Realia et naturalia

DISSERTATIONES
MATHEMATICAE
UNIVERSITATIS
TARTUENSIS
92

NAVED AHMED

Deriving Security Requirements from Business Process Models

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS
92

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS
92

NAVED AHMED

Deriving Security Requirements from Business Process Models

UNIVERSITY OF TARTU
PRESS
1632

Institute of Computer Science, Faculty of Mathematics and Computer Science, University of Tartu, Estonia.

Dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (Ph.D.) on October 31, 2014, by the Council of the Institute of Computer Science, University of Tartu.

Supervisors:

Assoc. Prof. PhD.	Raimundas Matulevičius Institute of Computer Science University of Tartu, Tartu, Estonia
Prof. PhD.	Marlon Dumas Institute of Computer Science University of Tartu, Tartu, Estonia

Opponents:

Prof. PhD.	Andreas L. Opdahl Department of Information Science and Media Studies University of Bergen, Bergen, Norway
Assoc. Prof. PhD.	Rafael Accorsi Department of Telematics University of Freiburg, Freiburg, Germany

The public defense will take place on December 16, 2014, at 16.15 in Liivi 2-404.

The publication of this dissertation was financed by Institute of Computer Science, University of Tartu.

ISSN 1024-4212
ISBN 978-9949-32-716-4 (print)
ISBN 978-9949-32-717-1 (pdf)

University of Tartu Press
www.tyk.ee

Abstract

The past couple of decades have seen enterprises deploy increasingly sophisticated methods for supporting their business processes by means of information systems. Moreover, given the dynamic business environment that the digital economy has brought about, enterprises need to continuously evolve their business processes and supporting information systems in order to cope with market changes and to take advantage of technology innovations. This confluence of factors has heightened the need for efficient and reliable approaches to identify security objectives for information systems and to map these objectives into security requirements.

Existing methods for security requirements analysis in information systems focus on eliciting security objectives and requirements at the level of individual functions. However, the complexity and rate of change of modern business processes requires a more holistic approach, wherein security objectives and requirements are elicited at the level of end-to-end processes.

In this setting, this thesis presents and evaluates a method for deriving security objectives and requirements from business process models. The thesis starts by proposing an alignment between concepts from security risk management and business process modeling concepts. From this analysis, a set of security risk-oriented patterns is developed to facilitate the elicitation of security objectives from business process models. These security patterns are classified via a taxonomy that helps analysts to apply these patterns in business process models.

These contributions form a foundation for a method called SREBP Security Requirements Elicitation from Business Processes. The method facilitates early security analysis by eliciting the security objectives from business process models and their systematic translation to security requirements. The SREBP method is validated on a case study within the Estonian Genome Centre. The results show that the SREBP method improves security requirements elicitation from business process models.

Acknowledgements

These past four years have greatly enriched my experiences, both within the field of my research and my life experience. This would not have been possible without the support and encouragement of family, friends and co-workers. I am grateful to my supervisor Raimundas Matulevičius for introducing me to the topic of security risk management, and for guiding me towards my first publications. Without his guidance and support, this thesis would not have been completed. I would also like to extend my warmest gratitude to Marlon Dumas for providing insightful criticism to remove the lacunae during this work and made sure that my research stayed focused and constructive. I would specially like to thank Fredrik Milani for the wonderful collaboration, all the discussions (scientific and social) and valuable suggestions he offered. I would also like to thank Rafik Chaabouni, who played a key role in balancing work and fun for the past three and half years. I am also grateful to the reviewers of my thesis, for their feedback and comments that have noticeably improved my thesis.

I wish to extend a special thanks to my parents, brothers and friends for their continuous support. Their repeated enquiries encouraged me to continue with my research, even when (and especially) at times when my morale was getting low. Finally, I wish to express my deepest gratitude to Maria, for bearing with me, for her appreciation when things were good and her unfailing encouragement and support when I faced challenges during my research.

This research was supported by European Social Fund via DoRa Programme and Estonian Research Council via grant ETF8704.

Publications Included in this Thesis

The publications included in thesis are listed below.

1 Ahmed, N., Matulevičius, R. (2014). Securing Business Processes using Security Risk-oriented Patterns. Computer Standards and Interfaces, 36(4), 723-733.

2 Ahmed, N., Matulevičius, R. (2013). A Taxonomy for Assessing Security in Business Process Modelling. In: 2013 IEEE Seventh International Conference on Research Challenges in Information Science (RCIS): 2013 IEEE Seventh International Conference on Research Challenges in Information Science (RCIS). IEEE, 1-10.

3 Matulevičius, R., Ahmed, N. (2013). Eliciting Security Requirements from the Business Process Using Security Risk-oriented Patterns. it - Information Technology, 55(6), 225-230.

4 Ahmed, N., Matulevičius, R., Milani, F. Security Requirements Elicitation from Business Processes (SREBP). *Submitted to Requirement Engineering Journal.*

Contents

List of Figures

Acronyms

AS/NZS	Australian/New Zealand Standards
BSI	Bundesamt für Sicherheit in der Informationstechnik
BPM	Business Process Management
BPMN	Business Process Model and Notation
CC	Common Criteria
CCTA	Central Computer and Telecommunication Agency
CIA	Confidentiality Integrity Availaibility
CORAS	Risk Assessment of Security Critical Systems
CRAMM	CCTA Risk Analysis and Management Method
DNS	Domain Name System
DoS	Denial of Service
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EPC	Event-Driven Process Chain
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSRM	Information System Security Risk Management
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
MEHARI	MEthode Harmonisée d'Analyse du Risque Informatique

KAOS	Knowledge Acquisition in Automated Specification
MOF	Meta Object Facility
MSRA	Multilateral Security Requirements Analysis
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
RBAC	Role-Based Access Control
SQUARE	Security QUAlity Requirements Engineering
SREBP	Security Requirement Elicitation from Business Processes
SROMUC	Security Risk-Oriented MisUse Cases
SRP	Security Risk-oriented Pattern
SP	Special Publication
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TR	Technical Report
TCP	Transmission Control Protocol
UML	Unified Modelling Language
WFMS	Work Flow Management System

Part I

Overview

Chapter 1

Introduction

As enterprises rely on their information systems to perform their business activities, the security concerns also grow to execute these business processes securely. A study from a business process magazine [Harm 10] states that more than 70% of business processes are deployed on information systems that are responsible for executing their business functions. Nowadays, enterprises operate in such an environment that requires flexible adoption of their systems to the dynamic changes and their easier integration of external resources. These challenging demands have increased the security needs of an enterprise [Bohr 13]. Furthermore, the nature of inherent risks lies in the routine operations and interactions with stakeholders, this makes the enterprises vulnerable to potential security risks. In today's business, the security of information systems is not only restricted to secure enterprise's assets from harm; but the enterprises must comply to the international security standards and also guarantee that these standards are strictly followed in executing their processes. At least the system should detect the occurences of any violation [Hamm 07, Bohr 13]. These assurances are required in today's business environment to develop a certain kind of trust with the business partners; otherwise no business transaction would take place at all [Tsia 05, Smit 14]. In [Schn 09], Schneier mentioned that a security is not a single product that can be added to the system and make it secure. Instead, it is a thorough process that analyses the enterprise's security needs, defines policies, implements the countermeasures, their validation, and reviews them periodically.

It is widely recognised that an insecure execution of enterprise's business processes can have devastated consequences [Acco 13]. The need for executing the enterprise's business processes is rising steadily. This trend demands a systematic

approach to determine the enterprise security needs for their information system, and their translation to security requirements that support the secure execution of their business processes. To consider this need, the approach taken in this thesis is to analyse the business processes from a security perspective. The analyses identify the enterprise's assets, determine their security objectives, and elicit security requirements to ensure their security during the execution of business process.

1.1 Problem Statement

Security engineering plays an important role to lower the risk of intentional harm to valuable assets to an acceptable level by preventing and reacting to malicious harm, misuse, threats and security risks [Fire 07]. Although the importance of introducing security engineering practices early in the development cycle has been acknowledged [Sind 05, Jurj 05], it has been oversighted in business processes and targets the improvement of business functions. The reason behind is that the business analysts are experts in their domain but having no clue about the security domain [Rodr 07]. There have been several attempts to engage the relatively matured security requirements engineering in business processes. However, the majority of studies either focuss on the graphical representation of security aspects in business process models [Menz 09, Mull 11, Pavl 08, Rodr 07] or enforce the security mechanisms [Herr 06, Wolt 09] or both [Mona 12, Rohr 04]. These studies have neglected the security requirements elicitation. The major problems in addressing security engineering in business process modelling are the following: firstly, the security requirements are specified in terms of security architectural design (i.e., security control) and missing the rationale about the trade-offs of the security decision; secondly, the requirements elicitation is either missing or haphazard that leads to miss some critical security requirements; and finally, due to the dynamic and complicated nature of business processes the studies only address varying aspects (i.e., authorization, access control, separation of duty or binding of duty) but not the overall security of business processes. These problems can be overcome by eliciting security objectives from the organizational business processes and by transforming them to the security requirements of the operational business processes where the technology supports the business processes execution. The thesis aimed at integrating security in business processes to facilitate business analyst in eliciting security requirements from business process models.

1.2 Scope of the work

This work stands in the business-process-security domain. In this section, we define the concepts and the boundaries of the thesis work.

1.2.1 Business Processes

Business processes have several definitions [ENV 95, Verg 08, Duma 13] in the literature. The definition of business processes related to the domain applied in the thesis is provided by Weske [Wesk 12] "a business process consists of a set of activities that are performed in coordination in an organisational and technical environment. These activities jointly realise a business goal."The domain of this thesis encompasses not only the activities within an enterprise whose execution is supported by the information system or its architecture, but also takes care of individuals and business partners coordinating with an enterprise's information system to achieve the business goals of enterprise. For means of this thesis, we use an artefact, business process model, to describe business processes. The thesis uses Business Process Model and Notation (BPMN) Version 2.0 as a modelling language. However, contributions (described in Section 1.3) are independent of any modelling language and are applicable to any ways of describing a business process.

1.2.2 Security Risk Management

A security approach used in this thesis is security-risk based. Therefore, the domain comprised of both the security and risk management. In the literature, security is understood in two different ways [Maye 09]. Firstly, the approaches [Fire 03a] that concern with deliberate harm on the information systems use the term *security*. Secondly, the approaches that concern with accidental harm to the information systems use the term *safety*. Similarly, another study [Fire 07] considers a broader notion that covers both the security and safety under the term *defensibility*. The notion of security that we adopt in this thesis, and that defines the scope, is the deliberate or intentional harm to the information systems.

There exist several definitions of risk in different standards. We adapted the domain model [Dubo 10, Maye 09] for information systems security risk management (ISSRM). In the ISSRM domain model (see Section 2.2.1), risk is defined as a combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. In this work, negative impact is considered in terms of information system's functionality that it could not able to provide in

the event of a successful attack rather than evaluating the monetary impact of risk on the asset. Similarly, risk management is defined as coordinated activities to direct and control an enterprise with regard to risk [ISOI 02]. In an enterprise, the risk management can address various kinds of issues [The 01, ISO 04] related to their enterprise's management (e.g., illness of a key person), finance (e.g., related to investment), environment (e.g., pollution), or security. The risk management in this thesis includes only those risks that are in the context of an information system related to the enterprise's business process execution.

Thus, the security risk management adopted in this thesis is defined as the coordinated activities to direct, prevent and control the risks, to an enterprise, caused deliberately by an insider or outsider to harm the enterprise asset(s) during the execution of their business processes.

1.3 Contribution and Research Questions

The thesis contribution aims at proposing a method for security requirements elicitation from business processes that enable business analysts to understand the security needs and define security requirements for their system-to-be. This thesis focusses on aligning modelling languages used in security engineering domain and business processes modelling. More specifically, the research question addressed in this thesis is:

How to identify assets and their security criteria in the enterprise's business processes, and to elicit security requirements for the information system in order to protect these assets?

The answer to this research question comprises of the following contributions proposed in this thesis. First, a set of security risk-oriented patterns [Ahme 14b] are developed to systematically integrate the security requirements into a business process. The contribution started by investigating the overlaps between security engineering and business process modelling. The investigation results in aligning the constructs in business process modelling language with the key concepts of security domain and identifies the shortcoming of business process modelling language in expressing security-risk related concepts [Altu 12]. The alignment gives a grounded and fine-grained reasoning for extending the business process modelling language to address these limitations. These extensions [Altu 13] are used in security risk-oriented patterns to express business assets and their security criteria, potential security risks, and their countermeasures. The security patterns facilitate the elicitation of security concerns by identifying assets from business

processes and determine their security objectives, followed by risk analysis that introduces security rationale and identifies the security requirements as constraints on assets. The idea is to facilitate business analysts by reusing solutions already implemented independently or to elicit different aspects of similar problems.

Second, considering that the number of patterns can grow that raises the importance of classifying these patterns in order to ease the patterns application, a taxonomy [Ahme 13] of business process security is proposed to define a process-oriented classification scheme for security risk-oriented patterns. The taxonomy aimed to integrate business process modelling with the security-risk. Furthermore, the taxonomy subsequently identifies the patterns' potential occurrences in business processes to facilitate their deployment.

Finally, the above contributions form a sound foundation for a method called SREBP –Security Requirements Elicitation from Business Processes– the main contribution of this thesis [Ahme 15, Ahme 14a]. The method allows early security analysis by determining the security objectives from business process models and their systematic translation to security requirements. The method uses security patterns to reason the risk analysis and rationale behind the security requirements. These requirements are then described in details using the system's contextual areas. On the one hand, it allows business analyst to understand how to secure business assets, on the other hand, it contributes to the alignment of business process models with the security domain. The method is validated to check its completeness and efficiency with respect to its ability in eliciting security requirements and how it contributes in securing business assets.

1.4 Publications and Contributions

This dissertation is based on four articles whose contributions are listed below.

- **Publication 1:** Securing Business Processes using Security Risk-oriented Patterns [Ahme 14b]
  - The article proposes a method to introduce security requirements to the business processes through the collaboration between business and security analysts. Introducing a set of security risk-oriented patterns supports the collaboration. The security patterns capture existing, time-proven solutions in a reusable manner and provide a rationale for security requirements. The performance of these patterns in identifying business assets, risks, and countermeasures is tested in the business

models of two business cases. In this paper, I conducted an extensive literature survey and developed the set of security patterns. Furthermore, I conducted the empirical studies that verified the usefulness of the proposed security patterns. I was the main author of this paper.

- **Publication 2:** A Taxonomy for Assessing Security in Business Process Modelling [Ahme 13]

  – The article proposes a comprehensive three-dimensional taxonomy for assessing security in business processes. It includes an in-depth insight of existing taxonomies used to classify business processes and security. The proposed taxonomy is subsequently used to classify a set of security risk-oriented patterns and identify their potential occurrences to deploy these security patterns in business processes. The taxonomy also defines a way of integrating security in business processes. The application of taxonomy is illustrated using an illustrative example. In this paper that I am the main author of, I performed an extensive literature survey, from which I derived and proposed a taxonomy for assessing security in business process models. In addition, I applied the taxonomy on an illustrative example for the purpose of validation.

- **Publication 3:** Eliciting Security Requirements from the Business Processes using Security Risk-oriented Patterns [Matu 13]

  – In this article, we refine the security requirements presented in security risk-oriented patterns and generate a security requirements model from a business process model. The article analyses the pattern, namely *securing confidential data using access control*, and defines the RBAC security model. The approach presented in this paper can be used to develop security requirements models for the remaining security risk-oriented patterns. For this paper, I performed the security requirements elicitation and developed a security model in RBAC.

- **Publication 4:** Security Requirements Elicitation from Business Processes (SREBP) [Ahme 15]

  – In this article, we use the security risk-oriented patterns to understand what business assets need to be secured, and to develop the security requirements elicitation from business processes (SREBP) method. The method supports elicitation of the security objectives and their systematic translation to detailed security requirements within the oper-

ational business processes. The method is applied and validated in the Estonian Genome Centre using a case study. In this paper, of which I am the primary author, I investigated the use of security risk-oriented patterns, and I developed a method –security requirements elicitation from business processes (SREBP). I applied SREBP method and empirically validated its completeness and efficiency compare to that of the SQUARE method. I was the one responsible for the design and execution of Genome Centre case study.

1.5 Structure of the Thesis

An overview of the thesis structure is as follows:

- Chapter 2 provides background information and introduces work related to the main topics of this thesis, particularly business processes, security risk management and model-driven security. Each of these domains starts by introducing their concepts in a general manner and then followed by a discussion of approaches presented in each domain.
- Chapter 3 corresponds to the publication *"Securing Business Processes using Security Risk-oriented Patterns"*. The chapter identifies the problems of addressing security in business process models and proposes a set of security risk-oriented patterns. The chapter illustrates how patterns enable the identification of security assets, their potential security risks and corresponding security requirements in business processes.
- Chapter 4 corresponds to the publication *"A Taxonomy for Assessing Security in Business Process Modelling"*. The chapter presents a taxonomy that integrates business process modelling with the security criteria aimed to define a process-oriented classification scheme for security risk-oriented patterns. The chapter illustrates the application of proposed taxonomy by classifying security patterns according to the taxonomy's dimensions; this enables a systematic security assessment in business processes.
- Chapter 5 corresponds to the publications *"Eliciting Security Requirements from the Business Processes using Security Risk-Oriented Patterns"* and *"Security Requirements Elicitation from Business Processes (SREBP)"*. In this chapter, we propose a method to systematically elicit security requirements from business processes using five contextual areas –access control,

communication channel, input interface, network infrastructure, and datastore. The method specifies these requirements using security requirements models and uses the security risk-oriented patterns in each contextual area to provide a rationale for the requirements. The method is validated to check its completeness and efficiency against the security quality requirements engineering (a.k.a., SQUARE) method.

- Finally, Chapter 6 summarises the findings of this thesis and outlines directions for the future work.

Chapter 2

Background

This section introduces the concepts of business processes and security risk management. After a description of the necessary concepts used in current literature, then, modelling languages for business processes and security risk are presented.

2.1 Business Processes

In the literature, the term business process is defined as:

- "*A process is a specific ordering of work activities across time and place, with a beginning, an end, and clearly identified inputs and outputs: a structure for action.*" [Dave 93]
- "*A business process is an ordered set of enterprise activities which can be executed to realise a given objective of an enterprise or a part of an enterprise to achieve some business value.*" [ENV 95]
- "*A set of one or more linked procedures or activities which collectively realise a business objective or policy goal, normally within the context of an organisational structure defining functional roles and relationships.*" [Work 99]
- "*A process is the set of activities (repeated steps or tasks) that accomplishes some business function.*" [Cong 11]
- "*A collection of inter-related events, activities and decision points that involve a number of actors and objects, and that collectively lead to an outcome that is of value to at least one customer.*" [Duma 13]

There exist several other definitions, for the means of this thesis we adopt the one proposed by Weske [Wesk 12]. The business process, there, is defined as "*a set of activities that are performed in coordination in an organisational and technical environment. These activities jointly realise a business goal. Each business process is enacted by a single organisation, but it may interact with business processes performed by other organisations.*" [Wesk 12].

Business processes are implemented using an artefact called business process model [Wesk 12]. A business process model is modelled in an appropriate modelling language that includes the activities, events and decision points, the organisational resources (users and departments) that perform these activities, the artefacts that are produced or manipulated, and specifies their relations. The act of developing these business process models is called business process modelling. Vergidis et al. [Verg 08] characterise the importance of expressing business processes that in the majority of cases, a business process would be expressive and communicative as the modelling language we have used to model it. Therefore, the elements and the capabilities of a modelling language are equally significant to describe and understand the business process. In this thesis, we have used Business Process Model and Notation (BPMN) Version 2.0 as a modelling language. The BPMN is widely adopted as a standard notation for representing business processes. The main purpose of BPMN models is to facilitate communication between domain analysts and to support decision-making. However, BPMN models are also used as a basis for specifying software system requirements, and in such cases, they are handed over to software developers [Ouya 09].

The concepts, methods and techniques that support the design, administration, configuration, enactment and analysis of business processes is referred as business process management (BPM) [Wesk 12]. The Business Process Management lifecycle comprises of various phases where a business process can be used [Wesk 12]. In the design and analysis phase, the processes are identified, and (re)designed. In the configuration phase, designs are implemented by configuring a process-aware information system (e.g., a WFMS). After configuration, the enactment phase starts where the operational business processes are executed using the system configured. In the evaluation phase, the operational processes are diagnosed to identify problems and to find things that can be improved.

In this thesis, we focus only on the first phase of BPM lifecycle where the aim is to analyse and (re)design the business process model. The method introduced in this thesis; *i*) analyses the business process model and identify the security criteria for business assets, and *ii*) elicits security requirements to satisfy these security

criteria. However, the rest of the phases pursue the execution of business process models, which is beyond the scope of this thesis.

The business process model is an abstraction of various details that vary at different levels from describing business goals to the technical implementation. Thus, we characterise a business process model using two aspects, *hierarchical abstraction* and *perspectives* described as follows:

2.1.1 Hierarchical Abstraction

Hierarchical abstraction is a common mechanism to describe abstraction in many of the existing languages for conceptual modelling [Krog 12]. It gives a better understanding of complex processes by presenting the required part at each level, and the modelling languages also include support for hierarchical constructs throughout the entire modelling and evolution activities [Krog 12]. Krogstie [Krog 12] describes four standard relations (i.e., classification, aggregation, generalization, and association) they characterise the correspondence between these hierarchies. We employ the concept of hierarchical abstraction to distinguish the hierarchy of business process models using the vertical abstraction defined by Weske [Wesk 12], that describes the hierarchy of a business process model (see details in Section 4.2.1). Since it is decomposition of business process model, therefore, the relation between the process hierarchical levels is aggregation. Aggregation means that the levels are interrelated, where the lower level objects make it up to a higher level component.

2.1.2 Modelling Perspectives

A modelling language has one or more core phenomena to express its goals, this phenomena is referred as the modelling perspective(s) of a language [Krog 12]. Krogstie [Krog 12] has listed eight perspectives of conceptual modelling approaches i.e., *behavior*, *functional*, *structural*, *goal and rule*, *object*, *communication*, *actor and role* and *topological* perspectives (see the details in [Krog 12]). Similarly, Curtis et al. [Curt 92] and Starke [Star 94] characterise four fundamental perspectives of business process modelling i.e., *functional*, *behavioral*, *organisational* and *informational*. In this thesis we use graphical description of business process models that is adopted from [Curt 92, Krog 12, Star 94]. It deals with the modelling perspectives (i.e., functional, behavioral, organisational and informational) of a business process model (see Section 4.2.2). These perspectives also serve as a foundation and are frequently used as a classification for business process modelling.

2.2 Security Risk Management

The thesis pursues the domain of security risk management. The term security is defined as "*the degree to which malicious harm to a valuable asset is prevented, reduced, and properly responded to*" [Fire 04]. Firesmith distinguishes particularly harm coming from intentional and unintentional source [Fire 07]. Therefore, security is defined as the concerns related with lowering the risk of intentional unauthorised harm to valuable assets to a level that is acceptable to the system's stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks [Fire 07]. In contrast to security, safety is defined as concerned with lowering the risk of unintentional unauthorised harm to valuable assets to a level that is acceptable to the system's stakeholders by preventing and reacting to such harm, mishaps (i.e., accidents and incidents), hazards, and safety risks [Fire 07]. He then introduces the concept of defensibility that is comprised of both security and safety. Within this thesis, security is only related to the harm coming from intentional source.

2.2.1 Domain Model for Security Risk Management

In this thesis, a domain model (see Fig. 2.1) for Information Systems Security Risk Management (ISSRM) [Dubo 10, Maye 09] is adopted to express the key concepts of security risk management and their relationships. ISSRM differs because along with the identification and specification of risks it also focuses on the whole IS, instead of defining security requirements for one or more IS components. Additionally a number of modelling languages (e.g., Secure Tropos [Matu 12a], Mal-activities [Chow 12], Misuse cases [Soom 13] and recently BPMN [Altu 13]) could be applied following the ISSRM guidelines; thus providing a systematic guidance for security risk management. ISSRM supports the 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 as illustrated in Fig. 2.1. Major concepts in ISSRM Domain Model are briefly introduced here.

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 a property or constraint on business assets describ-

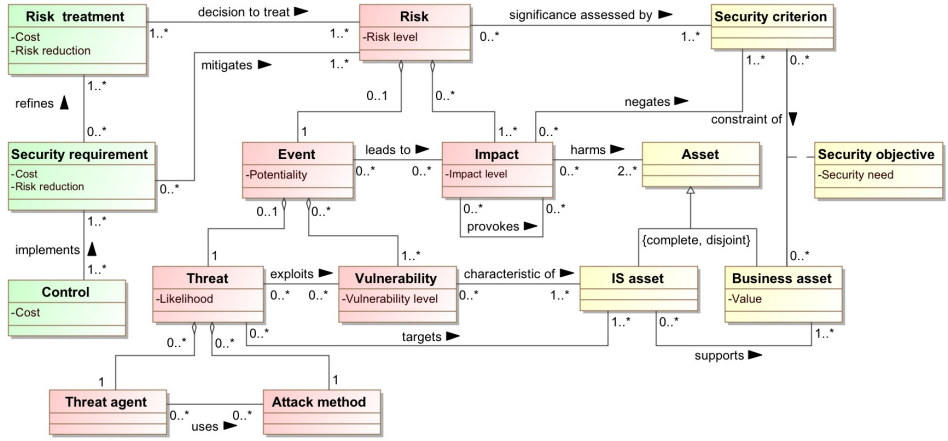

Figure 2.1: ISSRM domain model, adapted from [Dubo 10, Maye 09]

ing their security needs, which are, typically, expressed through confidentiality, integrity and availability.

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

The ISSRM application follows the general risk management process that is also based on the existing security standards, e.g. [DCSS 04, ENIS 04, ISOI 05a]. It is an iterative process consisting of six steps. Firstly a developer needs to define the organisational context and assets that need 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 decision would result in security requirements definition. Finally, security requirements are implemented into the 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 [Ahme 14b], we implicitly apply this security management process to develop security risk-oriented patterns for securing business processes.

2.2.2 Security Criteria

Security is a multifaceted attribute of an information system and requires four things to come together [Riaz 12]. A *security objective* defined as a high-level security goal (such as confidentiality, integrity, availability) defining the contributions to a security that the system is intended to achieve [Fire 04]. *Security policy*, a rule to define how far the assets of the system must be protected stating precisely the protection strategy of a system [Fire 04]. A *security control* is a mechanism or countermeasure (software elements, firmware, hard-ware, or procedures) included in the system for the satisfaction of security requirements [Fire 04]. A *security requirement* is functional and non-functional requirements relating security policies to security controls [Riaz 12]. Security requirements formalize security objectives without specifying their implementation. In this thesis, the security goal and security policy are expressed together as security criteria (desired protection level) for an asset, while security control is not the scope of the thesis as we focus on eliciting and specification of security requirements. The thesis specifies security requirements at two different levels: first, in security risk-oriented patterns where the security requirements are expressed at abstract level for its applicability in different scenarios. Second, the detailed level security requirements in SREBP method using several security models where the requirements are specific to the asset's context.

In the context of this thesis security criteria is expressed using CIA model [Info 91] that addresses three key security criteria, i.e. *Confidentiality*, *Integrity* and *Availability*. In [Fire 04], there exists other security criteria (i.e., authorization, non-repudiation and privacy) but they can be described in conjunction with these three security criteria. Thus, we consider confidentiality, integrity and availability as root security criteria that craft the foundation for security classification, the other security criteria can be listed as low-level objectives [Aviz 04, Scan 08]. For example, authorization (labeled *access control* in [Fire 04]) is a compound se-

curity criteria made up of *confidentiality of data*, *integrity of data*, and *integrity of application*. The security criteria are defined as follows:

Confidentiality It deals with the protection of data from unauthorised disclosure. A loss of confidentiality happens when the contents of a communication or a file are disclosed as well as when the fact is made known that a communication was carried out between certain parties.

Integrity It ensures the quality of data and system execution from impaired act, i.e., free from deliberate or inadvertent unauthorised manipulation. It means that neither the data nor the system has been altered or destroyed.

Availability It refers to the fact that data and systems can be accessed by authorised persons within an appropriate period of time. Reasons for loss of availability may be attacks (e.g. abusing known system vulnerabilities) or instabilities of the system or its components.

2.2.3 Security Standards and Methods

This section gives an overview of existing risk management and security standards and discusses security risk management methods.

Risk Management Standards The *ISO/IEC Guide 73:2009* standard [ISOI 02] provides the generic definitions for risk management concepts used in various activities, processes and frameworks related to the management of risk across different organisation. The guide addresses risk management in general and is applicable to information security. Similarly, The *AS/NZS ISO 31000:2009* standard [ASNZ 09] focuses on a generic risk management process for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. The standard is supported by: *ISO Guide 73:2009*, it provides a glossary for risk management concepts; and *IEC/ISO 31010:2009* [ISO 09], focuses on risk assessment concepts, processes and the selection of risk assessment techniques. Similar to *ISO/IEC Guide 73:2009* [ISOI 02], the standard is generic and can be applied to perform risk management in any domain.

Security Standards The *ISO/IEC 13335-1:2004* [ISOI 04] and *Common Criteria* [Comm 12] are widely used security standards that particularly focusses on the information security management but leaving behind the risk management

activities. The ISO/IEC 13335-1:2004 standard [ISOI 04] was initially published as technical reports and later became an international standard. The standard defines security concepts and models fundamental to a basic understanding of information and communication technology (ICT) security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. The *ISO/IEC 13335* series has been superseded and replaced by ISO/IEC 2700x series to comply with the security risk management standards. The Common Criteria for Information Technology Security Evaluation (CC) standard [Comm 12] specifies a set of security requirements along with the desired security objectives of a product or a system as security assurances. Next, the evaluators determine if the selected security requirements satisfy the security measures selected and implemented correctly. The Common Criteria (CC) defines three major constructs: *protection profile* is an implementation-independent set of security requirements to reduce the security risk; *Security target* contains the desired security objectives and requirements identified for a particular system or product, *Target of Evaluation* is a system or product that need to be evaluated.

Security Risk Management Standards The security risk management standards deal with security particularly focusing risk management activities. The most widely recognized security risk management standards are *ISO/IEC 2700x series* [ISOI 13], NIST (National Institute of Standards and Technology) Special Publication (SP) 800 Series, and BSI standards 100 series for information technology.

The *ISO/IEC 27001:2013* standard [ISOI 13] specifies the requirements necessary to establish, implement, maintain and continuously improve and manage an information security management system. The core concepts of information security risk management specified in ISO/IEC 27001 are supported by a standard *ISO/IEC 27005:2011* [ISOI 11] that proposes an information security risk management process. The process performs context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. The process uses an iterative approach for risk assessment and/or risk treatment activities. It uses the vocabulary of *ISO/IEC 31000:2009* [ASNZ 09] and, therefore, it easily integrates the risk management approaches with the information security risk management. Furthermore, the new standard includes detailed guidelines with examples on conducting a risk assessment that conforms to the requirements of *ISO/IEC 27001:2013*. Additionally, the standard contains risk scales, threats, vulnerabilities, likelihoods and impacts.

The NIST published a comprehensive set of NIST standards addressing security and risk in information system in their *800 series*. In particular, the standard, NIST SP 800-39 [NIST 11] describes a holistic risk management approach consisting four components: *1*) *frame* risk; *2*) *assess* risk; *3*) *respond* to risk; and *4*) *monitor* risk. The risk assessment component published in the NIST SP 800-30 [NIST 12] provides a step-by-step process for organisations on assessing information security risk and guides the communication between the risk assessments and other organisational risk management processes. The process in NIST SP 800-30 consists of 4 steps: *i*) Prepare for risk assessments; *ii*) Conduct risk assessments; *iii*) Communicate risk assessment results; and *iv*) Maintain the risk assessments.

The IT-Grundschutz – BSI series of standards is a set of German standards, based on a security management method. The series contains four standards: *Information Security Management Systems (ISMS)* [BSI 08a], *IT-Grundschutz Methodology* [BSI 08b], *Risk analysis on the basis of IT-Grundschutz* [BSI 08c] and *Business Continuity Management* [BSI 09] and is complemented by the knowledge-based materials referred as catalogues [IT G 13]. The catalogues contain lists of assets, threats and safeguards, and are updated and regularly extended considering the latest technical developments. The first BSI standard, *100-1: Information Security Management Systems (ISMS)* [BSI 08a] specifies the general requirements for an Information Security Management Systems (ISMS). The standard is compatible with *ISO/IEC 27001:2005* [ISOI 05a] and, moreover considers the recommendations of *ISO/IEC 27002:2005* [ISOI 05b]. The second BSI standard, *100-2: IT-Grundschutz Methodology* [BSI 08b] provides successive steps to assist an effective management system for information security. It includes details on, how to develop an information security policy, how to select information security safeguards and necessities for implementing the information security policy, and how to maintain and improve information security during its operation. The methodology relies on catalogues in implementing the requirements provided by the ISO/IEC standards. The third BSI standard, *100-3: Risk analysis on the basis of IT-Grundschutz* [BSI 08c] outlines the risk analysis methodology to supplement an existing IT-Grundschutz Methodology, to be used for additional security analysis. A supplementary security analysis should be performed on a particular set of assets (or target objects) identified in the IT-Grundschutz Methodology. The fourth BSI standard, *100-4: Business Continuity Management* [BSI 09] builds on the previous standards. The standard describes a systematic method, to detect the risks that can endanger the survival (i.e., economic existence) of an organisation, and to implement safeguards against such risks or even after incurring the risks. The BSI standards comprehensively describe a process for achieving

and maintaining an adequate level of security, and an approach to determine the level of security. The *IT-Grundschutz Catalogues* [IT G 13] comprised of standard security safeguards, threat scenarios usually, and detailed implementation of safeguards. These standards are freely available and are continuously subjected to update reflecting the latest IT developments.

Security Risk Management Methods A risk management method is a process that contains a set of activities executed systematically in a predefined sequence. The risk management method may not always comply to a published standard but comprised of activities that covers: the identification of threats, vulnerabilities, or risks and their impact on the organisations assets; risk assessment; risk mitigation planning; implementation strategies; and evaluate their effectiveness. The section provides an overview of available security risk management methods such as EBIOS [DCSS 04], MEHARI [CLUS 10], OCTAVE method [Albe 03], CRAMM Method [Koun 11] and CORAS approach [Lund 11].

The EBIOS method [EBIOS 14] is composed of five phases: the first phase identifies the essential elements of an organisation and components of their information system; The second and third phases determine the organisation's security needs and requirements, and the list of threats specific to their information system; The fourth phase maps the organisation's security needs to the identified threats including proof of necessary security objective in mitigating the identified risks; Finally, the security requirements are selected to achieve the identified security objectives. The method can be adapted to any particular context and easily integrated to the existing methods without disrupting the primary flow of the approach. The scope of EBIOS extends over the high-level analysis of an organisation's information system to detailed level components of the information systems (i.e., website, recruitment management, and etc.).

MEHARI [CLUS 10] process of risk assessment and management comply to the requirements provided by standard *IS0/IEC 27001:2005* [ISOI 05a] and adapted the guidelines defines in standard *ISO/IEC 27005:2008* [ISOI 08]. In MEHARI, the risk assessment and management is performed in three steps: *i*) *Stakes analysis and classification* analyses the business processes' activities and their goals to determine potential malfunctions and their seriousness (i.e., malfunction value scale). Next, classify the identified assets of information system based on the required security goal (i.e. confidentiality, integrity, availability) and their malfunction value. At last, an intrinsic impact table is build to evaluate the consequences of the risk independent of any security measures. The output of this step is the *malfunction value scale* and the *classified asset with an intrinsic impact table. ii*) *Assessment of*

security services quality starts by developing criteria to assess the security service. Next, the security services are compared with the state of the art of security by means of MEHARI knowledge base. The evaluation results identify the potential weaknesses in the security services; and *iii*) *risk assessment* starts by identifying the risks and focusses the analysis to the critical situations, then, review the seriousness of identified risks against the security service quality. The resulting identified risks together with an assessment of likelihood and impact are used in the next phase to define security requirements for their information system.

OCTAVE method [Albe 03] is a self-directed risk-based strategic assessment and planning approach that comprised of three phases. Firstly, build asset-based threat profiles from a different level of organisation, i.e., senior management, operational area and staff by conducting workshops. Secondly, the key components of the information system supporting critical assets are evaluated to identify the technological vulnerabilities. Finally, the risks are evaluated, and the risk profiles are developed to define appropriate security strategy and risk mitigation plans. OCTAVE method has two variants, OCTAVE-S [Albe 05] and OCTAVE Allegro [Cara 07]. The OCTAVE-S approach [Albe 05] is adopted for a small organisation, which rely on individuals knowledge of security and information systems rather than formal knowledge elicitation workshops. OCTAVE Allegro [Cara 07], a variant of standard OCTAVE that proposes a systematic process mainly focused on information assets (i.e., their usage, storage, transport, and processing, and their threats, vulnerabilities, and disruptions). However, each variant of OCTAVE method has its advantages. Users can select any of them that satisfy their security risk assessment needs.

The CRAMM (CCTA[1] Risk Analysis and Management Method) [Koun 11] ensures that security requirements are fully analysed and documented, avoid unnecessary safeguards and inconsistencies in risk assessments, and involve management in planning and implementing security throughout the various stages of system lifecycle. The CRAMM method is performed in three steps [Koun 11, Maye 09]. Firstly, identify the assets, their values are calculated. The physical assets' values are derived from their replacement cost. Data and software assets' values are derived from the impact of breaches of any of the security objectives, i.e., unavailable, destroyed, disclosed, or modified. Secondly, threat and vulnerability assessed using predefined mappings between threats and assets as well as between threats and impacts. This results in a risk matrix for each asset group. Finally, on the basis of risk analysis a set of countermeasures are selected from a large set of countermea-

[1]Central Computer and Telecommunications Agency

sures that are hierarchically organised in logical groups and sub-groups. The set of countermeasures contains necessary information from high-level security objectives to the technical implementation illustrated using examples required to manage the identified risks.

CORAS is a model-driven approach to risk analysis and adopted the core generic risk management process defined in AS/NZS ISO 31000:2009 standard [Lund 11]. CORAS consists of three tightly integrated artefacts: a language, a tool and a method. The *CORAS language* is a customised language that provides graphical symbols and its relations for risk modelling. These symbols are easy to use and to communicate with the stakeholders from different backgrounds (e.g., software development, security or business). The *CORAS tool* supports the language and is a graphical editor for making any CORAS diagram. Furthermore, the tool facilitates to document and present a risk analysis results. The CORAS method has adapted risk management process from ISO 31000:2009 standard [ASNZ 09] and provides detailed guidelines and techniques to facilitate various steps of CORAS risk analysis. The risk management process starts by identifying the stakeholders and vulnerabilities, and establishing the context, which system's parts, process or organisation will be analysed. Next, the risk assessment includes activities to identify risks, estimate risks and evaluate risks. Then, mitigation strategies are defined to treat the identified risks that involve a structured brainstorming, and are supported by CORAS treatment diagrams. Finally, connect the risk analysis process to the rest of the business, system or organisation and continuously monitor and review the risk management process.

2.3 Model Driven Security

This section gives an overview of security modelling languages used to elicit security requirements in early stages of information system development. Furthermore, the study discusses their extensions to adopt security risk concepts from risk management domain. In the end, the section provides details about security risk modelling in business processes.

2.3.1 Security Modelling Languages

Misuse Cases [Sind 05] are a security-oriented extension of the UML use cases [Business 14]. Misuse cases have graphical and textual representation like use cases. Misuse case diagrams are extended with misuser, misuse case, and security use cases constructs including threatens and mitigates relationships (see Fig. 2.2).

A *misuser* intends to harm the software system. A *misuse case* is a goal of misuser, the association is represented by a communication association. Misuser executes misuse case either by combine efforts of several misuse cases or independently. Threatens and mitigates relationships are used between use cases and misuse cases. Threatens relationship means a misuse case is potentially a threat to harm the use case. *Mitigates* relationship indicates that a use case is countermeasure against any misuse case. Security-use-case is a special use case to perform countermeasure against the identified threat. As illustrated in Fig. 2.2 misuse cases are integrated in use case diagrams to express the system unwanted behaviour (e.g., misuse cases `Money stolen`, `Enter pin code result repeatedly`, and `Transfer money to own account`) initiated by a misuser (e.g., `Attacker`). This depiction results in security use cases e.g., `Perform cryptographic procedures`.

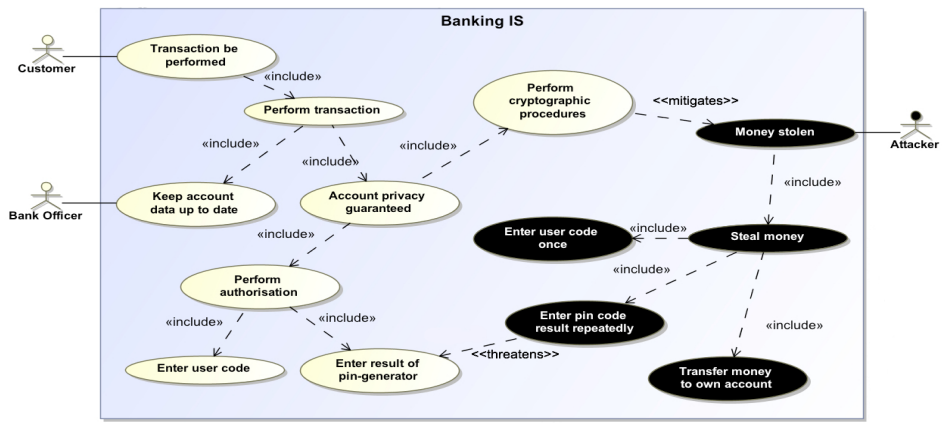

Figure 2.2: An example of misuse case diagram, adapted from [Ahme 12b]

Soomro and Ahmed [Soom 13] proposed security risk-oriented misuse cases (SROMUC) to strengthens the misuse case diagrams. The idea is to comply misuse cases with security risk management strategies because they lack several concrete constructs to represent secure assets, security-risks and their countermeasures. These limitations could lead to misinterpretation of the security-related concepts and results in inadequate security solutions. The work extends the syntax and semantics of misuse case diagrams [Sind 05]. The proposed graphical extensions are not intuitive, and they are related to the security concerns supported by the ISSRM domain model. However, the proposal keeps the SROMUC comprehensible and comply with the original definition of (mis)use cases. The SROMUC differentiates the constructs for impact and security criterion from the standard UML use case constructs. The security use case construct has been enhanced to differentiate

security requirements from the functional requirements, but the SROMUC does not address the risk treatment and control implementation.

Secure Tropos [Mour 03, Mour 07, Mour 06] enriches Tropos (an agent-oriented software development methodology) [Bres 04, Cast 02] by introducing security related constructs such as security constraint and threat. In Tropos and Secure Tropos the concepts of actor, (hard or soft) goal, plan and resource constructs are common. In addition, Secure Tropos defines the concepts of security constraint and threat. A *security constraint* is a security restriction that the system must satisfy. A *threat* represents circumstances, which lead to an event that endangers the security features of the system. Additionally, the notion of *vulnerability point* (any system's weakness) is introduced by Elahi and Yu in [Elah 07]. Constructs in Secure Tropos are connected using relationships: dependency (and its subtype of secure dependency), decomposition, means-ends, contribution, restricts and attacks. Matulevičius et al. [Matu 12b] extend Secure Tropos, called as Risk-aware Secure Tropos, to support the modelling of security risks and their countermeasures. The study proposes syntactic, semantic and methodological extensions to the Secure Tropos. The extensions mainly expressed in three conceptual groups, i.e., asset-related concepts, risk-related concepts and risk-treatment related concepts. The study main idea is to align Secure Tropos with the domain model of security risk management [Dubo 10, Maye 09]. The study also defined the methodological guidelines for applying the risk-aware Secure Tropos during early stages of information system development.

Mal(icious)-Activity Diagrams [Sind 07] is an extension of standard UML activity diagrams with the purpose to capture security in activity diagrams. In mal-activity diagrams the concepts of malicious activity, malicious actor and malicious decision are introduced. The *malicious activity* is an activity that can harm the system, represented as normal activity, but with inverted colour. A malicious activity is initiated by a *malicious actor* whose goal is to harm the system and represented by normal swimlanes with inverted colour. The *malicious decision* represents where malicious user makes the decision to perform a malicious activity; malicious decision is represented as ordinary decision box using inverted colour. The idea is similar to misuse cases where misuse cases provide an abstract overview of the required functions while missing the sequence of activities, which make it difficult to map the malicious activity with the system execution. In this case, mal-activity diagrams complements the security analysis by representing the

sequence of activities (i.e., detailed system design) in activity diagrams. It helps to change the execution of activities in order to address the mal-activity.

SecureUML is a UML-based modelling language proposed by Lodderstedt et al. [Lodd 02]. It supports the development of secured distributed systems by integrating the information relevant to their access control into the application models. SecureUML focuses on embedding role-based access control policies in UML class diagrams using a UML profile (i.e., annotating class diagrams with relevant access control information). The main RBAC concepts expressed using SecureUML are *users*, *roles*, *objects*, *operations* and *permissions*.

A *user* is a human being or a software agent, and role is a job function within the context of an organisation modelled using ≪role≫ stereotype. *Permissions* characterise role privileges to perform operations on the protected object. An *object* is a protected resource. An *operation* is an executable set of actions that can change the state of the protected resource by creating or manipulating its properties. Permissions specify the security actions –namely, *Create*, *Read* and *Update*– that the role can perform over the state of the protected resource. SecureUML formally expresses role-based access control policies for objects but does not consider an attacker model; similarly, the approach covers the security goals of confidentiality and integrity, but not availability [Fabi 10]. In this thesis, SecureUML is used in SREBP method to define security requirements for accessing and manipulating protected business assets in the business processes, which required satisfying the security criteria of confidentiality and integrity.

Attack tree [Schn 99] is a formal way of expressing a set of varying attacks against an information system. Attack tree connects more than one attack leaf from each node in a tree structure. The root node is the overall goal of the attack and nodes (i.e., leaf nodes) at all levels below the root represent different ways of achieving the overall goal of an attack. The idea is to understand the different ways in which the system can be attacked and identify the attackers to install the proper countermeasures to deal with the real threats. The leaf nodes are connected to the top node with logic operators *AND* or *OR*. Therefore, either a single node can fulfil the goal of the level above it or a combination of one or more sub-goals are required to achieve the goal of the level above. For instance, with an *OR* operator, the attack tree needs one of the leafs to satisfy the goal, whereas in case of *AND* operator all the leafs of the tree must be satisfied to meet the top-level goal. An example of an attack tree is illustrated in Fig 2.3.

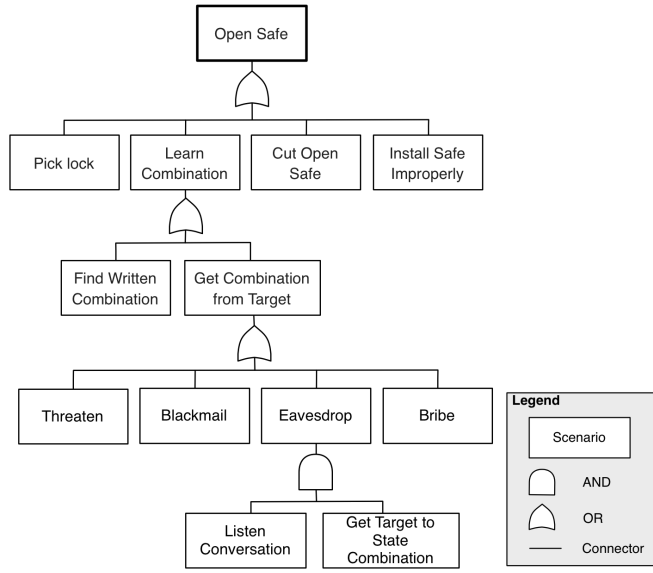

Figure 2.3: An example of attack tree, adapted from [Schn 99]

In this example, the leaves `Listen Conversation` and `Get Target to State Combination` having an *AND* logical operator. Therefore, both are required to execute successfully in order to achieve the goal of the level above it, i.e., (`Eavesdrop`). It is important to note that the rest of the attack leaves are connected in the attack tree using *OR* logical operator. Hence, if any of the attack leaves from the rest of the attack tree are satisfied, it is sufficient to satisfy the overall goal of the attack tree (i.e., `Open Safe`). In this thesis, attack trees are used to model attack methods during the security analysis performed by SQUARE method, when SREBP method is validated in a Genome Centre case study.

2.3.2 Security-Risk Modelling in Business Processes

Due to the nature of inherent risks in the routine operations and interactions with stakeholders, the enterprises are always vulnerable to potential security risks. Identifying and understanding the relationships between these risks and security solutions are essential to mitigate these risks effectively. However, business process modelling languages lack a systematic security risk management approach to address the security risk-related concepts. Eventually, in business processes modelling, security ends up as an afterthought because it is not well integrated with regular engineering processes. In [Altu 12], the business process modelling language,

Business Process Model and Notation (BPMN, version 2.0) [Dijk 08, Silv 09], is analysed at the fine-grained level to outline its capabilities to deal with security. BPMN notations are linked to a semantic model, which means that each shape has a particular meaning and defined rules to connect objects. Altuhhova et al. [Altu 13] mainly investigate: *i*) how business activities expressed using BPMN could be annotated with the security concerns; *ii*) how BPMN could be used to define security requirements; and *iii*) how the BPMN language itself could be used to reason for the security requirements through illustration of the potential security risks. In this analysis, the concepts of the ISSRM domain model [Dubo 10, Maye 09] are aligned with the BPMN constructs. This alignment results in proposing a set of security risk-oriented extensions for BPMN. The extensions enable BPMN application to analyse security risks by providing guidelines to express secure business assets, potential security risks, and their countermeasures.

This section briefly describes the analysis (i.e., lacking) [Altu 12] and the proposed set of security risk-oriented extensions (i.e., constructs) [Altu 13] to make the business process modelling language, risk-aware. Additionally, different colours are used to improve the expressibility of security risk analysis across the three concept groups, i.e., *i*) *black* for the asset related constructs, *ii*) *red* for the risk-related constructs, and *iii*) *blue* for the risk treatment-related constructs.

Asset-related concepts. In the first place, Altuhhova et al. [Altu 12] observe that its constructs, such as task, gateway, event and their connecting link, i.e., sequence flow, help describing valuable processes that correspond to ISSRM business assets. The flow objects (such as 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, the pool and lane constructs are aligned to the ISSRM information system assets. The BPMN data object, which describes the required or produced data, is aligned to the ISSRM business asset, and BPMN data store is defined as the ISSRM IS asset. Here, Altuhhova et al [Altu 12] indicated the importance to differentiate between meanings of the BPMN constructs when expressing different ISSRM concepts. For example, the BPMN task could be used to express both the ISSRM business assets and IS assets. In order to distinguish this two icons are introduced as illustrated in [Altu 13]. Additionally, a visual element – lock – is used to express the ISSRM security objective. The lock is placed (as the constraint of) on the business asset, representing its security needs. The security criterion is defined, then, in the annotation associated to the lock construct.

Risk-related concepts. The BPMN language does not contain the direct means to model security risks [Altu 12]. Therefore, the concrete syntax to express risk-related concepts are introduced in [Altu 13], where, the ISSRM threat agent could be expressed using the BPMN containers, i.e., pools and lanes, and the ISSRM attack method is defined as the combination of flow objects (i.e., event, gateway, and task) using sequence flows. The ISSRM vulnerability could be defined using annotations, which are assigned to the vulnerability point. This point is defined as the characteristic of the IS asset. Further, the notion of the ISSRM impact is introduced using unlock symbol. If the security criterion is negated then the security objective (defined using lock) is broken. The appropriate BPMN relationships (leads to relationships) are used to define how risk harms the business asset(s) and IS asset(s). Following the domain model, the ISSRM threat is defined as a combination of the BPMN constructs used to model threat agent and attack method; the ISSRM event is expressed through the combination of constructs for threat and vulnerability. The ISSRM risk is modelled using the BPMN constructs for event and impact.

Risk treatment-related concepts. The combination of flow objects (i.e., event, gateway, and task) is used to model the ISSRM security requirements and mitigation relationship [Altu 13]. Other ISSRM constructs are not explicitly expressed because *i*) the risk treatment is rather a decision done towards the mitigation of the identified risk, and *ii*) security control is a part of the system implementation stage (but not analysis, where BPMN is typically applied).

2.4 Conclusion

We conclude that an enterprise's business processes are key artefacts to address the security. They drive their information system to achieve the business goals, thus, addressing security in business processes allows early security analysis at the development of information systems. In this chapter, firstly, we give an overview of business processes, their implementation in business process model and how business process model enables the constituents of business process (i.e., perspectives) to model at different abstractions level. Secondly, we provide an overview of security risk management concepts and discuss the domain model for information system security risk management. The model gives foundation for security risk related work in this thesis. The chapter touches upon existing security risk management standards and methods used in the industry. Finally, we discuss several

model-driven security techniques used in security analysis to support the early security requirements elicitation in information system development.

In the next chapter, ISSRM domain model is used to develop security risk-oriented patterns. Chapter 4 integrates the characteristics of business process models (i.e., abstraction level and perspectives) with the security criteria in a three-dimensional taxonomy. On the basis of security patterns and ISSRM domain model, Chapter 5 proposes a systematic method for requirements elicitation and make use of model-driven techniques to express these requirements in detail.

Part II

Contributions

Chapter 3

Security risk-oriented patterns

In this contribution [Ahme 14b], we introduce security risk-oriented patterns that describe how to integrate the security requirements into business process models. Typically, security engineering requires a close collaboration between the business analyst (i.e., the specialist of the business domain) and security analyst (i.e., the specialist of the security domain). Being experts in business domain, business analysts have limited or no expertise in security engineering. They have to rely on the best security practices, information security standards, or security experts. To improve this situation, we propose to use security risk-oriented patterns. The idea is that the majority of the problems often do not require new solutions. Developers reuse similar solutions already implemented independently or elicit different aspects of similar problems; they have already solved in another situation. By introducing the security risk-oriented patterns, we potentially reduce the business analysts' need to ask for the help from the security analysts because patterns introduce both the security requirements and security rationale.

3.1 Security Patterns

Pattern-oriented software engineering has spread after the release of Gang-of-Four [Gamm 95]. Developers are using this approach to solve system development problems in a well-structured way. The success behind the patterns-oriented engineering is that patterns provide a basis for the development using a collective knowledge from the relevant domain.

According to Schumacher et al. [Schu 05] "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". Following this definition, we develop a set of *security risk-oriented patterns* (i.e., *generic scheme*). The patterns are based on understanding security risks (i.e., *recurring security problems*) that arise within business processes (i.e., *specific security context*). To mitigate the risks, the patterns recommend *security requirements* (i.e., *security solution*).

3.2 Research Method

The primary research objective is to develop security patterns for business processes (see details in Section 3.3.2) and illustrate their usage in business process models. We follow a 4-step research method, depicted in Figure 3.1. Firstly, a template for security risk pattern is developed in *Step 1*. The template (see Section 3.3.1) uses security risk concepts defined in ISSRM domain model [Dubo 10, Maye 09]. Secondly, we collect security-related information that includes system's vulnerabilities, risk and their attack methods from the literature and align it with the context of information system in *Step 2*. The collected information is structured into security patterns (see Section 3.3.2 & 3.3.3). Thirdly, security concepts from security patterns are expressed into business process modelling language using ISSRM-oriented modelling languages in *Step 3*. Security risk-aware extensions are published in [Altu 13] and briefly discussed in Section 2.3.2. Finally, in *Step 4*, we investigate the usefulness of these security patterns by applying them in two business cases.

3.3 Security Risk-oriented Patterns

The security risk-oriented patterns are developed using a structured specification, i.e., a security risk-oriented template, and graphically represented using risk-aware business process modelling language that business analysts can understand easily.

3.3.1 Security risk-oriented template

Initially, the security patterns [Fern 01] were developed using traditional software patterns e.g., Gang-of-Four [Gamm 95]. Therefore, the structure of these patterns were inspired or based on a design or architectural concerns. Such patterns are good enough to implement security at the design stage of information system.

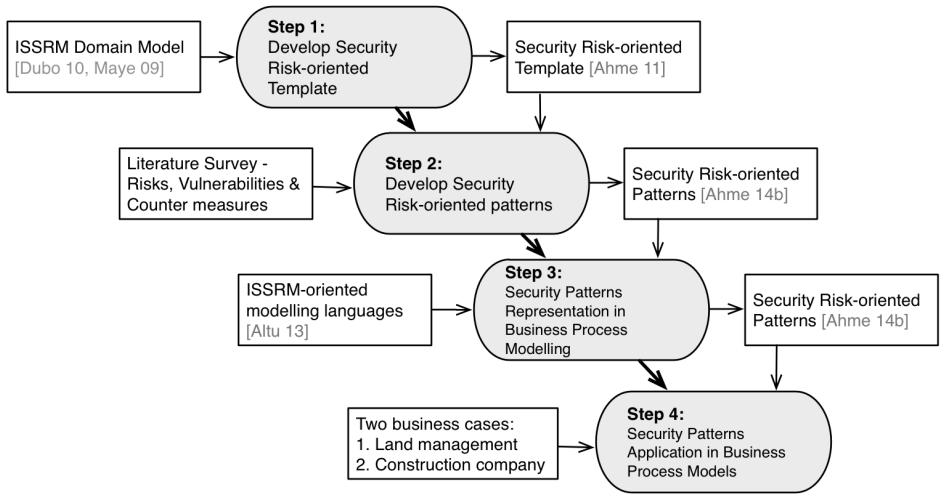

Figure 3.1: Research method for developing the security risk-oriented patterns

However, the main problem is their ability to capture security requirements from business processes. To overcome this limitation, we develop a security risk-based template [Ahme 11] that particularly focusses on the business process domain.

A security risk-based template follows the domain model for information systems security risk management (ISSRM) [Dubo 10, Maye 09]. The ISSRM domain model describes the security risk management in information system using three different concept groups, i.e., asset-related, risk-related, and risk treatment-related concepts. A security risk-based template (see Table 3.1) consists of three major entries, namely pattern name, pattern description, and related pattern(s), and three entries that support definitions of the ISSRM concepts. These entries include (*i*) *assets-related concepts* describe the security context by defining organisation's assets and their security criteria; (*ii*) *risk-related concepts* describe the security problem by defining a risk, its impact and the attack method to exploit vulnerabilities and execute threat; and (*iii*) *risk-treatment related concepts* describe security solutions to solve the identified security problems by defining one or more countermeasures applied to treat the risks.

In order to apply security risk concepts (expressed in security risk-oriented patterns) in business process modelling, we analyse a language for business process modelling with respect to ISSRM domain model [Dubo 10, Maye 09]. The analysis helps to understand the key aspects of business process modelling language in expressing secure assets, risks and risk treatment. It aligns the constructs in

Table 3.1: Security Risk-oriented Template

1. Organisational scenario & Security context identification	
Pattern name	It represents the pattern, and captures its security context. Usually, this attribute is used to remember and refer the pattern. Ideally, it should contain the name of the problem been addressed in the pattern.
Pattern description	It describes the scenario in which the pattern may apply. This attribute includes the detailed information about the business context; what are the input(s) and output(s), and under which circumstances it will be executed or processed.
Related pattern(s)	It is an optional attribute to save information about the other patterns related to current security pattern.
2. Asset identification & Security objective determination	
Asset	An asset is any valuable thing that plays a vital role to accomplish organisation's objectives.
Business Asset	A business asset describes the information, processes, capabilities and skills essential to the business and its core mission.
IS Asset	An IS asset is the IS component, valuable to the organisation since it supports business assets.
Security criteria	A security criterion is a property or constraint on business assets describing their security needs which are typically expressed through confidentiality, integrity and availability of business assets.
3. Risk analysis & assessment	
Risk	A risk is composed of one or more events and their negative impacts on one or more assets by harming them.
Impact	An impact is the potential consequences of a risk that may harm assets of the system when a threat (or the risk event) is accomplished.
Event	An event is an aggregation of threat and one or more vulnerabilities.
Threat	A threat is an incident initiated by a threat agent using attack method to target one or more IS assets by exploiting their vulnerabilities.
Vulnerability	A vulnerability is the characteristics of IS assets that exposes weakness or flaw.
Threat agent	A threat agent is an agent who has means to harm IS assets intentionally.
Attack method	An attack method is a standard means by which a threat agent executes threat.
4. Risk treatment & Security requirements	
Risk treatment	A decision (e.g., avoidance, reduction, retention, or transfer) to treat the identified risk.
Security requirement	Security requirement is the refinement of the risk treatment decision to mitigate the potential risks.
Security Control	A control that designates a means to improve the security by implementing the security requirements.

business process modelling language with the concepts of security domain and highlights the shortcoming of business modelling language in expressing security risk-related concepts. Furthermore, alignment provides foundation to introduce a set of security risk-oriented extensions for business process modelling language. These extensions make the modelling language security risk-aware, which could be used to express secure business assets, potential security risks, and their countermeasures identified in security risk-oriented patterns.

3.3.2 Security Risk-oriented Patterns Development

Once the structure (i.e., template) of security patterns is defined, security risk-oriented patterns are developed on the basis of three conceptual areas adopted from ISSRM domain model, i.e., asset, risk and risk treatment, -related concepts. The process of pattern development implicitly uses security risk management process described in ISSRM domain model (see Section 2.2.1). The process of pattern development comprises of the following five activities.

In asset-related concepts, the process starts with an (*i*) *identification of information system's context*, focusing on the asset identification. Initially, we have identified ten contexts (reported in [Ahme 12a]) for security patterns, which is then reduced to five contexts on the basis of six functions (proposed in [Alte 06], i.e., capture, transmit, store, retrieve, manipulate and display information) that information technology can perform to process information in an information system. Based on these categories, we currently develop five security risk-oriented patterns (see Section 3.3.3). First pattern secures data transmission, second ensures valid data entry into system, third makes the data available, fourth provides authorised data access and its manipulation, and last pattern secures stored data. Next, we (*ii*) *identify assets & determine security criteria* within each context. The security criteria are determined using CIA model (described in Section 2.2.2). The final output of this activity is a business process model that illustrates the identified asset and its security criteria with the help of security risk-oriented extensions proposed in [Altu 13] (see Section 2.3.2).

In risk-related concepts, we perform (*iii*) *analyse security risks* to identify security risks characterised by threats, vulnerabilities and risk impact (see ISSRM domain model in Section 2.2.1). The activity starts by identifying security flaws (listed in [Tsip 05]), followed by the risk analysis, and finally countermeasures are proposed to mitigate risks. These security expertises are collected from a variety of sources including relevant security literature (for each pattern details are provided in [Ahme 14b]). The risk-related concepts are documented in the template. These

concepts are represented in security risk-oriented model using security risk-oriented extensions for BPMN [Altu 13] (see Section 2.3.2).

Finally, in risk treatment-related concepts, first, we specify the (*iv*) *risk treatment decision* (see Section 2.2.1), and then (*v*) *identify security requirements* to mitigate the identified risks. These security requirements are presented in business process model using security risk-oriented extensions [Altu 13] described in Section 2.3.2. In the pattern template, we briefly suggest security control(s) to implement the security requirement(s). Currently, the scope of these patterns is to elicit security requirements for securing enterprise's business assets and identifies risks associated to these assets, and illustrate the rationale for these risks. Therefore, we briefly suggest security controls without going into their implementation details. However, in Chapter 5, we present an approach [Matu 13, Ahme 15] to develop security models that refine these security requirements in detail.

3.3.3 Overview of Security Risk-oriented Patterns

In [Ahme 14b], we described five security risk-oriented patterns to facilitate business analysts. These patterns follow a security risk template and define three major security concepts: *i*) *assets-related concepts*; *ii*) *risk-related concepts*; and *iii*) *risk-treatment related concepts*. The security patterns are expressed using the security risk-aware BPMN as described earlier and illustrate security requirements to protect the identified assets. The patterns are published in [Ahme 14b]. Here, we give an overview by highlighting the business assets (that need to be secured) and their security criteria. Each pattern contributes to the achievement of one or more security criteria, i.e., confidentiality and integrity of data, integrity and availability of business activity. A single pattern may have multiple criteria associated with it. Thus, one security requirement could potentially contribute to the accomplishment of more than one security criteria.

SRP 1 *Pattern secures the data transmitted between the business entities.*

This pattern addresses the electronic transmission of *data* between two entities i.e., *client* and *business*. In Fig. 3.2(*a*), SRP1 indicates that a client submits *data* to the *business* that is then employed by business. In this pattern *data* corresponds to *business assets* and avoids the risk of unauthorised interception of data during transmission because the unencrypted *data* could be misused (i.e., read and kept for a later use or modified and passed to the server). The threat negates the confidentiality and integrity of data. The pattern introduces the security requirements of *making data unreadable* and *verify the received data*.

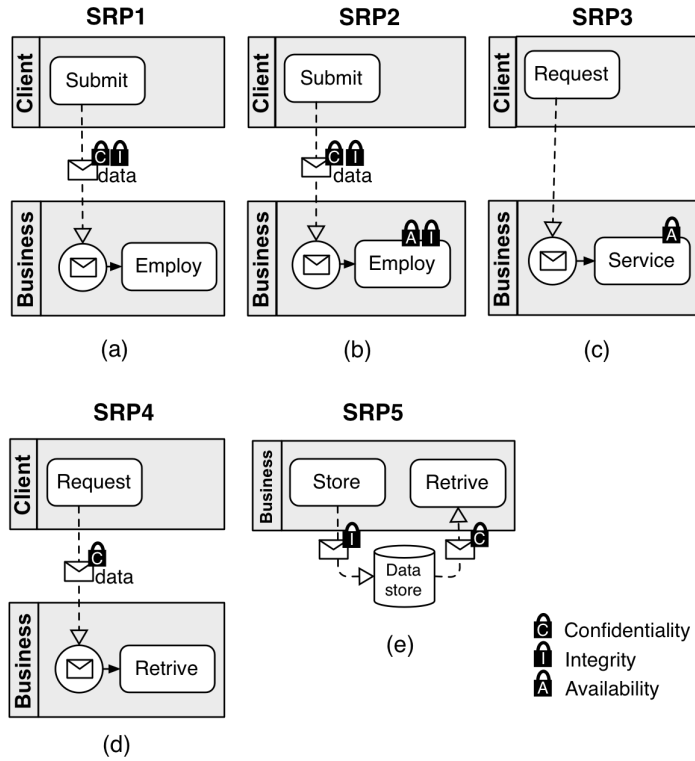

Figure 3.2: Asset-related concepts of security patterns adapted from [Ahme 14b]

SRP 2 *Pattern ensures valid data entry into business processes by rejecting the unwanted malicious data.*

This pattern (see Fig. 3.2(b)) secures the business activity *employ* (i.e., any activity after data is submitted), which *integrity* and *availability* have to be ensured. An attacker can exploit the activity *submit* to send malicious scripts. Executing these scripts risks the *confidentiality* and *integrity* of *data* itself, any activity after data is submitted may be harmed, become unavailable or loose its integrity; additionally the input interface would be compromised. To mitigate the risk(s), pattern introduces security requirement to *validate the incoming data*.

SRP 3 *Pattern ensures the availability of services or business assets by protecting the IS from denial of service (DoS) attack.*

This pattern addresses the Denial of Service (DoS) attacks and their protection strategies. The major idea is to protect the *business services* (i.e., business assets)

provided by a business, in order to guarantee the security criteria, i.e., *availability* of this business service. In Fig. 3.2(c), the SRP3 illustrates that a client requests the *service* provided by a business. In this situation, an attacker can target the *server* by exploiting the protocols (e.g., TCP, ICMP, or DNS) used at server. Thus, the *server* becomes incapable to operate the *business service* and becomes unavailable to their users. The threat provokes the loss of the business consumers' confidence in the service provider.To reduce such attack(s), pattern proposes a security requirement for *checking for incoming requests.*

SRP 4 *Pattern secures the confidential data by applying multi-level security.*

This pattern describes how to secure *confidential data* from access by the unauthorised people or devices. The pattern is based on the implementation of access control where (stakeholder or device) roles and data are classified to levels of trust and sensitivity. In Fig. 3.2(d), SRP4 exhibits a client requests *data* (a confidential business asset). In response to this request, the data are retrieved (using the retrieval interface characterised as the IS asset) and provided to the client. The problem arises if the retrieval of the *confidential data* is allowed to any user (independently whether s/he is malicious or not) without checking his or her access permissions to the data. To reduce such risk, the *check for the access rights* should be implemented. The requirement means one needs to authenticate an individual's access rights to create, access or manipulate a business asset.

SRP 5 *Pattern ensures the data privacy at the data store against insiders (i.e., administrators or malware that infects data store).*

The goal of this pattern is to prevent the leaking of confidential data from the enterprise's data store. In Fig. 3.2(e), there exists a *storing/retrieval interface* (i.e., IS asset), which helps business (i) to store the *data* (i.e., business asset) in the data store and (ii) to retrieve them when needed. If the *storing/retrieval interface* (also including the queries to the database) are designed in a way that data are saved/retrieved in a plain format. Therefore, unauthorised individuals can compromise the confidentiality and integrity of data. To reduce such security risk, one needs to introduce security requirements *making data invisible and visible* and *log the data store activities* when the data are stored and retrieved in the data store.

Security risk-oriented patterns present security requirements and rationale for security countermeasure, suggesting business analyst, the solutions on how to achieve the required security objectives. The security risks are visualised using

a security risk-aware extensions [Altu 13] to business process modelling language. The visualisation justifies security solution and helps the business analyst to determine what constitutes the overall risk level in terms of security event potentiality and impact level. However, the precise estimation depends on the analysed problem domain. Taking into account these measures, the business analyst can judge what security requirements should be implemented into the security control. The idea behind these security patterns is to present a holistic approach that closes the gap between security risk management and business process models. These security patterns show the application of the proposed approach. However, we acknowledge that the current set of security patterns is not complete and there is a need to develop more security patterns to secure business processes from variety of risks. The usage of these patterns is illustrated on the business models of two business cases *i*) land management organisation and *ii*) construction organisation. Their complex execution of activities, significant IT dependency, and continuous data exchange between various stakeholders (for details see [Ahme 14b]) are the reasons to select these business cases. Two authors of [Ahme 14b] have performed the experiment and the results are discussed in [Ahme 14b]. However, due to unavailability of stakeholders, results could not be validated from the process owners.

3.4 Related Work

The use of security patterns in addressing security is not novel. A detailed survey [Yosh 08] described the adoption of security patterns during different stages (i.e. requirement, design and implementation) of information system development. The study discussed the application and methodology of security patterns to make the system secure. The study emphasises on security pattern application starting from the requirements engineering to design and implementation. Particularly at requirements stage, patterns are classified to *analysis process patterns* and *model-based patterns*. The analysis process patterns comprised of several patterns for asset valuation, threat assessment, vulnerability assessment, risk determination and enterprise security patterns adopted from [Schu 05]. Moreover, model-based patterns use models for analysis and specification of security requirements. Similarly, the proposed security risk-oriented patterns [Ahme 14b] comply to the requirements stage as the details included in three concept groups correspond to the analysis process patterns. Also, their representations using risk-ware business process modelling language come under model-based patterns. However, the proposed patterns are focused on business processes models.

Another study [Vare 13] proposed an automated selection of countermeasures by adding the organisational metrics and constraints in security patterns. The security patterns are integrated with a model linking security goals, descriptions of problems (i.e., vulnerability database), and solutions (risk treatment). The study uses security patterns to specify the security countermeasures in business processes formally. Therefore, the patterns include information to evaluate how much pattern is suitable among others. In contrast, security risk-oriented patterns address the problem of security requirements elicitation and their specification. In addition to requirements, patterns include information to specify the rationale for these requirements.

Röhrig and Knorr [Rohr 04] presented a method to derive security requirements by assigning the security level to business process components (i.e., artefacts, activities and actors) using a formal descriptive language. They define security levels into several categories. These categories include confidentiality, integrity, availability and accountability. These security levels are assigned to artefacts and activities while actors are assigned to the corresponding clearance levels to satisfy the respective security level. Consistency checks ensure that there are no conflicts between the modelled security levels and that actors have appropriate clearances to perform the tasks they were assigned to. Next, the appropriate security measures are automatically derived from a configurable rule-base regarded as a predefined matrix that maps security objectives to the security control. The method produces a catalogue of security measures for each participant, activity, and artefact of business process. These security assignments depend on the predefined rule-base. The approach is supported by software tool that facilitates business analysts in implementing security. However, the approach produces a catalogue separately, and therefore security can only be applied when the processes are defined in advance. The approach does not provide any details how they performed security risk analysis for corresponding security requirements. Therefore, the rationale for requirements is missing and also in the future the approach cannot perform risk assessments and requirements prioritization. On the other hand, the proposed security risk-oriented patterns provide rationale for security requirements and also in the future there is a possibility to complement these patterns with valuation of assets, likelihood analysis of potential vulnerabilities and their impact analysis. Such analysis would help in assessing the value for the likelihood and the possible consequences of identified risks.

In [Rena 09], the method is presented to derive requirements using patterns. Likewise, in security risk-oriented patterns, their method determines the collaboration of customers and technical consultants. Their method can be used for eliciting

security requirements but lacks the emphasis on risk management. A collection of security patterns proposed in [Schu 05] addresses several levels of abstraction, which perform risk assessment and mitigation. However, their applicability in business processes requires mapping to business process constructs.

In comparison to pattern-based approaches, other studies integrate risk management with business processes. Muehlen and Rosemann [Mueh 05] identify risk as an inherent part of every business activity. They have developed the techniques for risk-aware process modelling and presented a graphical extension of Event-driven Process Chains (EPC) to express risks. Similarly, Cope et al. [Cope 10] introduced risk-extended process models using BPMN. Their approach supports risk assessment, specification of vulnerabilities and countermeasures, but it lacks the specification of security requirements. Varela-Vaca et al. [Vare 11] have also extended the BPMN meta-model to add the risk-based concerns. They have adapted the concept of UML profile to model threat scenarios in separate pools attached to the business processes, which is too technical for business analysts.

An asset-driven risk assessment approach [Khan 10] addresses the problems to track of dependencies between organisation's assets and their realistic values. The approach focuses on business goals that involves the identification and evaluation of risk on a business process level, then find the aggregation based on their criticality, role and importance. They extended existing risk assessment approaches by introducing the risk evaluation using business processes. In contrast to existing approaches, the focus is on the business processes value rather than the assets. The reason is that the core business processes of an enterprise and their results are directly linked to enterprise revenue and therefore more valuable than the assets used or involved in accomplishing this process. Assets are part of the process. Therefore, they are indirectly assessed. The approach is applied in two phases: risk assessment and risk treatment. Authors highlighted the problems by keeping a track of asset dependencies, which help in estimating the asset values. However, in-depth risk analysis is missing and provides no mechanism for eliciting and representing security requirements in business process models. Similarly, an IT risk reference model [Sack 08] is proposed to highlight the causes of IT risks and their effects on business processes. Risk management methods are extended with the process-oriented view to align both economic and technological perspectives of business. The model consists of four layers: business Processes, IT applications/IT infrastructure, vulnerabilities and threats. This reference model serves as a foundation for formal modelling of the relation between causes of IT risk and their effect on business processes. The model is described in an abstract way and is

not related to security requirements elicitation, further it lacks a detailed security risk analysis.

3.5 Limitations and Future Work

In this contribution [Ahme 14b], we have used security patterns to bridge the gap between the security engineering and business process domains. The proposal has several limitations. Here, we mention these limitations and outline further research as future work to strengthens the proposed security patterns. Currently, in asset-related concepts, the security patterns are limited only to the identification and annotation of business assets and their security criteria in business models. Therefore, security patterns required a scale or criteria to perform asset valuation. Similarly, the security patterns lack risk assessments. Thus, the risk-related concepts should be complemented with risk assessments using in-depth assessment of identified threats and vulnerabilities including their impact analysis. Risk treatment concepts should also include the cost measurement to support the security trade-off analysis. Finally, the security patterns are maintained manually; a tool support can make the patterns' data, easy to maintain. Also, interconnect the security concepts of a single pattern across several patterns, which opens the possibility to integrate the security patterns with other existing knowledge bases of vulnerabilities or risks.

Chapter 4

Assessing Security in Business Process Models

Security architects are encouraged to use the proven solutions for security problems using security patterns. Documenting and publishing security patterns has become an area of intense focus in recent years. We take a deeper look into the various taxonomies in which the business process models and security have been classified. We find that existing taxonomies do not support security across the business modelling perspectives. In this contribution [Ahme 13], we propose a comprehensive *three-dimensional taxonomy of business process security*. The taxonomy is subsequently used to classify security risk-oriented patterns and identify their potential occurrences to deploy these security patterns in business processes.

4.1 Research Method

The overall research method (see Figure 4.1) of developing *business process security taxonomy* consists of three steps. Initially, the survey of existing taxonomies and architectures for security assessment and business process modelling is conducted (i.e., *Step 1*). The goal is to identify the core concepts of both domains. The survey gives two primary outcomes. Firstly, two aspects of business process modelling, i.e., hierarchical abstraction and perspectives (see Section 4.2). Secondly, identify security objective, security policy, security control and security requirement as multifaceted attributes of security assessment in information system. On the basis of these outcomes, a taxonomy of business process security is developed in *Step 2* that defines the relations between the characteristics of both domains derived in

prior step (see Section 4.2). Finally, the application of taxonomy is performed in *Step 3* using an example process. The application of taxonomy classifies security risk-oriented patterns [Ahme 13]. Also, it illustrates how these patterns could be applied in business process models.

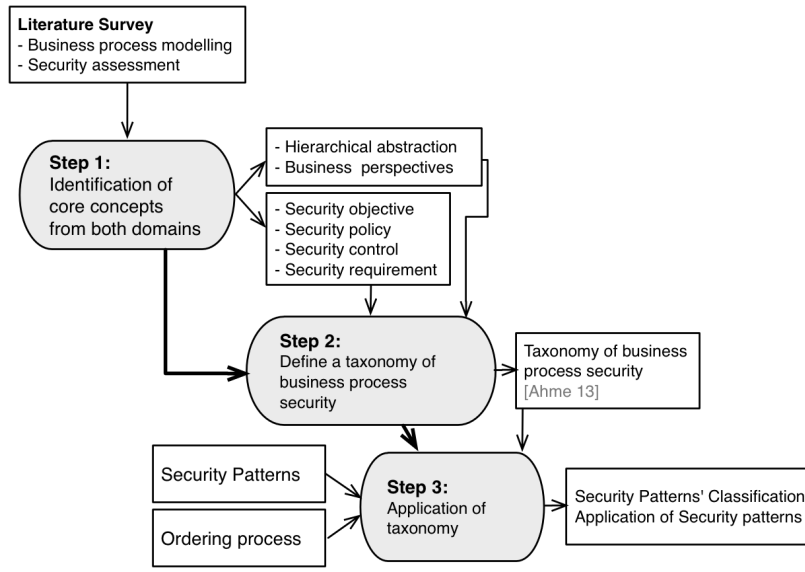

Figure 4.1: Research method applied for developing the business process security taxonomy

4.2 Taxonomy of Business Process Security

Security risk-oriented patterns [Ahme 12a, Ahme 14b] overlap two domains, namely business processes and security risk management, and comprehend three major concepts of ISSRM domain model (see Section 3.3.1): *i*) *security context* to define organisation's assets and their security criteria; *ii*) *security problem* describes a risk, its impact and the attack method to exploit vulnerabilities and execute threat; Also, *iii*) *security solutions* to solve the identified security problems by defining one or more countermeasures applied to treat the risks. Classification requires a common attribute of the pattern that exists in both domains (i.e., business processes and security), otherwise the pattern would capture information that belongs to a single domain. The organisational asset is identified as a common attribute that exists in business process models and also drives security risk analysis (see Section 2.2.1). In business process models, the organisation's asset exists at

one of the three hierarchical levels (described in Section 4.2.1) represented by one of the four business perspectives (see Section 4.2.2). Finally, security criteria (see Section 4.2.3) are defined as constraints on asset(s), in other words, they are constraints on the business perspectives. In order to present these details, proposed taxonomy of business process security characterises three dimensions, illustrated in Figure 4.2. The dimensions are conferring to the domains of business processes and security. The first two dimensions (i.e., business process hierarchy and business perspective) describe business processes. The third dimension addresses security concerns within the prior two dimensions. In accordance with the three concepts of the security pattern, the security context in a pattern characterises the organisation's assets and their security criteria. Therefore, we use *security context* of a pattern to derive the following attributes: *i*) what (i.e., asset), *ii*) how (i.e., security criteria) to secure and *iii*) where (i.e., at which level in business models) we can apply the security patterns. Next section briefly describes the granularity of these dimensions.

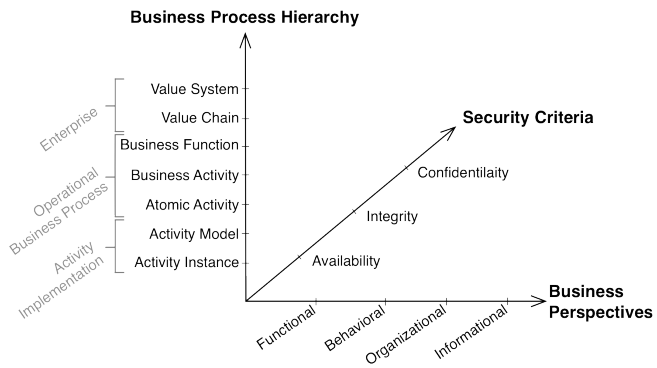

Figure 4.2: Three dimensions of the business process security taxonomy

4.2.1 Business Process Hierarchy

As described in Section 2.1.1, *hierarchical levels* deal with the levels of business process hierarchy and describe how the business performs based on the level of details provided in the business process diagrams. We have adopted the classification performed by Weske [Wesk 12] and grouped the vertical hierarchy of a business process model at the following three levels:

Enterprise comprises of *value system* and *value chain*. Value system characterises the relationship of an organisation to its business environment. Each

value system consists of a number of value chains, each of which is associated with one organisation. Value chains organize the enterprise business functions and relate them to each other (as businesses cooperate with each other to achieve their business goals), providing an understanding of how a company operates.

Operational business processes show the functional decomposition of the value chain. The business functions are broken down to functions of smaller hierarchy and ultimately, to activities of operational business processes. The leaf level functions of the decomposition are called activities. After decomposition, execution constraints are introduced to relate activities to each other. The phenomenon transforms the business functions to the operational business processes.

Activity implementation comprises of activity models and activity instances. Activity models show the description of an activity expressed in different forms, for instance, by plain text or by some formal specification or references to software components that implement them. For example, a user-defined model that lies at M1 layer of Meta Object Facility (MOF) [OMG 06] in OMG. The activity instances characterize the actual work conducted during business processes. For example, Object diagram lies at M0 layer of MOF [OMG 06]. Furthermore, each activity instance has different states i.e., *init*, *enabled*, *ready*, *skip*, *running*, *terminate* and *closed*.

The dimension can describe a complex business process at different level using dedicated constructs at each level. The relation between the process hierarchical levels is aggregation meaning the levels are interrelated, where, the lower level objects make it up to a higher level component [Krog 12]. In business process models, business functions are merely used and according to [Mueh 05, Cope 10, Vare 11, Khan 10] security risk is considered as an inherent part of business activity. Hence, in this thesis, we restricted our scope towards the business activities and its decomposition (i.e., atomic activity).

4.2.2 Business Process Perspectives

The second dimension is derived from [Curt 92, Krog 12, Star 94]. It deals with four modelling perspectives (i.e., functional, behavioral, organisational and informational) of a business process model, which represents business assets that a business process can have. These perspectives also served as a foundation and they are frequently used as classification of business process modelling. We have used following business perspectives to classify business assets in a business process model: *i*) *Functional perspective* represents activities that are being performed to transform the input to an output. Functional perspective includes function, pro-

cess, activity and task as process elements [Krog 12]. *ii*) *Behavioral perspective* represents the states and transition between states. It includes the following concepts of business process modelling language, state, event, condition and transition [Krog 12]. It describes the execution order of activities (e.g., sequencing) and the behavior how they are performed, i.e., loops, iteration, complex decision-making conditions, entry and exit criteria. *iii*) *Organisational perspective* represents the organisational unit, the role, the (individual) human, and the (automatic) resource, where and by whom the business activities are performed [Curt 92]. *iv*) *Informational perspective* describes the informational entities produced or manipulated by a process. These entities include data, artefacts, products (intermediate and end), and objects; it includes both the structure of informational entities and the relationships among them [Curt 92].

4.2.3 Security Criteria

In the taxonomy, this dimension represents security constraints on the assets. Therefore, we adopted security objective to identify the security dimension. To be consistent with security patterns, we use the CIA model [Info 91] that focusses on confidentiality, integrity and availability (see Section 2.2.2). As discussed in Section 2.2.2, there exists other security criteria (i.e., authorization, non-repudiation and privacy) but they can be formulated by combining the basic three security criteria used in this dimension.

4.3 Application of Business Process Security Taxonomy

The section demonstrates the application of *business process security* taxonomy. The goal of this application is to classify security risk-oriented patterns [Ahme 12a, Ahme 14b] and to facilitate business analysts to apply these patterns in the business process models. Now that a structural foundation is defined (i.e., taxonomy). Next, both the security patterns and business process models should correspond to it. Therefore, concrete steps are needed to classify both the security patterns and business models such that they correspond to the propoed taxonomy. The application process (depicted in Figure 4.3) of proposed taxonomy is divided into three activities.

1. Classification of security patterns. The goal of this activity is to align security patterns with the proposed taxonomy. Conferring to *security context*

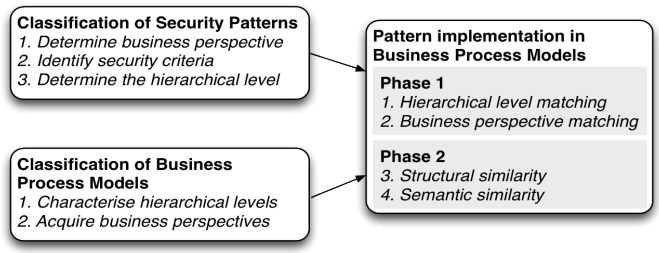

Figure 4.3: Application of security risk-oriented patterns using taxonomy

from security risk-oriented template [Ahme 11], in *Step* (*i*) *Determine business perspective*, we determine asset (i.e., business perspective) that a particular pattern secures. In *Step ii*) *Identify security criteria* identifies security constraint (i.e., security criteria) on asset. Then, we analyse the graphical representation of pattern in *Step* (*iii*) *Determine the process hierarchical level*, to determine the hierarchical level where the pattern can be applied. The concrete steps, illustrated in Figure 4.3, are defined in [Ahme 13] along with its application using an example. These steps result in *asset* (from Step (*i*)) and *hierarchical level* (from Step (*iii*)) that provide common foundation, which also exist in business process model. In later activities, the information is matched to see if pattern is applicable in a particular business process or not, if it is applicable then security information is added to business process model (for details see [Ahme 13]).

2. Classification of business process models. The goal of this activity is to align business process models with the two dimensions of taxonomy, namely *hierarchical levels* and *business perspectives*. The idea is to characterise hierarchical levels of business process (Step (*i*)) to find, which level of details are given in business process model. In Step (*ii*) we identify the business perspectives. The activity results in hierarchical level (from Step *i*) of a business process model and business asset(s) (from Step (*ii*)) that exists in this model. The output information of this activity is used to verify if a business process model has a particular asset that is secured by a particular security pattern. In [Ahme 13], we classify an example of business process models to illustrate the execution of this activity.

3. Pattern implementation. It is the final activity in the application process. The activity is carried out in two phases using a 4-step matching process as described in Figure 4.3. The first phase takes output from above activities. This phase ascertains that both the security pattern and operational business process have the required preliminaries to apply the pattern and is attainable using *hierarchical level matching* and *business perspective matching*. The second phase focusses

on finding the structural and semantic similarities between the elements of security pattern and business process (or fragment of business process). After performing a 4-step process, the results from each step are united to conclude if the security patterns can be applied in a business process or not. In this regard, the output of each step should approve that the pattern and a business process matches in their hierarchical level (Step 1) and business perspective (Step 2). Additionally, if the structure (Step 3) of the security pattern is similar to the elements or fragment of a business process model and also their semantics are identical, then, the pattern can be applied in a business process model. Otherwise, if any of the result from the above four activities dissuade, then, the security pattern is not applicable in the business process.

The objectives of proposed taxonomy are to classify security patterns and specify their implementation in the business process model. In [Ahme 13], we demonstrate how these objectives are achieved by applying the proposed taxonomy. During the application the steps in the first activity (i.e., Classification of security patterns) is used to classify security risk-oriented patterns [Ahme 14b]. The security patterns are classified on the basis of business asset (that they are protecting), their security criteria and where it can be applied in the business process model. Once the patterns are classified, next, we apply steps proposed in the second activity (i.e., Classification of business process models) to classify an example business process to identify business assets and their hierarchical level. This activity helps to align the process with security patterns. Finally, the output from these activities is matched in last activity (i.e., Pattern implementation). This activity checks if the security patterns are applicable in business process models (see details in [Ahme 13]).

4.4 Related Work

The notion of proposing taxonomy is not novel. The idea behind the taxonomy is to gain an understanding of the characteristics and nature of a language or domain (e.g., business processing modelling or security) to address the domain inadequacy or deficiency.

There exists several approaches for classifying different aspects of business process modelling as according to their needs. A framework [Agui 04] classifies business process modelling techniques using two dimensions, namely *purpose of the model* and *change model permissiveness*. In the first dimension, the business process models are classified into four types based their purpose, i.e., learning,

decision support for process development and their execution and control, support for information technology. The second dimension *change model permissiveness* characterises a model as active or passive models. The study focusses on tools classification rather than the structural classification of business modelling languages. The study [Verg 08] classifies business process modelling techniques in three sets. These sets comprised of diagrammatic models, formal/mathematical models and executable models. The classification focusses on the structural characteristics of a business process models and their capabilities specialised in the context of analysis and optimisation. In [Rych 11], business process modelling are classified in two categories, *prescriptive processes* (having have a predictable sequences of activities) and *descriptive processes* (illustrate actor collaboration and resource exchange with weak predictability of activity sequences). These categories are further distinguished as *context-specific process* that depends on the context and *configurable process* that need to be customised in accordance with the context. A conceptual framework [Mela 00] organises business processes in four different views, deterministic machines, complex dynamic systems, interacting feedback loops and social constructs. The primary focus is to understand and view different aspects of an organisation using business process modelling. These views overlap each other, and lack of formal distinction makes the classification less favorable. A framework [Giag 01] proposes three dimensions to integrate a business process modelling taxonomy and information systems modelling techniques. Firstly, *breadth* deals with the goals and objectives of a modelling language. Secondly, *depth* considers the modelling perspectives of a language adopted from [Curt 92]. Finally, *fit* illustrates the typical projects to which the technique can be applied. The framework assists the decision makers in evaluating and selecting suitable modelling techniques, depending on the characteristics and requirements of individual projects. Another framework [Aitk 10] aligns various concepts and representations of organisational actions within the context of business process modelling. It uses a top-down approach to hierarchically define four levels, i.e., contextual, conceptual, logical and physical. The framework has two alternative views, *service oriented view* deals with sequencing of actions, and *function oriented view* focusses on their classification. The framework guides in defining the scope of business concepts and their level of specificity in business process architecture, but it does not distinctly represents the modelling perspectives (i.e., function, behavior, resource or data) of a process.

The study [Fire 04] provides an overview of concepts used in security and illustrates their relationships to define security requirements. It describes security into a hierarchical taxonomy as quality subfactor. The taxonomy is applicable

to business process models at an abstract level as security is addressed as vulnerability in assets rather than describing as technical security solutions. The taxonomy is similar to the security dimension proposed in this chapter, although we have defined security objectives using CIA model [Info 91] and consider that other security objectives can be aggregated from them. A thorough study [Igur 08] examined the existing security-related taxonomies to see their efficacy in security assessment. The study proposed a basic set of characteristics to develop a new taxonomy for assessing security, which can be used as a framework to examine new systems in identifying their vulnerabilities. The study reveals that an efficient method to organise attack information is using a hierarchical method starts with the impact of an attack and move down to identify the vulnerabilities. The approach mainly focuses on the classification of attacks rather on the security itself. Another notable survey [Hafi 06] highlights the problems of finding security patterns and emphasises the necessity of scientific classification of security patterns. The study claims the pattern searching would be better if multiple views are incorporated in security patterns. In [Hafi 07], they classify patterns based on security objectives using CIA model [Info 91], application context, threat type using STRIDE model [Swid 04]. Moreover, they proposed a classification based on a tree structure combined with the STRIDE model to join the software and security view in terms of security patterns. Cheng et al. [Chen 03] classify security patterns using the aspect types [Gamm 95] of the patterns (i.e., creational, structural, or behavioral) and the abstraction level (network, host, or application). The classification of security patterns in [Schu 05] is based on Zachman's framework for enterprise architecture [Zach 87, Sowa 92]. It is presented along two dimensions. The vertical dimension illustrates the architectural views characterising these views on the interrogatives *what*, *how*, *where*, *who*, *when*, and *why*. The horizontal dimension deals with the levels of information models, where the top two layers cover the enterprise levels, and the bottom three address the system levels. The security should be implemented all levels of models from enterprise to technology; therefore, Schumacher et al. [Schu 05] introduce a new column to include security view. They have classified the security patterns only listed in their book. Their approach is similar to the one proposed in this chapter while it is more specific for business process modelling. Therefore, the vertical dimension represents the business processes hierarchically, and the horizontal dimension reflects the business perspectives and a new dimension is introduced to address security. The above classification of security patterns [Hafi 07, Chen 03, Schu 05] are mainly used to classify the security patterns that include technical details related to security controls while on the other hand our approach concerns with the

specification of security requirements and is generic for business process modelling. In [Ahme 13], we illustrate our concept using BPMN, though it can also be applied to other business modelling languages.

4.5 Limitations and Future Work

In [Ahme 13], we have presented a taxonomy that integrates business process modelling with the security criteria aimed to define a process-oriented classification scheme for security risk-oriented patterns. The taxonomy focusses on applying security patterns in business process models. Therefore, the current classification is restricted to the patterns' security context, which includes the attributes assets (i.e., business perspective), its constraint (i.e., security criteria) and hierarchical level of business process models. However, this classification scheme has a limitation that it does not consider the security risk management concepts (i.e., vulnerability, threat, attack method, risk and etc.), which can be a potential future work to extend this taxonomy. In proposed taxonomy, the security dimension only deals with security objective specification, which does not fully incorporate the requirement engineering perspectives to align the comprehensive security specification (as mentioned in Section 2.2.2). Therefore, together with the security objective specification, the security dimension requires specifying security policy, security requirement, security control and their smooth translation, within the business process hierarchy. This future work can be a valuable extension to the proposed taxonomy in defining a universal business process security model (e.g., ontology, meta-model). Another limitation of proposed taxonomy is the application of security patterns, which is currently performed manually. However, there are interesting approaches [Ekan 12, Dijk 11, Dong 08] presented in business process community in the area of business process similarity that support the structural and semantic similarity up to a certain extent, as in these offerings there is the potential to automate or at least semi-automate the patterns' application process. Finally, we also acknowledge the need of validating the taxonomy in an empirical fashion by testing its dimensions in real-world business process models.

Chapter 5

Security Requirements Elicitation from Business Processes

Security patterns facilitate business analysts in analysing security risks and provide a rationale for security requirements in a way that is understandable by business analysts. Also, the taxonomy of business process security integrates security with business processes making the patterns' application in business process models. However, these contributions lack a systematic elicitation of security requirements. Furthermore, requirements are described at a general level, which needs to be expressed in more detail with respect to particular context of an enterprise. To overcome these problems: firstly, security requirements described in security patterns are refined, and security requirement model is generated from business process model (see [Matu 13]). Secondly, we proposed a method –security requirements elicitation from business processes (SREBP)– to elicit security objectives from business process models and translate them to security requirements (see [Ahme 15]). We apply and validate SREBP method in the Genome Centre case study. In the validation, we check the completeness and efficiency of SREBP method against security quality requirements engineering (a.k.a., SQUARE) method.

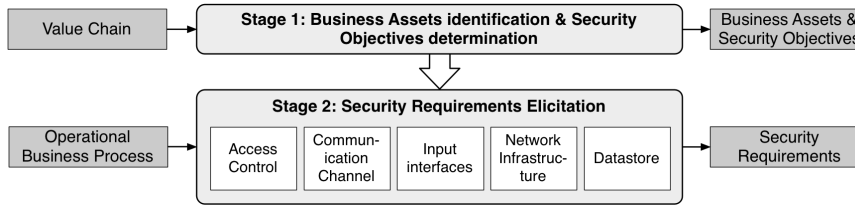

Figure 5.1: SREBP – Security Requirements Elicitation from Business Processes

5.1 Security Requirements Refinement

The idea behind the refinement of security requirement is to take the early requirements described in security risk-oriented patterns and generate the security model from a business process models that represents the detailed security requirements along with its context. In [Matu 13], we illustrate how early requirement *check for the access permissions*, presented in SRP4 [Ahme 14b], is refined to the RBAC security model. The approach is adopted in SREBP method (see Section 5.2) to develop security models for others security patterns [Ahme 14b] to elicit their detailed security requirements.

5.2 SREBP Method

The method is based on the domain model for information system security risk management (ISSRM) [Dubo 10] and the security risk-oriented patterns [Ahme 14b]. The section briefly introduces SREBP method. A detailed application of SREBP method is illustrated in [Ahme 15]. The method consists of two stages (as illustrated in Figure 5.1). Firstly, *Stage 1: Business assets identification & security objectives determination* describes how to identify business assets and to determine their security objectives from the value chain and business process diagrams. The identification of business assets and their security objectives is performed using the ISSRM domain model [Dubo 10] (for details see [Ahme 15]). Secondly, *Stage 2: Security requirements elicitation* supports eliciting security requirements from the operational business process within five contextual areas –access control, communication channel, input interface, network infrastructure, and data store. The contextual area of *Access control* is related to inter- and intra-organisational concerns and specifies the access control policy where different roles perform operations and access data in the system, to change the state of protected asset. In the case of *Communication channel*, one considers how data are exchanged or commu-

nicated between business entities or stakeholders. In the case of *Input interfaces*, one analyses how input data are treated before accepting them for processing. In the case of *Network infrastructure*, one needs to protect the network infrastructure connecting LIMS to an external or local networks used to perform business operations for their availability. Finally, the *Datastore* contextual area concerns data protection when storing or/and retrieving to/from the datastore. It is important to note that each artefact –*data* or *process*– separately considered and protected at each contextual area, contributes to the security of business assets identified at the first stage. The SREBP method uses security patterns to elicit security requirements in order to protect the identified assets. In SREBP, the security requirements are described in detail using security models (e.g., SecureUML and UML) in each contextual area. The requirements contribute to the achievement of one or more security criteria, i.e., confidentiality and integrity of data, integrity and availability of business activity. A single pattern may be associated to multiple security criteria; thus, one security requirement could potentially contribute in accomplishing more than one security criteria.

5.3 Security models

In SREBP method, security models are generated from the contextual area except for input interfaces. The idea is to analyse security for identified assets in detail because the respective security models (e.g., RBAC model) have dedicated constructs to explore the scenario. It leads to three major benefits: firstly, such security analysis would not be possible in business process modelling languages due to lack of dedicated constructs because the primary objective is to represent the enterprise's business process. Secondly, due to these independent representations of security models, the business process models are not overwhelmed with the security related details that have no primary use for a business analyst. Finally, the security models ease the implementation of security requirements, for instance there exists several mechanism to implement RBAC model. These security models are derived from a particular context (e.g., access control, communication channel and etc.) within a certain scenario (e.g., Genome Centre in [Ahme 15]). Therefore, the security models cannot be reused in any other scenario; however, the security patterns are defined in a general way, which can be reused in different scenarios.

The proposed taxonomy [Ahme 13] discusses different abstractions of business processes (i.e., enterprise level, operational business process and activity implementation). However, currently the thesis addresses security at operational

business processes particularly the enterprise's activities whose execution is supported by their information system or its architecture. It also includes individuals and business partners coordinating with these activities at this level. Therefore, SREBP method relies on the information captured in the business process models. During SREBP application in [Ahme 15], we assume that the business process models completely represent the scenarios necessary for their LIMS. Hence, any missing activity in the business process model would miss the security analysis performed in SREBP.

5.4 Case Study

5.4.1 Design

SREBP method is validated in the case study of Estonian Genome Centre. The advantages of using case study methodology are described in [Ahme 15]. We have adopted a holistic case study approach [Yin 09] where the case Genome Centre is studied as a single unit. The case study design (see Figure. 5.2) consists of three major activities, out of which the first activity (i.e., SREBP Application) illustrates the application of SREBP method details are provided in [Ahme 15], while the second activity corresponds to the application of SQUARE method (see Appendix I in [Ahme 15]). SQUARE method is used to validate proposed method by comparing the results from the application of both methods. The activity uses a comparison criteria (described in [Ahme 15]) to measure the *completeness* and *efficiency* of both methods. For this purpose, the activity input the resulting security requirements from the application of both methods.

5.4.2 Execution

The Genome Centre had already modelled their operational business processes, which served as input to the case study. The operational business processes include the enterprise's activities whose execution is supported by the information system or its architecture [Wesk 12]. They also highlight individuals and business partners coordinating with the enterprise's information system to achieve the business goals of the enterprise. Both methods are applied by a team of two persons (first and third author of [Ahme 15], having different expertise, security and business respectively) over the period of five weeks. Once the application is completed, we proceed to verify the elicited security requirements. The verification was carried out in two meetings with the domain expert, each of about 2 hours.

During these meetings the security requirements were verified in terms of their relevance to the system-to-be, i.e., LIMS, which is then followed by small revisions to few requirements. Next, the requirements elicited from both methods are categorised according to eight generic categories adopted from the existing literature [ITSE 91, Fire 03b, Schu 05]. These generic categories belong to the security domain that classify the application of security in an information system. The idea is to compare the completeness of these methods by reducing the comparison complexity by classifying the security requirements from both methods at a more granular level (i.e., each category) [Bail 96, Smit 81] (for details see [Ahme 15]).

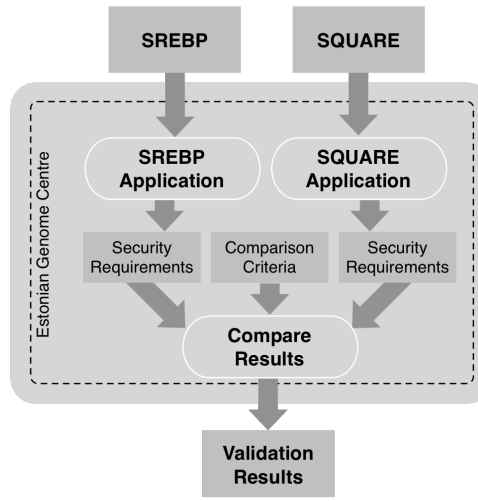

Figure 5.2: Validation process of SREBP method

Validation results consisting all the identified business assets of Genome Centre are presented in [Ahme 15]. The results show that SREBP method reaches a coverage of almost 80% of completeness in addressing security for the Genome Centre business assets whereas coverage of SQUARE is close to 44%. Similarly, application of SQUARE method took 17 person-hours more than that of SREBP method. Thus, SREBP is 27% more efficient (79/62=1,27, i.e., 27%) as compared to SQUARE. The results conclude that SREBP method is better suited in eliciting security requirements from business process models. The SREBP method enables early security analysis and allows business analysts not only to understand how to protect secure business assets, but also contributes to the alignment of business process models with the technology that supports the secure execution of business processes. The validity of case study results (presented in [Ahme 15]) may be

affected by few threats. We have discussed these threats in detail (see [Ahme 15]), particularly regarding reliability, construct validity and external validity.

To reduce the learning effects, first we performed the SREBP application. Therefore, the carry-over effects to perform SREBP application in less time is avoided because the participants are not familiar with the operational business processes. Whereas SQUARE application is effected by the carry-over effects because participants became familiar. Similarly, during the verification of security requirements, SREBP requirements are verified first to avoid the carry-over effects of performance. Because the domain expert spent time to understand the rationale for these requirements, whereas in SQUARE application the domain expert become aware of the security rationale and is performed relatively quick.

5.5 Related Work

Fabian et al. [Fabi 10] conducted a thorough study comparing the security requirements engineering methods and organized them into several categories. We have compared few of them with the SREBP method:

Multilateral approaches, such as Multilateral Security Requirements Analysis (MSRA) method [Gurs 06] and Security Quality Requirements Engineering (SQUARE) method [Mead 06] consider security requirements of all stakeholders and resolve conflicting security requirements from different stakeholders [Gurs 06]. MSRA analyses security needs for system-to-be, identify conflicting interests and security goals, and develop different stakeholder views. SQUARE facilitates the collaboration between the requirement engineers and stakeholders. MSRA and SQUARE, both methods use CIA [ITSE 91] in defining the security goals. SREBP method considers the security needs of other stakeholders particularly in access control context. However, only in the interest of information systems and exempt the security goals that are solely in the interest of other stakeholders, i.e., business partners. Currently, SREBP method focuses on security requirements elicitation without examining the conflicting security requirements between the system's business partners.

UML based approaches like Misuse cases [Sind 05], SecureUML [Lodd 02], and UMLsec [Jurj 05] focus on system design. Misuse cases represent unwanted behavior of the system-to-be. They are complemented with template that include details regarding security threats analysis. SecureUML is suitable to express role-based access control policies for distributed systems. UMLsec uses different UML diagrams to represent the requirements with the help of UML profile (i.e., stereo-

types, constraints, and tagged values). Like UML approaches, SREBP method uses security risk-oriented extensions [Altu 12, Altu 13] for business process modelling languages. These languages illustrate the security requirements graphically together with its rationale. Additionally, SecureUML and UML interaction diagrams are used to define the security models for SREBP's contextual areas, i.e., access control, communication channel, network infrastructure and datastore.

Goal-oriented approaches, such as Knowledge Acquisition in Automated Specification (KAOS) [Lams 07], Secure i^* [Elah 07], Secure Tropos [Mour 07], and Goal-Based Requirements Analysis Method (GBRAM) [Anto 01] facilitate the requirements elicitation and specification by providing the rationale for a particular requirement [Yu 98]. The introduction of goal analysis and specification remove ambiguity and conflicts from the requirements, bring transparency and traceability to the requirements specification. KAOS helps one to analyse requirements, their conflicts, and model anti-models to elicit security requirements. KAOS is targeted towards the completeness, consistency, and feasibility of requirements along with their specifications. Secure Tropos and Secure i^* deal with the whole system development process, but strongly focus on the early development steps. Similarly, GBRAM utilizes the goal and scenario-driven requirements to formulate privacy and security policies, but with a focus on the confidentiality. In business process modelling, there exists constructs to model the organisational aspects of enterprise especially focuses on the interaction of enterprise and stakeholders [Ahme 13]. SREBP utilises these features to elicit the security objectives from the value chain that are later considered and refined to security requirements. This hierarchical abstraction of business process modelling leads to trace these requirements to their origins naturally.

Security in business processes is integrated with several ways; security objective elicitation, security requirements specification/modelling, security risk-driven approaches and security requirements conformance checking. Majority of these practices correspond partially to the overall business security or applicable to a certain extent. A model-driven approach [Wolt 09] expresses security goals at the business process level. A generic security model specifies security goals, policies, and constraints based on a set of fundamental entities, such as objects, attributes, interactions, and effects. They further discuss a translation of security annotated business processes into security configurations. Similarly, a framework [Herr 06] distinguishes the business process elements and expresses the standard security requirements in 14 detailed security requirements. The security requirement are presented through the symbols mapped to business process elements. These approaches focus on the description of abstract security goals, and their

mapping to the technical specification to ensure that security constraints are not violated. However, they neither define any graphical notation for specifying security goals or security requirements in business process models nor explain the systematic elicitation of security goals or requirements. Therefore, the approaches will work fine if the business analysts already aware of their security goals.

In addition to keep the business rules consistent by introducing security mechanisms, [Rohr 04, Mona 12] provide means to express the security requirements in business process models. In [Rohr 04] a formal descriptive language is used to derive security requirements that assign security level to business process components. The levels are then checked for consistency, and security measures are derived using a configurable rule-base that maps security objectives to their controls. Similarly, a tool-supported framework [Mona 12] extends the modelling and execution of business processes to support the specification, execution and monitoring of the security and safety constraints protecting the business assets. These studies [Rohr 04, Mona 12] only provide means to express the security requirements in business process models.

Several approaches, [Menz 09, Rodr 07, Pavl 08, Mull 11], focus on the graphical aspects of security requirements and proposed extensions for business process modelling language to represent the security requirements graphically. Menzel et al. [Menz 09] proposed a model-driven approach by extending the security elements for business process modelling to describe security requirements. This allows evaluating enterprise assets, describe trust and later translating them to security controls for service-based systems. Rodríguez et al. [Rodr 07] also extended BPMN using padlocks to annotate business processes with security requirements. The early security requirements are expressed with a particular padlock symbols. Similarly, Christopher and Joe [Pavl 08] 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. Mülle et al. [Mull 11] proposed an annotation language embedded to express security requirements as structured text annotations in business process models. The annotation language covers the requirements from authorization, authentication, auditing, confidentiality, integrity, and security-, privacy- and trust-related user involvements. These approaches facilitate graphical aspects of security requirements and neglect the elicitation of security requirements. Furthermore, the approaches do not take into consideration the rationale for the security requirements.

A Model-driven framework [Vare 11] extend the meta-model of business process models to perform a risk assessment in different stages of modelling, from

a high abstraction level to an executable level. The framework performs an automatic checking to confirm if business process models conforms to the required security objectives.

Paja et al. [Paja 12] specify social commitments by analysing the participant's objectives and their interactions, which are considered as the high-level specification of security requirements. Security requirements are annotated in BPMN using conversation and choreography diagrams. Though it gives the rationale for security, but the requirements are limited to the exchange of resources. Moreover, a detail semantic mapping between organisational model and BPMN is also missing.

5.6 Limitations and Future work

Currently, SREBP method only deals with the intentional or deliberate security risks. In the future, we plan to extend the notion of security concept adopted to incorporate the security-risks related to unintentional or accidental harm to the information systems in SREBP. The new security concept would align the SREBP method with the comprehensive security specification defined in [Maye 09, Dubo 10]. Similarly, the security objectives are defined in terms of the CIA model [ITSE 91], other security objectives [Scan 08] (e.g., authorization, non-repudiation and privacy) are also a subject to change. Another limitation of SREBP method is that it does not perform the valuation of assets, likelihood analysis of potential vulnerabilities and their impact analysis. Such analysis would help in assessing the value for the likelihood and the possible consequences of identified risks. Thus, we propose a future work to strengthen SREBP method with the technique integrated with the business processes that performs the likelihood analysis of potential vulnerabilities and their impact analysis. Currently, SREBP method generates security models manually from the business process model; an automated approach is needed in the future to trace and apply changes in security models when the respective business process models are modified. Additionally, SREBP method does not prioritise the security requirements; a technique is needed to facilitate business analysts to decide, which security requirements should be implemented in case of limited time, resources, or finances.

Chapter 6

Conclusions

The overarching goal of this thesis is to gain a deeper understanding of exactly how security engineering can be aligned with business processes to elicit security requirements for an information system. For this purpose, we believe that we have provided more insight into the domains by considering two important aspects of security in business processes, namely the systematic elicitation of security requirements keeping their rationale intact on the one hand, and their graphical representation on the other hand.

In particular, the thesis has proposed three complementary contributions: Firstly, security risk-oriented patterns (in Chapter 3) that integrate the security risk analysis into business process models. The contribution includes a structured specification (i.e., security risk-oriented template), and a modelling language that supports security risk concepts in business process models that business analysts can understand easily. Secondly, the taxonomy for assessing security in business processes (in Chapter 4) that integrates security in business processes domain. The taxonomy classifies the proposed security risk-oriented patterns and identifies their potential occurrences to deploy these patterns in business process models. Finally, a method, security requirements elicitation from business processes (SREBP) (in Chapter 5), is developed. The method allows early security analysis by determining the security objectives from business process models and their systematic translation to security requirements. The method uses the domain model of information system security risk management and security patterns. The elicited security requirements are then described in detail using the system's contextual areas.

These contributions work together to support the security requirements elicitation from business processes, where *i*) the identification of business assets and determination of security objectives are carried out from the enterprise's organisational business processes. Moreover, *ii*) the elicitation of security requirements are performed on the operational business processes using contextual areas. The usefulness of the first contribution has been validated through the industrial cases. The second contribution is validated using a constructed example. The third contribution is validated using a case study to check its completeness and efficiency in eliciting security requirements and how it contributes in securing business assets against security quality requirements engineering (SQUARE) method.

Future work

In this thesis, we have aimed at a systematic approach for eliciting security requirements from business processes. The thesis bridges the gap between business process modelling and security domains using security patterns. Nevertheless, the contributions and limitations of the thesis highlight that substantial further research can be conducted in this area. In particular, we identify the following future works:

- The current set of security patterns is not complete. Therefore, we need to extend the current set of security patterns. The new security patterns would not only cover additional risks and vulnerabilities within the current scope, but also broaden the notion of security (defined in [Maye 09, Dubo 10]) to include more variety of security-risks and vulnerabilities. In addition, this will cover the unintentional or accidental harm to the information systems.
- Current approach is missing the in-depth assessment of assets, risks, and vulnerabilities. The work conducted in this thesis can be complemented with the in-depth assessment that includes assets' valuation, likelihood analysis of potential vulnerabilities and threats along with their impact analysis. On the basis of these assessments, security requirements can be prioritised to facilitate business analysts in selecting necessary security requirements. The prioritization can include cost measurement to support the security trade-off analysis in case of limited time, resources, or finances.
- The taxonomy only covers the specification of security objective in the security dimension; the scope of the security dimension can be extended to include security policy, security requirement, and security control. The ex-

tension can fully incorporate the requirement engineering perspectives to cover the security specification comprehensively.

- As demonstrated in this thesis, currently all the activities are performed manually. Therefore, a software tool support is needed to manage security patterns. The tool integration with existing knowledge bases (digitally available catalogue of vulnerabilities, risks or other security-related concepts) can keep the patterns up-to-date and improves the patterns' productivity. Moreover, the tool can help in finding the structural and semantic similarity up to a certain extent, to automate or at least semi-automate the application of security patterns in business process models and to generate the respective security models. Furthermore, it can help to guarantee the traceability between these models when different steps are performed in SREBP method.

References

[Acco 13] R. Accorsi. **Security in Business Process Management**. *it – Information Technology*, Vol. 55, No. 6, pp. 215–216, 2013. 17

[Agui 04] R. S. Aguilar-Savén. **Business process modelling: Review and framework**. *International Journal of Production Economics*, Vol. 90, No. 2, pp. 129 – 149, 2004. 63

[Ahme 11] N. Ahmed and R. Matulevičius. **A Template of Security Risk Patterns for Business Processes**. In: *Perspectives in Business Informatics Research, Riga, Latvia*, pp. 123–130, Riga Technical University, 2011. 47, 62

[Ahme 12a] N. Ahmed, R. Matulevičius, and N. H. Khan. **Eliciting Security Requirements for Business Processes Using Patterns**. In: *WOSIS 2012 - Proceedings of the 9th International Workshop on Security in Information Systems*, SciTePress, 2012. 49, 58, 61

[Ahme 12b] N. Ahmed, R. Matulevičius, and H. Mouratidis. **A Model Transformation from Misuse Cases to Secure Tropos.** In: *Proceedings of the CAiSE'2012 Forum*, pp. 7–14, CEUR-WS.org, 2012. 13, 37

[Ahme 13] N. Ahmed and R. Matulevičius. **A Taxonomy for Assessing Security in Business Process Modelling**. In: *RCIS*, pp. 1–10, IEEE, 2013. 21, 22, 57, 58, 62, 63, 66, 69, 73

[Ahme 14a] N. Ahmed and R. Matulevičius. **A Method for Eliciting Security Requirements from the Business Process Models**. In: *Proceedings of the CAiSE'2014 Forum*, pp. 57–64, 2014. 21

[Ahme 14b] N. Ahmed and R. Matulevičius. **Securing Business Processes Using Security Risk-oriented Patterns**. *Comput. Stand. Interfaces*, Vol. 36, No. 4, pp. 723–733, June 2014. 13, 20, 21, 30, 45, 49, 50, 51, 53, 56, 58, 61, 63, 68

[Ahme 15] N. Ahmed, R. Matulevičius, and F. Milani. **Security Requirements Elicitation from Business Processes (SREBP)**. *Submitted to Requirements Engineering*, 2015. 21, 22, 50, 67, 68, 69, 70, 71, 72

[Aitk 10] C. Aitken, C. Stephenson, and R. Brinkworth. **Process Classification Frameworks**. In: *Handbook on Business Process Management 2*, pp. 73–92, Springer Berlin Heidelberg, 2010. 64

[Albe 03] C. J. Alberts, A. J. Dorofee, J. Stevens, and C. Woody. **Introduction to the OCTAVE®Approach**. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2003. 34, 35

[Albe 05] C. J. Alberts, A. J. Dorofee, J. Stevens, and C. Woody. **OCTAVE®-S Implementation Guide, Version 1.0** . Handbook: CMU/SEI-2003-HB-003, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2005. 35

[Alte 06] Steven Alter. *The Work System Method: Connecting People, Processes, and IT for Business Results.* Work System Press, 2006. 49

[Altu 12] O. Altuhhova, R. Matulevičius, and N. Ahmed. **Towards Definition of Secure Business Processes**. In: *CAiSE International Workshops*, pp. 1–15, Springer, 2012. 20, 40, 41, 42, 73

[Altu 13] O. Altuhhova, R. Matulevičius, and N. Ahmed. **An Extension of Business Process Model and Notification for Security Risk Management**. *International Journal of IS Modeling and Design (IJISMD)*, Vol. 4, pp. 93–113, 2013. 20, 28, 41, 42, 46, 49, 50, 53, 73

[Anto 01] Annie I Antón and Julia B Earp. **Strategies for Developing Policies and Requirements for Secure and Private Electronic Commerce**. In: *E-Commerce Security and Privacy*, pp. 67–86, Springer US, 2001. 73

[ASNZ 09] AS/NZS ISO 31000:2009. **Risk management – Principles and guidelines**. International Organization for Standardization, Geneva, 2009. 31, 32, 36

[Aviz 04] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr. **Basic Concepts and Taxonomy of Dependable and Secure Computing**. *Dependable and Secure Computing, IEEE Transactions on*, Vol. 1, No. 1, pp. 11 – 33, 2004. 30

[Bail 96] Kennet D. Bailey. **Typologies and Taxonomies: An Introduction to Classification Techniques**. *JASIS*, Vol. 47, No. 4, pp. 328–329, 1996. 71

[Bohr 13] F. Böhr, L. Thao Ly, and G. Müller. **Business Process Security Analysis - Design Time, Run Time, Audit Time**. *IT - Information Technology*, Vol. 55, No. 6, pp. 217–224, 2013. 17

[Bres 04] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos. **Tropos: An Agent-Oriented Software Development Methodology**. *Autonomous Agents and Multi-Agent Systems*, Vol. 8, No. 3, pp. 203–236, 2004. 38

[BSI 08a] BSI Standard 100-1 version 1.5. **Information Security Management System (ISMS)**. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2008. 33

[BSI 08b] BSI Standard 100-2 version 2.0. **IT-Grundschutz Methodology**. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2008. 33

[BSI 08c] BSI Standard 100-3 version 2.5. **Risk analysis based on IT-Grundschutz**. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2008. 33

[BSI 09] BSI Standard 100-4 version 1.0. **Business Continuity Management**. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2009. 33

[Business 14] **Unified Modeling Language (OMG UML) Superstructure, V2.1.2**. Accessed: 02 Jun. 2014. `http://www.omg.org/spec/UML/2.1.2/Superstructure/pdf`. 36

[Cara 07] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson. **Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process**. Technical Report: CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2007. 35

[Cast 02] J. Castro, M. Kolp, and J. Mylopoulos. **Towards requirements-driven information systems engineering: the Tropos project**. *Information Systems*, Vol. 27, No. 6, pp. 365–389, 2002. 38

[Chen 03] B. H. C. Cheng, S. Konrad, L. A. Campbell, and R. Wassermann. **Using Security Patterns to Model and Analyze Security**. In: *In IEEE Workshop on Requirements for High Assurance Systems*, pp. 13–22, 2003. 65

[Chow 12] M. Chowdhury, R. Matulevičius, G. Sindre, and P. Karpati. **Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions**. In: *Proc. of REFSQ 2012*, pp. 132–139, Springer Berlin / Heidelberg, 2012. 28

[CLUS 10] CLUSIF. **MEHARI 2010: Fundamental Concepts and Principles-Specifications**. France, 2010. 34

[Comm 12] Common Criteria version 3.1 revsion 4. **Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model**. CCMB-2012-09-001, 2012. 31, 32

[Cong 11] S. Conger. *Process Mapping and Management. Business Expert Press information systems collection*, Business Expert Press, 2011. 25

[Cope 10] E. W Cope, J. M. Küster, D. Etzweiler, L. A. Deleris, and B. Ray. **Incorporating risk into business process models**. *IBM J. Res. Dev.*, Vol. 54, No. 3, 2010. 55, 60

[Curt 92] B. Curtis, M. I. Kellner, and J. Over. **Process modeling**. *Commun. ACM*, Vol. 35, No. 9, pp. 75–90, 1992. 27, 60, 61, 64

[Dave 93] T. H. Davenport. *Process Innovation: Reengineering Work Through Information Technology*. Harvard Business School Press, Boston, MA, USA, 1993. 25

[DCSS 04] DCSSI. **Section 1 – Introduction**. EBIOS – Expression of Needs and Identification of Security Objectives, France, 2004. 29, 34

[Dijk 08] R. M. Dijkman, M. Dumas, and C. Ouyang. **Semantics and analysis of business process models in {BPMN}**. *Information and Software Technology*, Vol. 50, No. 12, pp. 1281–1294, 2008. 41

[Dijk 11] R. Dijkman., M. Dumas, B. van Dongen, R. Käärik, and J. Mendling. **Similarity of Business Process Models: Metrics and Evaluation**. *Information Systems*, Vol. 36, No. 2, pp. 498 – 516, 2011. 66

[Dong 08] B. Dongen, R. Dijkman, and J. Mendling. **Measuring Similarity between Business Process Models**. In: *Proceedings of the 20th international conference on Advanced Information Systems Engineering*, pp. 450–464, Springer-Verlag, Berlin, Heidelberg, 2008. 66

[Dubo 10] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius. **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. 13, 19, 28, 29, 38, 41, 46, 47, 68, 75, 77

[Duma 13] M. Dumas, M.L. Rosa, J. Mendling, and H.A. Reijers. *Fundamentals of Business Process Management*. Springer, 2013. 19, 25

[EBIOS 14] **EBIOS 2010 - Expression of Needs and Identification of Security Objectives**. Accessed: 06 Jun. 2014. 34

[Ekan 12] C. C. Ekanayake, M. Dumas, L. García-Bañuelos, M. Rosa, and A. H. M. Hofstede. **Approximate Clone Detection in Repositories of Business Process Models**. In: *Business Process Management*, pp. 302–318, Springer Berlin Heidelberg, 2012. 66

[Elah 07] G. Elahi and E. Yu. **A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs**. In: *Conceptual Modeling - ER 2007*, pp. 375–390, Springer Berlin Heidelberg, 2007. 38, 73

[ENIS 04] **ENISA –Inventory of Risk Assessment and Risk Management Methods**. 2004. 29

[ENV 95] **ENV 12 204, Advanced Manufacturing Technology – Systems Architecture– constructs for Enterprise Modelling**. Tech. Rep., 1995. 19, 25

[Fabi 10] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt. **A Comparison of Security Requirements Engineering Methods**. *Requirements Eng.*, Vol. 15, No. 1, pp. 7–40, 2010. 39, 72

[Fern 01] E. B. Fernandez and R. Pan. **A pattern language for security models**. In: *proceedings of PLOP*, 2001. 46

[Fire 03a] D. G. Firesmith. **Common Concepts Underlying Safety Security and Survivability Engineering**. Technical Report CMU/SEI-2003-TN-033, Carnegie Mellon University - Software Engineering Institute, Pittsburgh, Pennsylvania, 2003. 19

[Fire 03b] Donald G Firesmith. **Engineering Security Requirements**. *Journal of Object Technology*, Vol. 2, No. 1, 2003. 71

[Fire 04] D. Firesmith. **Specifying Reusable Security Requirements**. *Journal of Object Technology*, Vol. 3, No. 1, pp. 61–75, 2004. 28, 30, 64

[Fire 07] D. G. Firesmith. **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. 18, 19, 28

[Gamm 95] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. *Design Patterns: Elements of Reusable Object-oriented Software*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1995. 45, 46, 65

[Giag 01] G. M. Giaglis. **A Taxonomy of Business Process Modeling and Information Systems Modeling Techniques**. *International Journal of Flexible Manufacturing Systems*, Vol. 13, pp. 209–228, 2001. 64

[Gurs 06] S. F. Gürses and T. Santen. **Contextualizing Security Goals–A Method for Multilateral Security Requirements Elicitation**. In: *Sicherheit*, pp. 42–53, GI, 2006. 72

[Hafi 06] M. Hafiz and R.E. Johnson. **Security Patterns and Their Classification Schemes**. *University of Illinois at Urbana-Champaign Department of Computer Science, Tech. Rep*, 2006. 65

[Hafi 07] M. Hafiz, P. Adamczyk, and R.E. Johnson. **Organizing Security Patterns**. *Software, IEEE*, Vol. 24, No. 4, pp. 52 –60, 2007. 65

[Hamm 07] M. Hammer. **The Process Audit**. *Harvard Business Review*, Vol. 85, No. 4, p. 111, 2007. 17

[Harm 10] P. Harmon and C. Wolf. **The State of Business Process Management. BPTrends Report**. 2010. 17

[Herr 06] P. Herrmann and G. Herrmann. **Security Requirement Analysis of Business Processes**. *Electronic Commerce Research*, Vol. 6, No. 3-4, pp. 305–335, 2006. 18, 73

[Igur 08] V. Igure and R. Williams. **Taxonomies of Attacks and Vulnerabilities in Computer Systems**. *Communications Surveys Tutorials, IEEE*, Vol. 10, No. 1, pp. 6 –19, 2008. 65

[Info 91] **Information technology security evaluation criteria**. Tech. Rep. version 1.2, Commission of European Communities, 1991. 30, 61, 65

[ISO 04] ISO 14001. **Environmental management systems – Requirements with guidance for use.** ISO, International Organization for Standardization, Geneva, 2004. 20

[ISO 09] ISO 31010:2009. **Risk management – Risk assessment techniques**. International Organization for Standardization, Geneva, 2009. 31

[ISOI 02] ISO/IEC Guide 73:2002. **Risk management – Vocabulary – Guidelines for use in standards**. International Organization for Standardization, Geneva, 2002. 20, 31

[ISOI 04] ISO/IEC 13335-1:2004. **Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management**. International Organization for Standardization, Geneva, 2004. 31, 32

[ISOI 05a] ISO/IEC 27001:2005. **Information technology – Security techniques – Information security management systems – Requirements**. International Organization for Standardization, 2005. 29, 33, 34

[ISOI 05b] ISO/IEC 27002:2005. **Information technology – Security techniques – Code of practice for information security management**. International Organization for Standardization, 2005. 33

[ISOI 08] ISO/IEC 27005:2008. **Information technology – Security techniques – Information security risk management**. International Organization for Standardization, 2008. 34

[ISOI 11] ISO/IEC 27005:2011. **Information technology – Security techniques – Information security risk management**. International Organization for Standardization, 2011. 32

[ISOI 13] ISO/IEC 27001:2013. **Information technology – Security techniques – Information security management systems – Requirements**. International Organization for Standardization, 2013. 32

[IT G 13] **IT-Grundschutz Catalogues**. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2013. 33, 34

[ITSE 91] **ITSEC: Information Technology Security Evaluation Criteria (Provisional Harmonised Criteria, Version 1.2**. pp. 92–826, 1991. 71, 72, 75

[Jurj 05] J. Jürjens. *Secure Systems Development with UML*. Springer, 2005. 18, 72

[Khan 10] K. Khanmohammadi and S. H. Houmb. **Business Process-Based Information Security Risk Assessment**. In: *NSS-4, Australia*, pp. 199–206, IEEE Computer Society, 2010. 55, 60

[Koun 11] J. Kouns and D. Minoli. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Wiley, 2011. 34, 35

[Krog 12] J. Krogstie. **Modelling Languages: Perspectives and Abstraction Mechanisms**. In: *Model-Based Development and Evolution of Information Systems*, pp. 89–204, Springer London, 2012. 27, 60, 61

[Lams 07] Axel van Lamsweerde. **Engineering Requirements for System Reliability and Security**. In: *Software System Reliability and Security*, pp. 196–238, 2007. 73

[Lodd 02] T. Lodderstedt, D. Basin, and J. Doser. **SecureUML: A UML-based Modeling Language for Model-driven Security**. In: *UML2002–The Unified Modeling Language*, pp. 426–441, Springer, 2002. 39, 72

[Lund 11] M. S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis - The CORAS Approach*. Springer, 2011. 34, 36

[Matu 12a] R. Matulevičius, H. Mouratidis, N. Mayer, E. Dubois, and P. Heymans. **Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management.** *J. UCS*, Vol. 18, No. 6, pp. 816–844, 2012. 28

[Matu 12b] R. Matulevičius, H. Mouratidis, N. Mayer, E. Dubois, and P. Heymans. **Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management**. *Journal of Universal Computer Science*, Vol. 18, No. 6, pp. 816–844, 2012. 38

[Matu 13] R. Matulevičius and N. Ahmed. **Eliciting Security Requirements from the Business Processes Using Security Risk-Oriented Patterns**. *it - Information Technology*, Vol. 55, No. 6, pp. 225–230, 2013. 22, 50, 67, 68

[Maye 09] N. Mayer. *Model-based Management of Information System Security Risk*. PhD thesis, University of Namur, 2009. 13, 19, 28, 29, 35, 38, 41, 46, 47, 75, 77

[Mead 06] N. R. Mead. **Identifying Security Requirements Using The Security Quality Requirements Engineering (SQUARE) Method**. *Integrating Security and Software Engineering*, pp. 44–69, 2006. 72

[Mela 00] N. Melão and M. Pidd. **A conceptual framework for understanding business processes and business process modelling**. *Information Systems Journal*, Vol. 10, No. 2, pp. 105–129, 2000. 64

[Menz 09] M. Menzel, I. Thomas, and C. Meinel. **Security Requirements Specification in Service-Oriented Business Process Management**. In: *ARES*, pp. 41–48, 2009. 18, 74

[Mona 12] G. Monakova, A. D. Brucker, and A. Schaad. **Security and Safety of Assets in Business Processes**. In: *Symposium on Applied Computing*, pp. 1667–1673, ACM, 2012. 18, 74

[Mour 03] H. Mouratidis, P. Giorgini, and G. Manson. **An Ontology for Modelling Security: The Tropos Approach**. In: *Knowledge-Based Intelligent Information and Engineering Systems*, pp. 1387–1394, Springer Berlin Heidelberg, 2003. 38

[Mour 06] H. Mouratidis, J. Jürjens, and J. Fox. **Towards a Comprehensive Framework for Secure Systems Development**. In: *Advanced Information Systems Engineering, 18th International Conference, CAiSE 2006, Luxembourg, Luxembourg, June 5-9, 2006, Proceedings*, pp. 48–62, Springer, 2006. 38

[Mour 07] H. Mouratidis and P. Giorgini. **Secure Tropos: A Security-Oriented Extension of the Tropos Methodology**. *International Journal of Software Engineering and Knowledge Engineering*, Vol. 17, No. 2, pp. 285–309, 2007. 38, 73

[Mueh 05] M. zur Muehlen and M. Rosemann. **Integrating Risks in Business Process Models**. In: *Proceedings of the 2005 Australasian Conference on Information Systems (ACIS 2005)*, pp. 62–72, Sydney, Australia, 2005. 55, 60

[Mull 11] J. Müllle, S. von Stackelberg, and K. Bohm. **Modelling and Transforming Security Constraints in Privacy-aware Business Processes**. In: *SOCA*, pp. 1–4, 2011. 18, 74

[NIST 11] NIST Special Publication 800-39. **Managing Information Security Risk – Organization, Mission, and Information System View**. National Institute of Standards and Technology, Gaithersburg, 2011. 33

[NIST 12] NIST Special Publication 800-30. **Guide for Conducting Risk Assessments**. National Institute of Standards and Technology, Gaithersburg, 2012. 33

[OMG 06] OMG. *Meta Object Facility (MOF) Core Specification Version 2.0*. 2006. 60

[Ouya 09] C. Ouyang, M. Dumas, W. M. P. Aalst, A. H. M. Ter Hofstede, and J. Mendling. **From Business Process Models to Process-oriented Software Systems**. *ACM Trans. Softw. Eng. Methodol.*, Vol. 19, No. 1, pp. 2:1–2:37, Aug. 2009. 26

[Paja 12] E. Paja, P. Giorgini, S. Paul, and P. Meland. **Security Requirements Engineering for Secure Business Processes**. In: *Workshops on BIR*, pp. 77–89, Springer, 2012. 75

[Pavl 08] C. J. Pavlovski and J. Zou. **Non-functional Requirements in Business Process Modeling**. In: *APCCM*, pp. 103–112, Australian Computer Society, Inc., 2008. 18, 74

[Rena 09] S. Renault, O. Mendez-Bonilla, X. Franch, and C. Quer. **PABRE: Pattern-based Requirements Elicitation**. In: *Proc. of RCIS*, pp. 81–92, april 2009. 54

[Riaz 12] M. Riaz and L. Williams. **Security requirements patterns: understanding the science behind the art of pattern writing**. In: *Requirements Patterns (RePa), 2012 IEEE Second International Workshop on*, pp. 29 –34, 2012. 30

[Rodr 07] A. Rodríguez, E. Fernández M, and M. Piattini. **A BPMN Extension for the Modeling of Security Requirements in Business Processes**. *IEICE-TIS(4)*, pp. 745–752, 2007. 18, 74

[Rohr 04] S. Röhrig and K. Knorr. **Security Analysis of Electronic Business Processes**. *Electronic Commerce Research*, Vol. 4, No. 1-2, pp. 59–81, 2004. 18, 54, 74

[Rych 11] I. Rychkova and S. Nurcan. **Towards Adaptability and Control for Knowledge-Intensive Business Processes: Declarative Configurable Process Specifications**. In: *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pp. 1–10, 2011. 64

[Sack 08] Stefan Sackmann. **A Reference Model for Process-Oriented IT Risk Management**. In: *16th European Conference on Information Systems, ECIS 2008, Galway, Ireland, 2008*, pp. 1346–1357, 2008. 55

[Scan 08] R. Scandariato, K. Yskout, T. Heyman, and W. Joosen. **Architecting Software with Security Patterns**. Tech. Rep., 2008. 30, 75

[Schn 09] B. Schneier. *Schneier on security*. John Wiley & Sons, 2009. 17

[Schn 99] B. Schneier. **Attack trees; Modeling security threats**. *Dobb's J.*, No. 12, pp. 21–29, 1999. 13, 39, 40

[Schu 05] M. Schumacher, E. Fernandez, D. Hybertson, and F. Buschmann. *Security Patterns: Integrating Security and Systems Engineering*. John Wiley & Sons, 2005. 46, 53, 55, 65, 71

[Silv 09] B. Silver. *BPMN Method and Style*. Cody-Cassidy Press, 2009. 41

[Sind 05] G. Sindre and A. L. Opdahl. **Eliciting Security Requirements with Misuse Cases**. *Requirements Engineering*, Vol. 10, No. 1, pp. 34–44, 2005. 18, 36, 37, 72

[Sind 07] G. Sindre. **Mal-Activity Diagrams for Capturing Attacks on Business Processes**. In: *Requirements Engineering: Foundation for Software Quality*, pp. 355–366, Springer Berlin Heidelberg, 2007. 38

[Smit 14] E. N. Smith. **Chapter 14 - The Wrap: Good Security Is Good Business**. In: *Workplace Security Essentials*, pp. 197 – 202, Butterworth-Heinemann, Boston, 2014. 17

[Smit 81] E. E. Smith and D. Medin. *Categories and Concepts*. Harvard university press, Cambridge, MA., 1981. 71

[Soom 13] I. Soomro and N. Ahmed. **Towards Security Risk-Oriented Misuse Cases**. In: Marcello Rosa and Pnina Soffer, editors, *Business Process Management Workshops*, pp. 689–700, Springer Berlin Heidelberg, 2013. 28, 37

[Sowa 92] J. F. Sowa and J. A. Zachman. **Extending and formalizing the framework for information systems architecture**. *IBM Syst. J.*, Vol. 31, No. 3, pp. 590–616, 1992. 65

[Star 94] G. Starke. **Business Models and their Description**. In: *Proceedings of the 9th Austrian-informatics conference on Workflow management: Challenges, Paradigms and Products*, pp. 134–147, R. Oldenbourg Verlag GmbH, 1994. 27, 60

[Swid 04] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Press, Redmond, WA, USA, 2004. 65

[The 01] The Project Management Institute. **Project Management Body of Knowledge**. 2001. 20

[Tsia 05] T. Tsiakis and G. Stephanides. **The Economic Approach of Information Security**. *Computers & Security*, Vol. 24, No. 2, pp. 105–108, 2005. 17

[Tsip 05] K. Tsipenyuk, B. Chess, and G. McGraw. **Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors**. *IEEE Security & Privacy*, Vol. 3, No. 6, pp. 81–84, 2005. 49

[Vare 11] A. J. Varela-Vaca, R. M. Gasca, and A. Jimenez-Ramirez. **A Model-Driven Engineering Approach with Diagnosis of Non-Conformance of Security Objectives in Business Process Models**. In: *Proc. of RCIS*, pp. 1–6, may 2011. 55, 60, 74

[Vare 13] A. J. Varela-Vaca, R. Warschofsky, R. M. Gasca, S. Pozo, and C. Meinel. **A Security Pattern-Driven Approach toward the Automation of Risk Treatment in Business Processes**. In: *International Joint Conference CISIS'12-ICEUTE'12-SOCO'12 Special Sessions*, pp. 13–23, Springer Berlin Heidelberg, 2013. 54

[Verg 08] K. Vergidis, A. Tiwari, and B. Majeed. **Business Process Analysis and Optimization: Beyond Reengineering**. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, Vol. 38, No. 1, pp. 69 –82, 2008. 19, 26, 64

[Wesk 12] M. Weske. **Business Process Management - Concepts, Languages, Architectures, 2nd Edition.** Springer Berlin Heidelberg, 2012. 19, 26, 27, 59, 70

[Wolt 09] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel. **Model-driven Business Process Security Requirement Specification**. *JSA.*, Vol. 55, No. 4, pp. 211–223, 2009. 18, 73

[Work 99] Workflow Management Coalition. **Terminology & Glossary**. Technical Report WFMC-TC-1011, The Workflow Management Coalition Specification, 1999. 25

[Yin 09] R. K. Yin. *Case Study Research: Design and Methods (Applied Social Research Methods).* Sage Publications, fourth edition. Ed., 2009. 70

[Yosh 08] N. Yoshioka, H. Washizaki, and K. Maruyama. **A Survey on Security Patterns**. *Progress in Informatics*, No. 5, pp. 33–47, 2008. 53

[Yu 98] Eric Yu and John Mylopoulos. **Why Goal-oriented Requirements Engineering**. In: *Proceedings of the 4th Intl. Workshop on REFSQ*, pp. 15–22, 1998. 73

[Zach 87] J. A. Zachman. **A framework for information systems architecture**. *IBM Syst. J.*, Vol. 26, No. 3, pp. 276–292, 1987. 65

Kokkuvõte (Summary in Estonian)
Turvanõuete tuletamine äriprotsesside mudelitest

Seoses ettevõtetes infosüsteemide poolt toetatud tegevuste osakaalu pideva kasvamisega on viimastel aastatel pidevalt kasvanud firmades ka äriprotsesside modelleerimise kasutamine. Paralleelselt on üha enam hakatud teadvustama vajadust turvapoliitikate väljattamise ja rakendamise järele. Tänapäevases dünaamilises keskkonnas on turvalisuse roll palju enamat kui pelgalt äritegevuse jätkusuutlikkuse tagamine ettevõtte varade kaitsmise läbi – mõnede autorite väitel on turvalisus lausa äritegevust edasiviiv jõud. Ettevõtte turvalisust puudutavate vajaduste tuvastamine ning nendele vastavate nõuete spetsifitseerimine on keeruline ettevõtte infosüsteemide ja äriprotsesside käitamise tiheda seotuse tõttu. Veelgi enam, turvaanalüüs nõuab ekspertteadmisi nii infosüsteemide kui ka äriprotsesside vallas.

Olemasolev kirjandus turvalisuse vallas piirdub peamiselt äriprotsessides kas turvakontseptsioonide graafilise esitamisega turvaanalüüsis või turvapiirangute jõustamisega. Katmata on turvavajaduste ilmutamine ja nende automaatne teisendamine loodava süsteemi turvanõueteks. Samas, äriprotsesside modelleerimise kaudu on võimalik juba täna väljendada ettevõtete organisatsioonkäitumist (nt. äriväärtused ja sidusgruppide huvid). See on kasutamata potentsiaal ettevõtete turvavajaduste kaardistamiseks varajase turvaanalüüsi käigus uute süsteemide nõuete spetsifitseerimisel ärianalüütikute poolt. Seetttu pakub käesolev töö välja meetodi tur-

vanõuete äriprotsessidest ilmutamiseks selliselt, et ärianalüütikud saavad aru turvalisust puudutavatest vajadustest ja on seeläbi võimelised defineerima süsteemide turvanõudeid vastavalt vajadusele.

Selle dissertatsiooni panused on järgnevad. Esmalt (Peatükk 3) arendatakse välja turvariskidele orienteeritud mustrid, mis võimaldavad süsteemselt integreerida turvanõudeid äriprotsessidesse. Selleks uuritakse algselt kattuvusi turvatehnika ja äriprotsesside modelleerimise vahel. Uurimise tulemusena joondatakse äriprotsesside modelleerimise keele konstruktsioonid turvavaldkonna põhimõistetega ja identifitseeritakse äriprotsesside modelleerimise keele puudujäägid turvariskidega seotud mõistete esitamise seisukohast. Joondus tagab põhjendatud ja peenekoelise argumentatsiooni äriprotsesside modelleerimise keele laiendamiseks tuvastatud puudujääkide käsitlemisel. Vastavaid laiendusi kasutatakse turvariskidele suunatud mustrites ärivarade ja nende turvakriteeriumite, potentsiaalsete turvariskide ja vastumeetmete esitamiseks. Turvariskidele suunatud mustrid kirjeldavad, kuidas ühendada turvanõuded äriprotsesside mudelitega. Üldiselt eeldab turvatehnika tihedat koostööd ärianalüütiku (konkreetset ärivaldkonda tundev spetsialist) ja turvaanalüütiku (turvavaldkonna spetsialist) vahel. Kuigi eksperdid oma ärivaldkonnas, on ärianalüütikutel piiratud või puudub üldse teadmine turvatehnikast. Nad peavad usaldama parimaid turvapraktikaid, infoturbe standardeid või turvaeksperte. Sellise olukorra parendamiseks pakutakse käesolevas töös välja turvariskidele suunatud mustrite kasutamine. Selle lahenduse intuitsiooniks on empiiriline teadmus, et enamike probleemide lahendamiseks ei ole tihti vaja uusi lahendusi ja piisab olemasolevate taaskasutamisest või kohendamisest. Turvariskidele suunatud mustrite kasutuselevõtuga vähendame me ärianalüütikute vajadust turvaanalüütikute abi järele, kuna mustrid kätkevad endas nii turvanõudeid kui nende põhjendust. Mustrite kasulikkust uurime läbi nende rakendamise kahes ärijuhtumis.

Teiseks (Peatükk 4), arvestades, et mustrite arv saab kasvada, siis nende rakendamise lihtsustamiseks on tähtis mustrite klassifitseerimine. Selleks pakume välja äriprotsesside turvalisuse taksonoomia, mis defineerib protsessipõhise klassifitseerimise skeemi turvariskidele suunatud mustrite jaoks. Väljapakutud taksonoomia iseloomustab kolme dimensiooni, mis on omased äriprotsesside modelleerimisele ja turvalisusele. Esimesed kaks dimensiooni (äriprotsesside hierarhia ja äriline perspektiiv) kirjeldavad äriprotsesse. Esimene dimensioon "äriprotsesside hierarhia" kirjeldab kuidas äri toimib vastavalt äriprotsesside diagrammide detailsuse tasemele. Teine dimensioon "äriline perspektiiv" käsitleb äriprotsesside mudelite nelja perspektiivi (funktsionaalne, käitumuslik, organisatsiooniline ja informatiivne) modelleerimist, mis esitavad ärivarasid äriprotsesside diagrammidel.

Kolmas dimension esitab varade turvakitsendusi, mis käsitlevad eelneva kahe dimensiooniga seotud turvalisuse teemasid. Taksonoomia eesmärgiks on äriprotsesside modelleerimise ühendamine turvariskidega. Lisaks, taksonoomia määrab mustrite potentsiaalse esinemise äriprotsessides ja lihtsustab mustrite rakendamist. Taksonoomia rakendamist demonstreerime illustreeriva näite baasil.

Lõpetuseks (Peatükk 5) formuleerime ülalkirjeldatud panuste baasil SREBP (Security Requirements Elicitation from Business Processes) meetodi, mis on käesoleva töö peamine panus. Arendatud meetod võimaldab varajast turvaanalüüsi tuvastades äriprotsesside mudelitest turvaeesmärgid ning tõlkides need süsteemselt turvanõueteks. Meetod baseerub infosüsteemide turvariskide haldamise valdkonnamudelil (information system security risk management (ISSRM)) ja turvariskidele suunatud mustritel. Meetod koosneb kahest etapist. Etapp 1, ärivarade ja turvaeesmärkide tuvastamine, kirjeldab kuidas tuvastada ärivarasid ja nende turvaeesmärke väärtusahelast ja äriprotsesside diagrammidest. Ärivarade ja nende turvaeesmärkide identifitseerimisel rakendatakse ISSRM valdkonnamudelit. Etapp 2, turvanõuete ilmutamine, toetab turvanõuete ilmutamist operatiivsetest äriprotsessidest viies kontekstis ligipääsukontroll, suhtluskanal, sisendliides, võrgu infrastruktuur ja andmehoidla. SREBP meetod kasutab turvariskidele suunatud mustreid ilmutamaks turvanõudeid. SREBP-s on turvanõuded kirjeldatud detailselt kasutades turvamudeleid (nt. SecureUML ja UML) igas nimetatud kontekstis. Turvamudelid võimaldavad põhjalikult analüüsida konkreetsete varade turvalisust kuna neis (nt. RBAC) on vastavad konstruktsioonid eri stsenaariumite vaatlemiseks. SREBP meetodi valideerime Eesti Geenivaramu juhtumiuuringu raames. Valideerimisel kontrollitakse SREBP täielikkust ja efektiivsust turvanõuete ilmutamise võimekuse võtmes.

Need panused üheskoos toetavad turvanõuete ilmutamist äriprotsesside mudelitest, kus i) ärivarade tuvastamine ja turvaeesmärkide tuvastamine teostatakse ettevõtte äriprotsesside põhjal ja ii) turvanõuete ilmutamine teostatakse käigusolevatel äriprotsessidel kasutades selleks määratud kontekste.

Part III

Papers

Curriculum vitae

General

Name:	Naved Ahmed
Date and Place of Birth:	23.11.1980, Pakistan
Citizenship:	Pakistan

Education

2010 – 2014	University of Tartu, Faculty of Mathematics and Computer Science, Doctoral studies, Specialty: Computer Science
2007 – 2009	Royal Institute of Technology (KTH), Sweden, Master studies, Specialty: Informatics
2000 – 2004	NWFP Agricultural University, Khyber Pakhtunkhwa, Pakistan, Bachelor studies, Specialty: Computer Science
... -- 1998	Govt. Jehanzeb Postgraduate College, Pakistan Higher Secondary School, Specialty: Pre-Engineering Group

Work experience

06/2005 – 08/2007	Advanced DataCom Solutions (ADCOMS) Pvt Ltd, Pakistan, IT Manager
03/2005 – 09/2007	Inikosoft Corporation / ClearLeads Corporation, Off-Shore Web Programmer.
03/2004 – 09/2005	Inikosoft Corporation / ClearLeads Corporation, Web Programmer.

Elulookirjeldus

Üldandmed

Nimi:	Naved Ahmed
Sünniaeg ja koht:	23.11.1980, Pakistan
Kodakondsus:	Pakistan

Haridus

2010 – 2014	Tartu Ülikool, Matemaatika-informaatikateaduskond, doktoriõpe, Eriala: arvutiteadus
2007 – 2009	Royal Institute of Technology (KTH), Rootsi, magistriõpe, Eriala: informaatika
2000 – 2004	NWFP Agricultural University, Khyber Pakhtunkhwa, Pakistan, bakalaureuseõpe, Eriala: arvutiteadus
... -- 1998	Govt. Jehanzeb Postgraduate College, Pakistan Higher Secondary School, Eriala: Pre-Engineering Group

Teenistuskäik

06/2005 – 08/2007	Advanced DataCom Solutions (ADCOMS) Pvt Ltd, Pakistan, IT Haldaja
03/2005 – 09/2007	Inikosoft Corporation / ClearLeads Corporation, Off-Shore Web Programmeerija.
03/2004 – 09/2005	Inikosoft Corporation / ClearLeads Corporation, Web Programmeerija.

List of Publications

Much of the material in this thesis appears in the following publications.

1 Ahmed, N., Matulevičius, R., Milani, F. Security Requirements Elicitation from Business Processes (SREBP). *Submitted to Requirement Engineering Journal*.

2 Ahmed, N., Matulevicius, R.: Application Guidelines for Security Requirements Elicitation from Business Processes. *Submitted to CAiSE Forum 2014 LNBIP proceedings*.

3 Milani, F., Dumas, M., Ahmed, N., Matulevicius, R.: Modelling Families of Business Process Variants: A Decomposition Driven Method. *Submitted to Information Systems Journal*.

4 Ahmed, N., Matulevičius, R. (2014). A Method for Eliciting Security Requirements from the Business Process Models. In: CAiSE Forum and Doctoral Consortium 2014, 57-64. CEUR-WS.org.

5 Ahmed, N., Matulevičius, R. (2014). Securing Business Processes using Security Risk-oriented Patterns. Computer Standards and Interfaces, 36(4), 723-733.

6 Ahmed, N., Matulevičius, R. (2014). SREBP: Security Requirement Elicitation from Business Processes . 20th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2014), (CEUR workshop proceedings), 145-146.

7 Altuhhova, O., Matulevičius, R., Ahmed, N. (2013). An Extension of Business Process Model and Notation for Security Risk Management. International Journal of Information System Modeling and Design (IJISMD), 4(4), 93-113.

8 Matulevičius, R., Ahmed, N. (2013). Eliciting Security Requirements from the Business Process Using Security Risk-oriented Patterns. it - Information Technology, 55(6), 225-230.

9 Soomro, I., Ahmed, N. (2013). Towards Security Risk-Oriented Misuse Cases. Business Process Management Workshops, Springer Berlin Heidelberg, 132(132), 689-700.

10 Ahmed, N., Matulevičius, R. (2013). A Taxonomy for Assessing Security in Business Process Modelling. In: 2013 IEEE Seventh International Conference on Research Challenges in Information Science (RCIS): 2013 IEEE Seventh International Conference on Research Challenges in Information Science (RCIS). IEEE, 1-10.

11 Ahmed, N., Matulevicius, R., Khan, N. H. (2012). Eliciting Security Requirements for Business Processes using Patterns. Security in Information Systems, SciTePress, 49-58.

12 Ahmed, N., Matulevičius, R., Mouratidis, H. (2012). A Model Transformation from Misuse Cases to Secure Tropos. Proceedings of the CAiSE'12 Forum, CEUR-WS.org, 7-14.

13 Altuhhova, O., Matulevičius, R., Ahmed, N. (2012). Towards Definition of Secure Business Process. In: Lecture Notes in Business Information Research: CAiSE 2012 International Workshops, Workshop on Information Systems Security Engineering, Springer Heidelberg, 1-15.

14 Ahmed, N., Matulevičius, R. (2011). Towards Transformation Guidelines from Secure Tropos to Misuse Cases (position paper). In: Proceeding of the 7th international workshop on Software engineering for secure systems. Waikiki, Honolulu, HI, USA, ACM, 36-42.

15 Ahmed, N., Matulevičius, R. (2011). A Template of Security Risk Patterns for Business Processes. In: Local Proceedings of the 10th International Conference on Perspectives in Business Informatics Research, Associated Workshops and Doctoral Consortium; Riga, Latvia: JUMI Publishing House Ltd., 123-130.

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS

1. **Mati Heinloo.** The design of nonhomogeneous spherical vessels, cylindrical tubes and circular discs. Tartu, 1991, 23 p.
2. **Boris Komrakov.** Primitive actions and the Sophus Lie problem. Tartu, 1991, 14 p.
3. **Jaak Heinloo.** Phenomenological (continuum) theory of turbulence. Tartu, 1992, 47 p.
4. **Ants Tauts.** Infinite formulae in intuitionistic logic of higher order. Tartu, 1992, 15 p.
5. **Tarmo Soomere.** Kinetic theory of Rossby waves. Tartu, 1992, 32 p.
6. **Jüri Majak.** Optimization of plastic axisymmetric plates and shells in the case of Von Mises yield condition. Tartu, 1992, 32 p.
7. **Ants Aasma.** Matrix transformations of summability and absolute summability fields of matrix methods. Tartu, 1993, 32 p.
8. **Helle Hein.** Optimization of plastic axisymmetric plates and shells with piece-wise constant thickness. Tartu, 1993, 28 p.
9. **Toomas Kiho.** Study of optimality of iterated Lavrentiev method and its generalizations. Tartu, 1994, 23 p.
10. **Arne Kokk.** Joint spectral theory and extension of non-trivial multiplicative linear functionals. Tartu, 1995, 165 p.
11. **Toomas Lepikult.** Automated calculation of dynamically loaded rigid-plastic structures. Tartu, 1995, 93 p, (in Russian).
12. **Sander Hannus.** Parametrical optimization of the plastic cylindrical shells by taking into account geometrical and physical nonlinearities. Tartu, 1995, 74 p, (in Russian).
13. **Sergei Tupailo.** Hilbert's epsilon-symbol in predicative subsystems of analysis. Tartu, 1996, 134 p.
14. **Enno Saks.** Analysis and optimization of elastic-plastic shafts in torsion. Tartu, 1996, 96 p.
15. **Valdis Laan.** Pullbacks and flatness properties of acts. Tartu, 1999, 90 p.
16. **Märt Põldvere.** Subspaces of Banach spaces having Phelps' uniqueness property. Tartu, 1999, 74 p.
17. **Jelena Ausekle.** Compactness of operators in Lorentz and Orlicz sequence spaces. Tartu, 1999, 72 p.
18. **Krista Fischer.** Structural mean models for analyzing the effect of compliance in clinical trials. Tartu, 1999, 124 p.

19. **Helger Lipmaa.** Secure and efficient time-stamping systems. Tartu, 1999, 56 p.
20. **Jüri Lember.** Consistency of empirical k-centres. Tartu, 1999, 148 p.
21. **Ella Puman.** Optimization of plastic conical shells. Tartu, 2000, 102 p.
22. **Kaili Müürisep.** Eesti keele arvutigrammatika: süntaks. Tartu, 2000, 107 lk.
23. **Varmo Vene.** Categorical programming with inductive and coinductive types. Tartu, 2000, 116 p.
24. **Olga Sokratova.** Ω-rings, their flat and projective acts with some applications. Tartu, 2000, 120 p.
25. **Maria Zeltser.** Investigation of double sequence spaces by soft and hard analitical methods. Tartu, 2001, 154 p.
26. **Ernst Tungel.** Optimization of plastic spherical shells. Tartu, 2001, 90 p.
27. **Tiina Puolakainen.** Eesti keele arvutigrammatika: morfoloogiline ühestamine. Tartu, 2001, 138 p.
28. **Rainis Haller.** *M(r,s)*-inequalities. Tartu, 2002, 78 p.
29. **Jan Villemson.** Size-efficient interval time stamps. Tartu, 2002, 82 p.
30. **Eno Tõnisson.** Solving of expession manipulation exercises in computer algebra systems. Tartu, 2002, 92 p.
31. **Mart Abel.** Structure of Gelfand-Mazur algebras. Tartu, 2003. 94 p.
32. **Vladimir Kuchmei.** Affine completeness of some ockham algebras. Tartu, 2003. 100 p.
33. **Olga Dunajeva.** Asymptotic matrix methods in statistical inference problems. Tartu 2003. 78 p.
34. **Mare Tarang.** Stability of the spline collocation method for volterra integro-differential equations. Tartu 2004. 90 p.
35. **Tatjana Nahtman.** Permutation invariance and reparameterizations in linear models. Tartu 2004. 91 p.
36. **Märt Möls.** Linear mixed models with equivalent predictors. Tartu 2004. 70 p.
37. **Kristiina Hakk.** Approximation methods for weakly singular integral equations with discontinuous coefficients. Tartu 2004, 137 p.
38. **Meelis Käärik.** Fitting sets to probability distributions. Tartu 2005, 90 p.
39. **Inga Parts.** Piecewise polynomial collocation methods for solving weakly singular integro-differential equations. Tartu 2005, 140 p.
40. **Natalia Saealle.** Convergence and summability with speed of functional series. Tartu 2005, 91 p.
41. **Tanel Kaart.** The reliability of linear mixed models in genetic studies. Tartu 2006, 124 p.

42. **Kadre Torn.** Shear and bending response of inelastic structures to dynamic load. Tartu 2006, 142 p.
43. **Kristel Mikkor.** Uniform factorisation for compact subsets of Banach spaces of operators. Tartu 2006, 72 p.
44. **Darja Saveljeva.** Quadratic and cubic spline collocation for Volterra integral equations. Tartu 2006, 117 p.
45. **Kristo Heero.** Path planning and learning strategies for mobile robots in dynamic partially unknown environments. Tartu 2006, 123 p.
46. **Annely Mürk.** Optimization of inelastic plates with cracks. Tartu 2006. 137 p.
47. **Annemai Raidjõe.** Sequence spaces defined by modulus functions and superposition operators. Tartu 2006, 97 p.
48. **Olga Panova.** Real Gelfand-Mazur algebras. Tartu 2006, 82 p.
49. **Härmel Nestra.** Iteratively defined transfinite trace semantics and program slicing with respect to them. Tartu 2006, 116 p.
50. **Margus Pihlak.** Approximation of multivariate distribution functions. Tartu 2007, 82 p.
51. **Ene Käärik.** Handling dropouts in repeated measurements using copulas. Tartu 2007, 99 p.
52. **Artur Sepp.** Affine models in mathematical finance: an analytical approach. Tartu 2007, 147 p.
53. **Marina Issakova.** Solving of linear equations, linear inequalities and systems of linear equations in interactive learning environment. Tartu 2007, 170 p.
54. **Kaja Sõstra.** Restriction estimator for domains. Tartu 2007, 104 p.
55. **Kaarel Kaljurand.** Attempto controlled English as a Semantic Web language. Tartu 2007, 162 p.
56. **Mart Anton.** Mechanical modeling of IPMC actuators at large deformations. Tartu 2008, 123 p.
57. **Evely Leetma.** Solution of smoothing problems with obstacles. Tartu 2009, 81 p.
58. **Ants Kaasik.** Estimating ruin probabilities in the Cramér-Lundberg model with heavy-tailed claims. Tartu 2009, 139 p.
59. **Reimo Palm.** Numerical Comparison of Regularization Algorithms for Solving Ill-Posed Problems. Tartu 2010, 105 p.
60. **Indrek Zolk.** The commuting bounded approximation property of Banach spaces. Tartu 2010, 107 p.
61. **Jüri Reimand.** Functional analysis of gene lists, networks and regulatory systems. Tartu 2010, 153 p.
62. **Ahti Peder.** Superpositional Graphs and Finding the Description of Structure by Counting Method. Tartu 2010, 87 p.

63. **Marek Kolk.** Piecewise Polynomial Collocation for Volterra Integral Equations with Singularities. Tartu 2010, 134 p.
64. **Vesal Vojdani.** Static Data Race Analysis of Heap-Manipulating C Programs. Tartu 2010, 137 p.
65. **Larissa Roots.** Free vibrations of stepped cylindrical shells containing cracks. Tartu 2010, 94 p.
66. **Mark Fišel.** Optimizing Statistical Machine Translation via Input Modification. Tartu 2011, 104 p.
67. **Margus Niitsoo**. Black-box Oracle Separation Techniques with Applications in Time-stamping. Tartu 2011, 174 p.
68. **Olga Liivapuu.** Graded q-differential algebras and algebraic models in noncommutative geometry. Tartu 2011, 112 p.
69. **Aleksei Lissitsin.** Convex approximation properties of Banach spaces. Tartu 2011, 107 p.
70. **Lauri Tart.** Morita equivalence of partially ordered semigroups. Tartu 2011, 101 p.
71. **Siim Karus.** Maintainability of XML Transformations. Tartu 2011, 142 p.
72. **Margus Treumuth.** A Framework for Asynchronous Dialogue Systems: Concepts, Issues and Design Aspects. Tartu 2011, 95 p.
73. **Dmitri Lepp.** Solving simplification problems in the domain of exponents, monomials and polynomials in interactive learning environment T-algebra. Tartu 2011, 202 p.
74. **Meelis Kull.** Statistical enrichment analysis in algorithms for studying gene regulation. Tartu 2011, 151 p.
75. **Nadežda Bazunova.** Differential calculus $d^3 = 0$ on binary and ternary associative algebras. Tartu 2011, 99 p.
76. **Natalja Lepik.** Estimation of domains under restrictions built upon generalized regression and synthetic estimators. Tartu 2011, 133 p.
77. **Bingsheng Zhang.** Efficient cryptographic protocols for secure and private remote databases. Tartu 2011, 206 p.
78. **Reina Uba.** Merging business process models. Tartu 2011, 166 p.
79. **Uuno Puus.** Structural performance as a success factor in software development projects – Estonian experience. Tartu 2012, 106 p.
80. **Marje Johanson.** $M(r, s)$-ideals of compact operators. Tartu 2012, 103 p.
81. **Georg Singer.** Web search engines and complex information needs. Tartu 2012, 218 p.
82. **Vitali Retšnoi.** Vector fields and Lie group representations. Tartu 2012, 108 p.
83. **Dan Bogdanov.** Sharemind: programmable secure computations with practical applications. Tartu 2013, 191 p.
84. **Jevgeni Kabanov.** Towards a more productive Java EE ecosystem. Tartu 2013, 151 p.
85. **Erge Ideon**. Rational spline collocation for boundary value problems. Tartu, 2013, 111 p.

86. **Esta Kägo**. Natural vibrations of elastic stepped plates with cracks. Tartu, 2013, 114 p.
87. **Margus Freudenthal.** Simpl: A toolkit for Domain-Specific Language development in enterprise information systems. Tartu, 2013, 151 p.
88. **Boriss Vlassov.** Optimization of stepped plates in the case of smooth yield surfaces. Tartu, 2013, 104 p.
89. **Elina Safiulina.** Parallel and semiparallel space-like submanifolds of low dimension in pseudo-Euclidean space. Tartu, 2013, 85 p.
90. **Raivo Kolde.** Methods for re-using public gene expression data. Tartu, 2014, 121 p.
91. **Vladimir Šor.** Statistical Approach for Memory Leak Detection in Java Applications. Tartu, 2014, 155 p.