



**UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE**

Institute of Computer Science
Department of Software Engineering

Inam Soomro

Alignment of Misuse Cases to ISSRM

Master's thesis (30 ECTS)

Supervisors:
Dr. Raimundas Matulevičius
Naved Ahmed

Author:	Inam Soomro	“.....”	Nov 2012
Supervisor:	Raimundas Matulevičius	“.....”	Nov 2012
Approved for defence			
Professor:	Marlon Dumas	“.....”	Nov 2012

TARTU, 2012

Abstract

As a line between digital and social life is diminishing, security concerns of information systems and information *per se*, also developing and maintaining system security are gaining a rising attention. Nevertheless, the existing practices report on numerous cases when security aspects were considered only at the end of the system development process, thus, missing the systematic security analysis during system and software requirements and design stages.

Misuse case diagrams are one of the possible ways to relate security analysis and system functional requirements definition. Their main goal is to model negative scenarios with respect to the defined system functional requirement elicitation and analysis. Despite this fundamental advantage, misuse cases tend to be rather imprecise; they do not comply with security risk management strategies, and, thus, could lead to misinterpretation of the security-related concepts. Such limitations could potentially result in poor security solutions. Quite often, the organizations have to adopt their own security solutions to safeguard their resources and assets.

In this thesis we will apply a systematic approach to understand how misuse case diagrams could help model organisational assets, potential system risks, and security requirements to mitigate these risks. More specifically we will align misuse case constructs with the concepts of the domain model for the information systems security risk management (ISSRM). In addition, based on such an ISSRM and language alignment we will investigate and develop rules to translate misuse case diagrams to the Secure Tropos model.

The contribution of this research has several benefits. Firstly, it will potentially help understand how misuse case could deal with security risk management. Secondly, it will define method to support reasoning for the security requirements introduction and implementation in the developed system. Finally the transformation to the Secure Tropos would potentially help developers (and other system stakeholders) to understand why security solutions are important and what different stakeholder trade-offs are.

We plan to validate our results where the quality model regarding its comprehensibility will be measured for the misuse case diagrams.

We believe that such alignment of the misuse cases with ISSRM and misuse case diagram transformation to the goal-oriented modelling language will be beneficial to system and software developers. Firstly, it will allow understanding security concerns at the earlier stages of development. Secondly it will help to view security problems from different angles, understanding different security development perspectives.

Acknowledgement

First and foremost I am so grateful to my supervisor Dr. Raimundas Matulevičius who provided me the exposure in the research area. It has been the utmost privilege to work under his guidance. I am also grateful to him for his advices, careful reviews and editing and patience during the preparation of this thesis work. I am also thankful to my second supervisor Mr. Naved Ahmed for his guidance and careful reviews for the completion of my thesis.

I would also like to thank my parents, my uncle, my brothers and sister and my friends for being so supportive and encouraging throughout my studies.

Contents

- Abstract2
- Acknowledgement..... 3
- List of Figures 7
- List of Tables..... 8
- Abbreviation and Acronyms 9
- Chapter 1
- Introduction.....10
 - 1.1 Scope.....10
 - 1.2 Information System10
 - 1.3 Information System Security Engineering.....11
 - 1.4 Security Risk Management11
 - 1.5 Motivation.....11
 - 1.6 Thesis Outline.....11
 - 1.7 PART I, Background11
 - 1.8 PART II, Contribution11
 - 1.9 PART III, Validation11
 - PART IV, Conclusion and Future Work11
- PART I
- BACKGROUND..... 12
- Chapter 2
- Information System Security Risk Management Domain Model 13
 - 2.1 Risk Management.....13
 - 2.2.1 Risk Management Methods.....13
 - 2.2.2 Why ISSRM?14
 - 2.3 ISSRM Domain Model.....15
 - 2.3.1 Asset-related concepts:15
 - 2.3.2 Risk related concepts:.....15
 - 2.3.3 Risk treatment related concepts:16
 - 2.6 ISSRM Process16
 - 2.7 Summary.....17
- Chapter 3
- Modelling Languages..... 19
 - 3.1 BPMN.....19
 - 3.1.1 Purpose19
 - 3.1.2 Construct and Example.....19

3.1.3 Relationship to ISSRM	19
3.2 Secure Tropos	20
3.2.1 Purpose.....	20
3.2.2 Construct and Example.....	20
3.2.3 Relationship to ISSRM	20
3.3 Mal-Activity	21
3.3.1 Purpose	21
3.3.2 Construct and Example.....	21
3.3.3 Relationship to ISSRM	21
3.4 Misuse Cases	22
3.4.1 Purpose	22
3.4.2 Construct and Example	22
3.4.4 Misuse cases and ISSRM	24
3.4.5 Textual Template for Misuse Cases.....	25
3.4.6 Summary	25
PART II	
CONTRIBUTION	26
CHAPTER 4	
Alignment of Misuse Cases to ISSRM.....	27
4.1 Research Method.....	27
4.2 Misuse Case Running Example	28
4.2.1 Scenario 1: SROMUC Modelling for Integrity.....	28
4.2.1.1 Asset model.....	28
4.2.1.2 Risk model.....	28
4.2.1.3 Risk treatment model.....	29
4.2.1.2 Scenario 2: SROMUC Modelling for Availability	29
4.2.1.3 Scenario 3: SROMUC Modelling for Confidentiality.....	30
4.3 Concept Alignment of SROMUC and ISSRM.....	30
4.3.1 Alignment of asset related concepts.....	30
4.3.2 Alignment of risk-related concepts.....	31
4.3.3 Alignment of risk treatment related concepts.....	31
4.4 Abstract Syntax of Security Risk-oriented Misuse Cases	31
4.5 Summary.....	33
CHAPTER 5	
Model Transformations	34
5.1 Transformation Rules from Misuse cases to Secure Tropos.....	34

5.2 Transformation from Secure tropos to Misuse Cases	37
5.3 Summary	42
PART IV	
Validation	43
Chapter 6	
Comprehensibility of SROMUC	44
6.1 Participant Selection	44
6.2 Survey for Measuring Comprehensibility of SROMUC	44
6.3 Results	44
6.4 Threat to Validity	46
6.5 Summary	46
PART V	
CONCLUSIONS AND FUTURE WORK	47
Chapter 7	
Discussion, Conclusion and Future Work	48
7.1 Related Work	48
7.2 Limitations	48
7.2 Conclusion	49
7.3 Future work	49
Bibliography	50
Abstract Eesti	52
Appendix A Online Survey	52
Appendix B – Online Questionnaire Results	56
Appendix C – Research Paper Submitted to an International Workshop	57
Appendix D – Research Paper	57

List of Figures

Fig. 2.1 ISSRM Domain Model.....	17
Fig. 2.2 ISSRM Process.....	18
Fig. 3.1. BPMN Risk Management.....	21
Fig. 3.2 Modelling with Secure Tropos.....	22
Fig. 3.3 MAL-Activity diagram and Legends.....	23
Fig. 3.4 Assets Modelling.....	24
Fig. 3.5 Threat Modelling.....	25
Fig. 4.1 Research Method.....	28
Fig.4.2 Asset Modelling.....	29
Fig.4.3. Threat Modelling.....	30
Fig.4.4. Security Requirement Modelling.....	30
Fig.4.5. Modelling for Availability of Service.....	31
Fig. 4.6. Modelling for Confidentiality of Data.....	31
Fig. 4.7. Meta Model of SROMUC.....	34
Fig. 5.1. System Actor.....	35
Fig. 5.2. Goal and Plan.....	35
Fig. 5.3. Security Criterion.....	36
Fig. 5.4. Actor.....	37
Fig. 5.5. Attacker.....	37
Fig. 5.6. Attacks and exploits.....	38
Fig. 5.7. Attacks, exploits and impact.....	38
Fig. 5.8. Asset Model.....	39
Fig. 5.9. Threat Model.....	39
Fig. 5.10. Security Model.....	40
Fig. 5.11. System Boundary.....	40
Fig. 5.12. Use cases.....	40
Fig. 5.13. Use cases and Security criterion.....	41
Fig. 5.14. Actor and Use cases.....	41
Fig. 5.15. Misuser and Misuse Cases.....	42
Fig. 5.16. Vulnerability.....	42
Fig. 5.17. Impact.....	42
Fig. 5.18. Security Use Case.....	43

List of Tables

Table 2.1 Comparison of Risk Management Approaches and Methods.....	15
Table 3.1 Alignment of Misuse cases with ISSRM.....	24
Table 3.2 Construct of Misuse Cases.....	25
Table 4.1 Asset Related Concepts (C – Concept, R – Relationships).....	32
Table 4.2 Alignment of Risk related Concepts(C – Concepts, R – Relationships).....	33
Table 4.3 Risk Treatment related Concepts (C – Concepts, R – Relationships).....	34
Table 6.1 Survey Results.....	45
Table 6.2 Comprehensibility of SROMUC.....	46

Abbreviation and Acronyms

BPMN	Business Process Modelling Notation
IS	Information System
IT	Information Technology
UML	Unified Modelling Language
MAD	Mal-Activity Diagram
MUC	Misuse Cases
SROMUC	Security Risk oriented Misuse Cases
ISSRM	Information System Security Risk Management
RE	Requirement Engineering
RiskREP	Risk-based Security Requirement, Elicitation and Prioritization

Chapter 1

Introduction

In this chapter we provide the introduction and the scope of our research. We will identify the research question. We introduce the Information System and the motivation for this research. Also we present the structure of the research work.

1.1 Scope

During the last two decades, line between digital and social life is diminishing, leading that modern society is mainly dependent on information system (IS) and its security. The demand for security of IS is constantly growing, also developing and maintaining system security is gaining a rising attention. Considering IS security at early stages of software development is also acknowledged [28]. Security breaches in IS can lead to the negative consequences. The practitioners of IS security must inspect security threats with negative perspective from the very beginning of IS development process. Consideration of security at early development stages assists to analyse and estimate security measures of the IS to be developed.

This research discusses the security risk management at requirement elicitation and analysis stage. We will answer the question “*how security risk management could be addressed using Misuse Case diagrams?*” To answer this question we analyse misuse cases proposed by Sindre and Opdahl [3, 17]. Misuse case diagrams are one of the possible techniques to relate security analysis and functional requirements of software systems. Their main goal is to model negative scenarios with respect to functional requirements. Misuse cases are already proved to be useful in the industries [25]. Existing misuse cases is a simple language, since it contains quite few elements to model security concerns. However the previous analysis shows the limitations of misuse cases in detail [17]. In this analysis, Matulevicius *et al.* highlighted that currently misuse cases do not have the concrete constructs to comply with security risk management strategies. Mainly, because of some missing constructs to model the security risk concepts. Likewise, distinct constructs for representing security risk concepts are not available. Thus, could lead to misinterpretation of the security-related concepts. Such limitations could potentially result in poor security solutions. This challenges to look for improvement of the misuse cases. In this research we apply a systematic approach to understand how misuse case diagrams could help to model organisational assets, potential system risks, and security requirements to mitigate these risks. More specifically we introduce new constructs to extend the misuse cases in order to align the constructs of misuse case diagram with the concepts of information systems security risk management (ISSRM) domain model [18]. The benefit of syntactical and semantic extensions is that they bring the missing semantics in to the language. The domain model is a touchstone to verify if the concepts presented in misuse cases are acceptable and appropriate for security risk management.

1.2 Information System

The term information system is best defined in the context of domain it is used for. We prefer to choose the definition of information system as, “A system for dissemination of data between persons - potentially, to increase their knowledge” [30]. Our goal is to comprise information technology i.e. system used for spreading of data and people's activities in this work as information system.

1.3 Information System Security Engineering

Security is usually seen in two different ways, dedicated malicious act and/or accidental harm to the system or to the organization. Here we take the definition as “security is the degree to which malicious harm is prevented, detected, and reacted.” [13]. Security covers broad range of areas including financial, environmental, information system. Here, we will only work with the security concepts at design stage of the information system.

1.4 Security Risk Management

Security risk is a very general concept and applies to different domain. Risk can be seen as combination of the probability of an event and its negative consequence. Risk management (RM) is defined as “coordinated activities to direct and control an organization with regard to risk” [35]. Risk management can be related to finance, organization, environment and security etc. Security risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. In this work we will only focus on the aspects of security risk management for information system at early requirement elicitation and analysis stage.

1.5 Motivation

Now days security has become a requirement for information technology and IS *per se* instead of an option but it is only seen during the later phases of the development process [3]. This approach often leads to threats and vulnerabilities that provide a potential for exploitation of IS.

1.6 Thesis Outline

The structure of the thesis is organised as follows: In Part I, we describe the related background knowledge and ISSRM domain model. Moreover, we discuss other security risk management methods and security modelling languages. In Part II, we develop Security Risk-oriented Misuse Case (SROMUC) and illustrate SROMUC approach through an online banking IS [1, 31]. Then, we provide the concept alignment of SROMUC to ISSRM. Section III measure the comprehensibility of the proposed models. In part IV, we discuss, conclude our work and present areas for future work.

1.7 PART I, Background

This section contains two chapters. The second chapter introduces the Information System Security Risk Management (ISSRM) domain model and its process and the overview of the current practices and research related to security risk management approaches. The third chapter discuss the security modelling languages that are already aligned to security risk management concepts.

1.8 PART II, Contribution

This section contains two chapters. The fourth chapter provides the alignment of MUC to ISSRM domain model and introduces the Security Risk-oriented MUC (SROMUC). The fifth chapter introduces the transformation from SROMUC to secure tropos and vice versa.

1.9 PART III, Validation

This section contains one chapter. The chapter discuss and measure the comprehensibility of the SROMUC. Also, we will investigate the threats to validity of our proposal.

PART IV, Conclusion and Future Work

This section summarizes the major findings and discusses the future work. It also shows the conclusion and highlights of the contribution.

PART I
BACKGROUND

Chapter 2

Information System Security Risk Management Domain Model

This chapter introduces the Information System Security Risk Management (ISSRM) domain model along with other information system security risk management approaches and methods.

2.1 Risk Management

The most generally agreed upon the definition of risk is it is defined as a combination of the probability of an event and its consequences [35]. Following this definition, RM is defined as coordinated activities to direct and control an organisation with regard to risk. Depending on the context, RM can address various kinds of issues. For example, risks can be related to the organisation's management (i.e., poor health of key personnel in regards to the business), finance (i.e., related to investment), environment (i.e., pollution), or security etc.

Security Risk Management is a process of identification and analysis of safety and security hazards to the system, their assessment and identifies the risk level of those hazards and also providing the mitigation strategies to those hazards with the aim of decreasing the risk by decreasing or eliminating its impact.

2.2.1 Risk Management Methods

Risk management methods define the methods to deal with security risk management activities. Following are few of the methods widely used:

2.2.1.1 EBIOS - An acronym for “Expression des Besoinset Identification des Objectifs de Sécurité” [32]. An expression of requirements and identification of security objectives is a methodological approach towards identification of IS security risks and proposes suitable security objectives and requirements. It was developed by DCSSI(general direction of Information system security) of French Defense Ministry. EBIOS consider all the entities including technical (software, hardware, network) and non-technical (human, organization and physical safety) aspects. The process includes context and environmental analysis, security requirement evaluation, risk Analysis, identification of security Objectives, and determination of security requirements.

2.2.1.2 MEHARI - An acronym for “Methode Harmoniséed' Analyse du RisqueInformatique“ or Harmonized Risk Analysis Method is an information system security risk analysis and risk management method developed by CLUSIF (French association of information security professionals) [33]. The method entirely depends on organizations needs and circumstances and guarantees the suitable strategy of the security risk management. MEHARI focuses on risk assessment and risk management techniques and works in different modules including security stakes analysis and classification by identifying and evaluating potential risks and their consequences, evaluation guide for security services by assessing the level of information system security and focusing on the main weaknesses of the system, risk analysis guide provides the description of security requirements for safeguarding the IS.

2.2.1.3 OCTAVE - Octave is a process-driven methodology to identify priorities and manage information security risks [4]. It is risk-based strategic assessment and planning technique for information security which helps organizations to define the essential components of a systematic information security risk assessment framework. Three OCTAVE methodologies were developed to manage risks, OCTAVE® was designed for large organizations,

OCTAVE-S was designed for small organization and OCTAVE allegro also known as next generation of OCTAVE which was designed to optimize the process of assessing information security risks in order for organization to obtain sufficient results with a small investment in time. Octave helps organizations to develop qualitative risk evaluation criteria based on operational risk tolerances, identify assets that are critical to the mission of the organization, identify vulnerabilities and threats to the critical assets, determine and evaluate potential consequences of the threats to organizations and finally to initiate corrective actions to mitigate risks and create practice-based protection strategy.

2.2.1.4 CRAMM - CRAMM is a risk analysis and management methodology developed by Central Computing and Telecommunications Agency (CCTA) of government of United Kingdom focusing on the IS security of the governmental departments [34]. Later on the methodology was redeveloped by Siemens Enterprise to make it a complete approach and tool for information system security and recommends the quantitative risk estimation. The CRAMM is composed of three phases containing asset identification and evaluation by defining the boundary of the analysis and valuing the physical and soft assets in a quantitative way, threat and vulnerability assessment by identifying the potential threats and vulnerabilities and their severity. Threat and vulnerabilities are calculated by measuring the risk with respect to the information of assets, and countermeasure selection and recommendation is a way to manage by providing a list of countermeasures to be applied to IS to mitigate the risk.

2.2.1.5 SQUARE - SQUARE is a nine step process, which elicits, categorizes and priorities security requirements [23]. Security requirements are specified before the critical architectural and design decision to get the most benefit out of this methodology. In this way the critical business risk can be addressed at the requirement engineering stage. The nine steps of the SQUARE method includes agree on definitions, identify security goals, develop artifacts to support security requirements, perform risk assessment, elicitation technique, elicit requirement, categorize and prioritize requirements, and requirement inspection.

2.2.2 Why ISSRM?

There are various approaches, methodologies and standards related to security risk management. ISSRM is a result of already existing methodologies and standards and cover the weaknesses of the previous approaches and includes their advantages. ISSRM is not specific to one organization but rather it covers the security risk management of all organizations considering their assets, risks and their treatment. Table 2.1 shows the comparison of ISSRM with other approaches. Risk Management Approach/Method column defines the methods used for security risk management. IS Based and Risk Management Based approach columns defines whether the method uses an IS and risk management approach. The alignment of modelling languages defines if a risk management method supports modelling languages.

Table 2.1 Comparison of Risk Management Approches and Methods

Risk Management Approach/Method	IS Based Approach	Risk Management Based Approach	Alignment of Modelling Languages
EBIOS	Yes	Yes	No
MEHARI	Yes	Yes	No
OCTAVE	Yes	Yes	No
CRAMM	Yes	Yes	No
SQUARE	Yes	Yes	No
ISSRM	Yes	Yes	Yes

2.3 ISSRM Domain Model

Information systems (IS's) are the baseline of the business in today's era. In many organizations, survival and even existence without extensive use of information system is inconceivable, and information system plays an important role in organizations productivity. Information systems are widely used in distributed environment therefore security in this context is an important issue in order to run and different security risk management techniques has been applied to secure the business. Security Risk Management has evolved from time to time and different security standards have been adopted.

Information system security risk management (ISSRM) domain model is a framework which addresses the most important points for handling the security related issues in an information system domain [18]. The domain model is defined after a careful survey of the risk management standards, security related standards and security risk management methods and software engineering frameworks. This reference model defines the fundamental concepts of ISSRM as collected from different security standards of risk management and other sources. The focus of ISSRM reference model is to secure the information system. ISSRM reference model is mainly structured into three different conceptual categories as shown in the Fig 2.1.

2.3.1 Asset-related concepts: It deals to protect some properties that have some value to an organization and the criteria to assure protection of those properties.

Asset: The resources and properties of an organization having some value that help an organization to achieve certain objectives.

Business Asset: An information processes that comply with the mission of organization to achieve certain objectives that benefit the business.

IS Asset: The elements of an information system required by the business asset to perform certain task (i-e: use of computer to perform certain task). Example: online transfer of funds in a bank, because the transaction will utilize the IS Asset to benefit some entity.

Security Criterion: It is the property or a constraint of a business asset that is supposed to be assured for the smooth flow of the transaction. Mainly security criterion describes the confidentiality, integrity and availability of the system.

Security Requirement: It is a countermeasure that is to be implemented to mitigate potential attacks to the system.

2.3.2 Risk related concepts: It defines the concept and exposure of harmfulness to assets.

Risk: Defines the possibility of harmfulness. It is consisted of the following elements, when combined together creates a negative consequences to the system and business.

Impact: Negative consequences of a risk that may harm assets of an organization when a threat is successful which eventually negates the security criterion and result in a loss of confidentiality, integrity, and availability of the resources.

Event: A set of actions that combine threat and vulnerability to harm the system or organization.

Vulnerability: It is a weakness or a flaw in a system that can be exploited by a hacker to harm assets in terms of IS security.

Threat: Intention to inflict an attack mainly to harm the IS and business Asset. The threat is carried out by a threat agent and attack method.

Threat Agent: An agent that produces a threat to harm the IS asset and is mainly a source of risk to the IS. Example: A hacker, an insider (employee of the organization)

Attack Method: A technique through which a threat agent produces a threat. Example: Exploiting an online message sending vulnerability to steal information.

(v) *Security Requirements Definition:* Security Requirements are dependent on the decision taken in step 4. Security requirements are the countermeasure to mitigate the risk and its consequences. Some security requirements decisions have to be taken. Once the security requirements are finalized, they must be verified for the security they provide; otherwise the risk treatment process should be revised again for proper protection.

(iv) *Control Selection and Implementation:* The process of improving the security of the system by setting some security policies and countermeasures and their implementation.

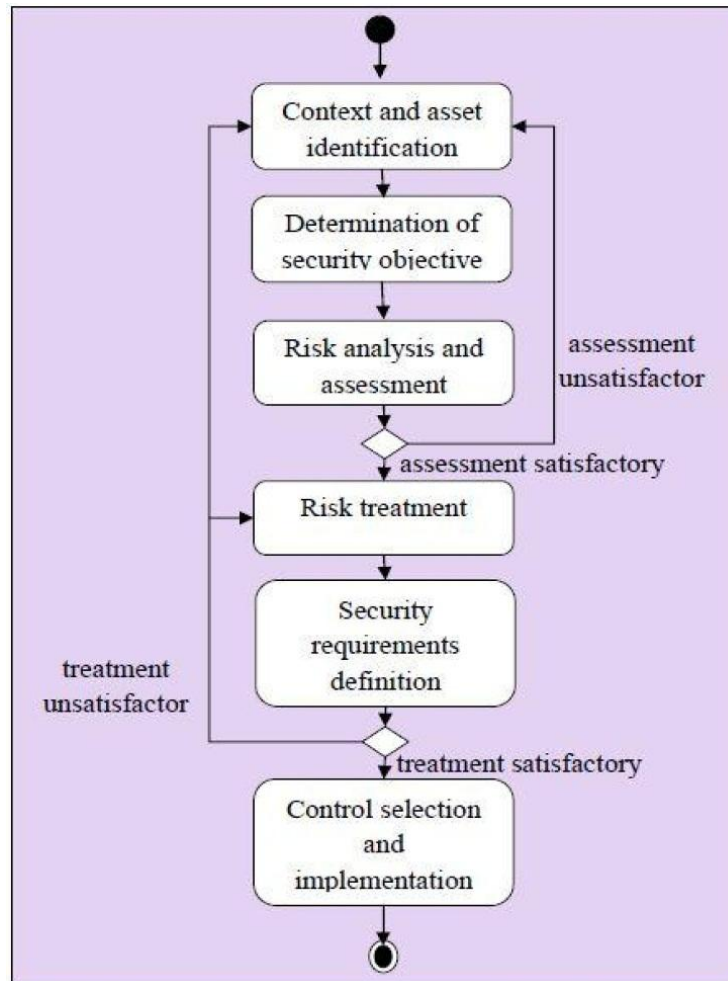


Fig. 2.2 ISSRM Process (taken from Mayer, 2009 [18])

2.7 Summary

The demand for security of IS is constantly growing and it is the most essential thing that needs to be catered during the early development process. Security breaches in IS can lead to the negative consequences. Considering the security at early stages assists to analyse and estimate security measures of the IS to be developed. Security risk management has evolved from time to time and different security standards have been adopted but many of the state of the art methodologies and standards ignore the importance of managing the risk at requirement elicitation phase. ISSRM domain model is a framework which addresses the most important points for handling the security related issues in an information system domain. The objective of ISSRM is to extend modelling languages with ISSRM concept alignment to analyze requirements at the early stage of the development. The focus of ISSRM reference

model is to secure the information system. ISSRM process is a security requirement engineering process based on the risk analysis methodology. As discussed in this chapter, we have come up with different terminologies like asset, risk, threat and vulnerabilities that are used in the domain of security risk management. Following are the reasons behind our decisions: It has already been used for concept alignment at requirement engineering.

- It defines and covers the security risk management concepts at three different conceptual levels and satisfies the security needs of an organisation.
- It allows the alignment of security modelling languages and has already been used for this purpose.
- The focus is to secure the information system.

Chapter 3

Modelling Languages

This chapter introduces the modelling languages with their construct and examples for security risk management. The languages include BPMN, Secure Tropos, Mal-Activity and misuse cases.

3.1 BPMN

3.1.1 Purpose

Business Process Modelling Notation (BPMN) is used to represent business processes graphically, their execution, analysis and monitoring [29]. It is used widely now days for information system management of the business processes. The business processes involves human interaction, software and information communication and physical artefacts. The business process includes events, activities and decisions that are logically related to each other.

3.1.2 Construct and Example

A process in BPMN is called a business process diagram and is consist of the four major categories of construct. It includes *events*, *activities*, *gateways and connections*, *objects and artefacts*. The *Events* represented by a circle are the starting and ending points of a process, they can be triggered with different messages, timers or signals to indicate a particular event. *Gateways* indicate a control flow of the activities and events based on the condition and are represented by a diamond shape. The *task or activities* are an atomic unit that represents a single unit of work, the multiple similar tasks are merged as a *subtask* or compound unit of work. *Swim lanes* is a way of categorizing tasks and usually contains *pools* and *lanes*.

A *Pool* is a representation of participants or resources in a BPMN Process and show the message flow between processes and participants and a *Lane* categorizes the flow of events and an organization unit. *Sequence flow* connects the gateways, events and activities to be performed. *Message Flow* shows the flow of messages across two or more pools, typically the flow of inputs or outputs from one pool to another and vice versa. Association links flow objects to artefacts and/or annotation. The BPMN artefacts are the data objects which show that what data is required by activities, data stores represents a way to store data and annotations is a way to attach additional information with objects. In Fig 3.1, we show an example of BPMN with its legends.

3.1.3 Relationship to ISSRM

The example in Fig. 3.1 has applied the construct of BPMN considering the attack scenario and providing the countermeasures in reference to ISSRM domain model. Asset Related concepts include valuable business assets like processes and information and can be observed in a BPMN construct, such as task, gateway, event and their connecting points. Risk-related concepts, In BPMN, there is no concrete way to model the security risk, however the pool represents the negative participant and can be characterized as a threat agent in BPMN construct and any task or an activity performed by threat agent is considered to be an attack method and same argumentation is applied to flow and data association flow. Risk treatment-related concepts deals with the actions to be taken and the decisions regarding implementation of the control to mitigate the risks. The approach of risk reduction, risk transfer, risk avoidance and risk acceptance can be applied to treat the risk depending on the mitigation of

the risk, in our example we have selected the risk reduction (i.e. risk treatment decision to mitigate the risk).

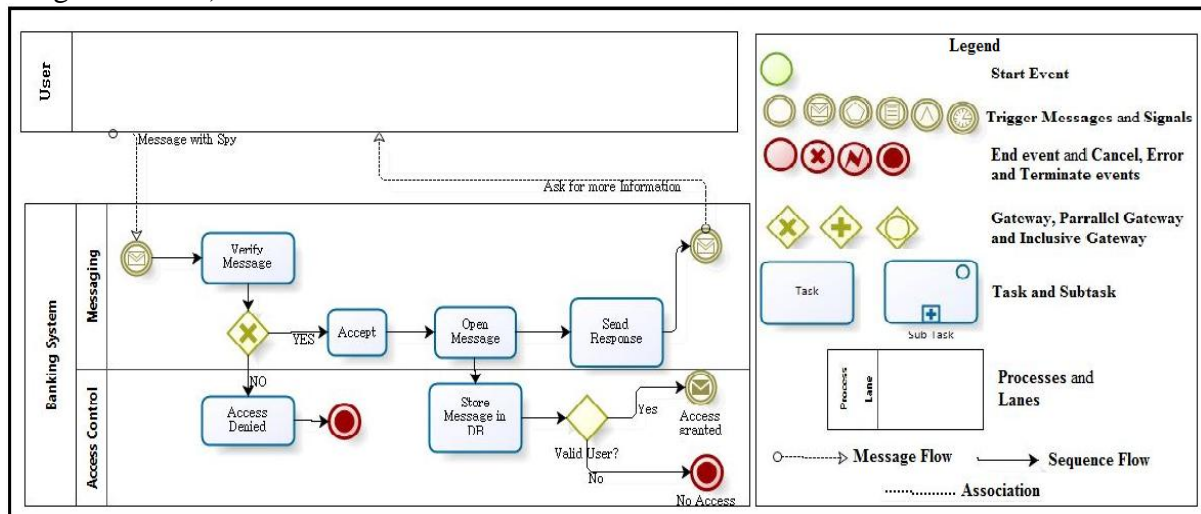


Fig. 3.1. BPMN Risk Management

3.2 Secure Tropos

3.2.1 Purpose

Secure Tropos is based on the core concept of Tropos. It is a security oriented extension of Tropos methodology which is used at early requirement analysis and later on defines the architectural and design level concepts [6, 20, 21].

3.2.2 Construct and Example

Secure Tropos has been extended from *i** modelling framework which consist of *actors*, *goals*, *tasks*, *resources* and *social dependencies*. Likewise, Secure Tropos are also consists of *actor* (An entity having strategic benefits and goals within the system), *goal* (represents actor's intentions within the system), *soft goals* (represents non-functional requirements), *resource* (Physical or Informational entity) and *plan* (represents a task or an activity). *Security constraint* (A restriction related to security of the system) and *threat* for modelling the security related concepts. The concrete elements of Secure Tropos are linked together with the relationship of *depender* and *dependee*. The legend of secure tropos and an example is shown in the Fig 3.3.

3.2.3 Relationship to ISSRM

The example in figure 3.3 has applied the construct of secure Tropos considering the attack scenario and providing the countermeasures in reference to ISSRM. *Asset-Related concepts*, in secure tropos, *actor*, *goal*, *softgoal*, *plan* and *resource* are used to identify the *business asset* and *IS Asset* and *security constraint* and *softgoal* as *security criterion*. *Risk-Related concepts* represents the potential risk and the construct in secure tropos are; *impact* represented by contribution between the threat and softgoal where *threat* is a *goal*, *plan*, *threat agent* is an *attacker* and *vulnerability* as *belief* and *attack method* is a *plan* and *relationship attacks*. *Risk-Treatment related concepts* represented through security criterion in secure Tropos with the construct of *actor*, *goal*, *softgoal*, *plan*, *resource* *security constraint*.

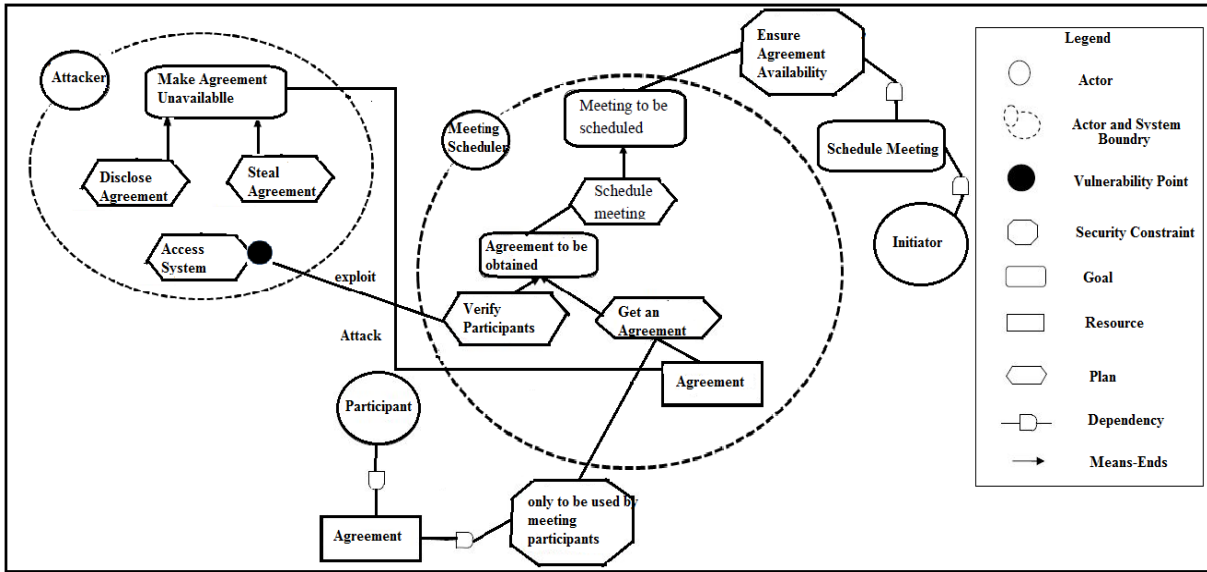


Fig. 3.2 Modelling with Secure Tropos

3.3 Mal-Activity

3.3.1 Purpose

The idea behind the Mal(icious)-activity is same as of standard UML activity diagrams but with the intentions of capturing the negative scenario at the early phase of RE and modelling of the system [7, 8]. It uses the same semantics and syntax of activity diagrams to draw the Mal-activity diagrams but only with a little change to capture the negative scenario. Mal-activity abbreviated as MAD describes the procedural logic, business process and work flow.

3.3.2 Construct and Example

Mal-Activity uses the same construct as of activity diagrams but the exception of construct that capture the negative scenario like *Mal-activity*, *Mal-swimlane*, and *Mal-decision* as show in a figure 3.3 along with other MAD constructs. All of the concrete elements of the MAD are connected with the *control flow* arrow. *Activity* describes an atomic unit of task and *Mal-Activity* describes the negative task performed by a hostile user. *Initial state* is the starting point of the activity whereas the *final state* is the ending point of an activity. The example of MAD is shown in figure 3.4 which shows the sequence of actions to update user's personal information while the hacker is intending to steal the user credentials from the user.

3.3.3 Relationship to ISSRM

The example in fig. 3.4 has applied the construct of MAL-Activity diagram considering the attack scenario and providing the countermeasures in reference to ISSRM. *Asset-Related concepts*, in MAD, *activity*, *decision*, *control flow* are used to identify the *business asset* and *swimlane* and *activity*, *decision* as *IS Asset*. *Risk-Related concepts* represents the potential risk and the construct in secure tropos are: *impact* as *Mal-Activity*, *threat agent* as *Mal-Swimlane* and attack method as *Mal-Activity*, *Mal-Decision*, *control flow* and *Mal-Swimlane*. *Risk-Treatment related concepts* define the security countermeasures and *mitigation-activity* is used as a security requirement for MAD.

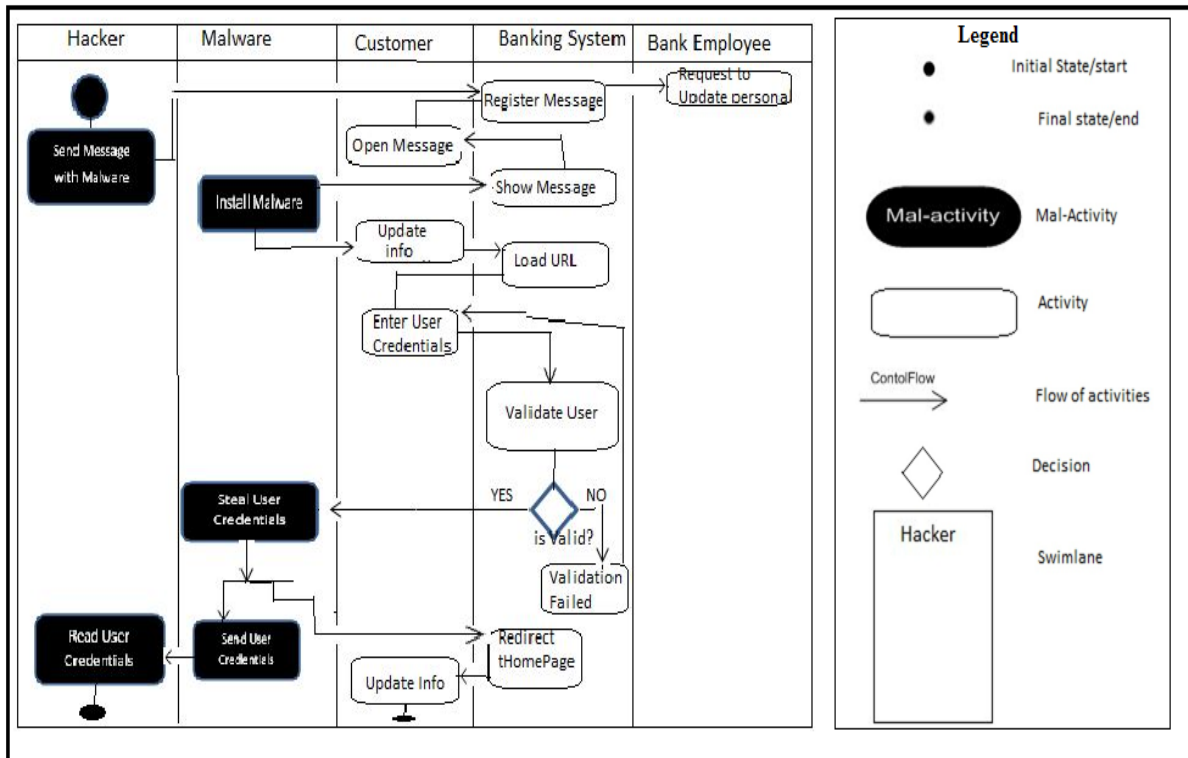


Fig. 3.3. MAL-Activity diagram and Legends

3.4 Misuse Cases











3.4.1 Purpose

Based on UML definition of use cases, Misuse cases are also defined as a sequence of actions required for the interaction between the *Misuse case* and a *Misuser* to achieve a certain goal in an undesired way [3, 17, 26]. *Misuse Case* is a list or sequence of steps, if performed by an agent successfully, cause harm to the stakeholder and/or to a system. A *Misuser* is an actor that is willing to use the system with unfavourable intents, deliberately or not deliberately.

3.4.2 Construct and Example

Graphical Notation describes the high level view of the systems functionality. Misuse case extends the use case notation to describe the security requirements of the system to be developed. The Fig 3.4 and Fig. 3.5 shows a basic example of use cases and misuse cases diagrams. The diagram uses the relationships of use cases including *includes* and *extends*, and it introduces the relationships *mitigates*, *threaten* and *exploits* to the model. The diagram also uses the use cases as *misuse case* in dark shadowy use cases. An actor plays a role of interacting with the system. An *actor* can be initiator or participant. A use case is a list of actions to be performed by an actor to achieve certain goals. The relationship *includes* and *extends* define that a use case can include or extend one or more use cases to itself. A misuse case is a list of hostile actions when completed successfully by misuser cause harm to the system assets or stockholder. A misuser is an actor or an agent who initiates a threat to the system deliberately or inadvertently. It can be an attacker or hacker. The threaten relationship indicates that a misuse case want to harm a use case whereas a mitigates relationship provides a countermeasure by means of a security use case to the use case.

Table 3.2 Construct of Misuse Cases

Misuse Case	Graphical Notation
Actor	
Use Case	
Threat	
Misuser	
Security Requirement	
Extends ,Includes	<code><<extends>></code>  <code><<includes>></code> 
Threatens, Exploits and Mitigates	<code><<threatens>></code>  , <code><<exploits>></code>  <code><<mitigates>></code> 

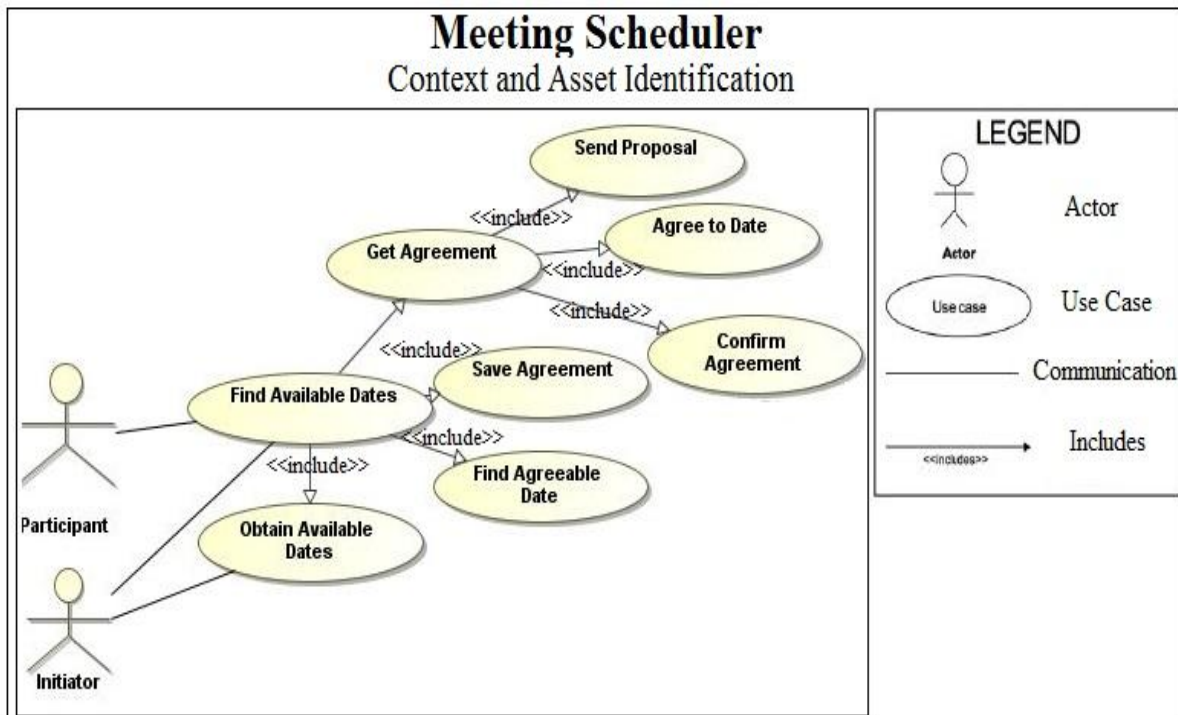


Fig. 3.4 Assets Modelling

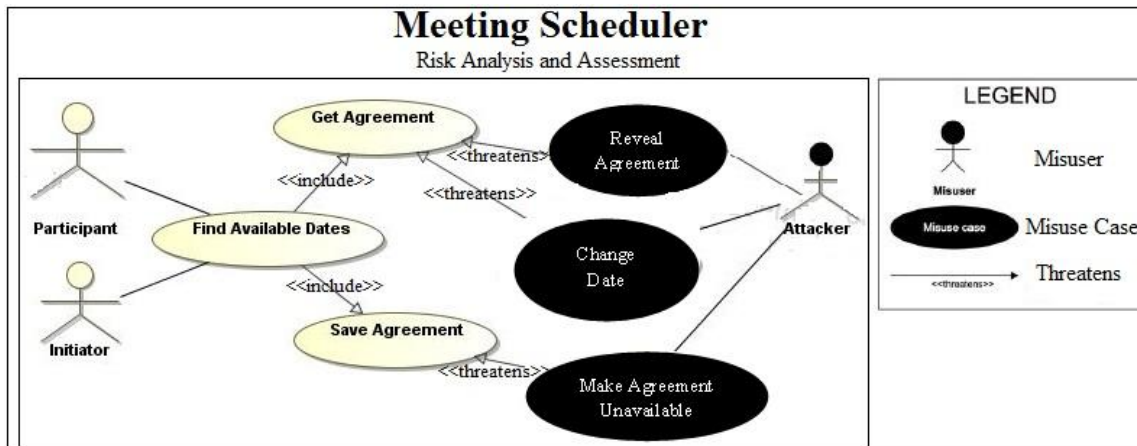


Fig. 3.5 Threat Modelling

3.4.4 Misuse cases and ISSRM

The existing alignment of misuse cases is not entirely aligned with ISSRM domain model but rather it present the correspondence, overlap or similarity of concepts between the Misuse cases and ISSRM domain model as shown in the Table. 3.1. Misuse case constructs are given in the Misuse case diagram column conforming to ISSRM domain model. Synonyms column defines the similar meanings found in the literature and ISSRM Domain model column defines the elements of ISSRM domain model. Assets in ISSRM domain model corresponds to Actor and Use cases in the graphical notation which also represent IS Assets and Business Assets. Risk (Threat) is represented as a misuser and misuse case where misuser is a threat agent and misuse case is an attack method. Risk Treatment only defines the security requirement by means of use case in misuse case diagrams. Rows with a “-” are not yet aligned with the concept of ISSRM reference model.

Table 3.1 Alignment of Misuse cases with ISSRM (Taken from [17])

ISSRM domain model		Misuse Cases	
		Synonyms	Misuse case diagram
Asset	Asset	Vulnerable asset, critical asset, materials, information, (virtual) location, (computerised) activities, knowledge and skills of workers	Actor and Use case
	IS asset	-	
	Business asset	Business use case	
	Security criteria	Security goal, type of security breach	-
Risk	Risk	Risk of various threats	-
	Impact	Cost of the damage, cost of potential losses	-
	Cause of the risk	-	-
	Vulnerability	-	-
	Threat	Security threat	Misuser and Misuse case
	Threat agent	-	Misuser
Risk treatment	Attack method	Action sequence, sequence of both action and interaction, step	Misuse case
	Risk treatment	-	-
	Security requirements	Security use case, security requirement, countermeasure	Use case
	Control	-	-

3.4.5 Textual Template for Misuse Cases

A misuse case diagram only gives a high level view of the functionality and security threats of the system to be developed, on the other hand, like use cases, the use of textual template can be very useful as it provides the detailed information about the functionality and security threats of the system by providing the description of the steps of sequence to be performed [26]. They are documented in a misuse case template. Misuse cases can be expressed in two different textual descriptions. Lightweight description and extensive description, these two descriptions are out of the scope of this research work.

3.4.6 Summary

In this chapter we introduced different modelling languages including BPMN, Secure Tropos, Mal-Activity and MUC. Business Process Modelling Notation (BPMN) is used to represent business processes graphically, their execution, analysis and monitoring [29]. It is used widely now days for information system management of the business processes. Secure Tropos is based on the core concept of Tropos. It is a security oriented extension of Tropos methodology which is used at early requirement analysis and later on defines the architectural and design level concepts [6]. The idea behind the Mal-activity is same as of standard UML activity diagrams but with the intentions of capturing the negative scenario at the early phase of RE and modelling of the system [7, 8]. MUC is based on UML definition of use cases, Misuse cases are also defined as a sequence of actions required for the interaction between the Misuse case and a Misuser to achieve a certain goal in an undesired way [3, 17]. We provide a simple introduction to the languages, its relation to ISSRM and the example of each language. We also introduced existing misuse cases and its relation to ISSRM along with the example.

PART II
CONTRIBUTION

CHAPTER 4

Alignment of Misuse Cases to ISSRM

The main objective of aligning misuse cases with ISSRM is to evaluate and assess the capability of misuse case for security risk management in reference to ISSRM. Also it will help firstly, in understanding security concerns at the earlier stages of the development. Secondly, to view security problems from different angles, understanding different security development perspectives.

4.1 Research Method

To align Misuse cases with ISSRM domain model, we applied the research method shown in Fig. 4.1. The main research objective of this study is to enable misuse cases in order to support the security risk management in IS development. Our research method is as 3-step process: firstly, we conducted literature review of security in information systems and the ISSRM domain model to identify the security risk concepts. Secondly, we investigated how existing misuse case diagrams model the security risk concepts. Here, we observed the limitation of misuse case diagrams in modelling the ISSRM concepts and executing the risk management processes. Lastly, we introduce extensions to the misuse case diagrams i.e. SROMUC. They include the extended meta-model of Misuse case diagrams with new constructs to address ISSRM concepts. The new meta-model provides concrete syntax and semantics to represent asset, risk and risk-treatment models using Misuse case diagrams. This work is a part of the larger effort to align several modelling languages to the ISSRM model, define their semantics at full extend and develop a systematic model transformation based security risk-driven method for secure system development.

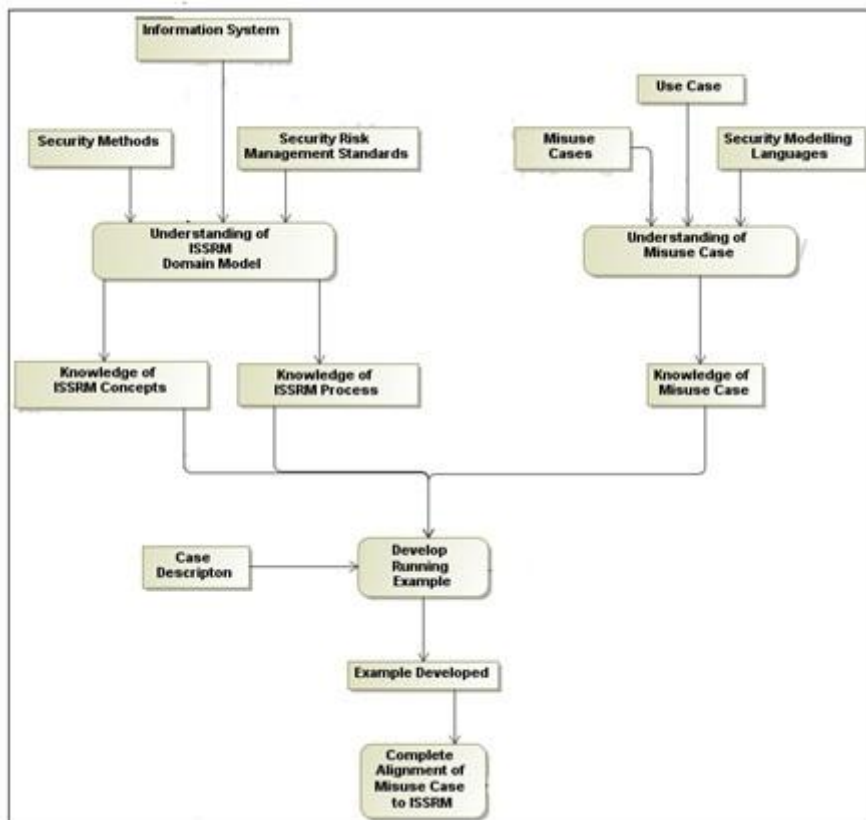


Fig. 4.1 Research Method

4.2 Misuse Case Running Example

4.2.1 Scenario 1: SROMUC Modelling for Integrity

This research applies modelling with SROMUC for an online banking IS [1, 31] and illustrates the usage of SROMUC. We split the example in asset model (see Fig. 4.2), threat model (see Fig. 4.3), and security requirement model (see Fig.4.4).

4.2.1.1 Asset model. In Fig.4.2, we present the context of an online banking IS modelled in a use case diagram along with the security criterion. A *security criterion* (see Fig. 2) is a security property imposed on *business use case* (i.e., business asset). The example focuses on the bank customer and bank officer who communicate with Banking IS. The Bank Customer and Bank Officer are the assets characterizing the users of the system in reference to ISSRM domain model. The bank customer seeks to Perform Transaction and bank officer seeks to Keep Account Data Up To Date. The Perform Transaction *includes* two use cases Pay Money and Keep Account Data Up To Date and *extends* Perform Transaction Via Online. Perform Transaction has a *security criterion* Integrity of Transaction represented as a *hexagon* (see Fig. 2) as it characterizes a security constraint of a *business use case* (i.e., Perform Transaction). In Fig. 2, a dotted line with stereo type *constraints of* is linked from *business use case* (i.e., Perform Transaction) to *security criterion* (i.e., Integrity of Transaction) shows the relationship between the two. According to ISSRM domain model we identified Perform Transaction as a business asset that has some business value and Perform Transaction Via Online support the business asset and is considered as an IS asset.

4.2.1.2 Risk model. In Fig. 4.3, we presents potential threat scenario modelled in SROMUC diagram. *Misuser* (i.e., Attacker) initiates a *misuse case* (i.e., Intercept Money *includes* Transfer money to another account and Change details of transaction) by exploiting the *vulnerability* (i.e., Unsecure Network Channel) in a *use case* (i.e., IS asset). In Fig. 3, the *vulnerability* is represented by filled grey use case. The *misuse case* Intercept Payment *threatens* the *use case* Perform Transaction Via Online (i.e., IS Asset). The threat Intercept Money *leads to* an *impact* (i.e., Money Transferred to Unintended Account) which *harms* the *business use case* (i.e., Perform Transaction) and disaffirms the *security criterion* (i.e., Integrity of Transaction). The *impact* is a state of system that is represented as *rounded rectangle* (see Fig. 3). *Misuse case* is linked to impact using *leads to* relationship. On one hand, *impact* disaffirms the *security criterion* linked with *negates* relationship. On another hand *impact* *harms* the *business use case* (i.e., Perform Transaction).

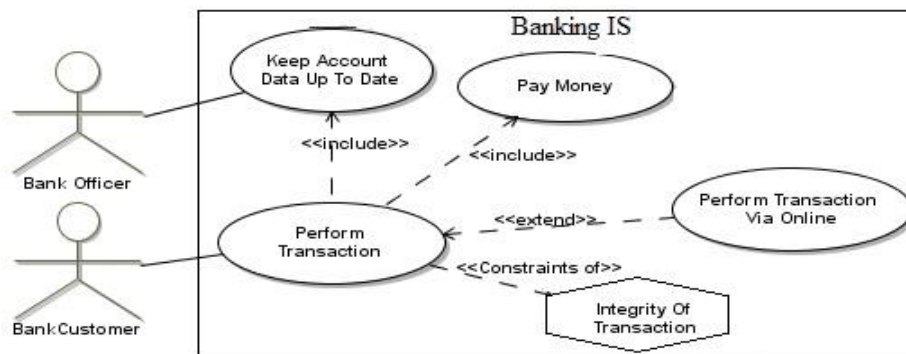


Fig.4.2 Asset Modelling

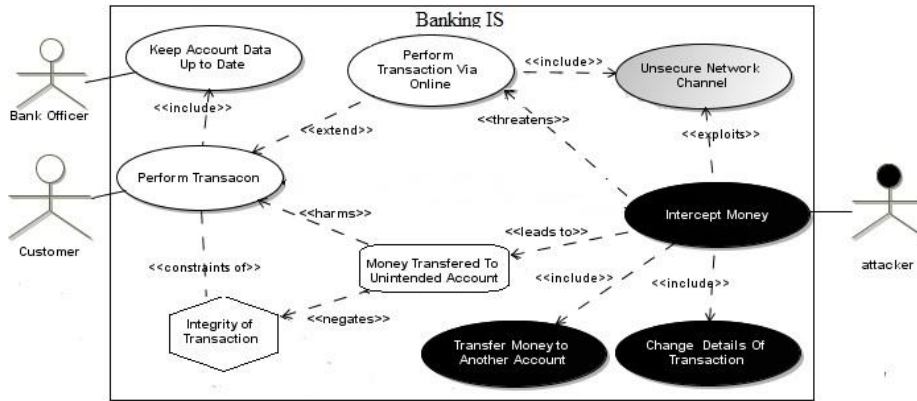


Fig.4.3. Threat Modelling

4.2.1.3 Risk treatment model. ISSRM domain model supports the risk treatment, control and its implementation. However, SROMUC does not support the modelling of these concepts but security requirement is modelled as a *security use case*. *Security use case* is represented as a *use case with a lock inside* (see Fig. 4.4). In Fig. 4, we present the security requirement for identified threats in our example. The *use case* Perform Transaction Via Online (i.e., IS Asset) *includes* a *security use case* (i.e., Apply Cryptographic Procedures and Use Secure Communication Protocol). The *security use case* *mitigates* the *misuse case* (i.e., Intercept Money). It ensures *security criterion* (i.e., Integrity of Payment) imposed by *business use case* (i.e., Perform Transaction).

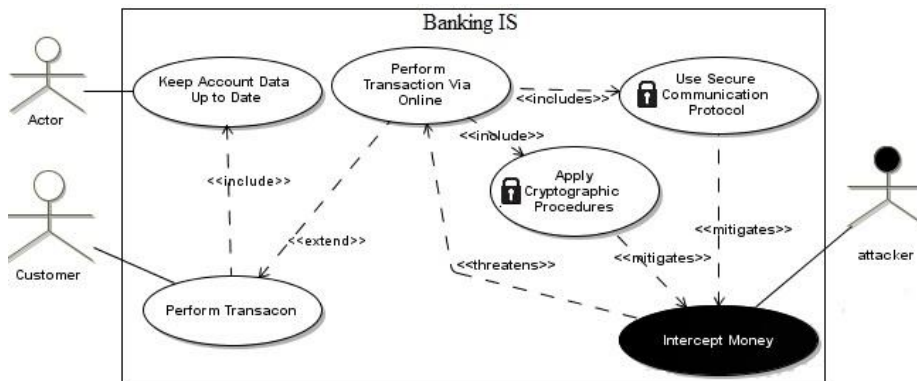


Fig.4.4. Security Requirement Modelling

4.2.1.2 Scenario 2: SROMUC Modelling for Availability

In Fig. 4.5, we model an online banking IS [1, 31] for Availability of Service. In our example, the *business use case* (i.e., Perform Transaction) has a constraint of *security criterion* (i.e., Availability Of Online Service). The *misuser* (i.e., Attacker) initiates a *misuse case* (i.e., Make Online Service Unavailable *includes* Initiate Half Opened Connections To Server). It exploits the *vulnerability* (i.e., Allow Unlimited Number Of Connections) included in a *use case* Perform Transaction Via Online (i.e., IS Asset). The *misuse case* Make Online Service Unavailable *threatens use case* Perform Transaction Via Online (i.e., IS asset) and *leads to* an *impact* (i.e., Availability Of Service Is Compromised), moreover, it *harms* the business use case Perform Transaction. The *impact* of the *misuse case* *negates* the *security criterion*.

4.2.1.3 Scenario 3: SROMUC Modelling for Confidentiality

In Fig. 4.6, we model the example of an online banking IS [1, 31] for the Confidentiality Of Data. In this example, the *business use case* (i.e., Perform Transaction) has a constraint of *security criterion* (i.e., Confidentiality Of Transaction). The *use case* Perform Transaction Via Online (i.e., IS asset) *includes* another *use case* (i.e., Ensure Account privacy *includes* Enter PIN Code) for securing an online transaction. The *misuser* (i.e., Attacker) initiates a *misuse case* (i.e., Steal Account Data *includes* Retrieve Transaction Data *includes* Disclose Transaction Data) by exploiting the *vulnerability* (i.e., Data Is Not Encrypted and Accept Malicious Data). The *misuse case* (i.e., Steal Account Data) *threatens* the *use case* Perform Transaction Via Online (i.e., IS asset) and *leads to* an *impact* (i.e., Confidentiality Of Data Is Compromised), moreover, It also *harms* the *business use case* (i.e., Perform Transaction). The *impact* of the *misuse case* *negates* the *security criterion*.

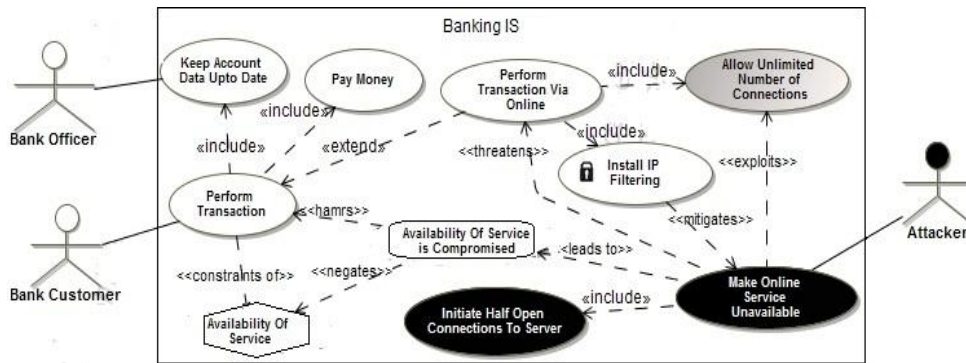


Fig.4.5. Modelling for Availability of Service

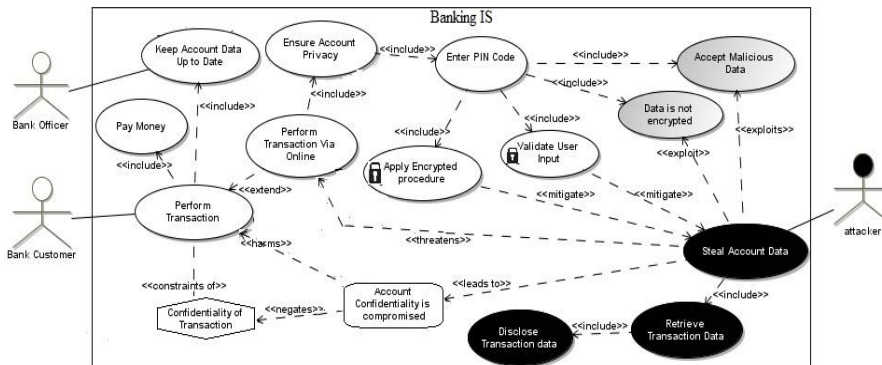


Fig. 4.6. Modelling for Confidentiality of Data

4.3 Concept Alignment of SROMUC and ISSRM

The existing alignment of misuse cases is not entirely aligned with ISSRM domain model but rather it presents the correspondence, overlap or similarity [2, 16]. In this section we describe the alignment of SROMUC with the concepts found in ISSRM domain model. In Table 4.1, 4.2 and 4.3, first column defines the concepts of ISSRM domain model. Second column defines the synonyms found in the literature. Third column differentiates the concepts and relationship. The last column defines the visual construct for SROMUC.

4.3.1 Alignment of asset related concepts. In Table 4.1, we introduce SROMUC syntax to represent the ISSRM asset related concepts. Assets in ISSRM domain model corresponds to *Actor* and *Use case* in SROMUC. The business asset and the IS assets are modelled as a *use case*. The *supports relationship* in ISSRM between IS asset and business assets is expressed using *extends* and *includes relationship*. We introduce *hexagon* construct in SROMUC to





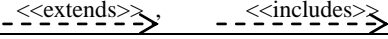
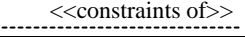
represent the *security criterion* from ISSRM. According to ISSRM *security criterion* is constraint of business asset therefore the *hexagon* is linked to *business use case* through dotted line with *constraint of relationship*.

4.3.2 Alignment of risk-related concepts. In Table 4.2, we introduce SROMUC syntax to represent the ISSRM risk-related concepts. *Misuser* is represented as a *Threat Agent*, *Attack Method* as *Misuse Case* and *Vulnerability* as a filled grey *use case* in SROMUC. The *Threat* is modelled as a combination of a *misuser* and *misuse case* (i.e., *Misuser* communicates with *Misuse Case*). The *targets relationship* in ISSRM domain model is represented as a *threatens relationship* in SROMUC. We used a *rounded rectangle* to model the *impact* concept of ISSRM.

In order to be compliant with ISSRM domain model, we also introduce the *exploits*, *leads to*, *harms* and *negates* relationships. *Exploits* relationship defines a link between *misuse case* and the *vulnerability* whereas *leads to* relationship defines a link between the *misuse case* and the *impact*. The *harms* relationship defines the link between an *impact* and a *business use case* whereas a *negates* relationship defines a link between an *impact* and the *security criterion* (see Table 4.2). We combine the concepts of *threat agent*, *attack method*, *vulnerability*, and *impact* all together to represent an *event*, where a *risk* is understood as a combination of *event* and the *impact*.

4.3.3 Alignment of risk treatment related concepts. In risk treatment related concepts, we update the visual syntax of *security use case* by adding a padlock to *security use case* which represents *security requirement* (see Table 4.3) in ISSRM. The *Mitigates relationship* of ISSRM is modelled with *mitigates relationship* from *security use cases* (i.e., security requirement) to *misuse case* in SROMUC.

Table 4.4. Asset Related Concepts (C – Concept, R – Relationships)

ISSRM Concepts	Synonyms	Type	SROMUC Syntax
Assets	-	C	
Business Asset	Business Use Case	C	
IS Asset	IS Use Case	C	
Security Criterion	Security Constraint	C	
Supports	-	R	
Constraints of	Restriction	R	

4.4 Abstract Syntax of Security Risk-oriented Misuse Cases

We presented the SROMUC before abstract syntax due to the simple introduction of the language. However, to illustrate the application of proposed SROMUC, we need to present the abstract syntax. In Fig. 4.7, the Meta model presents an abstract syntax of SROMUC. The major elements in the Meta model are an *Actor OR Misuser* and *Use OR Misuse Case*. *Actor OR Misuser* initiates the *communication* to interact with *Use OR Misuse Case*. Their cardinality shows that an *Actor or Misuser* can communicate with one or more *Use or Misuser Case*. *Actor* and *misuser* are the specialization of an *Actor OR Misuser*. *Use Or Misuse case* can *includes* or *extends* another *Use OR Misuse Case*. The *Use Case*, *Vulnerability* and *Misuse Case* are the specialization of *Use OR Misuse Case*. The *Use Case* includes one or more *Vulnerabilities* that can be exploited by one or more *misuse cases*. A *Misuse Case* threatens (i.e., *threatening*) one or more use cases. A *Misuse Case Leads To* one

or more *Impact*. An *Impact* will have *Harms* on one or more use cases by negating one or more *Security Criterion* defined as *Constraint Of* that *use case*. A *Security Use Case* is a specialized *Use Case*. One or more *Security Use Case Mitigates* one or more misuse Cases.

Table 4.5. Alignment of Risk related Concepts(C – Concepts, R – Relationships)








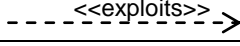
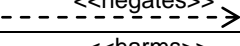
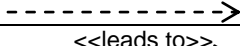
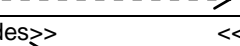
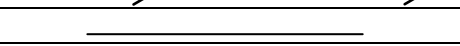
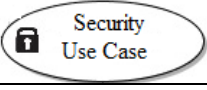
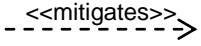
ISSRM Concepts	Synonyms	Type	SROMUC Syntax
Risk	Hazard	C	
Impact	Effect	C	
Event	Incident	C	
Attack Method	Violence	C	
Vulnerability	Weakness	C	
Threat Agent	Attacker	C	
Threat	Hazard	C	
Exploits	-	R	
Negates	Denies,	R	
Harms	-	R	
Leads to	-	R	
Characteristics of	-	R	
Uses	-	R	

Table 4.6. Risk Treatment related Concepts (C – Concepts, R – Relationships)

ISSRM Concepts	Synonyms	Type	SROMUC Syntax
Risk Treatment		C	
Security Requirement	Countermeasure	C	
Control		C	-
Refines		R	-
Mitigates	Diminishes	R	
Implements			-

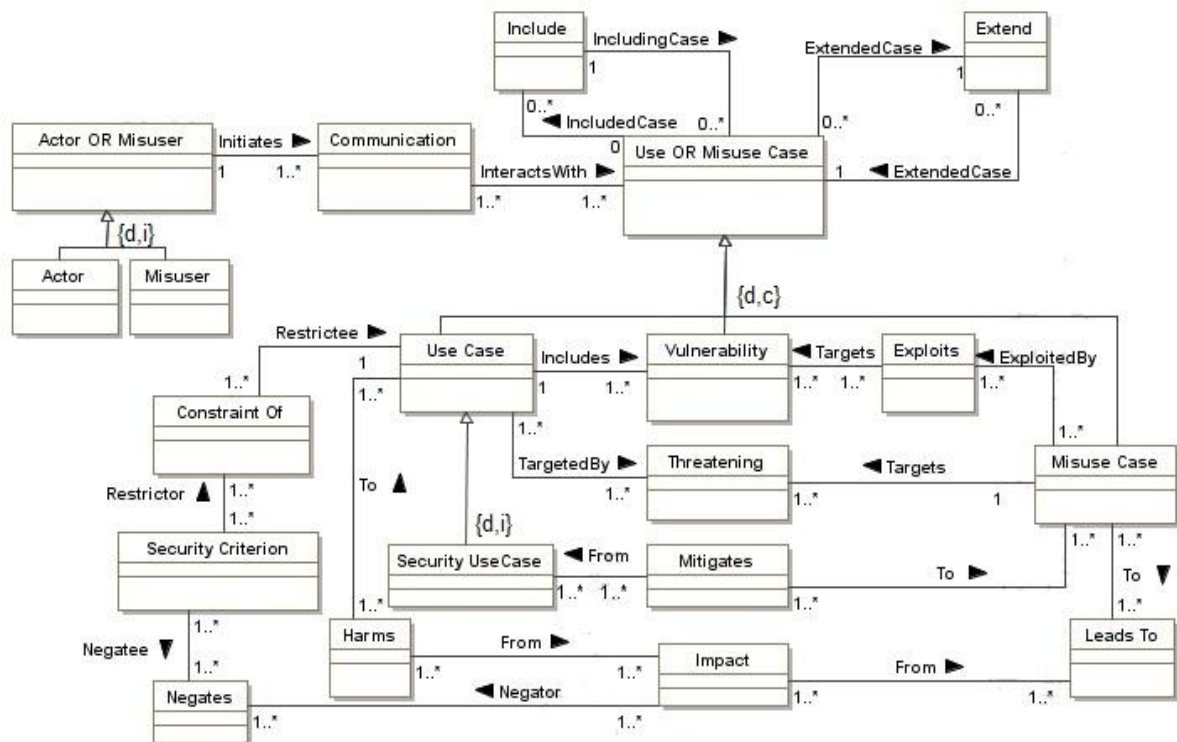


Fig. 4.7. Meta Model of SROMUC

4.5 Summary

In this chapter, we have analysed how Misuse Cases can be used to manage security risks at the early stages of the IS development. The main objective of aligning misuse cases with ISSRM is to evaluate and assess the capability of misuse case for security risk management in reference to ISSRM in understanding security concerns at the earlier stages of the development. we applied the research method shown in Fig. 4.1, we study the literature regarding security in information system and investigated how existing misuse case diagrams model the security risk concepts, we introduce extensions to the misuse case diagrams and introduces SROMUC and applied it on an online banking IS for Integrity, confidentiality and availability of service. We developed three scenarios to illustrate these concepts. we presented the alignment of SROMUC with the concepts of ISSRM domain model. Table 4.1, 4.2 and 4.3, gives a high level overview of the alignment. In the end, the abstract syntax of SROMUC was given which describe the application of SROMUC.

CHAPTER 5

Model Transformations

This chapter introduces a set of rules for translating SROMUC to Secure Tropos model. They are based on ISSRM domain model and its application process and the alignment of both the languages to ISSRM. We will apply the incremental model to transform the SROMUC to secure tropos rule by rule. To apply the transformation rules we will use the example presented in Fig. 4.3, 4.4, and 4.5 of scenario 1 – SROMUC modelling for Integrity of Section 4.2.1. The transformation presented here are the extension, correspondence and/or overlap of the transformation given by Naved *et al* [1, 2].

5.1 Transformation Rules from Misuse cases to Secure Tropos

TRMS 1: *A system boundary in SROMUC is translated to a system actor and its boundary in secure tropos.* This rule is based on alignment between the Secure Tropos actor and misuse case system boundary to the ISSRM IS asset. After applying TRMS 1, we will get the following model as shown in Fig. 5.1.

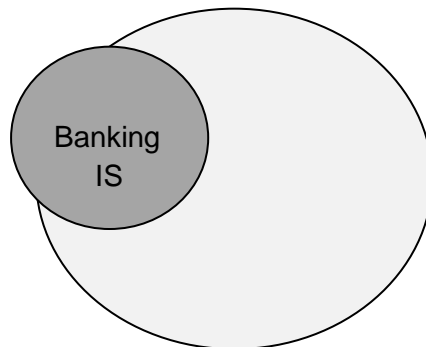


Fig. 5.1. System Actor

TRMS 2: *A use case in SROMUC is translated to a goal or a plan in secure tropos. Similarly, an includes or extends relationship is translated to a means-end where ends is the goal and means is the plan and decomposition link where some plan is decomposed.* Here the developer decides whether a use case is translated to Secure Tropos goal or a plan. In Fig. xx, we translated the use case Perform Transaction to a goal meaning that the use case Perform Transaction Via Online should be a plan because only a plan could be means to achieve the goal (ends) in Secure Tropos. Here, we also define two plans Keep Account Data Up To Date and Pay Money to achieve the goal as shown in Fig. 5.2.

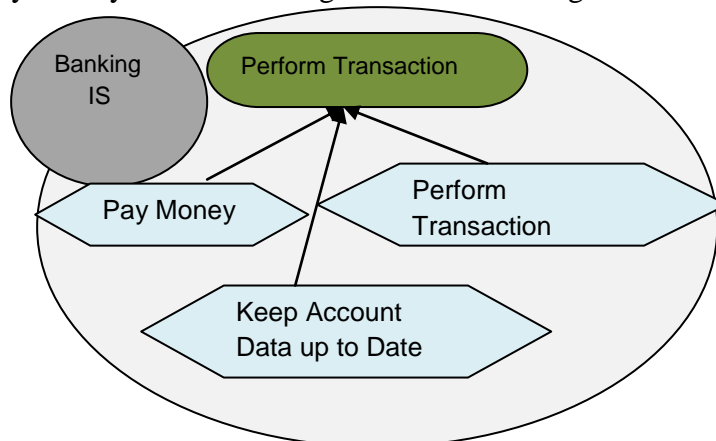


Fig. 5.2. Goal and Plan

TRMS 3. A security constraint in SROMUC is translated to a security constraint in secure tropos, moreover, a constraints of relationship is translated to restricts link in secure tropos. This rule represents the security criterion and constraints of element respectively in reference to ISSRM domain model as shown in Fig. 5.3.

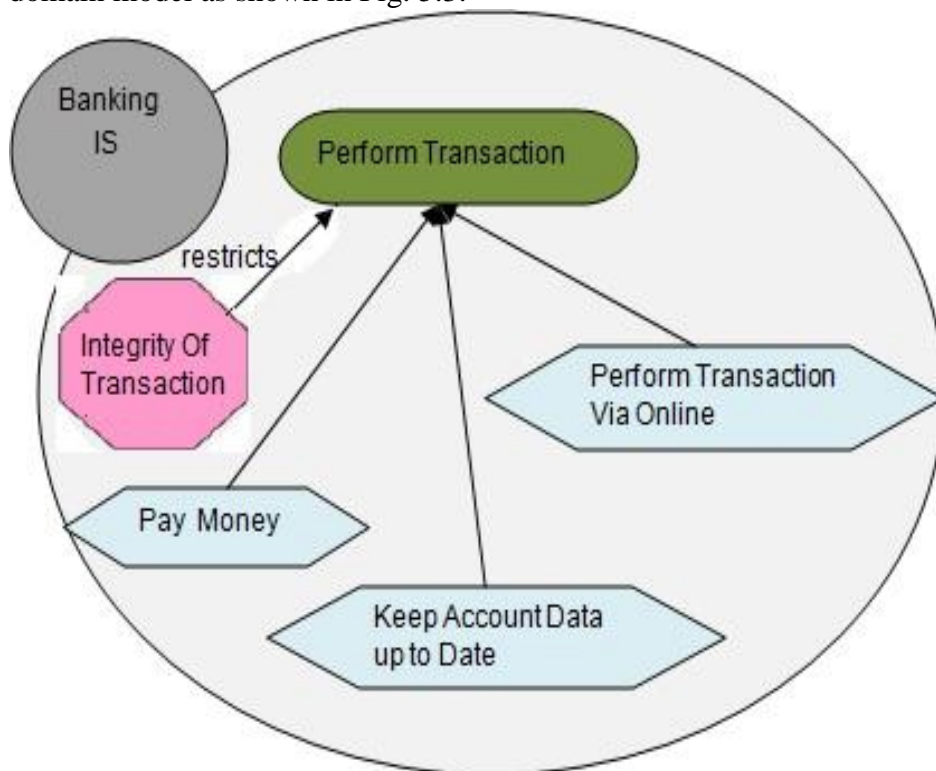


Fig. 5.3. Security Criterion

TRMS 4. An actor in SROMUC is translated to an actor in Secure tropos. Moreover, a communication relationship is translated to a dependency link in secure tropos.

In SROMUC, an actor collaborate with the system through a communication link while in secure tropos dependency link is used. In secure tropos, dependency link a depender, dependee and dependum as described here:

- If the system is depender, the communication link is translated as dependee and the developer has to specify the dependum.
- If the system is dependee, then communication link is translated as a depender and the use case (goal of the actor) becomes the dependum in secure tropos dependency.
- The security constraint on dependency links depends on the developers choice to set them manually as SROMUC does not support such thing. After applying

TRMS 4, we will get the model as shown in Fig. 5.4.

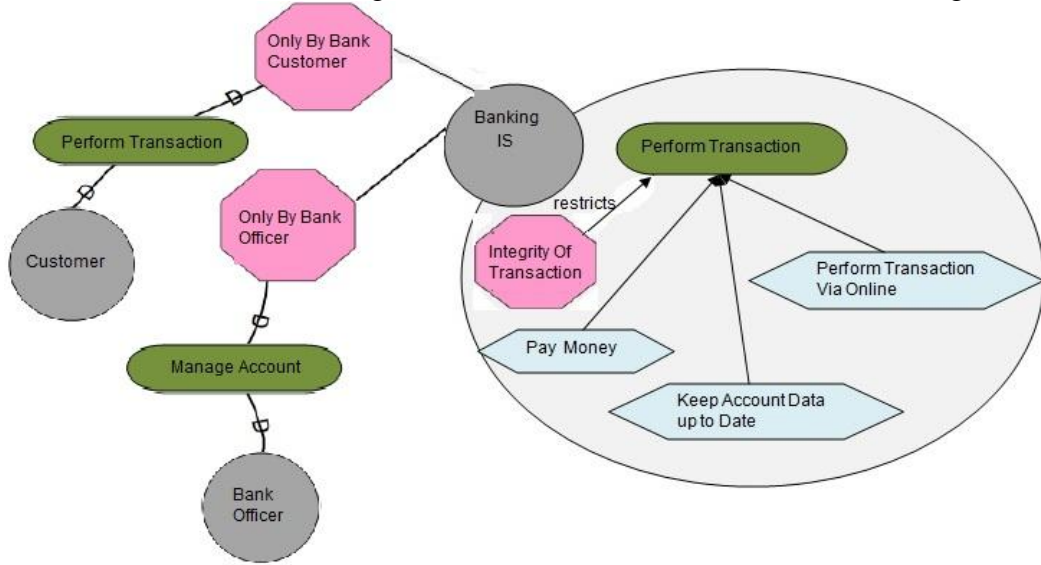


Fig. 5.4. Actor

TRMS 5: A misuser in SROMUC is translated to a threat agent (attacker) in secure tropos. Similarly, a misuse case is translated to a plan of a threat agent in secure tropos. They are linked through a communication relationship in SROMUC and means-end or decomposition link in secure tropos. It is based on the alignment of SROMUC and Secure tropos which identifies that the misuser and the Secure Tropos actor are aligned to the ISSRM threat agent. Thus in Fig. 5.5, we identify a threat agent as attacker.

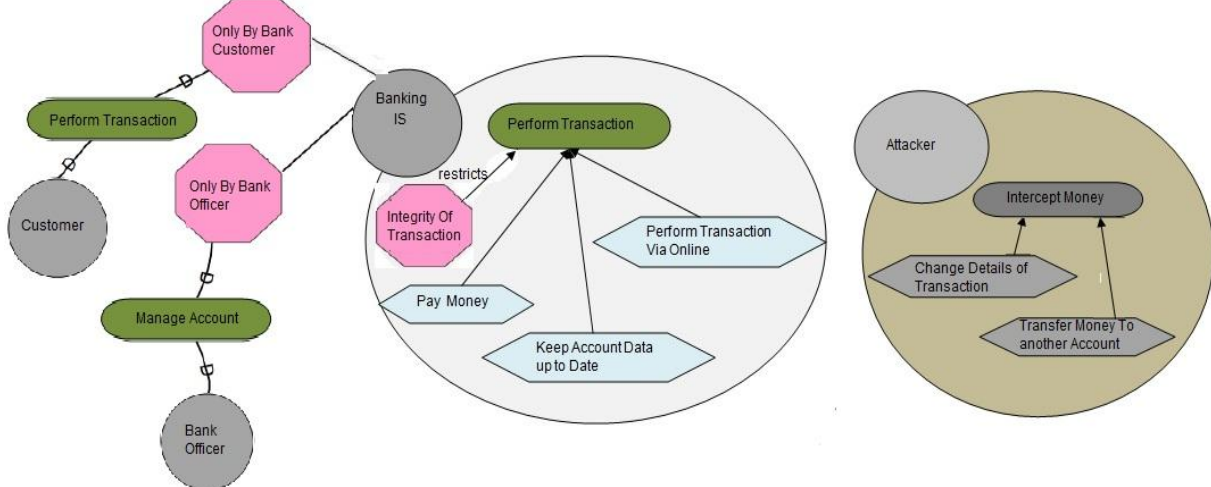


Fig. 5.5. Attacker

TRMS 6. Vulnerability in SROMUC is translated to a vulnerability point in secure tropos. Moreover, threatens and exploits relationship are translated to attacks and exploits link in secure tropos respectively. Vulnerability in SROMUC is represented as a use case and it defines the specific weakness in the system as a use case, but in secure tropos it is just represented with a black circle over a vulnerable asset, hence the developer has to apply the rule accordingly during the transformation. After applying TRMS 6, we will get the model as shown in Fig. 5.6.

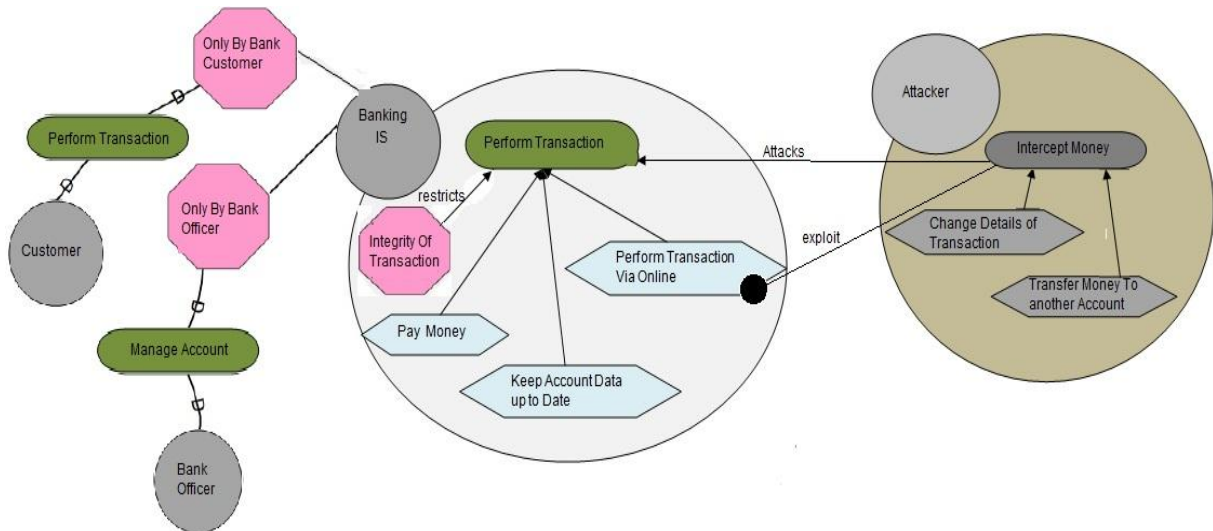


Fig. 5.6. Attacks and exploits

TRMS 7 : *Impact in SROMUC is translated to a combination of threat, impacts link and the plan. Moreover, from SROMUC, Negates, Harms and leads to relationship are translated to impacts relationship.* In SROMUC, impact has a concrete syntax, represented as a rounded rectangle where as in secure tropose, it is abstract meaning that developer has to identify the impact through the combination of impacts link and threat.

TRMS 8: *A security use case is translated to a security plan or goal in secure tropos. Similarly, a mitigates relationship is translated to a mitigates link in secure tropos.* We have translated the security use case Apply Cryptographic Procedures to a Plan as show in Fig. 5.7.

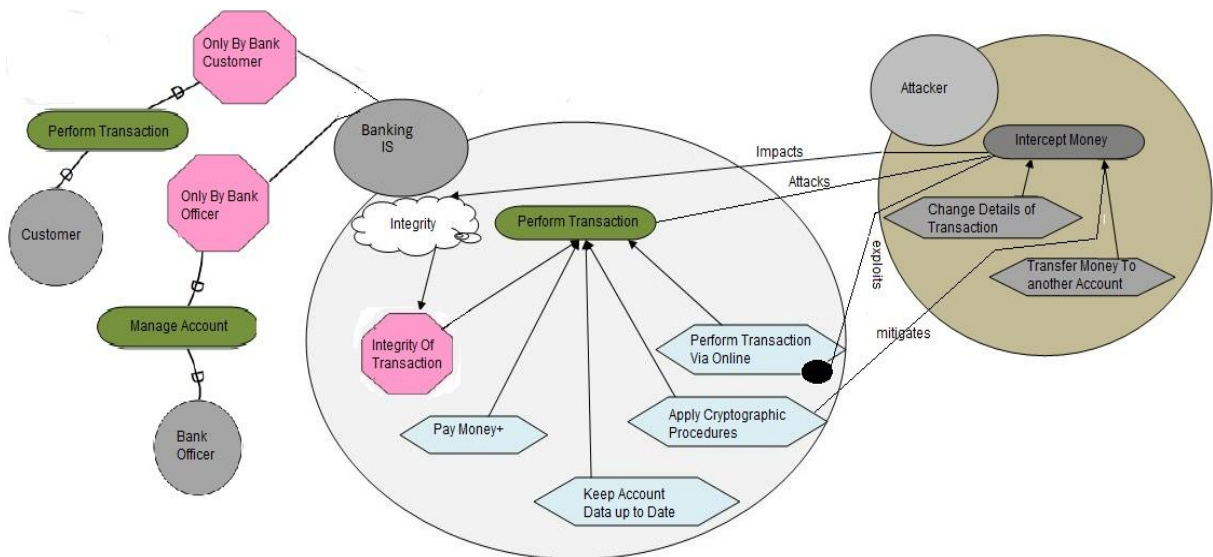


Fig. 5.7. Attacks, exploits and impact

5.2 Transformation from Secure tropos to Misuse Cases

This section defines a set of transformation rules from the Secure Tropos model to the SROMUC diagram. The transformation rules, presented in this section are based on the alignment between the ISSRM domain model. We will transform a meeting scheduler, a well-established exemplar in RE as shown in Fig.5.8, Fig. 5.9, and Fig. 5.10. It was also used in [2]. Again we apply the incremental model to transform the secure tropos model to SROMUC.

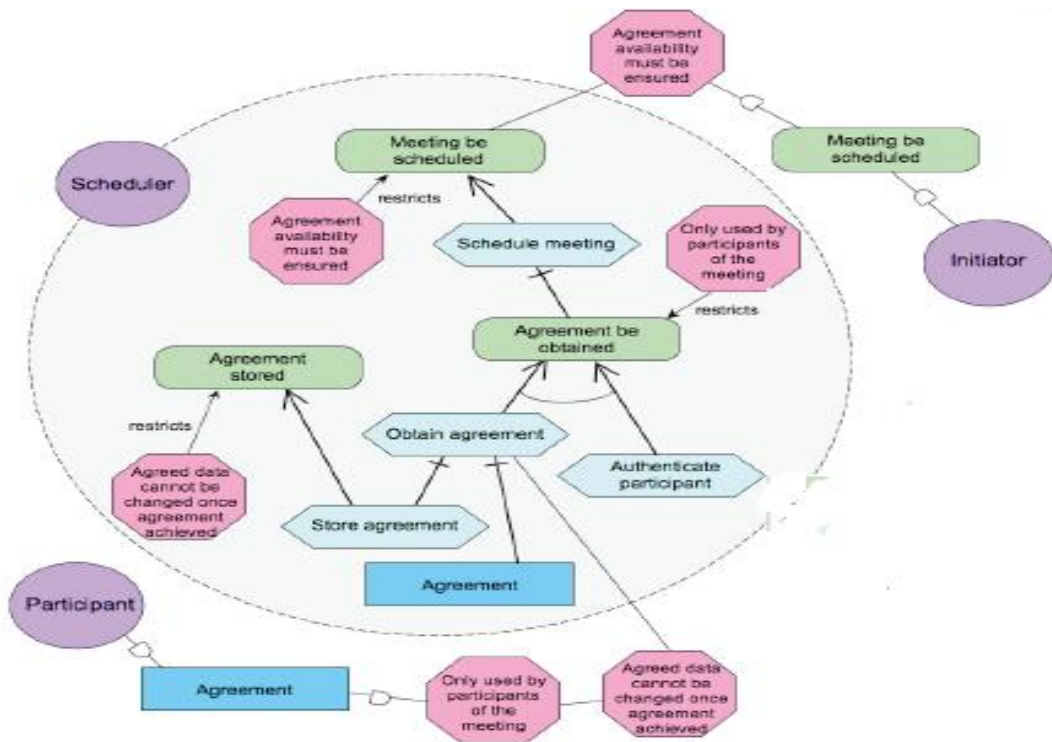


Fig. 5.8. Asset Model (Taken from [2])

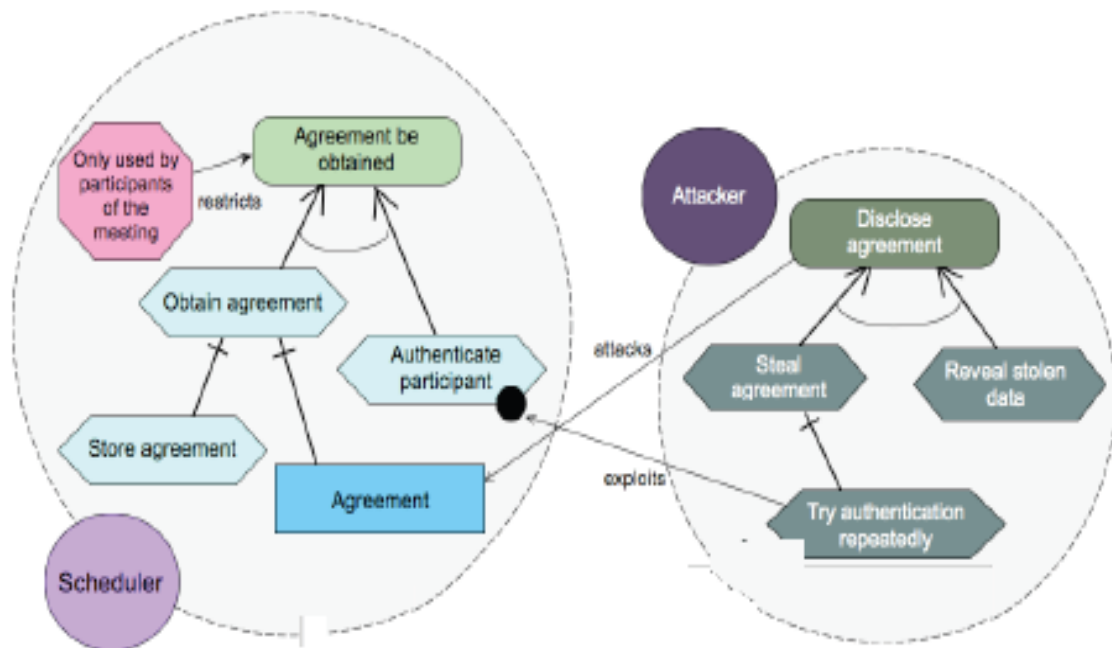


Fig. 5.9. Threat Model (Taken from [2])

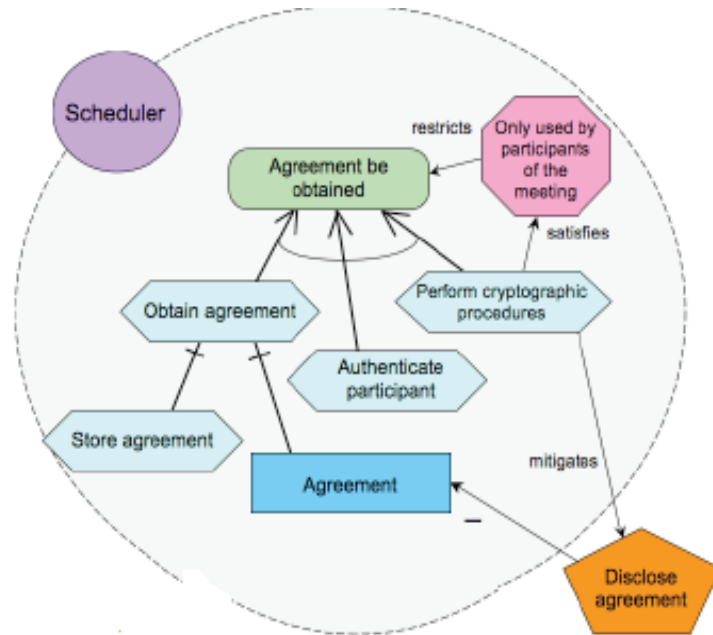


Fig. 5.10. Security Model (Taken from [2])

TRSM 1: A system actor and its boundary in secure tropos is translated to a system boundary in SROMUC. This rule is based on alignment between the Secure Tropos actor and SROMUC system boundary to the ISSRM domain model. After applying TRSM 1, we will get the following model as shown in Fig. 5.11.



Fig. 5.11. System Boundary

TRSM 2: A goal or a plan in secure tropos is translated to a use case in SROMUC. Similarly, a means-end where ends is the goal and means is the plan and decomposition link where some plan is decomposed is translated to an includes or extends relationship. After applying this rule, we will get the model as shown in Fig. 5.12

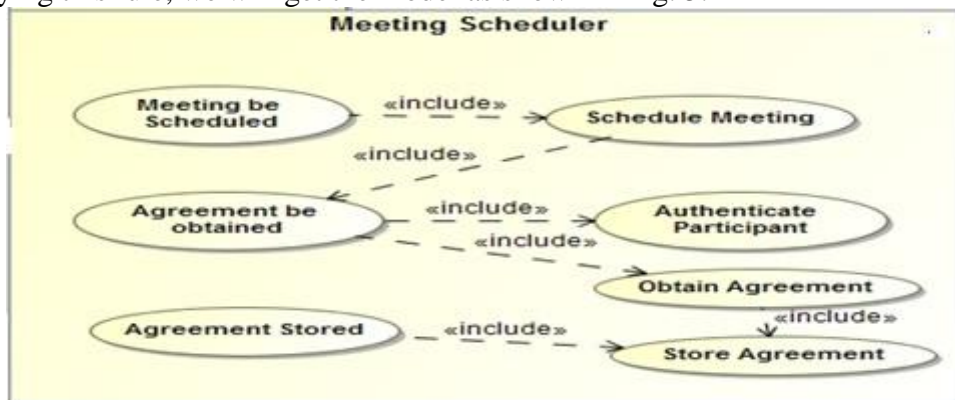


Fig. 5.12. Use cases

TRSM 3. A security constraint in secure tropos is translated to a security constraint in SROMUC, moreover, a restricts link is translated to constraints of relationship in SROMUC. This rule represents the security criterion and constraints of element respectively in reference to ISSRM domain model as shown in Fig. 5.13.

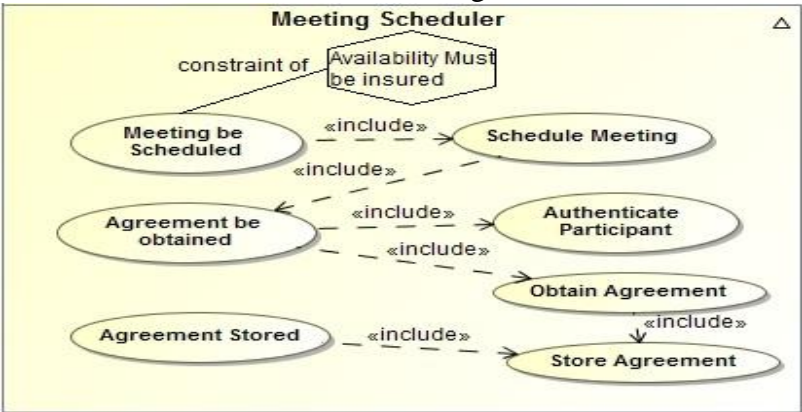


Fig. 5.13. Use cases and Security criterion

TRSM 4. An actor in secure tropos is translated to an actor in SROMUC. Moreover, a dependency link in secure tropos is translated to a communication relationship.

In secure tropos, dependency link is used for collaboration with the system. In secure tropos, dependency link a depender, dependee and dependum while in SROMUC, it is a straightforward and is translated to a communication relationship. A developer must exclude extra dependencies. After applying the TRSM 4, we will get the model as shown in Fig. 5.14.

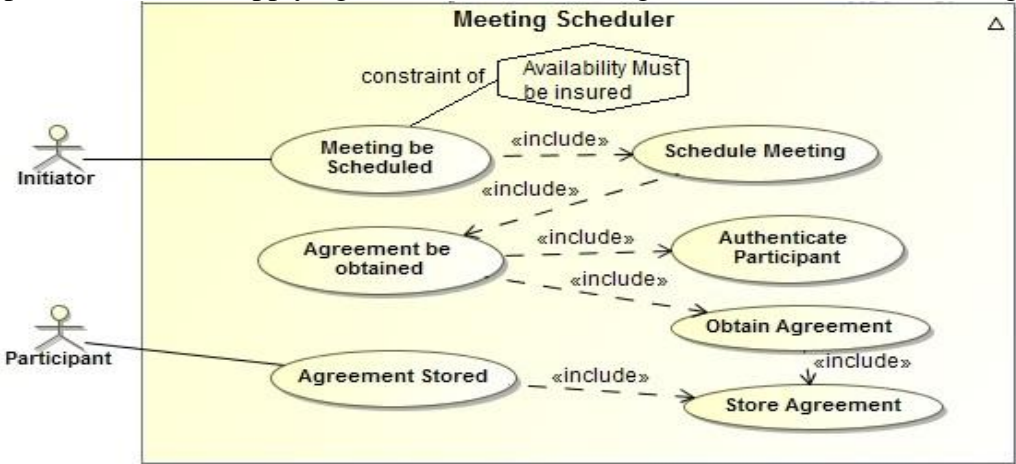


Fig. 5.14. Actor and Use cases

TRSM 5: A threat agent (attacker) in secure tropos is translated to a misuser in SROMUC. Similarly, a plan of a threat agent in secure tropos is translated to a misuse case in SROMUC. They are linked through a means-end or decomposition link in secure tropos and a communication relationship in SROMUC. It is based on the alignment of SROMUC and Secure tropos which identifies that the misuser and the secure tropos actor are aligned to the ISSRM threat agent as show in Fig. 5.15.

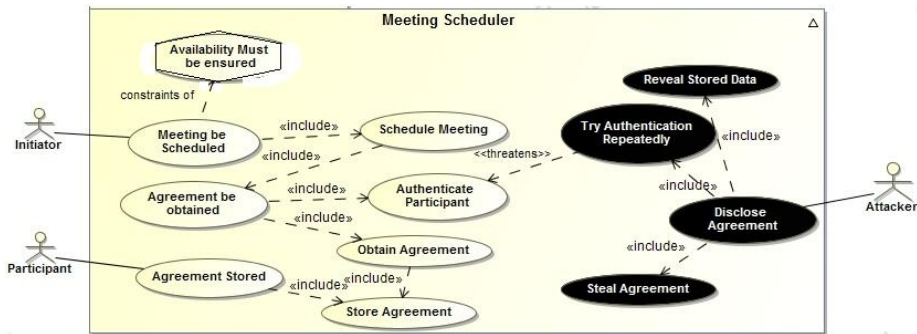


Fig. 5.15. Misuser and Misuse Cases

TRSM 6. Vulnerability point in secure tropos is translated to vulnerability in SROMUC. Moreover, attacks and exploits links are translated to a threatens and exploits relationship in SROMUC respectively. Vulnerability point in secure tropos is represented as a black circle over a plan but in SROMUC it define the specific weakness in the system as a use case, hence the developer has to apply the rule accordingly during the transformation. After applying TRMS 6, we will get the model as shown in Fig. 5.16.

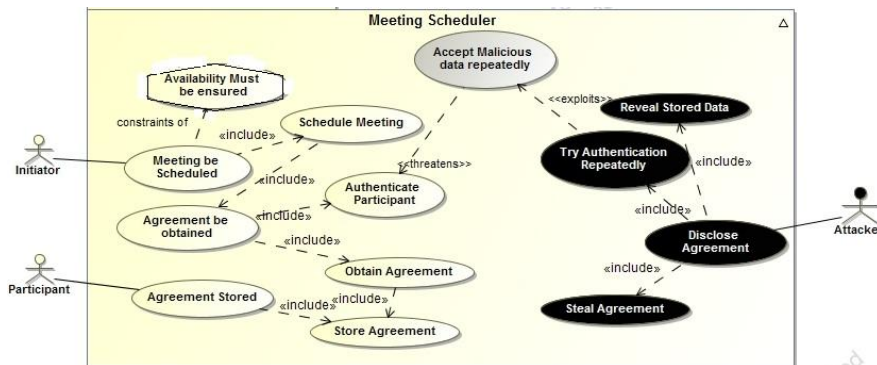


Fig. 5.16. Vulnerability

TRSM 7 : A combination of threat, impacts link and the plan is translated to an impact in SROMUC. Moreover, impacts relationship in secure tropos is translated to a negates, harms and leads to relationship in SROMUC. In SROMUC, impact has a concrete syntax, represented as a rounded rectangle where as in secure tropose, it is abstract meaning that developer has to identify the impact through the combination of impacts link and threat as shown in Fig. 5.17.

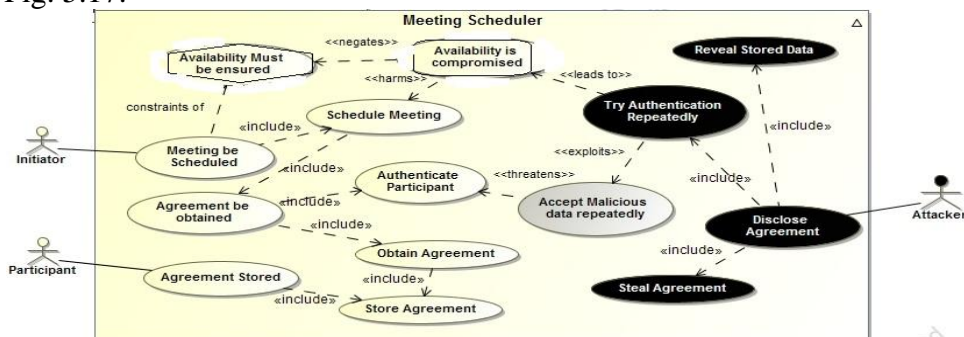


Fig. 5.17. Impact

TRMS 8: A security plan or goal is translated to a security use case in SRUMUC. Similarly, a mitigates link is translated to a mitigates relationship in secure tropos. We have translated the security plan *Apply Cryptographic Procedures* to a security use case as show in Fig 5.18.

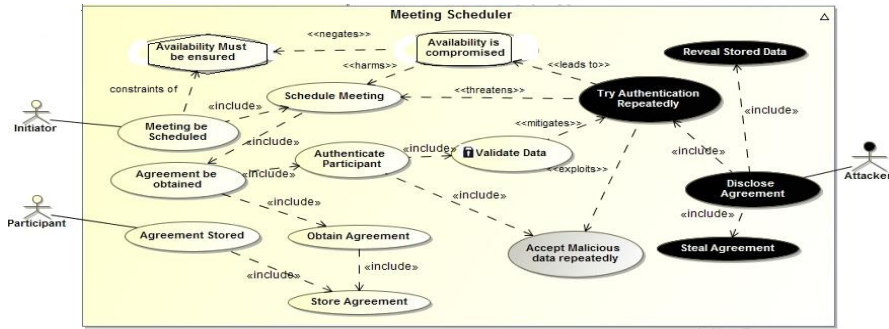


Fig. 5.18. Security Use Case

5.3 Summary

In this chapter, we tried to eliminate the gap between secure tropos and SROMUC by providing the translation between the two languages. We develop the transformation rules from secure tropos to SROMUC and from SROMUC to secure tropos. We applied the incremental model to apply the rules from one language to another. The translated models provide the information for tackling the security risk management from different perspective. The translation can be applied to existing system and to the new systems in IS development process.

PART IV
Validation

Chapter 6

Comprehensibility of SROMUC

In this chapter, we examine and measure the comprehensibility of SROMUC. Firstly, we define the approach to measure the comprehensibility of SROMUC and what we expect to receive as the results. Secondly, we ask the practitioners to answer a questionnaire (see appendix A) in order to measure the comprehensibility of SROMUC. Finally, we report how we carried out the study and summarize the results.

6.1 Participant Selection

In order to measure the comprehensibility of SROMUC, we contacted 50 software/IS practitioners including software analysts, business analysts, software engineers and architects. The participants were selected from different companies from all over the world in order to confirm how the different roles perceive SROMUC. All the participant were working in IS development industries which resulted in getting different evaluation.

6.2 Survey for Measuring Comprehensibility of SROMUC

We prepared a questionnaire (see appendix A) addressing the comprehensibility of the SROMUC and gathered responses from the participants. This provided us a closer feedback and allowed us to ask additional information when the answers were vague or shallow.

Firstly, we briefly introduced the concept of ISSRM and SROMUC and their alignment to the participants; we introduced the construct of SROMUC in reference to ISSRM domain model. Then we explained the concept by modelling the diagram using SROMUC for online banking IS. The survey results were analyzed based on correctly identifying the SROMUC construct and the concept defined in ISSRM domain model. After the survey, we categorized the participants into business analysts, software analysts and architects and software developers and requested them to answer the short questions. We were interested in the following aspects

- How comprehensible and easy the SROMUC is.
- How much satisfied are you with the alignment of SROMUC to ISSRM domain model.
- Does it help to measure the security risk using SROMUC.

6.3 Results

Each of the participants was asked to give the feedback for the comprehensibility of SROMUC by identifying the construct of SROMUC in terms of concepts defined in ISSRM domain model. Table 6.1 presents the questions from questionnaire and summarizes the survey results. We present the questions in column one, column two represents the total number of participant while column three represent the number of participants who responded to questions. Column four represents the total number of satisfied answers for each question and column five presents the total number of unsatisfied answers for each question. Last column provide the percentage of satisfied answers for each question. To calculate the percentage, we used

$$(\text{total number of participants responded} / \text{total number of satisfied answers}) * 100$$

For the comprehensibility, satisfaction and easiness of SROMUC, we requested the practitioners to rate the questions given in Table 6.2 based on the scale from 1 (lowest) to 5 (highest). We categorised the practitioners into business analyst, software analyst, software security analysts and software developers in order to perceive the results from different perspective. The results are shown in Table 6.2. In Table 6.2, column one represent the

questions, column two, three, four and five represents the answers from business analysts, software analyst, software security analysts and software developers respectively. The results presented are the average results given by each group of participants. For example, we asked 10 business analyst to rate all the questions presented in column one of Table 6.2, 08 of the rate the question 1 4 or above and question 2 and 3 as 3 or above.

How comprehensible and easy SROMUC is? All the participants consider the SROMUC comprehensible and easy to learn. People understood the application of ISSRM and SROMUC. They implied that the construct are vivid and easy to remember.

How satisfied are you with the alignment of SROMUC to ISSRM? This question turned out to be the hardest to answer. The participants had never used ISSRM for security risk management; it was new experience for them. While the participants did not say that they are satisfied or not with the alignment but they were also reluctant to confirm that it met their expectations.

Does it help to measure the security risk using SROMUC? All respondents understood clearly the benefits of the SROMUC – A security risk management using a modelling language. Majority of the participants agreed that the security risk management is rather easy to understand using SROMUC.

Table 6.1 Survey Results

Questions	Total No. Of Participants	Total No of Participants Responded	Total No. of Satisfied Answers	Total No. of Unsatisfied Answers	% of Satisfaction
Q1. Can you identify the "Business Asset" in figure 1?	50	41	38	3	92.68
Q2. Can you identify the "IS Asset" in figure 1?	50	41	37	4	90.24
Q3. Which of the following is represented as "Attack Method" in figure 1?	50	41	35	6	85.36
Q4. Which of the following represents a "Vulnerability" in figure 1?	50	41	36	5	87.80
Q5. Which of the following represents a "Security Criterion" in figure 1?	50	41	31	10	75.60
Q6. Which of the following represent the "Security Requirement" in figure 1?	50	41	36	5	87.80
Q7. Which of the following represent an "Impact" in figure 1?	50	41	33	8	80.48
Q8. Can you identify a "Threat Agent" in figure 1?	50	41	40	1	97.56
Q9. Which of the following represent a "Risk" in figure 1?	50	41	30	11	73.17
Q10. Which of the following represent a "Threat" in figure 1?	50	41	34	7	82.92
Q11. Which of the following represent an "Event" in figure 1?	50	41	32	9	78.04
Q12. Which of the following represent a "Risk Treatment" in figure 1?	50	41	33	8	80.48
Q13. Which of the following represent a "Control" in figure 1?	50	41	23	18	56.09

Table 6.2 Comprehensibility of SROMUC

Questions	Business Analysts	Software Analysts	Software Security Analysts	Software Developers
Comprehensible and easiness of SROMUC	4	5	4	4
Satisfaction of alignment of SROMUC and ISSRM	3	4	5	4
Measuring security risk using SROMUC	3	3	4	3

6.4 Threat to Validity

The ideal approach to measure the comprehensibility and validity may not be possible as every approach has its limitations depending on the context it is used in. Possible limitations of our approach are:

- The participants who were unable to answer correctly may not have gone through the guidelines to understand SROMUC and ISSRM. Thus, the answer from them may be based on their random choice.
- Repeatedly answering the questions may lead to bias and unrealistic results.

6.5 Summary

In order to measure the comprehensibility and validate our proposed alignment, we used a survey questionnaire to measure the comprehensibility and validity of our work. Then we summarised the results of the survey and identified the threats to the validity of our proposal. We acknowledge the industrial level case study to validate the correctness and comprehensibility of SROMUC.

PART V
CONCLUSIONS AND FUTURE WORK

Chapter 7

Discussion, Conclusion and Future Work

In this chapter, we provide the related work, discussion regarding the research done in this thesis and we will conclude our proposal and identify the paths for the future work.

7.1 Related Work

The ISSRM domain model not only cover the identification and specification of risks but also support the risk management process that focuses on whole IS, instead of defining security requirements for one or more IS components. It is applicable during the IS development while other approaches are mainly apply on an existing IS, but not applicable during the IS development. Although few can be used during the development by implementing the additional guidelines, however, they still lack the Requirement Engineering (RE) activities and wouldn't able to reason for security requirements from the early analysis. In CORAS method, the activities proposed a formal artefact but it is neither connected to RE activities nor applicable to the IS development and is disconnected from the standard terminology. ISSRM domain model integrate the risk management tasks throughout all the stages of IS development. Hence, the risk management tasks and IS development go parallel. Herrmann *et al.* [14] present a Risk-based Security Requirement, Elicitation and Prioritization (RiskREP) method for managing IT security risks. It defines a set of security requirements, which outline how security as the quality goal can be achieved. It performs Business-IT-alignment and prioritizes the IT requirement. Similarly, ISSRM align these concepts by supporting 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.

There has been several work carried out on misuse cases and its extension. McDermott and Fox proposed abuse cases. They explored how threats and counter-measures could be modelled using standard UML use case but keeping abuse cases in separate model. Abuse case focuses on security requirements where as our approach is aligned with ISSRM and focuses on the overall security risk management. It identifies the vulnerability and threats, and analyses the potential risk and its impact. Therefore, the elicited security requirements are aligned with the functional requirements of system. Alexander [3] used the notion of how security use cases can be threatened by other misuse cases. The SROMUC is based on the ISSRM process where the activities are iterative that identifies the risk associated with the security use case and helps to counter measures. Matulevicius *et al.* [17] has also aligned misuse cases with ISSRM but their work is not completely aligned with the security risk management strategies. However, our proposal is the extension of the work done by Matulevicius *et al.* [17] and provides the modelling support for overall security risk management strategy of an organization at early development stage.

7.2 Limitations

Like any other research work, this research has few limitations. Firstly, our work is based on the theoretical description; hence it contains a certain level of subjectivity. Also our work is focused on the comprehensibility; hence the correctness and effectiveness remains a question. The research work is based on specific banking IS scenario which may mean that some aspects of SROMUC and its application can be interpreted differently, if performed by other researchers in reference to ISSRM domain model. Secondly, we have decided to reduce the risk by implementing certain security requirements but the security requirement could be different if decision of risk avoidance is taken.

7.2 Conclusion

We presented and analyzed different security risk management frameworks and methods such as EBIOS, OCTAVE, SQUARE etc, and discussed the ISSRM domain model for security risk management. We decided to use ISSRM domain model for the alignment of SROMUC because of its coverage for security risk management and focus on IS development. Also ISSRM domain model is compliant with existing security risk management methods and covers most important aspect for security risk management. Another reason for choosing ISSRM domain model is that it is already used for the alignment of misuse cases by Matulevičius et al [17]. We analyzed the concepts and constructs of different security modelling languages (e.g., Misuse case diagrams, Secure Tropos diagrams). This analysis helped to understand the concept, constructs and usage of these languages. After the analysis, we have resulted in a SROMUC for security risk management at requirement elicitation and analysis stage. In our analysis, we investigated that SROMUC can be used for security risk management as it identifies and provides the construct for assets, risk and event and security requirement in reference to ISSRM domain model. Investigation of existing language alignments helped us to understand and analyze the modelling language at requirement elicitation and analysis stage.

After analysing the security modelling languages, we decided to align misuse case diagrams to ISSRM domain model because of the need of security risk management at early stage and misuse cases can be used to elicit security requirement at requirement elicitation and analysis stage. We have used existing alignment of misuse cases by Matulevičius et al [17]. We identified the limitations in existing alignment and extend the language syntax and semantics in order to respect the guidelines of ISSRM domain model by introducing new visual constructs and illustrate it with an online banking IS. The proposed SROMUC strengthens existing misuse cases by extending the graphical representation of misuse cases and its semantics. The graphical extension proposed are not intuitive but they express the security concerns in reference to ISSRM domain model for risk analysis. The idea is to make it easily understandable and to comply it with the original definition of use cases. We differentiate the construct for impact and security criterion from the standard UML use case constructs. Security use case construct has been enhanced to differentiate security requirement from the functional requirements. In Table 4.4, 4.5 and 4.6, we present the coverage of SROMUC with respect to ISSRM domain model. Since, ISSRM domain model is used for the alignment of SROMUC and Secure Tropos, we also presented the translation rules between SROMUC and Secure Tropos for the interpretability of both the languages in reference to ISSRM domain model.

To validate our work, we have measure the comprehensibility of SROMUC, we conducted a survey and include the results in the report and we identify the threats to the validity.

7.3 Future work

We have applied our proposal to the running online banking IS example. However, we acknowledge more practice-oriented case study is necessary for the quality and correctness of SROMUC with regards to security risk management. The scope of this work is limited to the graphical representation of SROMUC but the alignment and extension of textual template of MUC with ISSRM domain model can be treated as a future work in this context. Our focus was on the comprehensibility of SROMUC, hence the correctness and effectiveness will remain the subject for future work. We have provided the transformation with secure tropos for interoperability but it also opens the doors for interoperability with other security modelling languages.

Bibliography

1. Ahmed, N., Matulevičius, R., Mouatidis., H.: A Model Transformation from Misuse Cases to Secure Tropos, The accepted papers will be included in the special proceedings issue titled “CAiSE Forum”, which will be formally published by CEUR, 2002.
2. Ahmed, N., Matulevičius, R.: Towards Transformation guidelines from Secure Tropos to Misuse Cases (Position Paper).
3. Alexander, I.: Misuse Cases: Use Cases with Hostile Intent. IEEE Software, Pages 58-66,203.
4. Alberts C.J., Dorofee A.J.: OCTAVE Method implementation Guide Versoin 2.0. Carnegie Mellon University – Software Engineering Institute, Pennsylvania, (2001).
5. Braber, F., Hogganvik, I., Lund, M.S., Stølen, K., Vraalsen, F.: Model-based security analysis in seven steps — a guided tour to the coras method. BT Technology Journal 25, 101–117 (2007).
6. Bresciani B., Perini A., Giorgini P., Fausto G. and Mylopoulos J., “*TROPOS: an Agent oriented Software Development Methodology*”. Journal of Autonomous Agents and Multi-Agent Systems, Volume 25, pages 203–236, 2004.
7. Chowdhury, M.J.M.: Modelling Security Risks at the System Design Stage: Alignment of Mal-Activity Diagrams and SecureUML to the ISSRM Domain Model. Master theses (2011), <http://nordsecmob.tkk.fi/thesis.html>.
8. Chowdhury, M.J.M., Matulevicius R., Sindre G., and Karpati P., Aligning Mal-activity Diagram and Security Risk Management for Security Requirements Definations, University of Tartu, Estonia, Norwegian University of Science and Technology, Norway.
9. Chowdhury, M.J.M., Matulevičius R., Sindre G., Karpati P., “ Modeling Security Risks at the System Design Stage ”,Master’s thesis, June, 2011.
10. Dubois E., Heymans P., Mayer N. and Matulevičius R., “*A Systematic Approach to Define the Domain of Information System Security Risk Management*”. Book published from Springer-Verlag, ISBN: 978-3-642-12543-0 ,2010.
11. Ekelhart, A., Fenz, S., Neubauer, T.: Aurum: A framework for information security risk management. In: HICSS-42. pp. 1–10. IEEE Computer Society (2009).
12. Firesmith., D.: Security use cases. Journal of Object Technology, 2(3):53–64, 2003.
13. Firesmith., D.: G., “*Common Concepts Underlying Safety, Security, and Survivability Engineering*”. Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute, Pittsburgh, Pennsylvania, December 2003.
14. Herrmann, A., Morali, A., Etalle, S., Wieringa, R.J.: Risk rep: Risk-based security requirements elicitation and prioritization. In: Perspectives in BIR. pp.155–162 (2011).
15. Hoo K. J. S., “How Much Is Enough? A Risk-Management Approach to Computer Security”. Working Paper, Consortium for Research on Information Security and Policy (CRISP), June 2000.
16. Lee S. W., Gandhi R., Muthurajan D., Yavagal D. and Ahn G. J., “Building problem domain ontology from security requirements in regulatory documents”. In proceeding of the International Workshop on Software Engineering for Secure Systems, 2006.
17. Matulevičius, R., Mayer, N., Heymans, P.: Alignment of Misuse Cases with Security Risk Management. In: Proceedings of ARES. pp. 1397-1404. IEEE (2008).
18. Mayer, N.: Model-based Management of Information System Security Risk. Ph.D. thesis (2009).
19. Mayer, N. Heymans, P., and Matulevičius, R.: Design of a Modelling Language for Information System Security Risk Management. Technical report, CRP Henri Tudor and University of Namur, 2006.
20. Mayer, N. Dubois, E., Matulevicius R., Heymans P., “Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems.

21. Mouratidis H. and Giorgini P. Secure Tropos: A Security-oriented Extension of the Tropos Methodology. *International Journal of Software Engineering and Knowledge Engineering (IJSEKE)*, 17(2):285-309, 2007.
22. Mitnick Kevin. "The Art of Deception: Controlling the Human Element of Security". Wiley Publishing, Inc., Indianapolis, 2002.
23. Mean NR, Hough ED, Stehney TR (2005) Security Quality Requirements Engineering (SQUARE) methodology. Technical report CMU/SEI-2005-TR-009, ESC-TR-2005-009 Carnegie Mellon University – Software Engineering Institute, Pittsburgh, PA. Development", ISBN: 978-3-540-69533-2,2008.
24. Nancy R. Mead, Eric D. Hough, Theodore R. Stehney II, Security Quality requirements Engineering ,CMU/SEI-2005-TR-009-ESC-TR-2005-009,2005.
25. Pauli., J. and Xu., D.: Trade-off Analysis of Misuse Case based Secure Software Architectures: A Case Study. In Proceedings of the 3rd International Workshop on Modeling,Simulation, Verification and Validation of Enterprise Information System (MSVVEIS'05), pages 89–95. INSTICC Press, 2005.
26. Røstad., L.: An extended misuse case notation: Including vulnerabilities and the insider threat," Proc. 12th Working Conf. Requirements Eng.: Foundation for Software Quality (Refsq), Essener Informatik Beiträge, 2006.
27. Sindre, G., Opdahl, A.L.: Templates for misuse case description. In Seventh International Workshop on Requirements Engineering: Foundation of Software Quality (REFS'2001), Interlaken, Switzerland, 2001.
28. Sindre G.: and Opdahl A. L.: Eliciting Security Requirements with Misuse Cases. *Requirements Engineering journal*, 2005.
29. Silver B.: BPMN Method and Style: A level-based methodology for BPMN Process Modelling and improvement using BPMN 2.0, Cody-Cassidy Press, (2009).
30. Turban E., Volonino L., McLean E. and McLean J., "*Information Technology for Management: Transforming Organisations in the Digital Economy*". The seventh International student edition, 2010. ISBN: 978-0-470-40032-6.
31. Van Lamsweerde, A.: Elaborating Security Requirements by Construction of Intentional Anti-Models. In: ICSE 2004, UK. pp. 148-157. IEEE (2004).
32. DCSSI (2004) EBIOS – Expression of needs and identification of security objectives. <http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html> Last Accessed April 23, 2012.
33. CLUSIF (2007) MEHARI 2007: Concept and Mechanisms. <http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-risk-management.pdf>. Last accessed April 23, 2012.
34. Insight Consulting. CRAMM (CCTA Risk Analysis and Management Method) *User Guide Version 5.0*. SIEMENS, 2003.
35. ISO/IEC Guide Risk management Vocabulary Guidelines for use in standards International Organization for Standardization, Geneva, 2002.

Abstract Eesti

Viimine väärkasutamine juhtudel ISSRM

Inam Soomro
Magistritöö

Digitaalse ja sotsiaalse elu vaheline piirjoon on hägunemas ning informatsiooni süsteemide turvalisuse ja informatsiooni per se turvalisus tekitab muret. Samuti pälvib tähelepanu süsteemide turvalisuse arendamine ja säilitamine. Olemasolevad uurimused viitavad mitmetele juhtumitele, kus turvalisuse aspekti võeti arvesse ainult süsteemi väljatöötamise protsessi lõpus, jättes välja süstemaatilise turvalisuse analüüsi süsteemi ja tarkvara nõuete ja kavandamise etappidel.

Misuse case diagrams on üks võimalikke viise seostada turvalisuse analüüsi ja süsteemi funktsionaalsete nõuete definitsiooni. Nende peamine eesmärk on negatiivsete stsenaariumite modeleerimine, seoses defineeritud süsteemi funktsionaalsete nõuete esilekutsumise ja analüüsiga. Hoolimata sellest eelisest on väärkasutatud juhtumid üsna ebatäpsed; nad ei täida riskianalüüsi organiseerimise strateegiaid, ja seega võivad viia valetõlgendamiseni turvalisusega seotud konseptsioonides. Sellised limitatsioonid võivad potentsiaalselt viia puudulike lahendusteni turvalisuse alal. Sageli tuleb organisatsioonidel leida enda turvalisuse lahendused, et kaitsta oma ressursse ja varasid.

Käesolevas töös rakendame süstemaatilist lähenemist, et mõista kuidas *Misuse case diagrams* aitavad organiseerida ettevõtete varasid, potentsiaalseid süsteemiriske ja turvalisuse nõudeid, et leevendada riske.

Täpsemalt ühtlustame *Misuse case* konstruktsiooni domeeni mudeli kontseptiga, informatsiooni süsteemi turvalisusriski haldamiseks (Information Systems Security Risk Management; ISSRM). Lisaks, põhinedes ISSRM ja keelelisele ühtlustamisele, uurime ja arendame reeglid, et tõlkida *Misuse case diagrams* Secure Tropos mudelile.

Käesoleva uurimuse panusel on mitmeid eeliseid. Esmalt aitab potentsiaalselt mõista, kuidas *Misuse case* turvalisuse riski haldamisega tegeleb. Teiseks määratleb meetodi, mis toetab turvalisuse nõuete põhjendamist arendatud süsteemi kehtestamisel ja rakendamisel. Viimaseks, Secure Troposi transformeerumine aitab potentsiaalselt arendajatel (ja teistel süsteemi vahendajatel) mõista miks turvalisuse lahendused on olulised ning millised on erinevate huvigruppide kompromissid.

Plaanime kinnitada saadud tulemused, kus mudeli kvaliteet seoses selle arusaadavusega on mõõdetud *Misuse case diagram* jaoks.

Usume, et selline *Misuse case* seadistamine koos ISSRM ja *Misuse case diagram* transformeerumine eesmärgile orienteeritud modelleerumisele, on kasulik süsteemi ja tarkvara arendajatele.

Esmalt aitab mõista turvalisusega seotud probleeme varajastes arendamise staadiumites. Teiseks aitab vaadata probleemi erinevatest vaatenurkadest, mõistes erinevaid turvalisuse arendamise perspektiive.

Appendix A Online Survey

<https://docs.google.com/spreadsheets/embeddedform?formkey=dGI2MWF5X1RtTXJwNzN0QVNkOU15NHc6MQ>

In Appendix A, we present the online questionnaire conducted for measuring the comprehensibility of SROMUC which was sent to IS practitioners. Questionnaire was given as a multiple choice questions from where participant had to identify the correct answer.

Survey for measuring the comprehensibility of Security Risk-oriented Misuse Cases (SROMUC)

This Survey is part of my research work based on the security of the Information System during requirement elicitation and analysis stage using a modeling language called Mis(use Cases).

A Model for survey questions (i.e., Figure 1) is attached in the word document. In Figure 1, an example of SROMUC diagram for online banking information system is modeled.

After analyzing the Figure 1, please answer the following questions.

If the information given in the document is not sufficient, you may want to go through my research paper for details in following link <http://www.inf.unibz.it/sbp12/papers/P5-Soomro.pdf>

* Required

Q1. Can you identify the "Business Asset" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- Availability of Service
- Perform Transaction via Online
- Perform Transaction
- Keep Account Data up to Date
- Make Online Service Unavailable
- Availability of Service is Compromised
- Other:

Q2. Can you identify the "IS Asset" in figure 1? *

*Refer to figure 1 and Table 1 in attached document sent to you in email

- Availability of Service
- Perform Transaction via Online
- Perform Transaction
- Availability of Service is Compromised
- Make Online Service Unavailable
- Keep Account Data up to Date
- Other:

Q3. Which of the following is represented as "Attack Method" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- Pay Money
- Make Online Service Unavailable
- Initiate Half Opened Connections to server
- Availability of service
- Install IP Filtering
- None of the above
- Other:

Q4. Which of the following represents a "Vulnerability" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- Allows Unlimited Number of Connections
- Keep Account Data up to Date
- Make Online Service Unavailable
- Availability of Service is Compromised
- Install IP Filtering
- None of the above
- Other:

Q5. Which of the following represents a "Security Criterion" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- Availability Of Service
- Install IP Filtering
- Make Online Service Unavailable
- Availability of Service is Compromised
- Keep Account Data up to date
- None of the above
- Other:

Q6. Which of the following represent the "Security Requirement" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- Install IP Filtering
- Availability of service
- Availability of service is compromised
- Make online service unavailable
- Allows unlimited number of connections
- None of the above
- Other:

Q7. Which of the following represent an "Impact" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- Allows Unlimited Number of Connections
- Keep Account Data up to Date
- Make Online Service Unavailable
- Availability of Service is Compromised
- Install IP Filtering
- None of the above
- Other:

Q8. Can you identify a "Threat Agent" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- Bank Customer
- Bank Officer
- Attacker
- Install IP Filtering
- First, Second and Third Option
- First and Second Option
- None of the Above
- Other:

Q9. Which of the following represent a "Risk" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- Allows Unlimited Number of Connections
- A combination of misuser, threat, vulnerability, Impact and Asset.
- A combination of misuser and threat
- A combination of impact and security criterion
- Make Online Service Unavailable
- None of the Above
- Other:

Q10. Which of the following represent a "Threat" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- A combination of misuser and misuse case
- A combination of misuser, threat, vulnerability and Impact.
- A combination of impact and security criterion
- Make Online Service Unavailable
- All of the Above
- None of the Above
- Other:

Q11. Which of the following represent an "Event" in figure 1? *

*Hint *Refer to figure 1 and Table 1 in attached document sent to you in email*

- A combination of misuser and misuse case
- A combination of misuser, threat, vulnerability and Asset.
- A combination of impact and security criterion
- Make Online Service Unavailable
- All of the Above
- None of the Above
- Other:

Q12. Which of the following represent a "Risk Treatment" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- Make Online Service Unavailable
- A combination of misuser and misuse case
- A combination of impact and security criterion
- A combination of misuser, threat, vulnerability and Asset.
- All of the Above
- None of the Above
- Other:

Q13. Which of the following represent a "Control" in figure 1? *

Hint *Refer to figure 1 and Table 1 in attached document sent to you in email

- A combination of misuser, threat, vulnerability and Asset
- A combination of misuser and misuse case
- A combination of impact and security criterion
- A combination of impact and security criterion
- All of the Above
- None of the Above
- Other:

Thank You For Your Precious Time - I would appreciate your comments and Feedback for the improvement of my research work.

Appendix B – Online Questionnaire Results

We present the online questionnaire results in Appendix B in the raw format. The survey questions are listed in the first column and the following columns contain the answers of the participants.

<https://docs.google.com/spreadsheets/cc?key=0AvJILwDOMIo5dGI2MWF5X1RtTXJwNzNOQVNkOU15NHc&pli=1#gid=0>

	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Q1. Can you identify the "Business Asset" in figure 1?	Q2. Can you identify the "TS Asset" in figure 1?	Q3. Which of the following is represented as "Attack Method" in figure 1?	Q4. Which of the following represents a "Vulnerability" in figure 1?	Q5. Which of the following represents a "Security Criterion" in figure 1?	Q6. Which of the following represent the "Security Requirement" in figure 1?	Q7. Which of the following represent an "Impact" in figure 1?	Q8. Can you identify a "Threat Agent" in figure 1?	Q9. Which of the following represent a "Risk" in figure 1?	Q10. Which of the following represent a "Threat" in figure 1?	Q11. Which of the following represent an "Event" in figure 1?	Q12. Which of the following represent a "Risk Treatment" in figure 1?	Q13. Which of the following represent a "Control" in figure 1?	Thank You For Your Precious Time - I would appreciate your comments and Feedback for the improvement of my research work.
4	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	A combination of misuser, threat, vulnerability, misuse case	A combination of misuser, threat, vulnerability and Asset	None of the Above	None of the Above	Good Work
5														I have my general comment about the uselessness of usecases without scenarios here. Usecase diagram are a medium for economists. They neither help the developer nor the requirement analyst. Your example has therefore a very artificial and abstract quality. I can't see any part in a software development process, which can be facilitated or clarified by these. Your symbols seem to be clear but as soon as you use combinations and claim that some concepts would be visible from this selection the clarification boxes, which is also visible in my answers.
6	Keep Account Data up to Date	Perform Transaction	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	A combination of misuser, threat, vulnerability and misuse case	A combination of misuser, threat, vulnerability and Asset	Not clear from description - closest would be IP Filtering	Not clear from description - closest would be IP Filtering	
7	Perform Transaction	Perform Transaction via Online	Initial Half Opened Connections to server	Allows Unlimited Number of Connections	Install IP Filtering	Availability of service is compromised	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	A combination of impact and security criterion	A combination of misuser and misuse case	Make Online Service Unavailable	A combination of impact and security criterion	This really is a good topic to conduct research on. Security of Data online is of utmost important. The more will be the secure transactions, the greater will be the trust developed. Several encryption algorithms can be used to secure the data. On of them I can think of is SHA1 algorithm. I think, this is good going. Keep up the good work.
8	Perform Transaction	Availability of Service	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset	None of the Above	None of the Above	
9	Availability of Service	Availability of Service	Make Online Service Unavailable	Availability of Service is Compromised	Availability Of Service	Make online service unavailable	Install IP Filtering	Attacker	Allows Unlimited Number of Connections	A combination of impact and security criterion	A combination of misuser, threat, vulnerability and Asset	A combination of misuser and misuse case	A combination of impact and security criterion	A combination of misuser and misuse case
10	Availability of Service	Perform Transaction	Pay Money	Install IP Filtering	Availability of Service is Compromised	Make online service unavailable	Make Online Service Unavailable	First, Second and Third Option	A combination of misuser, threat, vulnerability, Impact and Asset	A combination of impact and security criterion	A combination of misuser, threat, vulnerability and Asset	A combination of misuser and misuse case	A combination of impact and security criterion	A combination of misuser and misuse case
11	Keep Account Data up to Date	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	None of the above	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	Make Online Service Unavailable	A combination of misuser, threat, vulnerability and Asset	A combination of misuser and misuse case	A combination of impact and security criterion	A combination of impact and security criterion
12	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability of Service is Compromised	Install IP Filtering	Allows Unlimited Number of Connections	Bank Customer	A combination of misuser and threat	Make Online Service Unavailable	A combination of misuser, threat, vulnerability and Asset	A combination of impact and security criterion	A combination of misuser, threat, vulnerability and Asset	
13	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset	Make Online Service Unavailable	A combination of misuser, threat, vulnerability and Asset	None of the Above	None of the Above	This research is done with alot of hardwor. Excellent job. -- Itam
13	Availability of Service	Perform Transaction via Online	Make Online Service Unavailable	Keep Account Data up to Date	Make Online Service Unavailable	Availability of service is compromised	Make Online Service Unavailable	Bank Officer	A combination of impact and security criterion	Make Online Service Unavailable	A combination of impact and security criterion	A combination of impact and security criterion	A combination of impact and security criterion	

14	Perform Transaction	Perform Transaction via Online	Initiate Half Opened Connections to server	Allows Unlimited Number of Connections	Install IP Filtering	Availability of service	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
15	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
16	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	The work is a good effort to secure IS development during early stages of the development.
17	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
18	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
19	Keep Account Data up to Date	Perform Transaction via Online	Initiate Half Opened Connections to server	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
20	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	
21	Perform Transaction	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	None of the Above
22	Keep Account Data up to Date	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Install IP Filtering	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	None of the Above
23	Keep Account Data up to Date	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	I think IS security needs to be factored from the phase, doing it through modelling language which might not be an interesting thing to do in the end is the low level implementation.
24	Keep Account Data up to Date	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	None of the Above
25	Keep Account Data up to Date	Perform Transaction via Online	Make Online Service Unavailable	Allows Unlimited Number of Connections	Availability Of Service	Install IP Filtering	Availability of Service is Compromised	Attacker	A combination of misuser, threat, vulnerability, Impact and Asset.	A combination of misuser and misuse case	A combination of misuser, threat, vulnerability and Asset.	None of the Above	None of the Above	None of the Above

Appendix C – Research Paper Submitted to an International Workshop

A research paper submitted to SBP'12 JOINT WORKSHOP ON SECURITY IN BUSINESS PROCESSES in conjunction with the 10th International Conference on Business Process Management (BPM 2012).

<http://www.inf.unibz.it/sbp12/papers/P5-Soomro.pdf>

Appendix D – Research Paper

Towards Security Risk-oriented Misuse Cases

Inam Soomro and Naved Ahmed

Institute of Computer Science, University of Tartu

J. Liivi 2, 50409 Tartu, Estonia

{inam, [naved](mailto:naved@ut.ee)}@ut.ee

Abstract. Security has turned out to be a necessity of information systems (ISs) and information per se. Nevertheless, existing practices report on numerous cases when security aspects were considered only at the end of the development process, thus, missing the systematic security analysis. Misuse case diagrams help identify security concerns at early stages of the IS development. Despite this fundamental advantage, misuse cases tend to be rather imprecise; they do not comply with security risk management strategies, and, thus, could lead to misinterpretation of the security-related concepts. Such limitations could potentially result in poor security solutions. This paper applies a systematic approach to understand how misuse case diagrams could help model organisational assets, potential risks, and security countermeasures to mitigate these risks. The contribution helps understand how misuse cases could deal with security risk management and support reasoning for security requirements and their implementation in the software system.

Keywords: Security risk management, Misuse cases, Security engineering, Information system security

¹ We would like to express our gratitude to *Dr. Raimundas Maulevičius* for his invaluable contributions in completing this research.

1 Introduction

During the last two decades, line between digital and social life is diminishing, leading that modern society is mainly dependent on information system (IS) and its security. The demand for IS security is constantly growing. Also developing and maintaining system security is increasingly gaining attention. Consideration of IS security at the early stages of software development is also acknowledged in [18]. The security breaches in IS can lead to the negative consequences. The practitioners of IS security must inspect security threats with a negative perspective from the very beginning of IS development process. Consideration of security at early development stages assists to analyse and estimate security measures of the IS to be developed.

This paper discusses the security risk management at requirement elicitation and analysis stage. We will consider the question “how security risk management could be addressed using misuse case diagrams?”. To answer this question we analyse misuse cases proposed by Sindre and Opdahl [18]. The misuse case diagrams [17, 18] are one of the possible techniques to relate security analysis and functional requirements of software systems. The main goal is to model negative scenarios with respect to functional requirements. The misuse cases are already proved to be useful in industry [15]. Existing misuse cases is relatively a simple language, since it contains few constructs to model security concerns. However the previous analysis [9] showed several limitations of misuse cases; for example, misuse cases do not comply with security risk management strategies, because they lack several concrete constructs to address secure assets, security risks and their countermeasures; misuse cases lack distinct constructs for representing security risk concepts. These limitations could result in misinterpretation of the security-related concepts leading to poor security solutions. In this paper we tend to propose few improvement to the misuse cases diagrams.

We apply a systematic approach to understand how misuse case diagrams could help to model organisational assets, potential system risks, and security requirements to mitigate these risks. More specifically we introduce new constructs to extend the misuse cases in order to align their constructs with the concepts of Information Systems Security Risk Management (ISSRM) domain model [11,12]. The benefit of syntactical and semantic extensions is that they introduce the missing semantics in to the language. The domain model is a touchstone to verify if the concepts presented are acceptable and appropriate for the security risk management.

The structure of the paper is organised as follows: in Section 2 we provide background knowledge needed for our study. In Section 3, we describe our research method and introduce Security Risk-oriented Misuse Cases (SROMUC) through an online banking example [1,8]. Next we discuss alignment of SROMUC to ISSRM. In Section 4 we review the related work, discuss our results and conclude our study.

2 Background

2.1 Information System Security Risk Management (ISSRM)

Information System Security Risk Management (ISSRM) [11,12] is a systematic approach, which addresses the security related issues in an IS domain. The model is defined after a survey of risk management and security related standards, security risk management methods and software engineering frameworks [12]. The domain model (see Fig. 1) supports the alignment of security modelling languages. It improves the IS security and security modelling languages as it conforms to the security risk management of organizations. The model describes three different conceptual categories:

Asset-related concepts describe the organization’s assets grouped as business asset and IS asset. It also defines the security criterion as a constraint of a business asset expressed as integrity, confidentiality and availability.

Risk-related concepts define risk, potential harm to business, it is composed of a threat that contains one or more vulnerabilities, if executed successfully, harms the system assets which has negative consequences on assets defined as an impact. They negate the security criterion imposed by the business asset. An event is an abstraction aggregated as a threat and vulnerability where vulnerability is a weakness in a system that can be exploited by threat agent. A threat is a way to inflict an attack. It harms IS and business asset carried out by a threat agent and an attack method to target IS assets. Threat Agent is an attacker that initiates a threat to harm the IS asset. Attack Method is a mean through which a threat agent executes a threat.

Risk treatment related concepts define a risk treatment decision to avoid, reduce, retain, or transfer the potential risks. It is refined by the security requirement. A control implements the security requirement.

The ISSRM process [11,12] is a 6-step process, based on existing risk analysis methodologies and standards. It starts with context and asset identification of the organization, proceeding to determine the security objectives for identified assets. Next, risk analysis and assessment to examine and estimate potential risks and its impacts. In next step, risk treatment decisions are taken to identify the security requirements. Finally, security control is

implemented as security requirement. The process is iterative which may identify new risks and security controls.

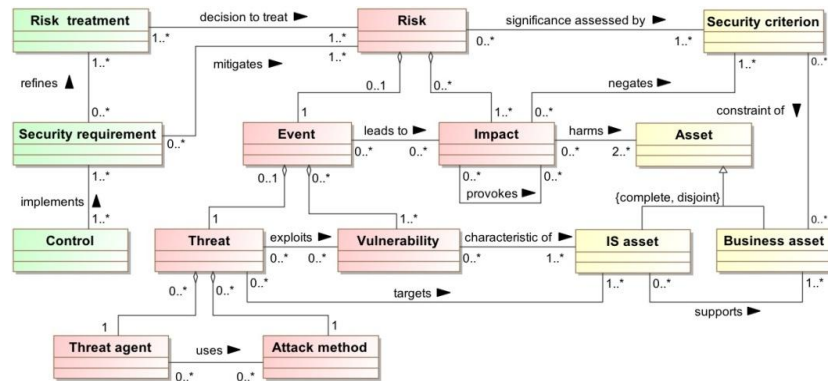


Fig. 1. ISSRM Domain Model [11]

2.2 Misuse Cases

Misuse cases are proposed by Sindre and Opdhal in [18]. They have extended the standard UML use cases to model security concerns at the early stages of software system development. The misuse cases include both the graphical notation and textual representation. Sindre and Opdahl define misuse case as a list or sequence of steps, if performed by an agent successfully, cause harm to the stakeholder and/or to the system. They define misuser as an actor that is willing to use the system with unfavourable intents. Initially, only threats were modelled as misuse cases. Later on, Sindre and Opdahl adapted the concept of security use case discussed by Firesmith [6] where security use cases are defined as a function to protect the system assets from the identified risks. In [16] Røstad has extended the misuse cases with a concept of vulnerability as weakness of the system (see a grey-filled use case in Fig. 3).

3 Security Risk-oriented Misuse Cases (SROMUC)

This section describes the research method used to develop SROMUC. We illustrate SROMUC using three different security scenarios on asset integrity (see Fig. 2, 3, and 4), confidentiality (see Fig. 5), and availability (see Fig. 6) in an example of online banking. This section results in a conceptual alignment between SROMUC and ISSRM domain model.

3.1 Research Method

The main research objective of this study is to enable misuse cases to support the security risk management during the IS development. We followed a 3-step research method: firstly, we conduct literature review of security in IS and the ISSRM domain model to identify the security risk concepts. Secondly, we investigate how the misuse case diagrams express the security risk concepts. Hence, we observed the limitations of misuse cases in modelling the ISSRM concepts and executing the risk management process. Lastly, we define misuse case extensions, thus resulting in the Security Risk-oriented Misuse Cases (SROMUC). The extensions are done on all three components of the modelling language, namely concrete syntax, meta-model and semantics.

3.2 Scenario 1: SROMUC Modelling for Integrity

We illustrate the application of SROMUC using the online banking example [1, 8]. This scenario is particularly focussed on the IS integrity. To achieve better understandability, we split the scenario to 3 models²: one for assets (see Fig. 2), one for security threats (see Fig. 3), and one for security requirements (see Fig. 4).

² To create these models we use the Microsoft Visio tool.

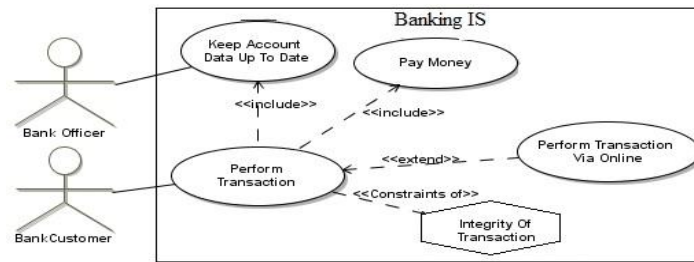


Fig. 2. Asset Modelling

Asset model. In Fig. 2, we illustrate the context of an online banking IS in a use case diagram. A security criterion is a security constraint imposed on business use case (i.e., business asset). The example focusses on the bank customer and bank officer who both communicate with Banking IS. The Bank Customer and Bank Officer are the assets characterising the users of the system in reference to ISSRM domain model. The bank customer seeks to Perform Transaction and bank officer seeks to Keep Account Data Up To Date. The Perform Transaction includes two use cases Pay Money and Keep Account Data Up To Date and extends Perform Transaction Via Online. Perform Transaction has a security criterion Integrity of Transaction represented as a hexagon (see Fig. 2) as it characterises a security constraint of a business use case (i.e., Perform Transaction). In Fig. 2, a dotted line with stereo type constraints of is linked from business use case (i.e., Perform Transaction) to security criterion (i.e., Integrity of Transaction) shows the relationship between the two. According to ISSRM domain model we identified Perform Transaction as the business asset that has some business value. Hence Perform Transaction Via Online supports the business asset and is considered as an IS asset.

Risk model. In Fig. 3, we model the potential security threat scenario. A misuser (i.e., Attacker) initiates a misuse case (i.e., Intercept Money includes Transfer money to another account and Change details of transaction) by exploiting the vulnerability (i.e., Unsecure Network Channel) in a use case (i.e., IS asset). Following [10] in Fig. 3, this vulnerability is represented by filled grey use case. The misuse case Intercept Payment threatens the use case Perform Transaction Via Online (i.e., IS Asset). The threat Intercept Money leads to an impact (i.e., Money Transferred to Unintended Account) which harms the business use case (i.e., Perform Transaction) and disaffirms the security criterion (i.e., Integrity of Transaction). An impact is a state of system that is represented as rounded rectangle (see Fig. 3). A misuse case is linked to impact using leads to relationship. On one hand, an impact disaffirms the security criterion linked with negates relationship. On another hand impact harms a business use case (i.e., Perform Transaction).

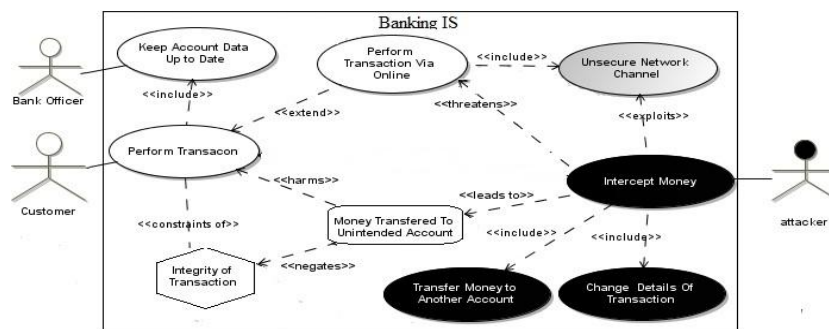


Fig. 3. Threat Modelling

Risk treatment model. The ISSRM domain model defines the risk treatment, control and its implementation. However, SROMUC does not support the modelling of these concepts but security requirement is modelled as a security use case. The security use case is represented as a use case with a lock inside (see Fig. 4). In Fig. 4, we present the security requirement for identified threats. The use case Perform Transaction Via Online (i.e., IS Asset) includes a security use cases (i.e., Apply Cryptographic Procedures and Use Secure Communication Protocol). The security use case mitigates the misuse case (i.e., Intercept Money). It ensures security criterion (i.e., Integrity of Payment) imposed by business use case (i.e., Perform Transaction).

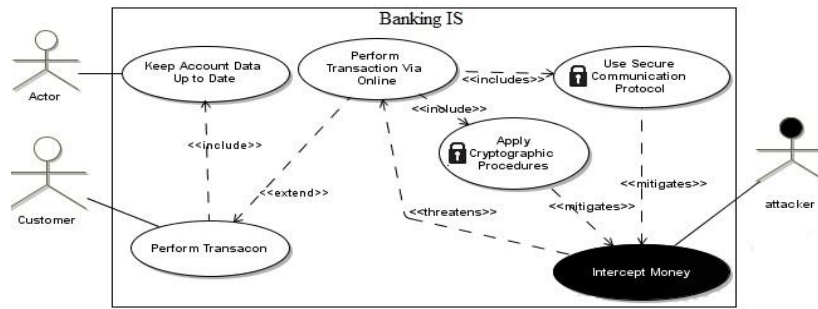


Fig. 4. Security Requirement Modelling

3.3 Scenario 2: SROMUC Modelling for Availability

In Fig. 5, we model an online banking IS [1, 8] for Availability of Service. In our example, the business use case (i.e., Perform Transaction) has a constraint of security criterion (i.e., Availability Of Online Service). The misuser (i.e., Attacker) initiates a misuse case (i.e., Make Online Service Unavailable includes Initiate Half Opened Connections To Server). It exploits the vulnerability (i.e., Allow Unlimited Number Of Connections) included in a use case Perform Transaction Via Online (i.e., IS Asset). The misuse case Make Online Service Unavailable threatens use case Perform Transaction Via Online (i.e., IS asset) and leads to an impact (i.e., Availability Of Service Is Compromised), moreover, it harms the business use case Perform Transaction. The impact of the misuse case negates the security criterion.

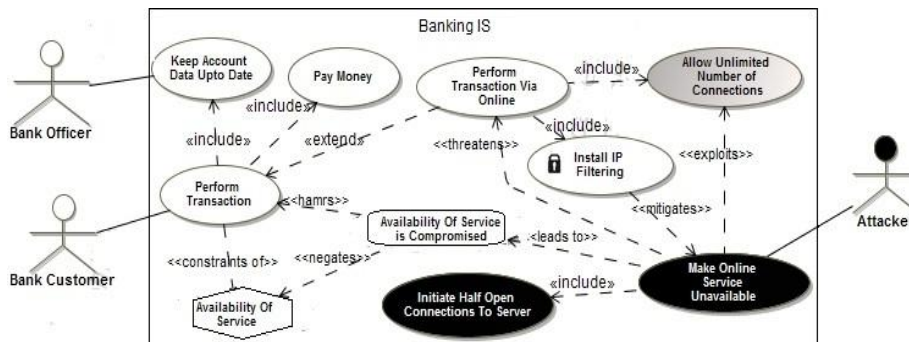


Fig. 5. Modelling for Availability of Service

3.4 Scenario 3: SROMUC Modelling for Confidentiality

In Fig. 6, we model the example of an online banking IS [1, 8] for the Confidentiality Of Data. In this example, the business use case (i.e., Perform Transaction) has a constraint of security criterion (i.e., Confidentiality Of Transaction). The use case Perform Transaction Via Online (i.e., IS asset) includes another use case (i.e., Ensure Account privacy includes Enter PIN Code) for securing an online transaction. The misuser (i.e., Attacker) initiates a misuse case (i.e., Steal Account Data includes Retrieve Transaction Data includes Disclose Transaction Data) by exploiting the vulnerability (i.e., Data Is Not Encrypted and Accept Malicious Data). The misuse case (i.e., Steal Account Data) threatens the use case Perform Transaction Via Online (i.e., IS asset) and leads to an impact (i.e., Confidentiality Of Data Is Compromised), moreover, It also harms the business use case (i.e., Perform Transaction). The impact of the misuse case negates the security criterion.

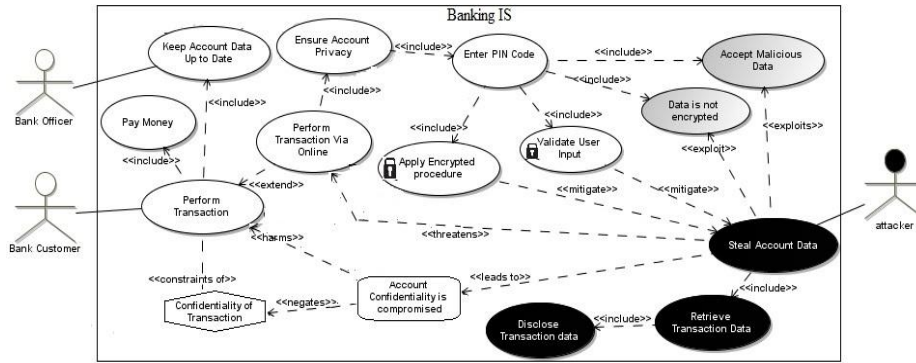


Fig. 6. Modelling for Confidentiality of Data

3.5 Concept Alignment of SROMUC and ISSRM

In [9] authors discuss the alignment between the misuse cases and the ISSRM domain model. However it presents only the correspondences, overlaps or/and similarities. In this section we describe the alignment of SROMUC with the concepts found in ISSRM domain model. In Table 1, 2 and 3, first column outlines the ISSRM concepts. The second column expresses their synonyms found in the literature. The third column distinguishes the concepts and relationship. The last column defines the SROMUC visual constructs.

Alignment of asset-related concepts. In Table 1, we introduce SROMUC syntax to represent the ISSRM asset-related concepts. In ISSRM domain model, assets correspond to Actor and Use case in SROMUC. The business asset and the IS asset are modelled as a use case. The supports relationship in ISSRM between IS asset and business assets is expressed using extends and includes relationships. We introduce hexagon construct in SROMUC to represent the ISSRM security criterion. A security criterion is the constraint on business asset therefore the hexagon is linked to business use case through dotted line with constraint of relationship.

Table 7. Asset Related Concepts (C – Concept, R – Relationships)

ISSRM Concepts	Synonyms	Type	SROMUC Syntax
Assets		C	
Business Asset	Business Use Case	C	
IS Asset	IS Use Case	C	
Security Criterion	Security Constraint	C	
Supports	-	R	<code><<extends>></code> <code><<includes>></code>
Constraints of	Restriction	R	<code><<constraints of>></code>

Alignment of risk-related concepts. In Table 2, we introduce the SROMUC syntax to represent the ISSRM risk-related concepts. In SROMUC, a threat agent is represented as misuser, attack method as misuse case and vulnerability as a use case filled in grey. A threat is modelled as a combination of misuser and misuse case (i.e., misuser communicates with misuse case). The ISSRM targets relationship is represented as an SROMUC threatens relationship. We introduced a rounded rectangle to model the impact concept of ISSRM.

In order to be compliant with ISSRM domain model, we also introduce the exploits, leads to, harms and negates relationships. Exploits relationship defines a link between misuse case and the vulnerability whereas the leads to relationship defines a link between the misuse case and the impact. The harms relationship defines the link between an impact and a business use case whereas a negates relationship defines a link between an impact and the security criterion (see Table 2). We combine the concepts of threat agent, attack method, vulnerability, and impact all together to represent an event, where a risk is understood as a combination of event and the impact.

Alignment of risk treatment-related concepts. In risk treatment-related concepts, we update the visual syntax of security use case by adding a padlock to security use case, which represents security requirement (see Table 3). The ISSRM mitigates relationship is modelled with mitigates relationship from security use cases (i.e., security requirement) to misuse case in SROMUC.

Table 8. Alignment of Risk related Concepts(C – Concepts, R – Relationships)

ISSRM Concepts	Synonyms	Type	SROMUC Syntax



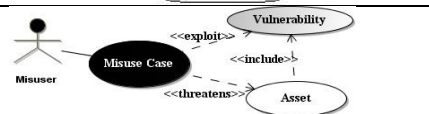




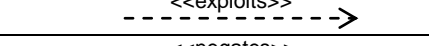
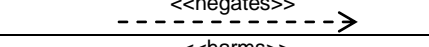
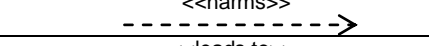
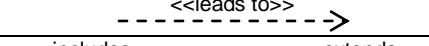
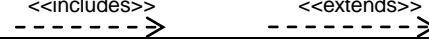

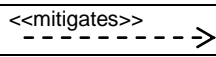
Risk	Hazard	C	
Impact	Effect	C	
Event	Incident	C	
Attack Method	Violence	C	
Vulnerability	Weakness	C	
Threat Agent	Attacker	C	
Threat	Hazard	C	
Exploits	-	R	
Negates	Denies,	R	
Harms	-	R	
Leads to	-	R	
Characteristics of	-	R	
Uses	-	R	

Table 9. Risk Treatment related Concepts (C – Concepts, R – Relationships)

ISSRM Concepts	Synonyms	Type	SROMUC Syntax
Risk Treatment		C	
Security Requirement	Countermeasure	C	
Control		C	-
Refines		R	-
Mitigates	Diminishes	R	
Implements			-

3.6 Abstract Syntax of Security Risk-oriented Misuse Cases

In Section 3.1, we presented the SROMUC before abstract syntax due to the simple introduction of the language. However, to illustrate the application of proposed SROMUC, we need to introduce its abstract syntax in Fig. 7. The major elements in the meta-model are an Actor OR Misuser and Use OR Misuse Case. Actor OR Misuser initiates the communication to interact with Use OR Misuse Case. Their cardinality shows that an Actor or Misuser can communicate with one or more Use or Misuser Case. Actor and misuser are the specialisations of an Actor OR Misuser. Use Or Misuse case can includes or extends another Use OR Misuse Case. The Use Case, Vulnerability and Misuse Case are the specialization of Use OR Misuse Case. The Use Case includes one or more Vulnerabilities that can be exploited by one or more misuse cases. A Misuse Case threatens (i.e., threatening) one or more use cases. A Misuse Case Leads To one or more Impact. An Impact Harms one or more use cases (see Fig. 3) by negating one or more Security Criterion define as Constraint Of on that use case. A Security Use Case is a specialised Use Case that Mitigates one or more Misuse Cases.

4.2 Discussion

SROMUC is an approach to elicit security requirements at the early stages of the system development. It will potentially help designers, architects and analysts to understand the potential threats and security attacks. At both the architecture and design stages, risk analysis is a necessity. The SROMUC approach enables the security analysts to discover the architectural flaws so that their mitigation could begin early in the system development. Otherwise disregarding the risk analysis at this level leads to costly problems later. In practice, system stakeholders are not motivated to invest on security concerns, as it does not add direct value to the systems' functionality. The proposed SROMUC strengthens the misuse case diagrams by extending their syntax and semantics. The proposed graphical extensions are not intuitive and they related to the security concerns supported by the ISSRM domain model. However the primary idea is to keep it comprehensible and to compliable with the original definition of (mis)use cases. We differentiate the construct 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. In [9] Matulevičius et al. have suggested to differentiate the concepts of the IS asset and the business asset. But here, we did not differentiate the assets as it changes the definition of original use case construct. We make an exception regarding the security use because it addresses the system functionality in terms of security countermeasures. Regarding the completeness of alignment between SROMUC and ISSRM domain model, SROMUC does not address the risk treatment and control implementation.

SROMUC is not the only approach that has been aligned to ISSRM domain model. Currently ISSRM is becoming a common model [11] to understand security risk modelling using different modelling languages, like BPMN [3], Secure Tropos [10], KAOS extensions to security [11], and Mal-activities [4]. Finally, this may lead to interoperability between different security languages.

Although in the online banking example we have illustrated the applicability and performance of our proposal, we acknowledge the importance of the industrial case study to validate the SROMUC in the practice. As a future work, we also plan to experiment the language in a case study to validate its usefulness and effectiveness.

References

1. Ahmed, N., Matulevičius, R., Mouratidis, H.: A Model Transformation from Misuse Cases to Secure Tropos. In: Proc of the CAiSE'12 Forum at the 24th International Conference (CAiSE). pp. 7–14. CEUR-WS (2012)
2. Alexander, I.: Misuse cases: Use cases with Hostile Intent. *IEEE Soft.* 20(1), 58–66 (2003)
3. Althhova, O., Matulevičius, R., Ahmed, N.: Towards Definition of Secure Business Processes. In: CAiSE Workshops. vol. 112, pp. 1–15. Springer (2012)
4. Chowdhury, M., Matulevičius, R., Sindre, G., Karpati, P.: Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions. In: REFSQ, vol. 7195, pp. 132–139. Springer Berlin / Heidelberg (2012)
5. Ekelhart, A., Fenz, S., Neubauer, T.: AURUM: A Framework for Information Security Risk Management. In: HICSS '09. pp. 1–10. IEEE Computer Society (2009)
6. Firesmith, D.: Security Use Cases. *Journal of Object Technology* 2(3), 53–64 (2003)
7. Herrmann, A., Morali, A., Etalle, S., Wieringa, R.J.: RiskREP: Risk-based Security Requirements Elicitation and Prioritization. In: Perspectives in Business Informatics Research, Riga, Latvia. pp. 155–162. Riga Technical University (2011)
8. van Lamsweerde, A.: Elaborating Security Requirements by Construction of Intentional Anti-Models. In: Proceedings of the 26th International Conference on Software Engineering. pp. 148–157. ICSE '04, IEEE Computer Society (2004)
9. Matulevičius, R., Mayer, N., Heymans, P.: Alignment of Misuse Cases with Security Risk Management. In: Proceedings of 3rd International Conf. on Availability, Reliability and Security. pp. 1397–1404. IEEE Computer Society (2008)
10. Matulevičius, R., Mouratidis, H., Mayer, N., Dubois, E., Heymans, P.: Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management. *J. UCS* 18(6), 816–844 (2012)
11. Mayer, N.: Model-based Management of Information System Security Risk. Ph.D. thesis, University of Namur (2009)
12. Mayer, N., Heymans, P., Matulevičius, R.: Design of a Modelling Language for Information System Security Risk Management. In: Proceedings of the First International Conference on Research Challenges in Information Science, RCIS 2007. pp. 121–132 (2007)
13. McDermott, J.: Abuse-Case-Based Assurance Arguments. In: Proc. of the 17th Annual Comp. Security Applications Conf. pp. 366–. ACSAC '01, IEEE Computer Society (2001)
14. McDermott, J., Fox, C.: Using Abuse Case Models for Security Requirements Analysis. In: Proceedings of ACSAC'99. pp. 55–, IEEE Computer Society (1999)
15. Pauli, J.J., Xu, D.: Trade-off Analysis of Misuse Case-based Secure Software Architectures: A Case Study. In: Proc. of MSVVEIS Workshop. pp. 89–95. INSTICC Press (2005)
16. Røstad, L.: An Extended Misuse Case Notation: Including Vulnerabilities and The Insider Threat. In: Proc. 12th Working Conf. REFSQ'06 (2006)
17. Sindre, G., Opdahl, A. L.: Templates for Misuse Case Description. In: Proc. of the 7th International Workshop on REFSQ'01 (2001)

18. Sindre, G., Opdahl, A. L.: Eliciting Security Requirements with Misuse Cases. *Requir. Eng.* 10(1), 34–44 (2005)