Eliciting Security Requirements for Business Processes using Patterns

Naved Ahmed, Raimundas Matulevičius and Naiad Hossain Khan

Institute of Computer Science, University of Tartu
J. Liivi 2, 50409 Tartu, Estonia

Abstract. Business process modelling and security engineering are two important concerns when developing information system (IS). However current practices report that security is addressed rather at the later development stages (i.e., design and implementation). This raises a question whether the business processes are performed securely. In this paper, we propose a method to align business process modelling and security engineering. We develop a set of security risk-oriented patterns. Such patterns help to understand security risks that potentially arise within business processes, and to introduce security solutions. To ease the applicability the security risk-oriented patterns are defined using BPMN notations. The proposal is tested in an industrial business model and the findings indicate a positive usefulness to identify important business assets, their security risks and countermeasures.

1 Introduction

Business process modelling (BPM) is an activity of representing enterprise processes, so that the current processes may be analysed and improved. *Security engineering* is concerned with lowering the risk of intentional unauthorised harm to valuable assets to level that is acceptable to the system's stakeholders by preventing and reacting to malicious harm, misuse, threats and security risks [10]. Assuming that business analysts concentrate on improving the business performance, early security analysis could help discovering and discarding system design alternatives that do not offer sufficient security levels. Although the importance of addressing security concerns is now acknowledged [7], common practice is to consider security when the system is about to be implemented or deployed [11]. One of the reasons is that, business analysts are experts in business domain, they have limited or no expertise in security engineering; thus they depend on the practices, security standards [2, 3], or security experts. Such a situation potentially contains several limitations. Thus, here we investigate the following research question: *how to facilitate elicitation of security concerns during business process modelling?*

According to Schumacher *et al.* "a security pattern describes a particular recurring security problem that arises in a specific security context and presents a well-proven generic scheme for a security solution"[17]. Following this definition, in this study we develop a set of *security risk-oriented patterns* (i.e., *generic scheme*). These patterns are based on understanding security risks (i.e., *recurring security problems*) that potentially

Ahmed N., Matulevičius R. and Hossain Khan N..
Eliciting Security Requirements for Business Processes using Patterns.
DOI: 10.5220/0004100200490058
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 49-58
ISBN: 978-989-8565-15-0

arise within business processes (i.e., *specific security context*). To mitigate these risks, the patterns recommend *security requirements* (i.e., *security solution*). In other words, our approach aligns business processes and security requirements elicited using security risk-oriented patterns. In order to understand usefulness of these patterns we apply them in business models. Our study, thus, results in the guidelines to elicit security assets, potential security risks and their countermeasures in the business processes.

The rest of the paper is structured as follows: Section 2 discusses the related work in the domain of business processes security and compares the security risk management approaches. Section 3 describes the security risk-oriented patterns, this is the major contribution of our work. Next, Section 4 demonstrates the example of pattern application in the business model. In Section 5 we discuss and conclude the paper and outline the future work.

2 Background

2.1 Security in Business Process Modelling

There exists several studies relating business processes and security requirements elicitation. Röhrig and Knorr [16] derive security requirements by assigning the security level to business process components using a formal descriptive language. However, security measures are applied after the definition of the business processes. Rodríguez *et al.* [15] extend BPMN using *padlocks* to annotate business processes with security requirements. The early security requirements are expressed with a specific padlock symbols. Similarly, Christopher and Joe [14] proposed two new artefacts − *operating condition* and *control case* − to express the constraints on business processes. Modelling constraints helps in mitigating risk and facilitate the early discovery of security requirements. These practices [16, 15, 14] express the security requirements. However, they are not align with risk analysis and the rationale is absent. Paja *et al.* [13] specify commitments by analysing the participant's objectives and their interactions which are considered as high-level specification of security requirements. They are annotated in BPMN using conversation and choreography diagrams. Though it gives rationale for security, but the requirements are limited to the exchange of resources. And a detail semantic mapping between organisational model and BPMN is also missing.

2.2 Security Risk Management

A domain model (see Fig. 1) for Information Systems Security Risk Management (ISSRM) [8] expresses the key concepts and their relationships used to define the security risk-based template [4]. ISSRM helps identify and specify security risks. It also addresses the risk management approaches to support the risk management process that focuses on whole IS, instead of defining security requirements for one or more IS components. ISSRM applies security in the IS development while other approaches are mainly applied on an existing IS, but not applicable in the IS development. Although, few can be used by implementing additional guidelines, however they still lacks the Requirement Engineering (RE) activities and wouldn't able to reason for security requirements.

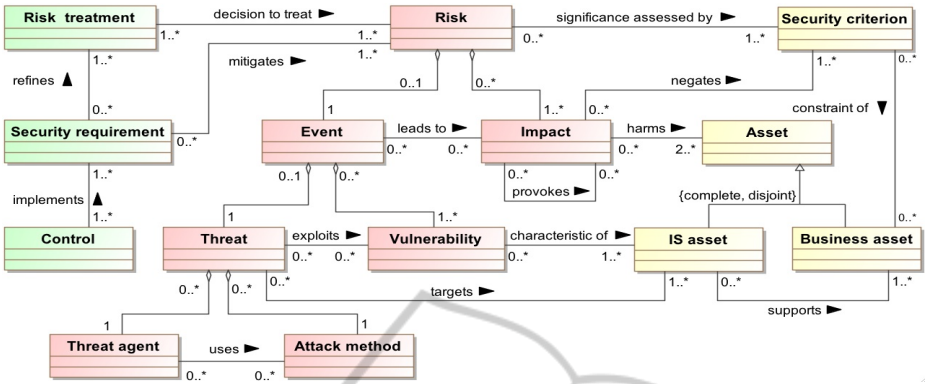

Fig. 1. ISSRM Domain Model, adapted from [8].

Risk management methods (see details in [8]) produce analysis in natural language, which hinders to automate their activities for reasoning, evolution, monitoring or traceability, except CORAS [6]. In CORAS, each activity proposed a structured artefact but it is neither connected to RE activities nor applicable to the IS development and is disconnected from the standard terminology.

3 Security Risk-oriented Patterns

3.1 Developing Patterns

We followed the 3-steps pattern-oriented approach to develop our security patterns: Firstly, we have developed the security risk-oriented template (see [4] for template details). Secondly, a set of security risk-oriented patterns are defined, by identifying the security flaws (listed in [18]), followed by the risk analysis and the countermeasures are developed using available security standards (e.g. [2, 3]) to mitigate these risks. Finally, we apply our approach in a business model to illustrate its feasibility. We have developed ten security risk-oriented patterns. These patterns are the major contribution of our research study and are briefly described below and the respective details are given in a technical report [12].

SRP 1. *Pattern secures the data transmitted between the business entities i.e., stakeholders involved in the business process.* If attacker intercepts the transmission medium that can lead to the loss of data confidentiality and its integrity. To reduce risk this pattern proposes to make the data unreadable before transmitting, and calculate the checksum value. To avoid risk this pattern proposes to change the transmission medium that cannot be intercepted.

SRP 2. *Pattern ensures valid data entry into business processes by rejecting the unwanted malicious data.* The risk analysis identifies that invalid data can cause the loss of business process integrity and also attacker can make the business entity unavailable for their clients. To avoid these risks this pattern proposes to define a structured format for incoming data and restrict any other format data.

SRP 3. *Pattern verify the origin of the business entity that sends the data and secure the integrity of business processes.* It investigates the legitimacy of sender, and ensures that sender should not deny the sending of data, i.e., non-repudiation. The identified risks are malfunction strategies and incorrect initiation of a business activity (e.g., process invalid purchase order). To reduce the problem this pattern introduces the requirement of verifying sender's identity.

SRP 4. *Pattern ensures the availability of business service by protecting the IS from denial of service (DOS) attack.* It addresses the problem of services offered by business which are exposed to their clients. Therefore, are more vulnerable to external attackers. The risk is that an attacker can make the service unavailable and prevent the legitimate users. To reduce the risk of DOS attacks this pattern proposes to restrict the packets using proper router configuration.

SRP 5. *Pattern secures data from misuse by applying multilevel access rights to the retrieval interface.* It addresses the problem of unauthorised access and missing system log which has information about who read the data. This raises the risk of leaking data that can be misused. To reduce the risk this pattern proposes to restrict anonymous access at retrieval interface, establish access levels of data and give it to relevant individuals, and keep track of data retrieval.

SRP 6. *Pattern secures data store by storing the confidential data in invisible format.* If data store saves data in plain format then attacker able to read it easily. This compromises the confidentiality of data and its misused can have negative impacts. Pattern proposes two solution to this problem: reduce the risk by storing the data in invisible format (e.g., encrypted), and do not store the data in data store instead ask clients when the it is needed.

SRP 7. *Pattern describes a flow to handle more than one request in parallel to avoid the deadlock condition.* Here, a deadlock situation is addressed when a business activity holds a resource and request for other resources. An attacker can deliberately create such scenario and can crash an activity or service, making it unavailable for users. To reduce the risk this pattern proposes all the resources should be requested in advance or released before requesting new resource.

SRP 8. *Pattern ensures the atomicity of business transaction to protect the data integrity during its storage in the database.* A failure of single activity causes the transaction to abort abnormally resulting in writing conflicting data. It risks data integrity and leads business to malfunction strategies. This pattern proposes to implement an external mechanism to track transaction and invoke the compensation logic in case of failure to undo all the changes.

SRP 9. *Pattern secures multiple access to a shared data by protecting its integrity in TimeOfCheck/TimeOfUse (TOCTOU).* When several activities from different locations access the data in a single time, this risks the loss of data integrity that can lead business to malfunction strategies. To reduce the risk this pattern proposes to implement locking protocol on data accessibility.

SRP 10. *Pattern prevents the leakage of system information when an exception is thrown.* It addresses the problem of system information leakage, when run-time ex-

ception arises. The attacker can intentionally raise the exception to get internal system information i.e., application configuration, which help him to launch sophisticated attacks. To reduce the risk this pattern proposes to handle the errors and exceptions correctly.

3.2 Security Risk-oriented Pattern Example

This section presents an example of security risk-oriented pattern "*Securing data that flows between the business entities*". Its major structural details are defined textually in Table 1 and the graphical representation (BPMN using the alignment [5]) is illustrated in Fig. 2(a), 3(a) and 4(a).

Table 1. Security Risk-oriented Pattern (SRP1).

1. Organisational scenario & **Security context identification**		
Pattern name	Securing *data* that flow between the *business entities*	
Pattern description	This pattern secures the *data* transmit between the business entities	
Related pattern(s)	No related patterns	
2. Asset identification & **Security objective determination**		
Business Asset	*Data* submitted and employ by business	
IS Asset	*Input interface*, *Transmission medium* that transfers data and *business/server*	
Security criteria	–Confidentiality of data –Integrity of data	
3. Risk analysis & **assessment**		
Risk	An attacker intercepts the transmission medium and misuses the data leading to loss of data confidentiality or integrity.	
Impact	1. Harm of at least one business asset (i.e., harm of data submitted and stored in the database) 2. Harm of at least one IS asset (i.e., loss of reliability of the transmission medium) 3. Negation of security criteria (i.e., negation of data confidentiality and integrity)	
Event	An attacker intercepts the transmission medium due to its characteristics to be intercepted and misuses the data due to the lack of crypto-functionality at the input interface and server [18].	
Threat	An attacker intercepts the transmission medium and misuse the data.	
Vulnerability	– Characteristics of transmission medium to be intercepted [18] – Lack of crypto-functionality at input interface and server [18]	
Threat agent	An attacker with means to intercept transmission medium by acting as a proxy	
Attack method	1. Intercept transmission medium by establishing a proxy between input interface and server [1]. 2. Misuse data: (a) Capture, modify and pass data to the database. (b) Capture, read and keep data for the later use.	
4. Risk treatment & **Security requirements**		
Risk treatment	Risk reduction	Risk avoidance
Security requirement	– Make data unreadable to attackers. (Mitigates the risk of data confidentiality) – Verify the received data with the original. (Mitigates the risk of data integrity)	Change the transmission medium that does not have the ability to be intercepted
Control	– Cryptographic algorithm – Checksum algorithm	– Physically delivery of data. – Employee enters data.

In Table 1, the first part describes the pattern's name (see the entry *pattern name* and *description*). The *related patterns* entry could be used to link other related security patterns. The second part, called as *asset identification and security objective determination*, is used to define *business* and *IS assets*. Following the ISSRM domain model [8]

we identify *business assets* (i.e., data) and the *IS assets* defined in the pattern (i.e., input interface, transmission medium and business/server) which support business assets. *Security criteria* (i.e., confidentiality and integrity of data) are constraints on business assets and is presented in Fig. 2(a) using padlocks (adapted from [15]).

In ISSRM domain model [8], *risk* is a composition of impact, vulnerability, threat agent and attack method. In the SRP1 (see Table 1) we define that there might exist a threat agent (i.e., attacker) who has motivation and means (i.e., intercept transmission medium by acting as a proxy) to threatens the system. He is able to target the IS assets by exploiting the vulnerabilities (i.e., Characteristics of transmission medium to be intercepted and Lack of crypto-functionality at input interface and server). As the risk event happened it potentially leads to impact (listed in Table 1). The situation is illustrated graphically in Fig. 3(a) where *vulnerability* in an IS asset is represented by *asterisk* ($*$) (adapted from [9]). Such a model provide rationale for the security requirements defined later in Section 4 under *reasoning about security requirements*.

According to the ISSRM domain model [8], there exists 4 potential risk treatment decision (e.g., *avoidance, reduction, retention, or transfer*) choosing one or another decision influences the actual design of security countermeasures. In SRP1 (see Table 1), we introduce two alternative decisions i.e., *risk reduction* and *risk avoidance*, which are refined to different security requirements. In case of *risk reduction*, security requirements could be potentially implemented by cryptography or checksum algorithms. In the second case (i.e., *risk reduction*) security requirement (i.e., Change the transmission medium that does not have the ability to be intercepted) is implemented by introducing the physical data delivery. As analysed in [5], BPMN does not model ISSRM controls, however, the security requirements are potentially introduced using *combination of tasks, gateways and events* [5] or *business model is annotated* (adapted from [13]). We have used later approach to keep the business models simple for business analyst (see Fig. 3(a)).

4 Pattern Usability

To test the usability and performance of our approach we have applied the patterns to the business models of land management organisation. Major objectives to choose this example are: the complex execution of activities, large IT dependency and the data exchange between the stakeholders, and business model (see overall size description in Table 2) is expressed in BPMN. The research goal of this application is twofolds. Firstly, develop application guidelines for our patterns. Secondly, investigate the usefulness of our approach to discover potential security flaws and implements the countermeasures. We continue the application with the example pattern, SRP1 (see Table 1).

Table 2. Size of Land management organisation business models.

Processes	Sub-process	Events	Gateways	Pools	Tasks[1]	Message flows[1]	Sequence flows[1]
9	73	109	83	68	186	129	492

[1] In Section 4.2 we consider their sum to estimate the size of the business model.

4.1 Application Guidelines

Identifying Pattern. The first step is to identify the occurrences of security pattern in business model. This is a manual activity, that potentially requires a good comprehension of the modelled domain and problem. For example in Fig. 2(b) we illustrate an occurrence of SRP1. Here we could see the correspondence between the processes *log on to portal* (Fig. 2(b)) and *submit data* (Fig. 2(a)), since both these activities are about entering the data (i.e., *user log on details* in Fig. 2(b) and *data* in Fig. 2(a)) using their input devices (i.e., *lodging party* in Fig. 2(b) and *input interface* in Fig. 2(a)). Similarly there is a correspondence between processes *validate user* (in Fig. 2(b)) and *employ data* (in Fig. 2(a)). Since they both concern with the operations which employ the received data.

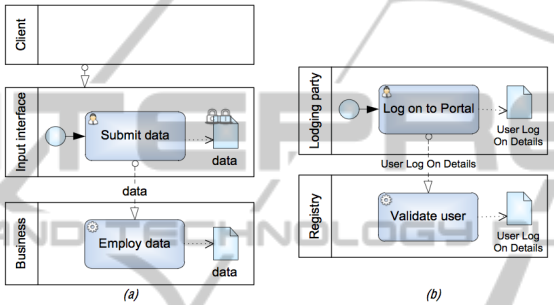

Fig. 2. (a) Organisational scenario (b) Pattern occurrence in business model.

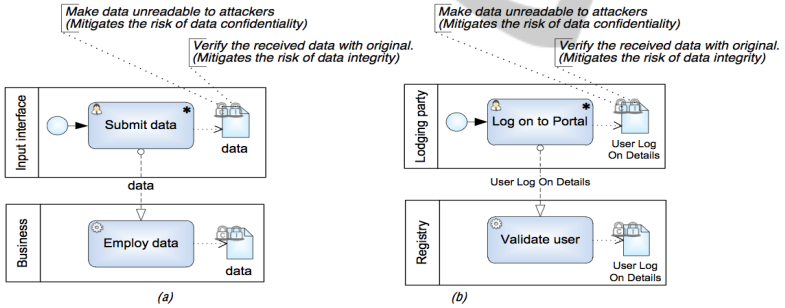

Fig. 3. Annotated *Security criteria* & *Security requirements* in (a) Security pattern, (b) Pattern's occurrence in business model.

Annotating Model with Security Criteria. After finding the pattern in the business model we potentially annotate assets that require security consideration. For example in Fig. 3(b) *user log on to details* is annotated with padlocks (that correspond to the ISSRM security criterion [5]) to highlight that it needs to be considered for *confidentiality* (C) and *integrity* (I).

Introducing Security Requirements. Next, the business model is annotated with security requirements (see Fig. 3(b)), derived when defining the security risk-oriented pattern. Alternatively, security requirements could be defined using combination of the task, gateway, event constructs as discussed in [5].

Reasoning about Security Requirements. Some security risk-oriented patterns have alternate risk-treatment decisions; for instance applying SRP1, different security requirements could be derived when selecting *risk reduction* or *risk avoidance*. Different requirements, result in different security controls (and thus, different system implementation). Selecting one or another risk-treatment is security trade-off that analyst should make. To support the decision on risk-treatment and to reason why security requirements are introduced, the risk analysis and assessment (for SRP1, see Table 1) could provide reasoning why one or another risk-treatment should be taken, or why security requirements should be considered when implementing the system. For example, taking into account SRP1, analyst could potentially comprehend (see Fig. 4(b)) how *user log on details* can be intercepted by an attacker.

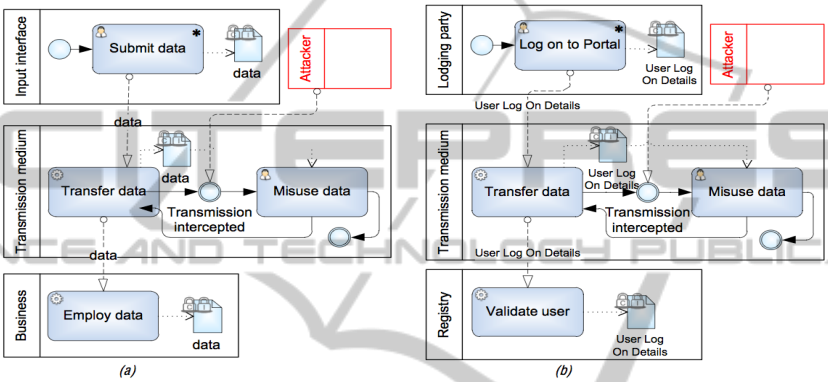

Fig. 4. (a) Pattern threat analysis (b) applied in the business model.

4.2 Pattern Occurrences

We have conducted analysis using all the ten patterns. The findings are illustrated in Table 3. In this table we report on an extend, at which the patterns influences the business process model. This extend is defined as a correspondence between the number of model elements considered by pattern (e.g., multiplication of total number of pattern constructs an number of model pattern occurrences in the model; in case of SRP1, 4 x 33 = 132) and size of the business model (which equals to a sum of *Tasks*, *Message flows*, and *Sequence flows*, 807, as defined in Table 3). Number of the pattern occurrences could suggest the amount of decisions, which analyst needs to make about the trade-offs of the security requirements (and their corresponding controls) in the business model. Furthermore, each pattern, as defined in [12] contributes to the mitigation of at least 1 or 2 security risks. Thus, having the number of pattern occurrences we potentially identify the number of risks that are possible to mitigate using our approach.

5 Discussion & Conclusions

5.1 Discussion

Currently business process models are mainly analyzed manually but the patterns provide a way to structure information (for SRP1, see Table 1). This creates the possibility

Table 3. Patterns' Occurences in Land management business model.

Pattern ID	No# of language constructs used to define pattern				No# of pattern occurrence in business model	An extend, at which pattern influences the business process model
	Task	Message flow	Sequence flow	Total		
SRP1	2	2	0	4	33	16%
SRP2	2	2	0	4	33	16%
SRP3	3	2	0	4	33	16%
SRP4	2	1	0	3	35	13%
SRP5	1	1	1	3	39	14%
SRP6	2	1	3	5	6	4%
SRP7	3	2	0	5	12	7%
SRP8	8	0	10	18	0	0%
SRP9	2	1	3	6	4	3%
SRP10	2	2	3	7	8	7%

to automate the process of searching patterns in business models. The patterns identification also depends on how the business processes have been modelled. If the business models include detail information then the patterns can be easily automated without requiring any manual efforts from the domain expert. The scope of our patterns are software errors described in taxonomy [18] therefore, the paper focuses on the IT security risks. There is no list of risks to compare the completeness of our patterns (e.g., how many risks are covered?). Although there are several surveys conducted to categorise the risks but usually they are subjective and focuses on system domain. Therefore, we calculate the completeness of patterns by comparing the 85 security errors described in the taxonomy [18] with the vulnerabilities identified in the security patterns. We keep in mind that there exists several other flaws but they are not currently analysed. The analysis of pattern' occurrences shows the patterns covered 68 vulnerabilities from 85 listed in taxonomy [18]. The remaining 17 vulnerabilities are tool dependent, therefore, it is not possible to address them. These occurrences are subjective, so it can vary from analysis to analysis.

5.2 Conclusions

In this paper we introduce security risk-oriented patterns to address security concerns. The patterns are developed taking into account the well-known taxonomy of security errors [18]. The pattern application results in a set of guidelines that business analysts can apply our method to understand the security risks and to envision costs and rationale for implementing these security decisions without asking for help from the security designer. Although the graphical pattern is defined using BPMN, this is not specific to any modelling language and other modelling languages could be used to create graphical pattern expressions, if these languages are understood in terms of the ISSRM domain model [8].

Our future work includes developing an approach for semi-automatic identification of these patterns in the business models. In addition we plan to equip the security patterns with the metrics for asset value, risk level and risk-treatment cost measurement to support the security trade-off analysis.

References

1. Common attack pattern enumeration and classification, available at http://capec.mitre.org/data/definitions/94.html
2. DCSSL EBIOS expression of needs and identification of security objectives (2004), available at http://www.bsi.de/english/gshb/manual/download/index.html
3. ENISA -inventory of risk assessment and risk management methods (2004)
4. Ahmed, N., Matulevičius, R.: A template of security risk patterns for business processes. In: Perspectives in Business Informatics Research, Riga, Latvia. pp. 123–130. Riga Technical University (2011)
5. Altuhhova, O., Matulevičius, R., Ahmed, N.: Towards Definition of Secure Business Processes. In: M. Bajec and J. Eder (Eds.): CAiSE 2012 Workshops, LNBIP 112. pp. 1–15. Springer-Verlag (2012)
6. 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 25, 101–117 (2007)
7. Devanbu, P. T., Stubblebine, S.: Software engineering for security: a roadmap. In: The Future of Software Engineering. pp. 227–239. ACM Press (2000)
8. Dubois, E., Heymans, P., Mayer, N.and Matuleviɣius, R.: A systematic approach to define the domain of information system security risk management. In: Intentional Perspectives on IS Engg., pp. 289–306. Springer (2010)
9. Elahi, G., Yu, E.: A goal oriented approach for modeling and analyzing security trade-offs. Security 4801(7), 375–390 (2007)
10. Firesmith, D.: Engineering safety and security related requirements for software intensive systems. In: Software Engineering - Companion. ICSE 2007 Companion. 29th International Conference on. p. 169. IEEE Computer Society (2007)
11. Jürjens, J.: Secure systems development with UML. Springer (2005)
12. Khan, N. H., Ahmed, N., Matulevičius, R.: Security Risk Oriented Patterns. Tech. rep., University of Tartu, Department of Computer Sciences (04 2012), http://www.cs.ut.ee/∼naved/Security_Risk_Oriented_Patterns.pdf
13. Paja, E., Giorgini, P., Paul, S., Meland, P. H.: Security requirements engineering for business processes. In: Perspectives in Business Informatics Research, Riga, Latvia. pp. 163–170. Riga Technical University (2011)
14. Pavlovski, C. J., Zou, J.: Non-functional requirements in business process modeling. In: Proceedings of the 5th Asia-Pacific conf. on Conceptual Modelling. pp. 103–112. APCCM, Australian Computer Society, Inc. (2008)
15. Rodríguez, A., Fernández-Medina, E., Piattini, M.: A bpmn extension for the modeling of security requirements in business processes. IEICE - Trans. Inf. Syst. 90-D(4), 745–752 (2007)
16. Röhrig, S., Knorr, K.: Security analysis of electronic business processes. Electronic Commerce Research 4(1-2), 59–81 (2004)
17. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering (2006)
18. Tsipenyuk, K., Chess, B., McGraw, G.: Seven pernicious kingdoms: A taxonomy of software security errors. IEEE Security & Privacy 3(6), 81–84 (2005)