UNIVERSITY OF TARTU

Institute of Computer Science
Software Engineering Curriculum

Madis Kaasik

A Tool for Supporting Multi-Perspective System Development Through Security Risk Management

Master's Thesis (30 ECTS)

Supervisor: Raimundas Matulevičius, PhD

Tartu 2018

A Tool for Supporting Multi-Perspective System Development Through Security Risk Management

Abstract:

Information systems are used more and more in various fields in everyday life. Broad usage of information systems means that security of these systems is vital. The importance of bearing security in mind in early stages of developing new systems has been acknowledged. One possible approach is to model security into models when designing the system. This master thesis will give an overview what is Information System Security Risk Management domain model and how secure extensions of different modelling languages have been aligned to it. The main output of this thesis is a developed tool which helps users learn and understand those alignments as well as learn the process of how to transform models about same system from one secure modelling language to another. In the final part of the thesis, the created solution is validated.

Keywords:

ISSRM, Security Risk-aware Secure TROPOS, Security Risk-oriented BPMN, Security Risk-oriented Misuse Cases, Mal-Activities for Security Risk Management

CERCS:

T120 - Systems engineering, computer technology

Rakendus toetamaks mitmevaatelise süsteemi arendamist turvariskide haldamise kaudu

Lühikokkuvõte:

Infosüsteemid leiavad tänapäeval järjest enam ja enam kasutust erinevates valdkondades. Laialdane infosüsteemide kasutamine tähendab, et nende süsteemide turvalisus on ülimalt oluline. Aru on saadud, et tähtis on turvalisuse peale mõelda juba süsteemide varajases arenguprotsessis. Üks võimalik lähenemine on modelleerida turvalisus mudelitesse juba süsteemi disainimise faasis. Käesolev magistritöö annab ülevaate, mis on infosüsteemi turvariski haldamise domeenimudel ja kuidas erinevate modelleerimiskeelte turvalaiendused on selle domeeni mudeliga joondatud. Töö põhiväljund on arendatud rakendus, mis aitab kasutajatel õppida ja mõista eelpool mainitud joondusi ning õppida ka kuidas transformeerida sama süsteem mudeleid erinevatesse modelleerimiskeeltesse. Töö viimases osas valideeritakse loodud lahendus.

Võtmesõnad:

Infosüsteemi turvariski haldamine, Turvariskiteadlik TROPOS, Turvariskile suunatud BPMN, Turvariskile suunatun Misuse Case diagrammid, Turva riskide haldamine Mal-Activity diagramme kasutades

CERCS:

T120 - Süsteemitehnoloogia, arvutitehnoloogia

Contents

1 Introduction 5

2 Modelling Languages and Security Risk Management 7

2.1 Domain Model for Information Systems Security Risk Management 7

2.2 Security Risk-Aware Secure TROPOS 9

2.3 Security Risk-Oriented BPMN 11

2.4 Security Risk-Oriented Misuse Cases 13

2.5 Mal-Activities for Security Risk Management 15

2.6 Summary 17

3 A Tool for Multi-Perspective Security Risk Management 18

3.1 Tool Description 18

3.2 Requirements and Design 18

3.2.1 Analysis of User's Goals 19

3.2.2 Scenarios 21

3.2.3 Mockups 29

3.2.4 Rules for Risk-Related Concepts 30

3.2.5 Functional Requirements 31

3.2.6 Non-Functional Requirements 35

3.3 Summary 35

4 Validation 36

4.1 Description of the Validation Process 36

4.2 Feedback Questionnaire 37

4.3 Discussion 45

4.4 Threats to Validation 47

4.5 Summary 48

5 Conclusion 49

5.1 Limitations 49

5.2 Answers to Research Questions 49

5.3 Conclusion 50

5.4 Future Work 50

1 Introduction

Security risk management plays an important role in software system's development. The concerns for addressing security from the beginning of system development process is emphasised more and more [1]. Every modelling languages illustrates different aspects of the system. This means that in order to see all aspects of the system, more than one modelling language is often needed. Using multiple languages for representing the same system means, that there is need for transformations from one modelling language to another. Although multiple automatic transformers between modelling languages exist, there is no tool which would help with learning how to model in security risk-oriented languages and help in learning and understanding the transformation process from one secure modelling language to another.

This thesis gives an overview of what is domain model for information systems security risk management (ISSRM) and how it is used for secure modelling. Four secure modelling languages: Security Risk-aware Secure TROPOS, Security Risk-oriented BPMN, Security Risk-oriented Misuse cases and Mal-Activities for Security Risk Management are chosen for this thesis. Already proposed alignments between those modelling language constructs and ISSRM domain model concepts are researched and taken as an input for the tool developed in this thesis.

The main aim of this thesis is to design and implement a tool, which can be used by universities and students to teach and learn modelling in Security Risk-oriented modelling languages. The tool helps the users understand how to create models in these languages, which constructs to use, how they are connected to one another and also shows the constructs alignments to ISSRM domain model concepts. Since the tool supports four modelling languages mentioned earlier, potentially it could be useful for learning how to transform between those four modelling languages, while keeping security aspects intact. Following research questions are set for this thesis.

1. **RQ1:** How are secure modelling languages aligned to ISSRM domain model?

2. **RQ2:** What are the requirements for tool to help the users learn alignment to ISSRM domain model concepts and transformations between secure modelling langauges?

3. **RQ3:** How easy is to learn modelling language alignment to ISSRM domain model concepts using the proposed solution?

4. **RQ4:** How easy is to learn transformations between secure modelling languages with help from tool which shows alignments to ISSRM domain model concepts?

This thesis is structured as follows. In this introduction chapter we explained the motivation for this thesis set scope of which modelling languages are chosen and also set research questions addressed in this thesis. In the second chapter we answer research question 1 by researching chosen modelling languages and their security risk-oriented extensions and how those extensions are currently proposed to be aligned to ISSRM domain model. In third chapter we answer research question 2 by identifying and analysing users goals and which scenarios are needed for the user to achieve them. In the fourth chapter we answer research questions 3 and 4 by describing the validation process of the developed solution and results.

2 Modelling Languages and Security Risk Management

This chapter will answer research question 1 "How are secure modelling languages aligned to ISSRM domain model?". For doint that we describe what is domain model for information systems security risk management and what concepts it consists of. Then we are going to introduce security risk-aware secure TROPOS, security risk-oriented BPMN, security risk-oriented misuse cases and mal-activities for security risk management. We also give an overview of already proposed alignments between those modelling language constructs and ISSRM domain model concepts.

2.1 Domain Model for Information Systems Security Risk Management

Domain model for ISSRM was proposed in [2]. Figure 1 pictures the ISSRM domain model. Domain Model for Information Systems Security Risk Management consists of three concept groups [2], [3]: asset related concepts, risk related concepts, risk treatment related concepts. In figure 1 the asset related concepts are colored yellow, risk related concepts red and risk treatment related concepts are marked with green.

Description of ISSRM domain model is based on [2]. Asset related concepts describe which assets in an organization are important to protect and what are the criteria for assets security. An asset may be anything that is needed by the company in order to achieve its objectives. Assets are divided into two: business assets and information system (IS) assets. A business asset describes processes, capabilities, skills and information essential for the business to achieve its objectives. IS assets is a component or part of the information system and is needed for achieving objectives. IS assets are usually immaterial. Security criteria, sometimes called security property is a constraint of business asset that characterizes the security need for the asset. Security criteria are mostly expressed through confidentiality, integrity and availability [2].

Risk related concepts define risk and its sub-components. Risk is a combination of potentially harmful event and impact, which harm system assets. Impact is a potential negative outcome of risk, which may harm assets and negate security criterions. Event is a combination of threat and one or more vulnerabilities. A vulnerability is a characteristic of an asset or assets, which exposes flaws in system security. Vulnerabilities can be intentionally or accidentally exploited by threat. A threat is an incident or an attack initiated by a threat agent, who uses an attack method for targeting one or more IS assets by exploiting their vulnerabilities. A

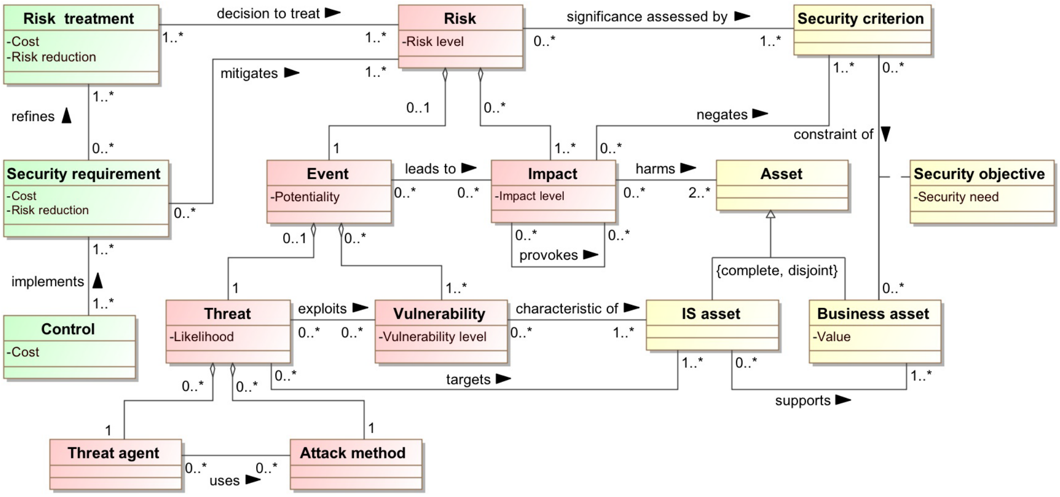

Figure 1: The ISSRM Domain Model [4]

threat agent is an agent who has means to initiate the attack and harm assets. An attack method describes by which means the threat is executed by threat agent [2].

Risk treatment related concepts consist of risk treatment, security requirements and controls. Risk treatment decisions show how to treat identified risks. Risk treatment decisions can be divided to four categories:

- Risk avoidance - Decision to avoid the identified risk. Systems functionality is modified or discarded.
- Risk reduction - Actions to reduce risk probability. In order to reduce the risk security requirements are selected.
- Risk transfer - Sharing the burden of loss from risk with third party.
- Risk retention - Accepting the risk and not changing system design.

A security requirement is a refinement of a risk treatment decision for mitigating risk. Control is an implementation of a security requirement. Security controls may be processes, policies, devices, practices or other components which act to reduce risks [2].

2.2 Security Risk-Aware Secure TROPOS

Tropos [5] approach consists of four phases: early requirements, late requirements, architectural design and detailed design. Each phase complements existing model. In early requirements phase the stakeholders are identified and modeled as social actors. All actors depend on one another in order to achieve goals, complete plans and provide resources. In late requirements phase new actor with its dependencies is added to the model. The new actor represents system. Architectural design phase breaks system down to subsystems. Subsystems are connected to each other with data and control flows. Subsystems are represented by actors and flows are represented as dependencies. The detailed design phase specifies each components capabilities and interactions such as input, output and control [5].

Tropos consists of following main constructs:

1. **Actor** is an entity with strategic goals.
2. **Goal** is entity's strategic interest. Goals are divided into soft goals and hard goals. Hard goals can be satisfied or not satisfied. Soft goals can be satisficed.
3. **Plan** describes what needs to be done in order to achieve goals.
4. **Resource** is a physical or informational entity.
5. **Dependency** is a relationship between two actors. dependency expresses how depender depends on the dependee in order to achieve a goal, execute a plan or deliver a resource.

Secure Tropos [6] is an extension of tropos language. Secure Tropos is applied in early requirements and late requirements phase. Secure Tropos introduces new elements such as security constraint, secure dependency, secure goal and secure plan. Security constraint represents a restriction related to security issues. Secure dependency shows that actors depend on a security constraint to be satisfied. Secure goals are used to express actors strategic interest in respect to security, they are connected to actors using secure dependencies. Secure tasks describe how to achieve secure goals. Attacks relationship shows what is the attacker targeting with plan. Security Risk-aware Secure TROPOS describes the alignment between ISSRM domain model concepts and Secure TROPOS approach [4]. This alignment of Secure TROPOS constructs to ISSRM domain model concepts is shown in Table 1.

Secure Tropos has many models, which support analysing security considerations during an information systems development [4]. Firstly there is the security enhanced actor model (SEAM). This model is used to identify and analyse actors

Table 1: ISSRM domain model concepts alignment to Secure TROPOS constructs. Adapted from [4].

ISSRM construct	**Secure Tropos Construct**
Asset	1) Actor, hard goal, plan, resource, secure goal 2) Composition of actor, hard goal, plan, resource, secure goal using dependency, means-end, contribution and decomposition relationships.
Business asset	1) Actor, hard goal, plan, resource, secure goal 2) Composition of actor, hard goal, plan, resource, secure goal using dependency, means-end, contribution and decomposition relationships.
IS Asset	1) Actor, hard goal, plan, resource, secure goal. 2) Composition of actor, hard goal, plan, resource, secure goal using dependency, means-end, contribution and decomposition relationships.
Security criterion	Soft goal, security constraint, contribution, security constraint decomposition.
Risk	Combination of a threat element and impacts relationship.
Event	1)Composition of an actor, goal, plan, targets, exploits and vulnerability point. 2) Threat element.
Impact	Impact relationship
Threat	1) Goal 2) Plan
Vulnerability	Vulnerability is not modelled, but vulnerability points can be identified by the attributes of the assets.
Threat agent	Agent
Attack method	Plan
Risk treatment	-
Security requirements	1) Actor, hard goal, plan, resource, secure goal. 2) Composition of actor, hard goal, plan, resource, secure goal using dependency, means-end, contribution and decomposition relationships.
Controls	1) Actor, hard goal, plan, resource, secure goal. 2) Composition of actor, hard goal, plan, resource, secure goal using dependency, means-end, contribution and decomposition relationships.

of the environment and system and dependency relationships between those actors [4]. Second model is the security enhanced goal model (SEGM). SEGM model completes SEAM model with how actors reason about their goals, plans and resources. SEGM model elements are linked to one another by the means-ends, decomposition and contribution relationships [4].

2.3 Security Risk-Oriented BPMN

Business process model and notation (BPMN) is meant for modeling business processes. It allows to study and evaluate organization's processes so that the processes add value to organization and its customers [7]. BPMN is considered being business-friendly, because it uses same approach notions as traditional flowcharting [8]. BPMN uses graphical elements, that are are familiar to most modellers and all elements used in BPMN have specific meaning, defined rules and connections between them [8].

Major BPMN constructs according to [9] are pool, which is a container for a process. Lane, which divides pool into smaller parts. Task describes an activity. Event is used for signalling that something happens during the process. Sequence flow connects activities, gateways and events in the pool. Message flow is used for sending messages between different pools. Gateways express control points in the process. Data stores and data objects are connected to tasks with data association relationships. Annotation is used to represent text about objects, annotations are connected to objects using association relationship [9].

The BPMN language is not designed for security modeling, but its domain model can be extended to take security problems into account as well. Multiple papers, that propose extensions for BPMN to support security modelling have been published. For the tool to be developed we use [8] work. Altuhhova proposed in [8] how BPMN could be extended to security risk-oriented BPMN so it does not lose its original purpose, but could be used to model security aspects as well. Table 2 shows alignment between Security Risk-oriented BPMN constructs and ISSRM domain model concepts.

Starting with ISSRM domain model asset-related concepts. Combination of events, gateways, tasks and sequence flow is used for representing organization's valuable assets (both business and IS assets [8]. Labels are used to differ task asset type. Data object can be used for representing business asset [8]. Data stores, containers and pools support business assets and are therefore mapped to IS assets. For constraint a new construct "lock" is proposed. The letter inside lock element describes the business assets security objective [8]. Annotation is used for giving additional information. Since constructs are aligned to different ISSRM domain model concepts Altuhhova proposes also to use different color for depicting different concepts. Asset-related concepts are presented like in normal

Table 2: ISSRM domain model concepts alignment to BPMN constructs. Adapted from [4, 8].

ISSRM construct	**BPMN Construct**
Asset	Combination of flow objects(event, gateway, activity) using sequence flow
Business asset	Data object
IS Asset	a) Data store b) Containers
Supports	a) Container supports combination of Flow Objects (Business assets) by containing them. b) Sequence flow between Flow Objects c) Data association flow between task and data object and task and data store
Constraint of	a) Lock and Association Flow, which point from the Lock to an Annotation. b) Lock is a property of constructs that describe business assets.
Security criterion	Annotation
Security objective	Property of a Lock that can have a value
Risk	Combination of event and outcome
Event	Combination of constructs for Threat and Vulnerability
Impact	a) Unlock b) Unlock is a property of constructs that describe the Business assets.
Threat	Combination of construct for Threat Agent and Attack method.
Vulnerability	Annotation
Threat agent	Pool and Lane
Attack method	Combination of events, gateways and activities
Risk treatment	-
Security requirements	Combination of flow objects.
Controls	-

BPMN black border, risk-related concepts are marked with red and risk treatment-related concepts with blue. Using colors helps to keep the models clearer and easier to understand [8].

For ISSRM risk-related concepts new element "Vulnerability point" was introduced. It is part of characteristics of concept from ISSRM. Vulnerability point is an property of constructs that describe data objects and tasks. Textual annotation is used for describing vulnerability. Pools and lanes are used for expressing threat agents. Attack method is composed of sequence flow and flow objects. [8] also introduces new element "unlock", which presents impact, harms and negates relationships. It is portrayed as an open lock, letter inside the lock represents which security criterion was broken. Complex concepts threat, event and risk are compositions of other concepts.

For risk treatment-related concepts only security requirements and mitigates relationship was defined by [8]. Combination of flow objects and sequence flow is used for representing those concepts. Other risk treatment-related concepts were found to be inessential and extensive for being depicted in the process diagram. It was said, that other concepts should be mentioned as a textual annotation or added to the description or report of the model.

2.4 Security Risk-Oriented Misuse Cases

Use case is a set of actions or events to describe the interaction between an actor and system for an actor to achieve some goal. An actor may be an user or another system. An "include" relationship defines that a use case contains the behaviour defined in another use case. An "extends" relationship specifies an extended behaviour of the targeted use case [4].

Misuse cases [10] extend standard use cases and show how an actor may be able to exploit the system and cause harm to stakeholders [11, 12]. In [13] Security Risk-Oriented Misuse Case (SROMUC) is developed and described in detail how the constructs of SROMUC align to ISSRM domain model concepts. Following chapters describe SROMUC alignment to ISSRM domain model [13]. Table 3 shows alignment between Security Risk-oriented Misuse cases constructs and ISSRM domain model concepts.

Regarding asset-related concepts: assets in ISSRM domain model are modelled as Actor and Use case in SROMUC. The business assets are represented as use cases. System assets can be either use cases or system boundaries [4]. The ISSRM domain model supports relationship between business asset and system asset is expressed using extends and includes relationships. For security criterion concept new type (security criterion) of use case is added to SROMUC. It is linked to business asset with constraint of relationship.

Table 3: ISSRM domain model concepts alignment to Misuse case constructs. Adapted from [4, 13].

ISSRM construct	**Misuse Case Construct**
Asset	Actor
Business asset	(Business) Use case
IS Asset	(IS) Use case System boundary
Supports	1) include relationship 2) Extend relationship
Security criterion	Security criterion
Constraint of	Constraint of relationship
Risk	Combination of constructs used to express event and impact
Impact	Impacts stereotype
Event	Combination of constructs used to express threat and vulnerability.
Attack method	Misuse cases
Vulnerability	Vulnerability stereotype
Threat agent	Misuser
Threat	Combination of misuser and misuse case using communication link
Targets	threaten link
Exploits	exploit link
Negates	negate link
Harms	harm link
Lead to	lead to link
Characteristic of	include link
Risk treatment	-
Security requirements	(Security) use case.
Controls	-

Risk-related concepts: misuser corresponds to threat agent, misuse case represents attack method concept. For vulnerability a new type of use case (vulnerability) is used. ISSRM targets relationship is modelled as threatens relationship in SROMUC. In order to comply to ISSRM domain model, SROMUC introduces new Impact stereotype and 4 new relationships: exploits, leads to, harms and negates. Exploits relationship defines a link between vulnerability and misuse case, leads to links misuse case to impact. Harms relationship links impact to business use case and negates connects impact and security criterion. Threat concept is combination of misuser and misuse case using the communication link. Event is a combination of constructs used to represent threat and vulnerability, whereas risk is combination of constructs used for modelling event and impact. In risk treatment-related concepts SROMUC updates the graphical representation of security use case by adding a padlock to it. The padlock represents security requirement. The ISSRM domain model mitigates relationship is modelled with SROMUC mitigates link between security use case and misuse case. For controls and risk treatment there is no correspondence given.

2.5 Mal-Activities for Security Risk Management

Activity diagrams represent behaviour of system. They include step by step actions and activities and support choice, iteration and concurrency [4]. Activity diagrams can be used to model both computational and organizational processes.

Mal-activity diagrams (MAD) deal with behavioural aspects of security problems [4]. They are constructed by extending activity diagram concepts [14]. Mal-activity diagrams are mostly build against activity diagrams with a goal of achieving systems unwanted behaviour. Mal-activity diagrams introduce mal-activity, mal-swimlane and mal-decision, which are opposite to activity diagrams activity, swimlane and decision [14]. Alignment of MAD constructs to ISSRM domain model concepts are shown in the Table 4.

In [15] alignment between ISSRM domain model concepts and MAD is proposed. In ISSRM domain model business asset is defined as information, process or skill that is needed for business objectives. Activity diagrams show business workflow by combining activity and decision constructs connected by control flow relationship. So these constructs are aligned to ISSRM business assets. In addition data is recognised as business asset as well [15]. In [15] it is said that ISSRM IS assets could be represented using swimlane, decision, activity and control flow. In [15] no alignment is given for security criterion concept, but in [4] it is proposed that security constraint can be represented as an informal comment linked to business asset.

Regarding risk-related concepts: in MAD mal-swimlane is used for representing malicious actor, therefore mal-swimlane is aligned to ISSRM threat agent concept.

Table 4: ISSRM domain model concepts alignment to Malactivity diagram constructs. Adapted from [4, 15].

ISSRM construct	**Mal-activity diagram Construct**
Asset	Process described using activity, decision and controlflow constructs
Business asset	(Implicit) Objects used to perform activities
IS Asset	Swimlane
Supports	Controlflow
Security criterion	Linked comment to business asset
Constraint of	Linked comment to business asset
Risk	Combination of constructs representing event and impact.
Impact	Mal-activity
Event	Combination of constructs used to express threat and vulnerability.
Vulnerability	Linked as a comment to vulnerable assets
Threat	Combination of constructs representing threat agent and attack method
Threat agent	Mal-swimlane
Attack method	a) Process described using Mal-activity, Mal-decision and control flows. b) Swimlane (as means to perform the attack)
Risk treatment	-
Security requirement	Mitigation activity
Controls	Swimlane

Inverses of decision and activity mal-decision and mal-activity combined with control flow are aligned to ISSRM attack method concept. Since malicious actor could use means defined as mal-swimlane, mal-swimlane construct is aligned to attack method concept as well [15]. MAD does not include constructs for representing vulnerability, so [4] has introduced comment linked to vulnerable system assets for alignment to ISSRM vulnerability concept. In MAD ISSRM impact concept could be expressed as mal-activity. ISSRM threat is a combination of constructs used to represent threat agent and attack method. Event is a combination of constructs used to represent threat and vulnerability, whereas risk is combination of constructs used for modelling event and impact.

Risk treatment-related concepts. MAD Mitigation activity is aligned to ISSRM security requirement concept and since swimlane is used for holding mitigation activities, it is aligned to ISSRM control concept.

2.6 Summary

In this chapter we described ISSRM domain model, what concepts it consists of and why it is important. We answered research question 1 "How are secure modelling languages aligned to ISSRM domain model?". For that we examined security risk-aware secure TROPOS, security risk-oriented BPMN, security risk-oriented misuse cases, mal-activities for security risk management and their proposed alignments to ISSRM domain model. In the next chapter we answer research question 2 by identifying users goals, use case scenarios and setting functional and non-functional requirements for the tool.

3 A Tool for Multi-Perspective Security Risk Management

This chapter describes the tool to be developed for this thesis and answers research question 2 "What are the requirements for tool to help the users learn alignment to ISSRM domain model concepts and transformations between secure modelling langauges?". Firstly we talk about why is the solution needed and to whom is the tool targeted at. After explaining the motivation, we go through requirements engineering process by analysing users goals. For satisfying the goals we create use cases and scenarios. From these we can derive functional and non-functional use cases for the solution to be developed. We also introduce the layout of the solutions UI by showing mockups and explaining it in detail.

3.1 Tool Description

Tool is developed for education purpose and is to be used as an learning instrument for students in courses where secure modelling languages and ISSRM domain model are taught. The tool concentrates on Security risk management, Alignments between constructs and concepts and Modelling languages, therefore the tool shall be called SAM. SAM should help the student in understanding and learning security risk-oriented BPMN, security risk-aware secure TROPOS, security risk-oriented misuse cases and mal-activities for security risk management diagram construct alignments to ISSRM domain model concepts. For that SAM combines three main elements of modelling using secure modelling language. Firstly the metamodel of modelling language, this shows what elements the language consists of and how the elements are connected to each other. Secondly the graphical representation of constructs and thirdly the alignments between language constructs and ISSRM domain model concepts. Since SAM shows ISSRM domain model concepts alignment to modelling language constructs, it would also help the users learn how to transform from one security risk-oriented modelling language to another security risk-oriented language.

3.2 Requirements and Design

This chapter describes in detail the requirements engineering process. For identifying users and systems goals we use TROPOS modelling technique. From discovered goals we derive scenarios. Based on created scenarios we can derive solution oriented functional requirements for SAM. In addition to functional requirements, SAM also needs to meet some non-functional requirements.

3.2.1 Analysis of User's Goals

The process of requirements engineering starts with identifying and analysing users and SAMs goals. For this we use TROPOS modelling technique. TROPOS model also helps to understand what resources and tasks are needed in order to satisfy identified hard goals and satisfice the soft goals. Figure 2 shows the created TROPOS model for user and SAM. Model has two actors: user and SAM. Since the tools main purpose should be to help the user learn and understand how to add security to models by using secure modelling language extensions the main soft goals identified for the user are:

1. **SG1** Learn secure modelling
2. **SG2** Learn alignment between language construct and ISSRM domain model concepts
3. **SG3** Learn transformations between modelling languages.

Hard goals that help the user to satisfice his soft goals are:

1. **HG1** See modelling language element's graphical representation
2. **HG2** See modelling language's metamodel
3. **HG3** See language's construct alignment to ISSRM domain model concepts
4. **HG4** See modelling language constructs used to represent ISSRM domain model concepts

All identified hardgoals depend on resources from SAM in order to be met. HG1 depends on the graphical representation of the modelling language. HG2 depends on SAM displaying the metamodel. HG3 and HG4 both depend on SAM to show the alignment between language model construct and ISSRM domain model concept. Soft goals set for SAM are similar to user's soft goals, if the goal of the user is to learn alignments between modelling languages then SAM's corresponding soft goal is to help the user lean those alignments. For user's soft goal to learn transformations between modelling languages, SAM's soft goal is to help the user learn those transformations. For satisficing its sof goals, SAM has supporting hard goals such as displaying language construct alignment to ISSRM domain model concepts, displaying modelling language's metamodels and displaying modelling language's graphical representation.

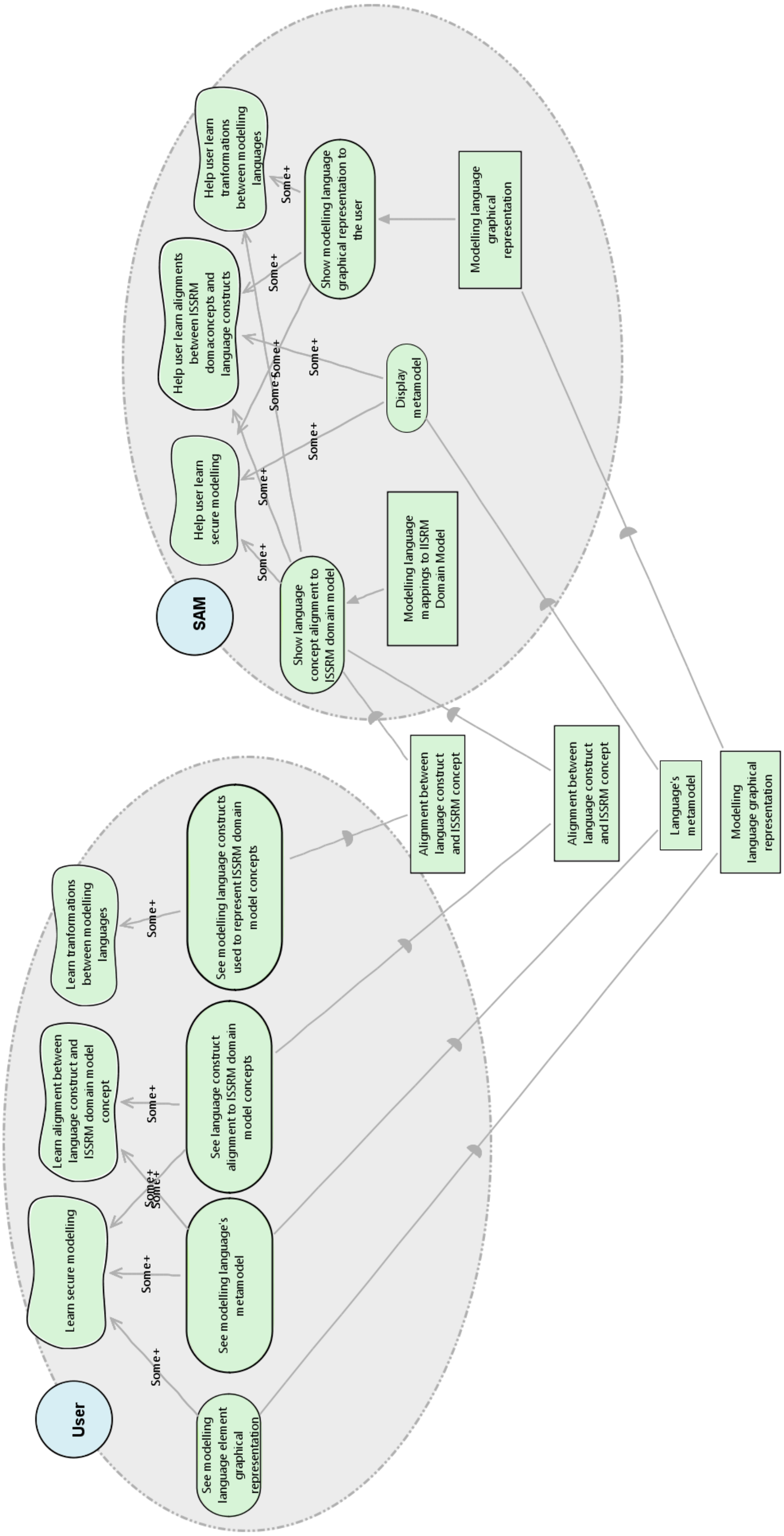
SAM
Help user learn tranformations between modelling languages
Show modelling language graphical representation to the user
Modelling language graphical representation
Help user learn alignments between ISSRM domaconcepts and language constructs
Display metamodel
Help user learn secure modelling
Show language concept alignment to ISSRM domain model
Modelling language mappings to ISSRM Domain Model
Some+
Alignment between language construct and ISSRM concept
Alignment between language construct and ISSRM concept
Language's metamodel
Modelling language graphical representation
User
Learn tranformations between modelling languages
Learn alignment between language construct and ISSRM domain model concept
Learn secure modelling
See modelling language constructs used to represent ISSRM domain model concepts
See language construct alignment to ISSRM domain model concepts
See modelling language's metamodel
See modelling language element graphical representation

Figure 2: Analysis of user's goals

3.2.2 Scenarios

From identified user goals in previous chapter use case scenarios can be derived. This chapter focuses on creating and explaining in detail derived use case scenarios. Figure 3 presents all scenarios created to help the user and SAM fulfil set goals. All use case scenarios for interaction between SAM and user are described using textual and template representation. Tables 5, 6, 7, 8, 9, 10, 11, 12 describe the use cases in detail using template representation.

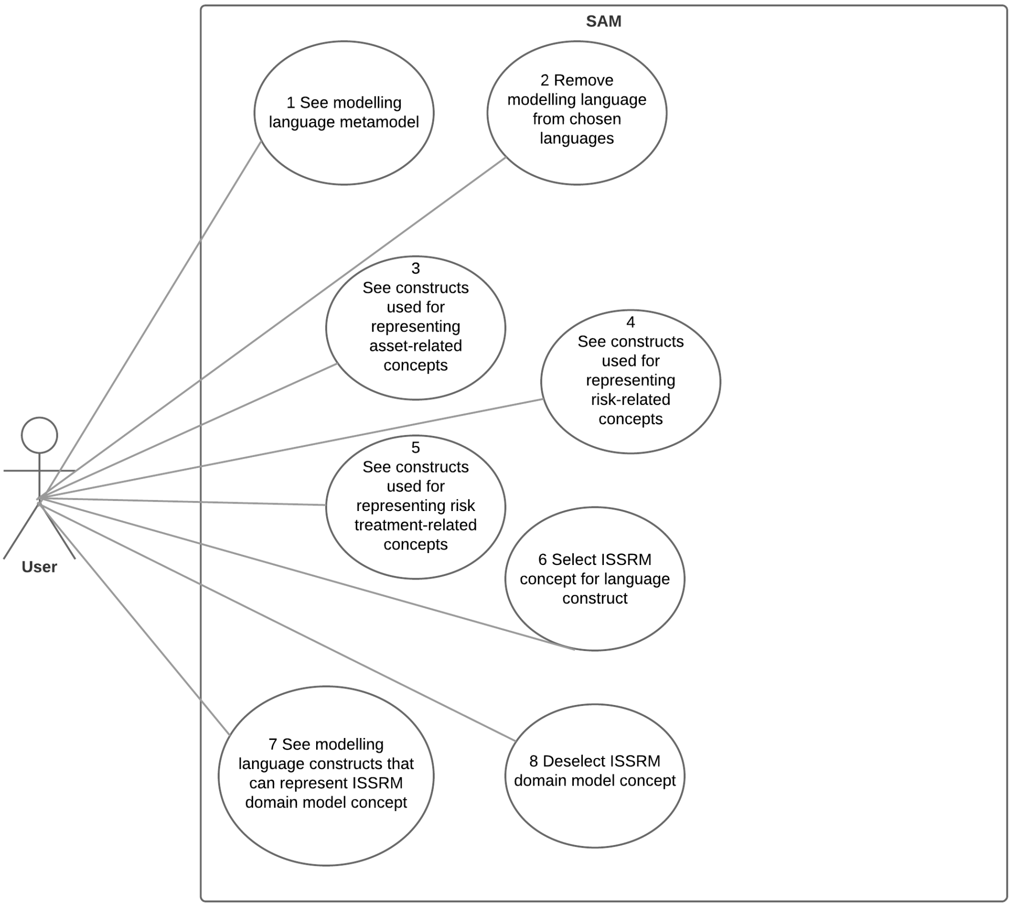
SAM
1 See modelling language metamodel
2 Remove modelling language from chosen languages
3 See constructs used for representing asset-related concepts
4 See constructs used for representing risk-related concepts
5 See constructs used for representing risk treatment-related concepts
6 Select ISSRM concept for language construct
7 See modelling language constructs that can represent ISSRM domain model concept
8 Deselect ISSRM domain model concept
User

Figure 3: User scenarios

Use case 1 is described in Table 5. This use case shows how the user can see modelling language's metamodel to satisfy his hard goal HG2 which helps to satisfice softgoals SG1 and SG2. Four buttons for modelling languages are displayed to the user. If the button with language's name is green, it means that

that modelling language is not chosen and its metamodel is not displayed to the user. If the user clicks button, the metamodel should be displayed on the screen and clicked button should be colored red, indicating that this modelling language is currently chosen and its metamodel is displayed to the user.

Table 5: Use Case 1: See modelling language metamodel

Use Case Id	**UC-1**
Goal number	**HG2**
Use Case Name	See modelling language metamodel.
Actors	1. User 2. SAM
Trigger	User wishes to see modelling language's metamodel.
Preconditions	Language's metamodel is not already visible to the user.
Postconditions	1. Language's metamodel is displayed to the user. 2. Button with language's name is colored red.
Normal flow	1. User decides which language's model he wants to see. 2. User clicks on green button with language's name. 3. SAM displays chosen language's metamodel on the screen. 4. SAM changes button with language's name color to red.

Use case 2 is described in Table 6. Use case 2 has opposite effect from use case 1. It describes how the user can undo use case 1, if he no longer wishes to see chosen language's metamodel. If language's button is colored red, it indicates that the language is chosen and can now be unchosen. If the user clicks the button with langauges name, SAM stops displaying that languages metamodel and constructs if constructs were shown to the user. Button with languages name colors back to green indicating that this language is currently not chosen and can be chosen if the user wishes to.

Table 6: Use Case 2: Remove modelling language from chosen languages.

Use Case Id	**UC-2**
Goal number	-
Use Case Name	Remove modelling language from chosen languages.
Actors	1. User 2. SAM
Trigger	User wishes to remove previously chosen modelling language.
Preconditions	User has chosen at least one modelling language.
Postconditions	Modelling language's metamodel is no longer displayed to the user. Button with language's name is green.
Normal flow	1. User decides which language to unchoose. 2. User clicks on red button with languages name. 3. SAM stops displaying language's metamodel on the screen. 4. SAM changes language's button with language's name color to green.

Use case 3 is described in Table 7. This use case shows how the user can see all modelling language's constructs that are aligned to ISSRM domain model asset-related concepts. This use case helps to satisfy TROPOS model goals HG1 and HG4. For simplicity the user can see all constructs that are aligned to one or more asset-related concepts with a click of a single button. The only precondition for this is that atleast one modelling language is chosen (its metamodel is shown to the user). After clicking the "Select Asset-related" button, all elements of modelling language metamodel, that are aligned to asset-related concept are highlighted. Different concepts are colored differently. If one construct can be used for representing multiple ISSRM domain mode concepts, its metamodel representation is colored with multiple colors. Graphical representations of modelling constructs are displayed to the user for all highlighted constructs.

Table 7: Use Case 3: See constructs used for representing asset-related concepts.

Use Case Id	**UC-3**
Goal number	**HG1, HG4**
Use Case Name	See constructs used for representing asset-related concepts.
Actors	1. User 2. SAM
Trigger	User wishes to see all constructs used for representing asset-related ISSRM domain model concepts.
Preconditions	User has selected at least one modelling language.
Postconditions	1. Chosen language's metamodel constructs which are aligned with asset-related ISSRM domain model concepts are colored. 2. Graphical representations of all colored constructs are displayed to the user. 3. All asset-related concept names in legend are colored green.
Normal flow	1. User clicks "Select Asset-related" button. 2. SAM colors all elements of chosen language's metamodel(s), that are aligned to one or more asset-related ISSRM domain model concept(s). 3. SAM changes color of text "Business asset" in legend to green. 4. SAM changes color of text "System asset" in legend to green. 5. SAM changes color of text "Security Criterion" in legend to green. 6. SAM displays graphical representations of all highlighted metamodel elements.

Use case 4 is described in Table 8. This use case shows how the user can see all modelling language's constructs that are aligned to ISSRM domain model risk-related concepts. This use case also helps to satisfy TROPOS model goals HG1 and HG4. Similarly to selecting asset-related concepts, all risk-related concepts can be seen with a click of a single button as well. The precondition that atleast one modelling language is chosen applies for this use case as well. After clicking the "Select Risk-related" button, all elements of modelling language metamodel, that are aligned to risk-related concept are highlighted. Different concepts are colored differently. If one construct can be used for representing multiple ISSRM domain mode concepts, its metamodel representation is colored with multiple colors. Graphical representations of modelling constructs are displayed to the user for all highlighted constructs.

Table 8: Use Case 4: See constructs used for representing risk-related concepts.

Use Case Id	**UC-4**
Goal number	**HG1, HG4**
Use Case Name	See constructs used for representing risk-related concepts.
Actors	1. User 2. SAM
Trigger	User wishes to see all constructs used for representing risk-related ISSRM domain model concepts.
Preconditions	User has selected at least one modelling language.
Postconditions	1. Chosen language's metamodel constructs which are aligned with risk-related ISSRM domain model concepts are colored. 2. Graphical representations of all colored constructs are displayed to the user. 3. All risk-related concept names in legend are colored green.
Normal flow	1. User clicks "Select Risk-related" button. 2. SAM colors all elements of chosen language's metamodel(s), that are aligned to one or more risk-related ISSRM domain model concept(s). 3. SAM changes color of text "Risk" in legend to green. 4. SAM changes color of text "Event" in legend to green. 5. SAM changes color of text "Impact" in legend to green. 6. SAM changes color of text "Threat" in legend to green. 7. SAM changes color of text "Vulnerability" in legend to green. 8. SAM changes color of text "Threat Agent" in legend to green. 9. SAM changes color of text "Attack method" in legend to green. 10. SAM displays graphical representations of all highlighted metamodel elements.

Use case 5 is described in Table 9. This use case shows how the user can see all modelling language's constructs that are aligned to ISSRM domain model risk treatment-related concepts. This use case satisfies TROPOS model goals HG1 and HG4. With a click of one button, the user can see constructs aligned to every risk treatment-related concept. Atleast one modelling language must be chosen in order to start this use case. After clicking the "Select Risk Treatment-related" button, all elements of modelling language metamodel, that are aligned to risk treatment-related concepts are highlighted. Different concepts are colored differently. If one construct can be used for representing multiple ISSRM domain mode concepts, its metamodel representation is colored with multiple colors. Graphical representations of modelling constructs are displayed to the user for all highlighted constructs.

Table 9: Use Case 5: See constructs used for representing risk treatment-related concepts.

Use Case Id	**UC-5**
Goal number	**HG1, HG4**
Use Case Name	See constructs used for representing risk treatment-related concepts.
Actors	1. User 2. SAM
Trigger	User wishes to see all constructs used for representing risk treatment-related ISSRM domain model concepts.
Preconditions	User has selected at least one modelling language.
Postconditions	1. Chosen language's metamodel constructs which are aligned with risk treatment-related ISSRM domain model concepts are colored. 2. Graphical representations of all colored constructs are displayed to the user. 3. All risk treatment-related concept names in legend are colored green.
Normal flow	1. User clicks "Select Risk Treatment-related" button. 2. SAM colors all elements of chosen language's metamodel(s), that are aligned to one or more risk treatment-related ISSRM domain model concept(s). 3. SAM changes color of text "Risk Treatment" in legend to green. 4. SAM changes color of text "Security Requirement" in legend to green. 5. SAM changes color of text "Control" in legend to green. 6. SAM displays graphical representations of all highlighted metamodel elements.

Use case 6 is described in Table 10. Use case 6 helps the user satisfy goals HG1 and HG3. Precondition for this use case is that atleast one modelling language is chosen by the user and its metamodel is displayed to the user. When user clicks on construct in metamodel, a list of all ISSRM domain model concepts that are aligned to that construct is displayed. When user selects and clicks on one ISSRM domain model concept from list, all constructs aligned to that concept are colored in displayed metamodel. Graphical representations of modelling constructs are displayed to the user for all highlighted metamodel constructs. Concept name is colored green in legend indicating that concept's alignments are shown to the user.

Table 10: Use Case 6: Select ISSRM concept for language construct.

Use Case Id	**UC-6**
Goal number	**HG1, HG3**
Use Case Name	See constructs used for representing risk treatment-related concepts.
Actors	1. User 2. SAM
Trigger	User wishes to select an ISSRM domain model concept aligned to modelling language construct.
Preconditions	User has selected at least one modelling language.
Postconditions	1. Chosen language's metamodel constructs which are aligned to selected concept are colored. 2. Graphical representations of all colored constructs are displayed to the user. 3. Selected concept name in legend is colored green.
Normal flow	1. User clicks on modelling language construct in metamodel. 2. SAM displays all ISSRM concepts that are aligned to that construct. 3. User clicks on an ISSRM domain model concept. 4. SAM colors all constructs aligned to concept selected in step 3. 5. SAM changes color of concept name in legend to green. 6. SAM displays graphical representations of all highlighted metamodel elements.

Table 11 describes use case 7. Use case 7 describes the interactions that help the user to satisfy goals HG1 and HG4. Precondition for this use case is that atleast one modelling language is chosen by the user. In order to see all constructs that are aligned to specific ISSRM domain model concept the user can click on concept's name. Clicking on the concept's name selects the concept and all metamodel constructs that are aligned to selected concept are colored. Metamodel construct color matches the color shown to the user in legend. When an ISSRM domain model concept is selected, its name is colored green. If the concept is not selected its name is displayed to the user with black color.

Table 11: Use Case 7: See modelling language constructs that can represent ISSRM domain model concept.

Use Case Id	**UC-7**
Goal number	**HG1, HG4**
Use Case Name	See modelling language constructs that can represent ISSRM domain model concept.
Actors	1. User 2. SAM
Trigger	User wishes to choose an ISSRM domain model concept and see all modelling language's constructs aligned to it.
Preconditions	1. User has selected at least one modelling language. 2. The ISSRM domain model concept user wants to see aligned constructs for is not already shown to the user.
Postconditions	1. Chosen language's metamodel constructs which are aligned to user chosen ISSRM domain model concept are colored. 2. Graphical representations of all colored modelling language constructs are displayed to the user. 3. Selected concept name in legend is colored green.
Normal flow	1. User clicks on ISSRM domain model concept name in legend. 2. SAM colors all constructs aligned to selected concept. 3. SAM changes color of concept name in legend to green. 4. SAM displays graphical representations of all highlighted metamodel elements.

Table 12 describes use case 8. UC-8 desribe two flows how the user can deselect an ISSRM domain model concept. Preconditions for both flows are that modelling language's metamodel is displayed and atleast one ISSRM domain model concept is selected. First way to deselect ISSRM domain model concept is to click on its name in legend. Second way is to click on modelling language construct that is aligned to that concept. Then a list of all aligned concepts is shown to the user. If user clicks on the selected concept's name, then the concept is deselected. Postconditions for both flows are the same: Deselected concept name is displayed as black colored text. Metamodel constructs are no longer colored with the color representing that ISSRM domain model concept. If no ISSRM domain model concepts are selected any more then all constructs are colored white. If all constructs are colored white then no graphical representations of modelling constructs are displayed to the user, if some constructs are highlighted(colored) in metamodel then graphical representations for those constructs are still displayed to the user.

Table 12: Use Case 8: Deselect ISSRM domain model concept.

Use Case Id	**UC-8**
Goal number	-
Use Case Name	Deselect ISSRM domain model concept.
Actors	1. User 2. SAM
Trigger	User no longer wishes to see language construct that are aligned to domain mode concept.
Preconditions	1. User has selected at least one modelling language. 2. User has selected at least one ISSRM domain model concept.
Postconditions	1. Alignment to deselected ISSRM domain model concept is no longer displayed to the user. 2. Deselected concept name in legend is colored black.
Normal flow	1. User clicks on ISSRM domain model concept name in legend. 2. SAM removes color related to ISSRM domain model concept from metamodel construct. 3. SAM changes color of concept name in legend to black.
Alternative flow	1. User clicks on modelling language construct in metamodel. 2. SAM displays all ISSRM domain model concepts aligned to clicked construct. 3. User clicks on ISSRM domain model concept. 4. SAM removes color related to ISSRM domain model concept from metamodel construct. 5. SAM changes color of concept name in legend to black.

3.2.3 Mockups

In addition to functional aspects of the tool, user interface is designed for the tool as well. Figure 4 shows how the tool would look like once implemented. On the left upper part of the screen the buttons for choosing and unchoosing modelling languages are located. Bottom left part of the screen (legend part) lists all ISSRM domain model concepts. Colored boxes show what color is used for representing that concept. If concept text is green it means that the concept is active, unactive concepts are marked with black text. Since all buttons and concepts don't fit to the screen, the left pane is scrollable. Right top part of the window is where languages' metamodels are located. Constructs aligned to active concepts are colored respectfully. Bottom right part of window is dedicated for icons.

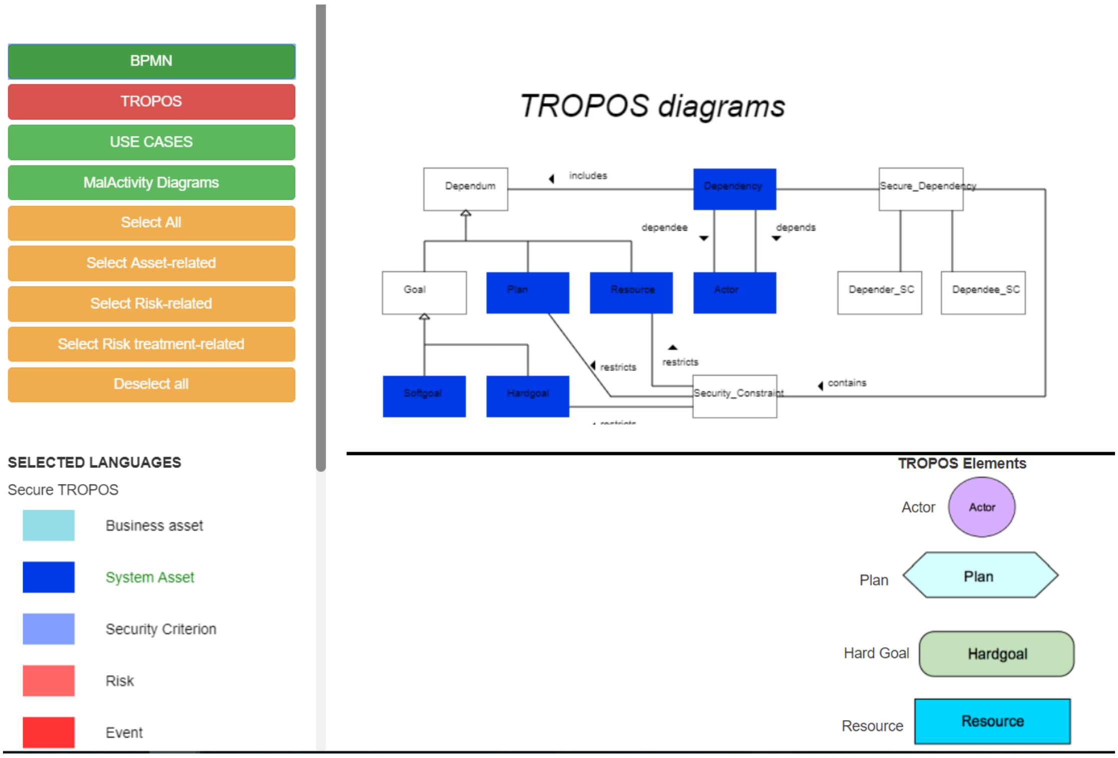

Figure 4: Tool to be developed

3.2.4 Rules for Risk-Related Concepts

In ISSRM domain model some risk related concetps are combinations of its sub-concepts. Risk is combination of event and impact, event is combination of threat and vulnerability, vulnerability is combination of attack method and threat agent. This means that in order for the risk to exist, event and impact must be present. We want our tool to adhere to this condition as well. So rules which risk related concepts must be selected or deselected, when any risk related concept is selected/deselected by user were created. Rules are following.

1. When user selects risk concept, then risk, event, impact, threat, vulnerability, threat agent and attack method concepts are shown to the user.

2. When user deselects risk concept, then risk, event, impact, threat, vulnerability, threat agent and attack method concepts are deselected.

3. When user selects event concept, then event, threat, vulnerability, threat agent and attack method concepts are shown to user as well. If impact was previously selected, then risk concept is selected as well.

4. When user deselects event concept, then risk, event, threat, vulnerability, threat agent and attack method are deselected. Impact selection is not changed.

5. When user selects impact concept, then impact is show to the user and if event was previously selected, then risk is selected as well.

6. When user deselects impact, then impact and risk are both deselected.

7. When user selects threat concept, then threat, threat agent and attack method concepts are selected. If only vulnerability was previously selected then event is also selected. If vulnerability and impact were both previously selected then risk and event are selected as well.

8. When user deselects threat concept, then theat, threat agent and attack method concepts are also deselected. If vulnerability was previously selected, then event is deselected. If vulnerability and impact were both previously selected then event and risk concepts are deselected as well.

9. When user selects vulnerability concept, then vulnerability concept is shown to the user. If threat was previously selected then event is also shown. If threat and impact were both previously selected then event and risk are shown.

10. When user deselects vulnerability concept, then event and risk concepts are deselected.

11. When user selects threat agent concept, then threat agent concept is shown to the user. If attack method was previously selected, then threat is also shown to the user. If attack method and vulnerability were previously selected then threat and event concepts are shown to the user as well. If attack method, vulnerability and impact were all previously selected then risk, event and threat concepts are shown to the user.

12. When user deselects threat agent concept, then threat, event and risk concepts are deselected.

13. When user selects attack method concept, then attack method is shown to the user. If threat agent was previously selected, then threat is also shown. If threat agent and vulnerability were both previously selected then threat and event are shown. If threat agent, vulnerability and impact were all previously selected then risk, event and threat are shown.

14. When user deselects attack method concept, then threat, event and risk are deselected.

3.2.5 Functional Requirements

Models, mockups and requirements scenarios are basis for written system requirements. Previous chapters' models, scenarios and mockups result in following functional requirements. Requirements are ordered by scenarios ordering. If same functional requirement applies for multiple scenarios, it is listed only in first use case it applies to and is not duplicated under requirements for later scenarios.

1. UC-1 See modelling language metamodel

1.1. If BPMN modelling language is not chosen, green button with language's name is shown to the user.

1.2. If Secure TROPOS modelling language is not chosen, green button with language's name is shown to the user.

1.3. If Misuse cases modelling language is not chosen, green button with language's name is shown to the user.

1.4. If Malactivity diagrams modelling language is not chosen, green button with language's name is shown to the user.

1.5. If BPMN modelling language is added to chosen languages, its metamodel is displayed.

1.6. If Secure TROPOS modelling language is added to chosen languages, its metamodel is displayed.

1.7. If Misuse cases modelling language is added to chosen languages, its metamodel is displayed.

1.8. If Malactivity diagrams modelling language is added to chosen languages, its metamodel is displayed.

2. UC-2 Remove modelling language from chosen languages

2.1. If BPMN modelling language is chosen, red button with language's name is shown to the user.

2.2. If Secure TROPOS modelling language is chosen, red button with language's name is shown to the user.

2.3. If Misuse cases modelling language is chosen, red button with language's name is shown to the user.

2.4. If Malactivity diagrams modelling language is chosen, red button with language's name is shown to the user.

2.5. If BPMN modelling language is removed from chosen languages, its metamodel is no longer displayed.

2.6. If Secure TROPOS modelling language is removed from chosen languages, its metamodel is no longer displayed.

2.7. If Misuse cases modelling language is removed from chosen languages, its metamodel is no longer displayed.

2.8. If Malactivity diagrams modelling language is removed from chosen languages, its metamodel is no longer displayed.

3. UC-3 See constructs used for representing asset-related concepts

3.1. Button for selecting all ISSRM domain model concepts is displayed to the user.

3.2. Button for selecting all asset-related ISSRM domain model concepts is displayed to the user.

3.3. When button for selecting all ISSRM domain model concepts is clicked, all ISSRM domain model concept names are colored green.

3.4. When button for selecting all asset-related ISSRM domain model concepts is clicked, all asset-related ISSRM domain model concept names are colored green.

3.5. When button for selecting all asset-related ISSRM domain model concepts is clicked, all non asset-related ISSRM domain model concept names are colored black.

4. UC-4 See constructs used for representing risk-related concepts

4.1. Button for selecting all risk-related ISSRM domain model concepts is displayed to the user.

4.2. When button for selecting all risk-related ISSRM domain model concepts is clicked, all risk-related ISSRM domain model concept names are colored green.

4.3. When button for selecting all risk-related ISSRM domain model concepts is clicked, all non risk-related ISSRM domain model concept names are colored black.

5. UC-5 See constructs used for representing risk treatment-related concepts

5.1. Button for selecting all risk treatment -related ISSRM domain model concepts is displayed to the user.

5.2. Button for deselecting all ISSRM domain model concepts is displayed to the user.

5.3. When button for selecting all risk treatment-related ISSRM domain model concepts is clicked, all risk treatment-related ISSRM domain model concept names are colored green.

5.4. When button for selecting all risk treatment-related ISSRM domain model concepts is clicked, all non risk treatment-related ISSRM domain model concept names are colored black.

  - **5.5.** When button for deselecting all ISSRM domain model concepts is clicked, all ISSRM domain model concept names are colored black.

6. UC-6 Select ISSRM concept for language construct

  - **6.1.** Language constructs in metamodel must be clickable.
  - **6.2.** When metamodel construct is clicked, list of all aligned ISSRM domain model concepts must be displayed to the user.
  - **6.3.** Already selected concepts are marked in the displayed list with checked mark.
  - **6.4.** Concepts not selected are marked in the displayed list without checked mark.
  - **6.5.** Clicking on unselected concept from the list selects the concept.
  - **6.6.** Clicking on selected concept from the list deselects the concept.
  - **6.7.** Metamodel elements aligned to selected ISSRM domain model concepts are colored with same colors are shown in legend part next to concept name.
  - **6.8.** All ISSRM domain model concepts are highlighted with different color.
  - **6.9.** ISSRM domain concepts must be highlighted with same color in all languages' metamodels.
  - **6.10.** Icons representing highlighted constructs must be displayed to the user.
  - **6.11.** If one icon is used for multiple concepts, it is displayed only once.
  - **6.12.** Metamodel elements not aligned to selected ISSRM domain model concepts have white background.
  - **6.13.** Disabling concept affects all chosen languages' metamodels.

7. UC-7 See modelling language constructs that can represent ISSRM domain model concept

  - **7.1.** Clicking on unselected concept name in legend selects that concept.
  - **7.2.** All selected ISSRM domain model concepts' names are displayed with green text.

8. UC-8 Deselect ISSRM domain model concept

  - **8.1.** Clicking on selected concept name in legend deselects that concept.
  - **8.2.** All deselected ISSRM domain model concepts' names are displayed with black text.

3.2.6 Non-Functional Requirements

1. After inital application startup, on averate selecting and deselecting concepts should not take more than half a second.

2. Application must be available throughout the day.

3. Application must be usable using Google Chrome version Version 66.0.3359.181.

4. Application must support 50 concurrent users.

3.3 Summary

In this chapter we answered research question 2 "What are the requirements for tool to help the users learn alignment to ISSRM domain model concepts and transformations between secure modelling langauges?". We gave an overview of the solution to be developed. Analysed users needs and goals and based on identified goals created use case scenarios and set functional and non-functional requirements. In the next chapter we are going to concentrate on validating the solution described in this chapter.

4 Validation

This chapter focuses on answering research questions 3 "How easy is to learn modelling language alignment to ISSRM domain model concepts using the proposed solution?" and 4 "How easy is to learn transformations between secure modelling languages with help from tool which shows alignments to ISSRM domain model concepts?". Chapter starts with describing the validation process and talks in detail about results collected during the validation process. Results are analysed and discussed. Validation chapter ends with identifying threats to done validation.

4.1 Description of the Validation Process

This chapter describes the validation process of created tool. Since the tool was designed to be used for learning purposes in courses, that teach ISSRM domain model and modelling using security risk-oriented languages, it was decided that the validation of the tool will be done in a form of a questionnaire given to students of "Principles of Secure Software Design" course. It was decided that the tool will be introduced in one of the courses seminars.

First a short demo was done by the author to the students showing which languages are supported by the tool. Author also showed the process of how the tool can be used to see language construct mappings to ISSRM domain model concepts and how to see which constructs can be used to represent ISSRM domain model concepts. After this demo a short questionnaire (questionnaire 1) with 20 questions was given to the students. Questionnaire 1 had 4 sections, one for each modelling language(BPMN, secure TROPOS, misuse cases, mal-activity diagrams), for every language the questionnaire had 5 questions. Questions asked which language constructs could be used in a language to represent some ISSRM domain model concept. The students were given 15 minutes to answer all the questions with help from using the tool. After 15 minutes had passed all questions in the questionnaire were discussed and explained how the students could have used the tool to get right answers.

Then another demo was done showing how students could benefit from the tool when they need to transform from one modelling language to another, while keeping the security aspects intact. After the demo another questionnaire (questionnaire 2) was given to the students. Questionnaire 2 consisted of 3 sections, each section had 5 questions. Questions were about how to transform security enhanced model from one modelling language to another. Once again the students were given 15 minutes to answer the questionnaire with help from tool. After 15 minutes had passed all the questions in the questionnaire were discussed and explained how the students could have used the tool to get the right answers.

After this third questionnaire was given to the students of the course. The third questionnaire asked for students feedback about the tool. In the next chapter we describe in detail the questions and responses collected from the students for the third questionnaire.

4.2 Feedback Questionnaire

After process described in previous chapter the students were given third questionnaire, that gathered feedback about whether the students found that SAM fulfilled its purpose and how much did SAM help them to see language mappings and help with understanding transformations between security risk-oriented modelling languages.

The questionnaire consisted of 24 questions. Six questions for each language supported by the tool(BPMN, secure TROPOS, misuse cases, mal-activity diagrams). The questionnaire was open for students from 22.03.2018 until 29.03.2018. In total 32 students answered the feedback questionnaire. Seven answers from the questionnaire were left out from analysation process. These seven responses were not analyzed, because the answers to all the questions was same throughout the entire questionnaire. It is probable to assume that those students just answered the questionnaire because it was required from them by the teacher and did not try to give real feedback and just chose the default answer to all questions. So only 25 questionnaire results are described in this chapter.

First question "How easy is to understand language constructs alignment to ISSRM domain model concept using the tool?" focused on getting student feedback about the understandability of the tool regarding alignments between language constructs and ISSRM domain model concepts. This question was asked for all chosen languages separately. For BPMN 64 % of the answered students found it rather easy or very easy to understand the alignment, 16 % found it moderate and 20 % rather difficult. Figure 5 shows how the answers were distributed. For Secure TROPOS 44 % of the answered students found it rather easy or very easy to understand the alignment, 28 % found it moderate and 28 % rather difficult or very difficult. Figure 6 shows how the answers were distributed. For Misuse cases 56 % of the answered students found it rather easy or very easy to understand the alignment, 32 % found it moderate and 12 % rather difficult. Figure 7 shows how the answers were distributed. For Malactivity diagrams 56 % of the answered students found it rather easy or very easy to understand the alignment, 28 % found it moderate and 16 % rather difficult or very difficult. Figure 8 shows how the answers were distributed.

Second question was "How easy is to learn language constructs alignment to ISSRM domain model concept using the tool?". This question was also asked for all chosen languages separately. For BPMN 40 % of the answered students found it rather easy or very easy to learn the alignment, 28 % found it moderate and 32 %

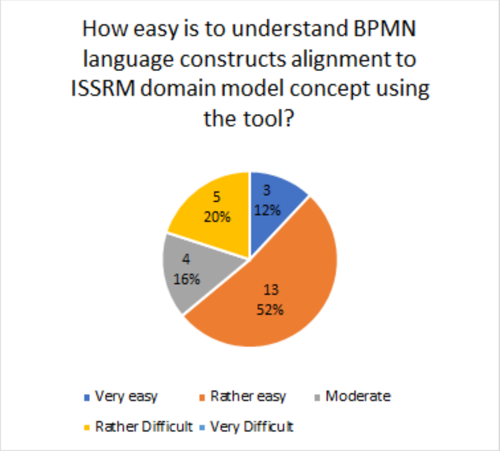

Figure 5: How easy is to understand BPMN language constructs alignment to ISSRM domain model concept using the tool?

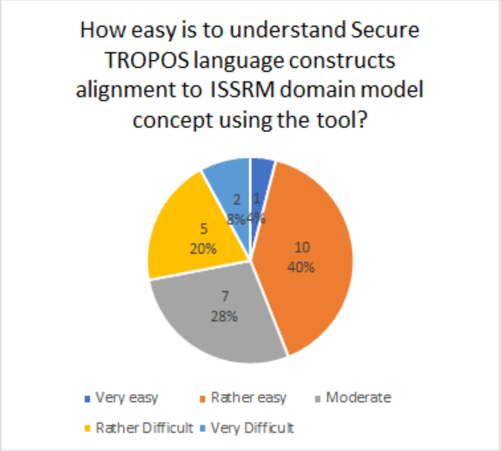

Figure 6: How easy is to understand Secure TROPOS language constructs alignment to ISSRM domain model concept using the tool?

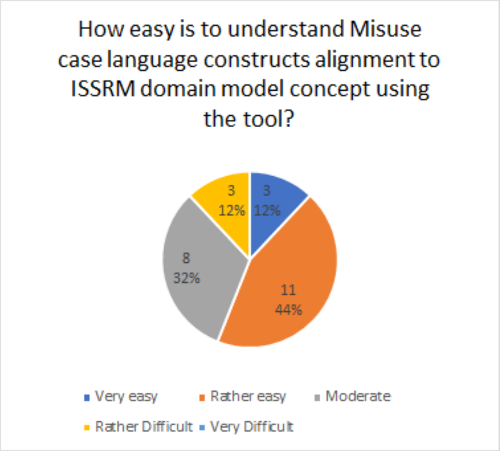

Figure 7: How easy is to understand Misuse case language constructs alignment to ISSRM domain model concept using the tool?

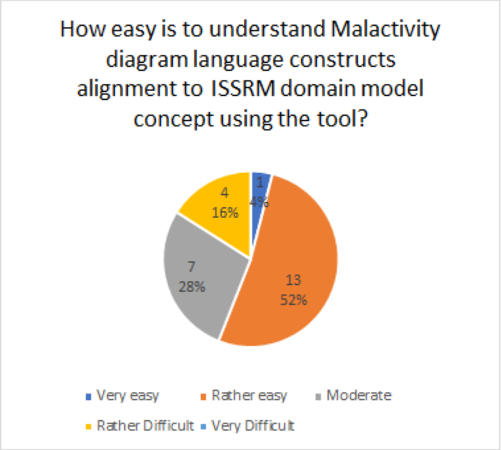

Figure 8: How easy is to understand Malactivity diagram language constructs alignment to ISSRM domain model concept using the tool?

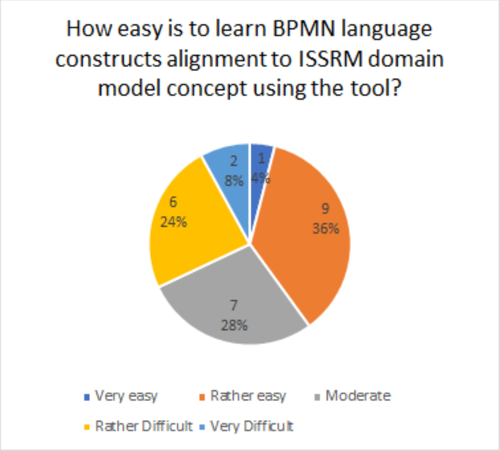

Figure 9: How easy is to learn BPMN language constructs alignment to ISSRM domain model concept using the tool?

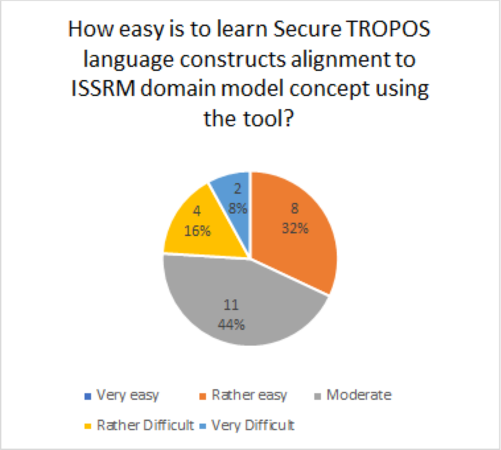

Figure 10: How easy is to learn Secure TROPOS language constructs alignment to ISSRM domain model concept using the tool?

rather difficult or very difficult. Figure 9 shows how the answers were distributed. For Secure TROPOS 32 % of the answered students found it rather easy to learn the alignment, 44 % found it moderate and 24 % rather difficult or very difficult. Figure 10 shows how the answers were distributed. For Misuse cases 40 % of the answered students found it rather easy or very easy to learn the alignment, 44 % found it moderate and 16 % rather difficult. Figure 11 shows how the answers were distributed. For Malactivity diagrams 32 % of the answered students found it rather easy or very easy to learn the alignment, 48 % found it moderate and 20 % rather difficult. Figure 12 shows how the answers were distributed.

Third question was "How easy is to remember language constructs alignment to ISSRM domain model concept using the tool?". Like previous questions this question was also asked for all chosen languages separately. For BPMN 28 % of the answered students found it rather easy or very easy to remember the alignment to ISSRM domain model, 44 % found it moderate and 28 % rather difficult or very difficult. Figure 13 shows how the answers were distributed. For Secure TROPOS 36 % of the answered students found it rather easy to remember the alignment to ISSRM domain model, 36 % found it moderate and 28 % rather difficult or very difficult. Figure 14 shows how the answers were distributed. For Misuse cases 36 % of the answered students found it rather easy or very easy to remember the alignment, 44 % found it moderate and 20 % rather difficult or very difficult. Figure 15 shows how the answers were distributed. For Malactivity diagrams 24 % of the answered students found it rather easy or very easy to remember the alignment to ISSRM domain model, 52 % found it moderate and 24 % of the students found it

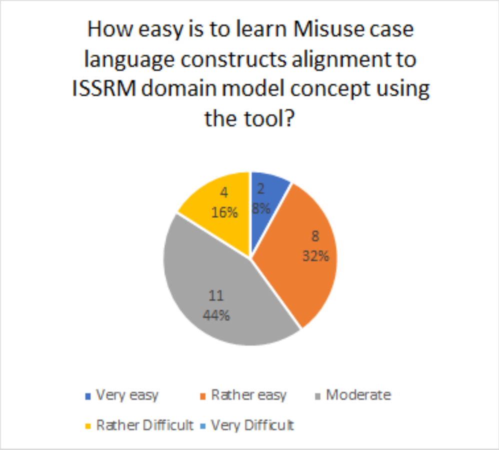

Figure 11: How easy is to learn Misuse case language constructs alignment to ISSRM domain model concept using the tool?

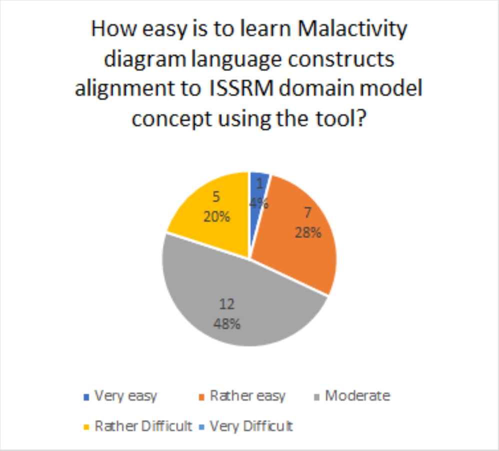

Figure 12: How easy is to learn Malactivity diagram language constructs alignment to ISSRM domain model concept using the tool?

rather difficult or very difficult. Figure 16 shows how the answers were distributed.

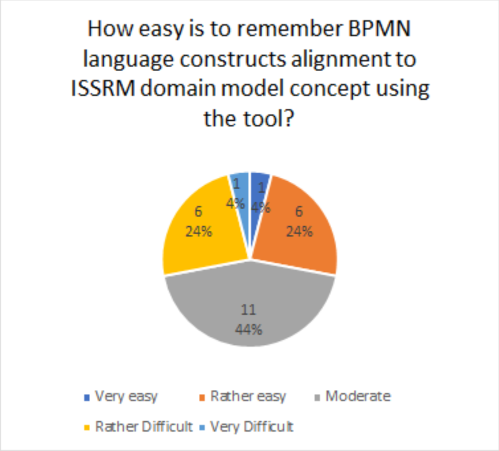

Figure 13: How easy is to remember BPMN language constructs alignment to ISSRM domain model concept using the tool?

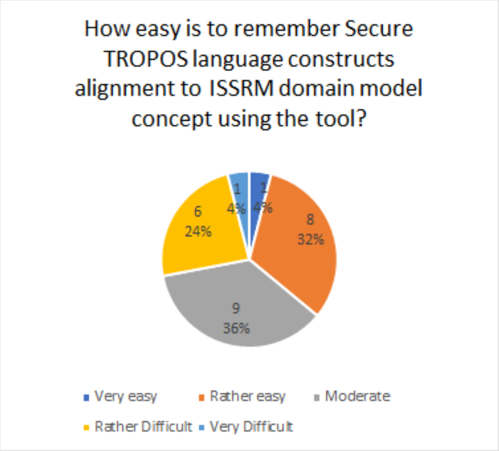

Figure 14: How easy is to remember Secure TROPOS language constructs alignment to ISSRM domain model concept using the tool?

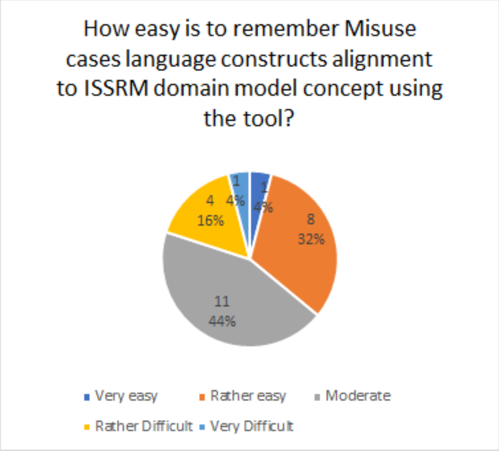

Figure 15: How easy is to remember Misuse case language constructs alignment to ISSRM domain model concept using the tool?

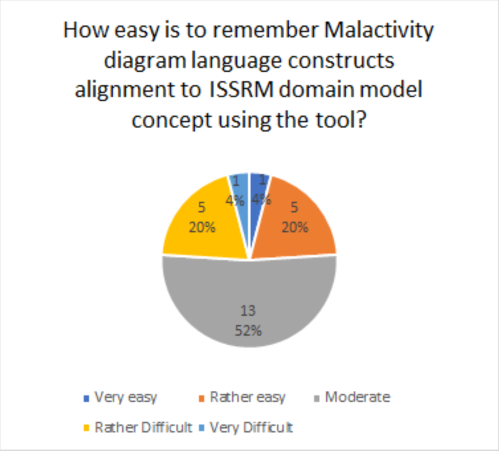

Figure 16: How easy is to remember Malactivity diagram language constructs alignment to ISSRM domain model concept using the tool?

Fourth question was "How easy is to understand transformations from one language to another with help from the tool?". This question was in 3 different forms. Using the tool made understanding transformations from BPMN to Secure TROPOS rather easy or very easy for 52 % of the students, 20 % found it moderate and 28 % rather difficult. Figure 17 shows how the answers were distributed. Understanding transformations from Secure TROPOS to Misuse cases was rather easy or very easy for 48 % of the answered students, 24 % found it moderate and 28 % rather difficult. Figure 18 shows how the answers were distributed. Transformations from Misuse cases to Malactivity diagrams were rather easy or very easy to understand for 48 % of the answered students, 24 % of the students found it moderate and 28 % rather difficult. Figure 19 shows how the answers were distributed.

Fifth question was "How easy is to learn transformations from one language to another with help from the tool?". This question was also asked for 3 types of transformations between languages. Using the tool made understanding transformations from BPMN to Secure TROPOS rather easy or very easy for 32 % of the students, 48 % found it moderate and 20 % very difficult or rather difficult. Figure 20 shows how the answers were distributed. Understanding transformations from Secure TROPOS to Misuse cases was rather easy or very easy for 44 % of the answered students, 36 % found it moderate and 20 % rather difficult. Figure 21 shows how the answers were distributed. Transformations from Misuse cases to Malactivity diagrams were rather easy or very easy to understand for 36 % of the answered students, 40 % of the students found it moderate and 24 % rather difficult. Figure 22 shows how the answers were distributed.

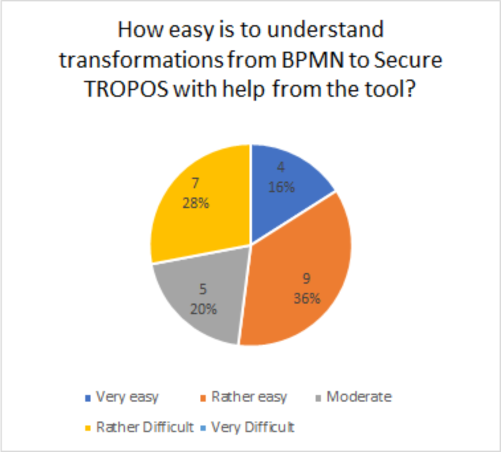

Figure 17: How easy is to understand transformations from BPMN to Secure TROPOS with help from the tool?

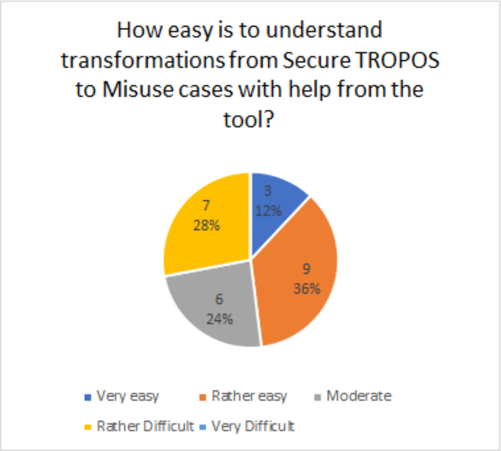

Figure 18: How easy is to understand transformations from Secure TROPOS to Misuse cases with help from the tool?

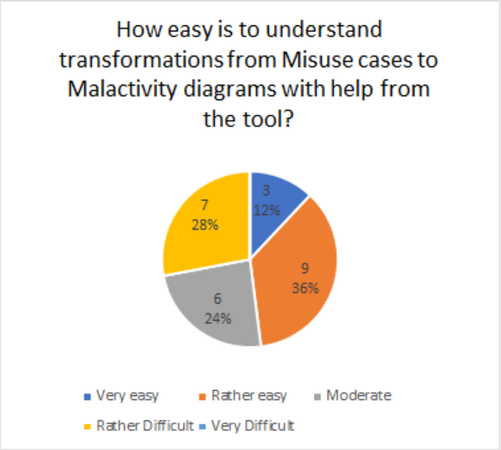

Figure 19: How easy is to understand transformations from Misuse cases to Malactivity diagrams with help from the tool?

Sixth question was "How easy is to remember transformations from one language to another with help from the tool?". This question was also asked for 3 types of transformations between languages. Using the tool made understanding transformations from BPMN to Secure TROPOS rather easy for 24 % of the students, 56 % found it moderate and 20 % rather difficult. Figure 23 shows how the

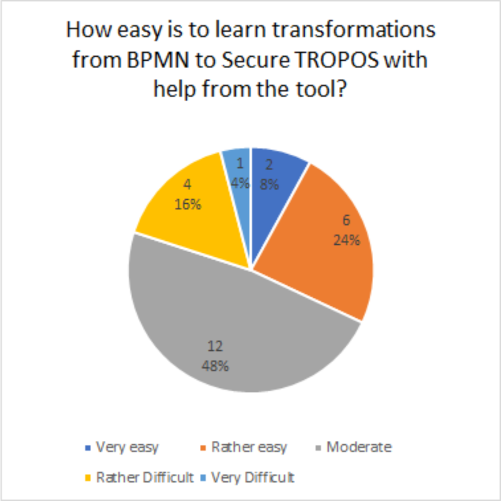

Figure 20: How easy is to learn transformations from BPMN to Secure TROPOS with help from the tool?

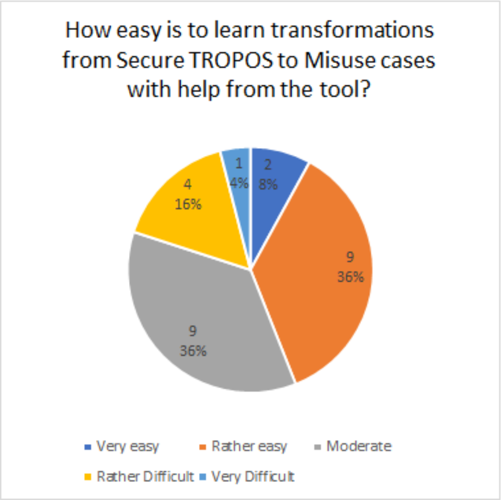

Figure 21: How easy is to learn transformations from Secure TROPOS to Misuse cases with help from the tool?

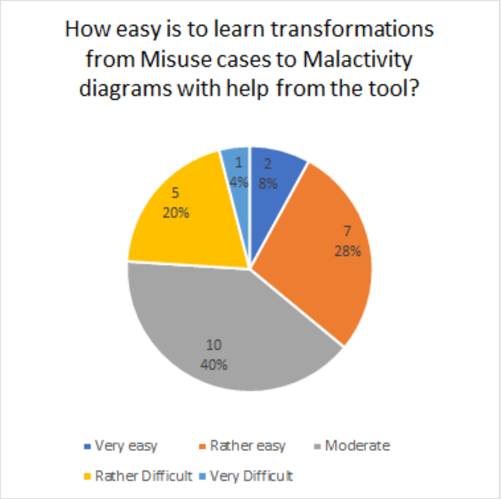

Figure 22: How easy is to learn transformations from Misuse cases to Malactivity diagrams with help from the tool?

answers were distributed. Understanding transformations from Secure TROPOS to Misuse cases was rather easy for 24 % of the students, 52 % found it moderate and 24 % rather difficult. Figure 24 shows how the answers were distributed. Transformations from Misuse cases to Malactivity diagrams were rather easy to understand for 24 % of the students who answered the questionnaire, 48 % of the students found it moderate and 28 % rather difficult. Figure 25 shows how the answers were distributed.

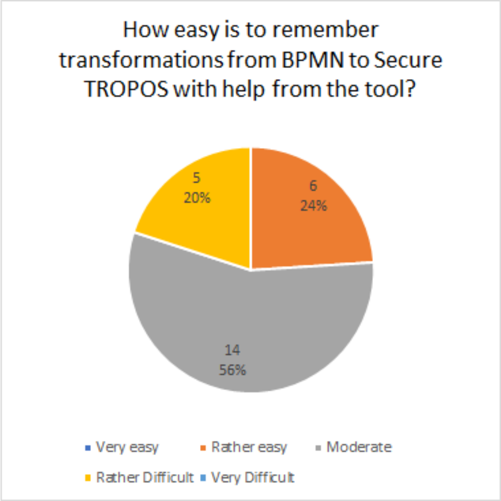

Figure 23: How easy is to remember transformations from BPMN to Secure TROPOS with help from the tool?

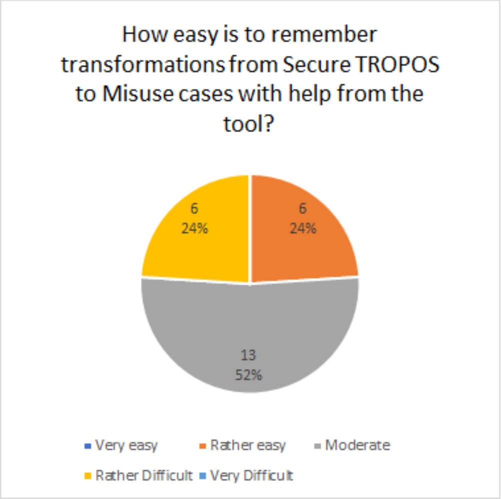

Figure 24: How easy is to remember transformations from Secure TROPOS to Misuse cases with help from the tool?

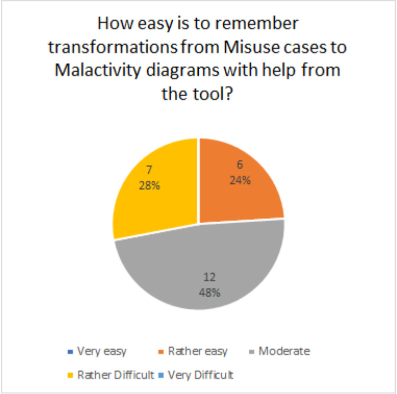

Figure 25: How easy is to remember transformations from Misuse cases to Malactivity diagrams with help from the tool?

4.3 Discussion

For the validation of the tool the feedback questionnaire is analyzed and midterm exam results for exercises regarding alignment between language constructs and ISSRM domain model concepts and transformations between modelling languages are observed as well. Same 25 questionnaire responses looked into in the previous chapter were chosen again. From the midterm exam all 50 exam results were taken.

In order to get statistical parameters such as mean and standard deviation, the responses were transformed from text to numerical values in increasing order of difficulty. Label "Very easy" was mapped changed to 1, "Rather easy" to 2, "Moderate" to 3, "Rather difficult" to 4 and "Very difficult" was marked as 5. Questions 1-3 of third questionnaire asked for feedback about understandability, learnability and rememberability of alignments between ISSRM domain model concepts and modelling language constructs. Means and standard deviations for third questionnaire questions 1-3 are illustrated in table 13. Green cells indicate below moderate results(under 3) and blue cells mark where average was equal to moderate difficulty.

Question	BPMN		Secure TROPOS		Misuse cases		Malactivity diagrams	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
How easy is to understand language constructs alignment to ISSRM domain model concept using the tool?	2,44	0,96	2,88	1,05	2,44	0,87	2,56	0,82
How easy is to learn language constructs alignment to ISSRM domain model concept using the tool?	2,96	1,06	3	0,91	2,68	0,85	2,84	0,8
How easy is to remember language constructs alignment to ISSRM domain model concept using the tool?	3	0,91	2,92	0,95	2,84	0,9	3	0,87

Table 13: Means and standard deviations for feedback questions 1-3.

Taken from the students feedback average difficult of understanding language construct alignment to ISSRM domain model concept with tool's help was below moderate for all languages. For BPMN the average was 2,44 with standard deviation of 0,96, average for Secure TROPOS was 2,88 with standard deviation of 1,05, respective numbers for Misuse cases were 2,44 and 0,87 and average for Malactivity diagrams was 2,56 with standard deviation of 0,82. From these numbers it seems, that all alignments were rather easy to understand and Misuse cases was the easiest. Regarding learning alignments between language constructs and ISSRM domain model concepts BPMN average was 2,96 with standard deviation of 1,06. For Secure TROPOS mean was 3 and standard deviation was 0,91. Misuse cases had an average of 2,68 with standard deviation of 0,85 and Malactivity diagrams had an average of 2,84 with standard deviation of 0,8. Easiness of remembering BPMN language construct alignment to ISSRM domain model concept was assessed by the students with average of 3 and standard deviation of 0,91. For Secure TROPOS the indicators were 2,92 and 0,95. Misuse cases had an average easiness of 2,84 with standard deviation of 0,9 and Malactivity diagrams had and average easiness of 3 with standard deviation of 0,87.

From feedback questions it appears that the easiest language for the students to understand, learn and remember alignments between constructs and concepts was Misuse cases and hardest was secure TROPOS, the midterm exam results confirm that. Average score for Misuse cases alignment related questions from the midterm was 1,07, second best was BPMN with score of 0,92, followed by Malactivity diagrams (0,71) and lowest points were received for exercises about Secure TROPOS.

Questions 4-6 asked for feedback about understandability, learnability and rememberability of transforming from one modelling language to another after using SAM. Means and standard deviations for questions 4-6 are illustrated in table 14.

Students feedback for easiness of understanding transformatios between languages was the following. Average easiness for understanding transformations from BPMN to Secure TROPOS with the help of tool was 2,6 with standard deviation of 1,08. Mean for transformations from Secure TROPOS to Misuse cases was 2,68 with standard deviation of 1,03. And for transformations from Misuse cases to Malactivity diagrams the responding measures were same as for transformation from Secure TROPOS to Misuse cases 2,68 and 1,03. Regarding learning transformations between languages, mean for BPMN to Secure TROPOS was 2,84 with standard deviation of 0,94. From secure TROPOS to Misuse cases the average was 2,72 and standard deviation was 0,98, for transformations from Misuse cases to Malactivity diagrams mean was 2,84 with standard deviation of 0,99. Easiness of remembering transformations from BPMN language to Secure TROPOS was assessed by the students with average of 2,96 (standard deviation 0,68). For transformations from Secure TROPOS to Misuse cases the average feedback was that it was moderately easy to remember(3), standard deviation was 0,71. For transformations from Misuse cases to Malactivity diagrams the mean score was

Question	BPMN to Secure TROPOS		Secure TROPOS to Misuse cases		Misuse cases to Malactivity diagrams	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
How easy is to understand transformations from one language to another with help from the tool?	2,6	1,08	2,68	1,03	2,68	1,03
How easy is to learn transformations from one language to another with help from the tool?	2,84	0,94	2,72	0,98	2,84	0,99
How easy is to remember transformations from one language to another with help from the tool?	2,96	0,68	3	0,71	3,04	0,73

Table 14: Means and standard deviations for feedback questions 4-6.

3,04 with standard deviation of 0,73. Similar to alignment related questions the tool helped better with learning and understanding than with remembering.

From feedback questions it appears that with tools help, all transformations had about the same difficulty levels. Best score were for BPMN to Secure TROPOS, followed by Secure TROPOS to Misuse cases and Misuse cases to Malactivity diagrams. In transformation related exercises in the midterm exam, the scores for transformations were almost the same as well. BPMN to secure TROPOS 1,7 points, secure TROPOS to misuse cases 1,68 points and Misuse cases to malactivity diagrams 1,75 points.

4.4 Threats to Validation

This section describes the weakpoints of validating the tool with feedback survey from the students. First threat to validation is that there was only 25 feedback questionnaire answers analyzed. That is too small of a number for statistically conclusive results for the practicality of the tool. Secondly the tool was shown to students in the middle of the semester, so that they could use it for preparing some exercise types of the exam. It was not given to them when they were starting the course and they could only use it to revise for the exam not use it while they started learning about the alignments. Most of the students answered the questionnaire shorty after the seminar course in which the tool was introduced. Probably the results would have been different, if the students had had more time to use the tool throughout the entire course.

4.5 Summary

In this chapter we described the validation process of SAM, presented the results for feedback questionnaire we used for answering research questions 3 and 4. We analysed the results of the students questionnaire and compared them to midterm exam results. Feedback questionnaire results indicate that the students benefited from using SAM and found that SAM helped them learn, understand and remember language construct alignment s to different ISSRM domain model concepts.

Regarding using the tool to support understanding, learning and remembering transformations between chosen languages the results were promising as well. The averages and standard deviations for the questions about transformations show that students found learning and understanding transformations while using the tool's support rather easy to learn and understand. The difficulty of remembering the transformations with help from the tool was around moderate.

5 Conclusion

In this thesis we researched about existing security risk-oriented modelling languages extensions such as security risk-aware secure TROPOS, security risk-oriented BPMN, security risk-oriented misuse cases and mal-activities for security risk management and their construct alignments to ISSRM domain model concepts. We designed and implemented a tool SAM to support learning and understanding these alignments and how to transform between chosen modelling languages. We introduced SAM in "Principles of Secure Software Design" course and asked for students feedback about the easiness of using the tool to learn and understand alignments and transformations. This feedback was analysed and using the analysed results SAM was validated and found to be useful in that course.

5.1 Limitations

The developed tool uses alignments proposed in research papers discussed in Chapter two, but some proposed modelling language extensions are not complete. In some modelling languages, there are ISSRM domain model concepts, that have no corresponding modelling language elements. Other current limitation of the tool is that for some ISSRM domain model concepts, a set of language constructs is shown. Since the tool currently does not provide and explain the transformation rules, additional assistance from teacher or individual research may be needed with learning the transformations.

5.2 Answers to Research Questions

In introduction we set four research questions for this thesis.

RQ1: How are secure modelling languages aligned to ISSRM domain model? To answer this question, different secure extensions of modelling languages were chosen and different research papers studied to find currently proposed alignments between ISSRM domain model and secure modelling languages.

RQ2: What are the requirements for tool to help the users learn alignment to ISSRM domain model concepts and transformations between secure modelling langauges? In Contribution chapter we created a TROPOS model for identifying the goals of users and SAM, from those goals we created use cases for satisfying those goals. From use cases functional requirements were derived. Also mockups describing the system's appearance were created.

RQ3: How easy is to learn modelling language alignment to ISSRM domain model concepts using the proposed solution? To answer this question, we created a questionnaire for students in "Principles of Secure Software Design". The questionnaire results indicated that the solution developed for this master's thesis made it rather easy for students to learn alignments between ISSRM concepts and language constructs.

RQ4: How easy is to learn transformations between secure modelling languages with help from tool which shows alignments to ISSRM domain model concepts? Answer to this question was taken from created questionnaire for students in "Principles of Secure Software Design" as well. The questionnaire results indicated that the solution developed for this master's thesis made it rather easy for students to learn alignments between ISSRM concepts and language constructs. Easiest being transformation from Secure TROPOS to Misuse cases and a bit harder being the learning from BPMN to Secure TROPOS and from Misuse cases to Malactivity diagrams.

5.3 Conclusion

The developed solution SAM was validated by analysing feedback from students of "Principles of Secure Software Desgin" course. Results showed that SAM helped the students learn, understand and remember alignments between ISSRM domain model concepts and secure modelling language constructs. Since feedback results were promising, hopefully SAM will be used in next years course to help the students learn course topics regarding the alignments and transformations.

5.4 Future Work

Developed solution supports currently only 4 modelling languages. More secure modelling languages could be added to be supported by the tool. Currently proposed alignments are not complete, if they are improved, the tool should be improved as well. Feedback about user experience was not collected, probably some improvements could be made to improve it. Currently the tool supports seeing alingments between ISSRM domain concepts and modelling language constructs. Relationships are considered to be part of concept, in the future they could be diverged so that the user could choose only relationships.

References

[1] Premkumar T. Devanbu and Stuart Stubblebine. Software engineering for security: A roadmap. In *Proceedings of the Conference on The Future of Software Engineering*, ICSE '00, pages 227–239, New York, NY, USA, 2000. ACM.

[2] Nicolas Mayer. *Model-based Management of Information System Security Risk.* PhD thesis, University of Namur, 2009.

[3] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. *A Systematic Approach to Define the Domain of Information System Security Risk Management*, pages 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[4] Raimundas Matulevicius. *Fundamentals of Secure System Modelling.* Springer, 2017.

[5] Paolo Bresciani, Anna Perini, Paolo Giorgini, Fausto Giunchiglia, and John Mylopoulos. Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3):203–236, May 2004.

[6] HARALAMBOS MOURATIDIS and PAOLO GIORGINI. Secure tropos: A security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02):285–309, 2007.

[7] Marlon Dumas, Marcello La Rosa, Jan Mendling, and Hajo A. Reijers. *Fundamentals of Business Process Management.* Springer Berlin Heidelberg, 2013.

[8] Olga Altuhhova. An extension of business process model and notation for security risk management. Master's thesis, University of Tartu, 2013.

[9] Bruce Silver. *BPMN Method and Style: A Levels-based Methodology for BPMN Process Modeling and Improvement using BPMN 2.0.* Cody-Cassidy Press, 2009.

[10] sindreGuttorm Sindre and Andreas L. Opdahl. Eliciting security requirements with misuse cases. *Requirements Engineering*, 10(1):34–44, jun 2004.

[11] Ian Alexander. Misuse cases: use cases with hostile intent. *IEEE Software*, 20(1):58–66, jan 2003.

[12] Raimundas Matulevicius, Nicolas Mayer, and Patrick Heymans. Alignment of misuse cases with security risk management. In *2008 Third International Conference on Availability, Reliability and Security.* IEEE, mar 2008.

[13] Inam Soomro. Alignment of misuse cases to issrm. Master's thesis, University of Tartu, 2012.

[14] Guttorm Sindre. Mal-activity diagrams for capturing attacks on business processes. In *Requirements Engineering: Foundation for Software Quality*, pages 355–366. Springer Berlin Heidelberg, 2007.

[15] Mohammad Jabed Morshed Chowdhury, Raimundas Matulevičius, Guttorm Sindre, and Peter Karpati. Aligning mal-activity diagrams and security risk management for security requirements definitions. In *Requirements Engineering: Foundation for Software Quality*, pages 132–139. Springer Berlin Heidelberg, 2012.

Non-exclusive licence to reproduce thesis and make thesis public

I, Madis Kaasik (date of birth: 18th of May 1992),

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1 reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2 make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

A Tool for Supporting Multi-Perspective System Development Through Security Risk Management

supervised by Raimundas Matulevičius

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, 21.05.2018