Databases and Information Systems IX
G. Arnicans et al. (Eds.)

doi:10.3233/978-1-61499-714-6-129

Application of the Enterprise Model Frame for Security Requirements and Control Identification

Marite KIRIKOVA[a,1], Raimundas MATULEVICIUS[b], and Kurt SANDKUHL[c]
[a] *Department of Artificial Intelligence and Systems Engineering, Riga Technical University, Kalku 1, LV-1658, Riga, Latvia*
marite.kirikova@cs.rtu.lv
[b] *Institute of Computer Science, University of Tartu, J.Liivi 50409 2, 50409, Tartu, Estonia*
rma@ut.ee
[c] *Chair Business Information Systems, University of Rostock, Albert-Einstein-Str. 22, 18059 Rostock, Germany*
Kurt.Sandkuhl@uni-rostock.de

Abstract. It is generally accepted that security requirements have to be identified as early as possible to avoid later rework in the systems development process. However, in practice quite often security aspects are considered either at the later stages of development cycles (increments in agile projects) or addressed only when problems arise. One of the reasons for difficulties of early detection of security requirements is the complexity of security requirements identification. In this paper we discuss an extension of the method for security requirements elicitation from business processes (SREBP). The extension includes the application of the *enterprise model frame* to provide an enterprise architecture context for analyzed business process models. The enterprise model frame covers practically all concepts of the information security related definitions; the use of the frame with the SREBP method complies with the common enterprise modeling and enterprise architecture approaches; and it use helps to consider security requirements and control at the business, application, and technology levels simultaneously.

Keywords. Security requirements elicitation, business process models, enterprise modeling

Introduction

Security requirements elicitation is a part of security engineering that plays an important role in high quality system development [1]. Although the importance of introducing security engineering practices early in the systems development lifecycle has been acknowledged [2, 3], in practice security often is considered at the later stages of the lifecycle or when security problems arise in operations and maintenance. This either causes rework in initial designs and slows down the later stages of system

[1] Corresponding Author: Marite Kirikova.

development, or extends system maintenance with unplanned activities. Security has been subject of research during many years in different areas of business and information systems development including enterprise modeling [4]. Nevertheless, new approaches are continuously developed. This may be explained by the fact that, despite a large number of methods created in different research projects, it is still difficult to use them in practice.

In this paper we discuss how *information security solutions (i.e., security countermeasures) could be related to enterprise modeling*. The study was a part of the ITSE project[2], where the main goal was to transfer a method for Security Requirements Elicitation from Business Processes (SREBP) [5, 6] to the practice of small and medium-sized enterprises (SMEs). The SREBP method was applied to SMEs with well-defined processes and high awareness of the importance of well-defined security requirements. From discussions with the employees of one of the SMEs we learned that while in general the SREBP method was quite well appreciated by the enterprise, some underlying enterprise modeling was needed to support and structure the analysis. So the identification of appropriate enterprise modeling support for successful application of the SREBP method in SMEs was set as one of our research goals. To achieve this goal we applied the following research method consisting of four steps. First, we applied the SREBP method to understand the security requirements within some SMEs. As mentioned above - this resulted in the observation that some enterprise modeling support was needed for putting the SREBP method into the organizational context. Second, we analyzed information security definitions to highlight important enterprise modeling concepts. These concepts were then analyzed in the fourth step. Third, we surveyed related work on business process related security requirements identification to learn from this research about important enterprise modeling concepts that can support information security requirements elicitation. Fourth, taking into account the results from the second and the third steps we applied a particular *enterprise model frame* and verified it against security and enterprise modeling concepts. As the result we proposed the use of the enterprise model frame to establish the linkage between the security requirements elicitation from business processes and enterprise modeling. The research results were published in [7] where we have focused on the conceptual definitions. More specifically, we have identified and aligned concepts from enterprise modeling and information security, which are relevant for security requirements elicitation based on business processes. Next we have discussed theoretically the applicability of the business process-oriented security requirements elicitation together with enterprise modeling approaches.

In this paper we focus more on practical application of the enterprise model frame. We have applied the frame on business process models of several enterprises operating in different business domains such as information technology services, aviation, and education. The way how the frame is applied and the identified benefits are invariant regarding the business domains of the enterprise. Therefore, we include here the illustrative example of just one enterprise. The paper is structured as follows: In Section 1 we discuss security relevant enterprise modeling concepts and link them to the approaches for information security requirements identification. In Section 2 we show how theoretically the SREBP method can be extended with the enterprise model

[2] ITSE: "Improvement of IT-Security in Enterprises based on Process Analysis and Risk Patterns (ITSE)", involving university partners from: Estonia, Latvia, and Germany, URL: http://hochschulkontor.lv/en/projects/247

frame for more informed discussions about security requirements; and provide an illustrative example and discussion of practical usage of the frame. The applicability of the frame as an extension of the SREBP method is discussed in Section 3. In Section 4 we present conclusion and future work.

1. Background

There exist a number of approaches, methods, and methodologies proposed for security engineering. A comprehensive survey of these is available in [5]. In this section we will focus only on those approaches that utilize business process models or data flow diagrams. We deliberately limit our paper to this type of approaches because (1) our practical experience covers only business process analysis based approach to security requirements elicitation; and (2) business process models and data flow diagrams can represent information assets (on which we focus in this paper) that are to be secured when they are transferred from one process step (or function, or database) to another.

In Section 1.1 we discuss security relevant enterprise modeling concepts from information security, information, and data definitions. In Section 1.2 we address relevant enterprise modeling concepts from business process oriented security requirements elicitation approaches.

1.1. Enterprise Modeling Concepts in Information Security Definitions

In this section we consider some information security related definitions with the purpose of illustrating enterprise modeling concepts relevant for supporting information security requirements elicitation. The definitions are extracted from [8] (basic enterprise modeling related concepts are highlighted by *italic*):

- protection of *information* and *data* so that unauthorized *persons* or *systems* cannot read or modify them and authorized *persons* or *systems* are not denied access to them (ISO/IEC 12207:2008 Systems and software engineering–Software life cycle processes, 4.39);
- the protection of *computer hardware* or *software* from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to *personnel*, *data*, *communications*, and the physical protection of *computer* installations. (IEEE 1012-2012 IEEE Standard for System and Software Verification and Validation, 3.1);
- all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of a *system* (ISO/IEC 15288:2008 Systems and software engineering–System life cycle processes, 4.27);
- degree to which a *product* or *system* protects information and *data* so that *persons* or other *products* or *systems* have the degree of *data* access appropriate to their types and levels of authorization (ISO/IEC 25010:2011 Systems and software engineering–Systems and software Quality Requirements and Evaluation (SQuaRE)–System and software quality models, 4.2.6) Security also pertains to *personnel*, *data*, communications, and the physical protection of *computer* installations.

In ISO/IEC/IEEE 24765c:2014 information security is defined as follows: “Preservation of confidentiality, integrity, and accessibility of *information* <...> in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.” The concept "Accessibility" is closely related to the concept "Availability". In the context of security requirements elicitation from business processes using the enterprise model frame, we focus on the concepts *people*, *software*, *hardware*, and *information* and *data*. Concepts of *system* and *product* are also mentioned above in the definitions. However, the discussion of these two concepts is beyond the scope this research.

There are also definitions of *information*, utilized by some standards, where *information* is defined based on the notion *knowledge* but not on the notion of *data* that could be expected in information technology related contexts. The information is defined as:

- *knowledge* that is exchangeable amongst users, about things, facts, concepts, and so on, in a universe of discourse (ISO/IEC 10746-2:2009 Information technology–Open Distributed Processing–Reference Model: Foundations, 3.2.6);
- in information processing, *knowledge* concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context have a *particular* meaning (ISO/IEC 2382-1:1993 Information technology–Vocabulary–Part 1: Fundamental terms, 01.01.01) It is also important to note that although *information* should necessarily have *a representation* form in order to make it communicable, the interpretation of this representation (the *meaning*) is especially relevant.

The emphasis on knowledge requires considering *knowledge* as one more relevant enterprise modeling concept being utilized for information security requirements identification. Therefore, such elements and *official meaning* and *actors's meaning* are included in the enterprise model frame (see Section 2).

Finally, the definitions of *data* follow; according to them *data* is:

- a representation of facts, *concepts*, or instructions in a manner suitable for communication, interpretation, or *processing* by *humans* or by *automatic means* (ISO/IEC/IEEE 24765:2010 Systems and software engineering–Vocabulary);
- a collection of *values* assigned to base *measures*, derived measures and/or *indicators* (ISO/IEC 15939:2007 Systems and software engineering–Measurement process, 3.4);
- *a representations of information* dealt with by information *systems* and *users* thereof (ISO/IEC 10746-2:2009 Information technology – Open Distributed Processing – Reference Model: Foundations, 3.2.1);
- a re-interpretable *representation of information* in a formalized manner suitable for communication, interpretation, or processing. (ISO/IEC 25000:2014 Systems and software Engineering–Systems and software product Quality Requirements and Evaluation (SQuaRE)–Guide to SQuaRE, 4.4) (ISO/IEC 2382-1:1993 Information technology–Vocabulary–Part 1: Fundamental terms, 01.01.02).

From the point of view of enterprise modeling, it is important to highlight concepts of *concept*, *value*, and *measure*. However, they do not directly relate to security issues. Thus, only the notions *knowledge* and *meaning* have been utilized in the enterprise model frame.

1.2. Process Related Information Security Requirements Identification

There exist approaches for handling security concerns via business processes [4, 9] and to enforce information security by introducing security mechanisms [10, 11, 12]. For instance, the UMLsec approach [10] introduces stereotypes to define secure systems from business processes expressed in activity diagrams. Elsewhere security extensions [11, 12] to the BPMN language are proposed to define access control, separation of duties, and similar constraints.

DFD for security risk management. In [13] Spears proposes a holistic method for information systems risk identification. This approach is relevant to our work as it uses data flow diagrams (which are better equipped for information modeling than BPMN) and information systems architecture. The method identifies core business functions within the organization and their critical business processes. Then, for these business processes, the relevant information systems are found and the list of information technology assets is identified. These assets and the context, in which they are used, are modeled using Data Flow Diagrams that helps to update the list of information technology assets. The security decisions concerning the assets are made on the basis of envisioned risk scenarios.

Socio-technical systems model for eliciting security requirements. The Socio-Technical Systems model based approach [14, 15] is toll supported and uses the social view, the information view, and the authorization view that concerns goals and information units from the social and information views. The business process is designed according to and verified against security policies that are defined on the basis of security requirements.

SREBP. The SREBP method [6] has no tool support and has less graphical annotations than the approach proposed in [14] and [15]. However, the method is based on a generic threat model, takes into consideration assumed attacker capabilities, and suggests security risk oriented patterns to identify threats, to mitigate these threats by introducing security requirements (and their potential controls as constraints on the business process diagram). The SREBP method consists of two stages. In the first stage one has to identify business assets and determine security objectives. In the second stage, one applies the security risk-oriented patterns to:

1. Identify pattern occurrences in the business process model.
2. Extract the security model based on the pattern occurrences.
3. Derive (textual) security requirements from the graphical security model.

During the first step, one performs activities [16] to identify security risk-oriented patterns in the analysed business process model. Once the pattern occurrences are determined, one can extract the security model depending on the security risk-oriented pattern used. Typically this model is expressed using the (security extensions of the) UML modeling language. For instance, when applying a pattern for *securing data from unauthorised access*, one would need to create a UML class diagram describing the role-based access control model; an application of pattern for *securing data that flow between business entities* would result in the UML activity diagram describing the secure communication establishment. This also means that depending on the chosen contextual area (and its associated patterns) different activities for security model extraction could be performed. Once the security model is derived, one can document security requirements textually.

Using the SREBP method, the business process model is a primary source for deriving information security requirements, like the data flow diagram in the DFD based security risk management [13]. Also [14], [15], and [17] demonstrate that in practical settings, the business processes are a convenient abstraction level for discussing information security issues. Therefore, taking into consideration that the business process based security requirements elicitation considers information flows in business processes, the extension of the SREBP method was developed for relating information flows in a business process model to the specific enterprise model element structures–the enterprise model frames. The proposed extension is described in the next section.

2. Relating Business Processes to Enterprise Model Frames

In this section we show, how the enterprise model frame extends the SREBP method. In Section 2.1 the theoretical background is explained and in Section 2.2 the illustrative example is given.

2.1 Extending SREBP with the enterprise model frame

In the SREBP approach [18], five security risk-oriented patterns are defined to derive security requirements from business processes. These patterns are based on the domain model for Information Systems Security Risk Management (ISSRM) [19] that supports the definitions of asset-related concepts, risk-related concepts and risk treatment-related concepts. The patterns are used within five contextual areas (i.e., one pattern in each area), such as access control, communication channel, input interfaces, network infrastructure, and data store. Pattern application is performed in three steps:

1. *Pattern occurrence identification* in the business process diagram. Pattern identification potentially could be performed using hierarchical level matching, business perspective matching, structural similarity and semantic similarity methods [16]. Once the pattern occurrences are found in the business process model, the second step – security model extraction – is performed.
2. *Security model extraction* is performed following the activities, which differ from pattern to pattern. For instance, to create a security model within the access control contextual area, one has to (i) identify resource, (ii) identify roles, (iii) assign users, (iv) identify secured operations, and (v) assign permissions.
3. *Security requirements derivation* from the security model. Typically, the security requirements are expressed as conditions that need to be fulfilled by implementing security controls (i.e., countermeasures).

Although *security model extraction* (i.e., Step 2) differs for each pattern, the information object (i.e., business asset, how it is addressed in the SREBP approach) is always identified in the BPMN diagram when applying each pattern. To improve the clarity with respect to this asset, we related the BPMN model to the enterprise model frame, used for the analysis of information circulation in viable systems [20]. The enterprise model frame[3] is illustrated in Figure 1 (see the right-side of the figure). Here, it is used to distinguish between various types of information processors (e.g., human, software, and hardware). The frame also helps to separate the levels of security required (e.g., Business, level, Application level, and Technology level). Additionally, the frame illustrates what relationships in the enterprise model should be activated for the particular information object during its transfer from one activity to another. For instance, when sending an e-mail message, only business actors, information representation, e-mail system (application) and hardware are involved; while when transferring the paper format data that is stored in the database, all elements reflected in the frame might be involved. The enterprise model frame helps visualizing concerns important in security requirements identification.

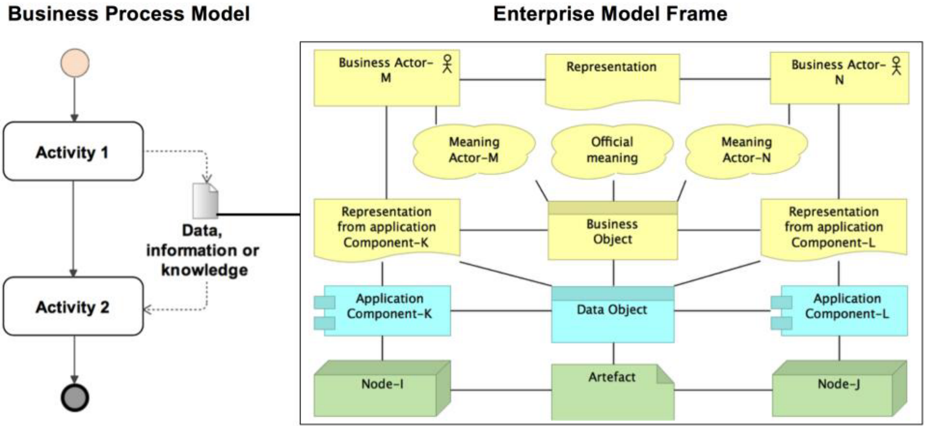

Figure 1. Security Requirements Elicitations Supported by Enterprise Model Frame (adopted from [7], represented in ArchiMate language [21])

The frame also could extend the data flow based approach with reference to business level elements. The compliance of the frame to ArchiMate language and enterprise modeling methods suggests an opportunity to extend the SREBP patterns to security goals and other concepts if these are present in the enterprise architecture or enterprise model. In Section 3 we will discuss the usefulness of the frame with respect to the SREBP method in more detail.

2.2 Illustrative Example

The illustrative example presented here concerns application of SREBP method in the case study used for the evaluation of the SREBP method at an executive department of the University of Rostock, called HQE [22]. HQE handles topics like quality management and controlling in study. Supporting university management and faculties regarding the installation of new study courses and teaching modules or reorganization of existing studies is another duty of the department. Since HQE plays an important

[3] In security requirements elicitation context, the enterprise model frame was presented in [7]

role in most of the business processes, a new online database has been developed that makes the whole process easier and clearer due to the fact that not only members of the HQE can access it but also the faculties, professors, and students regarding their rights.

A simple scenario from the case study is presented in Figure 2. Here the Responsible Professor enters a new teaching module (see *process* Enter new module) to the University DBMS[4]. Once the data is received (see event Request to enter new module received) to the server, the new course entry is created (see *process* Create new study course) in the Module data store. Hence, the *data object* New module could be captured and expanded as the Enterprise Model Frame, as illustrated in Figure 3.

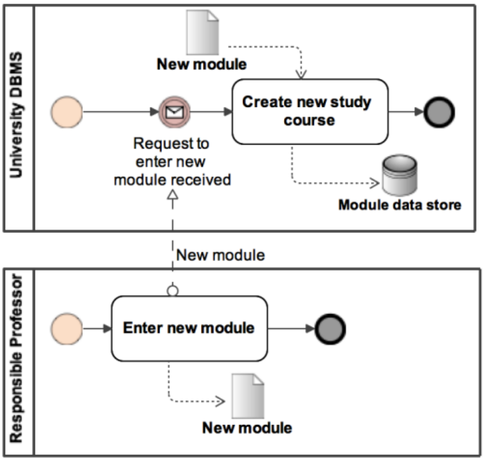

Figure 2. Business Process Model (and extract of the University Study System)

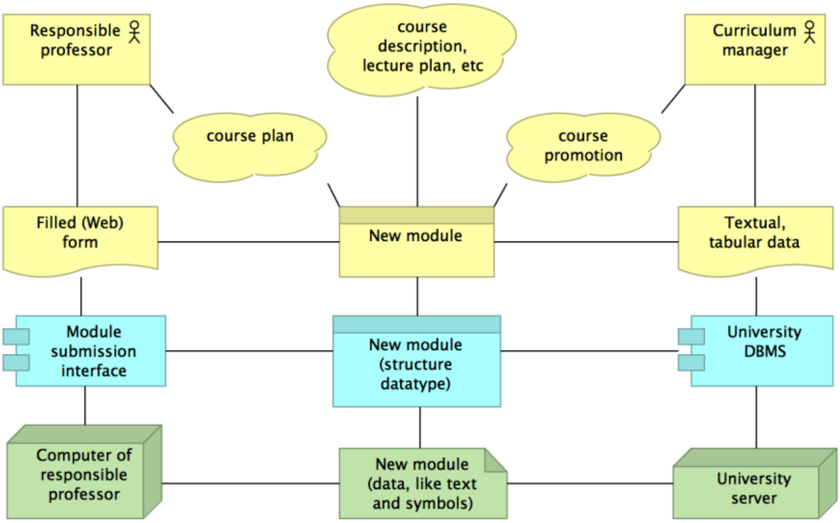
Responsible professor
course description, lecture plan, etc
Curriculum manager
course plan
course promotion
Filled (Web) form
New module
Textual, tabular data
Module submission interface
New module (structure datatype)
University DBMS
Computer of responsible professor
New module (data, like text and symbols)
University server

Figure 3. Enterprise Model Frame for the New module (and extract of the University Study System)

[4] DBMS = database management system. The University DBMS basically is a software module from the university-wide campus management system. This module is used for managing essential data structures and records.

The central element in Figure 3 is *business object* New module. It could have different meanings depending on the perspective of the *business actor*. For example, Responsible actor understands new module as the course plan; then the Curriculum manager sees it as the course promotion material. At the application layer the New model is treated as the data object taking emphasis on its structure and used data types. It is handled both by the *application components*, such as Module submission interface and University DBMS. At the technology layer the New module is treated as artifact, handled by architectural nodes, such as Computer of the responsible professor and University server.

Application of the security risk-oriented patterns (SRP) results in introduction of new business tasks as reaction to *security requirements*. For instance, Figure 4 illustrates introduction of security requirements derived after application of SRP1: *Securing data from unauthorized access* and SRP2: *Ensuring secure data transmission between business entities*. SPR1 helps to derive security requirement Check access rights. After applying SRP2, one can derive requirements to Make new module unreadable, to Make the new module readable and to Verify new module with original.

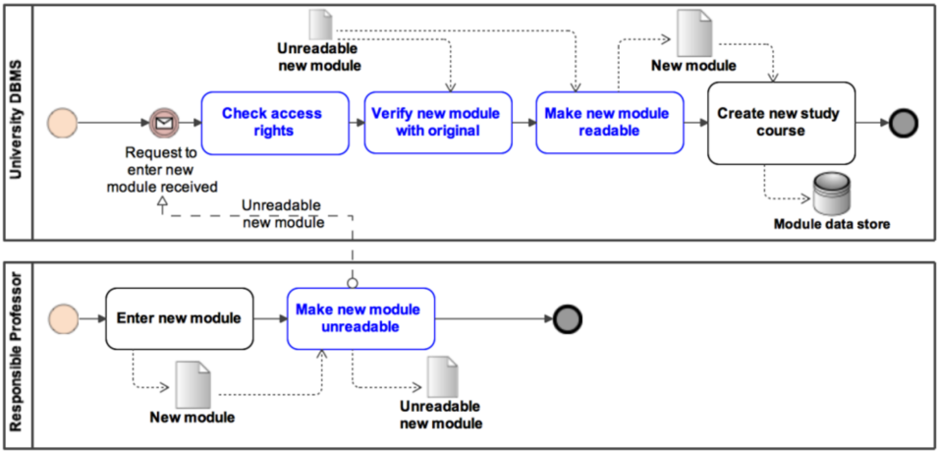

Figure 4. Introduction of New Business Tasks after Application of SRPs

The newly introduced business tasks also influence the representation of the enterprise frame. Figure 5 presents the updated enterprise frame for the new module. In the updated enterprise model frame the new *application component* Check access module is defined and linked to the Responsible professor, indicating that his access rights should be checked before creating the new study course. Similarly, the new *representation* Unreadable new module of the *business object* New module is created to indicate that it is being manipulated during the process. This representation is then linked to the *application components* Encrypt module, Decrypt module, and Check sum module.

The illustrative example presented in this section shows that the enterprise frame helps defining *security controls* (for example, as the *application components*), which must be implemented once security requirements are derived using security risk-oriented patterns. These security requirements could be incorporated to the system architecture. This helps to illustrate how security countermeasures contribute to the developed system, how they could be linked to other system components, and how they could ensure the required level of the developed system security. On the other hand, the enterprise model frame gives an opportunity to take into consideration also such security measures that does not concern information technology issues, e.g., access to manual documents that are stored in offices of employees, or, in other business domains (like aviation), access to storages of physical things.

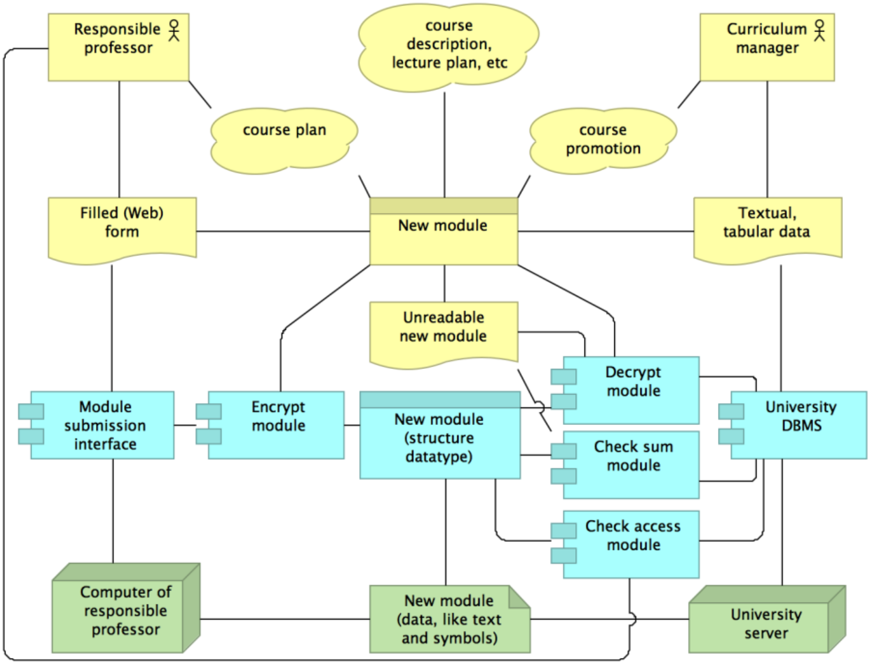

Figure 5. Updated Enterprise Model Frame for the New module

3. Usefulness of the Enterprise Model Frame for SREBP

The usefulness of the enterprise model frame application to extend the SREBP method for security requirements and control identification can be considered from the following perspectives:

1. Compliance with enterprise modeling concepts with respect to security definitions (also see Section 1.1).
2. Compliance with enterprise architecture elements directly related to the SREBP patterns.
3. Compliance with enterprise modeling approaches.
4. Practical application.

From the first perspective, comparing the enterprise modeling related concepts revealed in security oriented definitions with the elements presented in the enterprise model frame, we can see that the enterprise model frame covers practically all concepts revealed from different definitions presented in Section 1.1 [7]. The only exception is the *Knowledge* concept. However, it can be directly related to the *Actor's* concept; and also the *Meaning* concept can be used as a "synonym" of *Knowledge* (assuming that the *Meaning* is explicitly represented, i.e., expressed by a conceptual structure or sub-ontology). This observation indicates that the enterprise model frame will allow one to express all the main concepts related to security, thus, exposing a certain level of conceptual completeness with respect to security concepts.

Concerning the *second perspective*, we first can consider the alignment between concepts of SREBP patterns and enterprise architecture concepts expressed in ArchiMate [23], and then compare the enterprise architecture concepts, which corresponded to the security patterns, to the concepts of the enterprise model frame reflected in Figure 1. Analysis reported in [24] concludes that the expression of the SREBP patterns concerns all enterprise architecture layers, including Business layer, Application layer, and Technology layer, represented in ArchiMate. The correspondence between the concepts of the enterprise model frame and the concepts of enterprise architecture identified in [24] is reflected in detail in [7], where it is indicated that the enterprise architecture concepts identified in [24] are similar to the concepts used in the enterprise model frame. However, the concepts of the enterprise model frame are more *actor-oriented* than the concepts identified by [24]. In the enterprise model frame there is *Business actor* instead of *Business role*, which is identified in [24]; and the concepts of the enterprise model frame require considering *representation* and *meaning* of business objects. The use of the enterprise model frame also requires more thorough analysis at the Application level of the enterprise architecture to compare to what is intended in [24], because in the proposed enterprise model frame particular Application components are also concerned, while in the [24] only Data objects were identified at the Application layer of the enterprise architecture.

There are also concepts that are not considered in the enterprise model frame, but were identified in [24] at the Business layer of an enterprise's architecture, namely, the enterprise model frame does not consider such concepts as Business event, Business process and Function identified in [24]. Thus, we can see that the use of the enterprise model frame in the SREBP method is possible, because (1) there is a possibility of relating the frame to the enterprise architecture elements relevant to particular security risk-oriented patterns via Data object, Artefact, and Device and (2) it is possible to establish the relationship between Business role and Business actor as well as the relationship between Representation and Business Object. The use of the enterprise model frame makes the analysis of the security risk-oriented patterns and related security requirements more concrete as it prescribes consideration of specific enterprise actors and their understanding of the situation (see Representation concept and Meaning concept in the frame) addressed by the security-oriented pattern. However, the frame does not include all concepts of the enterprise architecture related to the security patterns, therefore, for elicitation of security requirements, it should not be separated from the SREBP patterns.

Regarding the compliance of the enterprise model frame with enterprise modeling methods (*the third perspective*), we can see that the enterprise model frame (Figure 1) consists of concepts adopted from the ArchiMate language [21], which is used in enterprise modeling and enterprise architecture management. In addition the frame is well aligned with contemporary enterprise modeling methods (e.g., 4EM [23]). From the point of view of enterprise modeling, the SREBP method extended with the enterprise model frame is conceptually richer than the approach used in [13], since the Business layer, Application layer, and Technology layer of the enterprise architecture are taken into consideration instead of just information systems architecture addressed in [13]. The frame also allows representing knowledge issues (via meaning), which by definition (Section 1.1) are important in information security requirements identification, but are currently scarcely addressed in other business process oriented security requirements elicitation approaches.

From the fourth (practical usage) perspective, the application of the enterprise model frame together with the SREBP method is rather comprehensible and easy. The illustrative example presented in Section 2.2 shows that the frame is useful for looking at the security issues from business, application and technology perspectives, thus, having a holistic view on the security issues. It also helps to interpret the security requirements in enterprise architecture terms and illustrate in advance the difference between enterprise architecture before and after the fulfillment of security requirements.

The above discussion shows that working with the enterprise model frame is useful and it does not contradict holistic [13] and socio-technical-systems model based [14, 15] methods of information security requirements elicitation. The enterprise model frame might potentially be helpful in supporting these methods; however, further research is needed to understand whether it is applicable for security requirements elicitation outside the context of the SREBP method.

4. Conclusions and Future Work

In this paper we discussed how to enrich security requirements elicitation from business process models using enterprise modeling. We considered theoretical concepts of information security definitions and current business process-oriented security requirements elicitation approaches. Our study resulted in the application of the *enterprise model frame*, which is based on the ArchiMate modeling language and complies with the common enterprise modeling methods. In the paper we discussed the conceptual basis of the enterprise model frame, its application example, and its usefulness as an extension the SREBP method, which is of one the business process based security requirements identification methods. We have concluded that the use of the enterprise model frame as an extension to the SREBP method is useful as it can bridge the security requirements and control elicitation from business processes and enterprise modeling for the following reasons:

- the enterprise model frame covers practically all concepts identified in theoretical analysis of information security related definitions;
- the enterprise model frame complies with common enterprise modeling and enterprise architecture representation approaches;
- the enterprise model frame gives an opportunity to have a holistic view on business, application and technological issues of security;
- the enterprise model frame gives an opportunity to show security control (e.g., as application components) necessary to support identified security requirements.

At the current state the enterprise model frame is theoretically validated against the basic concepts of information security and some contemporary enterprise modeling approaches. Some practical experiments in different business domains have been performed. The experiments of the enterprise frame application for the SME's processes and procedures, represented in business process modeling language BPMN 2.0, indicated that it is rather easy to use the frame by analysts having knowledge of enterprise modeling, business process modeling, and security requirements engineering. Future work involves further experiments with the enterprise model frame for security requirements elicitation and tool development to further simplify security requirements and control identification; as well as the comparison of the enterprise architecture frame extended SREBP method with a larger scope of security-oriented approaches (also beyond the ones directly utilizing business processes) in order to enrich the method, if applicable, with useful new features.

Acknowledgements

The research reflected in this paper was supported in part by the Baltic-German University Liaison Office, German Academic Exchange Service (DAAD), with funds from the Foreign Office of the Federal Republic Germany and in part by the Latvian Council of Science grant for project No 342/2012, and in part by the Latvian National research program SOPHIS under grant agreement No 10-4/VPP-4/11.

References

[1] Firesmith, D.: Engineering Safety and Security Related Requirements for Software Intensive Systems. In: ICSE 2007 Companion, p. 169. IEEE (2007)
[2] Jürjens, J.: Secure Systems Development with UML. Springer (2005)
[3] Sindre, G., Opdahl, A.L.: Eliciting Security Requirements with Misuse Cases. Requirements Engineering 10(1), 34–44 (2005)
[4] Muñante, D., Chiprianov, V., Gallon, L., Aniorté, P.: A Review of Security Requirements Engineering Methods with Respect to Risk Analysis and Model-Driven Engineering. In: Availability, Reliability, and Security in Information Systems, Lecture Notes in Computer Science, vol. 8708, pp. 79–93 (2014)
[5] Ahmed, N.: Deriving Security Requirements from Business Process Models, PhD thesis, University of Tartu, 2014
[6] Ahmed, N., Matulevičius, R.: Presentation and Validation of Method for Security Requirements Elicitation from Business Processes. In: Information Systems Engineering on Complex Environments, CAiSE Forum 2014, Selected extended papers, Springer LNBIP, pp. 20–35, 2015.
[7] Kirikova, M., Matulevičius, R., Sandkuhl, K.: Enterprise Model Supported Security Requirement Elicitation from Business Processes, In: Databases and Information Systems, Springer International Publishing, vol. 615, pp. 229–241 (2016)
[8] Software and Systems Engineering Vocabulary, http://pascal.computer.org/sev_display/index.action (2015)
[9] Leitner, M., Miller, M., Rinderle-Ma, St.: An Analysis and Evaluation of Security Aspects in Business Process Model and Notation. In: Proceedings of the Eighth International Conference on Availability, Reliability and Security (ARES), 2013, pp. 262–267 (2013)
[10] Jürjens, J.: Developing Secure Systems with UMLsec from Business Process to Implementation, Verlässliche IT-Systeme 2001, DuD-Fachbeiträge, pp. 151–161(2001)
[11] Brucker, A., Hang, I., Lückemeyer, G., Ruparel, R.: SecureBPMN: Modeling and Enforcing Access Requirements in Business Processes. In: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT'12), pp. 123–126 (2012)
[12] Rodriguez, A., Fernandez-Medina, E., Piattini, M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE-TIS(4), pp. 745–752 (2007)
[13] Spears, J.L.: A Holistic Risk Analysis Method for Identifying Information Security Risks. In Security Management, Integrity, and Internal Control in Information Systems IFIP International Federation for Information Processing, vol. 193, pp. 185–202 (2006)

[14] Salnitri, M., Dalpiaz, F., Giorgini, P.: Modeling and Verifying Security Policies in Business Processes Enterprise. In: Business-Process and Information Systems Modeling, Lecture Notes in Business Information Processing, vol. 175, pp. 200–214 (2014)

[15] Salnitri, M., Paja, E., Giorgini, P.: Preserving Compliance with Security Requirements in Socio-Technical Systems, Cyber Security and Privacy, CCIS 470, Springer, 2014, pp. 49–61(2014)

[16] Ahmed, N., Matulevičius, R.: A Taxonomy for Assessing Security in Business Process Modeling. Proceeding of RCIS, 2013: IEEE, pp. 1–10

[17] Weske, M.: Business Process Management: Concepts, Languages, Architectures. Springer (2012)

[18] Ahmed, N., Matulevičius, R.: Securing Business Processes Using Security Risk-oriented Patterns. Computer Standards and Interfaces 36(4), pp. 723–733 (2014)

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

[20] Kirikova, M., Pudane, M.: Viable Systems Model Based Information Flows. In: New Trends in Databases and Information Systems. Advances in Intelligent Systems and Computing, vol. 241, Part 1, Springer, pp. 97–104 (2014)

[21] ArchiMate 2.1 Specification, Open Group (2013), http://pubs.opengroup.org/architecture/archimate2-doc/

[22] Schiller, R., Blum, O.: Analysis of Security Requirements in Business Processes: Evaluation of SREBP, University of Rostock (2016)

[23] Sandkuhl, K., Stirna, J., Persson, A., Wißotzki, M.: Enterprise Modeling Tackling Business Challenges with the 4EM Method, Springer (2014)

[24] Cjaputa, K.: Business Process Based Introduction of Security Aspects in Enterprise Architecture, Master Thesis, RTU (2016)