, vol. 25(1), pp.101–117. (2007)
6. DCSSL. EBIOS – Expression of Needs and Identification of Security Objectives (2004)
7. 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 Engineering*. pp. 289-306. Springer (2010)
8. ENISA, Inventory of Risk Assessment and Risk Management Methods (2004)
9. Gaaloul, K., Schaad, A., Flegel, U., Charoy, F.: A Secure Task Delegation Model for Workflows. In *Proceedings of the 2nd International Conference on Emerging Security Information Systems and Technology*, pp 10-15. IEEE Computing Society, (2008)
10. ISO, Information technology – Security techniques – Information security management systems – Requirements, International Organisation for Standardisation, (2005)
11. Mayer, N.: Model-based Management of Information System Security Risk. Doctoral Thesis, University of Namur (2009)
12. Matulevičius, R., Mayer, N., Heymans, P.: Alignment of Misuse Cases with Security Risk Management. In: *Proceedings of ARES'08*, pp. 1397-1404. IEEE Computer Society (2008)
13. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N.: 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 (2008)
14. Remco, M., Dijkman, R.M., Dumas, M., Ouyang, C.: Formal Semantics and Analysis of BPMN Process Models using Petri Nets. Queensland University of Technology, Tech. Rep., 2007
15. Rodriguez, A., Fernandez-Medina, E., Piattini, M.: 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 (2007)
16. Seel, C., Vanderhaeghen, D.: Meta-Model Based Extensions of the EPC for Inter-Organisational Process Modelling. In: *Proceedings of the 4th GI-Workshop EPK 2005 – Geschäftsprozessmanagement* (2005).
17. Silver, B.: BPMN Method and Style: A Levels-based Methodology for BPMN Process Modeling and Improvement using BPMN 2.0, Cody-Cassidy Press, 2009
18. Sindre, G.: Mal-activity Diagrams for Capturing Attacks on Business Processes. In *Proceedings of REFSQ 2007*, pp. 355-366, Springer Heidelberg (2007)
19. White, S.A.: Introduction to BPMN, IBM, 2004,
http://www.bpmn.org/Documents/Introduction_to_BPMN.pdf