

UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Institute of Computer Science
Software Engineering Curriculum

Atilio Rrenja
Pattern Based Security Requirement Derivation
with
Security Risk-aware Secure Tropos
Master's Thesis (30 ECTS)

Supervisor(s): Dr. Raimundas Matulevičius

Tartu 2015

Pattern Based Security Requirement Derivation with Security Risk-aware Secure Tropos

Abstract

Information systems (IS's) support a multitude of functions vital to the modern society. IS's carry an ever increasing volume of data and information, including personal pictures, health data or financial transactions. Continuously increasing rates of cyber-attacks have led to the subsequent need to rapidly develop secure IS. To develop secure IS's, security goals need to be identified and fulfilled accordingly. Goal-oriented development fulfils the achievement of security goal by providing a methodology that enables security requirement elicitation throughout the entire development of an information system. This is achieved by considering every component of a system as an actor that is driven by goals that the actor strives to achieve. Nevertheless goal-oriented modeling has proven itself to be valid it maintains multiple shortcomings. The main disadvantage lays in the high granularity of the process making it complex very fast and subsequently raising the level of complexity of the overall process. Therefore a structured approach that would provide a step-by-step guide throughout the application of the process would be essential. Security patterns are proven to be reusable solutions that address recurring security problems which are commonly faced during the process of software development. In this master thesis we investigate the integration of a pattern based security requirement elicitation process in the goal-oriented IS development. By performing this integration we aim at providing a process that enables the elicitation of security requirements from Security Risk-aware Secure Tropos (RAST) models. RAST is a security goal-oriented modeling language that is applicable throughout the complete process of software development from early to late requirements, architecture, detailed design and final implementation.

The contribution of this thesis are five Security Risk-aware Patterns expressed using RAST. The thesis outlines the steps to be executed to apply the proposed security patterns. We validated our contribution by performing a case study that confirmed the overall usability of our proposed patterns and the pattern application process. Additionally the case study determined that the provided patterns can be used as a starting point for a faster and more efficient in identifying security requirements.

Keywords: *Security engineering, Security risk-oriented patterns, Secure Tropos, Security requirement*

Mustripõhiste Turvalisusnõuete Derivatsioon Security Risk-aware Secure Tropos Mudeli Abil

Sisukokkuvõte

Informatsioonisüsteem (IS) toetab suurt hulka modernse ühiskonna jaoks olulisi funktsioone. IS sisaldab üha suurenevat hulka andmeid ja informatsiooni, sealhulgas personaalseid pilte ja andmeid tervise või finantstehingute kohta. Üha suurenev küberrünnakute arv on tinginud vajaduse turvaliste infosüsteemide kiiremaks loomiseks. Et arendada turvalist IS-i, tuleb tuvastada turbe-eesmärgid ning need vastavalt ellu viia. Tulemuspõhine arendus tagab turbe-eesmärkide tulemuslikkuse, pakkudes metodoloogiat, mis võimaldab turvalisuse nõuete induktsiooni läbi kogu informatsioonisüsteemi arenduse protsessi. See on saavutatav, kui võtta igat süsteemikomponenti kui eesmärgile orienteeritud osa. Olgugi, et tulemuspõhine modelleerimine on kasulikuks osutunud, on sellel ka mõningaid puuduseid. Peamine puudus peitub detailsuses, mille tõttu see protsess võib lühikese ajaga muutuda komplekseks, tõstes ka kogu ülejäänut protsessi keerukusetaset. Seetõttu on oluline kasutada struktureeritud lähenemisviisi, mis võimaldab kogu protsessi jooksul samm-sammulist juhendit rakendada. Turvalisuse mustrid on korduvkasutatavad ja võimaldavad lahendada tarkvaraarenduse protsessi käigus sagedasti ilmnevaid probleeme. Käesolevas magistritöös uuritakse mustripõhise turvanõuete kogumise protsessi integreerimist, tulemuspõhise IS-i arendamisel. Selle eesmärgiks on SRP'd (*Security Risk-oriented Patterns*) kasutades pakuda protsessi, mis võimaldab turvanõuete induktsiooni RAST (*Security Risk-aware Secure Tropos*) mudelis. RAST on turvalisuse tulemuspõhise modelleerimise keel, mis on kohaldatav läbi kogu tarkvaraarenduse protsessi nii varasematele kui hilisematele nõudlustele, arhitektuurile, üksikasjalikule projekteerimisele kui ka lõplikule rakendamisele.

Käesoleva magistritöö panus on viie SRP avaldamine, kasutades selleks RAST modelleerimise keelt. Töös tuuakse välja sammud, mida väljapakutud turvalisuse mustrite rakendamiseks kasutada. Töö autor annab omapoolse panuse viies läbi juhtumiuuringu, mis kinnitab autori poolt pakutud mustrite üldise kasutamise selle rakenduse protsessist. Juhtumiuuringust selgus ka, et töös välja pakutud mustreid on võimalik kasutada süsteemi analüüsi alguspunktina, et kiirendada turvalisuse nõuete väljaselgitamisprotsessi ning seda efektiivsemaks muuta.

Võtmesõnad: Turvalisusetehnika, Turvalisuse Riskorienteeritud Mustrid, Secure Tropos, Turvalisuse nõuded

Table of Contents

Abstract	2
Table of Figures	6
List of Tables.....	8
1 Introduction	10
2 Security Risk Management for Information Systems	12
2.1 Domain Model.....	12
2.2 Security Risk Management Process	13
2.3 ISSRM Process Example.....	14
2.4 Summary.....	14
3 Modelling Languages for Security Risk Management.....	15
3.1 Mal-Activity Diagrams.....	15
3.2 Misuse Cases	15
3.3 Secure Tropos	16
3.4 Security Risk-Aware Secure Tropos	18
3.5 Summary.....	22
4 Security Patterns.....	23
4.1 Security pattern classification.....	23
4.2 Enterprise security and risk management patterns	24
4.3 Security Risk-oriented Pattern Representation with RAST	25
4.4 Summary.....	29
5 Security Risk-Oriented Patterns Used in Secure Tropos	30
5.1 Model Pre-Processing.....	30
5.2 Pattern Application Process.....	31
5.3 Other Patterns	36
5.4 Further Steps.....	40
5.5 Summary.....	40
6 Validation	41
6.1 Case Study Questions	41
6.2 Introductory Lecture	41
6.3 Pattern Application Task	41
6.4 Case Study Model.....	41
6.5 Case Study Questionnaire.....	42
6.6 Case Study Participants	42
6.7 Threats to Validity	43

6.8	Individual Participant Task Results.....	44
6.9	Case Study Group Comparative Discussion.....	45
6.10	Questionnaire Summary of the Results	45
6.11	Case Study Concluding Remarks	47
6.12	Answers to the Case Study Questions	48
6.13	Summary.....	48
7	Conclusion.....	49
7.1	Related Work.....	49
7.2	Answer to Research Question & Conclusions.....	49
7.3	Limitations.....	50
7.4	Future Work.....	50
8	References	51
	Appendix	52
I.	Abstract Syntax of RAST	52
II.	SRP2 - Securing business activities from submitted data	54
III.	SRP3 - Securing business activities from DoS attacks	57
IV.	SRP4 - Securing business data from unauthorized access	60
V.	SRP5 - Securing business data stored/retrieved from a data store	63
VI.	Case Study Participant Reports	66
VII.	Correct Pattern Applications	82
VIII.	Case Study Questionnaire Answers.....	90
IX.	License.....	91

Table of Figures

Fig 2.1 - ISSRM Domain Model; adapted from (Dubois et al., 2010) and (Mayer, 2009)	12
Fig 2.2 - ISSRM Process; adapted from (Mayer, 2009).....	13
Fig 3.1 - Example Modelling of Business Assets	19
Fig 3.2 - Example Modelling of IS Assets.....	20
Fig 3.3 - Example Attack Identification	20
Fig 3.4 - Example Potential Attack Scenario	21
Fig 3.5 - Example Risk Treatment and Security Requirements Definition	22
Fig 4.1 - The sequence of enterprise SRMP; adapted from (Schumacher et. al., 2013).....	24
Fig 4.2 - SRP1 Modelling of Business Assets	27
Fig 4.3 - SRP1 Modelling of IS Assets.....	27
Fig 4.4 - SRP1 Attack Identification.....	28
Fig 4.5 - SRP1 Potential Attack Scenario	28
Fig 4.6 - SRP1 Risk Treatment and Security Requirements Definition	28
Fig 5.1 - Model for a computer-supported meeting scheduling configuration; adapted from (Yu, 1994)	30
Fig 5.2 - Meeting Scheduler Example without Security Constraints Applied	31
Fig 5.3 - Meeting Scheduler Running Example with Security Constraints and Criteria	32
Fig 5.4 - SRP1 occurrence in model	33
Fig 5.5 - Pattern Application Example, STEP 2 (a).....	33
Fig 5.6 - Pattern Application Example, STEP 2 (b).....	34
Fig 5.7 - Pattern Application Example, STEP 3	34
Fig 5.8 - Pattern Application Example, STEP 4	35
Fig 5.9 - SRP1 Integrated in the Main Model.....	35
Fig 5.10 - SRP2 Occurrence in the Meeting Scheduler Example	36
Fig 5.11 - SRP2 Applied in the Meeting Scheduler Example	36
Fig 5.12 - SRP3 Occurrence in the Meeting Scheduler Example	37
Fig 5.13 - SRP3 Applied in the Meeting Scheduler Example	37
Fig 5.14 - SRP4 Occurrence in the Meeting Scheduler Example	38
Fig 5.15 - SRP4 Applied in the Meeting Scheduler Example	38
Fig 5.16 - SRP5 Occurrence in the Meeting Scheduler Example	39
Fig 5.17 - SRP5 Applied in the Meeting Scheduler Example	39
Fig 5.18 - The Entire Model with All the Patterns Applied	40
Fig 6.1 - Internet Store Registration; adapted from (Altuhhova, 2013)	42
Fig 8.1 - SEAM Abstract Syntax; adapted from (Matulevičius et al., 2012)	52
Fig 8.2 - SEGM Abstract Syntax; adapted from (Matulevičius et al., 2012)	52
Fig 8.3 - Abstract Syntax of Security Constraint and Threat; adapted from (Matulevičius et al., 2012)	53
Fig 8.4 - Abstract Syntax of Security Attack Scenario; adapted from (Matulevičius et al., 2012)	53
Fig 8.5 - SRP2 Modelling of Business Assets	55
Fig 8.6 - SRP2 Modelling of IS Assets.....	55
Fig 8.7 - SRP2 Attack Identification.....	56
Fig 8.8 - SRP2 Potential Attack Scenario	56
Fig 8.9 - SRP2 Risk Treatment and Security Requirements Definition	56

Fig 8.10 - SRP3 Modelling of Business Assets	58
Fig 8.11 - SRP3 Modelling of IS Assets.....	58
Fig 8.12 - SRP3 Attack Identification.....	59
Fig 8.13 - SRP3 Potential Attack Scenario	59
Fig 8.14 - SRP3 Risk Treatment and Security Requirements Definition	59
Fig 8.15 - SRP4 Modelling of Business Assets	61
Fig 8.16 - SRP4 Modelling of IS Assets.....	61
Fig 8.17 - SRP4 Attack Identification.....	62
Fig 8.18 - SRP4 Potential Attack Scenario	62
Fig 8.19 - SRP4 Risk Treatment and Security Requirements Definition	62
Fig 8.20 - SRP5 Modelling of Business Assets	64
Fig 8.21 - SRP5 Modelling of IS Assets.....	64
Fig 8.22 - SRP5 Attack Identification.....	65
Fig 8.23 - SRP5 Potential Attack Scenario	65
Fig 8.24 - SRP5 Risk Treatment and Security Requirements Definition	65
Fig 8.25 - PA SRP2 applied STEP 2 (a)	66
Fig 8.26 - PA SRP2 applied STEP 2 (b).....	67
Fig 8.27 - PA SRP2 applied STEP 3	67
Fig 8.28 - PA SRP2 applied STEP 4	67
Fig 8.29 - PA SRP4 applied STEP 2 (a)	68
Fig 8.30 - PA SRP4 applied STEP 2 (b).....	68
Fig 8.31 - PA SRP4 applied STEP 3	68
Fig 8.32 - PA SRP4 applied STEP 4	69
Fig 8.33 - PB SRP5 applied STEP 2 (a)	70
Fig 8.34 - PB SRP5 applied STEP 2 (b).....	70
Fig 8.35 - PB SRP5 applied STEP 3.....	70
Fig 8.36 - PB SRP5 applied STEP 4.....	71
Fig 8.37 - PC SRP1 applied STEP 2 (a)	72
Fig 8.38 - PC SRP1 applied STEP 2 (b).....	72
Fig 8.39 - PC SRP1 applied STEP 3.....	73
Fig 8.40 - PC SRP1 applied STEP 4.....	73
Fig 8.41 - PC SRP3 applied STEP 2 (a)	73
Fig 8.42 - PC SRP3 applied STEP 2 (b).....	74
Fig 8.43 - PC SRP3 applied STEP 3.....	74
Fig 8.44 - PC SRP3 applied STEP 3.....	74
Fig 8.45 - PD SRP4 applied STEP 2 (a).....	76
Fig 8.46 - PD SRP4 applied STEP 2 (b).....	76
Fig 8.47 - PD SRP4 applied STEP 3	76
Fig 8.48 - PD SRP4 applied STEP 4	77
Fig 8.49 - PE SRP1 applied STEP 2 (a).....	78
Fig 8.50 - PE SRP1 applied STEP 2 (b)	78
Fig 8.51 - PE SRP1 applied STEP 3.....	79
Fig 8.52 - PE SRP1 applied STEP 4.....	79

Fig 8.53 - PF SRP2 applied STEP 2 (a).....	80
Fig 8.54 - PF SRP2 applied STEP 2 (b).....	80
Fig 8.55 - PF SRP2 applied STEP 3	81
Fig 8.56 - PF SRP2 applied STEP 4	81
Fig 8.57 - SRP's identified in the Internet Store model	82
Fig 8.58 - Case Study, SRP1 Correct Application STEP2 (a)	82
Fig 8.59 - Case Study, SRP1 Correct Application STEP2 (b)	83
Fig 8.60 - Case Study, SRP1 Correct Application STEP3.....	83
Fig 8.61 - Case Study, SRP1 Correct Application STEP4.....	83
Fig 8.62 - Case Study, SRP2 Correct Application STEP2 (a)	84
Fig 8.63 - Case Study, SRP2 Correct Application STEP2 (b)	84
Fig 8.64 - Case Study, SRP2 Correct Application STEP3.....	84
Fig 8.65 - Case Study, SRP2 Correct Application STEP4.....	85
Fig 8.66 - Case Study, SRP3 Correct Application STEP2 (a)	85
Fig 8.67 - Case Study, SRP3 Correct Application STEP2 (b)	85
Fig 8.68 - Case Study, SRP3 Correct Application STEP3.....	86
Fig 8.69 - Case Study, SRP3 Correct Application STEP4.....	86
Fig 8.70 - Case Study, SRP4 Correct Application STEP2 (a)	86
Fig 8.71 - Case Study, SRP4 Correct Application STEP2 (b)	87
Fig 8.72 - Case Study, SRP4 Correct Application STEP3.....	87
Fig 8.73 - Case Study, SRP4 Correct Application STEP4.....	87
Fig 8.74 - Case Study, SRP5 Correct Application STEP2 (a)	88
Fig 8.75 - Case Study, SRP5 Correct Application STEP2 (b)	88
Fig 8.76 - Case Study, SRP5 Correct Application STEP3.....	88
Fig 8.77 - Case Study, SRP5 Correct Application STEP4.....	89
Fig 8.78 - All the Patterns Correctly Re-Integrated In the Model (STEP5).....	89

List of Tables

Table 1 - Running Example In Terms of Security Domain Model Concepts	14
Table 2 - Security Risk-oriented Pattern Template; adapted from (Ahmed & Matulevičius, 2011).....	25
Table 3 - SRP1 Asset Identification and Mitigation	26
Table 4 - Patterns Applied by Each Study Participant	43
Table 5 - Case Study Participant Pattern Application Errors	45
Table 6 - SRP2 Asset Identification and Mitigation	54
Table 7 - SRP3 Asset Identification and Mitigation	57
Table 8 - SRP4 Asset Identification and Mitigation	60
Table 9 - SRP5 Asset Identification and Mitigation	63

Abbreviations:

IS - Information System

SRP - Security Risk-aware Pattern

RAST - Security Risk-aware Secure Tropos

ISSRM - Information System Risk Management

ST - Secure Tropos

MUC - Misuse Cases

MAD - Mal-Activity Diagrams

1 Introduction

Goal-oriented information system development enables security requirement elicitation through goals. Following this methodology goals represent objectives of a system. The system itself is considered as an actor striving to achieve the aforementioned goals. Following a traditional security solution development methodology in a goal-oriented environment is a favorable approach. Nonetheless given an information system with a moderate complexity, identifying risks and vulnerabilities can become a complicated task. To address this complexity we propose the integration of Security Risk-oriented Patterns (SRP's) in the goal-oriented information system development. A pattern-based approach encompasses a number of advantages in comparison to a traditional methodology. Advantages include: faster development, proven security results and ease of application by inexperienced analysts.

The scope of this thesis is the elicitation of security requirements using SRP's in a goal-oriented environment such as Security Risk-Aware Secure Tropos (RAST) (Matulevičius et al., 2012). In order to analyze the various scenarios we employ Information System Security Risk Management (ISSRM) (Mayer, 2009) (Dubois, et al., 2010) - that is a framework for risk analysis. Beyond the scope of thesis is the prioritization and implementation of the various controls represented by the pattern, therewith it will not be considered within this thesis.

In this thesis we resolved research question:

RQ: *How to integrate security risk-oriented patterns in the goal-oriented information system development?*

The contribution of this work is a proposed integration of SRP's in the goal-oriented information system development. We achieved this by constructing a process that represents SRP's using RAST in conjunction with the Security Risk-oriented Pattern Template (Ahmed & Matulevičius 2014). Also using our proposed representation we introduce five SRP's. In addition to the core contribution of the pattern representation we describe a pattern application method to be used to apply SRP's in RAST models. Finally we conducted a case study to confirm the usability of our proposed pattern application process. The results, affirmed our research contribution.

This master thesis includes seven chapters. Chapter 1 is dedicated to the introductory overview of this master thesis. This chapter explains the motivation for this paper in addition to the scope, main research question, as well as the contribution and structuring of the thesis. Chapter 2 examines an overview of the process and domain model of the Information System Security Risk Management methodology adapted from (Mayer, 2009) and (Dubois et al., 2010). Chapter 3 is devoted to a brief overview of modeling languages for security risk management i.e. Mal(icious)-Activity Diagrams (Sindre, 2007) (Chowdhury et. al, 2012), Misuse Cases (Sindre & Opdahl, 2002), (Soomro & Ahmed 2013), Secure Tropos (Mouratidis, 2007) in addition to presenting the main modeling language for this thesis - Security Risk-aware Secure Troops (Matulevičius et al., 2012) - followed by an illustrative example using one of our running examples. Chapter 4 overviews security patterns and their classification (Schumacher et. al., 2013), and presents one of the SRP's that are part of the contribution of this master thesis. Chapter 5 illustrates our contribution where we present the pattern application process using a model from (Yu, 1994) and SRP1, additionally a brief representation of all the patterns applied in the previously mentioned model. Chapter 6 outlines the case study conducted in order to validate the usability of the patterns illustrated

in this thesis and their application process. In the closing Chapter 7, we address the research question and close with concluding remarks and suggestions for future research on these issues. The appendix includes the rest of our proposed patterns that are part of this thesis's contribution in addition to the abstract syntax of Risk Aware Secure Tropos, as well as the complete case study reports of each participant.

2 Security Risk Management for Information Systems

In this chapter we overview the Information System Security Risk Management (ISSRM) domain model. Moreover, we examine the process followed by the ISSRM approach in order to elicit security requirements. We conclude by providing an illustrative example of the security risk management process using a running example.

2.1 Domain Model

ISSRM is a methodology that assists in detection, evaluation and mitigation of security risks. Moreover it improves upon the entirety of crucial matters in the development of secure information systems (Mayer 2009). The ISSRM domain model is composed three main conceptual categories - asset related concepts, risk related concepts and risk treatment related concepts (see domain model in Figure 2.1).

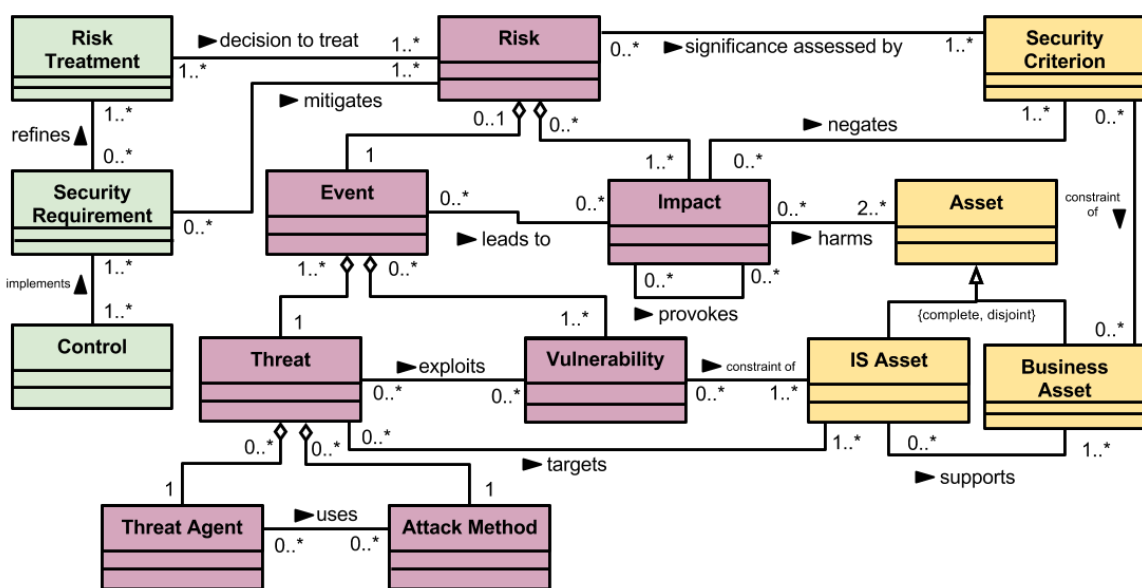


Fig 2.1 - ISSRM Domain Model; adapted from (Dubois et al., 2010) and (Mayer, 2009)

Asset-related concepts describe valuable subjects and objects of an organization that require protection. They are divided into security criteria, business and IS assets. *Security criterion* is characterized as a constraint to an asset that defines its security needs. *Business assets* include assets of an organization that represent its core business process and result in the organization achieving the desired outcomes related to its functional aspects. *IS assets* are assets related to the IS infrastructure.

Risk related concepts define risk levels that assets are exposed to. These concepts are *risk*, *impact*, *event*, *threat*, and *threat agent*, *vulnerability*, and *attack method*. *Risk* identifies the level of harmfulness of a threat towards a specific asset. *Impact* describes the result of exposure of an asset, to a specific risk. *Event* is defined as a potentially harmful combination of threat and one or more vulnerabilities of the system. *Vulnerability* is a flaw of an asset that compromises system security. A *threat* is the malicious intention of a threat agent to cause harm to the organization. *Attack method* refers to the process of a *threat agent* to cause damage or exploit an organization.

Risk treatment related concepts mitigate potential risks of the system. Main concepts are *risk treatment*, *security requirements* and *control*. A *risk treatment* refers to the process of mitigating a risk identified by a risk related concept. Propositions of these concept group, include how to improve a company's security level by means of reducing, avoiding, and transferring or retaining a risk. A *security requirement*, identified by the risk related concept group, refers to an IS requirement suggesting on how to deal with potential risks. *Control* is defined as the process of countering a risk with a strategy suggested previously by a security requirement concept, avoiding a threat and stabilizing the condition.

2.2 Security Risk Management Process

The risk management process consists of six steps that can be seen in Figure 2.2. It initiates with the general study of the system and clear establishment of the assets included. As a second step the security objectives of the system are identified. The third step of the process is the performance of a risk analysis, where potential security objectives or assets that are at risk are identified. Here at the end of this step an assessment is performed and in case the assessment is satisfactory a fourth step follows by establishing the risk treatment for the risks identified in the previous step. The fifth step suggests the elicitation of IS security requirements followed by a final step - control selection and implementation. In this step specific countermeasures established in the previous phases get approved as main strategy and executed to avoid the threat and reach a condition of security and stability.

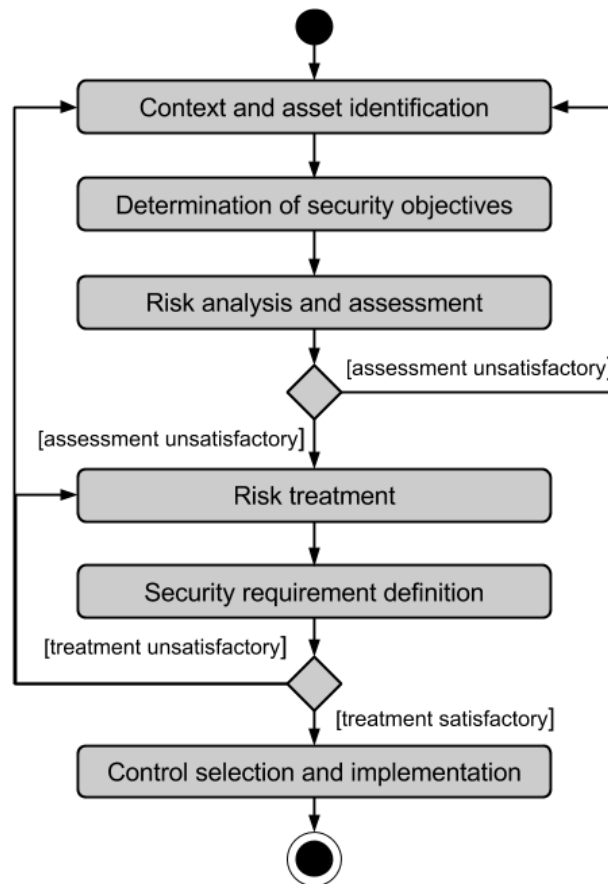


Fig 2.2 - ISSRM Process; adapted from (Mayer, 2009)

2.3 ISSRM Process Example

Following the ISSRM security risk management process we decompose and analyze our running example following previously described six steps.

Our running example is of an individual that is exposed to a shoulder surfing attack. In this example at some point in time an individual while being in a public environment decides to use his email account. The individual proceeds to login unsuspecting of anyone looking at him. An attacker by using the method of shoulder surfing observes the password and the email. The attacker proceeds to use the persons email account to login into various websites where the user is a member and by resetting the password set by the user and extorts sensitive data.

The first step includes content and asset identification. We identify as business asset the user's email and password data information and IS asset we identify the user himself as a person due to the fact that he supports the business data. In the second step we identify the security objectives. Here we specify the confidentiality of the email and the confidentiality of the password of the user as main security objective. As a third step that is risk assessment and analysis we identify a threat agent as an attacker with social engineering skills and willingness to shoulder surf and obstruct the data. In the fourth step as risk treatment we specify *risk reduction*. The fifth step we define as a security requirement "Use the email and password in private". Finally, the sixth and last step the security control that we introduce is to make sure that no one is watching you while entering the password. In Table 1 we decompose the example to it's of the ISSRM domain model assets.

Table 1 - Running Example In Terms of Security Domain Model Concepts

Asset-related Concepts	
Business Asset	User email, User password
IS Asset	User
Security Criterion	Confidentiality of the user's email. Confidentiality of the user's password.
Risk-related Concepts	
Risk	Attacker performs shoulder surfing and memorizes the users email login data due to user inattentiveness towards personal data. Resulting in the loss of the confidentiality of the email and the confidentiality of the password.
Impact	Loss of the confidentiality of the user's email. Loss of the confidentiality of the user's password.
Event	Attacker performs shoulder surfing and memorizes the users email login data due to user inattentiveness towards personal data.
Vulnerability	User inattentiveness towards personal data.
Threat	Attacker performs shoulder surfing and memorizes the users email login data.
Threat Agent	An attacker with social engineering skills and willingness to shoulder surf and obstruct the data.
Attack Method	Shoulder surf and memorize the email or password.
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Use the email and password in private.
Control	Make sure that no one is watching you while entering the password.

2.4 Summary

In this chapter we overviewed the ISSRM domain model. We described the ISSRM process followed to elicit security requirements. Lastly using our running example, we illustrated the core concepts of ISSRM and its processes.

3 Modelling Languages for Security Risk Management

In this chapter we provide an overview of modeling languages from the relevant literature. Additionally we provide an introduction to Security risk-aware Secure Troops the modeling language utilized in this master thesis followed by a textual and illustrative example.

3.1 Mal-Activity Diagrams

Mal(icious)-Activity Diagrams (MAD) complement UML Activity Diagrams by integrating a workflow that introduces security requirement elicitation within the context of the early design phases of an IS's (Sindre, 2007). Syntactically and semantically MAD follows the same design as UML activity diagrams. MAD adds a *malicious activity* in a separate swim lane, and indicates a *malicious actor* by using the invert color scheme from the one of the *actors* of the same diagram. Additionally a malicious decision box is introduced that depicts the malicious action options that a malicious actor performs with a malicious activity wherever appropriate.

In (Chowdhury et. al, 2012) a concept alignment between ISSRM and MAD is introduced. *Asset related* concepts of *business asset* map to the concepts of *decision, activity, and control flow* whereas *IS assets* map to the concepts contained within a swim lane, concept alignment to security criterion cannot be determined. *Risk related* concepts of *threat agent* aligns to the *mal-swim lane* and attack method to the combination of *mal-activity constructs, impact* aligns to *mal-activities*. Nonetheless there is no alignment to a construct of MAD that represent *vulnerabilities*. *Risk treatment* concepts of *control* align to *swim lane* and security requirement to the *mitigation activity*.

3.2 Misuse Cases

Misuse Cases (MUC) are an extension to Unified Modeling Language (UML) Use Cases (Sindre & Opdahl, 2002). They address the inability of use cases to extensively elicitate security requirements in the early phases of the design process of an IS. MUC align misusers to actors and use cases to misuse cases. A *misuser* is an actor that with or without the intention compromises a system through a misuse case. A *misuse case* is the process followed by a misuser that leads to unwanted results for the entity that are imposed to. In Table.1 we showcase the MC constructs.

In (Soomro & Ahmed 2013) a risk-oriented extension to MC is introduced, Security Risk-oriented Misuse Cases (SROMUC) enables elicitation of security requirements following the ISSRM process. *Asset related concepts* align to the Actor concept, business and IS concepts are represented by a respective use case type, security criterion is represented by a security constraint construct and support relationships are represented by the <<extends>> and <<includes>> relationships. *Risk-related concepts* of attacker are represented by the MC concept of misuser, attack method is described by a misuse case and vulnerability by a gray colored misuse case. Threats are aligned to the combination of a misuser and a misuse case whereas the targets relation maps to the *threatens* relationship of SROMUC. A rounded rectangle is introduced with the purpose of representing ISSRM concept of impact. Additionally *exploits* is defined as a relationship between a *misuse case* and *vulnerability, leads to* is represented by the relationship of *misuse cases* and *impact* and *harm* is defined by the relationship of *impact* and *business use case*. Moreover *negates* is

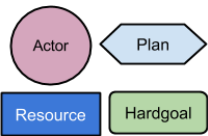
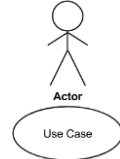
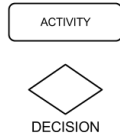


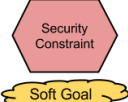

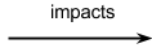










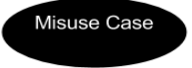


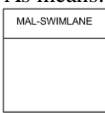
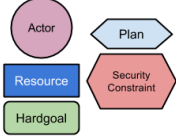

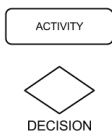

represented by the link of *impact* and *security criterion* whereas a combination of *threat agent*, *attack method*, *impact* and *vulnerability* represents an *event* and *risk* is introduced as the combination of *event* and *impact*. **Risk treatment-related concepts** in SROMUC update the modeling syntax of security use case. By adding a padlock within the label of a security use case that aligns to the security requirement concept of ISSRM. The mitigates relationship aligns to a mitigates relationship from security use case.

3.3 Secure Tropos

Secure Tropos (ST) (Mouratidis, 2007) is an agent oriented security requirements elicitation and modelling methodology. It is an extension of the Tropos methodology (Bresciani et. al, 2004). The proposed methodology addresses the inability of Troops to clearly and distinctly represent and model security requirements. ST follows the process of software development, starting entirety from early to late requirements, architecture, detailed design and final implementation. The methodology focuses on actors, their goals, accessible resources, performed tasks and social dependencies. ST incorporates all the major elements and concepts that render Tropos a multi agent system methodology. In brief an Actor is an entity that is part of the multi agent system and is driven by certain goals and intentions. A role is the set of distinctive characteristics that characterize the behavior within the system of an actor. As a Hard-goal is defined the desired state that an actor is determined to achieve, whereas a Soft-goal is again a desired state yet there is no clear determination of how this state is to be achieved. A task is the sequence followed by an actor in order to achieve and satisfy a certain goal. As a resource is stated to be an important item of information required by an actor. Between two or more actors Dependencies exist in terms of achieving a goal. Capability is the definition of the ability of an actor to carry and complete a certain task. All the corresponding modeling elements can be seen in Table.2. In addition to the using the Tropos concepts ST introduces concepts that enable ST to elicitate and model security requirements. More extensively Constraint and Security Constraint is a security related limitation or restriction that crucially impacts the development of the system in design, limit the liberties that might be taken from certain agents or is in conflict with another component of the architecture. Additionally ST introduces a Secure Dependency that describes one or more security contrarians. These constraints have to be achieved in order for the dependency that relies on them to be resolved.

In Table 2 we present a side by side representation of all the modeling constructs of all the previously overviewed modeling language. All the constructs are represented in terms of their aligning of ISSRM concepts. The constructs in the table are from the resulting alignment of each modeling language to ISSRM

Table 2 - Language Correspondence to ISSRM Regarding Concepts; adapted from (Matulevičius et al., 2012)

ISSRM	SECURE TROPOS/RAST	MISSUSE CASES	MAL-ACTIVITIES
Asset-related Concepts			
Business Asset	 <p>Combined using dependency, contribution, means-ends and decomposition links</p>	 <p>Combined using <i>extends</i>, <i>includes</i> and <i>combination</i> links</p>	 <p>Combined using <i>control flow</i></p>
IS Asset			
Security Criterion	 <p>Combined using contribution and security constraint decomposition</p>		-
Risk-related Concepts			
Risk	Combination of Impact and Event	Combination of Impact and Event	Combination of Impact and Event
Impact			 <p>Combined in the <i>mal-swim lane</i> that expresses attack method</p>
Event	 <p>Or: Combination of <i>vulnerability</i> and <i>threat</i>.</p>	Combination of <i>vulnerability</i> and <i>threat</i> .	Combination of <i>vulnerability</i> and <i>threat</i> (Implicitly defined).
Vulnerability	 <p>Added to the IS asset such as <i>goal</i>, <i>task</i> or <i>resource</i>.</p>		-
Threat		Combination of attack method and <i>threat agent</i>	Combination of attack method and <i>threat agent</i>
Threat Agent			
Attack Method	 <p>Potentially combined with other <i>tasks</i> using <i>decomposition</i> links</p>	 <p>Potentially combined with other <i>misuse cases</i> using <i>includes</i> and <i>extends</i> links</p>	<p>As method:</p>   <p>Combined using <i>control flow</i> links</p> <p>As means:</p> 
Risk Treatment-related Concepts			
Risk Treatment	-	-	-
Security Requirement	 <p>Combined using dependency, contribution, means-ends and decomposition links</p>	 <p>Combined using <i>extends</i>, <i>includes</i> links</p>	 <p>Combined using <i>control flow</i> links</p>
Control	-	-	

3.4 Security Risk-Aware Secure Tropos

Security risk-aware Secure Tropos (RAST) (Matulevičius et al., 2012) is a syntactic, semantic and methodological extension of the ST methodology focused on the enhancement of the early stages of IS development. The proposed methodology addresses the void of addressing assets, risks and risk treatments alike, with a cohesive modeling approach that follows the ISSRM methodology. This extension of ST provides the ability of using ST modeling concepts wherever possible utilizing the already existing constructs. Additionally, whenever void or ambiguity exists, new constructs are introduced to address risk related scenarios. In detail the core constructs of RAST are: The *Actor*, which is an entity that is part of a system and is driven by certain goals and intentions. The *Goal*, which is defined as the desired state that an actor is determined to achieve. The *Plan*, which is a course of action followed by an actor in order to achieve and satisfy a goal. The *Resource*, which is an important item of information required by an actor. The *Threat*, which is the course of action followed by an attacker to harm the system. The *Attacker*, which is a malicious entity with intention to harm the system. The *Malicious Goal*, which is a goal that indicates a malicious goal of an attacker. The *Vulnerability*, that is an additional construct utilized in order to indicate that a plan/resource/goal are vulnerable assets. The *Malicious Plan*, which is a plan that indicates a malicious plan of an attacker. Moreover for a deeper understanding of the modeling process of RAST the abstract syntax can be found in the appendix.

RAST - ISSRM Alignment

Asset Related Concepts: The ISSRM modeling concepts of *assets* are modeled using the already existing ST constructs of *goal*, *softgoal*, *actor*, *plan* and *resource*. The relationships between the assets, are modeled using the construct of *contribution* which indicates a connection where a construct positively or negatively contributes in the achievement of a plan or goal. The *means-ends* relationship, which indicates a connection where a construct such as plan/resource/goal is the means to achieve another plan/goal. *Decomposition* which provides a decomposition of a goal/or plan into sub-goals and sub-plan respectively. The *support* between *business assets* and *IS assets* is modeled using the respective to the circumstances ST relationship. *Security criterion* is modeled and represented by combining a *softgoal* and/or a *security constraint*. The *constraints of* relationship can be modeled both implicitly and explicitly. Implicitly by restricting a *task*, *goal* or *resource* as a *dependum* and explicitly by restricting through a relationship.

Risk Related Concepts: In order to properly distinguish risk related concepts it is suggested to use darker colors. RAST represents a *threat agent* through the *actor* construct, *attack method* as a *plan* and threat as a *goal* and/or *plan* respectively. *Vulnerability* is represented through the RAST introduced *vulnerability point*. The *targets* relationship is represented through the *attacks* relationship. Additionally, RAST introduces the exploits relationship that aims to represent the link between a *plan* and an *asset* that includes *vulnerability point*. An *event* is represented through the aggregation of *attack method*, *threat agent* and *vulnerability*. Moreover *risk* is modeled by combing a *risk* and an *event*.

Risk-Treatment Related Concepts: The risk-treatment related concepts of security requirement and control are to be modeled through the combination of a *goal*, *softgoal*, *plan* and *security constraint* using the modeling concepts with similar depiction with the addition of a dotted background. Additionally the, *mitigates* relationship is used to indicate a connection where a construct or group of constructs mitigate a certain threat to the system.

Why Risk-Aware Secure Tropos?

Contemplating on the individual characteristics of MUC, MAD, ST and RAST we decide to employ RAST as the main modeling language used for modeling security scenarios throughout this master thesis. We attribute the choice of this modeling approach to multiple reasons. RAST has an advantage over MUC and MAD due to the granularity of the models. Moreover RAST is advantageous over ST due to its alignment to ISSRM and ability to model risk assessment. Being an agent oriented language, RAST includes the advantage of being easy to comprehend and educate others. Moreover, we determined that this modeling language covers all the facets of the ISSRM process and additionally provides with a level of modeling granularity that is adequate to the complexity of the scenarios and patterns presented in this work.

Modeling activities of RAST using running example

For the purpose of illustrating the modeling activities of RAST in this section we use our running example presented in Chapter 1. The example describes an individual accessing his email in public and being subject to a shoulder surfing attack.

Stage 1. Asset identification and security objective identification

In this stage a separation is made in the modeling process between business and IS assets. Herby here two diagrams are created to model this two different assets. In Figure 3.1 we initiate by modeling our business assets that in the case of our example are the *Email* and *Password* of a user, and are modeled using the resource construct. Moreover here the main focus is to identify and model the goals, plans, resources and other actives of the business asset. Continuing, we identify the main goal of the user actor **Access Email** represented by the goal construct. This goal requires the execution of the plan **Remember email and password** in order to be fulfilled. As a next step following ISSRM principles security objectives are defined. These objectives can be defined using two different security objective identification techniques the “top-down” and “bottom-up”. In the “top-down” method softgoals (e.g. Confidentiality) represent general security objectives that are refined using security criteria that are expressed in the models through security constraints (e.g. Keep email and password confidential). In the ‘bottom-up’ approach implicit security requirements are defined through secure dependencies followed by the identification of security constraints (e.g. Access email only in private) that are inspected and identified according to higher level of security objectives (e.g. Keep email and password confidential).

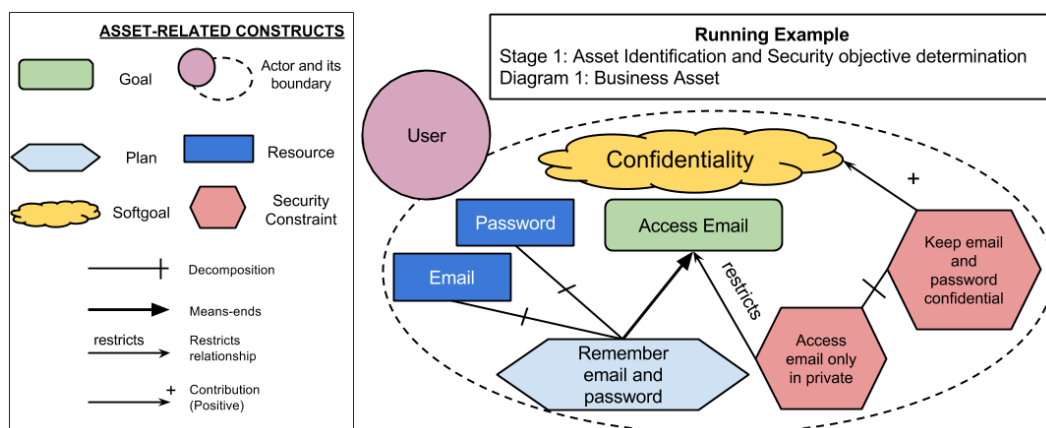


Fig 3.1 - Example Modelling of Business Assets

Next IS assets are modeled, in the model the main IS asset that we consider is the *User* actor that supports the business assets by executing the plan *Remember email and password*. In this modeling step concepts of business assets are modeled together with IS assets, due to the need of depicting how the IS assets support the business assets. In Figure 3.2 secure goals are considered as IS assets. *Keep email and password confidential* is fulfilled if the secure goal of *Confidentiality* of the password and email ensured is satisfied. The support of the business asset comes from ensuring security through *Ensure there are no observers* that satisfies the security goals that ultimately results in support through assuring the fulfilment of the security constraints.

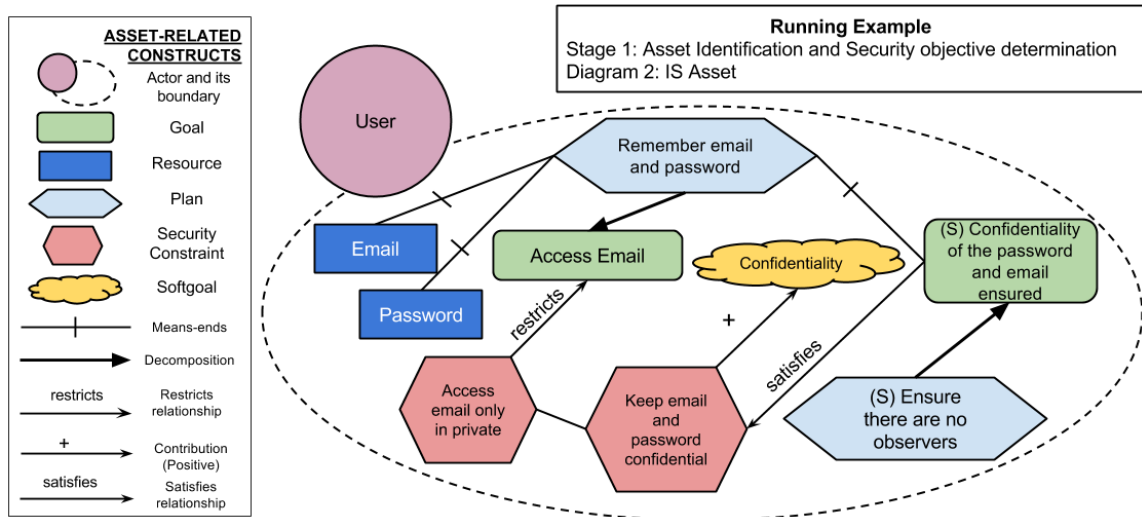


Fig 3.2 - Example Modelling of IS Assets

Stage 2. Risk analysis and assessment.

During the second stage potential harmful risks are introduced. This stage initiates with the identification of security events. As seen in Figure 3.3 we depict a possible risk that our assets will potentially be exposed to *Social Engineering Attack* at this point the attacker through social engineering means attempts to obstruct the email and password of the user. In this instance the attack impacts the *Confidentiality* of the system. Additionally, the harm at the business level can be observed.

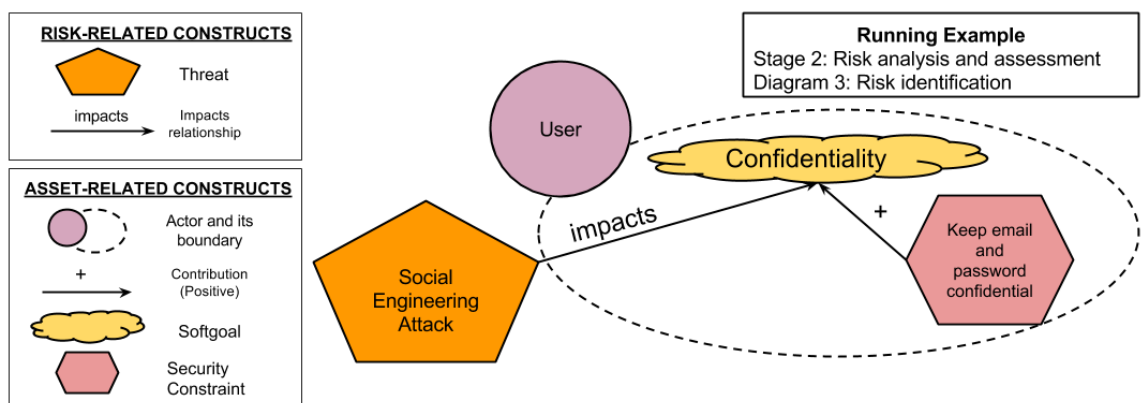


Fig 3.3 - Example Attack Identification

The step that follows the identification of risk, is the refinement of the model in terms of threat, threat agent, attack method and vulnerability. Here we see the process applied to our running example depicted in Figure 3.4. In this instance we identify the Attacker that poses a threat (Shoulders surf and memorize the users email login data) to our asset. The attacker exploits a vulnerability in the (Ensure there are no observers) in order to obtain the users email and password. By using the *exploits* link we can identify the relation of the attack method and the vulnerability of our IS asset.

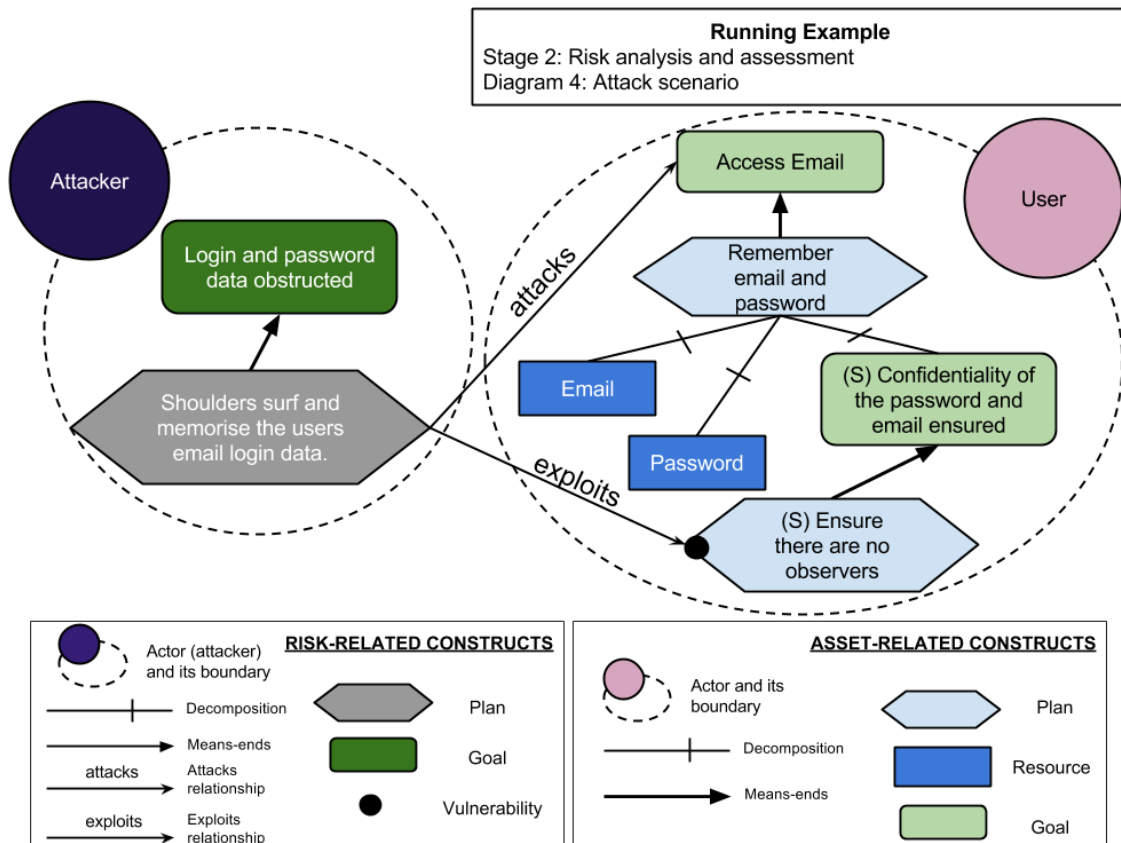


Fig 3.4 - Example Potential Attack Scenario

Stage 3. Security requirements definition.

As identified in our example of ISSRM process we identified *risk reduction* as our risk treatment method to mitigate the identified attack. Consequently goals and plans should be designed with the basis of *risk reduction*. In this step we introduce the security requirement Use the email and password in private. The requirement is represented with a dotted background Figure 3.5 in order to render clear the distinction from a plan. Subsequently the goal Confidentiality of the password and email ensured becomes Confidentiality ensured due to its contribution in mitigating the risk. Given the iterative nature of this process one could go and recheck the system in the current modeled state and introduce new threats and requirements given the need to do so.

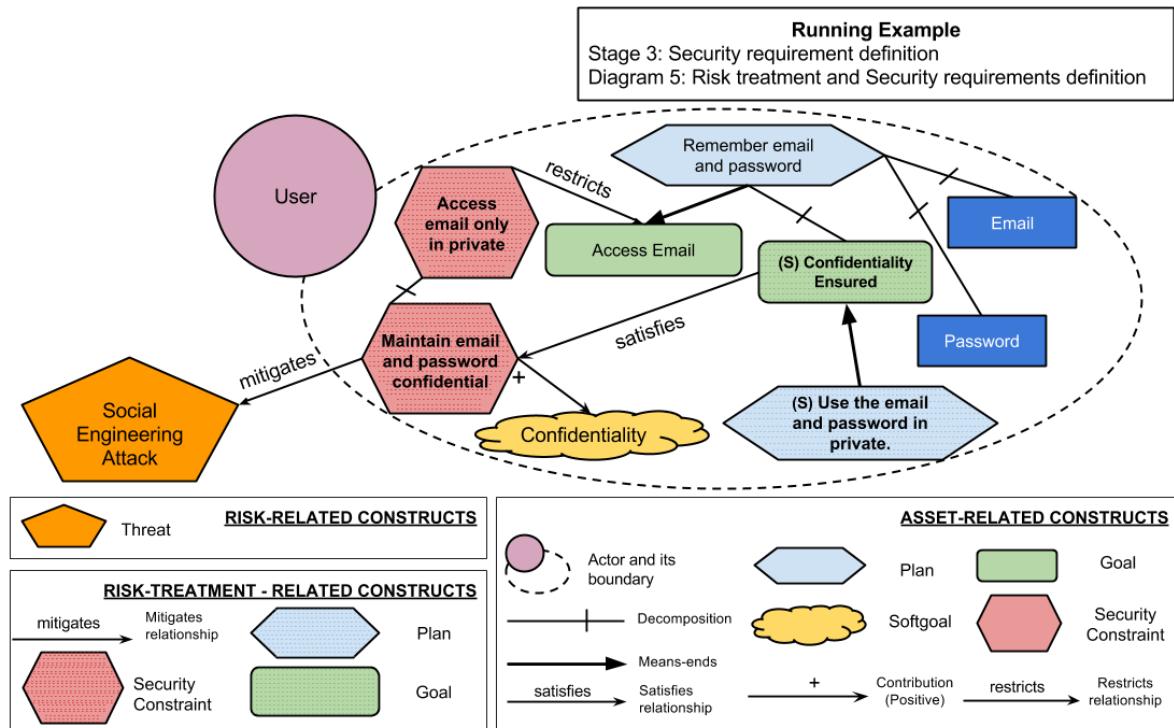


Fig 3.5 - Example Risk Treatment and Security Requirements Definition

3.5 Summary

In this chapter we overviewed MUC, MAD, ST, RAST and their ISSRM alignment. Moreover we justified our decision for choosing RAST as main modeling language of this master thesis. Finally we demonstrated the process of modeling with RAST and eliciting security requirements using our running example.

4 Security Patterns

In this chapter we overview security patterns and their classifications, focusing in enterprise security and risk management patterns. We introduce our contributed pattern representation process and finally present our contributed patterns.

In a software engineering environment, security patterns represent a collection of proven solutions and implementations to reoccurring security problems. The solutions delivered by security patterns are characterized by their reusability throughout a variety of different system implementations. Security patterns are researched extensively in the book “*Security Patterns Integrating Security and Systems Engineering*” Schumacher et. al. (Schumacher et. al., 2013) define security patterns as:

“A security pattern describes a particular recurring security problem that arises in specific contexts, and presents a well-proven generic solution for it. The solution consists of a set of interacting roles that can be arranged into multiple concrete design structures, as well as a process to create one particular such structure.”

4.1 Security pattern classification

With security patterns delivering solutions to known security problems, this results in a numerous amount of patterns that can be hard to navigate. Schumacher et. al. (Schumacher et. al., 2013) proposes patterns to be divided into a number of classes. This makes the selection of an appropriate pattern easier and faster. Below we give a brief description of the classes of security patterns related to this thesis.

- ***Enterprise Security and Risk Management Patterns:*** Enterprise security patterns focus in providing the enterprise with patterns that resolve security issues arising in the enterprise environment. The patterns are designed following close observation of the various functions of the enterprise and its security critical matters.
- ***Identification & Authentication Patterns:*** I&A patterns are mainly used in environments and conditions where secure identification and authentication of users and other stakeholders is crucial. These patterns use multiple different available security measures such as passwords and biometrics in order to deliver the best possible solutions to security problems.
- ***Operating System Access Control Patterns:*** These patterns are developed in order to provide secure access to the extensive intricate file structure and hierarchy of an operating system. Main scope of the introduction of these patterns is to securely dictate procedures which have to be followed in order to provide the appropriate access level to appropriate agents within the context of the system.
- ***Firewall Architecture Patterns:*** These patterns are crucial for security specialists and analysts in order for a successful determination of the tradeoff between overall system security against external attacks, network connectivity speed, and overall system complexity. Given the complex nature of the problem these patterns provide with out of solutions and assist in the secure implementation of this security mechanism.
- ***Cryptographic Key Management Patterns:*** These security patterns ensure the confidentiality, integrity and availability of files located within a system, or when in transmission. Additionally these patterns guide developers in the implementation of secure cryptographic algorithms that result in higher levels of security.

4.2 Enterprise security and risk management patterns

The main scope of enterprise security patterns (Schumacher et. al., 2013) is to provide the enterprise with security patterns aimed at resolving security issues that might arise within its operational context. These patterns are closely related to the mission and functions of the enterprise itself and can be seen in Figure 4.1. These patterns are: **Security Needs Identification for Enterprise Assets** patterns can be considered as the starting point of any of the enterprise's security related considerations, additionally, they take under consideration security criteria such as confidentiality integrity and availability. **Asset Valuation** patterns assist in pinpointing the important assets of a business, which in case of a compromise can cause crucial financial damage to the enterprise, **Threat Assessment** patterns provide with the ability to gauge and identify threats that may cause harm to the business. **Vulnerability Assessment** patterns cover the determination of potential vulnerabilities and the extent of the damage caused to the enterprise if they were to be exploited by an attacker. **Risk Determination** patterns utilize the previously identified assets, threat and vulnerabilities in order to determine risks potentially to be faced. **Enterprise Security Approaches** provide the enterprise with a selection of security approaches (i.e. prevention, detection and response) these approaches are mainly distinguished from others depending on combination of the assessed risks, and asset needed to be protected. Moreover this pattern serves as an initial point for the enterprise to define its security services. **Enterprise Security Services** patterns are mainly used following the **Enterprise Security Approaches** patterns and provides with the means for the enterprise to incorporate security services that will effectively protect the assets at risk. Finally **Enterprise Partner Communication** patterns provide with the means for the enterprise to securely incorporate third party services in order to enhance its security without compromising it.

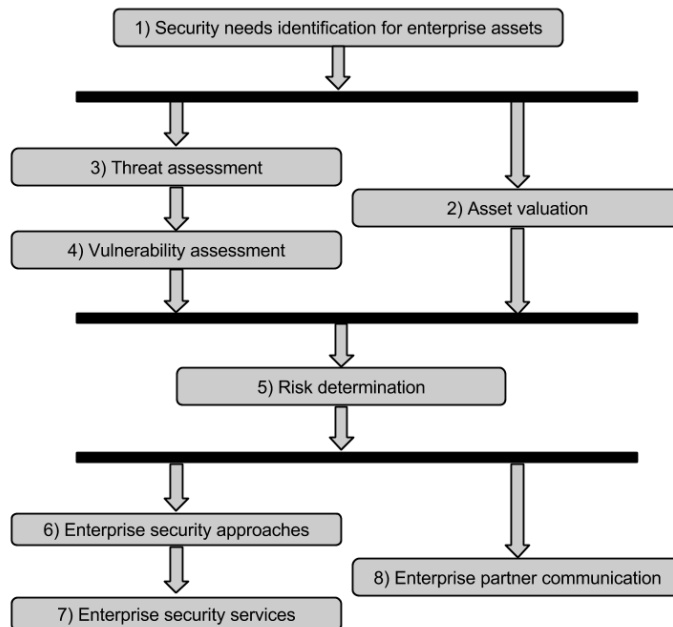


Fig 4.1 - The sequence of enterprise SRMP; adapted from (Schumacher et. al., 2013)

By aligning the security pattern relations depicted in Figure 4.1 with the ISSRM concepts Ahmed & Matulevičius (Ahmed & Matulevičius, 2011) propose a Security Risk-oriented Pattern Template as seen in Table 2. Following the proposed guidelines, we use the proposed template as part of the representation of the patterns illustrated in this thesis.

Table 2 - Security Risk-oriented Pattern Template; adapted from (Ahmed & Matulevičius, 2011)

ENTRY		DESCRIPTION
Pattern Name		This represents the pattern and its security context. It helps to remember and refer to a particular pattern. Normally, the name of the secured business activity is stated here.
Pattern Decision		It describes the potential pattern application scenario. This part includes information regarding the business activity, its input and outputs, and the circumstances in which it is applicable.
Asset-related Concepts	Assets	An asset is any valuable element which is necessary in accomplishing the organization's goal.
	Business Asset	A business asset can be the information, processes, or skills essential for business's main operation.
	IS Asset	An IS asset supports business asset, and it is a component of IS.
	Security Criterion	A security criterion is a constraint on business asset, which is expressed through confidentiality, integrity and availability of business asset.
Risk-related Concepts	Risk	A risk is composed of event(s) and their deleterious impacts on one or more assets.
	Impact	An impact is the potential bad consequences of a risk.
	Event	An event is a combination of threat and vulnerability.
	Threat	A threat agent initiates a threat by using attack method to harm one or multiple IS assets by exploiting their vulnerabilities.
	Vulnerability	A vulnerability is the weakness or flaw of IS asset.
	Threat Agent	A threat agent has means to cause harm to IS assets.
	Attack Method	An attack method is the technique using which a threat agent fulfils threat.
Risk Treatment related Concepts	Risk Treatment	A decision such as: avoidance, reduction, retention for risk mitigation.
	Security Requirement	Security requirement is the refined form of risk treatment decision.
	Control	A control is the implementation of security requirements.
Related Patterns(s)		The place for presenting information about the other related SRPs.

4.3 Security Risk-oriented Pattern Representation with RAST

In this section we demonstrate in detail our proposed representation of Security Risk-oriented Patterns. In order to represent a pattern we combine a textual description in addition to the Security Risk-oriented Pattern Template and RAST. The textual description provides initially with an overview of the pattern, followed by the description of the modeling steps performed during the modeling off the scenario with RAST. Next we use the Security Risk-oriented Pattern Template to describe the SRP's in regard to its ISSRM concepts. Finally we provide detailed models of the SRP's using RAST. In this thesis we describe five SRP's using RAST, in this section we describe SRP1, the rest of the illustrated patterns i.e. SRP2, SRP3, SRP4, SRP5 can be found in the respective section II, III, IV and V of the Appendix.

SRP1 - Securing data-flows between business entities

The main focus of the SRP1 (Ahmed & Matulevičius 2014), pattern is to secure the transmission of confidential data between business entities. This security scenario involves an attacker that has the ability to intercept the transmission medium between two business entities. The attacker intercepts the transmission between the input interface and the server, then obstructs and modifies the data. The attack is facilitated due to the transmission medium not being encrypted and data being stored in plaintext. Ultimately the attack leads to the loss of the confidentiality of the data and loss of the integrity of the data. In Table 3 we utilise the *security risk oriented pattern template* in order to represent a detailed overview of the pattern and move forward with the representation of the pattern using RAST

Table 3 - SRP1 Asset Identification and Mitigation

Security scenario & security context identification	
Pattern Name	Securing data-flows between business entities.
Pattern Decision	This patterns is employed in order to secure data that is transmitted between business entities.
Asset-related Concepts	
Business Asset	Submitted data
IS Asset	Input interface, Transmission medium, Server
Security Criterion	<ul style="list-style-type: none"> Confidentiality of the data. Integrity of the data.
Risk-related Concepts	
Risk	An attacker with the ability to intercept the medium intercepts a transmission between the input interface and the server, obstructs and modifies the data due to the transmission medium not being secure and data not being encrypted in the input interface and server, leading to the loss of the confidentiality of the data and loss of the integrity of the data.
Impact	<ul style="list-style-type: none"> Loss of the confidentiality of the data. Loss of the integrity of the data
Event	An attacker knowledgeable on how to intercept a transmission medium intercepts the transmission between the input interface and the server, obstructs and modifies the data due to the transmission medium not being secure and data not being encrypted in the input interface and server.
Threat	An attacker intercepts the transmission between the input interface and the server, obstructs and modifies the data.
Vulnerability	<ul style="list-style-type: none"> Non-secured transmission medium Data is not being encrypted in the input interface and server
Threat Agent	An attacker with the ability to intercept the medium.
Attack Method	An attacker intercepts the transmission between the input interface and the server, obstructs and modifies the data.
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Make the transmitted data unreadable to third parties. Cross verify the received data with the data sent from the original source.
Control	Cryptographic algorithm Checksum algorithm

In Figure 4.2 we identify as the main business asset the Submitted data that is represented by a resource. We identify as a security criterion for both actors (Server, Input Interface) the Confidentiality and Integrity of the submitted data. This security criterion has a positive contribution from the Maintain the integrity & confidentiality of the submitted data security constraint. Moreover, this constraint restricts the main goal of Data employed of the *Server* actor in addition to performing the same restriction to the Data submitted goal of the *Input interface*. In addition to the actor assets in Figure 4.2, the

dependency between the two actors is modeled. In this instance the **Submit Data** plan is the dependum between the two actors, and two constrains indicate that a double dependency occurs. In order for the dependency to be fulfilled and the plan to be executed and both actors are required to equally contribute.

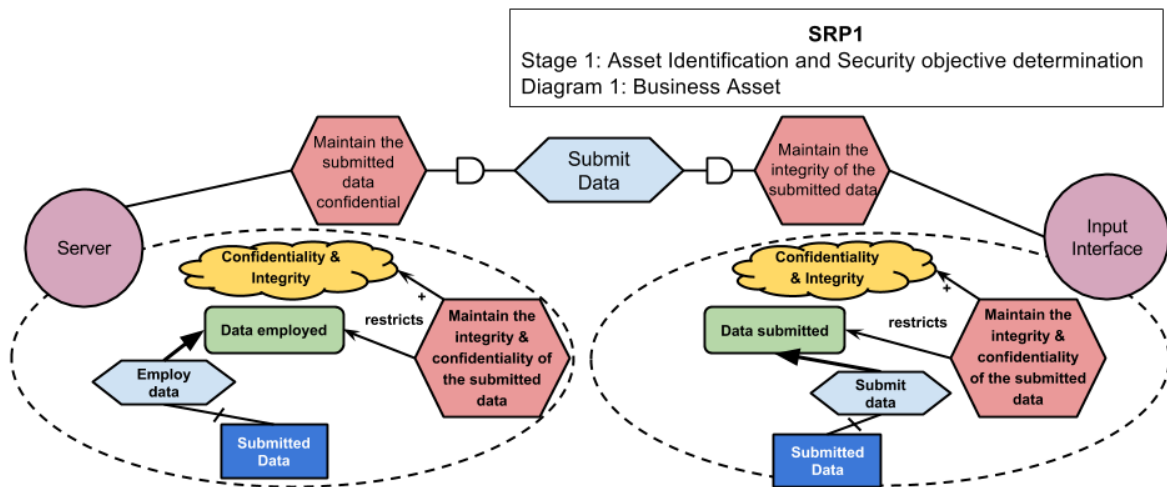


Fig 4.2 - SRP1 Modelling of Business Assets

Modeling the IS assets In Figure 4.3 we introduce the *Transmission Medium* actor that serves the purpose of transferring data from the *Input Interface* to the *Server*. Here the dependency between the *Server* and *Input Interface* is extended to include the *Transmission Medium* actor as well. Furthermore in this step the secure goal of **Data integrity & confidentiality ensured** is introduced satisfying the main constraints of the two actors. Moreover secure goals that are achieved by executing the secure plan of **Ensure the integrity & confidentiality of the submitted data** are introduced to satisfy the security constraints of both the *Server* and *Input Interface* actor.

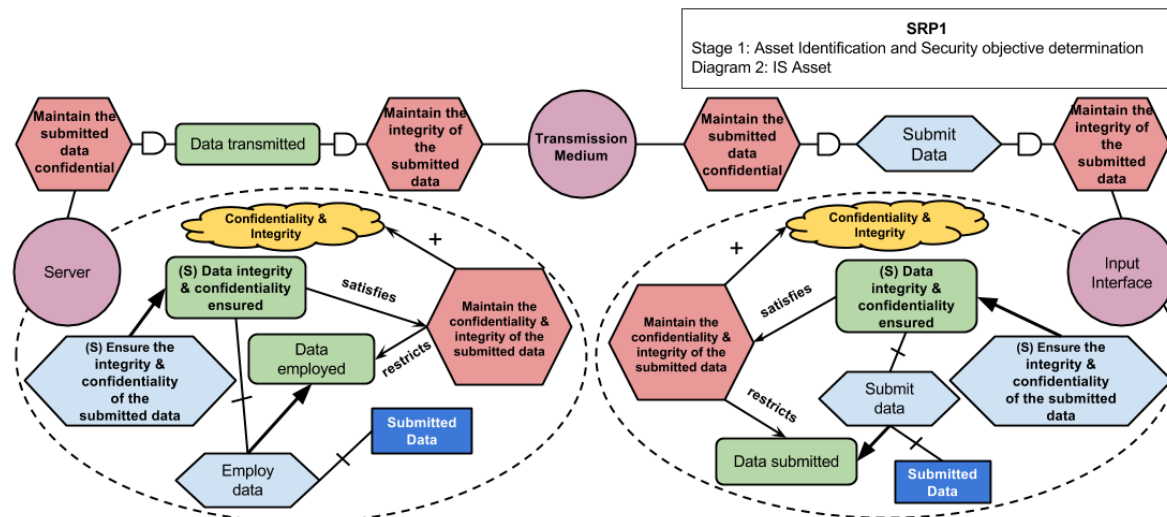


Fig 4.3 - SRP1 Modelling of IS Assets

In Figure 4.4 we identify as main security threat a *Man in the middle* attack that impacts the security criterion of **Confidentiality & integrity** of the transmitted data. In Figure 4.5 we represent **Submitted data** obtained as main goal of the attacker that is satisfied by the *Intercept transmission* plan that attacks the *Transfer the submitted data* plan of the *Transmission Medium* actor exploiting the non-fulfilment of the secure plan *Ensure the transmission is not intercepted*.

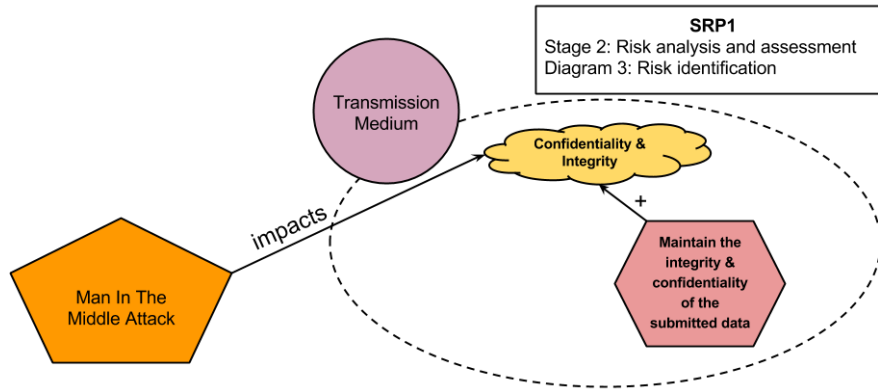


Fig 4.4 - SRP1 Attack Identification

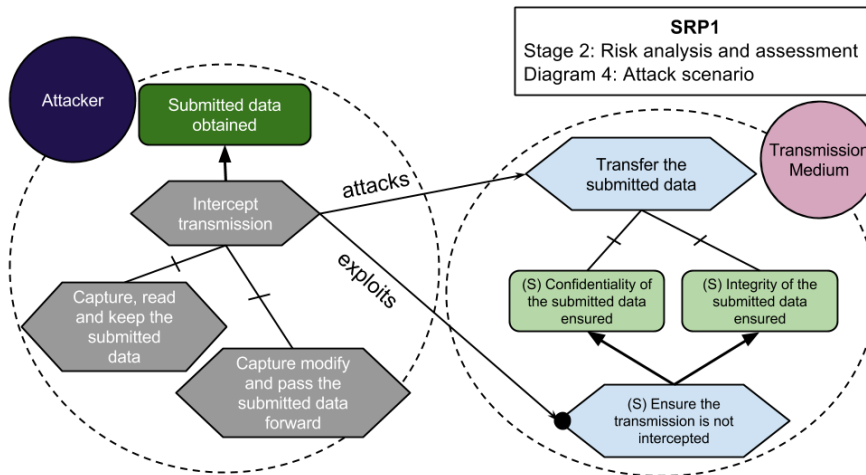


Fig 4.5 - SRP1 Potential Attack Scenario

In contemplation of the risks identified in the previous steps in Figure 3.6 we follow a risk reduction, risk treatment that mitigates those risks. We replace in both actors, the secure plan of the Ensure the integrity & confidentiality of the submitted data with the secure plan Perform cryptographic procedures and Perform checksum procedures. The replacements are performed in the according actor of the model. Here the dotted pattern of the constructs of each actor indicates, that they now all become security requirements that mitigate the Man in the Middle Attack.

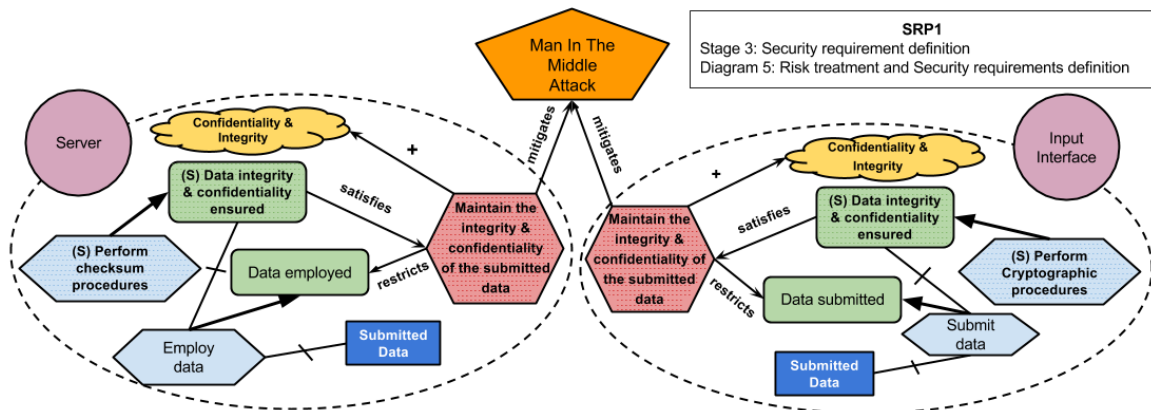


Fig 4.6 - SRP1 Risk Treatment and Security Requirements Definition

4.4 Summary

In this chapter we provided an overview of the security pattern landscape. We introduced our pattern representation process using the security risk-oriented pattern template and RAST. Moreover we introduced SRP1 one of the five SRP's that are part of this master thesis.

5 Security Risk-Oriented Patterns Used in Secure Tropos

In the previous chapters we introduced RAST and our SRP representation methodology. In this chapter we demonstrate in detail our pattern application process. In order to demonstrate our process we use a model extracted and adapted from (Yu, 1994). The selected model is an exempt from the designing phase of late requirements. The original modeling language used for the model is I*. We use the diagram from late requirements phase due to mainly one reason. In this phase, the system is introduced, making so that various interactions between the system and various actors can be identified. The pattern application process is as follows: Initially we search throughout the relevant literature and discover models relevant to this thesis. We pre-process the model in order to be compatible with RAST. We identify the occurrence of a pattern and extract all relevant assets to a new model. Then we introduce the various security mechanisms suggested by the SRP's. Finally re-introduce the extracted back in the initial model.

5.1 Model Pre-Processing

For the purpose of demonstrating the application process we use a model from the relevant literature. The selected model is extracted from (Yu, 1994) (See Figure 5.1). The model depicts a meeting scheduler service that automates meeting scheduling between various participants. Using a model from the literature, serves the purpose of validating the applicability pattern application process. Using this model we demonstrate that the pattern application process, is applicable to a variety of scenarios. In this section we overview the process employed in converting the running example model from I* modeling to RAST.

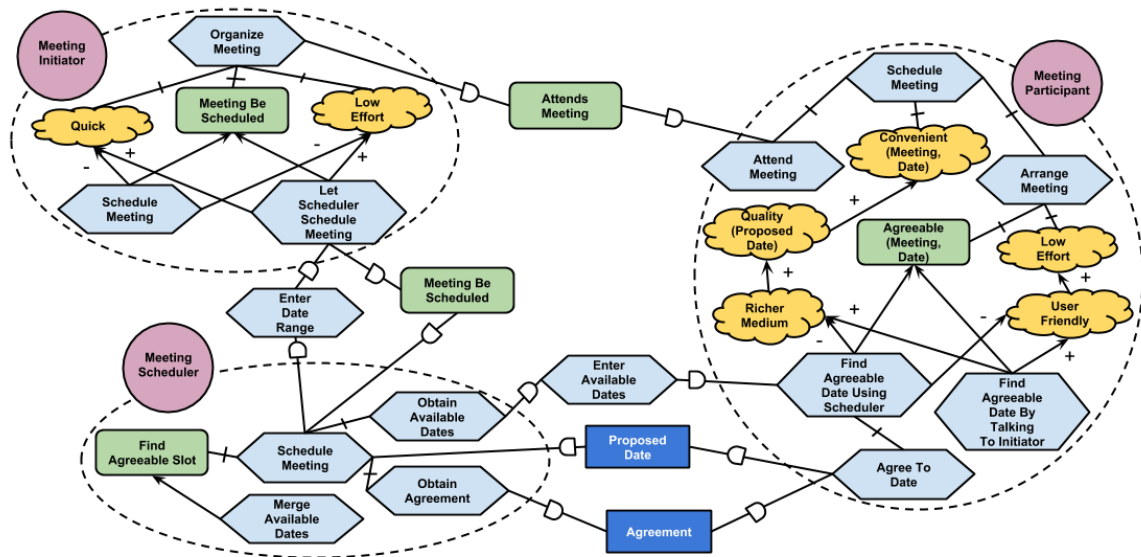


Fig 5.1 - Model for a computer-supported meeting scheduling configuration; adapted from (Yu, 1994)

The pre-processing process initiates by removing all non-essential or related to RAST elements. The resulting model can be viewed in Figure 5.2. We remove all the softgoals to reduce confusion. In I* this construct is used to depict non-functional requirements. In RAST softgoals are mainly utilized to represent security criteria. Moreover we add additional goals (Meeting data stored/retrieved), and rename (Agreeable (Meeting, Date) to Date Agreed) to the Meeting Scheduler due to their importance regarding the security of the system. Additionally we decompose using plans into resources

(Meeting Data, Date Data) that result from the employment of such plans from the meeting scheduler.

Following the manipulation of softgoals, goals and resources an analyst in this phase can follow one of two courses of action. First one being to terminate the pre-processing and move to the next stage. Second and as performed in this concrete case, is to apply the first stage of RAST. Here we point out that the possibility of modeling multiple security criteria together in one construct, for a given goal/plan/resource/dependencies exists. This practice is encouraged due to serving the double function of, reducing the required space in the diagram and is more distinguishable.

It is important to be noted that we do not apply security constraints to the whole model. We instead apply them only to assets involved in the pattern application process in Section 5.2. This is done in order to reducing presentation complexity.

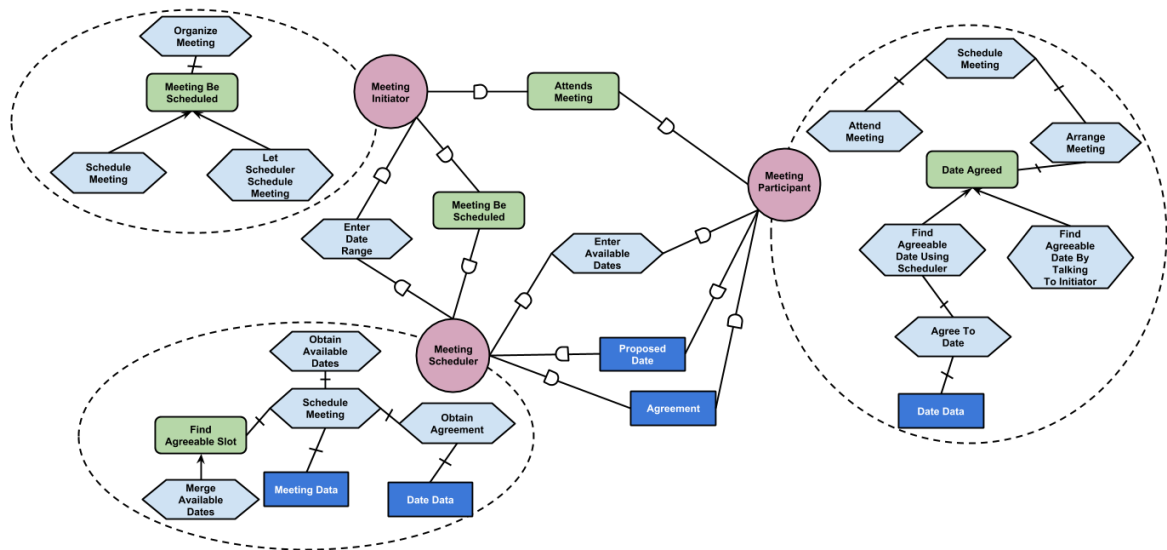


Fig 5.2 - Meeting Scheduler Example without Security Constraints Applied

5.2 Pattern Application Process

In this section we present in detail our proposed pattern application process. The model used as a basis to demonstrate our process is the model in Figure 5.3. The depicted model, was pre-processed and will be used to demonstrate the process of applying pattern SRP1 illustrated in Chapter 4.

STEP 1 - OCCURRENCE IDENTIFICATION & ASSET ALIGNMENT

In this step we manually search within the given system and evaluate if a pattern is applicable to a given scenario. In the model of the Figure 5.1 we aim to apply SRP1 that we presented previously. Main goal of SRP1 is to secure communications between two actors from a “*man in the middle*” attack. As stated, initially we examine the model and determine if the assets of the model align to the assets of SRP1. After observing the model we extract the scenario where a participant enters a meeting date and that is transmitted to the meeting scheduler. We advance by evaluating the alignment of the individual components involved:

- The Meeting Scheduler actor aligns to the Server actor of SRP1 given the similar interactions with the other actors.

- The Meeting Participant aligns to the Input Interface due to the connection to the Meeting Scheduler/Server. Given that a 1:1 occurrence not existing between SRP1 and the scenario under investigation, we assume that the Meeting Participant fulfils the Agree to Date plan by using an *input interface* provided by the Meeting Scheduler. This is why we rename the Meeting Participant actor to Meeting Participant Interface.
- As Transmission Medium we assume that such a structure exists in order to support the communication between the Meeting Participant and the Meeting Scheduler.

Moreover in order for the desired pattern to be applicable, the type of dependency should match, namely a double dependency should exist. According to SRP1 the Input Interface relies on a transmission medium to transmit data to the Server. In order for the data to be transmitted and the plan of Submit data has to be completed. Similarly, we assume, that the Enter Available Dates plan follows a similar process.

By making the previously mentioned alignments and assumptions, we ensure that the pattern is applicable to the model. Next we extract the portion of the model (see Figure 5.4) that corresponds SRP1. In the next steps we progressively place the matching security mechanisms in the assets suggested by the pattern.

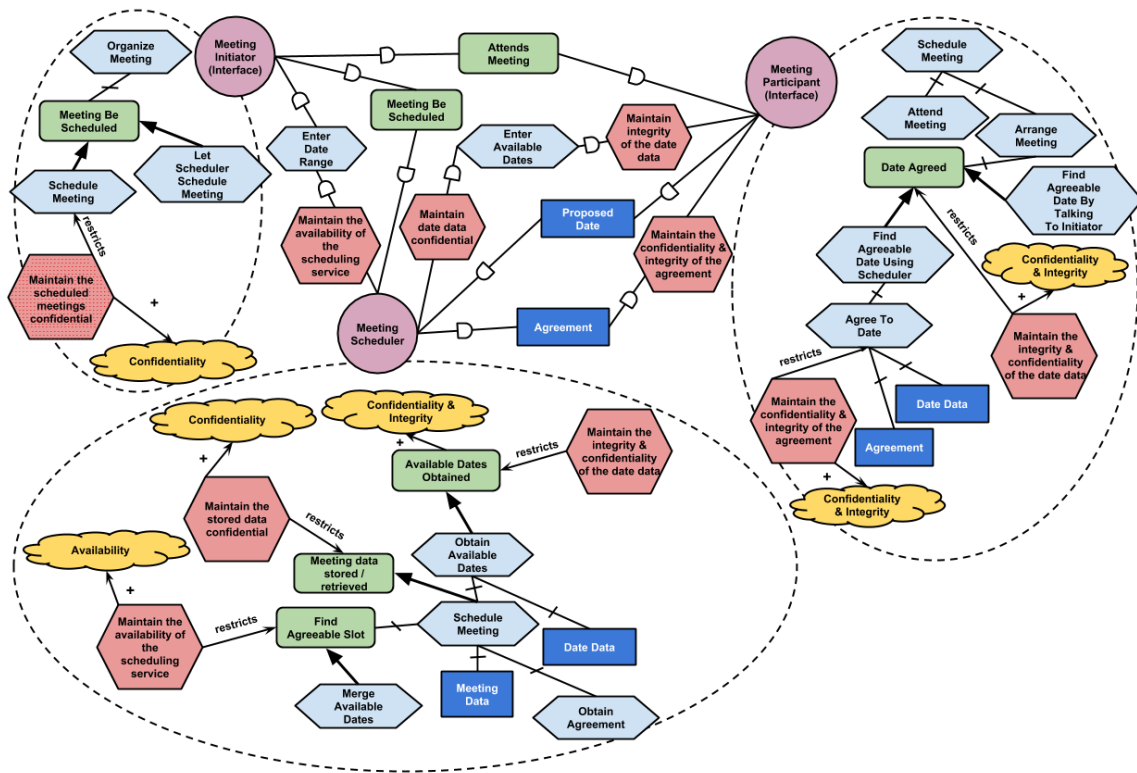


Fig 5.3 - Meeting Scheduler Running Example with Security Constraints and Criteria

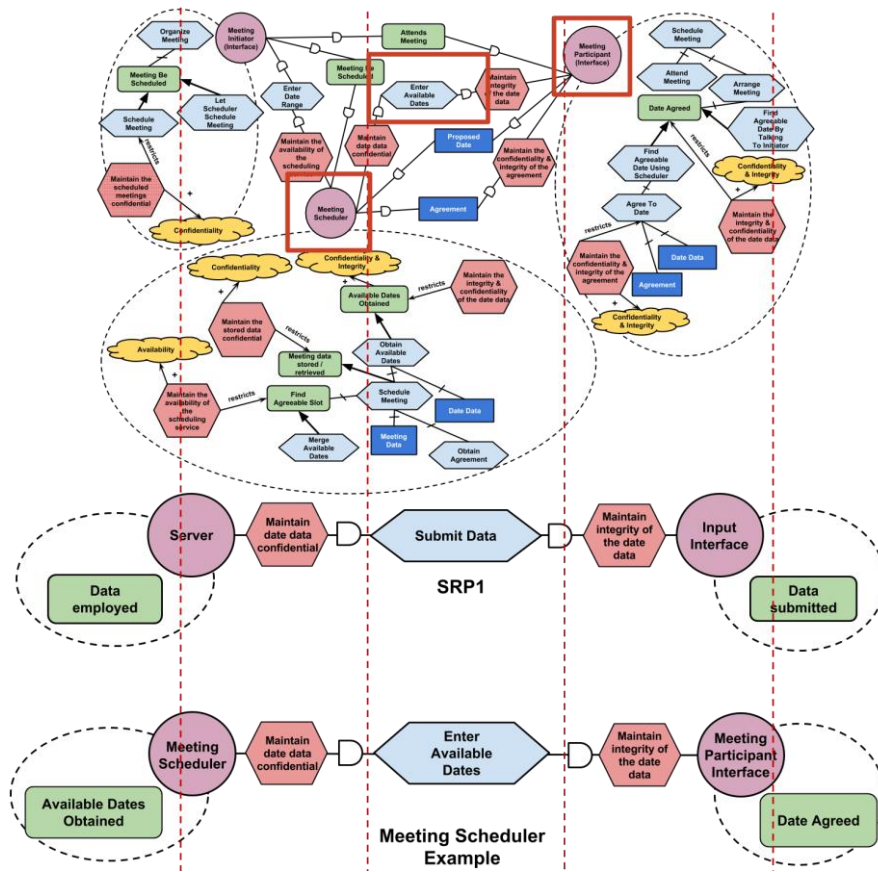


Fig 5.4 - SRP1 occurrence in model

STEP 2 - ASSET EXTRACTION & SECURE GOAL INTRODUCTION

In this step we start by extracting the portion of the model relevant to the pattern. Depending on whether security criteria were identified in the pre-processing step or not. In this step vulnerable assets are identified and security criteria and constraints are introduced. Here additionally we introduce in the diagram the Date Data resource that is not present in the original model given its low granularity. We introduce the resource here because it is crucial for the representation of the scenario. The process follows closely the RAST methodology of separately illustrating business and IS Assets as seen in Figure 5.5, 5.6. Additionally in this instance we introduce the secure goals and secure plans suggested by the pattern (see Figure 5.6). The secure goals and plans are introduced to their aligned goals.

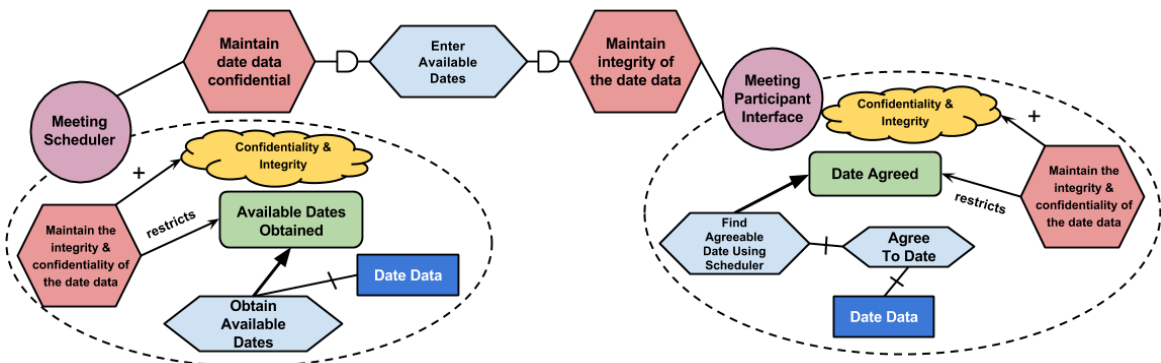


Fig 5.5 - Pattern Application Example, STEP 2 (a)

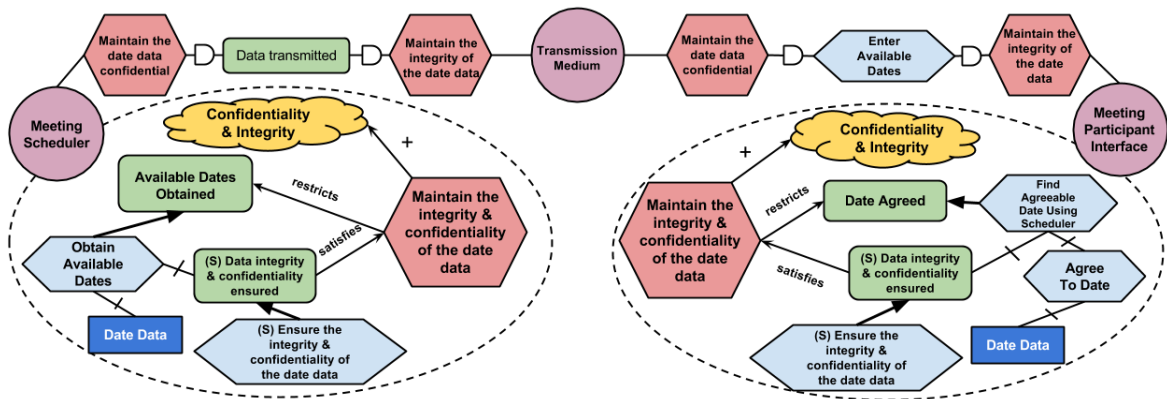


Fig 5.6 - Pattern Application Example, STEP 2 (b)

STEP 3 - SECURITY REQUIREMENT INTRODUCTION

Following the identification of the secure goals and plans suggested by the pattern we introduce the security requirements (see Figure 5.7). These requirements satisfy the secure goals that were introduced in STEP 2. The introduction of a requirement is performed by replacing existing vulnerable asset in our case **Ensure the integrity and confidentiality of the date data**. The assets are replaced in this case by the security requirements suggested by SRP1 (Perform checksum procedures, Perform Cryptographic procedures). As illustrated in the diagram and suggested by SRP1 the introduction of these requirements results in the mitigation the threat “*man in the middle attack*”

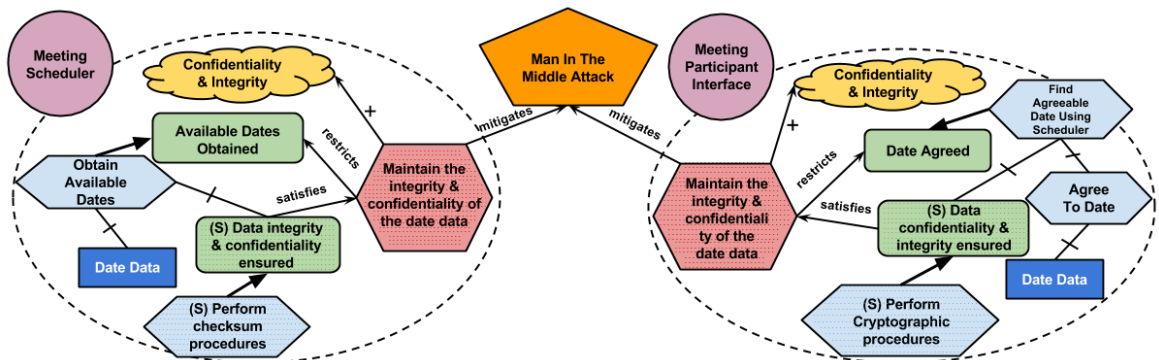


Fig 5.7 - Pattern Application Example, STEP 3

STEP 4 - SECURITY REQUIREMENT RATIONALE & VALIDATION

In this step using the diagram of Figure 5.8 we validate the newly introduced requirements. Here as the pattern suggests a “*Man in the middle attack*” is performed that attacks the transmission of the data. In case we apply the pattern and such an event does occur the date data will be encrypted and unusable to the attacker, additionally the event will be detected by the performance of the checksum algorithms, which will identify the occurrence and report it, so the breach will be detected and addressed accordingly. By observing the model we can see the direct impact of the non-employment of the previously stated security requirements, namely the Integrity and Confidentiality of the date data being compromised in the events of an attack.

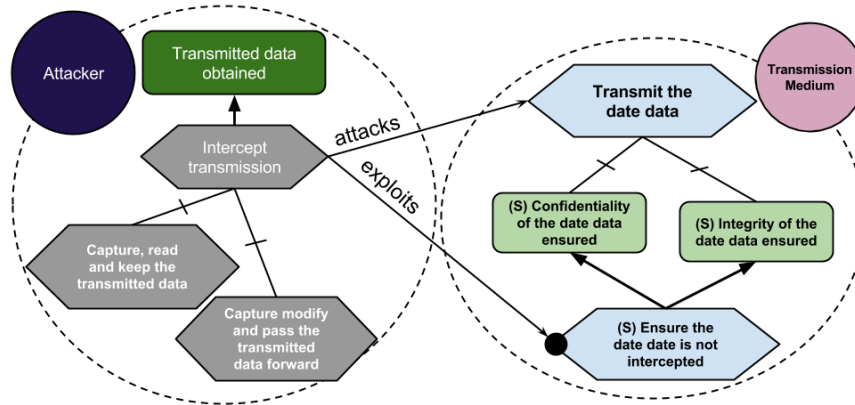


Fig 5.8 - Pattern Application Example, STEP 4

STEP 5 - MODEL INTEGRATION

In this step the security requirements with the additional secure mechanisms are integrated back into the main model (see Figure 5.9). Here we outline the newly introduced assets for ease of detection. Moreover is important to note that the pattern application process same as the RAST process is of an iterative nature and when one application is concluded more iterations can be performed.

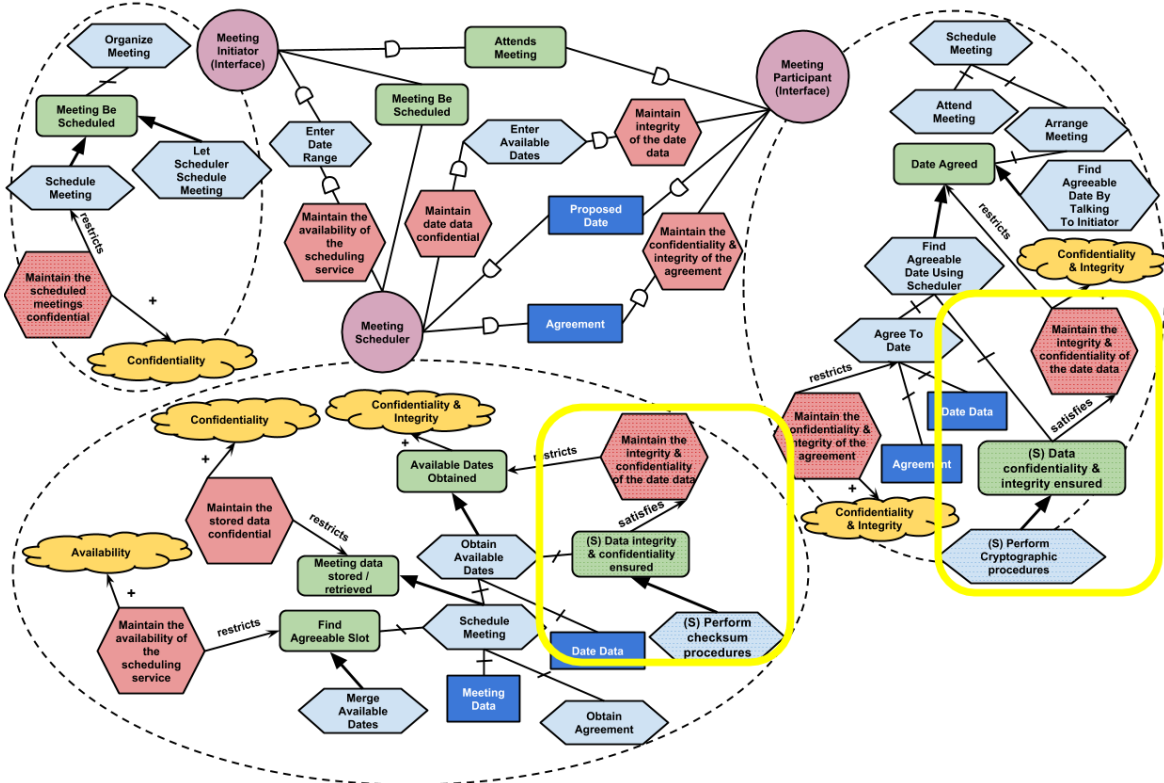


Fig 5.9 - SRP1 Integrated in the Main Model

5.3 Other Patterns

In this section we present all our proposed patterns applied to the meeting scheduler module. Given that the application process is illustrated in detail in the previous section. Here we present a brief overview of the process followed for each pattern. Additionally we overview all the security enhancement achieved.

SRP2 - Securing business activities from submitted data

SRP2 is relevant to our Meeting Scheduler example model due to its function to secure a business activity, against accepting and propagating malicious scripts. In this concrete scenario the meeting scheduler sends a proposed date to the meeting participant, and the participant responds with an agreement. In the extracted portion of Figure 5.10 we assume an existing possibility to attach an attachment along with the agreement, or sending a malicious agreement response exists. SRP2 introduces a filtering mechanism (see Figure 5.11) that monitors the incoming data and rejects any type of document that doesn't cope with the requirements, thus securing the system. In the concrete case of the scenario a filtering mechanism is in place making so only the desired data is passed to the meeting scheduler.

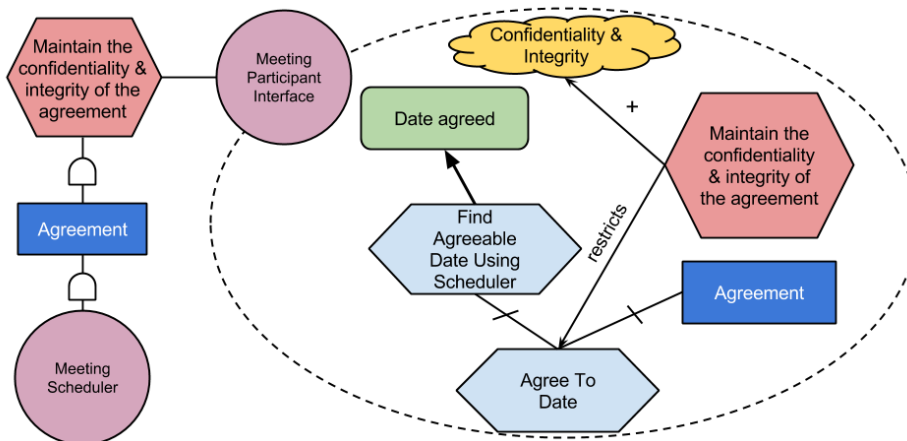


Fig 5.10 - SRP2 Occurrence in the Meeting Scheduler Example

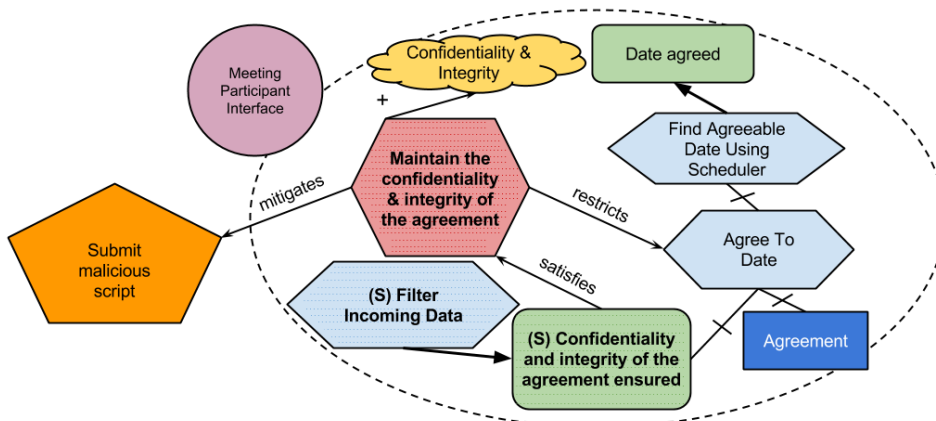


Fig 5.11 - SRP2 Applied in the Meeting Scheduler Example

SRP3 - Securing business activities from DoS attacks

SRP3 is applicable in the Meeting Scheduler actor due to the fact that the main function is to secure a system, against “denial of service” attacks. In the context of SRP3 the attackers render the service unavailable by sending multiple requests to a service thus compromising its ability to respond to each and every one of them. Here SRP3 proposes the introduction of a mechanism that monitors the number of requests and if a fluctuation occurs the system detects the malicious occurrence and doesn’t respond to the malicious requests. In the extracted portion of Figure 5.12 of the scenario an attacker pretending to be a meeting initiator floods the meeting scheduler by sending multiple date ranges thus rendering the scheduler system unavailable for other users. By employing the security requirements suggested by SRP3 (see Figure 5.13) the meeting scheduler is able to monitor the requests and reject the malicious ones if that occurs.

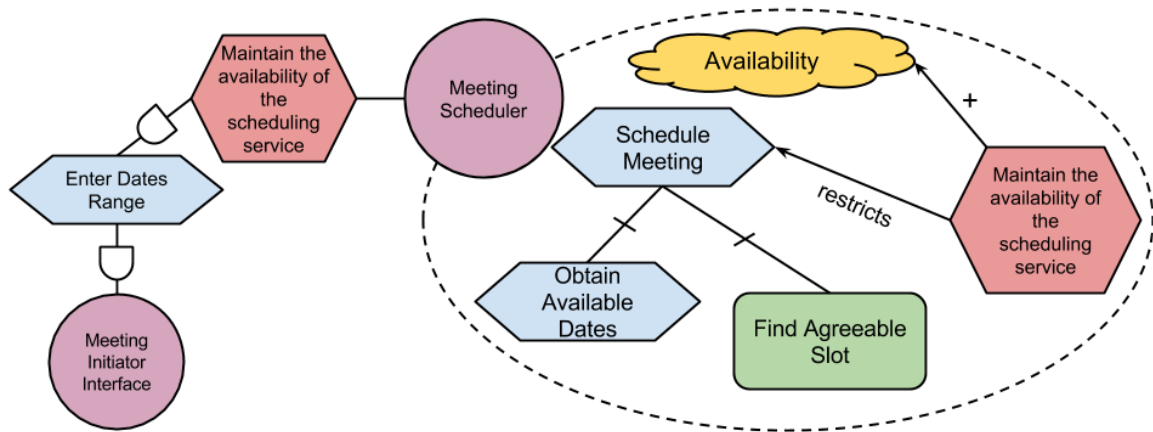


Fig 5.12 - SRP3 Occurrence in the Meeting Scheduler Example

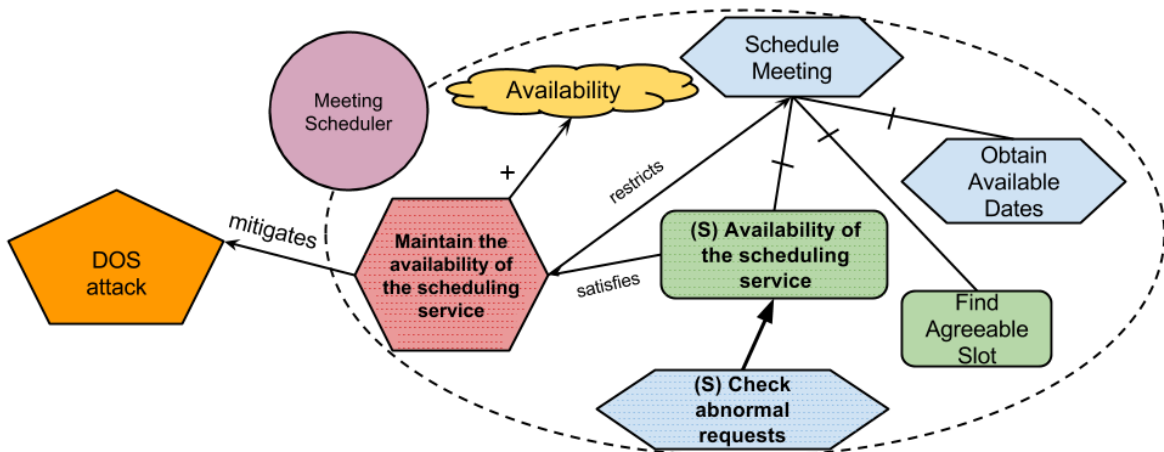


Fig 5.13 - SRP3 Applied in the Meeting Scheduler Example

SRP4 - Securing business data from unauthorized access

SRP4 applies to the model from the literature due to the reason that secures a system, against attacks of unauthorized access of data and other information. In the context of SRP4 the attackers taking advantage of no access control being in place, accesses confidential business data that he is not authorized, causing perpetual harm to confidential information. Here SRP4 suggests the introduction of a mechanism that checks if a user that accesses certain information, has the appropriate clearance. In the concrete case of the meeting scheduler (see Figure 5.15), anyone using the meeting initiator interface has access to the meeting scheduler, can schedule a meeting thus compromising confidentiality of scheduled meetings. By employing the SRP4 suggested security requirements (see Figure 5.15) the meeting initiator interface is able to at first confirm if a user has the appropriate clearance to access a meeting information and then provides accordingly access or not.

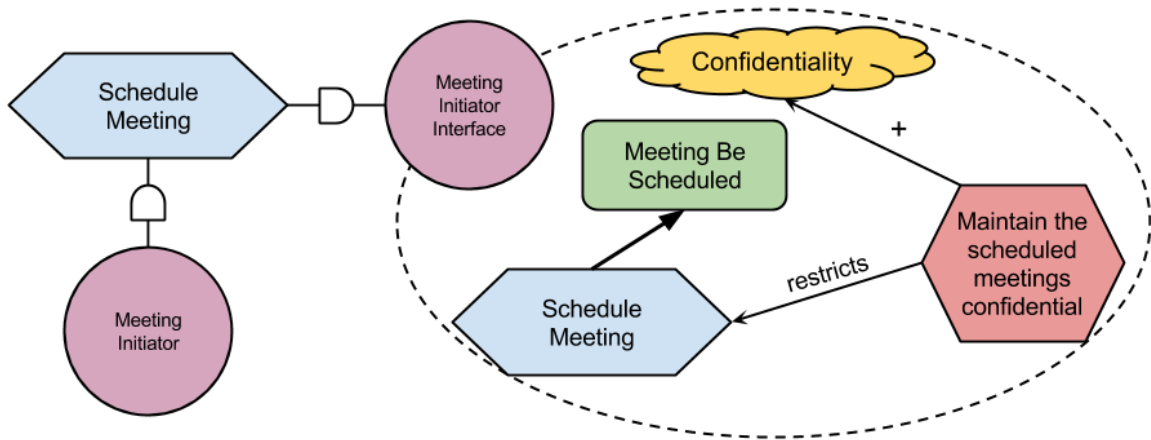


Fig 5.14 - SRP4 Occurrence in the Meeting Scheduler Example

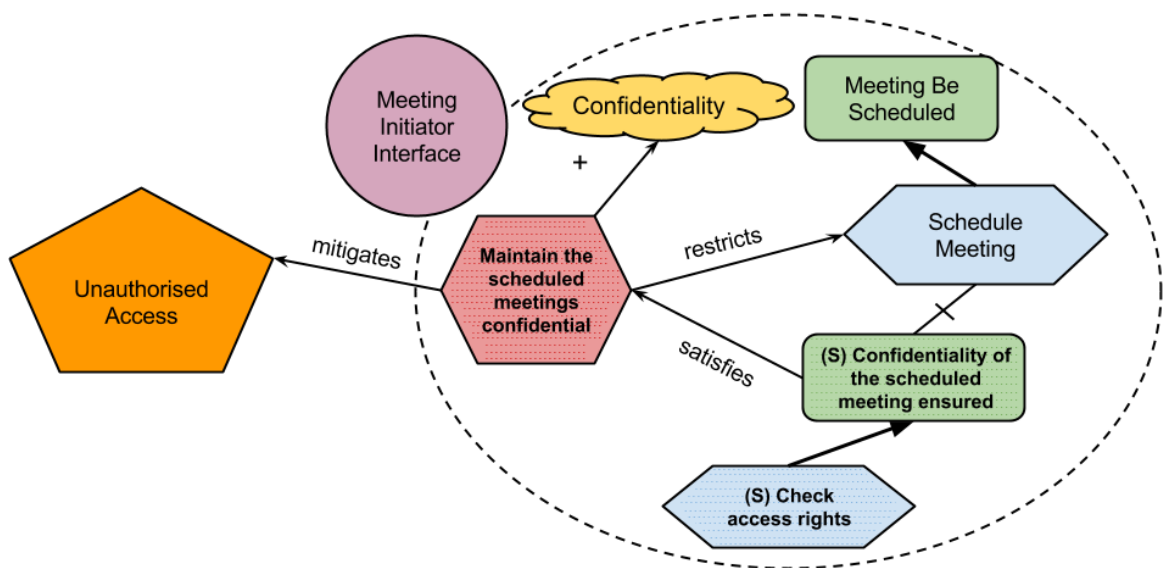


Fig 5.15 - SRP4 Applied in the Meeting Scheduler Example

SRP5 - Securing business data stored/retrieved from a data store

SRP5 is applicable in this scenario due to the main property to secure a system, against access of data that is stored in plaintext. In the context of SRP5 the attackers taking advantage that the data is being stored in plaintext, accesses, reads and obstructs it from the data store. Here SRP5 suggests the introduction of a mechanism that encrypts the data before it is stored in the data store thus rendering it illegible. Moreover if a request for accessing the data is perform the data is decrypted and thus delivered in a legible state. In the concrete case (see Figure 5.16) of the scenario as-is, any information regarding meetings is stored without any explicit encryption thus being vulnerable to attacks. By employing the SRP5 requirements (see Figure 5.17) the meeting scheduler is able to accordingly encrypt and decrypt any meeting data making it safe against attacks mentioned above.

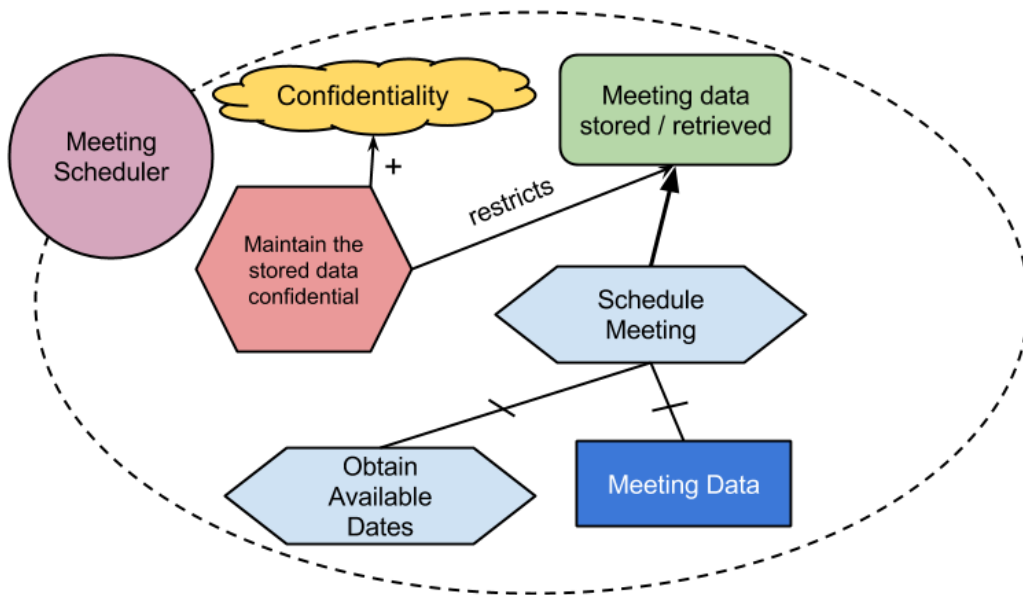


Fig 5.16 - SRP5 Occurrence in the Meeting Scheduler Example

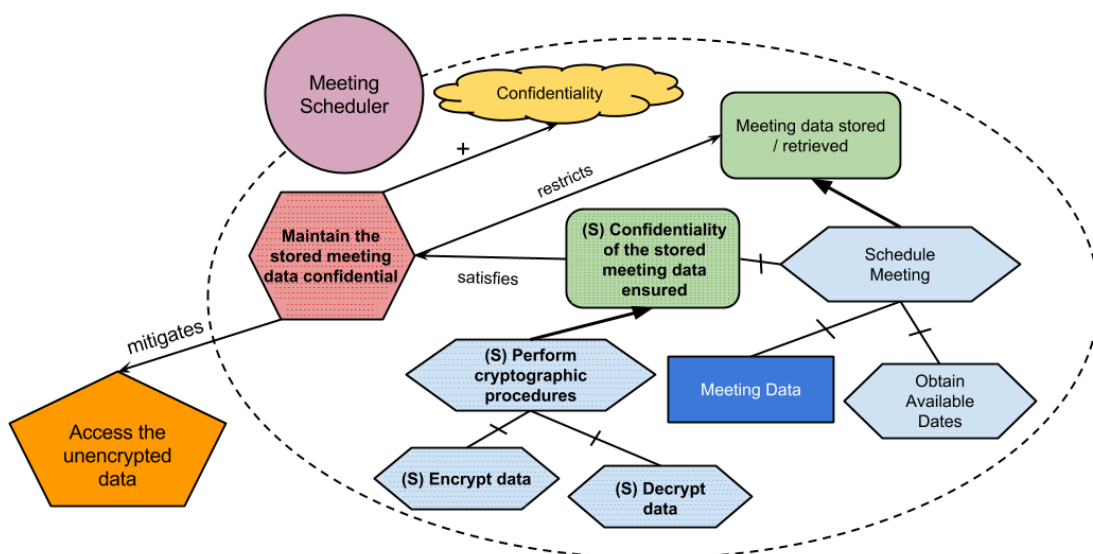


Fig 5.17 - SRP5 Applied in the Meeting Scheduler Example

The model with all the patterns discussed in this thesis applied can be seen in Figure 5.18. In this point we can observe the level of granularity that RAST introduces, making so that the entire system security can be overview by one single diagram. Nonetheless is important to mention that one of the major drawbacks of RAST is that the models/diagrams grow large in a very quick and this one of the issues to be tackle in future works.

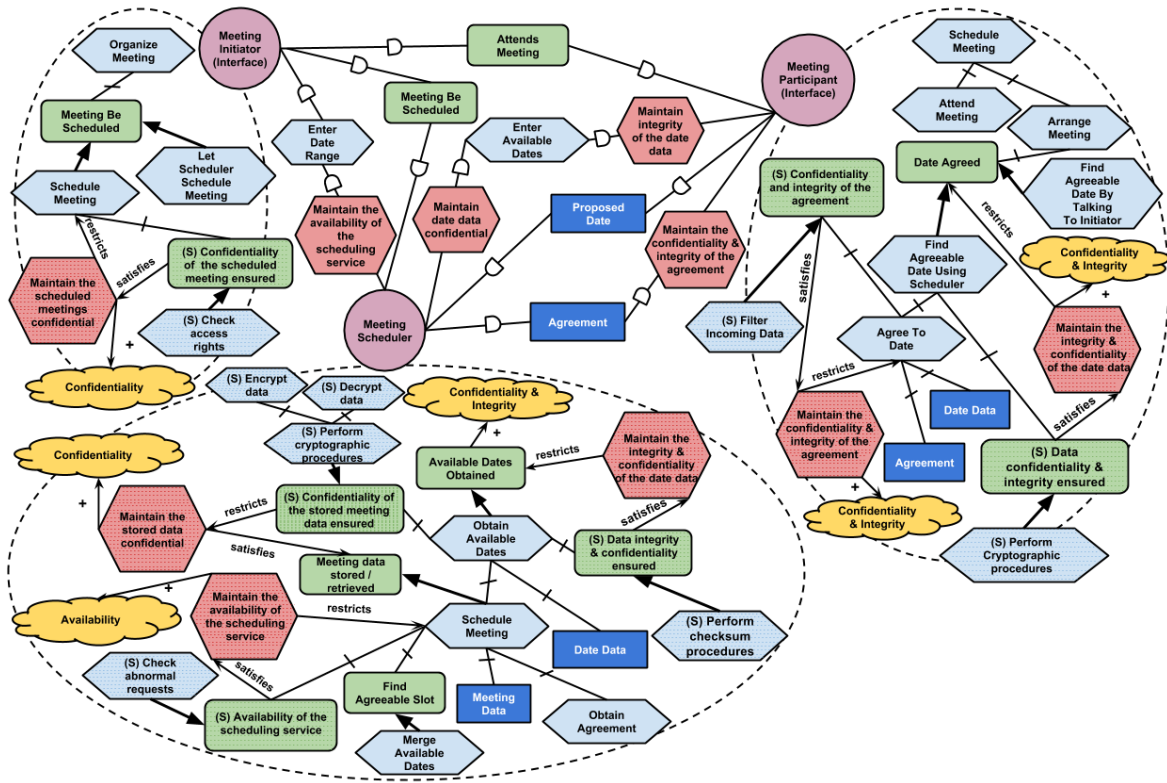


Fig 5.18 - The Entire Model with All the Patterns Applied

5.4 Further Steps

Following the completion of the application process of the patterns, a further suggested step would be to remove all the security constrains and criteria from the model in order to provide a clearer view of the system at hand. Moreover although it is outside the scope of this thesis, a trade-off analysis should be performed in order to select the most effective controls in terms of security and cost required for their implementation. Not all the requirements and controls introduced by the patterns are mandatory to be implemented within the system. We suggest following the process described in (Mayer 2009) where metrics are derived through the GQM method and costs are estimated through the ROSI concept in order to priorities and select the best course of action.

5.5 Summary

In this chapter we presented our pattern application process using SRP1. Moreover we briefly described the results of applying the rest of our proposed patterns. Finally we provide a brief description of further steps that can be taken after the completion of the pattern application process.

6 Validation

This chapter demonstrates the process followed in order to validate the proposed patterns and usability of the pattern application process. All participants of the case study were individuals with a software engineering background. Participants were required to undergo a small training regarding ISSRM, RAST, the proposed patterns expressed in RAST and the proposed pattern application process. Following the training, the participants were given a task involving the application of our proposed patterns, expressed in RAST into a model. Finally, a questionnaire was filled in order to assess the usability of the overall process. Moreover, the time required for the completion of the process by a participant was over three hours.

6.1 Case Study Questions

We consider the following questions:

- CSQ1. What is the correctness of the pattern applicability by the participant?*
- CSQ2. How understandable is the pattern application process for participants with a ISSRM background vs. participants without a ISSRM background?*
- CSQ3. What is the usability of the pattern application process?*

6.2 Introductory Lecture

In the beginning of the case study, we delivered an introductory lecture of the involved concepts. In this lecture we introduced the participants with the core concepts of the ISSRM domain model in addition to the risk management process. We continued with the introduction of the core concepts of RAST, giving an appropriate overview and an example of it. As an example for demonstrating RAST, we utilised the running example illustrated in the second chapter of the thesis. Additionally we provided a brief description of our representation of SRP1. The lecture was concluded with the demonstration of the pattern application of SRP1 to the model of chapter 5.

6.3 Pattern Application Task

After the introductory lecture, the participants were required to perform a task. The task focused mainly on the pattern application process described in Chapter 5. Participants were given a model described in Section 6.4 and were required to identify a pattern occurrence as well as apply the pattern. Participants were also given additional materials which included our pattern representations of the SRP's as well as the pattern application chapter of this thesis.

6.4 Case Study Model

Following the introductory lecture the participants were required to apply our proposed patterns to a model from the literature. The model was selected on the basis of two main criteria: ease of understanding and applicability of the patterns. The model of Figure 6.1 adapted from (Altuhhova, 2013) with the minor interventions fulfils both this two criteria. The model is of an internet store where a user registers to the service and his data

is processed accordingly. Important to enhance that the model does not include security criteria, constraints, goals or plans.

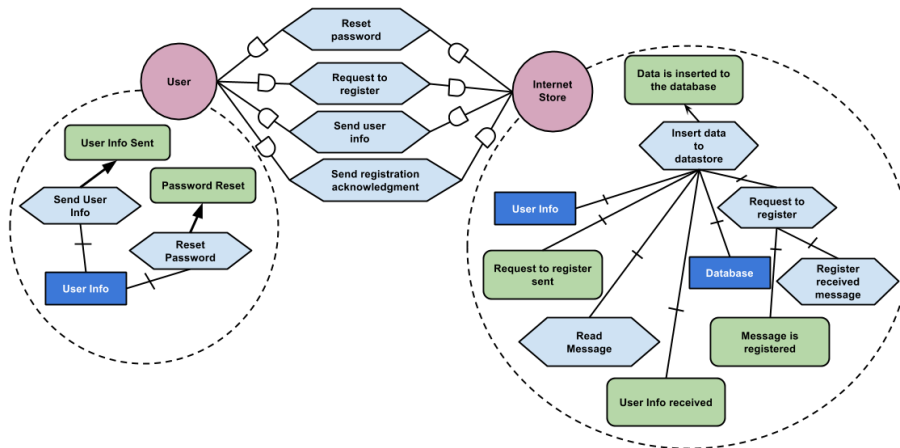


Fig 6.1 - Internet Store Registration; adapted from (Altuhhova, 2013)

6.5 Case Study Questionnaire

The questions of our questionnaire are focused on the usability of the RAST process, SRP's and pattern application process. The questions regarding RAST are included as an additional indicator of how the RAST process affects the overall process of presenting and applying an SRP. Questions aimed on determining how RAST affects the overall process evaluated the easiness and understandability of the process. Questions directed towards determining the usability of the individual patterns (without being applied) evaluated the easiness, satisfaction and understandability of the process. Questions aimed at determining the usability of the pattern application process evaluated easiness, satisfaction and understandability of the overall process. The individual answers from each participant in the case study can be found in the Appendix

6.6 Case Study Participants

We divided the participants of this case study into two main groups, GROUP A and GROUP B. In GROUP A we included participants with an IS-security background, who are working in the field of enterprise security and have prior knowledge of the ISSRM concepts. In GROUP B we included participants with a non-IS-security background, who have a software engineering background but lack knowledge regarding ISSRM concepts. The establishment of two groups was necessary to determine, how no prior knowledge of the topic affects the overall results. Individual background regarding each participant can be viewed in the Appendix. Given that each study required a considerable amount of time to be completed, the participants did not perform the pattern application process for all the patterns proposed in this work. The patterns applied by each participant can be viewed in Table 4. In this instance and the rest of the work we refer to the participants by a designated letter Participant A is referred as PA, Participant B is referred as PB and so on. PA, PB and PC belong to GROUP A. PD, PF and PE belong to GROUP B.

Table 4 - Patterns Applied by Each Study Participant

		SRP1	SRP2	SRP3	SRP4	SRP5
GROUP A	PA		X		X	
	PB					X
	PC	X		X		
GROUP B	PD				X	
	PE	X				
	PF		X			

6.7 Threats to Validity

In this section we describe what we consider to be threats to our validation process.

- The number of participants in the study is rather small (six participants) thus the sample may not be accurate. Making so that the results might differ if a larger number of participants are part of the study.
- The two different groups of participants involved in the case study were divided by generalising the participant's background. This was due to lack of participant with identical backgrounds. Selecting participants with identical backgrounds could influence the results of the study.
- Throughout the process of the study, participants received assistance. Questions regarding the process and other related matters were answered while performing the various tasks. It is estimated that in case the participant would not be assisted during the study results would differ.
- The conduction of each process required roughly three hours from the beginning to the end. Moreover, it was performed in various uncontrolled environments. Performing the study in a shorter or longer amount of time would have an impact on the results. In addition conducting the study in controlled environment would as well impact the results.
- Each of the different case studies were conducted separately. The participants were isolated from each other and the process was performed separately. If the study were to call for all the participant to participate in the study the results might differ due to participant cooperating or sharing or non-disclosing information between them.
- Each participant applied a different pattern. Ideally, all of the participants would have to complete all the patters for better results.
- Each participant had a different level of information retention from the case study lecture. No measure was implemented to reassure the level of retention. The implementation of such measure would result in all the participants having the same information retention. Thus the results would be more reliable.
- Participants had a varying level of prior knowledge of the concepts of ISSRM. Having participants with the same levels of ISSRM background knowledge would deliver more reliable result.

- The majority of the participants implemented the models using an online drawing tool. Implementing the models by hand or other method could impact the results of the process. Depending on the method the participants could deliver less accurate models or the opposite.
- The participants were not told that they were expected to perform in a certain way or that a specific result was expected from them. Stating expectations upfront would impact the overall performance of the participants. The performance could be enhanced in case the participant would want to perform according to the expectations. Or the participant could suffer from a type of performance anxiety and his result would be negatively affected.
- Participant had prior acquaintance with the conductor of the case study and author of the thesis. If no prior acquaintance would occur participants could not ask the same questions or perform in the same manner they would perform to another individual.
- A number of patterns were easier to be identified in the model comparatively to other patterns that were less obvious. If all the patterns would be identical in terms of identification ease the result would differ. Making a pattern easier or harder to identify results in the pattern application process becoming automatically easier or harder to be performed.

All the above factors had a high level of contribution to the overall results of the case study. We assume that in case of a more extensive study with a greater number of participants and different separation different results might be produced from the study.

6.8 Individual Participant Task Results

In this section we overview the results regarding the correctness of the tasks performed by the case study participants. Detailed reports for each of the participant's results can be found in section VI of the Appendix.

The correctness of each application is measured regarding the errors that were performed during the process. Hereby lower numbers denote higher correctness and vice versa. Errors are divided in two categories *Phrasing* and *Modelling* errors. Phrasing errors describe any error in regards to the phrasing of any of the components (e.g. labels in goals, plans, etc.) of the model. Modelling errors describe errors in regards to errors performed in the modelling of each asset of a model. Modelling errors include using wrong, linking between assets, dependency and asset modelling. Additionally as modelling mistakes are considered wrong colouring of the constructs. In order to determine a standard for measuring correctness we compare each of the models of the participants to the correct models depicted in section VII of the Appendix.

In Table 5 we overview the number of errors each participant performed. Comparing the total errors we can observe that PB made the least amount of errors compared to the other participants. Important is to point out that the errors of PA were minor in comparison to phrasing errors of the other participants. Thus if we were to overlook them PA would have no errors for the application of SRP2. Overall it is observed that the majority of the errors that the participants performed were phrasing errors. This is attributed to the non-existence of clear definitions in regards to phrasing.

Table 5 - Case Study Participant Pattern Application Errors

	Phrasing Errors	Modelling Errors	Total
PA (SRP2)	20*	0	20*
PA (SRP4)	_* ²	_* ²	_* ²
B (SRP5)	0	4	4
PC (SRP1)	11	0	11
PC (SRP3)	16	0	16
PD (SRP4)	11	0	11
PE (SRP1)	26	13	39
PF (SRP2)	10	0	10

* Minor Mistakes

*² Not Eligible for error counting due to the participant not using an existing construct but assumed that the system includes the functionality.

6.9 Case Study Group Comparative Discussion

GROUP A participants were able to apply and fully comprehend the described patterns as well as the pattern application process. GROUP B participants able to apply and moderately comprehend the patterns described in this work. GROUP A participants followed correctly all the pattern application steps described in the application process. Nonetheless mistakes were made in phrasing and resource decomposition. Moreover, they performed all the tasks given in a reasonable time frame and were confident in their results. GROUP B participants completed the pattern application process with moderate correctness. Similar to the participants of GROUP A, GROUP B made mistakes in phrasing and modeling. Furthermore, noticeable difference in the results was the level of confidence in the results of the application process. Participants of GROUP B were notably less confident than the participants of Group A in their results. Important to point out that the IS security background of these participants had a small impact to the overall results.

6.10 Questionnaire Summary of the Results

In this section we summarise the answers the participant gave to the questionnaire received after the completion of the study. All the questions required from the participants to answer on one of the different levels of ease, understandability and satisfaction. Namely the questions were separated in:

Not at all, Slightly, Moderate and Very...easy/understandable/satisfied.

With 'Not at all' being the lowest and 'Very' being the highest possible mark. The answers to the questionnaire in detail can be found in section VIII of the Appendix.

- The majority of the participants found that the RAST application process is moderately easy. (see Question 1 of section VIII in the Appendix)
- The participants of GROUP A found the RAST application process moderately understandable whereas participants of GROUP B found it slightly understandable. (see Question 2 of section VIII in the Appendix)
- The majority of participants found the patterns expressed in RAST moderately easy to learn. (see Question 3 of section VIII in the Appendix)
- The majority of the participants of GROUP A were very satisfied with the RAST patterns overall whereas participants of GROUP B were moderately satisfied. (see Question 4 of section VIII in the Appendix)
- The majority of participants found the patterns expressed in RAST moderately understandable. (see Question 5 of section VIII in the Appendix)
- All the participants of GROUP A found the pre-processing of a given model moderately easy whereas participants of GROUP B found it slightly easy. (see Question 6 of section VIII in the Appendix)
- The majority of the participants in both groups found identifying goals/plans/resources/dependencies that are under risk moderately easy. (see Question 7 of section VIII in the Appendix)
- Overall the participants of both groups found applying constraints and security criteria to goals/plans/resources/dependencies moderately easy. (see Question 8 of section VIII in the Appendix)
- Overall the participants of both groups found the identification of where a pattern is applicable moderately easy. (see Question 9 of section VIII in the Appendix)
- The majority of the participants of GROUP A found extracting the assets involved in a pattern from the main model, moderately easy whereas participants of GROUP B found it slightly easy. (see Question 10 of section VIII in the Appendix)
- Overall the majority of the participants of both groups stated that replicating and adjusting a pattern to a previously unknown model moderately easy. (see Question 11 of section VIII in the Appendix)
- The majority of the participants of GROUP A found identifying and applying secure goals to the assets of an actor slightly easy whereas participants of GROUP B found it moderately easy. (see Question 12 of section VIII in the Appendix)
- The majority of the participants found replacing secure goals with the controls suggested by a pattern moderately easy. (see Question 13 of section VIII in the Appendix)
- The majority of the participants found re-integrating the previously isolated portion of the main model with the security requirements applied moderately easy to be performed. (see Question 14 of section VIII in the Appendix)
- Participants of GROUP A found the security requirement introduction and re-integration of an extracted model step of the pattern application process as the hardest to perform whereas participants of GROUP B found occurrence identification, re-integration of an extracted model and security requirement introduction as the hardest. (see Question 15 of section VIII in the Appendix)

- Participants of GROUP A found the occurrence identification step of the pattern application process as the easiest to perform whereas participants of GROUP B found occurrence identification and asset extraction and secure goal introduction as the easiest. (see Question 16 of section VIII in the Appendix)
- The majority of the participants found the pattern application process to be moderately easy to learn overall. (see Question 17 of section VIII in the Appendix)
- The majority of the participants found the pattern application process to be moderately easy. (see Question 18 of section VIII in the Appendix)
- The majority of the participants found the pattern application process to be moderately efficient. (see Question 19 of section VIII in the Appendix)
- The majority of the participants found the pattern application process to be moderately understandable. (see Question 20 of section VIII in the Appendix)
- The majority of the participants of GROUP A were moderately satisfied but the overall process whereas participants of GROUP B were slightly satisfied. (see Question 21 of section VIII in the Appendix)

6.11 Case Study Concluding Remarks

Contemplating on the results of the pattern application process and the questionnaire results the following conclusions were achieved:

- The proposed pattern representation was, understood by all the participants.
- All participants involved in the case study completed the application of at least one pattern. Mistakes were observed in the phrasing and modeling of various assets of the models. In comparison less mistakes were made in modeling rather than phrasing.
- The fact that both groups were able to complete the tasks assigned, demonstrated that the process is useable as a starting point to elicit security requirements in a goal-oriented environment.
- The easiest part in the application process according to the majority of the participants was the pattern identification and asset alignment.
- The hardest step to be applied by the majority of the participants was security requirement introduction and extracted model re-integration.
- The pattern application process was according to the majority of the participants moderately easy to be applied.
- Having a background knowledge in IS security affects the process during the first applications.
- Having a background knowledge in IS speeds up moderately the process.
- Prior knowledge of an agent oriented language in combination ISSRM affects in moderation the overall results. Participant that had no prior knowledge were less confident about their results.
- RAST affects the overall process in a moderate level. We attribute the difficulties the participants faced during the security requirement introduction step to RAST.

6.12 Answers to the Case Study Questions

CSQ1: Overall the results were satisfactory. All the participants completed the application process. The process was overall followed semi-correctly with the main mistakes being made in the phrasing of the constructs.

CSQ2: The results of the case study demonstrated that the process is considerably more understandable to the participants of GROUP A comparatively to GROUP B. Overall the participants of GROUP A fully understood the process. GROUP B participants understood the process but had difficulties in the application of it. In some cases GROUP B participants would mechanically perform the steps without comprehending the purpose.

CSQ3: Overall the application process was found to be more usable by GROUP A than GROUP B. GROUP A participants found moderately usable the process whereas GROUP B participants found it slightly usable.

6.13 Summary

In this chapter, we outlined the process we followed in order to validate the contribution part of this master thesis. Initially we present the questions that guided the case study. We briefly summarized the introductory lecture as well as the task to be performed by the participants. Furthermore the model used in the case study was overviewed. Additionally we described the questionnaire to be filled by the participants. Moreover we provided with a brief description of the two groups of participants involved in our case study. The threats to validity were presented in addition to the results of the tasks performed and the answers to the questionnaire. Finally, we presented the questionnaire results, the validation process results and answer the questions posed by the case study.

7 Conclusion

In the beginning of this master thesis we presented our motivation, scope and research question. We followed with a brief overview of ISSRM that is the core security risk management framework of this thesis. Moreover we described various goal-oriented modeling languages as well as provided rationale for using RAST as main modeling language of this study. Furthermore we examined security patterns and introduced an approach for presenting an SRP in a goal oriented environment. We followed by presenting our illustrated SRP's in addition to introducing our pattern application process in order to apply a pattern to a given model. Additionally we presented with the process followed to validate the contributions of this thesis. In this concluding chapter we answer our research question with additional remarks. Finally we present our suggestions for future work.

7.1 Related Work

In (Naved, 2015) Naved presents Security Requirement Elicitation from Business Processes (SREBP) methodology that enables security requirements elicitation from Business Process Models using SRP's. Similar to the process of this master thesis the methodology proposed by SREBP identifies risks and addresses them using SRP's. The fundamental differences between the two works stand in methodology input, specialist cooperation and overall framework. The methodology introduced by Naved requires as an input the Value Chain and Business Process Model whereas our methodology requires a model from the late requirements design phase of RAST. The proposed process by SREBP requires the cooperation between security analysts whereas the methodology proposed in this master thesis requires a system analyst and optionally a security analyst. Moreover the two process differ in the overall perspective, SREBP focuses on process whereas this thesis focuses in the goals of a system.

7.2 Answer to Research Question & Conclusions

RQ: *How to integrate security risk-oriented patterns in the goal-oriented information system development?*

ANSWER: Integrating security risk-oriented patterns in the goal-oriented information system development is a threefold procedure. Initially one has to clearly define and describe a pattern. Following step is the identification of a pattern occurrence. Final step is introduction of the security mechanisms suggested by the pattern. In this work we presented with a pattern presentation structure as well as the application process. We describe a pattern by combining a security risk-oriented pattern template in addition to the modeling process of RAST. Additionally we present with an application process to be followed in order to apply the patterns into a goal oriented scenario. Our pattern application process covers the pre-processing of a given model. The method of identifying the occurrence of a pattern followed by the extraction of all relevant assets to a new model. Moreover describes the process of introducing the various security mechanisms suggested by the SRP's. Finally provides guidance for re-introducing the extracted assets back in the initial model. The contributed portion of this study was validated regarding its overall usability through the conduction of a case study. The results of the case study affirmed the usability of our pattern representation as well as the application process. Finally the results demonstrated that our proposed SRP's and pattern application process is usable as a starting point for more efficient identification of security requirements.

7.3 Limitations

Limitations of this work are:

- The scope of this master thesis excludes cost estimation for each security requirement and subsequent control. This limited the overall process into not including a mechanism that is utilised for evaluating costs. Subsequently this leads in no method existing in order to evaluate the costs-effectivity of controls.
- We illustrate only five patterns in this master thesis. Subsequently not all the types of risks that a system is faced with cannot be considered.
- All the SRP's are applied and modelled manually. This results in a number of possible errors occurring during the process. In particular the pattern occurrence identification is one of the steps involved that includes a number of sub steps. In order for all these steps to be executed critical thinking in addition to observational skills are required.
- Security Risk Aware Secure Tropos is a fairly new modelling procedure. This results in limited amounts of resources available. Subsequently related research is also limited and the amounts of models available in order to validate the process is small.

7.4 Future Work

We suggest that further work should mainly target the overall completion of the pattern application process using RAST. This would include the measurement of the effectivity of each suggested security requirement. In addition to the inclusion of a mechanism that would provide cost estimation metrics for each control. These two previously mentioned mechanisms in conjunction would provide with a basic trade off analysis between security and costs. Additionally the implementation of a software tool that would support the pattern application process would speed up considerably the overall process. Finally the representation of more patterns is crucial. Including more pattern would result in more risks and vulnerabilities to be identified. Subsequently this would enhance the resulting security of every system or scenario the process is applied.

8 References

- Ahmed, N., Deriving Security Requirements from Business Process Models, PhD thesis, University of Tartu, **2015**
- Ahmed, N. & Matulevičius, R., **2011** A Template of Security Risk Patterns for Business Process
- Ahmed, N.; Matulevičius, R.; Securing business processes using security risk-oriented patterns, *Computer Standards & Interfaces*, Volume 36, Issue 4, June **2014**, Pages 723-733, ISSN 0920-5489
- Altuhhova, O. **2013** An Extension of Business Process Model and Notation for Security Risk Management
- Bresciani, P.; Perini, A.; Giorgini, P.; Giunchiglia, F. & Mylopoulos, J. Tropos: An Agent-Oriented Software Development Methodology Autonomous Agents and Multi-Agent Systems, Kluwer Academic Publishers, **2004**, 8, 203-236
- Chowdhury, M.; Matulevičius, R.; Sindre, G. & Karpati, Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions Requirements Engineering: Foundation for Software Quality, Springer Berlin Heidelberg, **2012**, 7195, 132-139
- Dubois, E.; Heymans, P.; Mayer, N. & Matulevičius, R. A Systematic Approach to Define the Domain of Information System Security Risk Management Intentional Perspectives on Information Systems Engineering, Springer Berlin Heidelberg, **2010**, 289-306
- Matulevičius, R.; Mayer, N.; Mouratidis, H.; Dubois, E.; Heymans, P. & Genon, N. Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development *Advanced Information Systems Engineering, Springer Berlin Heidelberg*, **2008**, 5074, 541-555
- Matulevičius, R.; Mouratidis, H.; Mayer, N.; Dubois, E. & Heymans, P. Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management. *J. UCS*, **2012**, 18, 816-844
- Matulevičius, R., **2014** Model Comprehension and Stakeholder Appropriateness of Security Risk-Oriented Modelling Languages
- Mouratidis, H. & Giorgini, P. Secure Tropos: A Security-Oriented Extension of the Tropos Methodology *International Journal of Software Engineering and Knowledge Engineering*, **2007**, 17, 285-309
- Mayer, N. Model-based management of information system security risk University of Namur, **2009**
- Schumacher, M.; Fernandez-Buglioni, E.; Hybertson, D.; Buschmann, F. & Sommerlad, P. Security Patterns, Integrating Security and Systems Engineering, **2006**.
- Sindre, G. & Opdahl, A. Eliciting security requirements with misuse cases *Requirements Engineering, Springer-Verlag*, **2005**, 10, 34-44
- Sindre, G. Mal-Activity Diagrams for Capturing Attacks on Business Processes *Requirements Engineering: Foundation for Software Quality, Springer Berlin Heidelberg*, **2007**, 4542, 355-366
- Soomro, I. & Ahmed, N., Towards Security Risk-Oriented Misuse Cases Business Process Management Workshops, Springer Berlin Heidelberg, **2013**, 132, 689-700
- Yu, E. Towards Modelling Strategic Actor Relationships for Information Systems Development - With Examples from Business Process Reengineering. *Proceedings of 4th Workshop on Information Technologies and Systems, Vancouver, B.C., Canada, December 17-18, 1994*, pp. 21-28.

Appendix

I. Abstract Syntax of RAST

In this section we overview the abstract syntax of RAST (Matulevičius et al., 2012). The syntax includes two different meta-models the Security Enhanced Actor Model (SEAM) and Security Enhance Goal Model (SEGM).

The core of SEAM (see Figure 8.1) is an actor. An actor can be part of a dependency either as a depender ore a dependee. Security constraints represent security related constraints that are imposed to the hardgoals, resources or plans of an actor. A security constraint contains within one or more secure dependencies. The introduction of a secure dependency renders a security constraint(s) valid. Secure dependencies can be distinguished into three main core types: dependee secure dependency, deepener secure and a double secure dependency.

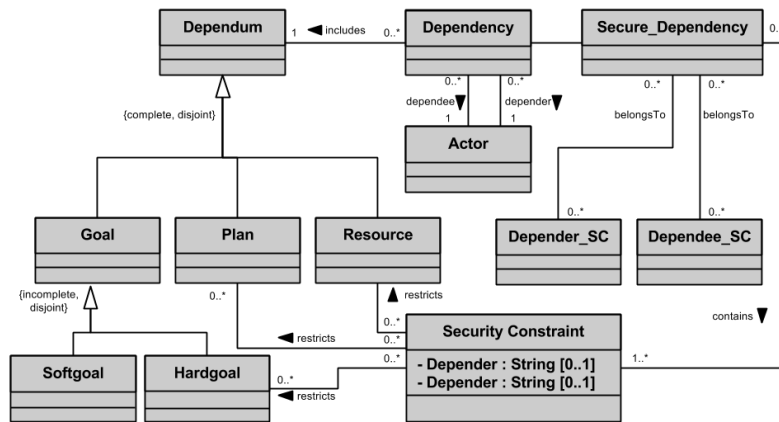


Fig 8.1 - SEAM Abstract Syntax; adapted from (Matulevičius et al., 2012)

Core of SEGM (see Figure 8.2) is an actor. An actor executes plans uses resources and goals. All the concepts that an actor makes use of can be decomposed further. Plans can be further decomposed into additional plans, resources or can be converted into hardgoals. The achievement of secure is performed through a means-ends relationship. In order to satisfy a softgoal a contribution should be imposed on other softgoals, resources plans or hardgoals.

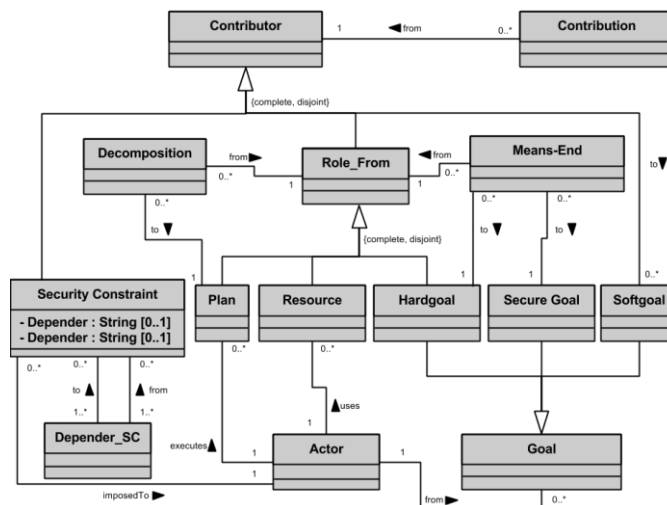


Fig 8.2 - SEGM Abstract Syntax; adapted from (Matulevičius et al., 2012)

Moreover a syntax for security constraint and threat is introduced Figure 8.3. A security constraint is imposed onto an actor and mainly functions by restricting the execution of plans, resource availability and hardgoals achieved by an actor. Secure goals introduce strategic security interest of an actor. The “satisfies” relationship is used to fulfil a security constraint by a secure goal. A secure plan constitutes of a plan that is devoted to the satisfaction of a secure goal. Secure resources represent security critical entities within the context of the system. Security constraint result in lowering the impact of threat towards plans, resources and hardgoals. Furthermore security constraints can be used to restrict plans resources and hardgoals.

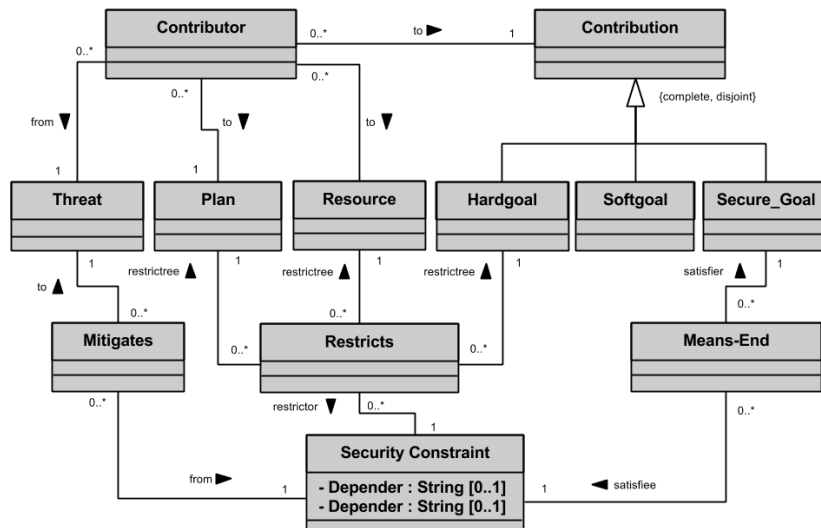


Fig 8.3 - Abstract Syntax of Security Constraint and Threat; adapted from (Matulevičius et al., 2012)

Security attack scenarios (see Figure 8.4) syntax is also addressed and introduced by RAST. It is used to distinguish between assets that are part of the system and malicious actors. This syntax introduces the attacker attribute to the actor. In this context the actor is represented as an attacker if the attribute is set to true. Subsequently an attacker executes a plan that either exploits a target or attacks a resource.

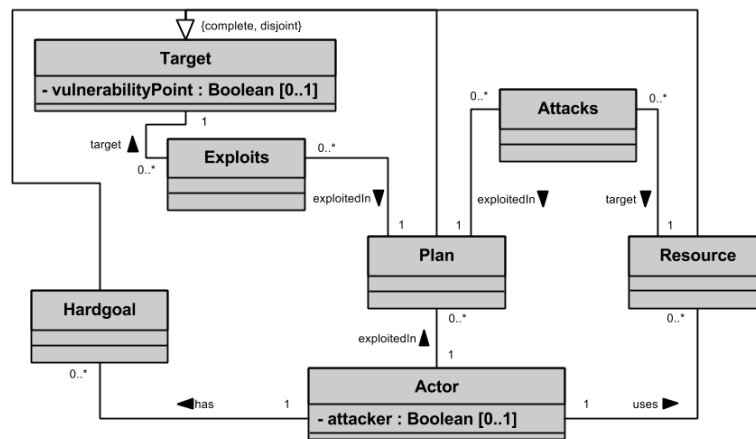


Fig 8.4 - Abstract Syntax of Security Attack Scenario; adapted from (Matulevičius et al., 2012)

II. SRP2 - Securing business activities from submitted data

SRP2 (Ahmed & Matulevičius 2014), enables validation of data submitted to a business activity, by predicting the need for a mechanism, that scans and detects malicious data before the data is forwarded to a business activity. This pattern counters an attacker that has information regarding the systems inner functionalities, and has the intention to harm the system. The malicious agent attacks by submitting through the input interface a malicious script that exploits the fact that incoming data are not filtered. The attack leads at the loss of confidentiality and the integrity of the business activity that is forwarded to. In Table 6 we utilise the *security risk oriented pattern template* in order to represent a detailed overview of the pattern and move forward with the representation of the pattern using RAST.

Table 6 - SRP2 Asset Identification and Mitigation

Security scenario & security context identification	
Pattern Name	Securing business activities from submitted data
Pattern Decision	This pattern validates data entry into a business IS by detecting malicious data.
Asset-related Concepts	
Business Asset	The respective business activity to which data is submitted.
IS Asset	The input interface.
Security Criterion	Confidentiality of the business activity. Integrity of the business activity.
Risk-related Concepts	
Risk	An attacker with the knowledge of the systems inner functionalities and intending to harm the business activity, submits through the input interface a malicious script exploiting the fact that incoming data are not filtered. Leading to the loss of the confidentiality and the integrity of the business activity where the data is submitted.
Impact	<ul style="list-style-type: none"> • Loss of the confidentiality of the business activity. • Loss of the integrity of the business activity. • Perpetual damage the malicious script can cause.
Event	An attacker intending to harm the business activity, submits through the input interface a malicious script exploiting that there is no screening process for the data.
Threat	An attacker with the knowledge of the systems inner functionalities and wanting harm the business activity submits through impute interface a malicious script.
Vulnerability	The incoming data to the business activity is not filtered.
Threat Agent	An attacker intending to harm/corrupt a business activity.
Attack Method	An attacker submits through impute interface a malicious script
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Check data for malicious content before submitting it to a business activity.
Control	Input data scanning mechanism - scans inputted data and blocks or isolates data flagged as harmful.

In Figure 8.5 we identify as the business asset the respective business activity where the data is submitted, that is represented by the goal **Data submitted to respective business activity** that is achieved by the plan of **Submit the data to respective business activity**. As IS asset we identify the Input interface that is represented by an actor diagram that includes the respective assets. Moreover, we identify as security criterion the confidentiality and integrity of the data, which is represented by a softgoal that has a positive contribution by the security constraint of **Maintain the confidentiality & integrity of the**

business activity. This constraint restricts the previously mentioned plan that assists in the achievement of the goal of the Input interface actor. In Figure 8.6 we introduce a secure goal of Confidentiality and integrity of the business activity ensured that satisfies the main security constraint of the actor. This secure goal is achieved by completing the secure plan of (S) Ensure data confidentiality and integrity of the business activity.

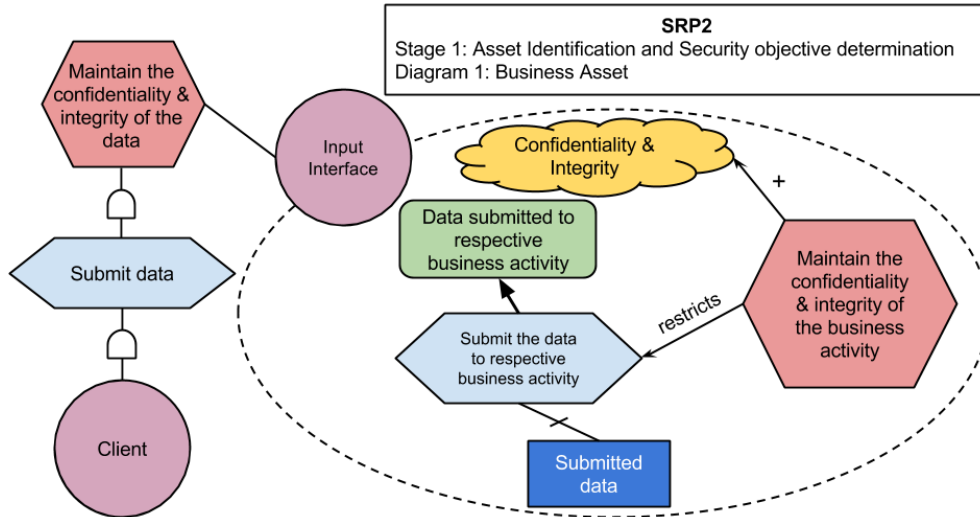


Fig 8.5 - SRP2 Modelling of Business Assets

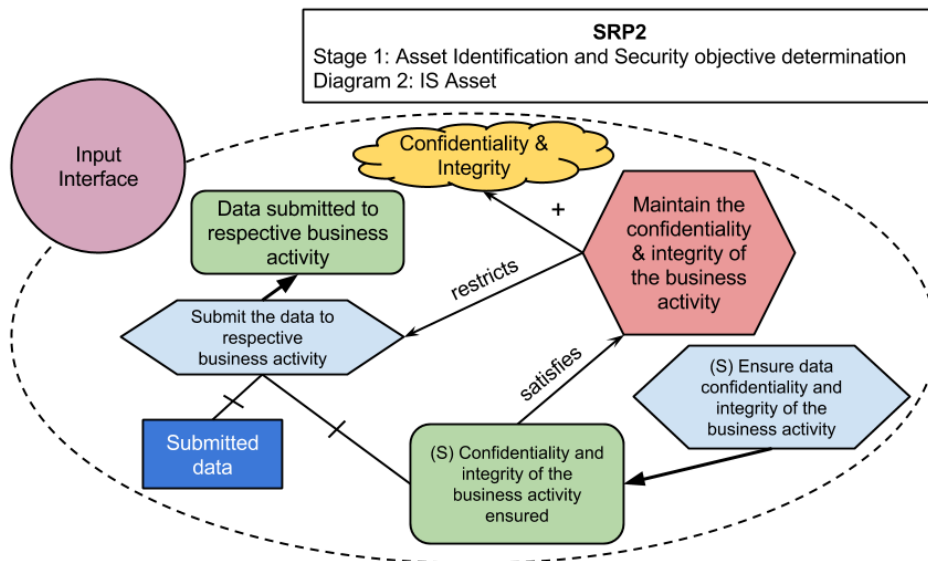


Fig 8.6 - SRP2 Modelling of IS Assets

In the event of an attack in Figure 8.7 we identify as a threat **Submit malicious script** that has an impact on the security criterion of **Confidentiality & integrity** resulting in harm. In Figure 8.8 we represent the potential attack scenario of an **Attacker** actor that having as main malicious goal **Business Activity Harmed** executes the malicious plan of **Submit malicious script** that attacks the plan **Submit the data to respective business activity** of the input interface actor. The malicious plan of the attacker exploits the non-fulfilment of the **Ensure data confidentiality and integrity** secure plan.

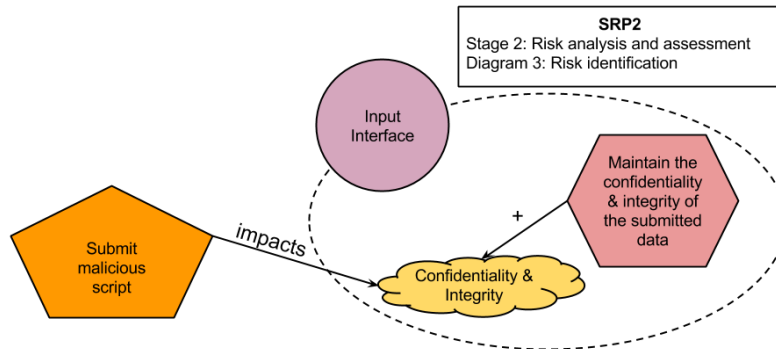


Fig 8.7 - SRP2 Attack Identification

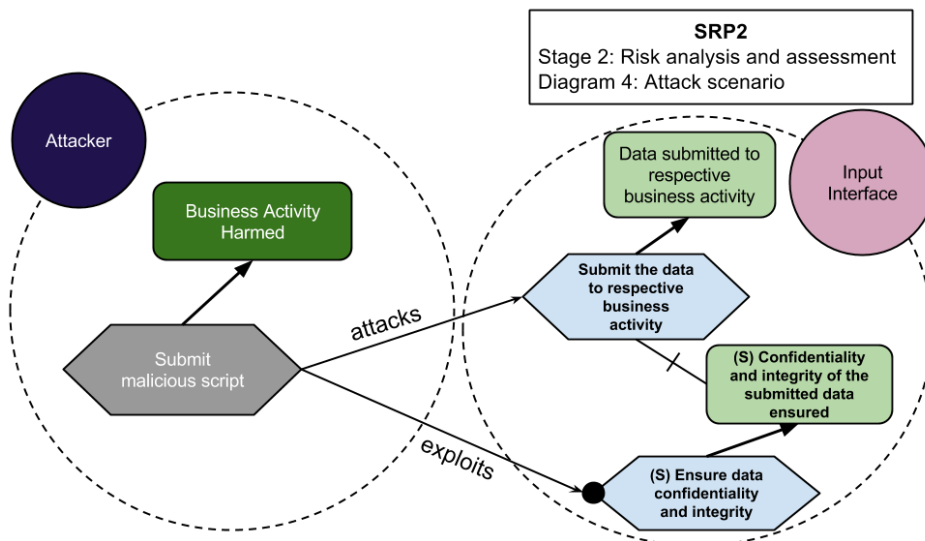


Fig 8.8 - SRP2 Potential Attack Scenario

In order to counter the identified risks SRP2 in Figure 8.9 introduces a filtering mechanism that scans the data to be submitted to a business activity and rejects or isolates any malicious data. Here we replace the secure plan of Ensure data confidentiality and integrity with Filter Incoming Data that is represented with a dotted pattern indicating that is along with the secure goal and constraint a security requirement.

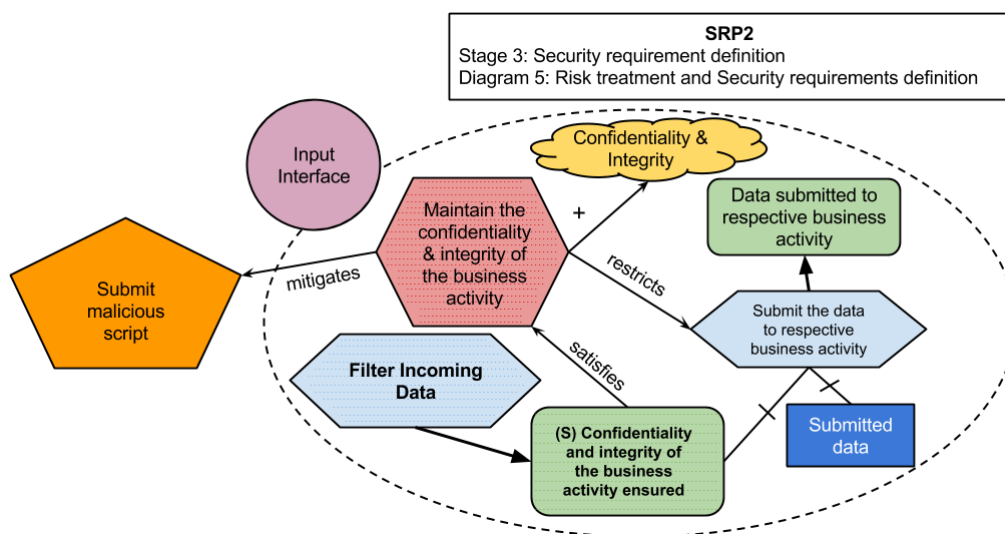


Fig 8.9 - SRP2 Risk Treatment and Security Requirements Definition

III. SRP3 - Securing business activities from DoS attacks

SRP3 (Ahmed & Matulevičius 2014), ensures the availability of a service in the event of a Denial of Service Attack (Dos). This pattern counters the actions of an attack, where due to an unlimited amount of request being forwarded to the server, a business service is rendered unresponsive. The attackers send an exponentially growing number of simultaneous requests to the system, resulting in the system crashing due to its ability to only serve a certain number of simultaneous clients. The attack leads to the loss of the availability of the service to the respective clients of the system and server functionality to be damaged. In Table 7 we utilise the *security risk oriented pattern template* in order to represent a detailed overview of the pattern and move forward with the representation of the pattern using RAST.

Table 7 - SRP3 Asset Identification and Mitigation

Security scenario & security context identification	
Pattern Name	Securing business activities from DoS attacks
Pattern Decision	This pattern ensures the availability of a service faced with a Denial of Service Attack.
Asset-related Concepts	
Business Asset	The provided business service.
IS Asset	Server
Security Criterion	Availability of the business service.
Risk-related Concepts	
Risk	An attacker with the knowledge of the systems inner functionalities and due to unlimited request being allowed by the system, sends multiple requests to the system simultaneously causing the system to not be non-responsive. Leading to the loss of the availability of the service and server functionality to be damaged.
Impact	<ul style="list-style-type: none"> • Loss of the availability of the service. • Damaged server functionality. • Perpetual business reputation damage.
Event	An attacker able to perform a DoS attack and due to unlimited request being allowed by the system, sends multiple requests to the system simultaneously causing the system to not be responsive.
Threat	An attacker with the knowledge of the systems inner functionalities sends multiple requests to the system simultaneously causing the system to not be responsive.
Vulnerability	Unlimited number of requests is allowed to be performed
Threat Agent	An attacker with the knowledge of the systems inner functionalities
Attack Method	An attacker sends multiple requests to the system simultaneously causing the system to not be responsive.
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Check incoming requests. Perform a classification of the incoming requests. Discard data classified as harmful.
Control	Abnormal incoming request classifier.

In Figure 8.10 we identify as the business asset the provided service, which is represented by the goal **Service provided** that is achieved by the plan of **Provide Service**, which relies on the plan of **Listen for requests**. As IS asset we identify the *Server* that is represented by an actor diagram. Moreover, we identify as security criterion the **Availability**

of the provided business service, which is represented by a softgoal that has a positive contribution by the security constraint of Maintain the availability of the provided service. This constraint restricts the previously mentioned goal of the *Server* actor. In Figure 8.11 we introduce a secure goal of Availability of the provided service ensured that satisfies the main security constraint of the actor. This secure goal is achieved by completing the secure plan of Ensure provided service availability.

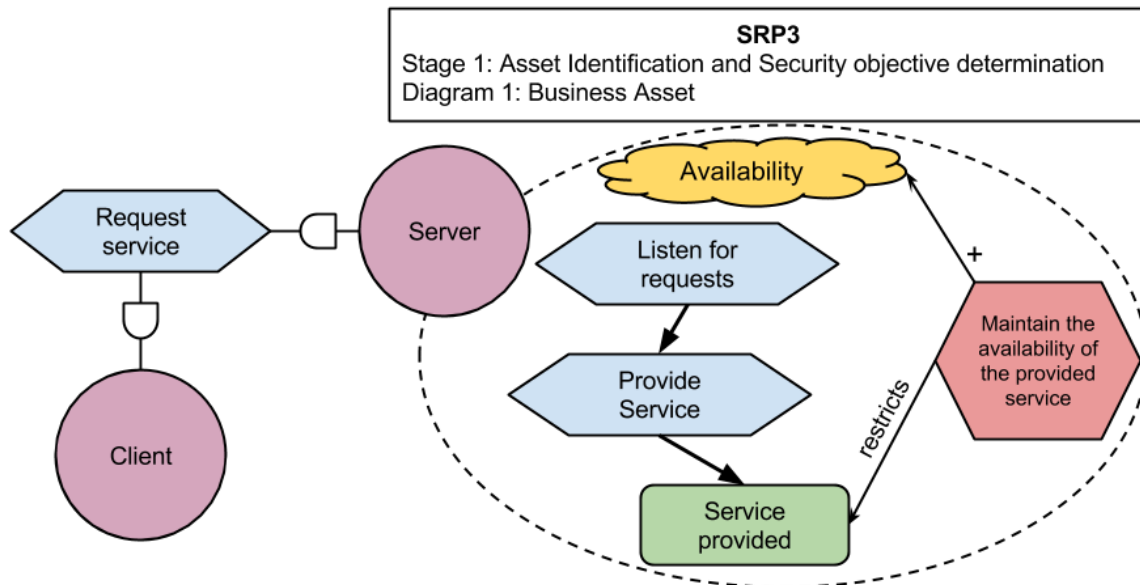


Fig 8.10 - SRP3 Modelling of Business Assets

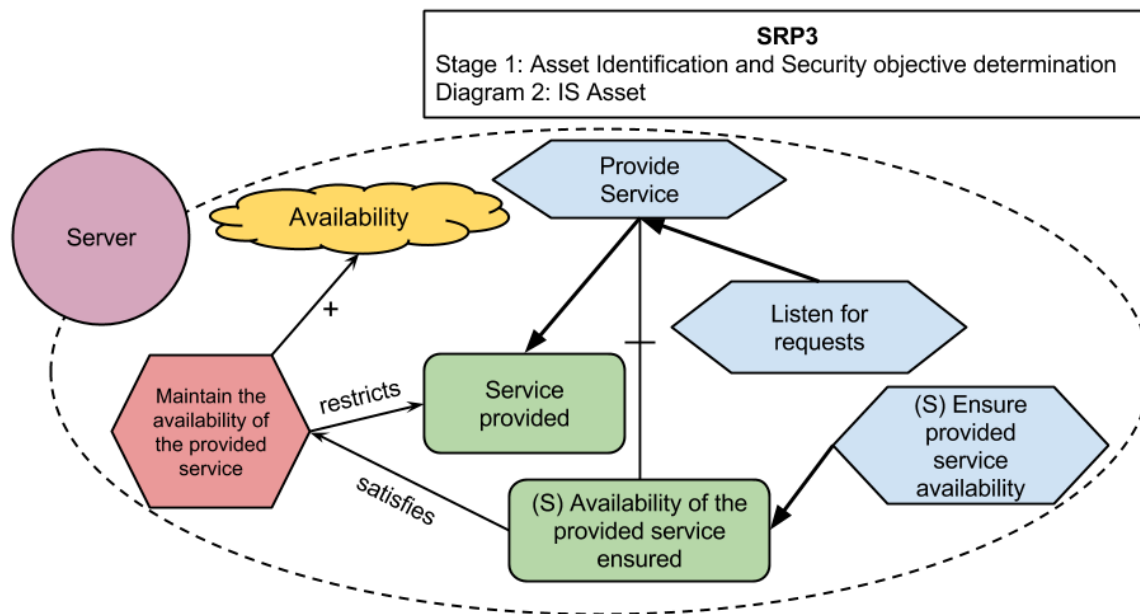


Fig 8.11 - SRP3 Modelling of IS Assets

In case of an attack in Figure 8.12 we identify as a threat **DOS attack** that has an impact on the security criterion of **Availability**, resulting in harm. In Figure 8.13 we represent the potential attack scenario of an Attacker actor that having as main malicious

goal Service rendered unavailable executes the malicious plan of Flood the service with requests that attacks the plan Listen for requests of the *Server* actor. The malicious plan of the attacker exploits the non-fulfilment of the Ensure provided service availability secure plan.

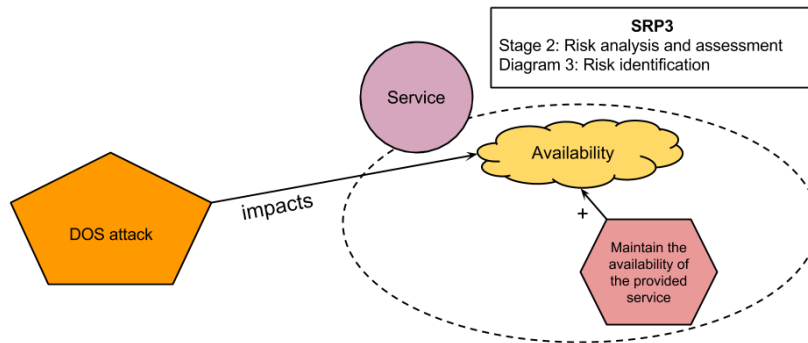


Fig 8.12 - SRP3 Attack Identification

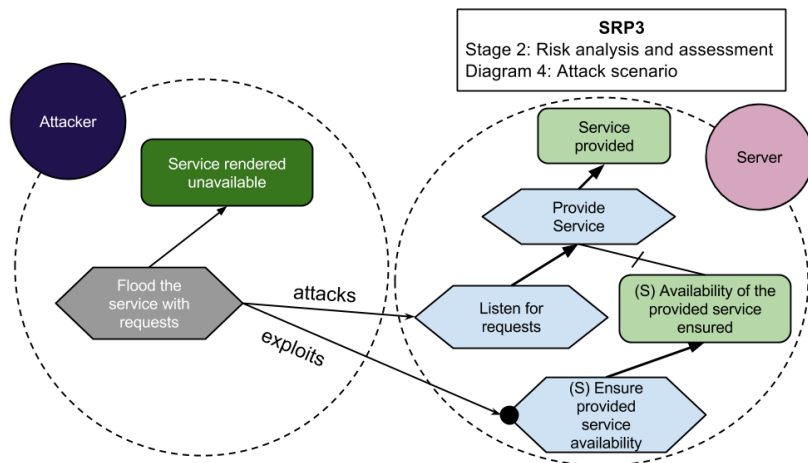


Fig 8.13 - SRP3 Potential Attack Scenario

Addressing the identified risks SRP2 in Figure 8.14 introduces checker for abnormal requests that discards them in the event of an anomaly. Here we replace the secure plan of Ensure provided service availability with Check for abnormal requests that is represented with a dotted pattern indicating that is along with the secure goal and security constraint a security requirement.

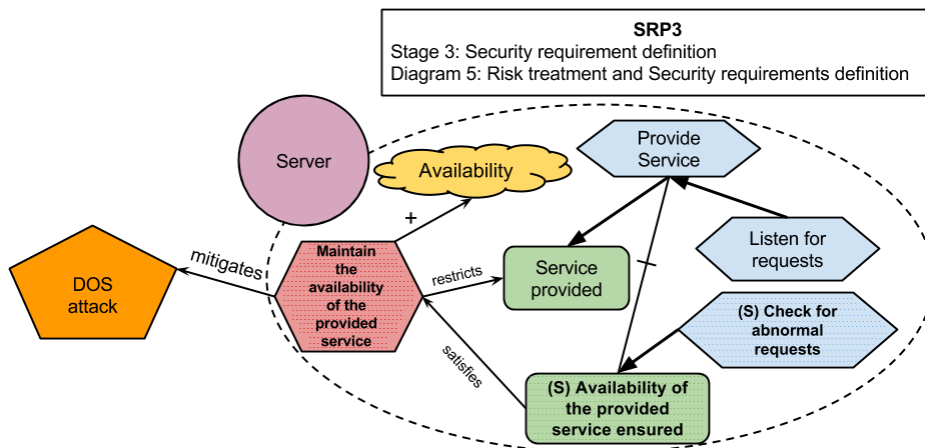


Fig 8.14 - SRP3 Risk Treatment and Security Requirements Definition

IV. SRP4 - Securing business data from unauthorized access

SRP4 (Ahmed & Matulevičius 2014), is focused the process of securing confidential information, from being accessed by unauthorised devices or people. The scenario that this pattern counters is of an attacker that gains access to sensitive business data through a commonly used retrieval interface. Due to the interface not incorporating an access control mechanism the malicious agent is able to retrieve the data. The attack leads in the compromise of the confidentiality of the business data that is compromised. In Table 8 we utilise the *security risk oriented pattern template* in order to represent a detailed overview of the pattern and move forward with the representation of the pattern using RAST.

Table 8 - SRP4 Asset Identification and Mitigation

Security scenario & security context identification	
Pattern Name	Securing business data from unauthorized access.
Pattern Decision	This pattern describes the process of securing confidential information, from being accessed by unauthorized devices or people.
Asset-related Concepts	
Business Asset	Requested data
IS Asset	Retrieval interface
Security Criterion	Confidentiality of the data.
Risk-related Concepts	
Risk	An attacker accesses data through the retrieval interface and due to the interface not having an access control mechanism he is able to retrieve data. The confidentiality of the data is compromised due to the privileges a client has, to access the retrieval interface - which displays the data without requiring for authorization.
Impact	<ul style="list-style-type: none"> • Loss of the confidentiality of the data. • Retrieval interface becomes prone to future attacks. • Further distribution of the data that harms the business.
Event	An attacker accesses data through the retrieval interface and due to the interface not having an access control mechanism is able to retrieve confidential business data.
Threat	An attacker accesses data through the retrieval interface and is able to retrieve confidential business data.
Vulnerability	Access control mechanism that grants access given a security clearance is not employed.
Threat Agent	An attacker unauthorized to access the retrieval interface.
Attack Method	The attacker accesses the retrieval interface.
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Check user access rights. Provide access only if the access rights of the user, match the access rights of the file.
Control	User access rights checker.

In Figure 8.15 we identify as the business asset the **Data** that is retrieved, and represented as a resource that is decomposed from the plan **Retrieve data**, which satisfies the main goal of the IS asset of the model the *Retrieval interface* actor, main goal of this actor being **Data retrieved**. Furthermore in this instance we identify as security criterion the **Confidentiality** of the retrieved business data, which is represented by a softgoal that has a positive contribution by the security constraint of **Maintain data confidentiality**. This constraint restricts the previously mentioned goal that assists in the achievement of the goal of the *Retrieval interface* actor. In Figure 8.16 we introduce a secure goal of **Confidentiality**

of data ensured that satisfies the main security constraint of the actor. This secure goal is achieved by completing the secure plan of Ensure the confidentiality of the data.

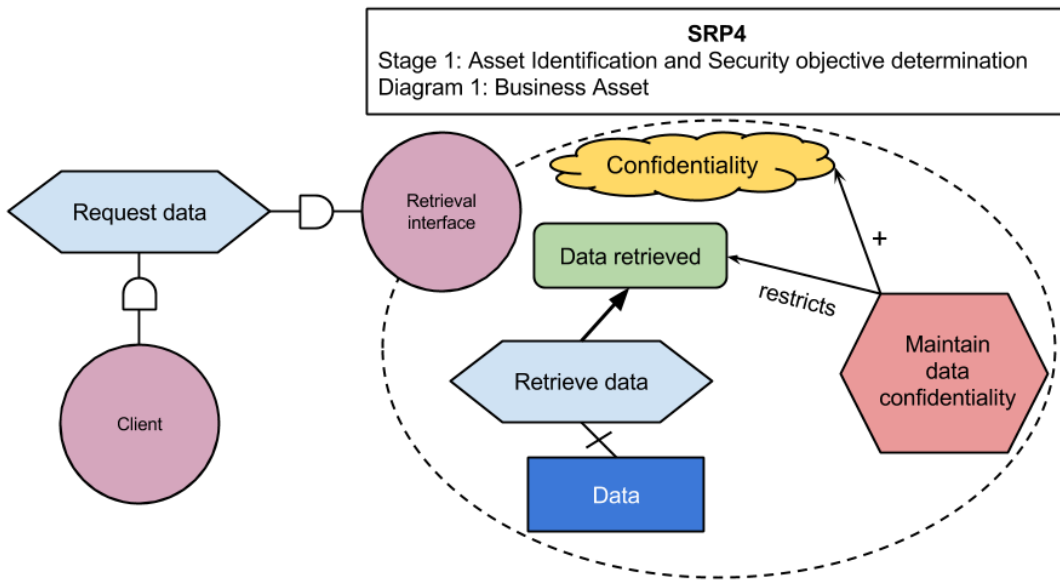


Fig 8.15 - SRP4 Modelling of Business Assets

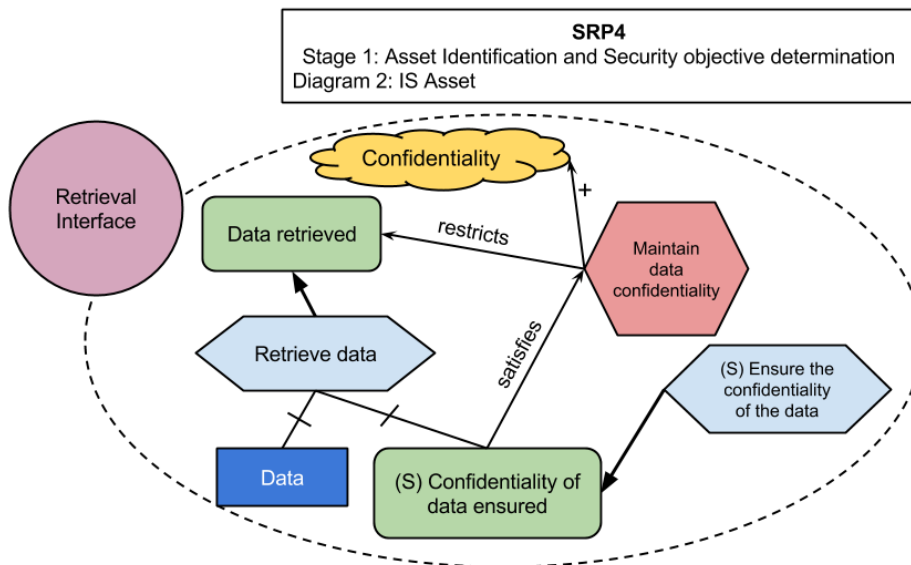


Fig 8.16 - SRP4 Modelling of IS Assets

In case of an attack in Figure 8.17 we identify as a threat Unauthorised access that has an impact on the security criterion of Confidentiality resulting in harm. In Figure 8.18 we represent the potential attack scenario of an Attacker actor that having as main malicious goal Data Obtained that executes the malicious plan of Access the data that attacks the plan Retrieve data of the Retrieval Interface actor. The malicious plan of the attacker exploits the non-fulfilment of the Ensure the confidentiality of the data secure plan.

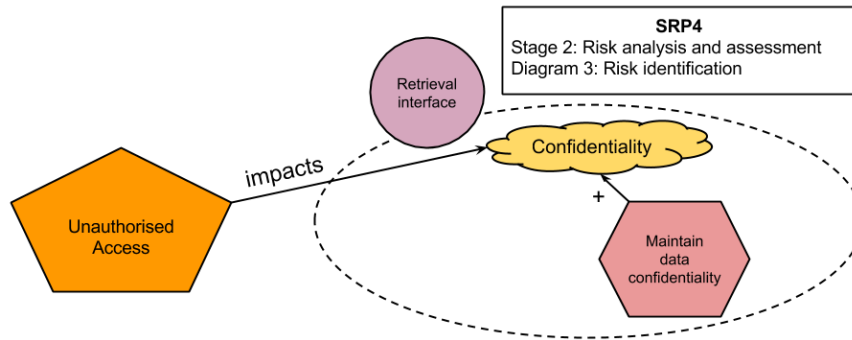


Fig 8.17 - SRP4 Attack Identification

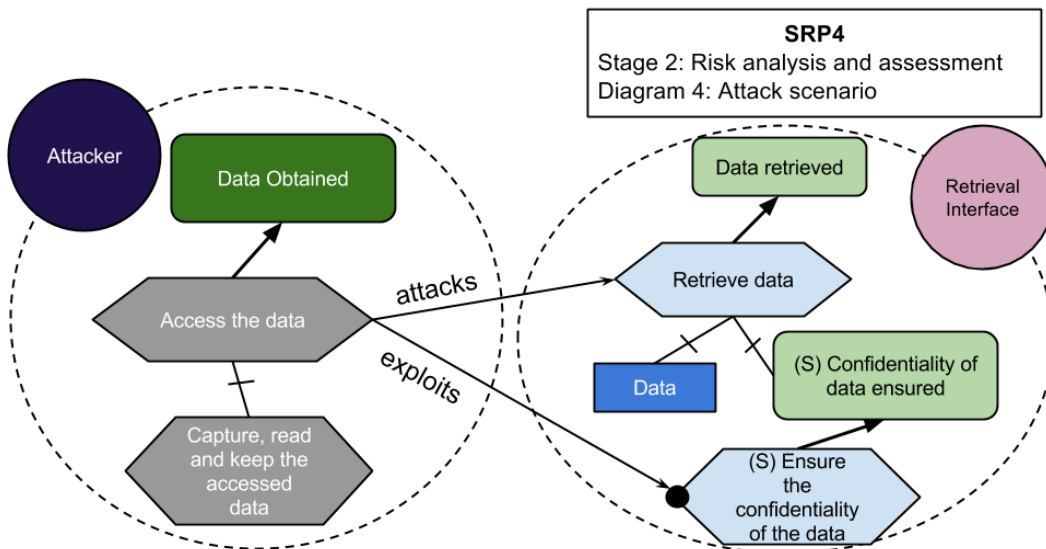


Fig 8.18 - SRP4 Potential Attack Scenario

Countering the risks identified SRP4 in Figure 8.19 introduces an access check mechanism that requires the clearance level of each client to be checked before data is retrieved. Here we replace the secure plan of Ensure confidentiality of the data with Check access rights that is represented with a dotted pattern indicating that is along with the secure goal and constraint are security requirement.

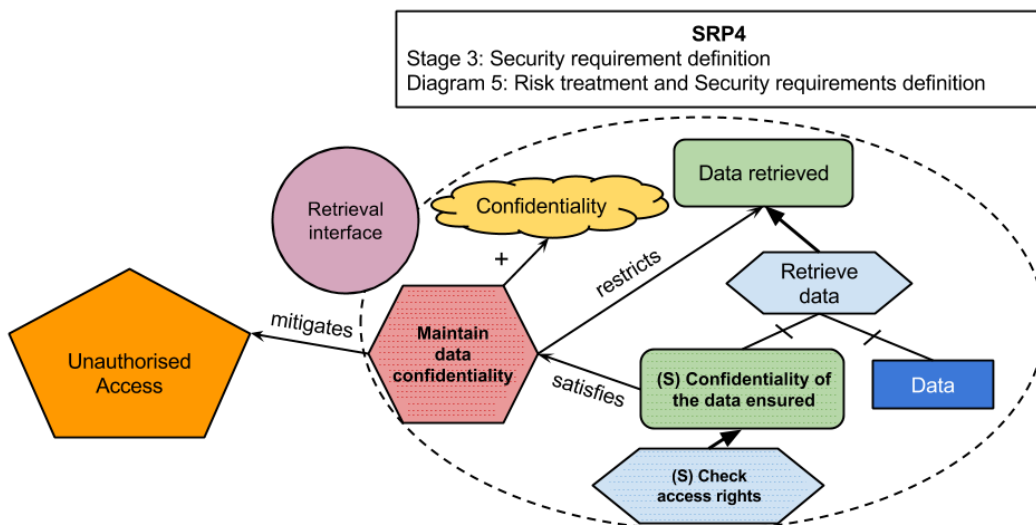


Fig 8.19 - SRP4 Risk Treatment and Security Requirements Definition

V. SRP5 - Securing business data stored/retrieved from a data store

SRP5 (Ahmed & Matulevičius 2014), has as main goal to secure data, that is stored into a business data store, against internal attacks that aim to obstruct the data, exploiting that the data is stored in plain text. In the described scenario an internal attacker or malware, attempting to access a business data store where sensitive data is stored. The attack occurs due to the data being stored in a plain format, and leads to the loss of the confidentiality of the stored data and the perpetual damage of the files residing in the same instance as malicious script. In Table 9 we utilise the *security risk oriented pattern template* in order to represent a detailed overview of the pattern and move forward with the representation of the pattern using RAST.

Table 9 - SRP5 Asset Identification and Mitigation

Security scenario & security context identification	
Pattern Name	Securing business data stored/retrieved from a data store.
Pattern Decision	This pattern ensures that the data stored in the businesses' data store is secure against internal attacks.
Asset-related Concepts	
Business Asset	Stored data
IS Asset	Data store
Security Criterion	Confidentiality of the stored data
Risk-related Concepts	
Risk	An attacker or malware with the intention to compromise the stored data directly accesses the data store in the data store enabled by the fact that the data is stored in a plain format leading in the loss of the confidentiality of the stored data, and additional perpetual damage to the files residing in the same instance as the malicious script.
Impact	<ul style="list-style-type: none"> • Loss of the confidentiality of the stored data • Perpetual damage to the files residing in the same instance as malicious script.
Event	An attacker or malware intending to obstruct the stored data directly accesses the businesses' data store, enabled by the data being stored in a plain text format.
Threat	An attacker or malware with the intention to compromise the stored data directly accesses the data in the data store.
Vulnerability	Data is stored in a plain format
Threat Agent	An attacker or malware with the intention to compromise the stored data in the data store.
Attack Method	An attacker or malware directly accesses the data store in the data store
Risk Treatment-related Concepts	
Risk Treatment	Risk reduction
Security Requirement	Make unreadable the data before storing them to the data-store. Make the data readable when it is retrieved from the data-store.
Control	Cryptographic algorithm - the data is encrypted after it is submitted in the data store from the input interface and decrypted when it needs to be presented to the client.

In Figure 8.20 we identify as the business asset the **Data** that is stored, and represented as a resource that is decomposed from the main **IS** asset of this scenario that is the **Data store** resource, which is decomposed from the plan **Store / retrieve the data** into the **data store** that is the means to the achievement of the main goal of **Data stored / retrieved** of the actor. In this instance we identify as security criterion the **Confidentiality** of the business data, which is represented by a softgoal that has a positive contribution by the security constraint of **Maintain the stored data confidential**. This constraint restricts

the previously mentioned goal that assists in the achievement of the goal of the *Storing / Retrieval Interface* actor. In Figure 8.20 we introduce a secure goal of Confidentiality of the stored data ensured that satisfies the main security constraint of the actor. This secure goal is achieved by completing the secure plan of Ensure data confidentiality.

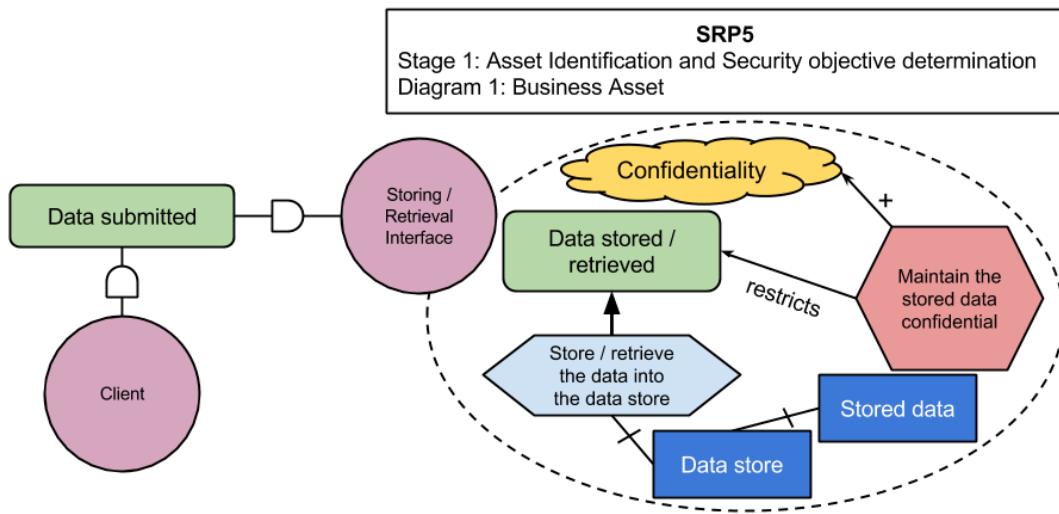


Fig 8.20 - SRP5 Modelling of Business Assets

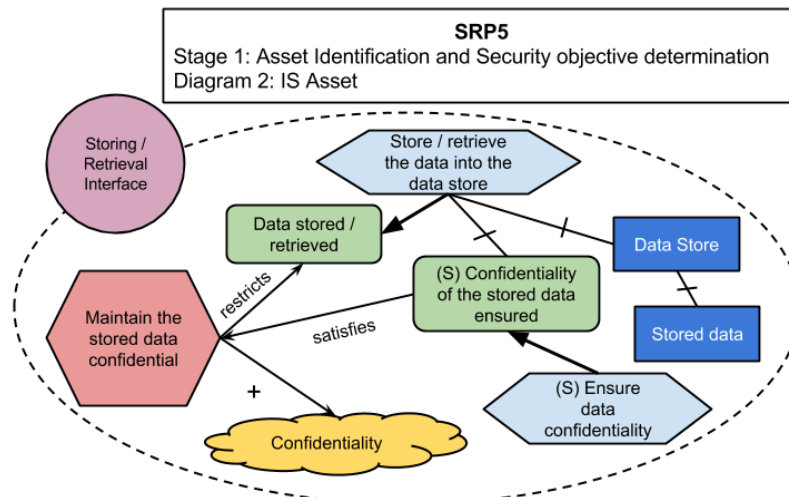


Fig 8.21 - SRP5 Modelling of IS Assets

In event of a security attack in Figure 8.22 we identify as a threat Access the un-encrypted data that has an impact on the security criterion of Confidentiality resulting in harm. In Figure 8.23 we represent the potential attack scenario of an Attacker actor that having as main malicious goal Stored data obtained executes the malicious plan of Access plain-text data in the data store that attacks the plan Access plain-text data in the data store of the *Data Store* actor. The malicious plan of the attacker exploits the non-fulfilment of the Ensure data confidentiality secure plan.

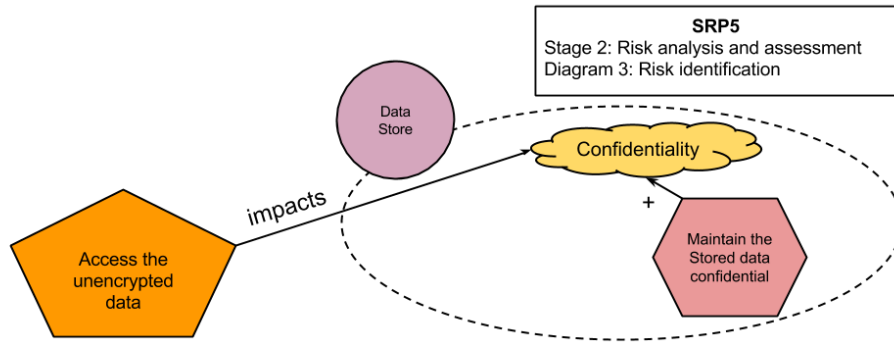


Fig 8.22 - SRP5 Attack Identification

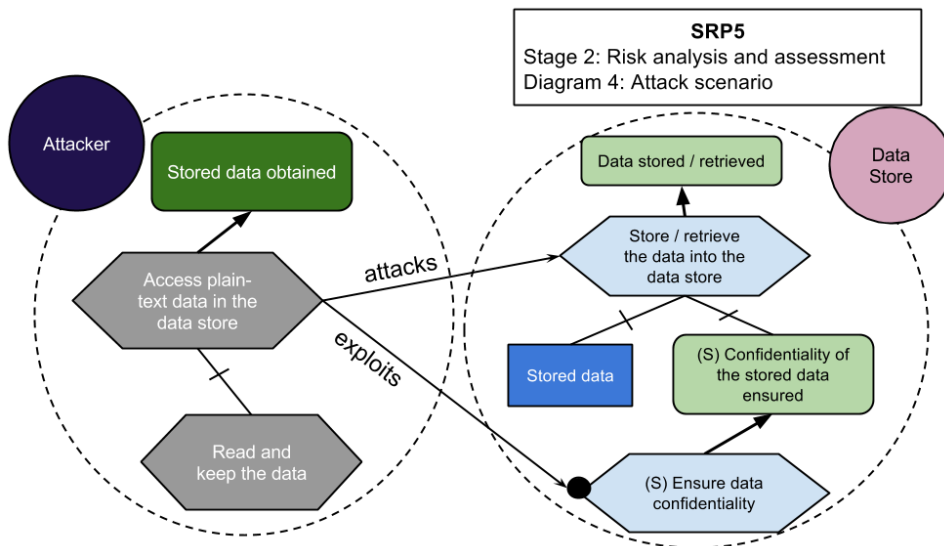


Fig 8.23 - SRP5 Potential Attack Scenario

In order to address the identified risks SRP5 in Figure 8.24 introduces a cryptographic procedure that encrypts the data before storing it and decrypts it before delivering it back to the requester. Here we replace the secure plan of Ensure data confidentiality with Perform cryptographic procedures decomposed into Encrypt data and Decrypt data represented with a dotted pattern indicating that is along with the secure goal and constraint are security requirement.

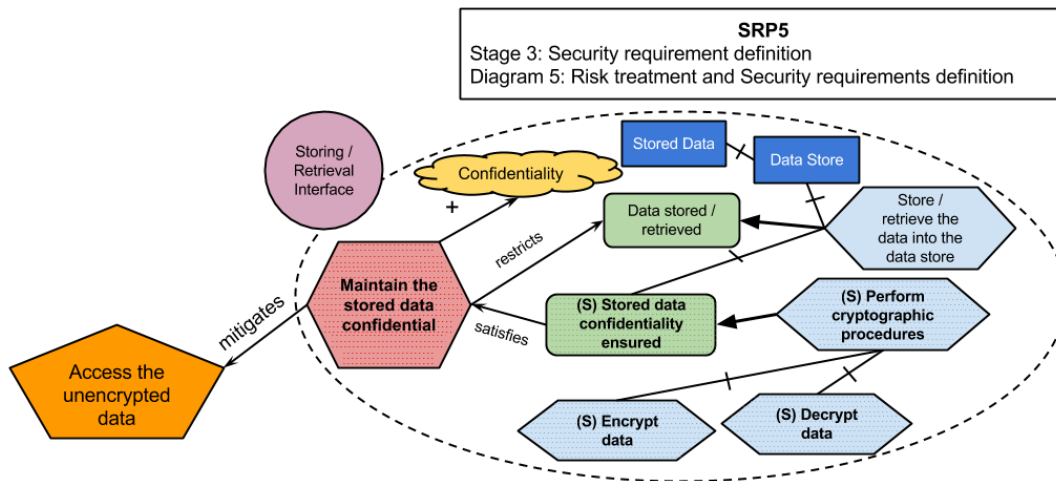


Fig 8.24 - SRP5 Risk Treatment and Security Requirements Definition

VI. Case Study Participant Reports

In this section we include reports for each of the participants of the Case Study of Chapter 6. In the reports certain pattern application diagrams are not included. The diagrams of asset extraction and model introduction are not included because they do not add value to the reports. Moreover we mark with a circle in each diagram mistakes made by the participants. As mistakes we consider all the solution that do not conform to the correct pattern applications of section VI of the Appendix.

PARTICIPANT A

Background

Participant A is at the time of the case study being conducted a Software Engineering master degree student. The participant has knowledge of the ISSRM domain model, process and security requirement elicitation. The participant attended the entire introductory lecture of the case study and completed the application of two patterns in the given model. The patterns to be applied by participant A are SRP2, SRP4.

Pattern Application

SRP2

The timeframe required by the participant in order to apply the SRP2 was roughly around one and a half hour. Participant A correctly identified that the pattern is applicable in the user interface actor of the case study model presented in Chapter 6. SRP2 identifies and mitigates the threat of malicious data being propagated between business services. The participant isolated correctly the assets involved in the pattern (see Figure 8.25) and applied security constraints and criteria that restrict the main goal. Moreover he followed the guidelines and applied correctly the secure goals. Furthermore he correctly introduced secure plans that assist in the achievement of the goals (see Figure 8.26). The participant made the minor phrasing mistake of adding “Data” to all the phrases that include “User Info”. The addition is unnecessary and it might introduce confusion in later steps.

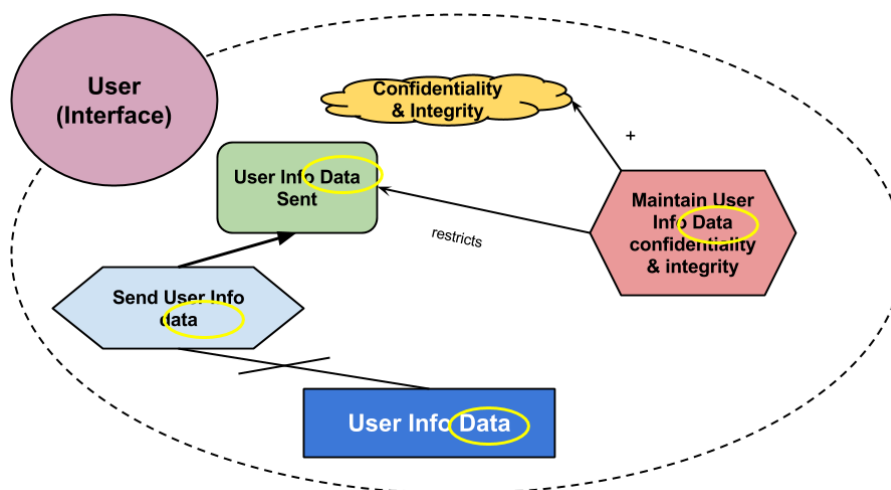


Fig 8.25 - PA SRP2 applied STEP 2 (a)

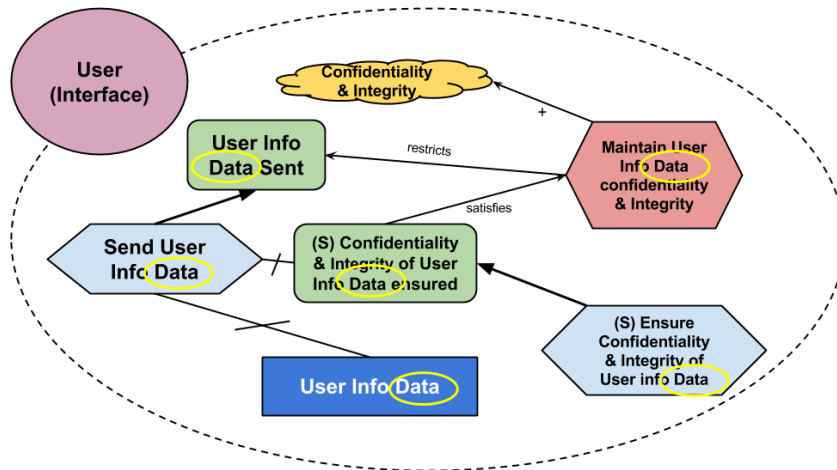


Fig 8.26 - PA SRP2 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans the participant correctly replaced the secure plan Ensure Confidentiality & Integrity of the User Info Data with the requirement suggested by the pattern (see Figure 8.27).

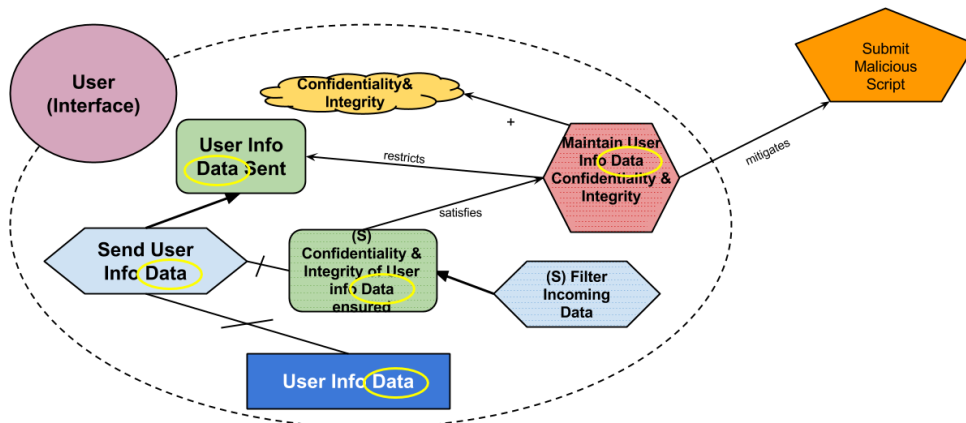


Fig 8.27 - PA SRP2 applied STEP 3

The application of the fourth step was as well performed correctly, demonstrating the events of an attack. The participant used correctly the model in order to justify the security requirements introduced in the previous third step (see Figure 8.28).

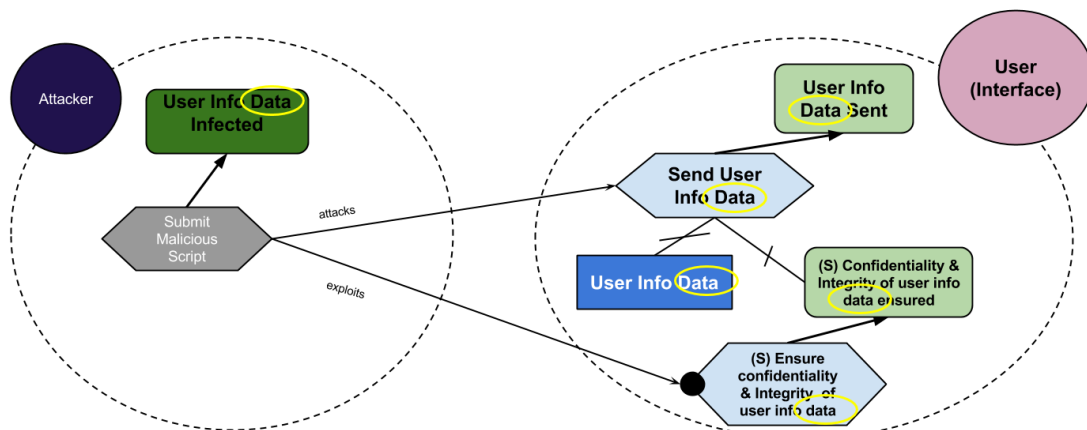


Fig 8.28 - PA SRP2 applied STEP 4

SRP4

In the application of this pattern the participant took the liberty of not applying it to an existing part of the model. Although the participant could apply the pattern to an existing part, he decided that the user interface provided the functionality of retrieving data and thus making SRP4 applicable (see Figure 8.29). The participant repeated the same phrasing minor mistake he made in the application of SRP2.

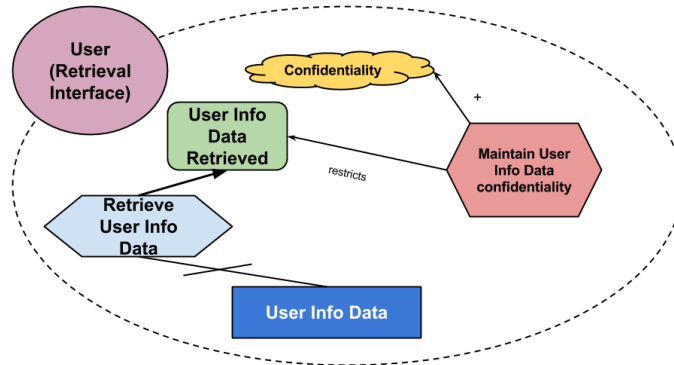


Fig 8.29 - PA SRP4 applied STEP 2 (a)

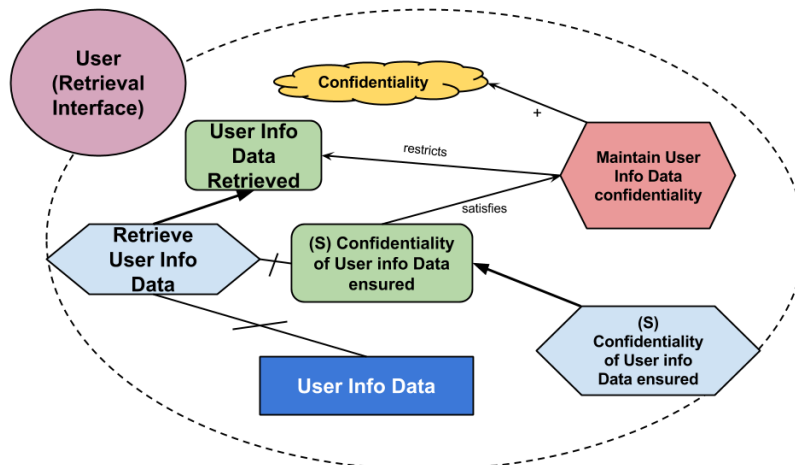


Fig 8.30 - PA SRP4 applied STEP 2 (b)

Following the participant's assumption, the rest of the process was correctly continued by introducing the suggested secure constructs (see Figure 8.30). Moreover the introduction of the new secure requirements was performed accurately (see Figure 8.31).

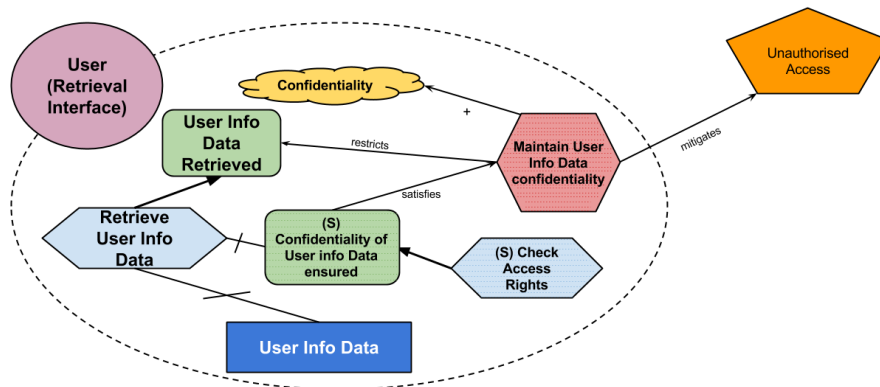


Fig 8.31 - PA SRP4 applied STEP 3

Lastly the validation and rationale step was performed correctly (see Figure 8.32). The participant correctly justified the assets to be attacked and exploited. Important to note that the participant followed all the phrasing conventions for goals and plans.

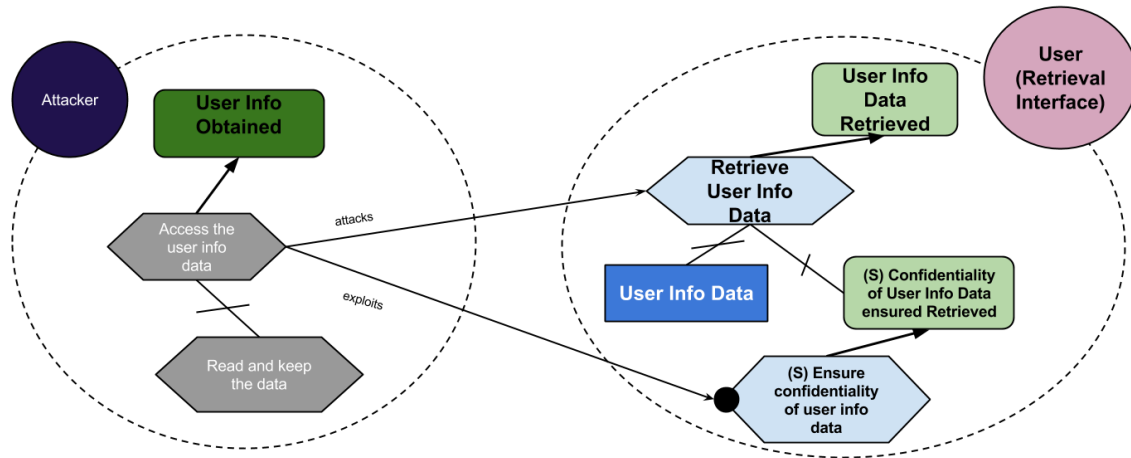


Fig 8.32 - PA SRP4 applied STEP 4

Observations

After the introductory lecture the participant had a few questions regarding phrasing and modeling of connections. Overall the process was completed accurately and the participant was able to use two patterns described by our suggested pattern representation. Furthermore we assess that the previous knowledge of the ISSRM principles had a positive contribution to the participants overall performance.

Remarks

The participant gave an overall positive feedback to all the questions of the questionnaire. Main question where related to the application process. Negative feedback was directed towards the limited time amount. On this behalf, the conclusion arises that more time is needed for grasping the process. Lastly, the participant had positive impressions regarding the pattern representation and application process.

PARTICIPANT B

Background

Participant B (PB) is a Software Engineering master degree graduate student at the time of the study being conducted. The participant is employed in the field of enterprise security. The participant is moderately familiar with the ISSRM domain model, process and security requirement elicitation. The participant attended the entire introductory lecture of the case study and completed the application of one pattern in the given model. The pattern applied by participant PB was SRP5.

Pattern Application

SRP5

PB required roughly 45 minutes in order to apply the SRP5. PB correctly identified that the pattern is applicable in the internet store actor of the case study model presented in Chapter 6. SRP5 identifies and mitigates the threat of business data stored in a data store being

obstructed. The attack occurs by exploiting the fact that the data is stored in plaintext. The participant isolated correctly the assets involved in the pattern (see Figure 8.33) and applied security constraints and criteria that restrict the main goal. Moreover he followed the guidelines and applied correctly the secure goals and the plans to be executed in order for them to be achieved (see Figure 8.34). The recurring mistake made by the participant is the decomposition of the resources. The participant decomposes the resource from the database resource incorrectly.

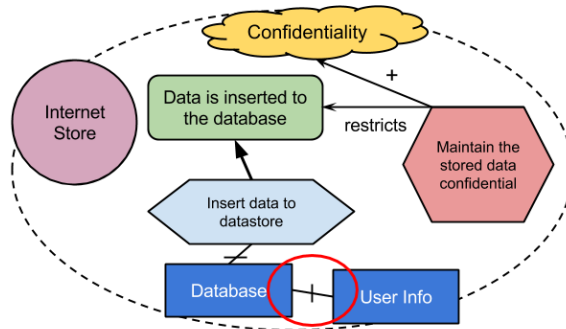


Fig 8.33 - PB SRP5 applied STEP 2 (a)

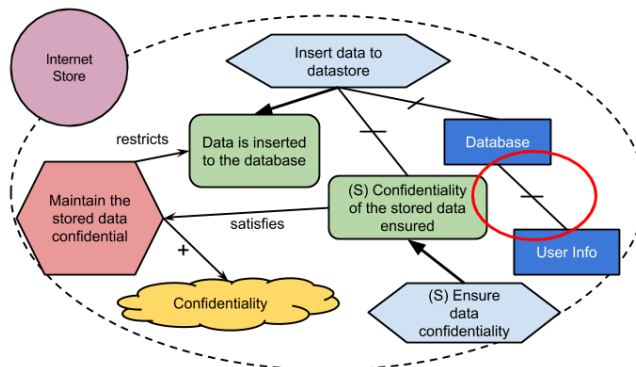


Fig 8.34 - PB SRP5 applied STEP 2 (b)

After the application of the security constraints, criteria, goals and plans PB succeeded and correctly replaced the secure plan of Stored data confidentiality ensured with the requirement suggested by the pattern (see Figure 8.35).

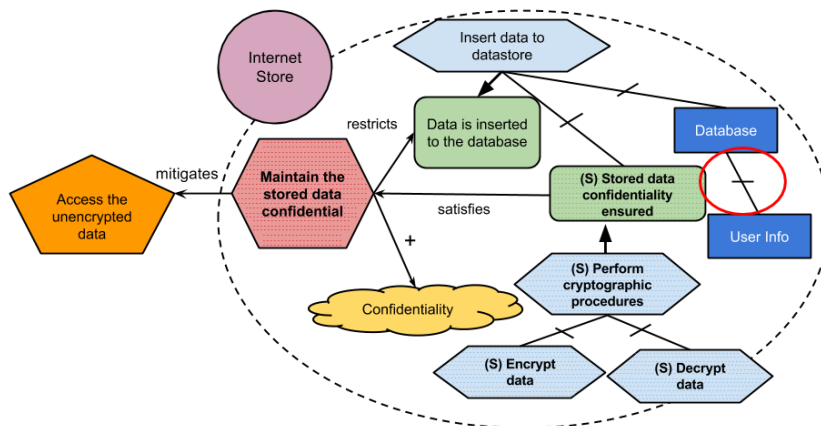


Fig 8.35 - PB SRP5 applied STEP 3

As participant A, PB executed the fourth step correctly demonstrating the events of an attack. The participant implemented successfully the model in order to justify the security requirements introduced in the previous third step (see Figure 8.36).

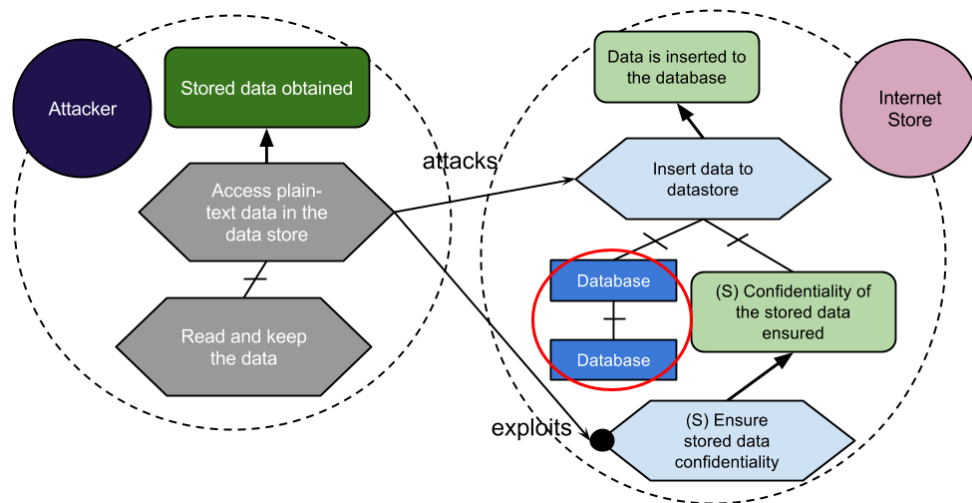


Fig 8.36 - PB SRP5 applied STEP 4

Observations

After the introductory lecture PB asked several questions concerning the performance of the pre-processing step. B preferred not to perform the pre-processing and moved directly forward by applying security constraints and criteria during step 2. In general, the process was executed accurately and PB was able to utilize one pattern described by our suggested pattern representation. B's previous knowledge of the ISSRM principles is interpreted as a success-factor of the participant's performance.

Remarks

The participant gave a positive feedback to all the questions of the questionnaire. Main comments concerned the RAST process. Similarly to other participants, PB also commented the given timeframe as too short. According to PB, participants would gain deeper understanding from more time. PB was moderately satisfied with the pattern presentation. One of his observations indicated that a larger amounts of examples would be required in order to better understand the overall process. The participant found the step of identifying the pattern occurrence as the easiest to perform. The most difficult step to be executed according to PB, was the introduction of the security requirements. Lastly the participant had positive impressions regarding the pattern representation and application process.

PARTICIPANT C

Background

Participant C (PC) is a Software Engineering master degree student at the time of the study being conducted. PC is employed in the field of IT enterprise security. The participant has previous knowledge of the ISSRM domain model, process and security requirement elicitation. The participant attended the entire introductory lecture of the case study and completed the application of two patterns in the given model. The patterns to be applied by participant PC are SRP1, SRP3.

Pattern Application

SRP1

Participant C required around 1 hour to apply the SRP1. PC successfully identified that the pattern is applicable in the user interface and internet store actor of the case study model presented in Chapter 6. SRP1 identifies and mitigates the threat of data being intercepted when transmitted between business services. The participant isolated correctly the assets involved in the pattern (see Figure 8.37) and applied security constraints and criteria that restrict the main goal. Moreover applied correctly the secure goals and the plans to be executed in order for them to be achieved (see Figure 8.38). In this instance the participant incorrectly phrased the secure goal where instead of “User Info” he wrote “Data”. The mistake here is crucial. This because it will affect the security requirements resulting from the process. Thus incorrectly security a different process and resources. Furthermore participant C did not specify that the user actor implies the existence of an interface. PC decided to follow a different modeling structure.

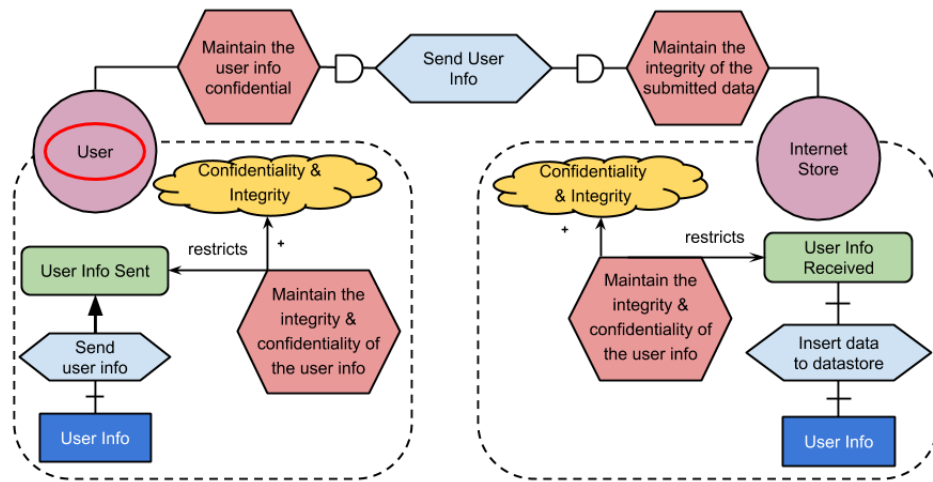


Fig 8.37 - PC SRP1 applied STEP 2 (a)

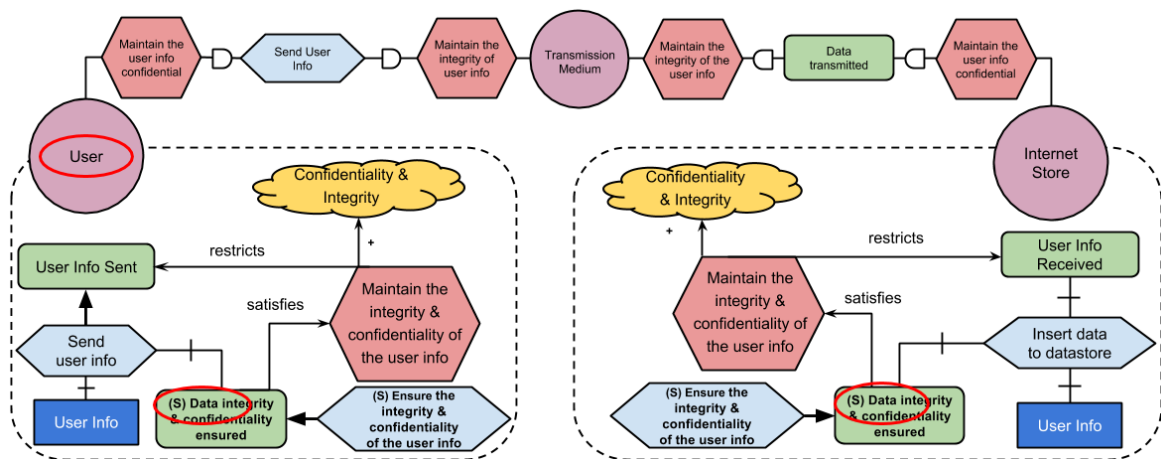


Fig 8.38 - PC SRP1 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans the participant correctly replaced the secure plan of Ensure Confidentiality & Integrity of the User Info in both the user interface and internet with the requirement suggested by the pattern (see Figure 8.39).

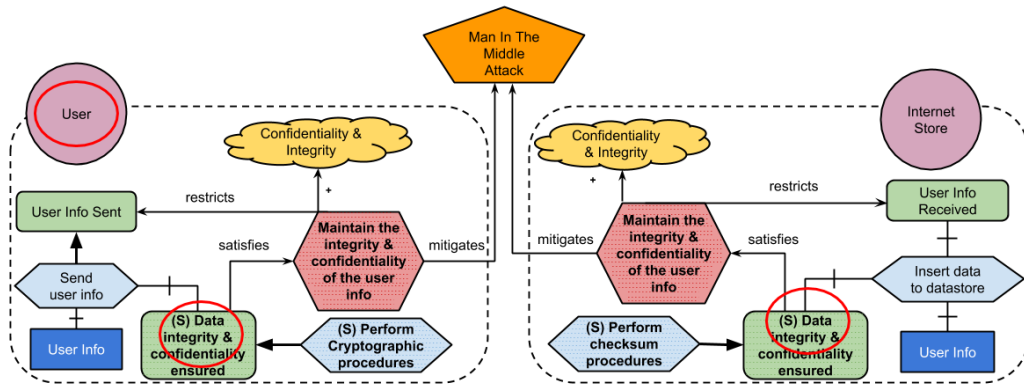


Fig 8.39 - PC SRP1 applied STEP 3

The participant executed the fourth step showing the events of an attack. The model justified the security requirements introduced in the previous step (see Figure 8.40). PC incorrectly phrased most assets of the Attacker and Transmission Medium. C incorrectly used in the phrasing “Submitted data” instead of “User info” that is the actual transmitted data.

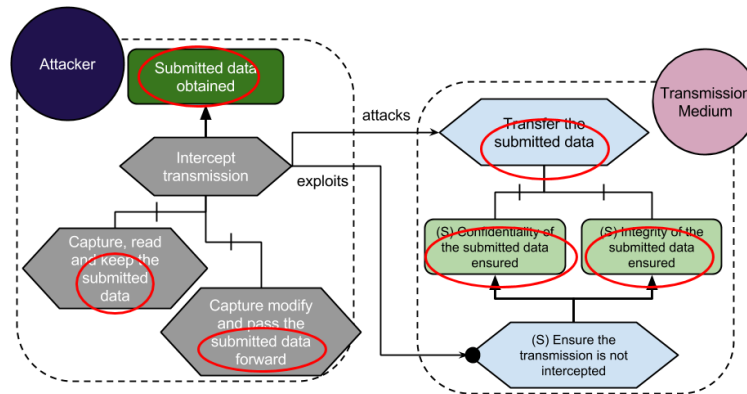


Fig 8.40 - PC SRP1 applied STEP 4

SRP3

PC identified that SRP3 is applicable in the internet store actor of the given model. SRP3 identifies and mitigates the threat of a denial of service attack to a business service. He identified and isolated incorrectly the assets involved in the pattern (see Figure 8.41) and applied security constraints and criteria that restrict the main goal. PC incorrectly phrases the security constraint and wrongfully decomposes the main plans. Additionally in STEP 2 (a) PC incorrectly restricts Message is registered goal (see Figure 8.42). As the other respondents, PC applied secure goals and plans to be executed. The participant incorrectly phrases the secure goals and plans where he does not specifically state the provided service.

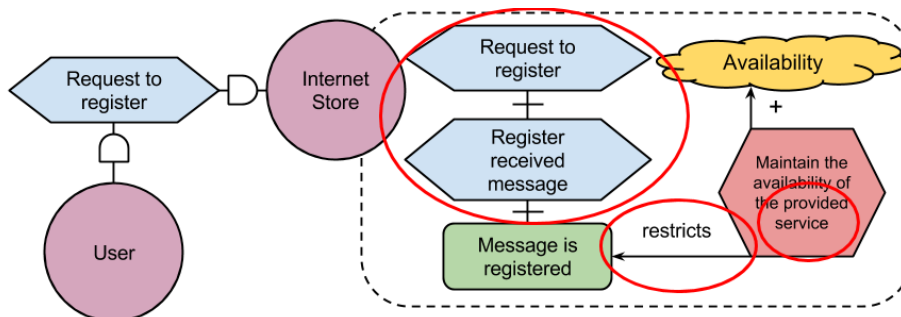


Fig 8.41 - PC SRP3 applied STEP 2 (a)

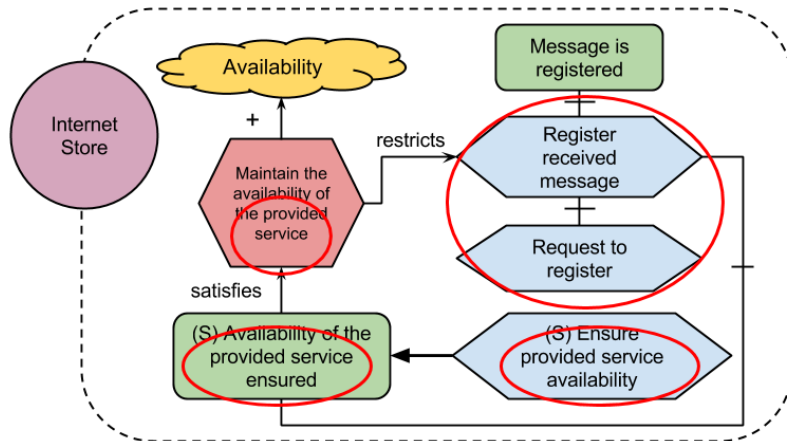


Fig 8.42 - PC SRP3 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans the participant correctly replaced the secure plan of Ensure provided service availability of the internet store actor with the requirement suggested by the pattern (see Figure 8.43).

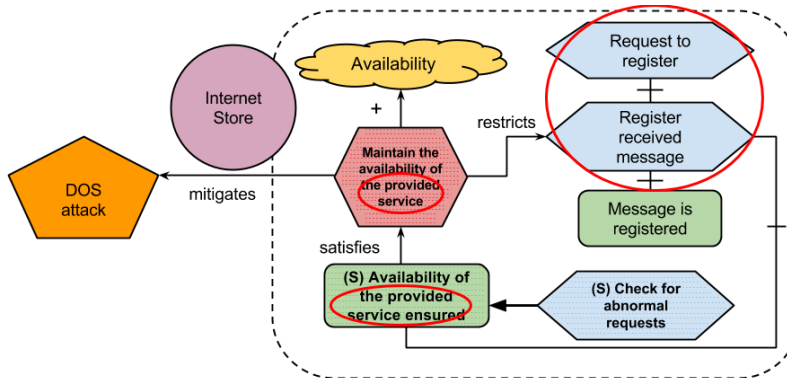


Fig 8.43 - PC SRP3 applied STEP 3

Lastly the validation and rationale step was performed incorrectly (see Figure 8.44). The participant incorrectly justified the assets to be attack and exploited. Though here he made a considerable number of phrasing mistakes. The mistakes made in this stage introduce ambiguity and defeat the purpose of validating the previously introduced requirements.

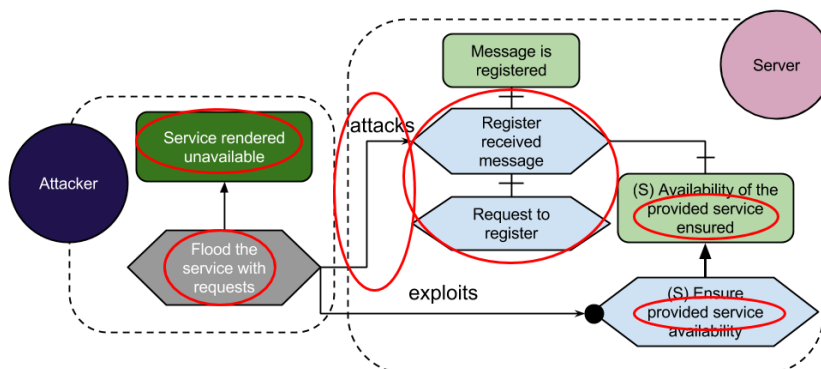


Fig 8.44 - PC SRP3 applied STEP 3

Observations

After the introductory lecture, PC had no questions due to his familiarity with the ISSRM process and previous knowledge of Secure Tropos. The overall process was executed accurately despite phrasing mistakes were made. Additionally the participant was able to utilize both patterns described by our suggested pattern representation. Furthermore we asses that the previous familiarity of the participant with the involved concepts had significant impact in the results leading us to confirm that the process of learning the pattern application process is easier for the participant with a security background.

Remarks

PC gave positive feedback, with main comments being directed towards the structuring of the constructs. Furthermore the participant found the step of identifying the pattern occurrence as the easiest to perform. The most difficult step to be executed according to the participant was the re-integration of the extracted assets. The participant had positive impressions regarding the pattern representation and application process.

PARTICIPANT D

Background

Participant D (PD) is Software Engineering master degree student at the time of the study being conducted. The participant was previously unfamiliar with the ISSRM domain model, process and security requirement elicitation. The participant attended the entire introductory lecture of the case study and completed the application of one pattern in the given model. The pattern applied by participant D was SRP4.

Pattern Application

SRP4

To apply the SRP5 PD required around one hour. PD precisely identified that the pattern is applicable in the user interface actor of the case study model presented in Chapter 6. SRP4 identifies and mitigates the threat of confidential business data being accessed by an attacker. The attack occurs by exploiting the fact that there is no access control mechanism in place. The participant isolated correctly the assets involved in the pattern (see Figure 8.45) and applied security constraints and criteria that restrict the main goal. Comparing D's models with the correct ones of section VII is identified that he incorrectly phrases in the security constraint "Maintain password confidentiality" instead of "Maintain data confidentiality". This leads to perpetual ambiguity regarding the subject that the security constraint restricts. Moreover he applied correctly the secure goals and the plans to be executed in order for them to be achieved (see Figure 8.46). The participant incorrectly phrased the secure goals and plans where instead of "password" he states "user info".

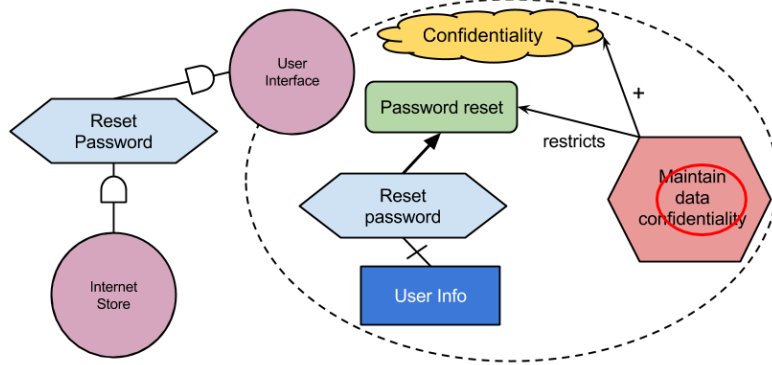


Fig 8.45 - PD SRP4 applied STEP 2 (a)

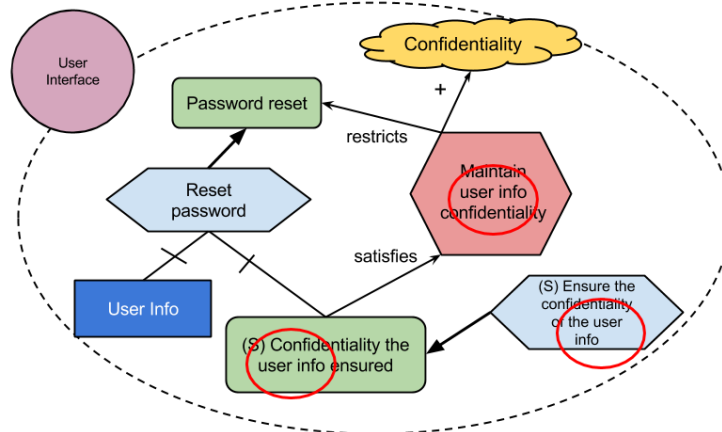


Fig 8.46 - PD SRP4 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans PD successfully replaced the secure plan of Ensure the confidentiality of the user info with the requirement suggested by the pattern (see Figure 8.47). Nonetheless here PD carries over the incorrect phrasing of the previous constructs.

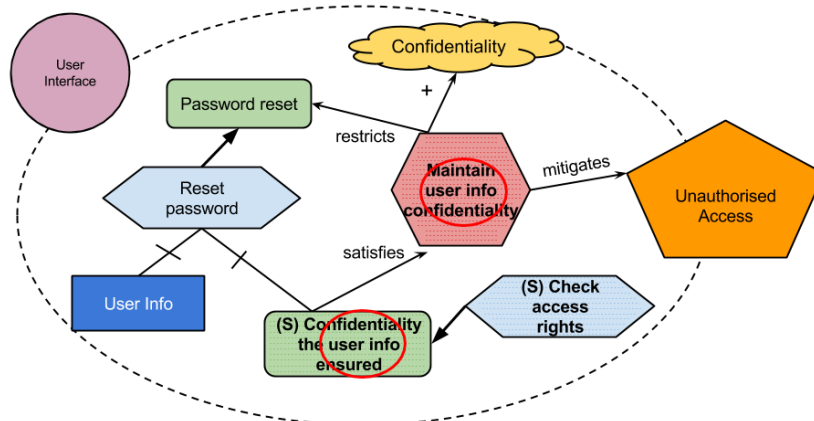


Fig 8.47 - PD SRP4 applied STEP 3

Participant D correctly executed the composition and modeling of the assets of the fourth step correctly, nonetheless mistakes were made in phrasing (see Figure 8.48). The incorrectness yet again in this case occurs in the phrasing of the assets. In this instance the assets of the attacker mistakenly refer “Data” as the subject of the attack instead of

“Password”. Additionally all the assets of the user interface actor incorrectly use the term “User Info” instead of “Password”.

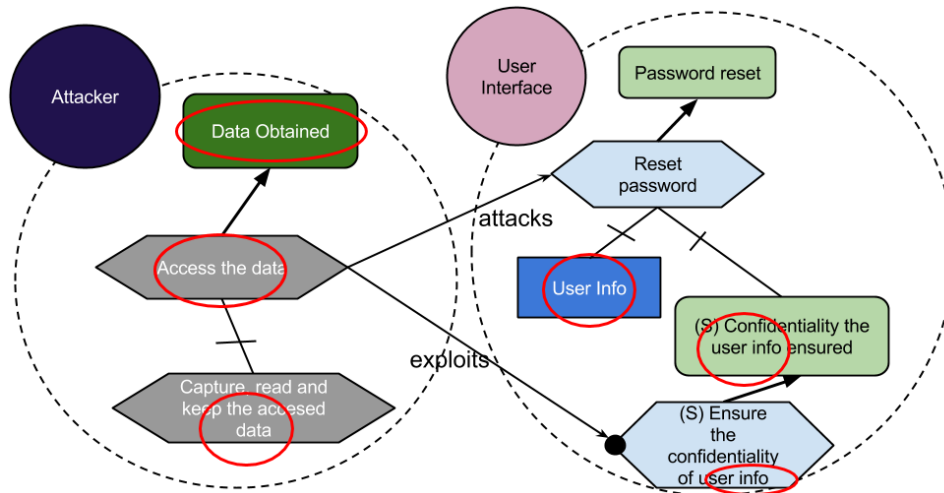


Fig 8.48 - PD SRP4 applied STEP 4

Observations

Due to lacking knowledge, PD had numerous questions after the introductory lecture. Most of the questions were concerned with the risk assessment process and the pattern application rationale. As the majority of the participants, PD chose not to perform the pre-processing. The participant applied the security constraints and criteria during the second step of the process. Overall the modeling part of the process was followed accurately though mistakes were made in the phrasing of the assets. Overall the participant was not confident in his performance. Furthermore we asses that the having no previous knowledge of the ISSRM principles did not affect the overall pattern application process.

Remarks

The participant gave an overall moderated assessment to the questionnaire. Most of the participants’ questions where directed towards the RAST process. Similar to other participants the limited timeframe was criticized. According to PD more time would ensure a better understanding of the pattern. The participant found the step of extracting the identified assets related to the pattern as the easiest to perform. The most difficult step to be executed according to the participant was the identification of the pattern occurrence. Lastly the participant had positive impressions regarding the pattern representation and application process.

PARTICIPANT E

Background

Participant E (PE) is a Software Engineering master degree student at the time of the study being conducted. The participant was previously unfamiliar with the ISSRM domain model, process and security requirement elicitation. PE attended the entire introductory lecture of the case study and completed the application of one pattern in the given model. The pattern to be applied by PE is SRP1.

Pattern Application

SRP1

E required around one and half hour to apply the SRP1. PE correctly identified that the pattern is applicable in the user interface actor of the case study model presented in Chapter 6. SRP1 identifies and mitigates the threat of data being intercepted when transmitted between business services. The participant isolated correctly most of the assets involved in the pattern (see Figure 8.49) except for the User info resource that was neglected. Additionally PE incorrectly connected the Insert data to datastore plan to the User info received goal with a Means-ends instead of the decomposition link. Comparing PE's models with the correct ones of section VII is identified that he incorrectly applied security constraints and criteria that restrict the main goals by overlooking the phrasing conventions and used the exact phrasing used for the assets of SRP1 pattern. Moreover he followed the guidelines and modeled correctly the secure goals and the plans, again by overlooking phrasing conventions (see Figure 8.50). Furthermore the participant did not model correctly the link between the security constraint and criterion (see Figure 8.49, 8.50). In addition PD incorrectly modeled the direction of the dependency in both STEP2 a and b.

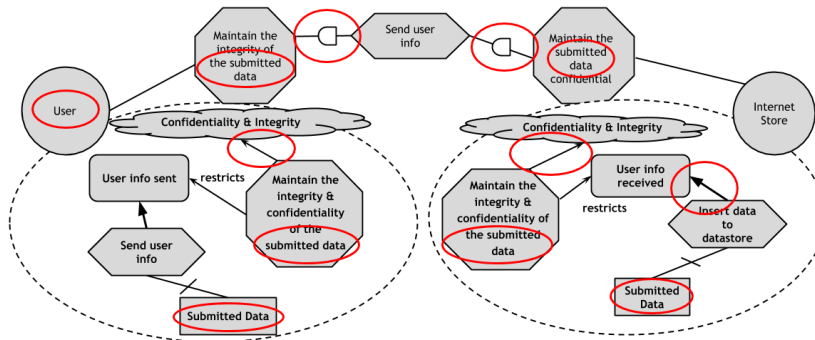


Fig 8.49 - PE SRP1 applied STEP 2 (a)

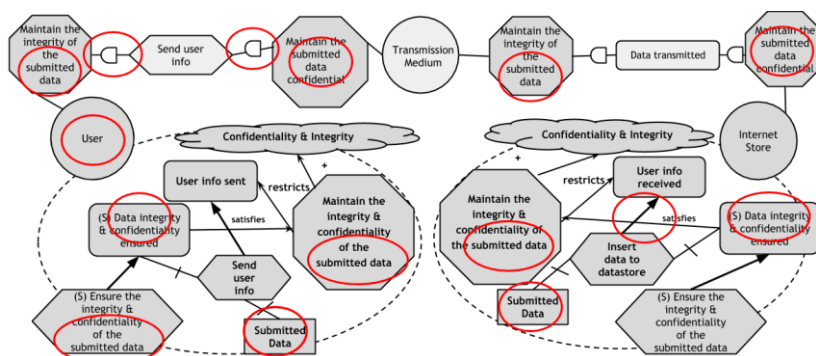


Fig 8.50 - PE SRP1 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans the participant correctly replaced the secure plan of Ensure confidentiality & integrity of the submitted data with the requirement suggested by the pattern (see Figure 8.51). In this step the participant modeled incorrectly the construct of the threat.

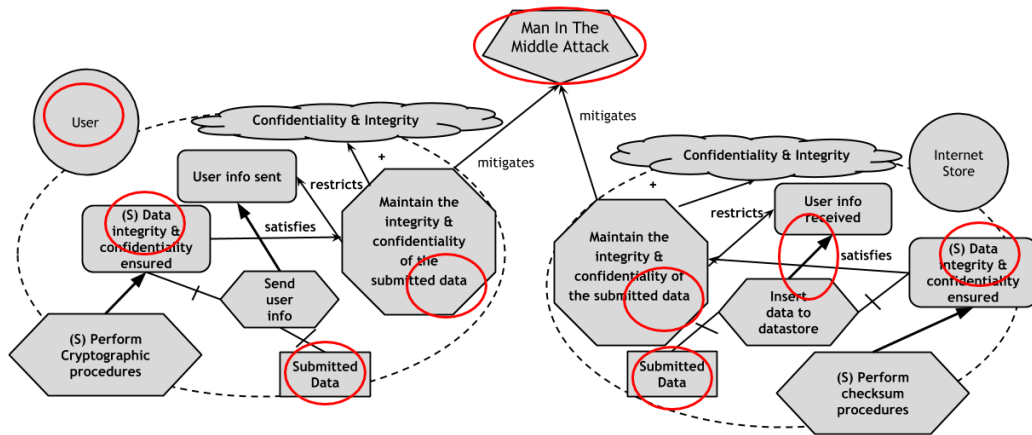


Fig 8.51 - PE SRP1 applied STEP 3

The application of the fourth step was performed incorrectly demonstrating the events of an attack (see Figure 8.52). Here PD repeatedly addresses the transmitted information as “Submitted” data instead of “User info”. This results in the diagram being unusable to justify the introduced requirements.

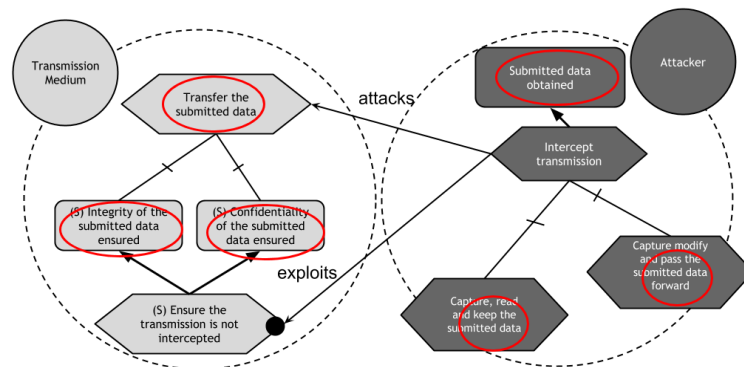


Fig 8.52 - PE SRP1 applied STEP 4

Observations

After the introductory lecture PE had multiple questions regarding the ISSRM process and the RAST process. Overall the process was not executed accurately despite the participant was able to utilize one pattern described by our suggested pattern representation. Additionally the phrasing and coloring conventions were not followed correctly. The participant stated that he did not comprehend the need for the differentiated phrasing and colors. In this case we assess that having no previous knowledge of the ISSRM principles had a negative contribution to the participants overall performance.

Remarks

The participant reported an overall moderate feedback to all the questions of the questionnaire. Main comments were stated regarding the ISSRM and RAST processes. One of his observations indicated that a greater amount of time is required for grasping the process. Furthermore the participant found the step of identifying the pattern occurrence as the easiest to perform. The most difficult step to be executed according to the participant was the introduction of the security

PARTICIPANT F

Background

Participant F (PF) is a Software Engineering master degree student at the time this study being conducted. The Participant is employed in the field of software engineering. The participant had a small familiarity with the ISSRM domain model and process. PF attended the entire introductory lecture of the case study and completed the application of one pattern in the given model. The pattern applied by F was SRP2.

Pattern Application

SRP2

PF required roughly 45 minutes to apply the SRP5. PF correctly identified that the pattern is applicable in the internet store actor of the case study model presented in Chapter 6. SRP2 identifies and mitigates the threat of malicious data being propagated between business services. The participant extracted correctly the assets involved in the pattern (see Figure 8.53) and applied security constraints and criteria that restrict the main goal. Moreover he followed the guidelines and applied correctly the secure goals and the plans to be executed (see Figure 8.54). In both steps the participant referees incorrectly in the secure constraint/goal/plan to the user info as data thus introducing ambiguity.

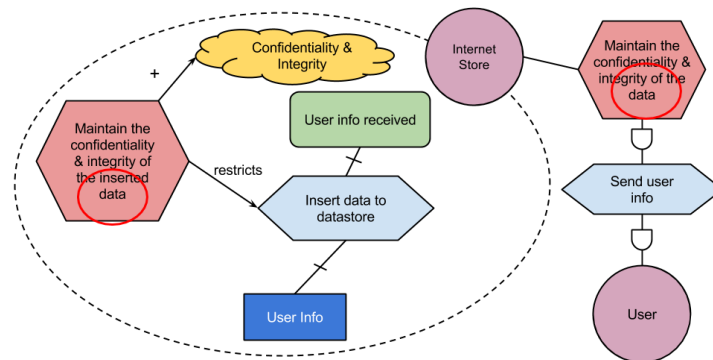


Fig 8.53 - PF SRP2 applied STEP 2 (a)

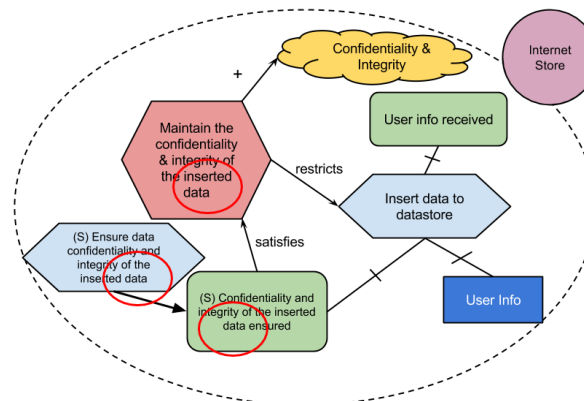


Fig 8.54 - PF SRP2 applied STEP 2 (b)

Following the application of the security constraints, criteria, goals and plans the participant correctly replaced the secure plan Ensure the confidentiality and integrity of the inserted data with the requirement suggested by the pattern (see Figure 8.55). In this instance participant F reuses the incorrect phrasing introduced in the first two steps.

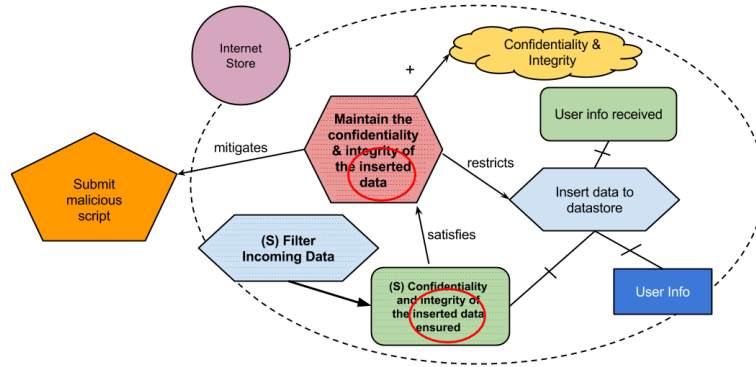


Fig 8.55 - PF SRP2 applied STEP 3

The modeling of the fourth step was performed correctly by the participant demonstrating the events of an attack (see Figure 8.56). Though here Comparing PF’s models with the correct ones of section VII we observe that the phrasing of the malicious goal is incorrect. The participant named the malicious goal as “Internet Store Activity Harmed” instead of “User info database harmed”.

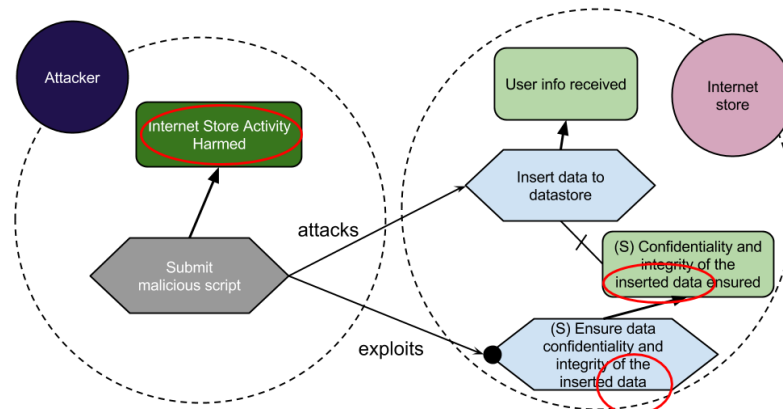


Fig 8.56 - PF SRP2 applied STEP 4

Observations

After the introductory lecture the participant had multiple questions regarding the pattern representation and application. PF chose not to perform the pre-processing step. Overall the process was executed moderately accurately and the participant was able to utilize one pattern described by our suggested pattern representation. Furthermore we asses that the small previous knowledge of the ISSRM principles had a considerable contribution to the participants overall performance.

Remarks

The feedback regarding the questionnaire of PF can be evaluated as overall positive. Main comments revolved regarding the pattern representation. F shared the negative aspect of lacking time as indicated by the other respondents. PF observed that a longer explanations are required for the patterns in order to be understandable at first glance. The participant found the step of identifying the pattern occurrence as the easiest to perform. The most difficult step to be executed according to the participant was the re-integration of the extracted assets. Finally the participant had positive impressions regarding the pattern representation and application process.

VII. Correct Pattern Applications

For the purpose comparing the results of the participants of the case study conducted in Chapter 6 in this section we present the correct models of the patterns presented in this work. The patterns are applied to the internet store model presented in Chapter 6. In Figure 8.57 we identify where each pattern is applicable in the model.

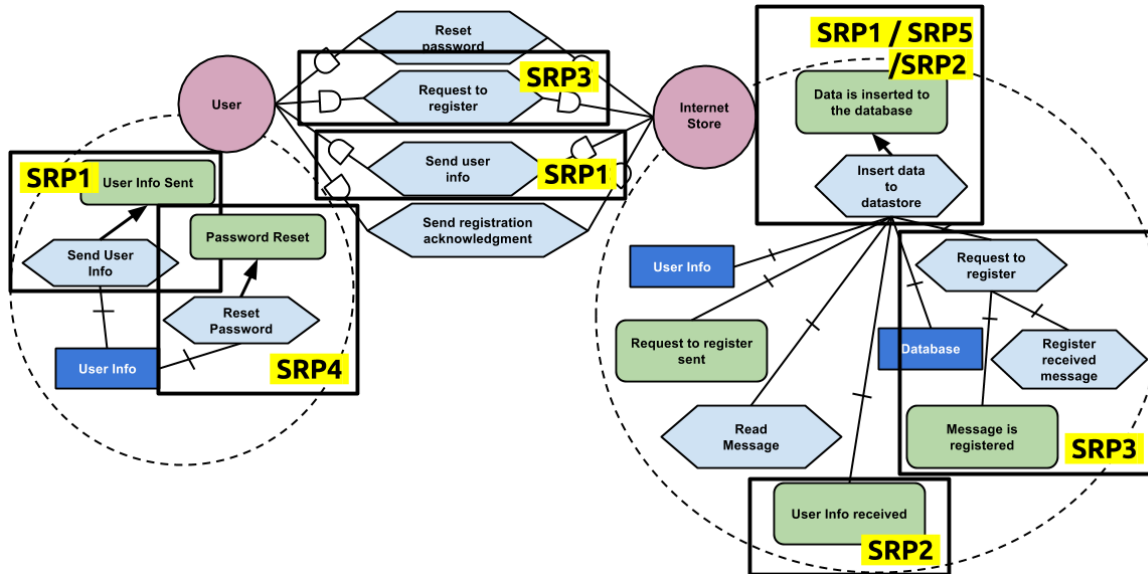


Fig 8.57 - SRP's identified in the Internet Store model

In detail individually the patterns are applicable for:

SRP1: Applicable in the User (User Interface) actor and Internet Store actor. SRP1 is applicable for the dependency of Send user info between the two actors.

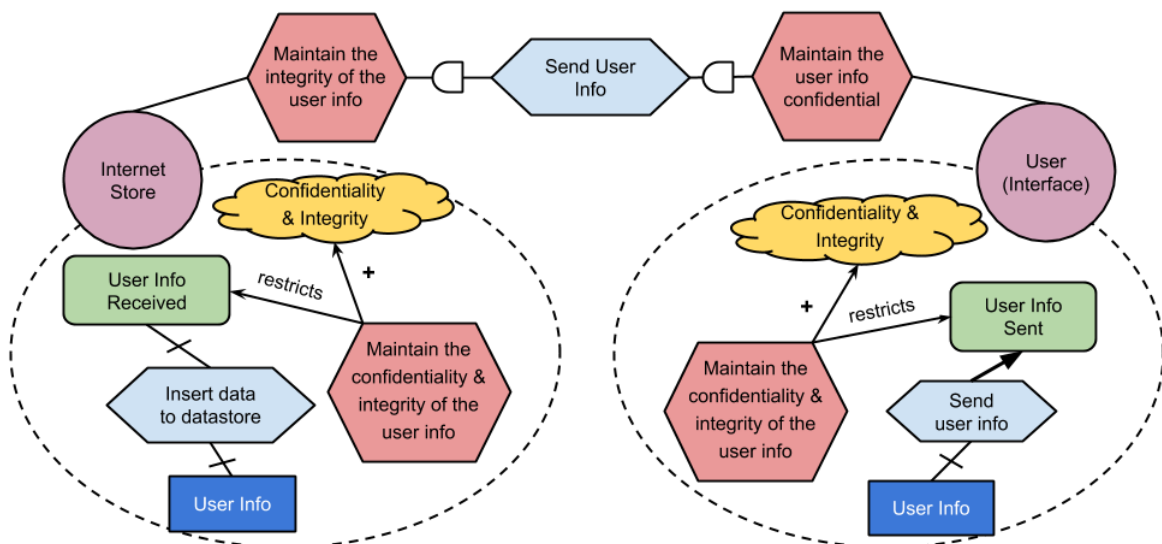


Fig 8.58 - Case Study, SRP1 Correct Application STEP2 (a)

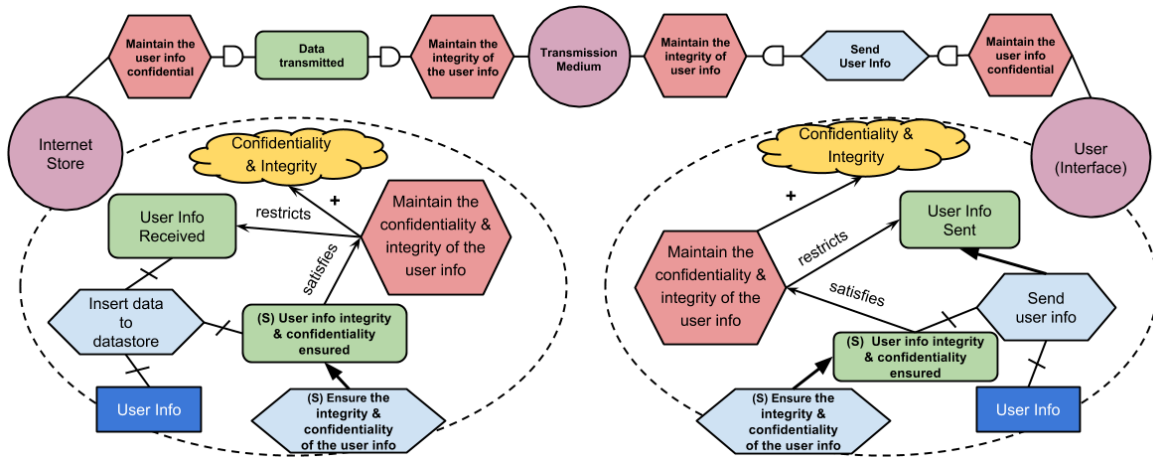


Fig 8.59 - Case Study, SRP1 Correct Application STEP2 (b)

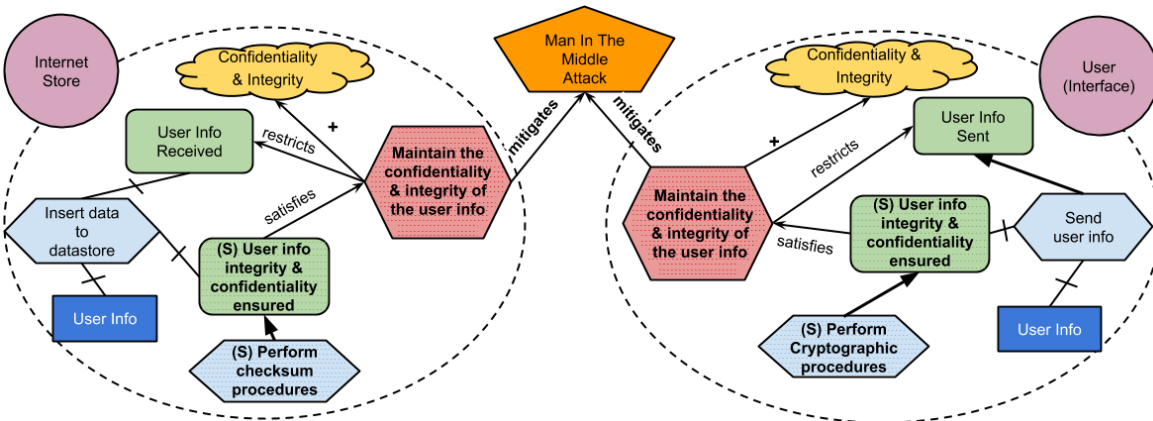


Fig 8.60 - Case Study, SRP1 Correct Application STEP3

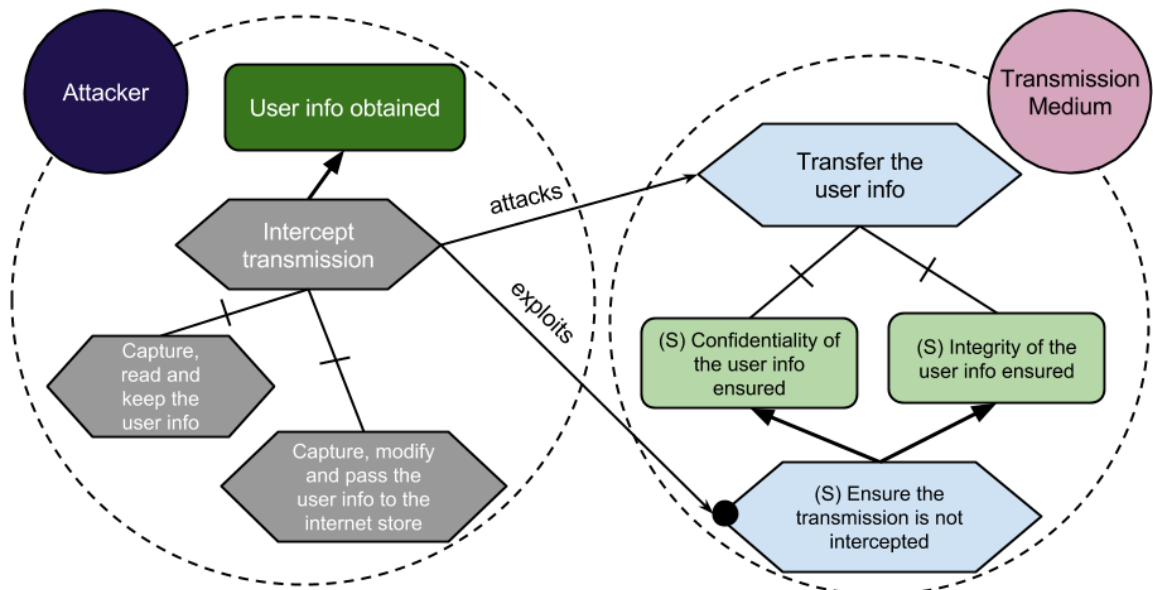


Fig 8.61 - Case Study, SRP1 Correct Application STEP4

SRP2: Applicable in the Internet Store actor for the goal of User info received.

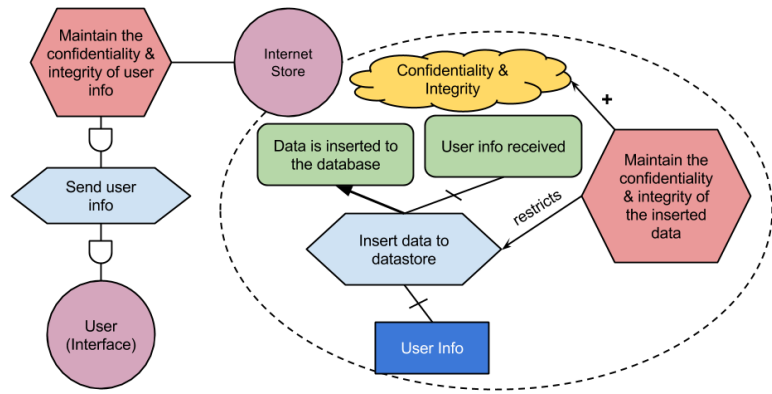


Fig 8.62 - Case Study, SRP2 Correct Application STEP2 (a)

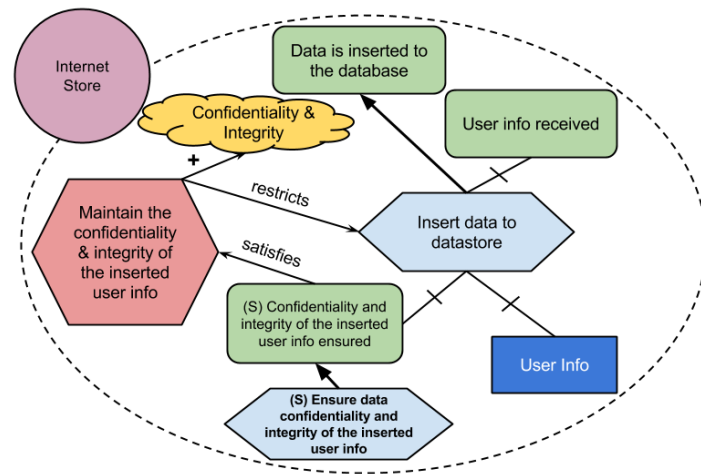


Fig 8.63 - Case Study, SRP2 Correct Application STEP2 (b)

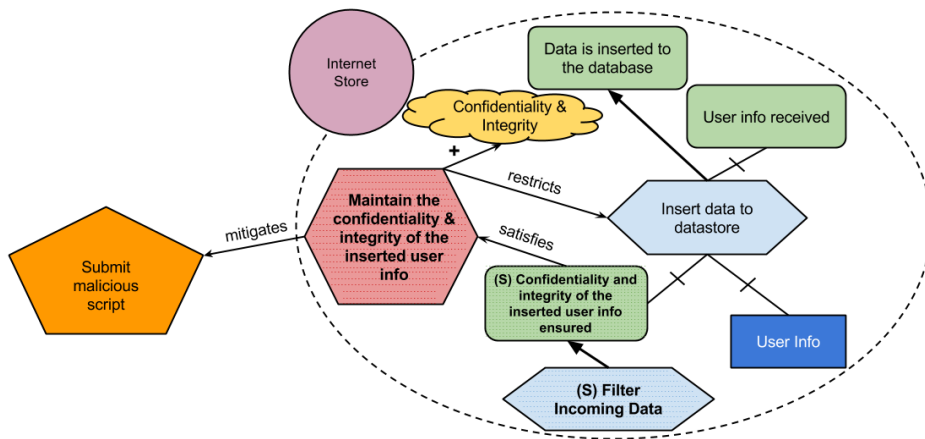


Fig 8.64 - Case Study, SRP2 Correct Application STEP3

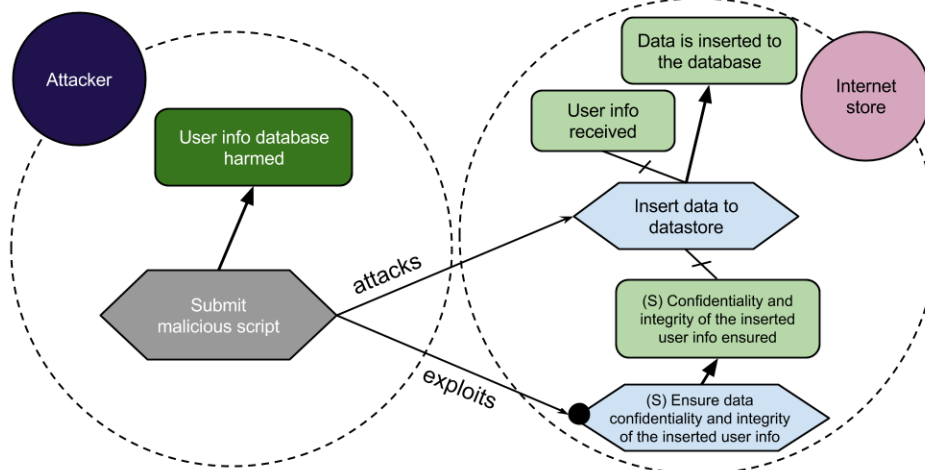


Fig 8.65 - Case Study, SRP2 Correct Application STEP4

SRP3: Applicable in the Internet Store actor. SRP3 applies for the dependency of Request to register between the User (User Interface) actor and Internet Store actor. The security measures related to this pattern are applicable for the Message is registered.

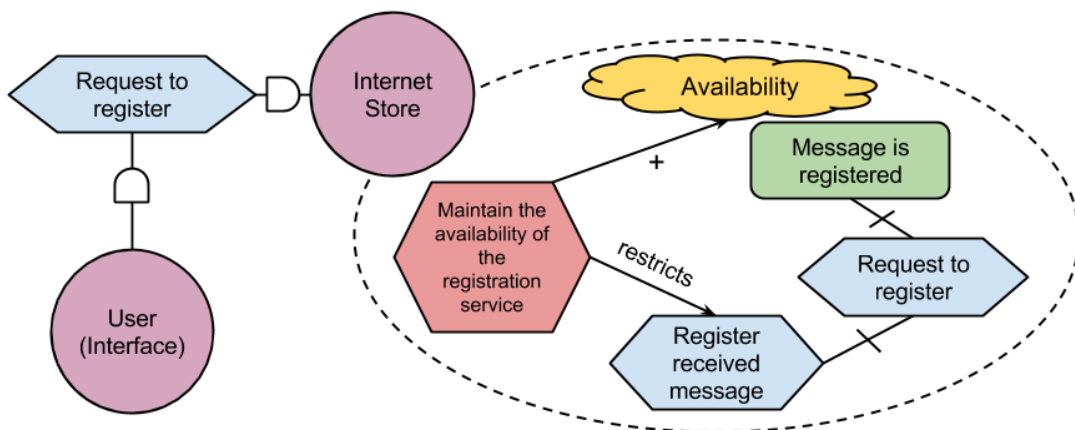


Fig 8.66 - Case Study, SRP3 Correct Application STEP2 (a)

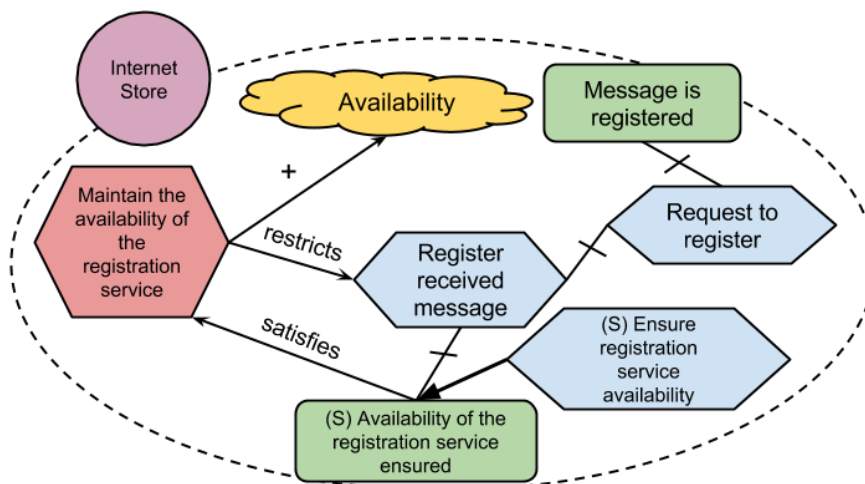


Fig 8.67 - Case Study, SRP3 Correct Application STEP2 (b)

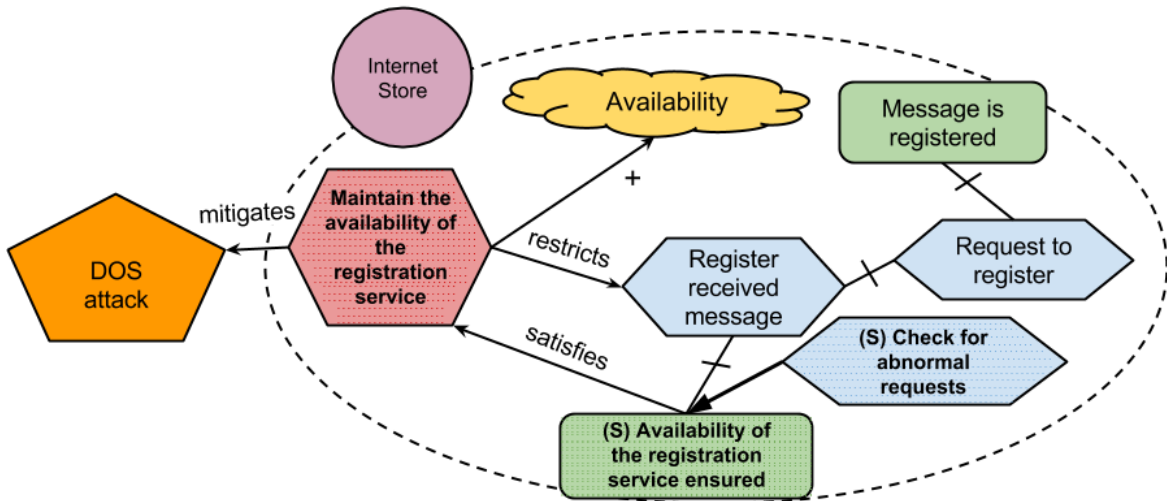


Fig 8.68 - Case Study, SRP3 Correct Application STEP3

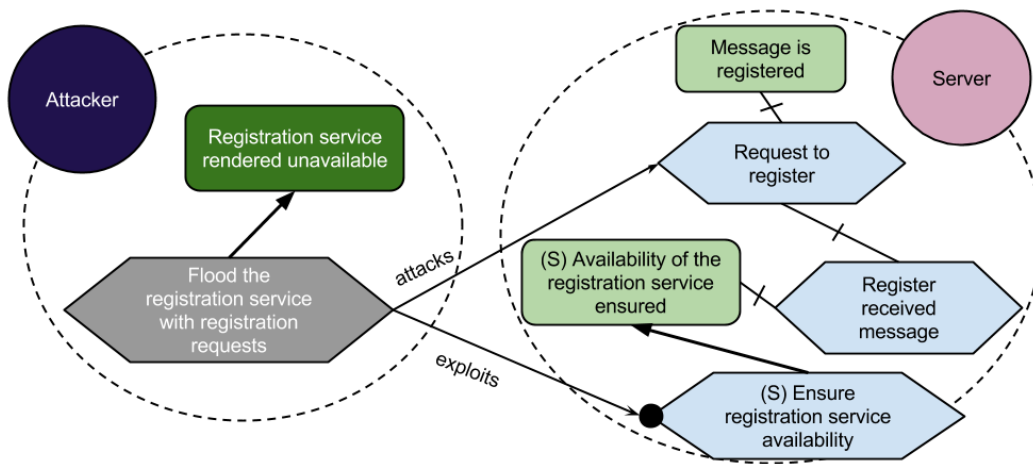


Fig 8.69 - Case Study, SRP3 Correct Application STEP4

SRP4: Applicable in the User (User Interface) for the goal of Password Reset.

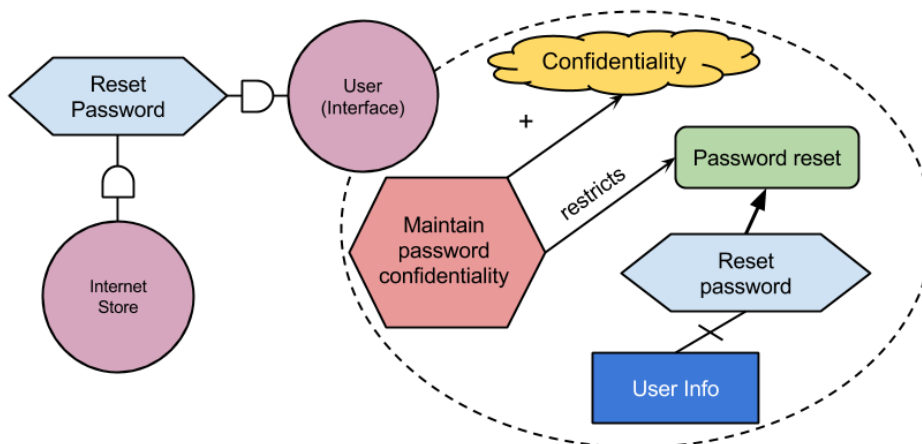


Fig 8.70 - Case Study, SRP4 Correct Application STEP2 (a)

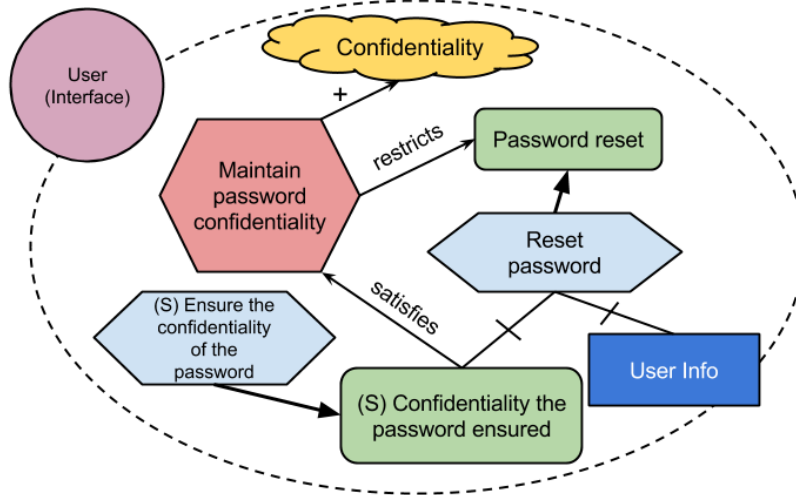


Fig 8.71 - Case Study, SRP4 Correct Application STEP2 (b)

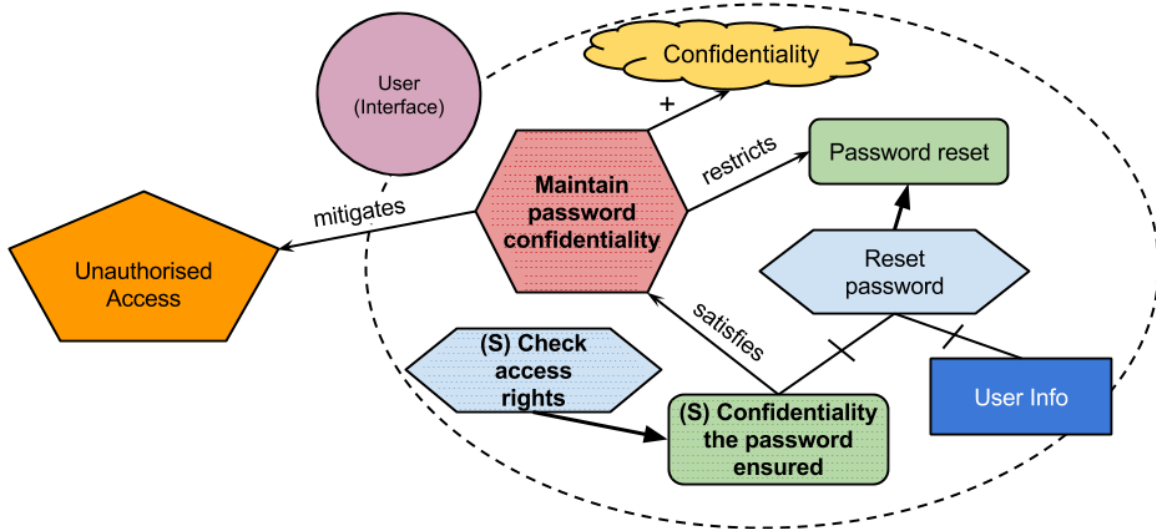


Fig 8.72 - Case Study, SRP4 Correct Application STEP3

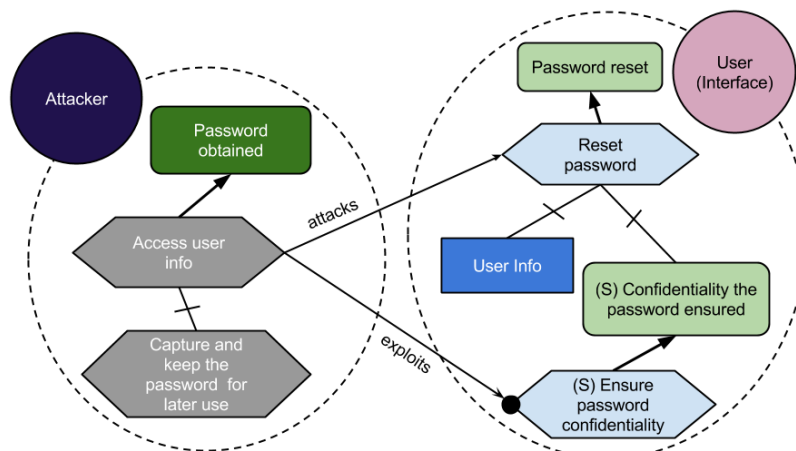


Fig 8.73 - Case Study, SRP4 Correct Application STEP4

SRP5: Applicable in the Internet Store actor at the goal Data is inserted to the database.

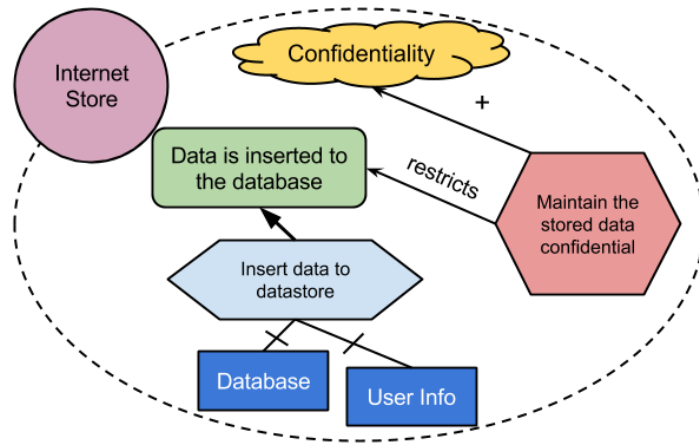


Fig 8.74 - Case Study, SRP5 Correct Application STEP2 (a)

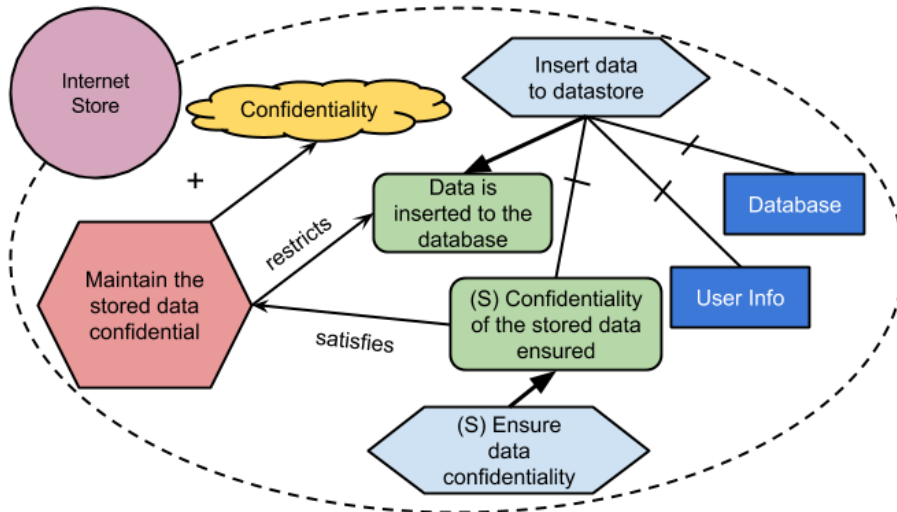


Fig 8.75 - Case Study, SRP5 Correct Application STEP2 (b)

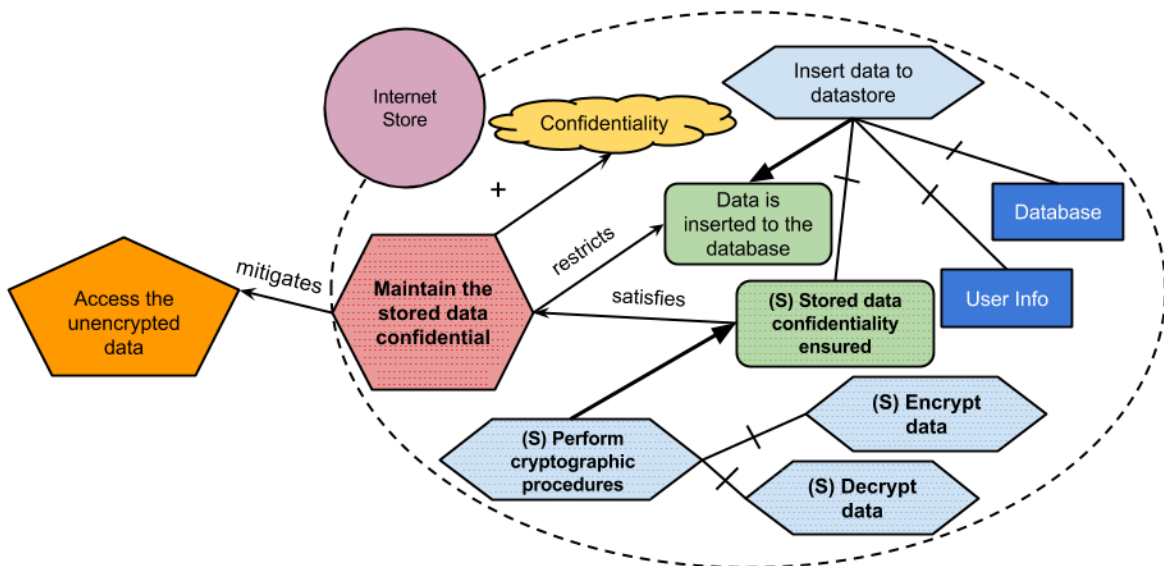


Fig 8.76 - Case Study, SRP5 Correct Application STEP3

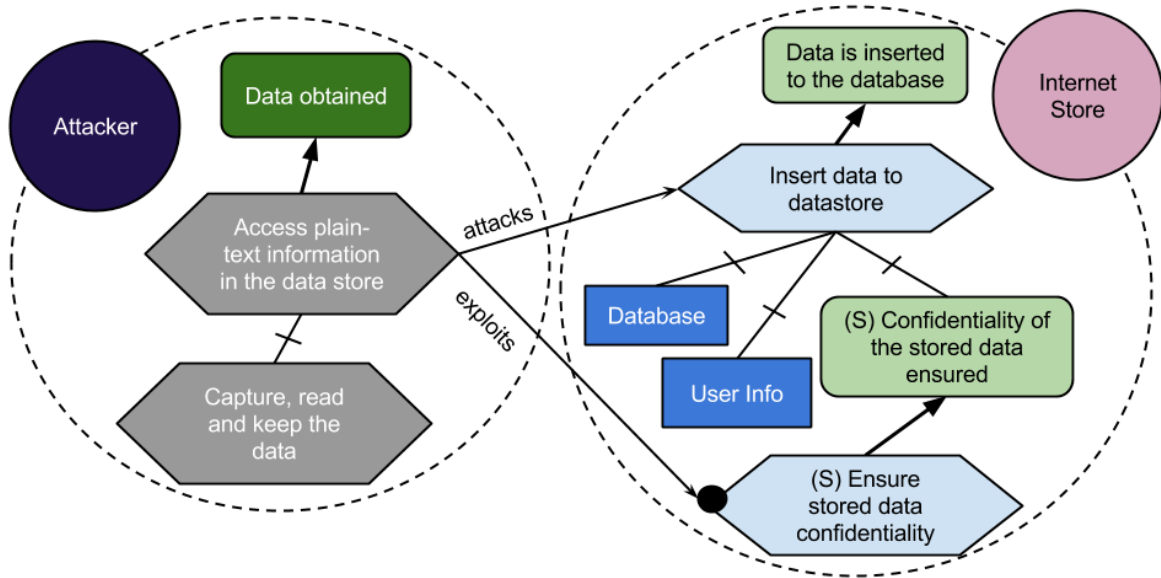


Fig 8.77 - Case Study, SRP5 Correct Application STEP4

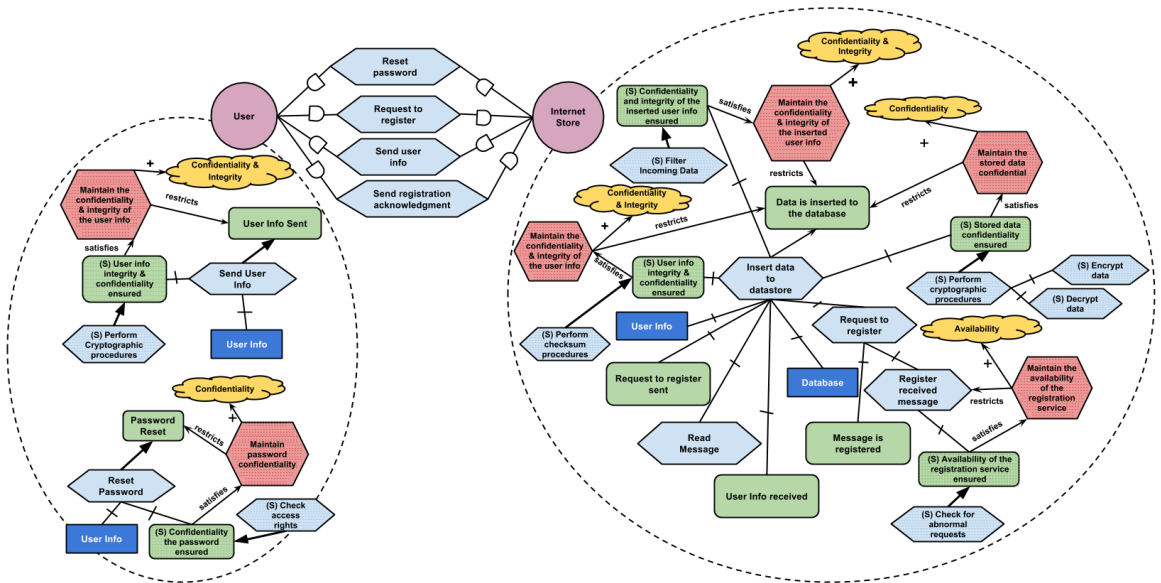


Fig 8.78 - All the Patterns Correctly Re-Integrated In the Model (STEP5)

VIII. Case Study Questionnaire Answers

Group A includes participants PA, PB, PC and Group B includes PD, PE and PF.

	PA	PB	PC	PD	PE	PF
1) How easy is to learn to apply the RAST process?	c	c	c	b	c	b
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
2) How understandable was the RAST application process?	c	b	c	b	c	b
a) Not at all Understandable b) Slightly Understandable c) Moderately Understandable d) Very Understandable						
3) How easy is to learn a pattern expressed in RAST?	c	c	d	c	d	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
4) How satisfied are you with the overall presentation of the RAST patterns?	c	d	d	c	d	c
a) Not at all satisfied b) Slightly Satisfied c) Moderately Satisfied d) Very satisfied						
5) How understandable were the RAST patterns?	c	c	c	c	c	c
a) Not at all Understandable b) Slightly Understandable c) Moderately Understandable d) Very Understandable						
6) How easy is to pre-process a given model?	c	c	c	b	a	b
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
7) How easy is to identify goal/plan/resource/dependencies that are under risk?	c	d	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
8) How easy is to apply constraints and security criteria to a goal/plan/resource/dependencies?	b	c	d	c	d	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
9) How easy is to identify where the pattern is applicable within the main model?	c	b	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
10) How easy is to extract the assets involved in pattern from the main model?	c	b	c	b	c	b
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
11) How easy is to replicate/adjust the pattern to a not previously encounter model?	b	c	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
12) How easy is to identify/apply secure goals and plans to the assets of an actor?	b	b	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
13) How easy is to replace secure goals and plans with the controls suggested by a pattern?	c	b	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
14) How easy is to re-integrate the previously extracted portion of the main model with the security requirements applied?	b	c	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
15) Which step of the application process steps was the most easiest to apply?	b	b	b	c	b	b
a) Step 0, Model Pre-Processing						
b) Step 1, Occurrence Identification & Asset Alignment						
c) Step 2, Asset Extraction & Secure Goal Introduction						
d) Step 3, Security Requirement Introduction						
e) Step 4, Security Requirement Rationale & Validation						
f) Step 5, Extracted Model Re-Integration						
16) Which step of the application process steps was the most difficult to apply?	d	d	f	b	d	f
a) Step 0, Model Pre-Processing						
b) Step 1, Occurrence Identification & Asset Alignment						
c) Step 2, Asset Extraction & Secure Goal Introduction						
d) Step 3, Security Requirement Introduction						
e) Step 4, Security Requirement Rationale & Validation						
f) Step 5, Extracted Model Re-Integration						
17) How easy is to learn the pattern application process overall?	d	c	c	c	c	d
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
18) How easy do you believe that the pattern application process is?	c	b	c	b	c	c
a) Not at all Easy b) Slightly Easy c) Moderately Easy d) Very Easy						
19) How efficient do you believe that the application process is?	d	c	c	c	c	c
a) Not at all Efficient b) Slightly Efficient c) Moderately Efficient d) Very Efficient						
20) How understandable was the pattern application process overall?	c	d	c	c	c	c
a) Not at all Understandable b) Slightly Understandable c) Moderately Understandable d) Very Understandable						
21) How satisfied are you with the results of the pattern application process overall?	c	b	c	b	c	b
a) Not at all satisfied b) Slightly Satisfied c) Moderately Satisfied d) Very satisfied						

IX. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Atilio Rrenja** (date of birth: 29.09.1987),

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,

of my thesis

Pattern Based Security Requirement Derivation with Security Risk-aware Secure Tropos,

supervised by Dr. 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, **21.05.2015**