UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Institute of Computer Science
Cyber Security Curriculum

Karl Kolk

An Empirical Comparison of Approaches for Security Requirements Elicitation

Master's Thesis (30 EAP)

Supervisor:Dr. Raimundas Matulevicius

Tartu 2015

Abstract

The importance of security engineering in the development cycle is widely accepted. In spite of the large variety of security requirements elicitation techniques, organizations struggle to select the most suitable security requirements elicitation method that would enable the elicitation of security requirements with the most complete coverage.

Two potential solutions exist to this problem; Security Quality Requirements Engineering (SQUARE) and Security Requirements Elicitation from Business Processes (SREBP). SQUARE is an already established and widely used security requirements elicitation method that addresses security early in the software development cycle. On the other hand, SREBP is a new approach that helps derive security requirements from operational business processes. To address the above mentioned issue, this thesis compares the two methods based on an empirical case study of the Estonian Football Association. The elicited security requirements are categorized and the completeness of their coverage is compared.

As a result, it was determined that SREBP provides more coverage of the security requirements. Such a result contributes to the existing literature by further strengthening the validity of SREBP.

Key words: Security Engineering, Security Quality Requirements Engineering (SQUARE), Security Requirements Elicitation from Business Processes (SREBP), Security requirements, Empirical comparison.

Turvanõuete Tuletamise Meetodite Empiiriline Võrdlus

Lühikokkuvõte

Kaasaegne töökeskond on tihedalt seotud infotehnoloogiaga (edaspidi IT). Seoses IT laialdase kasutamisega kõigis eluvaldkondades on üles kerkinud küsimus selle turvalisusest. Turvalisuse tagamine IT valdkonnas on tähtsal kohal. Vaatamata erinevate turvalisuse nõuete saavutamise meetodite rohkusele võib ettevõtetel ja asutustel olla keeruline leida sobivat meetodit tagamaks piisav IT turvalisus.

Antud probleemi lahendamiseks võrdlesin kaht meetodit Eesti Jalgpalliliidus (EJL) läbiviidud juhtumuuringus. Security Quality Requirements Engineering (SQUARE) on laialt kasutust leidev turvalisuse nõuete tuletamise metood, mis paneb rõhku varajase disainiastme riskikaalutlustele. Security Requirements Elicitation from Business Processes (SREBP) on uus metood, mis võimaldab tuletada turvalisuse nõudeid äriprotsesside analüüsist. Tuletatud turvalisuse nõuded paigutasin võrdlevatesse kategooriatesse, mille abil sain määrata nende tõhususastme.

Uuringu tulemusena selgus, et SREBP meetodi kasutamisel saadud tulem vastas rohkem turvalisuse tagamise nõuetele. See uuring kinnitab SREBP meetodi tulemuslikkust ja usaldusväärsust.

Võtmesõnad: Infoturve, SQUARE, SREBP, turvanõuded, empiirline võrdlus.

Acknowledgment

I would like to extend my greatest thanks to my supervisor, Dr. Raimundas Matulevičius, without whom this thesis would not have seen the light of day. I thank him for his continued patience and extreme helpfulness in assisting and guiding me with the preparation of this thesis. The Estonian Football Association and Tõnu Sirel have my thanks as well for working with me and providing me with the information and support needed for the case study.
I would also like to thank my family for supporting me and last, but not least, I would like thank Risa Kolk for her continued support throughout the entire time I spent writing this thesis.

Table of Contents

Abbreviations:

SREBP – Security Requirements Elicitation from Business Processes

SQUARE – Security Quality Requirements Engineering

BPMN – Business Process Modelling and Notation

RBAC – Role-Based Access Control

ERIS- Electronic Registration Information System

SQL – Structured Query Language

xPath – XML Path Language

EFA – Estonian Football Association (*Estonian: Eesti Jalgpalli Liit*)

CIA- Confidentiality, Integrity, Availability

ISSRM – Information System Risk Management

BA- Business Asset

IS- Information System

1 Introduction

Security Engineering and Requirements Engineering have become integral features of enterprise operations over the last decade. Security engineering is an engineering discipline, the aim of which is to lower the risk of intentional and unauthorized harm to stakeholder's assets to an acceptable level. This is done through preventing, detecting or reacting to such harm (Firesmith, 2007). Requirements engineering, a field closely related to security engineering, is an engineering discipline concerned with identifying, analyzing, specifying, managing, reusing and validating goals and requirements including security related requirements (Firesmith, 2007). These are vital to ensure that a business is able to complete projects on time and within budget constraints as the failure to properly carry out security and requirements engineering bears the risk of incurring additional development costs to rectify the mistakes made during development (Mead *et al.* 2005). As a result, security requirements engineering is carried out for both projects in the design phase and ongoing processes. It is important to integrate security engineering as early as possible into the project design phase as carrying out any changes to the design of the system or implementing new features is costly both in terms of time and resources. However, security engineering should also be carried out on processes and projects which have already been implemented in order to lower the risk of harm to the stakeholders' assets.

A number of different approaches (Demirörs *et al,* 2003; Backes *et al*, 2003; Hermann *et al*, 2011; Mead *et al.* 2005) exist to allow security engineers and business analysts to carry out security and requirements engineering, however these approaches are generally not applicable to the needs of all enterprises. Examples of the shortfalls of these methods include the lack of a systematic approach to security requirements elicitation (Hermann *et al*, 2011); (Backes *et al*, 2003) and the lack of a graphical or model based representation for requirements elicitation (Demirörs *et al,* 2003). Despite a large number of different security requirements elicitation techniques, organizations struggle to find the most suitable security requirements elicitation method that would produce security requirements with the most complete coverage.

Two potential solutions exist that address this issue. The first is Security Requirements Elicitation from Business Processes (SREBP, Ahmed, 2015) developed at the University of Tartu to address the issues mentioned above. SREBP allows for the elicitation of security requirements from business process models. This method addresses a number of the shortcomings that plague other approaches such as the lack of a systematic approach to requirements elicitation and the lack of a graphical representation for requirements elicitation by directly eliciting security objectives from the business processes and then systematically eliciting security requirements from the operational business processes (Ahmed, 2015).

The other potential solution to these issues is Security Quality Requirements Engineering (SQUARE) (Mead *et al.* 2005). The SQUARE method is a systematic, yet flexible nine-step method to elicit security requirements. SQUARE does not specify an exact technique for requirements elicitation; instead it allows the security engineer to choose a suitable technique for it themselves as a means of eliminating some of the shortcomings of other security requirements elicitation methods described previously.

Therefore, to find a solution to the underlying problems described above, this thesis aims to compare the two abovementioned methods to answer the following research question:

Research Question: Which security requirements elicitation method, SQUARE or SREBP, helps to identify a more complete list of security requirements?

To answer this research question, an empirical comparison of the coverage of the security requirements elicited with SQUARE and SREBP is carried out. The basis for the empirical comparison is the case study based on the Estonian Football Association (EFA).

The empirical comparison of the security requirements is carried out by applying a method developed in Ahmed and Matulevicius (2015). The security requirements are compared in terms of their completeness of coverage of confidentiality, integrity and availability in eight different categories (Ahmed and Matulevicius, 2015). For each category, the completeness of coverage can range from 0%, if the security requirements do not provide any coverage, to 100%, if the security requirements provide full coverage. The aggregated results are compiled together to determine the overall completeness of coverage provided by the security requirements elicited with both SQUARE and SREBP.

This thesis contributes to the existing research in the security engineering domain by providing an empirical analysis of two security requirements elicitation methods SREBP and SQUARE. SREBP has only been applied to one other case study based on a different organization. The case study examined in this thesis is based on the EFA, which did not have security solutions in place and did not have business processes modeled unlike the organization examined in the other case study. Despite these differences, the findings of this thesis are in line with previous work, thus contributing to reinforcing the validity of SREBP.

This thesis is divided into 7 chapters and the appendix. Chapter 1 covers the introduction, research question and main overview of the paper. Chapter 2 provides an overview of Security Engineering, Business Process Management and Security Requirements Engineering as background concepts of the field of study. Chapter 3 provides the overview of the two methods, SQUARE and SREBP along with a theoretical comparison of the two methods. Chapter 4 describes the research question and explains the design of the empirical study. Chapter 5 presents the application of SREBP and SQUARE as the empirical study of this thesis. Chapter 6 presents the outcome of the comparative analysis of the two methods along with the answer to the research question. Chapter 7 states the conclusions of the thesis with recommendations for areas for further study.

2 Background Information

Security Engineering is recognized to be critically important in any business project that aims to be successful. It helps save a significant amount of money during the development and contributes to the overall success chance of the project (Mead *et al,* 2005). This thesis is to contribute to the literature in such area of study. As background knowledge, this chapter explains the basic concepts in the Security Engineering domain and explains its connection to Business Process Management. Additionally, the different methods used for security requirements elicitation in the Security Engineering domain are listed. The shortcomings and issues that these methods face are covered as well. Two potential solutions to these problems are briefly mentioned. Lastly, an overview of the ISSRM Domain model is given to explain how the results of the security requirements elicitation are standardized.

2.1 Security Engineering and Business Process Management

Security engineering is an engineering discipline that is concerned with lowering the risk of intentional malicious harm to valuable assets through reacting to threats and security risks and implementing security measures (Andersen, 2001). It is a multifaceted discipline that makes use of a large variety of different methodological approaches and tools. These tools differ from each other in terms of their application and the results they produce.

An important facet of the Security Engineering domain is Business Process Management (BPM). It is a systematic and continuous approach to improving a company's workflow, marketing, management and other important aspects of a company's operations (Zairi, 1997). BPM can be used to link security concerns to business goals through the use of specific methods and business process modeling languages. One of these languages is Business Process Management and Notation (BPMN). BPMN provides graphical notations to describe the various steps in a business process using signifiers for events, actors, activities, artifacts, resources and their relations. The current version of BPMN being used is Version 2.0, released in 2011. In order to tackle security issues using BPM, an understanding of what constitutes a business processes must be achieved. According to the Workflow Management Coalition, a global organization consisting of individuals and organizations engaged in Business process management, a business process is "*a set of one or more linked procedures or activities which collectively realise a business objective or policy goal, normally within the context of an organisational structure defining functional roles and relationships*" (WMC, 1999). Business process based security requirements elicitation enables the elicitation of security requirements which are in-line with the organization's business goals.

2.2 Security Requirements Elicitation

One of the methods used within Security Engineering, utilizing BPM, is requirements engineering. Requirements engineering is an engineering discipline concerned with identifying, analyzing, specifying, managing, reusing and validating goals and requirements including security related requirements (Firesmith, 2007). Security requirements engineering is a subset of requirements engineering that focuses almost exclusively on security related requirements. A number of different methods exist for security requirements elicitation within the domain of Security Engineering. Ranging from multilateral approaches such as Multilateral Security Requirements Analysis (MSRA, Gürses *et al,* 2006) and SQUARE (Mead *et al,* 2005) to UML based approaches such as Misuse cases (Sindre *et al*, 2001), SecureUML (Lodderstedt *et al*, 2002) and UMLsec (Jürjens, 2003) and Goal based approaches such as Secure Tropos (Bresciani *et al,* 2004) and Knowledge Acquisition in Automated Specification (KAOS) (Bertrand *et al*, 1998).

In addition to the methods described above, there exist specific methods for security requirements elicitation, that use business processes as their basis. In Demirörs *et al* (2003) business processes are taken as the baseline from which security requirements are elicited. However security related concepts are not mentioned and no graphical notation of the security requirements elicitation is used, thus hampering the usefulness of the method. Another method is presented in Backes *et al* (2003) in which business process models are used as a baseline to implement cryptographic solutions to satisfy security requirements. However this process fails to explain how the security requirements themselves are elicited. A more thorough example of a business process based security requirements elicitation technique is presented in Hermann *et al* (2011). This method explains security domain concepts, business goals, controls and prioritization of requirements. However, it does not present a structured, systematic method to elicit security requirements. The drawbacks of the examples described illustrate the difficulties organizations face when trying to choose the security requirements elicitation method that would provide the most complete coverage.

As mentioned above, a number of shortcomings plague the security requirements elicitation methods which use business processes as their basis. There exist two potential solutions which can address these shortcomings. One of these solutions is SREBP, a novel security requirements elicitation technique which focuses on utilizing business processes to systematically elicit security requirements (Ahmed, 2015). The other potential solution is SQUARE, which offers a nine-step process for eliciting security requirements (Mead *et al*, 2005). These two approaches are explored in more detail in the subsequent chapter.

2.3 ISSRM Domain model

The ISSRM domain model presents commonly found concepts of the security risk domain based on the analysis of different IT security standards, security risk management methods and software engineering frameworks (Mayer *et al* 2007). These concepts and their relations are shown in Figure 1 as the ISSRM domain model which combines three concepts for its risk management approach: asset-related, risk-related and risk treatment-related concepts (Dubois *et al,* 2010).

Asset-related concept covers the definition of business and Information System (IS) assets and security criterion. Business assets are immaterial assets that bring value to the company, IS assets are material information system related assets that support the business assets. Security criterion refers to the security needs of the business assets based on Confidentiality, Integrity and Availability (CIA).

Risk-related concepts cover risk and its constituent parts such as threats, vulnerabilities, threat agents, events, impacts and attack methods (Dubois *et al,* 2010). Risk treatment-related concept covers risk mitigation. In this thesis, the author has used his discretion to choose the most appropriate security requirements based on the feasibility of the application for potential controls (Dubois *et al,* 2010).

The author utilizes the ISSRM domain model (Dubois *et al,* 2010) as the methodological framework to standardize the application of SREBP and SQUARE to make the results more comparable. SREBP utilizes the concepts outlined in the ISSRM domain model whereas SQUARE does not (Ahmed, 2015);(Mead *et al*, 2005). However for the purpose of this empirical study, the author utilizes the ISSRM domain model approach for security requirements elicitation within SQUARE to ensure that the elicited security requirements have comparability with security requirements elicited through SREBP.

Figure 1 illustrates the ISSRM Domain model and the relationships between the different concepts. To distinguish between the different conceptual areas, different colours are used to represent them.

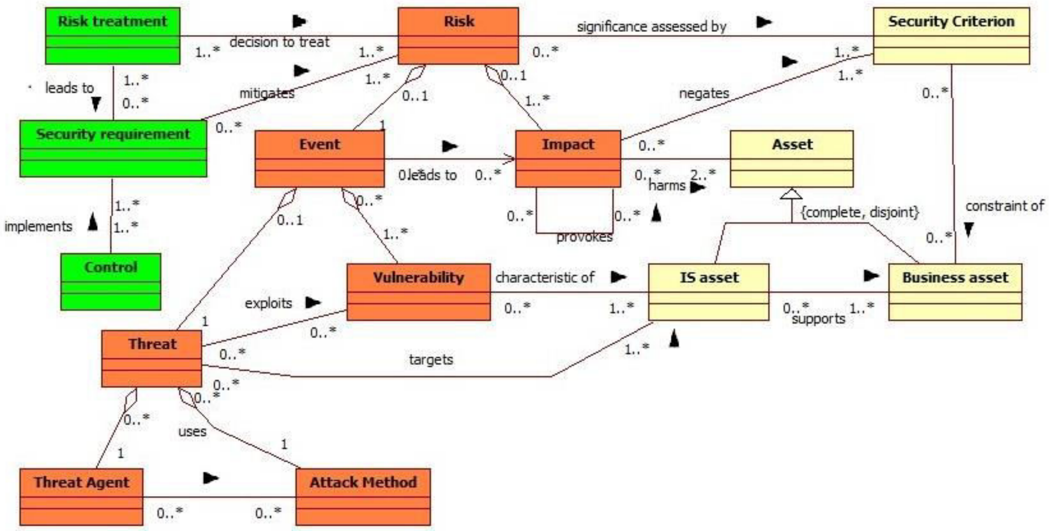


Figure 1: ISSRM model, adapted from (Dubois *et al*, 2010)

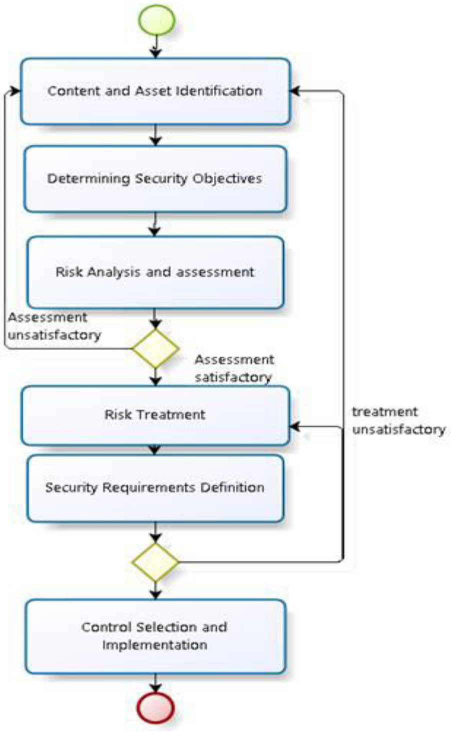

Content and Asset Identification
Determining Security Objectives
Risk Analysis and assessment
Assessment unsatisfactory
Assessment satisfactory
Risk Treatment
treatment unsatisfactory
Security Requirements Definition
Control Selection and Implementation

Figure 2: ISSRM 6-step process, adapted from (Mayer *et al* 2007)

Figure 2 presents the process integrated into ISSRM for risk management. These general steps are integrated into a number of risk management approaches such as OCTAVE (Alberts *et al,* 1999) SQUARE (Mead *et al,* 2005) and CORAS (Braber *et al,* 2007).

2.4 Summary

In this chapter, the various security engineering related concepts, such as BPM, Business processes, Security Requirements Engineering and ISSRM, were explained to provide background information regarding the security engineering domain. This revealed that there are certain problems with security requirements elicitation methods. The next chapter gives an in-depth look at two possible solutions to these problems, SQUARE and SREBP.

3 Approaches for Security Requirements Elicitation

In the previous chapter, SQUARE and SREBP were presented as the potential solutions for the problems present in the Security Engineering domain. In this chapter, the author introduces these two methods in detail and presents a theoretical comparison of both methods.

3.1 Security Quality Requirements Engineering (SQUARE) method

Security Quality Requirements Engineering (Mead *et al*, 2005) is a method to enhance the security of a product, from the early development stage in its life cycle. It has been in development for more than a decade by Nancy Mead, Donald Firesmith and Carol Woody at the Carnegie Mellon University in the United States (Mead *et al,* 2005).

The main aim of the method concerns Information Technology systems with a focus on software applications. It aims to list, categorize and prioritize security requirements for IT systems and applications (Mead *et al*, 2005). The method categorizes security requirements as non-functional, meaning that the main goal of the systems being analyzed is not necessarily about security. This allows the SQUARE method to be applied to projects which tackle the issues of security as an afterthought (Mead *et al*, 2005).

The approach consists of nine steps and facilitates the use of different approaches and techniques for artifact development, risk assessment, security requirements elicitation and filtering requirements. This means that the approach is flexible and can be used in a variety of different situations. However at the same time this also presents some drawbacks as the lack of clear guidance can lead to results that may seem disconnected or where it might be difficult to determine the exact workflow that produced these results (Mead *et al*, 2005).

In terms of validation, each step in the SQUARE process has exit criteria that must be met before the next step can begin. Additionally, the final step deals exclusively with validation of the security requirements (Fabian *et al*, 2010).

Figure 3 displays the necessary steps for carrying out SQUARE. These steps are used to develop concrete security requirements involving the work of the project stakeholders as well as the security requirements engineers.

The initial step for the application of SQUARE method involves the stakeholders in the project and the security requirements engineers. The goal for the first step is to agree on definitions for the process. These definitions need to be agreed upon to ensure that everyone involved in the process has a clear understanding of what each term that will be used means in the context of the SQUARE process (Mead *et al*, 2005).

The following step involves the stakeholders deciding upon the initial security goals. Stakeholders from different departments may have different priorities, hence it is important to agree on which issues need to be tackled first (Mead *et al*, 2005). The security goals should not hamper the operation of the system itself. The goals also need to be prioritized. A business goal and a number of security goals must be produced by the end of step 2.

3.1.1 SQUARE steps

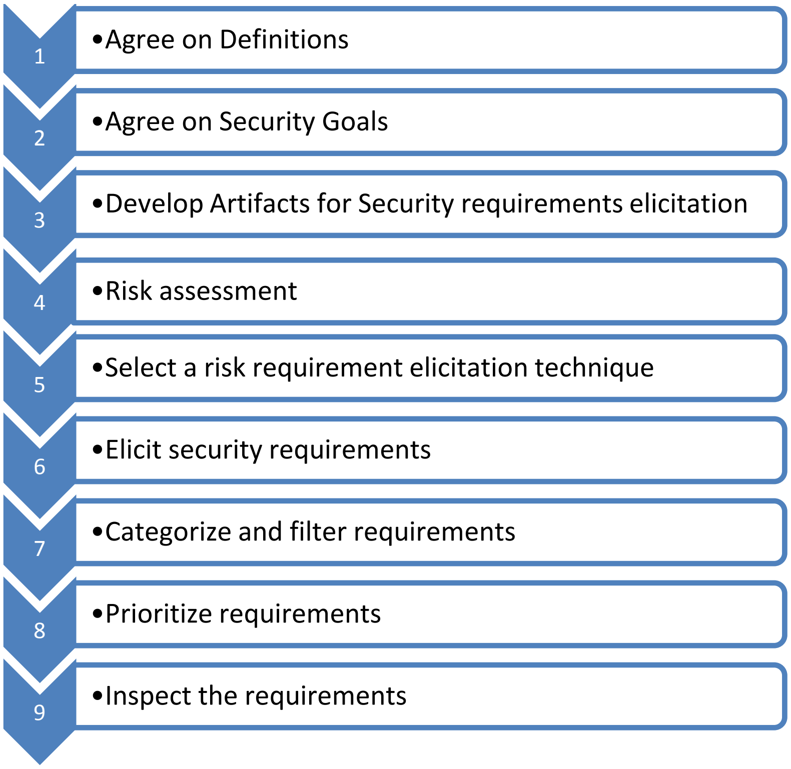

1
•Agree on Definitions
2
•Agree on Security Goals
3
•Develop Artifacts for Security requirements elicitation
4
•Risk assessment
5
•Select a risk requirement elicitation technique
6
•Elicit security requirements
7
•Categorize and filter requirements
8
•Prioritize requirements
9
•Inspect the requirements

Figure 3: SQUARE steps adapted from (Mead *et al*, 2005)

Step 3 involves developing or collecting artifacts of the system being worked on. These artifacts include misuse diagrams, goals, attack trees and other relevant diagrams (Mead *et al*, 2005). These are important as the security requirements elicitation will be based on those factors.

Step 4 is a thorough risk analysis. This should cover all the vulnerabilities along with a classification of all threats and their likelihoods as well. These results will have to be shared with the stakeholders as well (Mead *et al*, 2005). No specific method for carrying out the risk assessment is provided in SQUARE, instead the security requirements engineers will have to choose one at their discretion based on the project at hand.

Step 5 covers the selection of the most appropriate security requirements elicitation technique. The decision of choosing a particular technique must be based on the specifics of the company or the project being worked on.

Step 6, security requirements elicitation is arguably the most important step in the SQUARE method. Security requirements engineers will have to elicit concrete security requirements based on the results of the previous steps. These requirements will have to be concise and easily verifiable (Mead *et al*, 2005).

Step 7 concerns the categorization of the requirements. Security engineers will have to work together with the stakeholders to determine the appropriate categories for the security requirements. Additionally, requirements that will result in architectural constraints should be separated (Mead *et al*, 2005).

Step 8 is the prioritization of the security requirements. Stakeholders will have to decide which security requirements are the most vital. The requirements engineering team can additionally produce a cost effectiveness study to aid the stakeholders. (Mead *et al*, 2005)

The last step is the requirements inspection. In this step, the requirements which have been produced through the previous SQUARE steps will be scrutinized to ensure that each requirement is valid and verifiable. Each of the requirements should be financially feasible for implementation as well (Mead *et al*, 2005).

3.1.2 Previous Implementations of SQUARE

SQUARE has been implemented in a number of cases previously. Not all implementations of SQUARE make use of the nine steps laid out previously (Chen *et al,* 2004). This will also be the case in this study. This is due to the fact that some of the steps in SQUARE do not have a comparable equivalent in SREBP, thus a comparison between the two in this regard is not possible. Another example of SQUARE application is the development of SQUARE-Lite (Gayash *et al,* 2008). From these examples, it can be observed, that SQUARE steps can be omitted or combined when the approach is being implemented.

3.2 Security Requirement Elicitation from Business Processes (SREBP)

The SREBP method involves the identification of business assets and security objectives based on the business Value Chain (Ahmed and Matulevicius, 2014b). This is followed by the security requirements elicitation stage comprising of five steps. The SREBP method seeks to address many of the shortcomings of current security requirements elicitation methods using business processes. Security requirements elicitation is usually done haphazardly, which can result in critical requirements not being elicited. Other methods focus on particular contextual areas of business processes (access control, separation of duties) without exploring the overall security of the business processes. These methods often specify requirements in the context of security architectural design while not explaining the rationale behind the trade-offs of the security decisions (Ahmed and Matulevicius, 2014b). The SREBP method aims to address these shortcomings by giving a description of the overall security goals while focusing on the security requirements elicitation based on business processes.

3.2.1 SREBP stages

The initial stage in the SREBP method involves gathering information pertaining to the enterprise's value system which includes features such as the Value Chain and the business functions (Ahmed, 2015). The Value Chain displays the main business functions of the enterprise and shows how they are connected. Analysis of the Value Chain is vital in determining which business assets must be protected against security risks. Additionally, BPMN models are used to provide further details needed for the security requirements elicitation. After the identification of the business assets, the security objectives can be determined. This usually pertains to the protection of the Confidentiality, Integrity and Availability (CIA) of the business assets. The SREBP stages of implementation are presented in Figure 4.

The second stage involves the security requirements elicitation itself. The security requirements are elicited in five different contextual areas (Ahmed, 2015). These five contextual areas are derived from previous work covered by the authors of the SREBP method (Alter, 2006). SREBP offers a targeted and systematic analysis of the system's contextual areas in order to elicit security requirements. Other security requirement elicitation techniques that use business processes mainly focus on the graphical representation of security requirements, not on the actual requirements elicitation as explained in section 2.2.

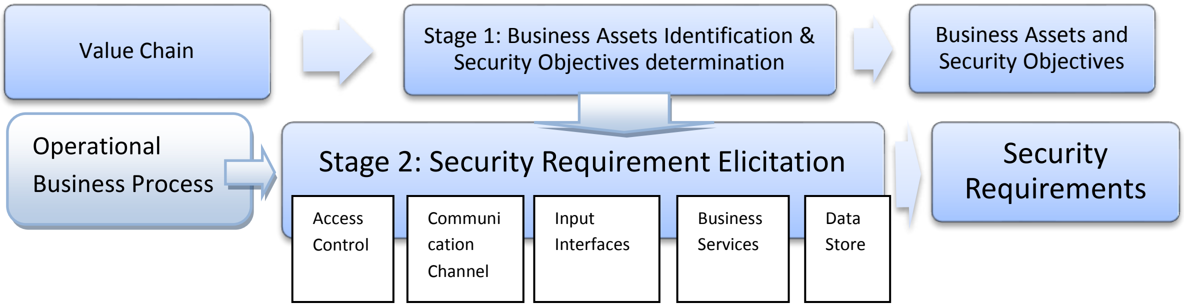

Value Chain
Stage 1: Business Assets Identification & Security Objectives determination
Business Assets and Security Objectives
Operational Business Process
Stage 2: Security Requirement Elicitation
Access Control
Communi cation Channel
Input Interfaces
Business Services
Data Store
Security Requirements

Figure 4: SREBP Security Requirements Elicitation Method adapted from (Ahmed et *al,* 2014)

SREBP also covers the development of security objectives and the conversion of these objectives into concrete security requirements. The five contextual areas for analysis in SREBP are:

- *Access control* – covers internal and external concerns in relation to access control policies that pertain to assignment of roles, which operations they are allowed to carry out in relation to the protected assets. The major aim is to protect the confidentiality of the identified business assets. The authors of SREBP have opted to use the Role-Based Access Control (RBAC) model to illustrate this step of the security requirements elicitation.
- *Communication channel* – covers data exchange between different entities. This entails the transmission of data over external networks such as the internet. If communications between two entities are compromised then there is a risk of misuse of the captured data.
- *Input interfaces* – covers how input data is treated before processing. The availability and integrity of activities that follow the input interface must be preserved as the threat agent may inject malicious scripts into the submission fields.
- *Network infrastructure* – covers the infrastructure of the network where business operations are carried out, also includes protection of business service availability. This concerns activities or tasks which are executed within the enterprise on behalf of the business partners.
- *Data store* – covers data protection in terms of storage and retrieving the data. This also covers the associated databases. If a threat agent is capable of accessing and retrieving the data, the confidentiality and integrity of the data can be compromised.

Each of these contextual areas is examined using a security risk oriented pattern (Ahmed and Matulevicius, 2015).

3.2.2 Security Patterns

Security patterns are particular reoccurring security problems that arise in specific context and provide a generic scheme for developing security solutions (Schumacher *et al*, 2006). These security patterns were further developed into security risk-oriented patterns which allow for business processes to be aligned with security requirements (Ahmed and Matulevicius, 2014a). For the application of the SREBP method, five security risk-oriented patterns outlined in Ahmed and Matulevicius, (2014a) are utilized, these were developed by the authors of SREBP. These patterns were developed by developing a template and identifying the context in which the security risk-oriented patterns would be used in. The context outlined in Alter (2006) is transformed into the five contextual areas described above, for each contextual area; one security risk-oriented pattern is utilized. An example of a security risk-oriented pattern is SRP 1, which has to secure the data transmitted between business entities (Ahmed, 2015). Data transmitted between the client and the business could be intercepted by a hostile party, thus violating the integrity and confidentiality of the data. SRP 1 therefore introduces the security requirement of making data unreadable and to verify the received data (Ahmed, 2015).

3.2.3 Previous Implementations of SREBP

At the time of writing of this paper, the SREBP method has only been applied on one case study. The Estonian Genome Centre was chosen as the case study and the implementation carried out produced a comprehensive set of security requirements (Ahmed, 2015). The referred paper also detailed a comparison between SREBP and SQUARE, both having been applied to the same case study. To compare both methods, the author had decided to compare the completeness of security requirements. To do that, several categories were elicited and each security requirement was categorized and analyzed. The study showed, that on average, the security requirements elicited via SREBP provided a 80% coverage whereas the security requirements elicited via SQUARE only provided a 36% coverage. That study concluded that SREBP provided better coverage of security requirements than SQUARE (Ahmed, 2015)

3.3 Theoretical Comparison of SQUARE and SREBP

After explaining SQUARE and SREBP above, this section presents a theoretical comparison of these methods in key contextual areas to illustrate the distinct similarities and differences in the application of both methods.

Definition of concepts: SREBP utilizes the concepts presented in accordance with Information System Security Risk Management (ISSRM) Domain model (Dubois *et al,* 2010) while SQUARE fails to define assets and vulnerabilities directly (Ahmed and Matulevicius, 2014b). These concepts may be present in the first step of SQUARE, the definition of terms, but they are not integrated into the framework of the method itself (Mead *et al*, 2005)

Requirements elicitation: SQUARE does not specify which methods should be used for security requirement elicitation. In SREBP, the security requirements elicitation takes place using security risk-oriented patterns. Both methods cover the early stage of requirements elicitation. SREBP utilizes the business Value Chain and the identification of business asset to elicit early security requirements. SQUARE utilizes the definition of security goals and business goals and the interactions with stakeholders to determine the initial security requirements (Ahmed and Matulevicius, 2014b).

Security Risk Management: As mentioned previously, SQUARE does not restrict the selection of techniques for security risk management and this leads to a lack of a systemic approach to security risk management (Mead *et al*, 2005). This could be alleviated however if the ISSRM domain model is used for security risk management as the steps in ISSRM would act to compensate for the inherent shortcomings of SQUARE. SREBP on the other hand has compliance to ISSRM due to utilizing security risk-oriented patterns (Ahmed and Matulevicius, 2014a) in terms of security risk management.

Traceability: SREBP facilitates the traceability of the security requirements as traceability is part of one of the main goals of the method itself (Ahmed and Matulevicius, 2014b). The close links between the business assets, the Value Chain and the security requirement elicitation activities facilitates this. The SQUARE approach is more rigid, due to the ambiguity in choosing the methods for several of its constituent steps, it may be difficult to connect all the individual steps together.

Validation and Prioritization: SQUARE integrates validation and prioritization into its steps. This allows for the security engineers and the stakeholders to determine which requirements are feasible for implementation and which are not (Mead *et al*, 2005). SREBP does not yet support any validation or prioritization of the elicited security requirements (Ahmed. 2015)

Security Requirement Reusability: SQUARE does not place restrictions on which method should be used for requirements elicitation. As a result, the reusability of security requirements depends entirely upon which requirements elicitation method is chosen by the security engineer (Mead *et al*, 2014). SREBP does not have any security requirement reusability set up either (Ahmed, 2015). This is something that can be improved in future implementations of SREBP.

Compatibility with the ISSRM process: As described in the background chapter, the ISSRM process exemplifies the common steps that are integrated into many risk management processes. Both SQUARE and SREBP incorporate some if not all of the steps.

1. Content and asset identification - SQUARE does not explicitly incorporate this step in its process, however in this thesis the ISSRM domain model is used as a baseline for the risk management step and thus this step is identified there. SREBP incorporates the content and asset identification as the first stage of the method.

2. Determining security objectives – SQUARE incorporates this step as stage 2 of the SQUARE method. In SREBP, this is incorporated into the first stage of the method.
3. Risk Analysis and Assessment – This step is incorporated into the SQUARE method as step 4. As mentioned above, SQUARE does not explicitly state which technique should be used for this. In SREBP, this step is covered by the use of security risk-oriented patterns which represent the recurring risks.
4. Risk Treatment – Neither SQUARE nor SREBP explicitly define this step. For SQUARE, it depends on which risk management technique is used, for SREBP, it is assumed that all risks in the form of security risk-oriented patterns will be mitigated.
5. Security Requirements definition – SQUARE integrates this as step 6 of its method, but does not specify the technique that should be used for this. In SREBP this is integrated into the method as stage 2.
6. Control Selection and Implementation – This step is missing in both SQUARE and SREBP, however this step can be followed with SQUARE if a technique for risk management is used as part of steps 4 and 6 of the SQUARE method.

3.4 Summary

Chapter 3 presented SQUARE and SREBP in detail as the potential solutions to the problems in the Security Engineering domain mentioned in the previous chapter. To illustrate the similarities and differences between the two methods, a theoretical comparison was also introduced to this chapter. The next chapter explains how the methods will be applied and eventually compared to each other.

4 Methodology

As mentioned in the previous chapter, SQUARE and SREBP could be the potential solutions for the existing problems in the security requirements elicitation domain. Therefore, in this thesis, the author is going to compare these two methods by applying both of them to the case study of the EFA to examine which method can address such problems more effectively. In this chapter, the research question to be examined in the empirical analysis is explained together with a brief overview of EFA. Secondly, the ISSRM domain model will be explained as the methodological framework to standardize the results of the application of the two methods. Subsequently a detailed explanation of the design of the empirical study will be presented. Lastly, the Value Chain and an example of the Operational Business Processes will be presented to represent the input used for the application of the two methods in the following chapter.

4.1 Research Question and Case Description

Research Question

In this thesis, the following research question will be examined to compare the two potential solutions to the issues at stake:

RQ: Which security requirements elicitation method, SQUARE or SREBP, helps to identify a more complete list of security requirements?

To answer this research question, the author applies the two methods to one case study. The completeness of the security requirements will be compared with regard to the percentage of the coverage provided by the two methods. As mentioned above, the EFA is chosen as the basis for the cases study.

To gather information about the EFA, interviews with a senior-level employee of the EFA were conducted. The interviews were carried out face to face in a semi-structured format with the Director-General of the EFA. The interview period ranged from October 2013 to May 2014. Each session lasted from 30 minutes to 2 hours. During the interviews it was determined that due to the organizational specifics of the EFA, namely their heavy reliance on a single information management system, that the application of the security requirements elicitation methods will be carried out on the utilization of that information management system.

Case Description

The Estonian Football Association (EFA) is a non-governmental organization that oversees the organization of national leagues and games within Estonia and also interacts with international organizations such as FIFA and UEFA for international co-operation when organizing football games. They also manage the databases for players, umpires and coaches in Estonia.

Structure of the organization: The Estonian Football Association is a small organization, employing approximately 30 personnel. The employees work in one office located in Tallinn.

IT system: The organization relies heavily on IT systems for their daily operations. The backbone of the system is an information management system called ERIS (Electronic Registration Information System). The system is a custom designed platform which allows for managing different databases (player database, team database etc.) as well as for publishing information to the association's public website. ERIS can only be accessed within the office from the local area network. VPN access for the system does exist, but this is only available to the company which designed the system and which performs maintenance and monthly backups of the databases.

External access to the ERIS is also supported in limited form to allow team representatives and umpires to modify their team entries and fill in match reports respectively. Authentication for the umpires and team representatives is carried out using the Estonian national ID card authentication.
Office staff use employer provided laptops running Windows XP. Staff's personal computers cannot connect to the local network and office laptops are to remain in the office at all times. The association also has a public website which is hosted elsewhere.

Security: The Estonian Football Association currently does not have any IT security policies in place and the overall security awareness is limited among the employees. One IT specialist is on site every day to deal with any issues that the employees may have. The association experienced targeted cyber attacks in 2005 aimed at trying to access player information in the database. As a result, the protection of personal information is considered a priority (Interview with *EFA* Director General).

4.2 Design of the Empirical Study

In the previous sections, the research goal and the description of the case were presented along with a description of how the ISSRM domain model is used as the methodological framework to standardize the results of the security requirements elicitation. Subsequently this section aims to explain in detail how the previously described aspects are brought together in the empirical study.

Figure 5 illustrates how the research question is answered in this thesis. Firstly the author examined the different methods in the Security Engineering domain to identify specific problems. From relevant literature, it was determined that two potential solutions exist to this problem. In light of this, the research question was developed and it was determined that an empirical comparison of the two methods should be carried out to determine which method provides a better solution to the problem. The methods, SQUARE and SREBP, are applied to EFA case study to elicit security requirements. In order to answer the research question, the security requirements are then compared using comparison criteria to determine which method produced a more complete set of security requirements.

4.4 Value Chain and Business Process Models of the EFA

To carry out the empirical study and the application of the security requirements methods described in the previous section, the Value Chain and Business Process models of the EFA are used as the inputs. These models were elicited based on the information gathered from the interviews with the EFA. The Director-General of the EFA was consulted throughout the development of these models to ensure their accuracy. For the purposes of this empirical study, no security solutions were modeled.

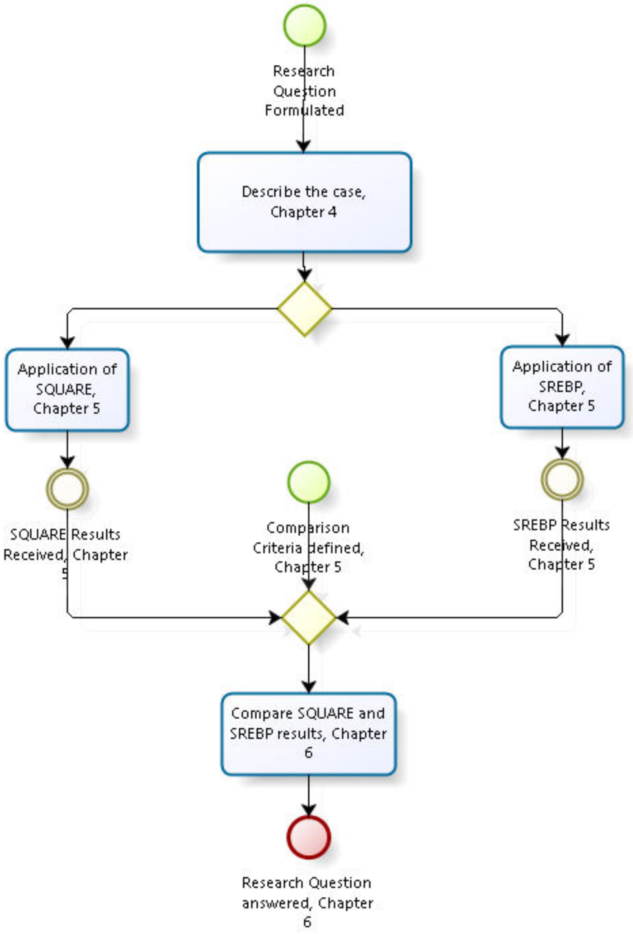

Research Question Formulated
Describe the case, Chapter 4
Application of SQUARE, Chapter 5
Application of SREBP, Chapter 5
SQUARE Results Received, Chapter 5
Comparison Criteria defined, Chapter 5
SREBP Results Received, Chapter 5
Compare SQUARE and SREBP results, Chapter 6
Research Question answered, Chapter 6

Figure 5: Design of the Empirical Study

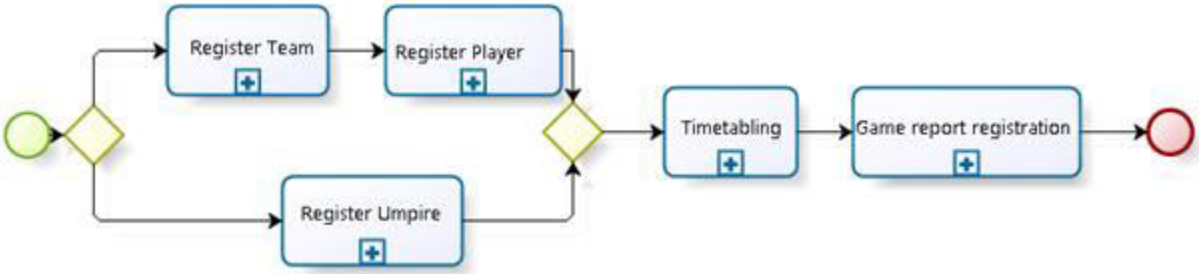


Figure 6: Value Chain of the EFA

Figure 6 presents the Value Chain of the EFA, listing business processes that bring value to the organization. The value chain process starts with the Register Team, to register a new team with the EFA, and Register Umpire, to register a new umpire with the EFA, processes starting in parallel. Once the team has been registered, the Register Player process can be started in which a player is able to register themselves with the EFA as part of the team. Once teams, players and umpires have registered, the Timetabling process starts to elicit a timetable for assigning teams and umpires to different games. Once the games have taken place, the game reports are registered in the Game report registration process.

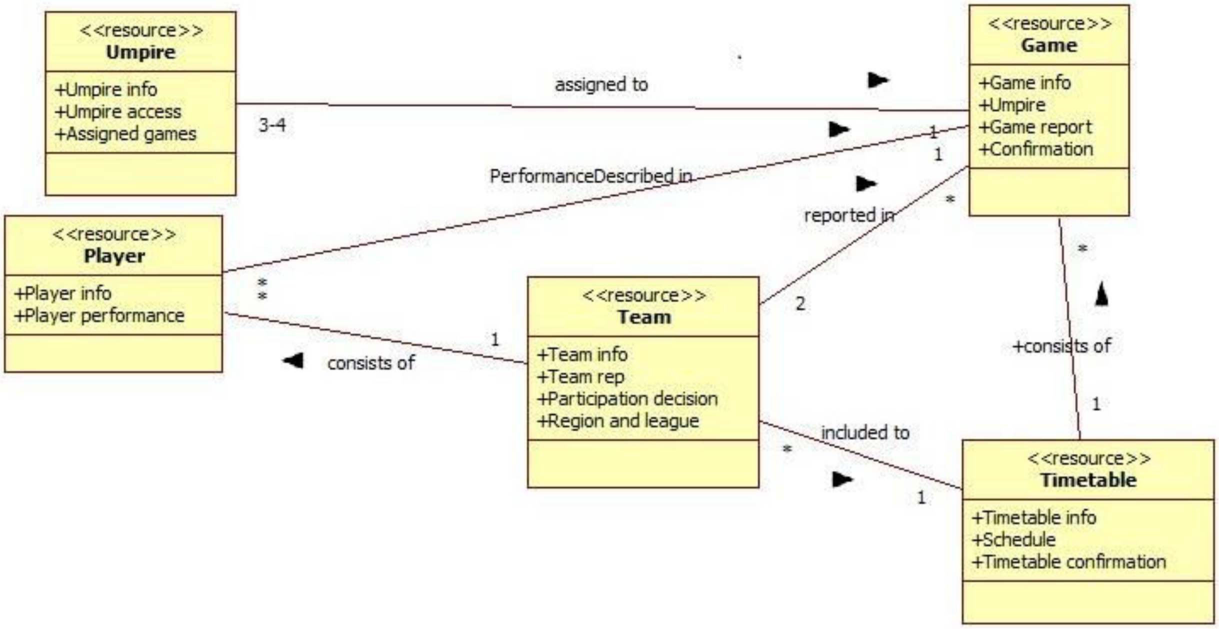


Figure 7: Business assets and their attributes

Figure 7 presents the Business assets derived from each of the processes in the value chain. Each asset also has their attributes listed; these were derived from the operational business process models. Each of these processes was elaborated in more detail, an example of this is shown in Figure 8 based on the

Register Team business process. The rest of the business process models of the EFA are in the Appendix, section A1.

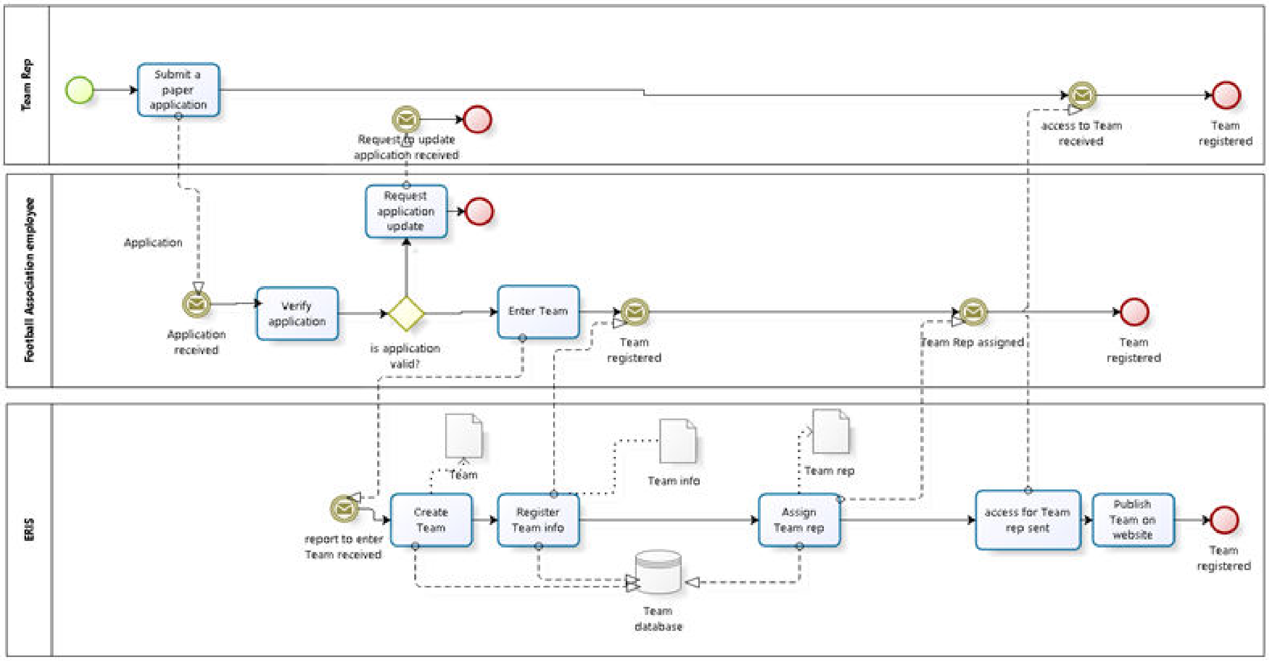


Figure 8: Register Team Operational Business Process model

In Figure 8, the Team representative and the EFA employee are represented as swimlanes, the same is the case with the information system, ERIS. The Register Team process starts with the Team Rep submitting a paper application to register a new team. This application is received by the EFA employee who then verifies the validity of the application. If the application is not valid, it is sent back to the Team Rep for review. Once the application has been accepted, a new Team is created in ERIS by the EFA employee. ERIS receives the request to create a new entry and does so. The new Team entry is saved in the Team database. The Team info, inputted by the EFA employee when creating the new Team, is saved in the newly created Team data file. A notification is sent to the EFA employee once this is completed. The Team info also contained information about the Team rep, who will have access to the Team information through ERIS. ERIS creates a new entry for the Team rep and a notification is sent to the EFA employee and the Team rep. Once this process is completed, ERIS automatically publishes Team's information on the EFA website.

4.5 Summary

Chapter 4 presented the research question and the overall research design, explaining in detail how the research question would be answered using the EFA as the basis of a case study. SQUARE and SREBP would be applied to the case study and the elicited security requirements would be compared to determine their completeness of coverage. The next section gives an overview of how exactly SQUARE and SREBP were applied.

5 Empirical Study: Application of SQUARE and SREBP

This chapter conducts the application SQUARE and SREBP according to the design specifications in the previous chapter. SQUARE and SREBP are applied to the case study of the EFA to elicit security requirements. Firstly SQUARE is applied and a summary of the security requirements elicited is shown. Subsequently, SREBP is applied and the elicited security requirements are displayed. Lastly, the comparative summary of these two applications is briefly presented.

5.1 Application of SQUARE

This section covers the application of the SQUARE methodology outlined in Mead *et al* (2005). The individual steps of this application of the SQUARE method are outlined here, with the elicited security requirements listed in Appendix Section A3. The security requirements elicited using this method are further analyzed in Chapter 6. As the input for this application of SQUARE, the Value Chain and business operational models of the EFA are used.

5.1.1 Agree on Definitions

The first step in the SQUARE process is agreeing upon the definitions that will be used for the subsequent steps. For this step, the contribution of both the security engineers and the stakeholders is required. In this case, the author of the paper and an executive member of the EFA discussed the definitions.

Output: The stakeholders relied on the discretion of the author of the thesis to choose the appropriate definitions. As a result, the along with the concepts and terms presented with ISSRM were chosen. Examples of the definitions adapted from ISSRM are presented according to Dubois *et al,* (2010). *Threat*- A potential attack, carried out by a threat agent that targets one or more IS assets and may lead to harm to those assets. It is constituted of a threat agent and an attack method. *Threat agent*- An actor that can potentially harm the IS. Constitutes a threat when combined with an attack method. *Vulnerability* - A characteristic of the IS asset that constitutes a weakness or a flaw. *Risk* - The combination of a threat and one or more vulnerabilities that can lead to a negative impact that harms the assets. *Asset* - Anything that has value to the organization in terms of achieving its objectives.

5.1.2 Identify Business and Security Goals

The second SQUARE step is the definition of security and business goals. The goals were initially presented by an executive member of the Estonian Football Association and were elaborated to ensure their applicability in the context of security requirements elicitation. For example, the goal of ensuring ‘fair play’ was transformed to two security goals: monitoring and integrity.

Output: The following business goal and security goals were elicited:

Business goal: Organizing national football championship and champions cup games.

Security goal 1.Confidentiality: Only authorized persons can access sensitive information stored in the databases. Much of the data in these databases is personal information of the players.

Security goal 2.Integrity: Only authorized persons are allowed to modify any data on the information system. This is vital to determine that no foul play is at hand and this is aligned with the 'fair play' principles.

Security goal 3.Availability: The data and services should be available at all times.

*Security goal 4.Monitoring***:** User activities and access attempts should be monitored. This contributes to the Confidentiality and Integrity of the assets as monitoring enables active protection of the aforementioned criterion.

Security goal 5.Authentication: User identity must be verified before access is granted to any of the services on ERIS, especially those that interact with databases. This also contributes to the Integrity of the assets as it prevents unauthorized access to the databases.

5.1.3 Develop Artifacts

Step three of the SQUARE methodology entails the creation of various artifacts which will be used for the risk assessment and security requirements elicitation. In this application of the SQUARE method, the Value Chain and the business operational models of the EFA represent the artifacts along with the Use case and Misuse case models.

5.1.4 Perform Risk Assessment and Security Requirements Elicitation

ISSRM was chosen as the method for the risk assessment and security requirements elicitation. Section 2.3.1 covered the advantages and features of ISSRM, additionally; using ISSRM within the SQUARE process eliminates some of the shortcomings of the SQUARE methodology, namely the lack of certain definitions of terms. Using ISSRM also allows for a more objective comparison of the security requirements elicited with both methods applied in this thesis as SREBP also utilizes the ISSRM approach.

Output: Presented here are the Business Assets (BA), Information System (IS) assets and use case models and misuse case models of the first Business Asset within the context of Risk 1. The remaining use case models and risk assessments are presented in the Appendix section A3.

Table 1: Estonian Football Association Business Assets (IS focus)

ID	Business Asset	Description	Security Criterion
BA1	**Player**	Contains the player's personal information.	**CIA**
BA2	**Team**	Contains the team's information, including player names and game dates.	**CIA**
BA3	**Umpire**	Contains the Umpire's personal information.	**CIA**
BA4	**Game**	Contains all the relevant information about each game including the game report	**I**
BA5	**Timetable**	Timetable of games taking place.	**I**

Table 1 lists the business assets elicited from the EFA Value Chain. A description of each of the Business Assets is given in the table along with the relevant security criteria. These criteria were specified by the EFA. Table 2 lists the IS assets that were elicited from the operational business models along with their descriptions.

Table 2: Estonian Football Association IS assets

ID	IS Asset	Description
IS1	**ERIS**	Information system used by the EFA to manage
IS2	**Team and player database**	Database to store player and team information
IS3	**Game database**	Database to store game entries and related information
IS4	**Timetabling software**	Software used to create timetables and schedules.
IS5	**Umpires and coaches database**	Database to store information and entries about coaches and umpires

The relationship between the IS and BAs is denoted with an x in the corresponding cell in the traceability matrix Table 3. This denotes which IS assets support the corresponding BAs.

Table 3: Business assets and IS assets traceability matrix

	IS assets				
Business Asset	**IS1**	**IS2**	**IS3**	**IS4**	**IS5**
BA1	**x**	**x**			
BA2	**x**	**x**			
BA3	**x**				**x**
BA4	**x**	**x**			
BA5	**x**			**x**	

Implementation of SQUARE: Based on the information gathered in the previous steps, the security requirements elicitation process will be explained for the first business asset. In this particular case, the first BA and second BA are both stored in their respective databases in the same way, as a result, the first risks identified apply to both BAs. During the security requirements elicitation process, it became apparent that this was also the case with other business assets. Figure 9 shows the use case model for Business Assets 1 and 2. The next step in the process calls for identifying threats and threat agents, this is illustrated using misuse cases in Figure 10. Based on the misuse cases model, the ISSRM methodology is applied to elicit security requirements, an example of this is given below based on Risk 1:

Initially the BA and IS are identified as the Team and the Team database respectively. This is followed by identifying a potential Threat Agent, the Hacker, and a potential Attack Method as hacking. The Threat Agent and the Attack Method are combined to form the Threat, which is that the hacker is able to hack into the database. To do this, the hacker exploits a Vulnerability: user permissions are not checked when data is accessed. This causes the Event: Hacker hacks into the database due to user permissions not being checked when data is accessed. The Impact of this Event is that there will be a loss of confidentiality of the BA. Combining the Impact and the Event, the following Risk is identified: Hacker hacks into the database thus negating the confidentiality of the data. To mitigate this, it is necessary to implement a Security requirement: Only authorized personnel should be able to access the database. User credentials must be checked. Finally, a suggested Control to satisfy the Security requirement is the implementation of the Estonian national ID card authentication software for authorizing users to access the database.

One use case diagram can be used to identify more than one risk and therefore more than one security requirement as both of the risks shown in Table 4 and Table 5 are derived from the misuse cases diagram in Figure 10. The control and control cost were elicited through discussions with stakeholders and present potential controls to the security requirements.

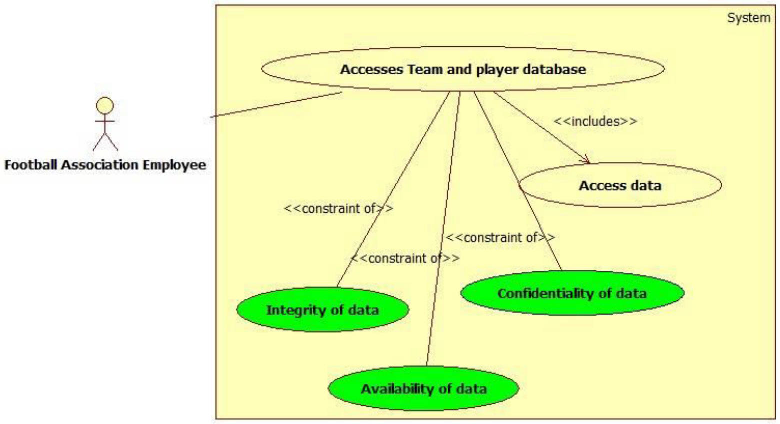


Figure 9: Use cases diagram for BA1 and BA2

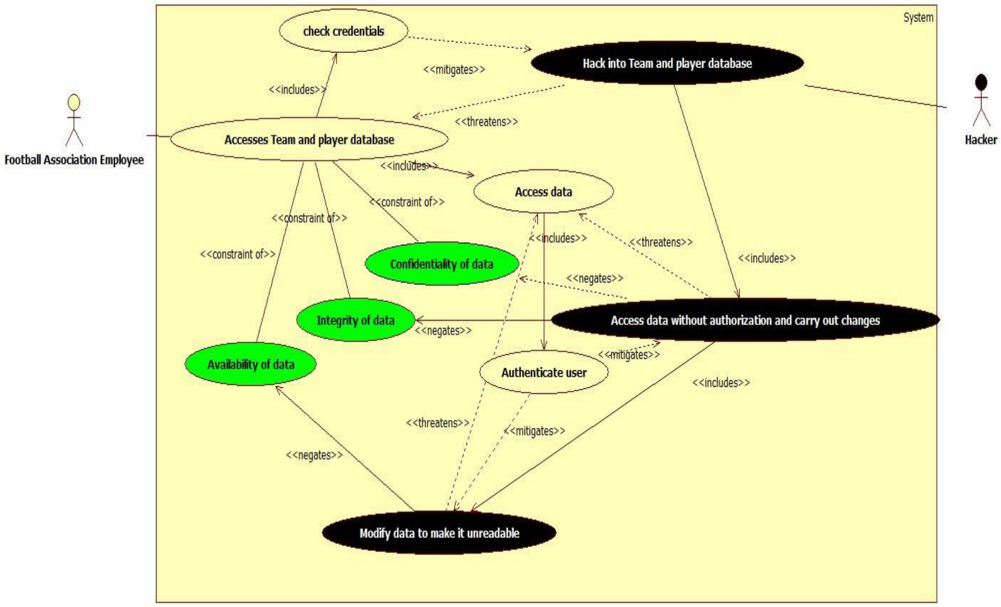


Figure 10: Misuse cases diagram for BA1 and BA2 – Hacking and unauthorized access

Table 4: Hacker accessing and modifying the Team and player database

Business asset	Player
Asset related concepts	
Risk ID	**R1**
IS Asset	**Team and player database**
Security criterion	Confidentiality of the Player's personal information.
Risk related concepts	
Risk	Hacker hacks into the database thus negating the confidentiality of the data.
Impact	Loss of confidentiality of the business asset.
Event	Hacker hacks into the database due to user permissions not being checked when data is accessed
Vulnerability	User permissions are not checked when data is accessed.
Threat agent	Hacker
Threat	Hacker is able to hack into the database
Attack method	Hacking the Team and player database
Risk Treatment related concepts	
Security requirement	Only authorized personnel should be able to access the database. User credentials must be checked
Security requirement ID	**SRQ1**
Control	Implementation of Estonian national ID card authentication software
Cost of control	**500 EUR**

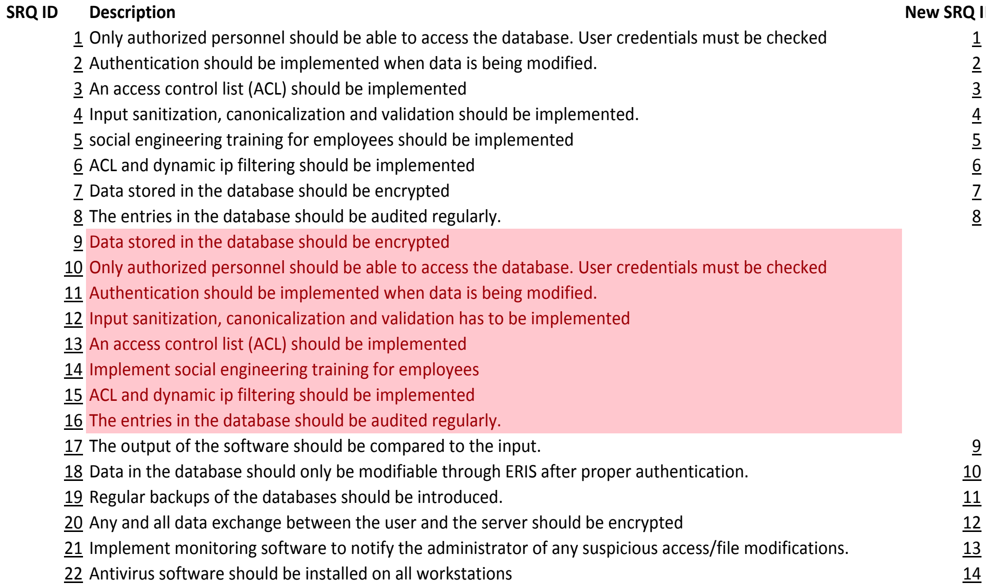
Table 5: Hacker hacks into the Team and player database to manipulate team's information.

Business asset	Player, Team
Asset related concepts	
Risk ID	**R2**
IS Asset	**Team and player Database**
Security criterion	Availability and integrity of the team's information.
Risk related concepts	
Risk	Hacker hacks into the database and changes data thus negating the availability and integrity of the data.
Impact	Loss of availability and integrity of the business asset.
Event	Hacker hacks into the database and changes the data.
Vulnerability	User permissions are not checked when data is being modified.
Threat agent	Hacker
Threat	Hacker can hack into the database and change data.
Attack method	Hacking the Team and player database
Risk Treatment related concepts	
Security requirement	Authentication should be implemented when data is being modified.
Security requirement ID	**SRQ2**
Control	Implement authentication software
Cost of control	**0-1000 EUR**

5.1.5 Results of SQUARE application

A number of security requirements were elicited using SQUARE on the EFA case study. The security requirements, identified as SRQ are shown below in Figure 11. The security requirements highlighted represent duplicate security requirements or architectural constraints and are thus not counted. The rest of the security requirements each represent general security requirements which were then applied to each BA where applicable.

Table 6 lists the breakdown of the number of security requirements applicable to each of the BAs identified using SQUARE. Table 4 lists the breakdown of the security requirements between the various Business Assets. The security requirements are listed in more detail in the Appendix, section A3



SRQ ID	Description	New SRQ I
1	Only authorized personnel should be able to access the database. User credentials must be checked	1
2	Authentication should be implemented when data is being modified.	2
3	An access control list (ACL) should be implemented	3
4	Input sanitization, canonicalization and validation should be implemented.	4
5	social engineering training for employees should be implemented	5
6	ACL and dynamic ip filtering should be implemented	6
7	Data stored in the database should be encrypted	7
8	The entries in the database should be audited regularly.	8
9	Data stored in the database should be encrypted	
10	Only authorized personnel should be able to access the database. User credentials must be checked	
11	Authentication should be implemented when data is being modified.	
12	Input sanitization, canonicalization and validation has to be implemented	
13	An access control list (ACL) should be implemented	
14	Implement social engineering training for employees	
15	ACL and dynamic ip filtering should be implemented	
16	The entries in the database should be audited regularly.	
17	The output of the software should be compared to the input.	9
18	Data in the database should only be modifiable through ERIS after proper authentication.	10
19	Regular backups of the databases should be introduced.	11
20	Any and all data exchange between the user and the server should be encrypted	12
21	Implement monitoring software to notify the administrator of any suspicious access/file modifications.	13
22	Antivirus software should be installed on all workstations	14

Figure 11 – SQUARE Security Requirements.

Table 6: SQUARE Security Requirements assigned to Business Assets

Business Asset	Security Requirements	Number of SRQ
BA1 - Player	SRQ1.1, SRQ2.1, SRQ3.1, SRQ4.1, SRQ5, SRQ6.1, SRQ7.1, SRQ8.1, SRQ10.1, SRQ11.1, SRQ12, SRQ13.1, SRQ14	13
BA2 - Team	SRQ1.2, SRQ2.2, SRQ3.2, SRQ4.2, SRQ5, SRQ6.2, SRQ7.2, SRQ8.2, SRQ10.2, SRQ11.2, SRQ12, SRQ13.2, SRQ14	13
BA3 - Umpire	SRQ1.3, SRQ2.3, SRQ3.3, SRQ4.3, SRQ5, SRQ6.3, SRQ7.3, SRQ8.3, SRQ10.3, SRQ11.3, SRQ12, SRQ13.3, SRQ14	13
BA4 - Game	SRQ1.4, SRQ2.4, SRQ3.4, SRQ4.4, SRQ5, SRQ6.4,SRQ7.4, SRQ8.4, SRQ10.4, SRQ11.4, SRQ12, SRQ13.4, SRQ14	13
BA5 - Timetable	SRQ1.5, SRQ2.5, SRQ3.5, SRQ4.5, SRQ5, SRQ6.5, SRQ7.5, SRQ8.5, SRQ9, SRQ10.5, SRQ11.5, SRQ12, SRQ13.5,SRQ14	14
Total number of security requirements:		66

5.2 Application of SREBP

This section covers the application of the SREBP method based on an example one operational business process from the case study. The Register Team business process will be used to illustrate the application of the method. The application of the SREBP method was carried out following the guidelines presented in Ahmed & Matulevičius, (2014b). The general instructions for each step are also shown in this chapter in the context of the first business asset.

5.2.1 Business Assets identification and determination of Security Objectives

Before security requirements elicitation, it is necessary to gather information about the organizational processes. The Value Chain of the EFA is used for this. The Value Chain displays the business processes which create value for the EFA and which utilize the information management system. The first step of the SREBP method is the identification of Business Assets. Accordingly, a number of Business Assets were identified from the EFA Value Chain; these are listed below. For each of the assets, their confidentiality, availability and integrity were considered as security objectives:

Team – Team registration
Player – Player registration
Umpire – Umpire registration
Timetable – Timetabling
Game – Game report registration

Each Business Asset identified consists of attributes which were elicited from the operational business models.

5.2.2 Security Requirements elicitation based on Register Team process

The second stage of the SREBP method is the security requirements elicitation. This is based on five contextual areas: access control, communication channel, input interfaces, network infrastructure and data store. These contextual areas are described in more detail in section 4.2.1.

5.2.2.1 Access control is the first contextual area for security requirement elicitation in SREBP. In the Team Registration process, the Team represents the business asset which must be protected, especially when it is manipulated by the IS asset, ERIS. An example of a threat is when the attributes of the Team such as Team info, are provided to the users without checking their access credentials. To mitigate this risk, the SREBP methodology utilizes access control mechanisms, such as Role Based Access Control (RBAC) and provides guidelines to elicit an RBAC model for security requirements elicitation. For this, the following steps must be performed:

Identifying resources: The business asset, The Team, is defined as a resource that needs to be protected in the Register Team example. The attributes of the Team business asset in the Register Team process are Team info and Team rep.

Identifying roles: The swimlanes in the operational business models represent the roles in the context of the RBAC model. In the case of the Register Team example, the Team rep and the Football Association employee are represented using the <<role>> stereotype in the RBAC model as they can both access the protected resource. ERIS is not included in the role stereotype as it is an information system through which the other two roles, Team Rep and Football Association Employee, are able to access the protected resource.

Assigning users: Roles are assigned to users, however in most cases it is not possible to elicit specific users from the operational business process.

Identifying secured operations: Operations are actions that can interact and change the state of the protected resource. In the Register Team example, these are Create Team, register Team info, assign Team rep etc. Usually, these operations are business activities from the operational business process that accesses the business resource.

Assigning permissions: Permissions are privileges given to roles that specify which operations the specified role is allowed to carry out on the protected resource. There are three categories of operations for which permissions are given, Create, Read and Update. In the Register Team example, Football Association employee can create the resource Team.

Using these steps, an RBAC model can be developed, for the Register Team example; to elicit security requirements as depicted in Figure 11. The model shows what the authorized parties are allowed to do vis-à-vis the protected resource. The RBAC model does not capture certain scenarios such as entailment constraints, delegation constraints and usage control. The assistance of business analysts and security analysts is usually needed to determine these requirements (Ahmed & Matulevičius, 2014b).

Figure 12 displays the RBAC model for the team registration process. From this model a number of security requirements can be elicited:

SRQ1: Football Association employee: should be able to: Create the Team
SRQ2: Football Association employee: should be able to: Read the Team info and Team rep.
SRQ3: Team representative should be able to: Read the Team info and Team rep.
SRQ4: Permission Access to Team received: READ should be given only to one user assigned to Team Rep. This user also receives permission Update Team info: UPDATE.

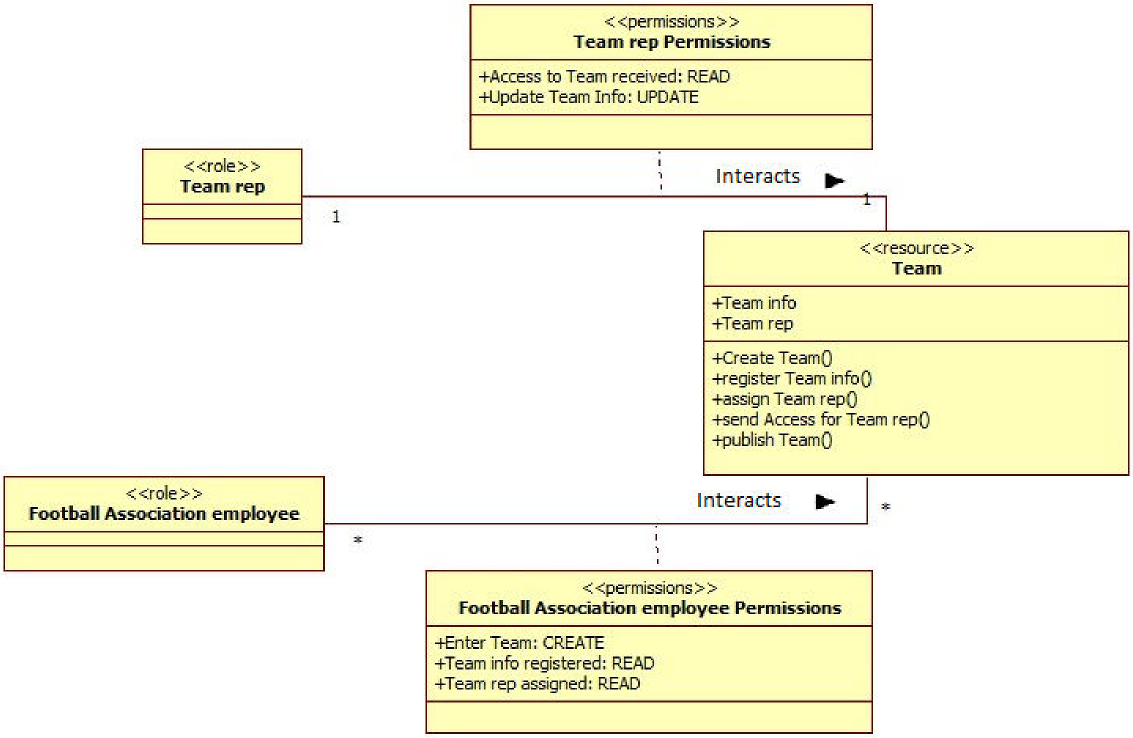


Figure 12: RBAC security model – Team registration business process

SRQ1 and SRQ 2 are elicited straight from the RBAC model, whereas RQ4 was elicited based on other considerations (Ahmed & Matulevičius, 2014b).

5.2.2.2 Communication Channel is the second contextual area used for requirements elicitation. This contextual area deals with data exchange between the business partners and the system over untrusted networks such as the internet. Keeping the data confidentiality and integrity are the main goals for this stage. In the Team Registration example, most of the processes happen within a secured local network, however when the Team Rep proceeds to Manage Team, the system is accessed externally and must be secured within this contextual area. To mitigate the potential risks, the following must be done:

Identification of communicators: It is necessary to determine which entities transmit or receive data. Using the business process model, it is possible to identify the information system used by the enterprise and the business partners that are communicated with. This is illustrated in Figure 13. In this figure, ERIS is shown to be the information system of the Football Association and the Football association Employee acts as the business partner.

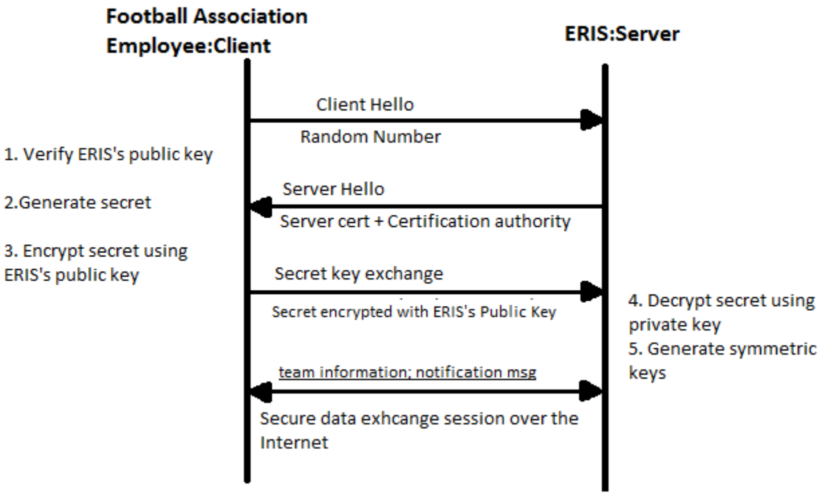

Football Association
Employee:Client
ERIS:Server
Client Hello
Random Number
1. Verify ERIS's public key
2.Generate secret
3. Encrypt secret using ERIS's public key
Server Hello
Server cert + Certification authority
Secret key exchange
Secret encrypted with ERIS's Public Key
4. Decrypt secret using private key
5. Generate symmetric keys
team information; notification msg
Secure data exhcange session over the Internet

Figure 13: TLS protocol implementation

Identifying data transmission: It is necessary to identify the relevant data (e.g. business asset) being transferred between the communicators over an untrusted communication channel such as the Internet. In the Register Team example, Team info is communicated to ERIS and thus needs to be protected.

Following these two steps, the following security requirements are elicited:

SRQ5: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority.

SRQ6: Football Association employee should encrypt and sign the Team info (and notification messages) using the keys before sending it to ERIS.

TLS or SSL protocols can be used to satisfy the security requirements. As illustrated in Figure 12, the client first sends a handshake message with a random number, the server replies with its certificate/public key and information about the certification authority. After the certificate has been confirmed by the client, they send a generated secret to the server which decrypts it with its private key and generates symmetric session keys which enable a secure data exchange session to be established (Ahmed & Matulevičius, 2014b).

5.2.2.3 Input interface is the third contextual area that is considered for requirements elicitation within SREBP. Input interfaces are used to input data that is then submitted by the business partners for example by the Team Rep. Input interfaces ensures that the data submitted by business partners is correct. To help with the security requirements elicitation in this contextual area, the following should be done:
Identifying input interfaces: Input interfaces can be determined from the operational business process by looking at incoming message flows. Input to the information system from the

business partners comprises input interfaces. Within the example of the team registration process the operations Enter Team information and Manage Team utilize input interfaces.

Identifying input data: Input data is the data received by the input interfaces from the business enterprises. Certain threats must also be considered in the context of input interfaces; malicious scripts can be submitted by threat agents (SSL injections, xpath injections etc.) which would compromise the integrity, availability of any further activities following the use of the input interfaces (Ahmed & Matulevičius, 2014b). Following the two steps outlined above and taking into account these considerations the following security requirements are elicited:

SRQ7:<u>Create Team</u> interface should filter <u>Team info.</u>
SRQ8: <u>Create Team</u> interface should sanitize the <u>Team info</u> to transform it to the required format
SRQ9: <u>Create Team</u> interface should canonicalize the <u>Team info</u> to verify it against its canonical representation. (Clarke *et al* 2012).

SRQ8 and SRQ9 are based on countermeasures suggested in Clarke *et al* 2008 for the most common SQL injection attacks.

5.2.2.4 Network infrastructure covers the protection of the network infrastructure in which business operations are carried out within the enterprise. This entails the enterprise being able to offer business services to the partner. As the Estonian Football Association is a small organisation, the most suitable solution for its network security needs would most likely be the stateful multilayer inspection firewall as it combines aspects from other firewalls. As a result, the following security requirements are elicited.

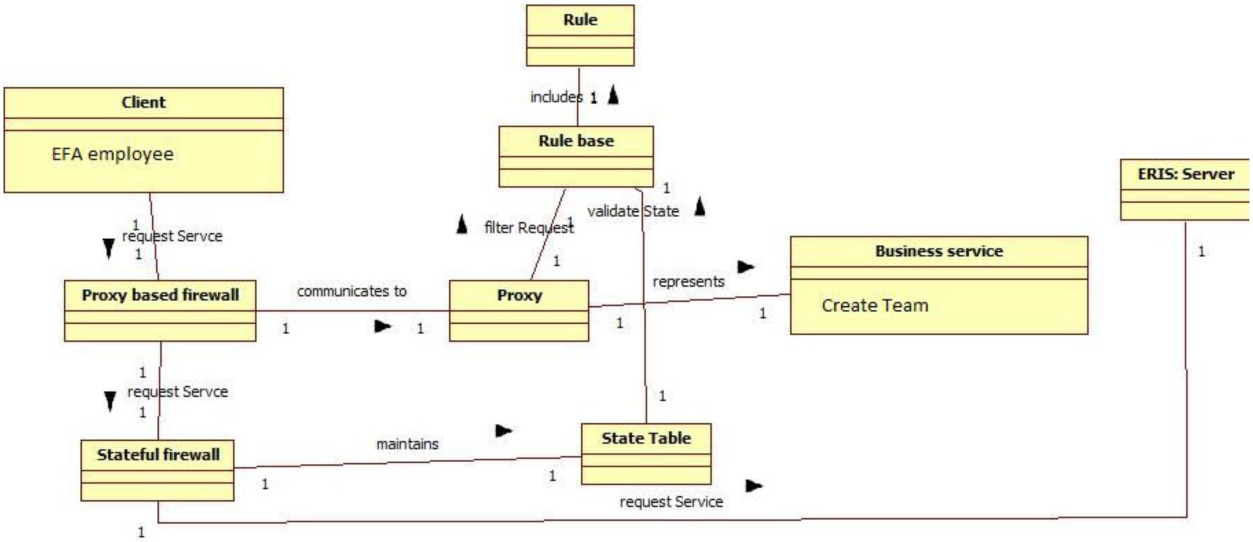


Figure 14: Firewall architecture

SRQ10: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQ11: Proxy based firewall should communicate to the proxy, which represents the Create Team, to determine the validity of the Team info received from the Football Association employee
SRQ12: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQ13: ERIS should block all default incoming ports by default until these ports are explicitly opened.

In most cases, the communication between the server and the business partners is bidirectional and similar security requirements must be taken into account when information is sent back from the server to the business partners. In the Register Team process, the server is assumed to be trusted and no requirements are thus elicited.

5.2.2.5 Data Store is the last contextual area examined within the framework of SREBP for security requirements elicitation, covering how data is stored and handled in the associated databases. Data confidentiality and integrity would be compromised if the threat agent were to get access to the data. There are several approaches to ensure that data remains protected, for example implementing encryption of the data itself. To facilitate the elicitation of security requirements, an RBAC model is used. The model is developed using the following steps:

Identifying datastore resource: In this contextual area, the datastore is identified as a singular entity. The business assets and relevant data are modeled as the resource attributes for the datastore. In the Register Team example, the attributes Team, Team info and Team rep are actually attributes of the business asset Team.
Identifying datastore's operations: In this contextual area, it is necessary to identify which operations save or retrieve data from the datastore. These operations are modeled as the operations of the datastore in the RBAC model.

Following these two steps, the roles and permissions are assigned using the methods described in the ***access control*** contextual area. The resulting RBAC model based on the Register Team example is shown in Figure 15. As a result of these considerations, the following security requirements are elicited:

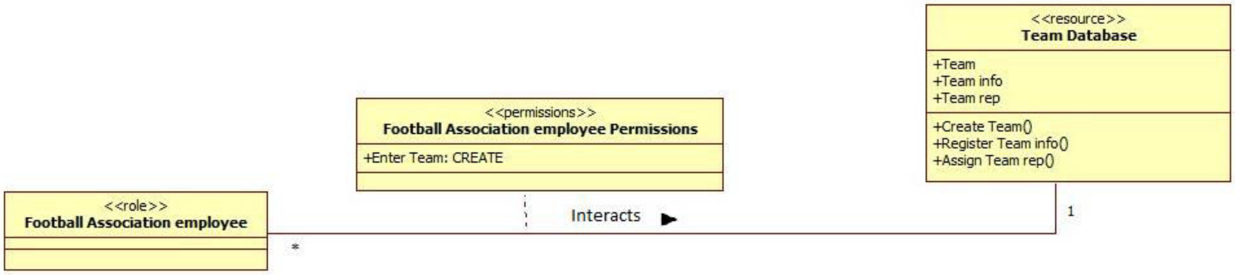


Figure 15: RBAC Security Model – Data Store

SRQ14: ERIS should audit the operations after the storage of Team, Team info and Team rep to the Team Database.
SRQ15: ERIS should perform an operation to hide Team when it is stored in the Team Database.
SRQ16: ERIS should perform an operation to hide Team info when it is stored in the Team Database.
SRQ17: ERIS should perform an operation to hide Team rep when it is stored in the Team Database.

SRQ14 entails monitoring and recording the events when the resource attributes are stored in the database. This allows for determining who performed what operations on which data at what time.
SRQ 15-17 require the implementation of a solution such as cryptographic algorithms. Even if physical access to the data store is gained by the attacker, they would not be able to violate the confidentiality of the data stored there.

5.2.3 Results of SREBP application

A number of security requirements were elicited using SREBP. The security requirements are listed in Table 7, assigned to their respective Business Assets. These security requirements are listed in more detail in the Appendix section A2.

Table 7: SREBP Security Requirements assigned to Business Assets

Business Asset	Security Requirements	Number of SRQ
Player	SRQBA1:1 SRQBA1:2 SRQBA1:3 SRQBA1:4 SRQBA1:5 SRQBA1:6 SRQBA1:7 SRQBA1:8 SRQBA1:9 SRQBA1:10 SRQBA1:11 SRQBA1:12 SRQBA1:13 SRQBA1:14 SRQBA1:15 SRQBA1:16 SRQBA1:17 SRQBA1:18	18
Team	SRQBA2:1 SRQBA2:2 SRQBA2:3 SRQBA2:4 SRQBA2:5 SRQBA2:6 SRQBA2:7 SRQBA2:8 SRQBA2:9 SRQBA2:10 SRQBA2:11 SRQBA2:12 SRQBA2:13 SRQBA2:14 SRQBA2:15 SRQBA2:16 SRQBA2:17 SRQBA2:18 SRQBA2:19 SRQBA2:20 SRQBA2:21 SRQBA2:22 SRQBA2:23 SRQBA2:24 SRQBA2:25 SRQBA2:26 SRQBA2:27 SRQBA2:28 SRQBA2:29 SRQBA2:30 SRQBA2:31 SRQBA2:32	32
Umpire	SRQBA3:1 SRQBA3:2 SRQBA3:3 SRQBA3:4 SRQBA3:5 SRQBA3:6 SRQBA3:7 SRQBA3:8 SRQBA3:9 SRQBA3:10 SRQBA3:11 SRQBA3:12 SRQBA3:13 SRQBA3:14 SRQBA3:15 SRQBA3:16 SRQBA3:17 SRQBA3:18 SRQBA3:19 SRQBA3:20 SRQBA3:21 SRQBA3:22 SRQBA3:23 SRQBA3:24 SRQBA3:25	25
Game	SRQBA4:1 SRQBA4:2 SRQBA4:3 SRQBA4:4 SRQBA4:5 SRQBA4:6 SRQBA4:7 SRQBA4:8 SRQBA4:9 SRQBA4:10 SRQBA4:11 SRQBA4:12 SRQBA4:13 SRQBA4:14 SRQBA4:15 SRQBA4:16 SRQBA4:17 SRQBA4:18 SRQBA4:19 SRQBA4:20 SRQBA4:21 SRQBA4:22 SRQBA4:23 SRQBA4:24 SRQBA4:25 SRQBA4:26 SRQBA4:27 SRQBA4:28 SRQBA4:29	29
Timetable	SRQBA5:1 SRQBA5:2 SRQBA5:3 SRQBA5:4 SRQBA5:5 SRQBA5:6 SRQBA5:7 SRQBA5:8 SRQBA5:9 SRQBA5:10 SRQBA5:11 SRQBA5:12 SRQBA5:13 SRQBA5:14 SRQBA5:15 SRQBA5:16 SRQBA5:17 SRQBA5:18 SRQBA5:19 SRQBA5:20 SRQBA5:21 SRQBA5:22	22
Total number of security requirements:		126

5.3 Summary

To sum up, the application of SQUARE resulted in the elicitation of 66 security requirements. On the other hand, the application of SREBP resulted in the elicitation of 126 security requirements; a significantly larger number. A further analysis of the differences between the two results is conducted in the next chapter to determine the completeness of coverage of the security requirements in order to answer the research question of this thesis.

6 Results and Validity

This chapter analyses the outcomes of the empirical study that was conducted in the previous chapter. Firstly the result and validity of the empirical study are scrutinized in detail to find the answer to the research question, to do so, the author categorizes and evaluates the coverage of the security requirements. Finally, threats to the validity of the findings are covered.

6.1 Evaluation of the Coverage of the Security Requirements

For the purposes of this thesis, the comparison criteria and the method for comparing completeness, developed in by Ahmed (2014), will be used to compare the results of the empirical study. In (Ahmed, 2014) eight generic security categories are chosen and used as a baseline to see to what extent the security requirements satisfy the security criterion of these eight categories. These categories are as follows:

- Identification – security requirements that connect an individual or an application to a unique identity before it interacts with the information system.
- Authentication – security requirements that recognize and validate the user's identity before interacting with the information system.
- Authorization – security requirements that characterize the role or the user authorized to access business assets or related data within the information system.
- Accounting – security requirements to record security related events or actions and make this info accessible at a later point.
- Audit – security requirements to analyze the security actions captured by accounting security requirements and to then compare them against a rule set to determine whether security violations occurred.
- Non-repudiation - security requirements that record evidence of the users who have participated in an activity to provide proof of their involvement later on.
- Immunity – security requirements that specify the ability of an information system to resist unauthorized access or attacks from viruses
- Data exchange – security requirements that protect the confidentiality of data from unauthorized access during transmission over unsecured mediums such as the internet.

This method considers the security requirements to have 100% coverage if all the security criterion of each category have been met. These criteria are Confidentiality, Integrity and Availability. However not all categories consider all three criteria. For example, for the non-repudiation category, only the Integrity of the data is important. Each category contributes 12.5% of the complete coverage. A 5 stage scale, from 0% to 100%, increasing in 25% increments is used to measure the completeness of coverage in each category. 0% coverage means that none of the security requirements meet the security criterion of that category whereas 100% coverage means that the security requirements satisfy all of the relevant security criteria of that category for that business asset. Additionally security requirements can satisfy more than one criterion for each category and some requirements are applicable to more than one category, an example of this is SRQBA2:10 which covers a number of different categories.

To illustrate this, an example based on the Team business asset is shown in Table 8. Based on the Team business asset, the application of SREBP yielded security requirements that provided 81.3% coverage, whereas the security requirements elicited using SQUARE only yielded 45.87% coverage. The rest of the tables with the application results for each business asset can be found in the Appendix section A3.

The overall completeness comparison of the security requirements elicited using SQUARE and SREBP is presented in Table 9. To sum up, it is apparent from the results that for every business asset, SREBP security requirements provide significantly more coverage. The difference of coverage of SQUARE and SREBP ranges from 31.25% with security requirements elicited for the Timetable business asset to 39% for the Umpire business asset. Based on this data the research question can be answered: it is clear that SREBP allows for the elicitation of a more complete set of security requirements for the Estonian Football Association compared to SQUARE.

6.2 Threats to Validity

Although the empirical study of this thesis presents the thorough comparative analysis of SQUARE and SREBP, the author admits certain limitations in its validity.. The main threat to validity of this study lies with the author's limited experience of implementing both SREBP and SQUARE. The research presented in this thesis represents the first time the author has had to apply either method to a real case study. Additionally, the Estonian Football Association did not have its business processes modeled and as a result, there may be discrepancies between the operational business models presented in this study and the actual business operations of the organization. Another potentially limiting factor is the order in which the security requirements elicitations were carried out. By the time the author carried out the second security requirements elicitation, a certain familiarity with the topic had already been developed.

Table 8: Completeness of Business Asset Team related security requirements

Asset: Team										
Requirements Categorization			**Requirements (SREBP)**	**Coverage**				**Requirements (SQUARE)**	**Coverage**	
1. Identification	C	6.25	SRQBA2:4	75%	4.69	C	6.25	SRQ1.2	50%	3.13
	I	6.25	SRQBA2:4	75%	4.69	I	6.25		0%	-
	A	-				A	-			
2. Authentication	C	4.17	SRQBA2:4, SRQBA2:5, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:27, SRQBA2:28, SRQBA2:29	100%	4.17	C	4.17	SRQ1.2, SRQ 3.2	75%	3.13
	I	4.17	SRQBA2:4, SRQBA2:5, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:27, SRQBA2:28, SRQBA2:29	100%	4.17	I	4.17	SRQ2.2	50%	2.09
	A	4.17	SRQBA2:5, SRQBA2:10	100%	4.17	A	4.17	SRQ2.2	50%	2.09
3. Authorization	C	4.17	SRQBA2:1, SRQBA2:2, SRQBA2:3, SRQBA2:4, SRQBA2:18, SRQBA2:19, SRQBA2:20, SRQBA2:21	100%	4.17	C	4.17	SRQ1.2, SRQ3.2	100%	4.17
	I	4.17	SRQBA2:1, SRQBA2:2, SRQBA2:3, SRQBA2:4, SRQBA2:18, SRQBA2:19, SRQBA2:20, SRQBA2:21	100%	4.17	I	4.17	SRQ2.2	50%	2.09
	A	4.17	SRQBA2:10 SRQBA2:13	50%	2.085	A	4.17	SRQ6.2, SRQ2.2	25%	1.04
4. Accounting	C	4.17	SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:27, SRQBA2:28, SRQBA2:29	75%	3.128	C	4.17	SRQ8.2, SRQ13.2	100%	4.17
	I	4.17	SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:27, SRQBA2:28, SRQBA2:29	75%	3.128	I	4.17	SRQ8.2, SRQ13.2	100%	4.17
	A	4.17	SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:27, SRQBA2:28, SRQBA2:29	75%	3.128	A	4.17	SRQ13.2	75%	3.13
5. Audit	C	4.17	SRQBA2:14, SRQBA2:30	75%	3.128	C	4.17		0%	-
	I	4.17	SRQBA2:14, SRQBA2:30	75%	3.128	I	4.17	SRQ13.2	25%	1.04
	A	4.17	SRQBA2:14, SRQBA2:30	75%	3.128	A	4.17		0%	0.00
6. Non repudiation	C	-				C	-			
	I	12.5	SRQBA2:14, SRQBA2:30	75%	9.375	I	12.5		0%	0.00
	A	-				A	-			
7. Immunity	C	4.17	SRQBA2:6, SRQBA2:7, SRQBA2:8, SRQBA2:9, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:15, SRQBA2:16, SRQBA2:17, SRQBA2:18, SRQBA2:22, SRQBA2:23, SRQBA2:24, SRQBA2:25, SRQBA2:26, SRQBA2:27, SRQBA2:28,	100%	4.17	C	4.17	SRQ4.2, SRQ14	75%	3.13
	I	4.17	SRQBA2:6, SRQBA2:7, SRQBA2:8, SRQBA2:9, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:15, SRQBA2:16, SRQBA2:17, SRQBA2:18, SRQBA2:22, SRQBA2:23, SRQBA2:24, SRQBA2:25, SRQBA2:26, SRQBA2:27, SRQBA2:28, SRQBA2:29, SRQBA2:31, SRQBA2:32	100%	4.17	I	4.17	SRQ4.2, SRQ14	75%	3.13
	A	4.17	SRQBA2:6, SRQBA2:7, SRQBA2:8, SRQBA2:9, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:15, SRQBA2:16, SRQBA2:17, SRQBA2:18, SRQBA2:22, SRQBA2:23, SRQBA2:24, SRQBA2:25, SRQBA2:26, SRQBA2:27, SRQBA2:28, SRQBA2:29, SRQBA2:31, SRQBA2:32	100%	4.17	A	4.17	SRQ4.2, SRQ14	75%	3.13
8. Data Exchange	C	4.17	SRQBA2:5, SRQBA2:6, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:22, SRQBA2:23, SRQBA2:27, SRQBA2:28, SRQBA2:29	100%	4.17	C	4.17	SRQ12	50%	2.09
	I	4.17	SRQBA2:5, SRQBA2:6, SRQBA2:10, SRQBA2:11, SRQBA2:12, SRQBA2:13, SRQBA2:22, SRQBA2:23, SRQBA2:27, SRQBA2:28, SRQBA2:29	100%	4.17	I	4.17	SRQ12	50%	2.09
	A	4.17		0%	0	A	4.17	SRQ6.2, SRQ12	50%	2.09
Coverage %					81.30					45.87

Table 9: Overall completeness comparison of SQUARE and SREBP

Methods		SREBP									SQUARE									Difference
Business Assets	Categories	Identification	Authentication	Authorization	Accounting	Audit	Non-repudiation	Immunity	Data exchange	TOTAL	Identification	Authentication	Authorization	Accounting	Audit	Non-repudiation	Immunity	Data exchange	TOTAL	
		12.5	12.5	12.5	12.5	12.5	12.5	12.5	12.5	**100**	12.5	12.5	12.5	12.5	12.5	12.5	12.5	12.5	**100**	
Player	Reqs.	2	12	12	15	3	1	30	12	**87**	1	4	5	5	1	0	6	4	**26**	61
	%age	75%	100%	75%	75%	75%	75%	100%	67%	**80%**	25%	58%	58%	92%	8%	0%	75%	50%	**46%**	34%
	Coverage	**9.38**	**12.50**	**9.38**	**9.38**	**9.38**	**9.38**	**12.50**	**8.33**	**80.21**	**3.13**	**7.29**	**7.29**	**11.46**	**1.04**	**0.00**	**9.38**	**6.25**	**45.83**	**34.375**
Team	Reqs.	2	18	18	21	6	2	66	22	**155**	1	4	5	5	1	0	6	4	**26**	129
	%age	75%	100%	83%	75%	75%	75%	100%	67%	**81%**	25%	58%	58%	92%	8%	0%	75%	50%	**46%**	35%
	Coverage	**9.38**	**12.50**	**10.42**	**9.38**	**9.38**	**9.38**	**12.50**	**8.33**	**81.25**	**3.13**	**7.29**	**7.29**	**11.46**	**1.04**	**0.00**	**9.38**	**6.25**	**45.83**	**35.4167**
Umpire	Reqs.	2	12	14	15	6	2	51	22	**124**	1	4	5	5	1	0	6	4	**26**	98
	%age	75%	100%	83%	100%	75%	75%	100%	67%	**84%**	25%	58%	58%	92%	8%	0%	75%	50%	**46%**	39%
	Coverage	**9.38**	**12.50**	**10.42**	**12.50**	**9.38**	**9.38**	**12.50**	**8.33**	**84.38**	**3.13**	**7.29**	**7.29**	**11.46**	**1.04**	**0.00**	**9.38**	**6.25**	**45.83**	**38.5417**
Game	Reqs.	4	24	14	30	3	1	66	24	**166**	1	4	5	5	0	1	6	4	**26**	140
	%age	75%	100%	83%	100%	75%	75%	100%	67%	**84%**	25%	58%	58%	92%	0%	25%	75%	50%	**48%**	36%
	Coverage	**9.38**	**12.50**	**10.42**	**12.50**	**9.38**	**9.38**	**12.50**	**8.33**	**84.38**	**3.13**	**7.29**	**7.29**	**11.46**	**0.00**	**3.13**	**9.38**	**6.25**	**47.92**	**36.4583**
Timetable	Reqs.	2	20	12	21	3	1	48	18	**125**	1	4	5	5	2	1	6	4	**28**	97
	%age	75%	100%	67%	100%	75%	75%	100%	67%	**82%**	25%	58%	58%	92%	25%	25%	75%	50%	**51%**	31%
	Coverage	**9.38**	**12.50**	**8.33**	**12.50**	**9.38**	**9.38**	**12.50**	**8.33**	**82.29**	**3.13**	**7.29**	**7.29**	**11.46**	**3.13**	**3.13**	**9.38**	**6.25**	**51.04**	**31.25**
TOTAL	%age	75%	100%	78%	90%	75%	75%	100%	67%	**83%**	25%	58%	58%	92%	10%	10%	75%	50%	**47%**	35%
	Coverage	**9.38**	**12.50**	**9.79**	**11.25**	**9.38**	**9.38**	**12.50**	**8.33**	**82.50**	**3.13**	**7.29**	**7.29**	**11.46**	**1.25**	**1.25**	**9.38**	**6.25**	**47.29**	**35.2083**

6.3 Summary

Chapter 6 introduced the criteria used for comparing the security requirements elicited as a result of the empirical study illustrated in Chapter 5. Subsequently, it carried out comparative analysis of the requirement engineering process of SQUARE and SREBP. Consequently, such comparison showed that SREBP security requirements provide better coverage than SQUARE security requirements. In the next chapter, the study is concluded; the limitations of the thesis, findings and potential future work are explained.

7 Conclusion

This thesis explored the topic of security requirements elicitation within the Security Engineering domain. Several problems in the domain of security requirements elicitation were illustrated and SREBP and SQUARE are potential solutions for these problems.

7.1 Limitations

This thesis has a number of limitations. The primary limitation of this thesis is that the applicability of the results of the empirical study is limited by the security elicitation methods only being applied to one case study. Further comparisons should be carried out to support the findings of this thesis.. The author also recognizes that the inherent differences between SQUARE and SREBP may have contributed to the outcome of the empirical study. SQUARE is aimed at security analysts and offers additional steps after the security requirements elicitations which were not carried out as part of this study. Additionally, SREBP was designed with the use of operational business processes in mind whereas using these with SQUARE requires additional security domain knowledge. SQUARE also requires more extensive interaction with the stakeholders compared to SREBP, something which was not always possible during the empirical study portion of this thesis. A certain amount of subjective bias must also be accounted for in terms of the models and security requirements elicited; different security analysts may come up with slightly different models and security requirements, however the overall picture should stay largely the same.

7.2 Answer to Research Question

In this thesis the following research question was posed:

RQ: Which security requirements elicitation method, SQUARE or SREBP, helps to identify a more complete list of security requirements?

The research question was answered by carrying out an empirical study on the EFA. SQUARE and SREBP were applied to elicit security requirements based on this case study. These security requirements were then categorized and their completeness of coverage based on several categories was measured.

The results of the empirical study showed that security requirements elicited using SREBP provide, on average 35.2% better coverage than the security requirements elicited using SQUARE. In every category, the security requirements elicited using SREBP provided better coverage than SQUARE security requirements. The findings of the empirical study allow the research question to be answered: SREBP helps identifying a more complete list of security requirements.

This thesis contributes to the existing research in the security engineering domain by providing an empirical analysis of two security requirements elicitation methods. By doing so, the thesis adds another empirical analysis of the newly introduced SREBP method which has only been applied to one other case study so far. Moreover this study differentiates itself from the previous application by applying SQUARE and SREBP on the EFA which did not have any security solutions in place and did not have business processes modeled. Despite such a difference, this thesis produced results which were in line with previous work. Thereby this thesis contributes to the reinforcement of the validity of SREBP.

7.3 Future Work

For future research, a number of possible avenues of improving both methods exist. For SREBP, one possible avenue for future work could be the comparison of SREBP to other business process based security requirements elicitation methods. To improve SQUARE, further integration with the ISSRM process could be explored for risk assessment and security requirements elicitation in order to produce better security requirements. Finally, the option of integrating SREBP within SQUARE would probably security requirements with better coverage than either method applied individually, therefore the author suggests that this avenue of research should be explored in the future.

References

1. Alberts, C. J., & Dorofee, A. (2002). Managing information security risks: the OCTAVE approach.

2. Alter, S. (2006). The work system method: connecting people, processes, and IT for business results. Work System Method.

3. Ahmed, N. Matulevičius, R. (2014a) Securing business processes using security risk-oriented patterns in Computer Standards & Interfaces, Volume 36, Issue 4, Pages 723-733.

4. Ahmed, N. Matulevičius, R. (2014b) A Method for Eliciting Security Requirements from the Business Process Models, Submitted as the extended paper to CA ISE2014 quorum proceedings & Springer LMBIP

5. Ahmed, N., (2014) Deriving Security Requirements from Business Process Models, PhD Thesis, University of Tartu

6. Anderson, R. (2001, December). Why information security is hard-an economic perspective. In Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 358-365). IEEE.

7. Backes, M., Pfitzmann, B., & Waidner, M. (2003). Security in business process engineering. In Business Process Management (pp. 168-183). Springer Berlin Heidelberg.

8. Bertrand P, Darimont R, Delor E, Massonet P, van Lamsweerde A., (1998) GRAIL/KAOS: an environment for goal drivent requirements engineering. In: ICSE'98—20th international conferenceon software engineering

9. Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. BT Technology Journal, 25(1), 101-117.

10. Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., & Mylopoulos, J. (2004). Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems, 8(3), 203-236.

11. Chen, P., Dean, M., Ojoko-Adams, D., Osman, H., & Lopez, L. (2004). Systems quality requirements engineering (square) methodology: Case study on asset management system (No. CMU/SEI-2004-SR-015).

12. Clarke, J. (Ed.). (2012). SQL injection attacks and defense.

13. Demirors, O., Gencel, Ç., & Tarhan, A. (2003, September). Utilizing business process models for requirements elicitation. In Euromicro Conference, 2003. Proceedings. 29th (pp. 409-412). IEEE.

14. Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In Intentional Perspectives on Information Systems Engineering (pp. 289-306).

15. Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. Requirements engineering, 15(1), 7-40.

16. Firesmith, D. G. (2007)Engineering Safety and Security Related Requirements for Software Intensive Systems, Companion to the proceedings of the 29th International Conference on Software Engineering, p.169, May 20-26,

17. Gayash, A., Viswanathan, V., Padmanabhan, D., & Meed, N. R. (2008). SQUARE-lite: Case study on VADSoft project (No. CMU/SEI-2008-SR-017).

18. Gürses, S., Berendt, B., & Santen, T. (2006). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. In Proceedings of the UKDU Workshop (pp. 51-64).

19. Herrmann, P., & Herrmann, G. (2006). Security requirement analysis of business processes. Electronic Commerce Research, 6(3-4), 305-335

20. Jürjens, J. (2005). Secure systems development with UML. Springer Science & Business Media.

21. Lodderstedt, T., Basin, D., & Doser, J. (2002). SecureUML: A UML-based modeling language for model-driven security. In ≪ UML≫ 2002—The Unified Modeling Language (pp. 426-441).

22. Mayer, N., Heymans, P., & Matulevicius, R. (2007). Design of a Modelling Language for Information System Security Risk Management. In RCIS (pp. 121-132).

23. Mead , N. R. Stehney, T. Security quality requirements engineering (SQUARE) methodology, Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications, p.1-7 (2005)

24. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). Security Patterns: Integrating security and systems engineering. John Wiley & Sons.

25. Sindre, G., & Opdahl, A. L. (2001). Capturing security requirements through misuse cases. NIK 2001, Norsk Informatikkonferanse 2001,

26. Workflow Management Coalition (WMC) (1999), Terminology & Glossary. Technical Report WFMC-TC-1011, The Workflow Management Specification

27. Zairi, M. (1997). Business process management: a boundaryless approach to modern competitiveness. Business Process Management Journal, 3(1), 64-80.

28. Business Process Model and Notation, Object Management Group, http://www.bpmn.org/ (last accessed 01/02/2015)

Appendix

Section A1: EFA value chain and operational business models

The operational business process models as well as the value chain of the EFA are shown in this section.

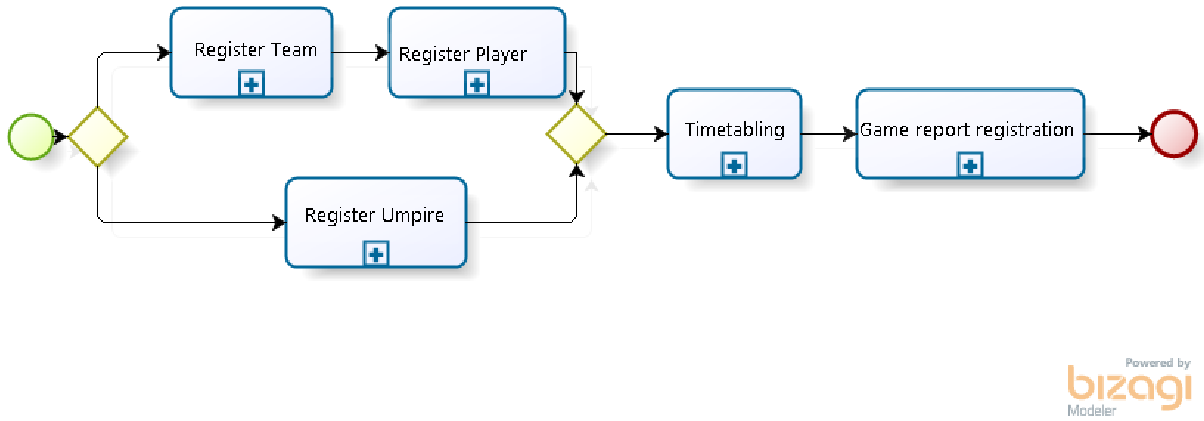


Figure A 1 Football Association Value Chain

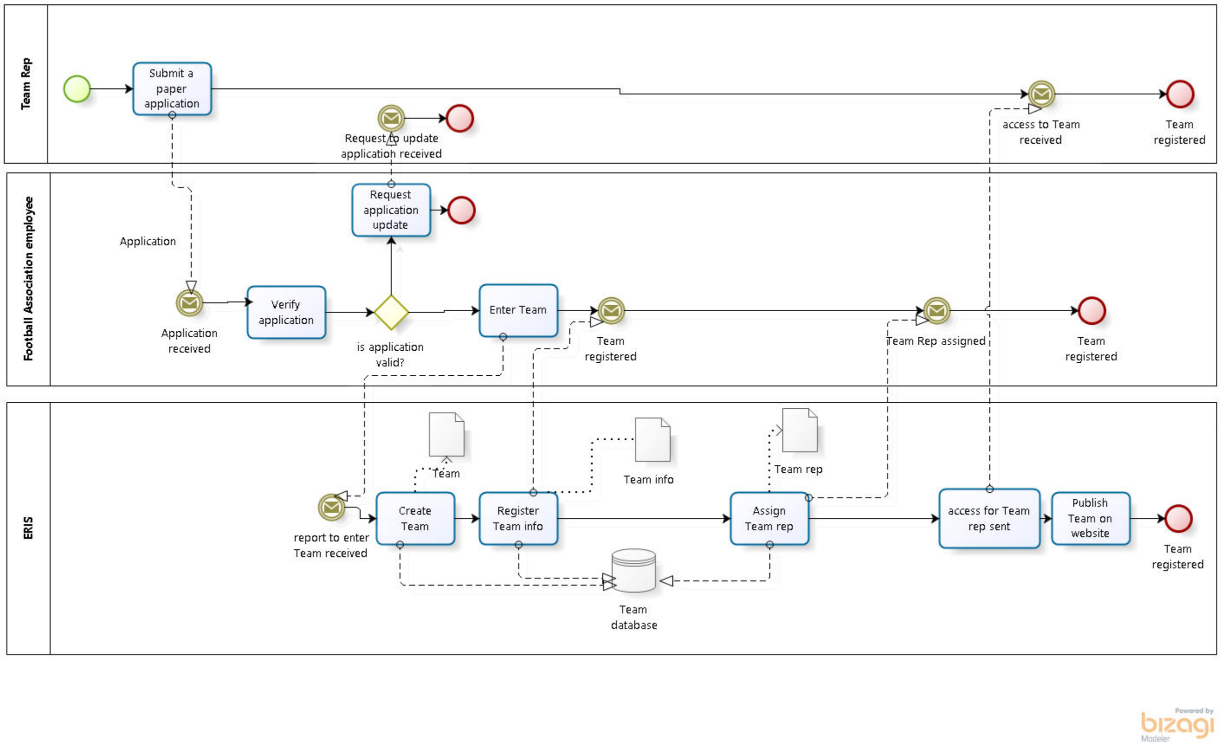


Figure A 2 Register Team business process

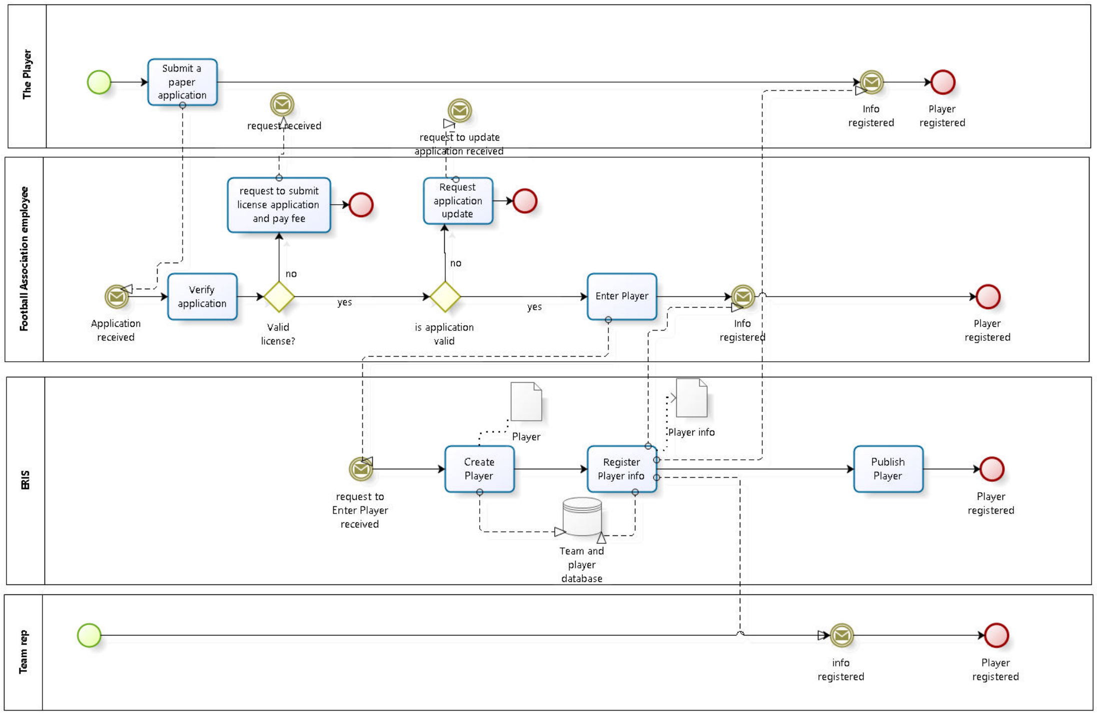


Figure A 3 Register Player business process

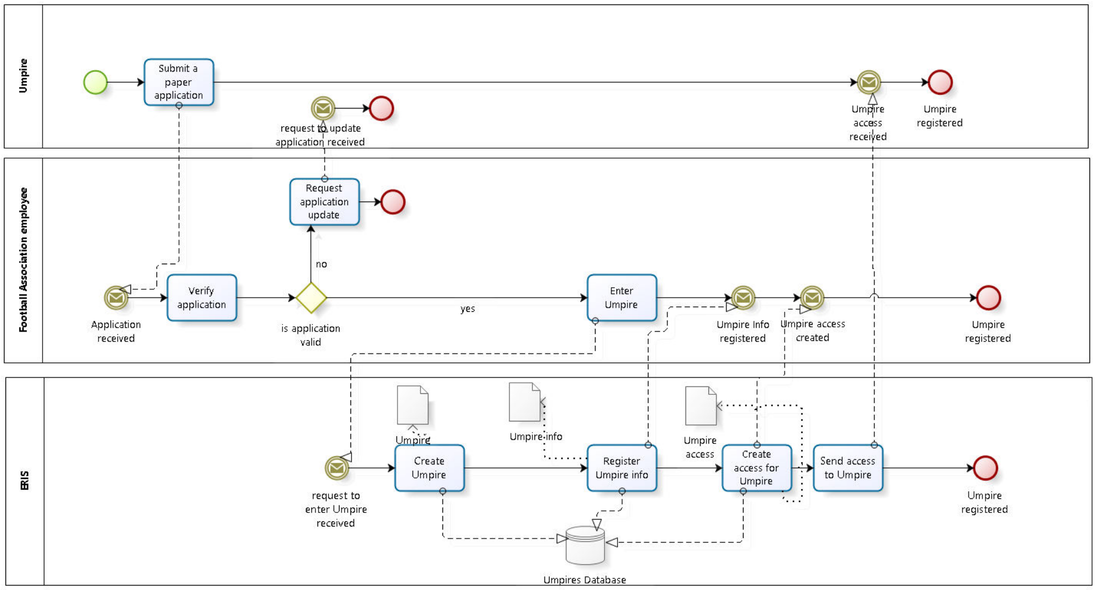


Figure A 4 Register Umpire business process

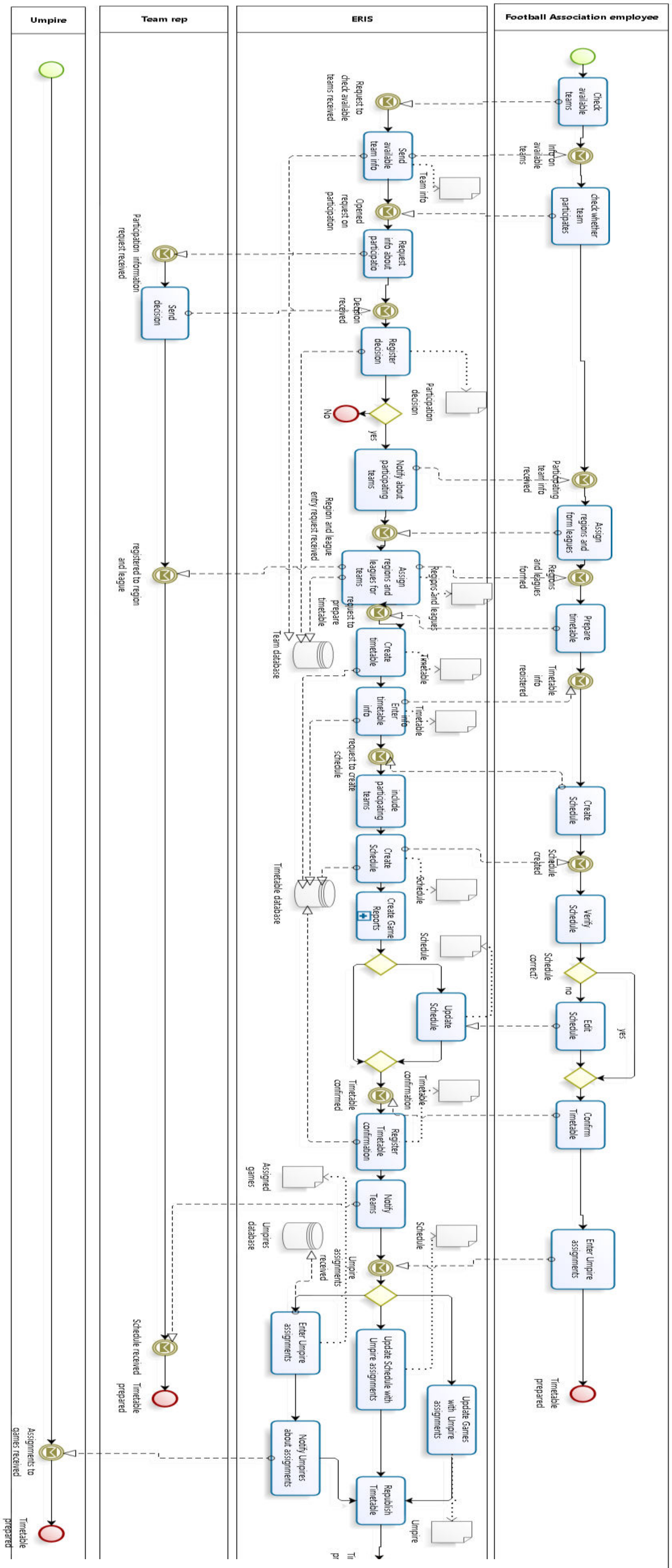

Umpire
Team rep
ERIS
Football Association employee
Check available teams
Request to check available teams received
Send available team info
Inform on available teams
Team info
Check whether team participates
Opened request on participation
Request info about participation
Participation information request received
Send decision
Decision received
Register decision
Participation decision
No
yes
Notify about participating teams
Participating team info received
Assign regions and form leagues
Region and league entry request received
Assign regions and leagues for teams
registered to region and league
Regions and leagues formed
Regions and leagues
Prepare timetable
request to prepare timetable
Create timetable
Timetable
Team database
Timetable info registered
Enter timetable info
Timetable info
request to create schedule
Create Schedule
include participating teams
Create Schedule
Schedule created
Schedule
Timetable database
Create Game Reports
Verify Schedule
Schedule correct?
no
yes
Schedule
Update Schedule
Edit Schedule
Timetable confirmation
Timetable confirmed
Register Timetable confirmation
Confirm Timetable
Assigned games
Notify Teams
Schedule
Umpires database
Umpire assignments received
Enter Umpire assignments
Enter Umpire assignments
Update Schedule with Umpire assignments
Update Games with Umpire assignments
Schedule received
Timetable prepared
Timetable prepared
Notify Umpires about assignments
Assignments to games received
Republish Timetable
Umpire
Timetable prepared
Ti
pr

Figure A 5 Timetabling business process

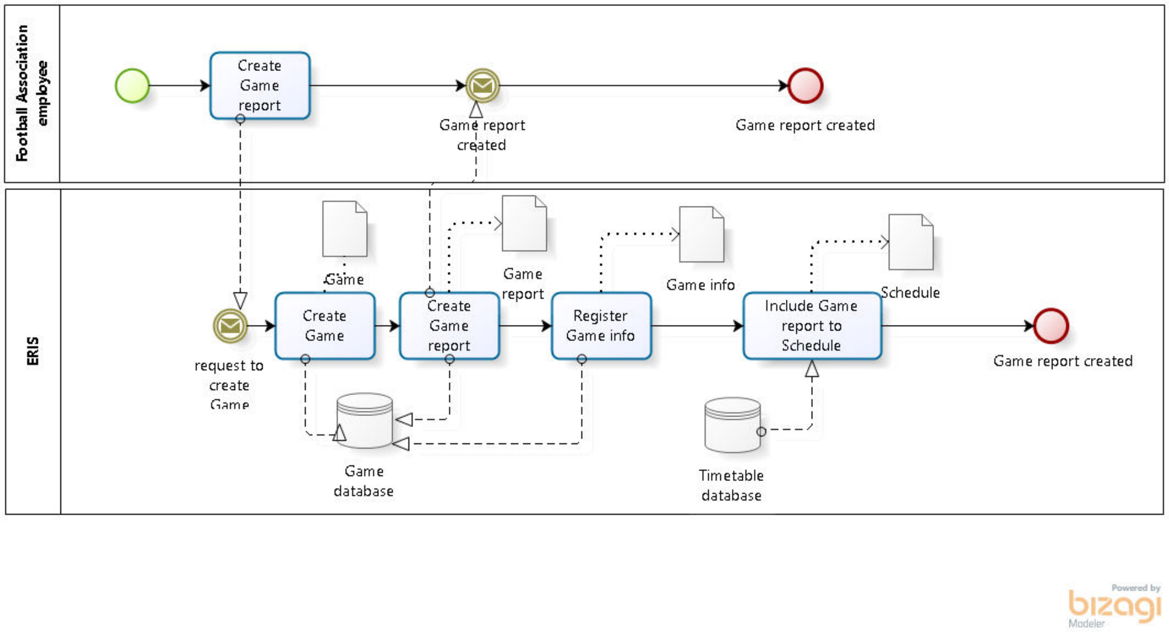


Figure A 6 Game report registration, Create Game business model

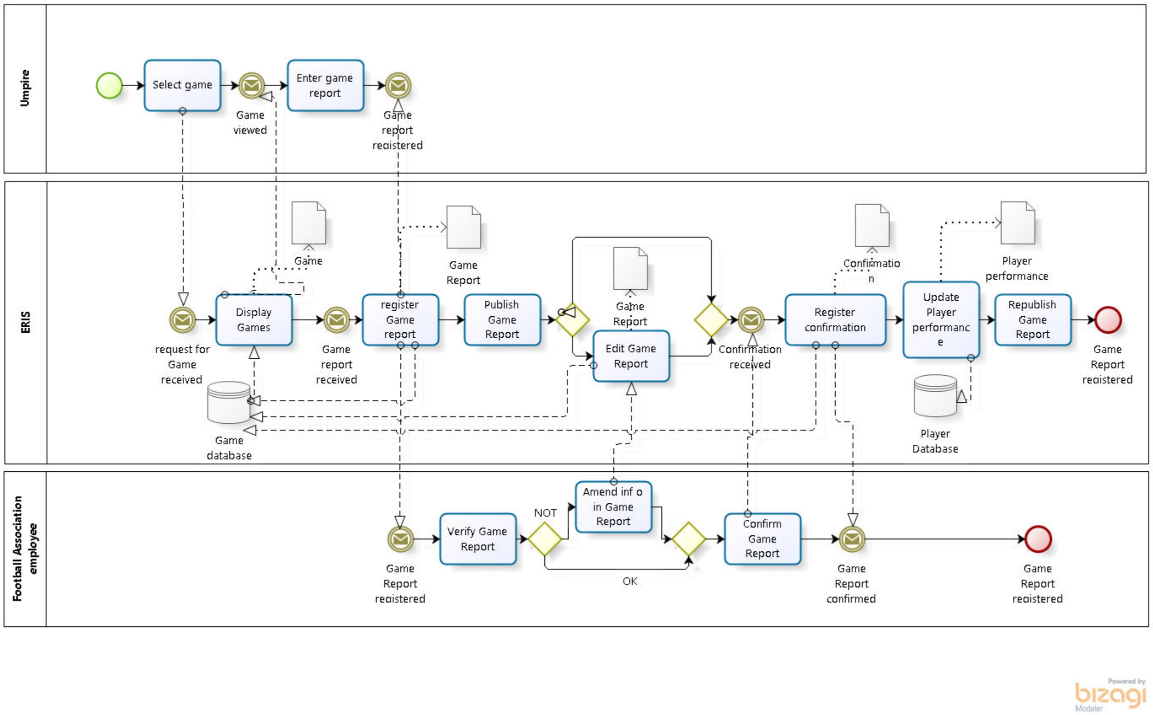


Figure A 7 Game report registration business model

Section A 2: SREBP implementation

Register Player

The following represents the SREBP implementation on the Register Player business process

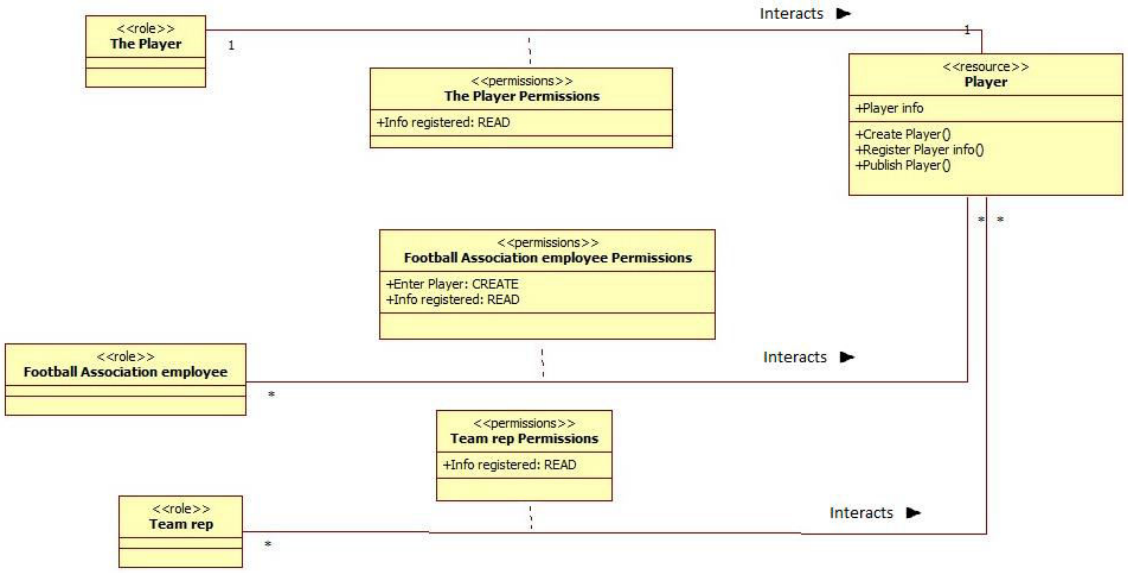


Figure A2 1 *Register Player RBAC model*

SRQ18: Football Association employee: should be able to: Create the Player
SRQ19: : Football Association employee: should be able to: Read the Player info.
SRQ20: The Player should be able to: Read the Player info.
SRQ21: The Team rep should be able to Read the Player info.
SRQ22: Permission Info registered: READ should be given only to one user assigned to The Player role.

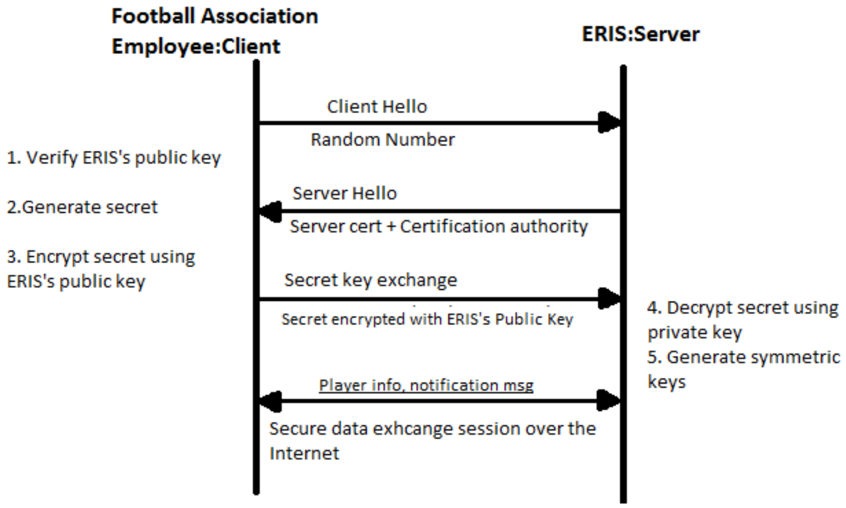


Figure A2 2 TLS/SSL Protocol implementation, adapted from (Ahmed & Matulevičius, 2014)

SRQ23: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority

SRQ24: Football Association employee should encrypt and sign the Player info (and notification messages) using the keys before sending it to ERIS.

SRQ25: Create Player interface should filter Player info.

SRQ26: Create Player interface should sanitize the Player info to transform it to the required format

SRQ27: Create Player interface should canonicalize the Player info to verify it against its canonical representation.

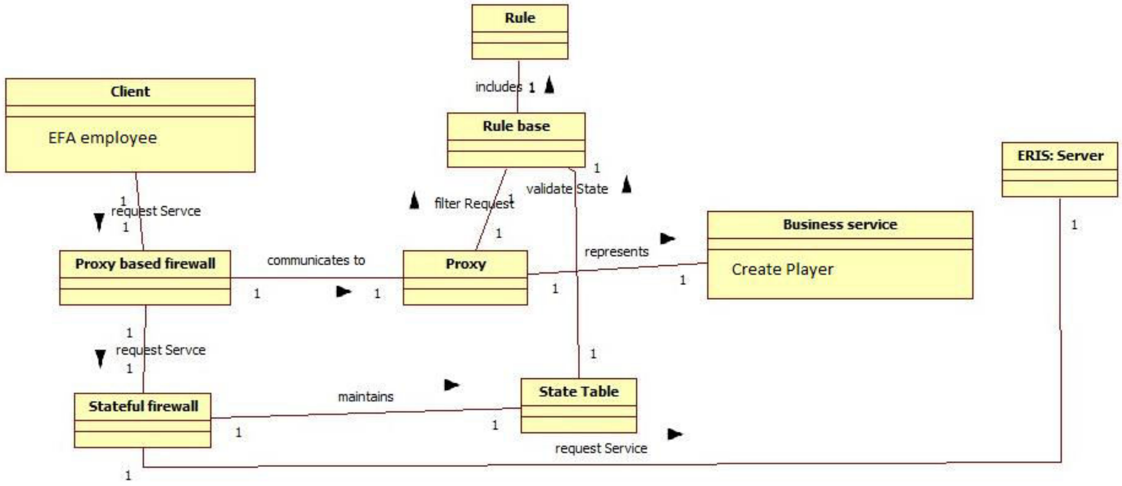


Figure A2 3 *Register Player Business service model*

SRQ28: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQ29: Proxy based firewall should communicate to the proxy, which represents the Create Player, to determine the validity of the Player info received from the Football Association employee
SRQ30: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQ31: ERIS should block all default incoming ports by default until these ports are explicitly opened.

In most cases, the communication between the server and the business partners is bidirectional and similar security requirements must be taken into account when information is sent back from the server to the business partners. In the Register Player process, the server is assumed to be trusted and no requirements are thus elicited.

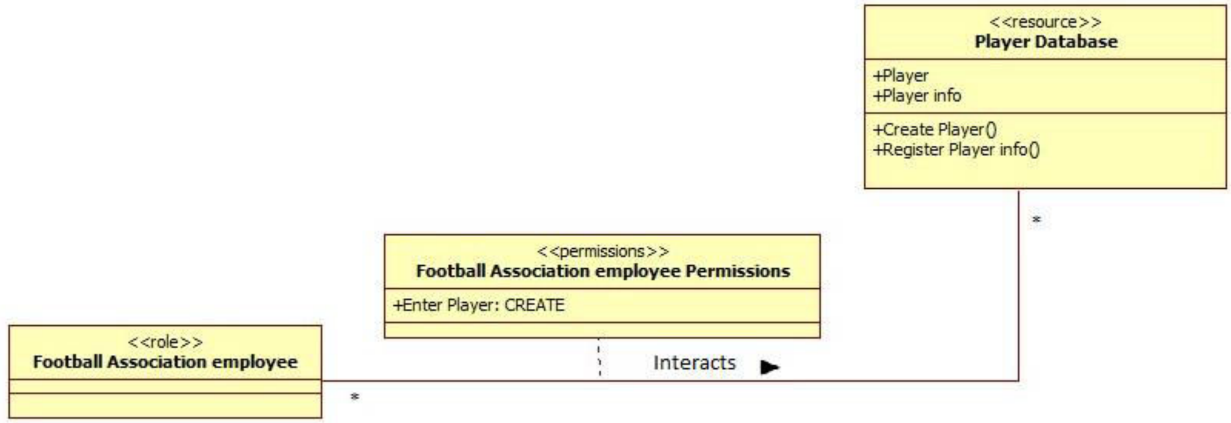


Figure A2 4 *Register Player Database RBAC model*

SRQ32: ERIS should audit the operations after the storage of Player and Player info to the Player Database.
SRQ33: ERIS should perform an operation to hide Player when it is stored in the Player Database.
SRQ34: ERIS should perform an operation to hide Player info when it is stored in the Player Database.

Register Umpire

The following represents the SREBP implementation on the Register Umpire business process

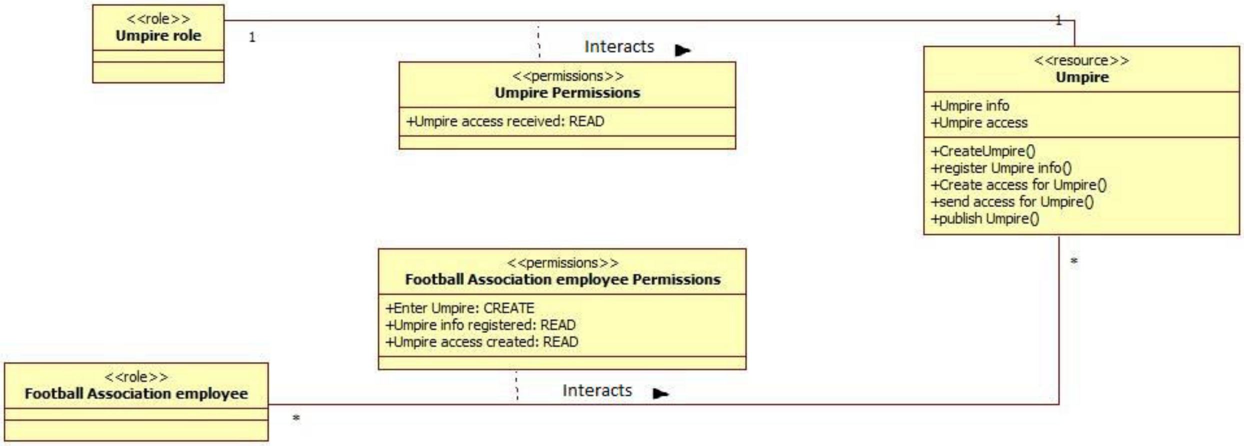


Figure A2 5 *Register Umpire RBAC model*

SRQ35: Football Association employee: should be able to: Create the Umpire .
SRQ36: Football Association employee: should be able to: Read the Umpire info and Umpire access.
SRQ37: Umpire should be able to: Read the Umpire info and Umpire info message.
SRQ38: Permission Umpire access received: READ should be given only to one user assigned to The Umpire role.

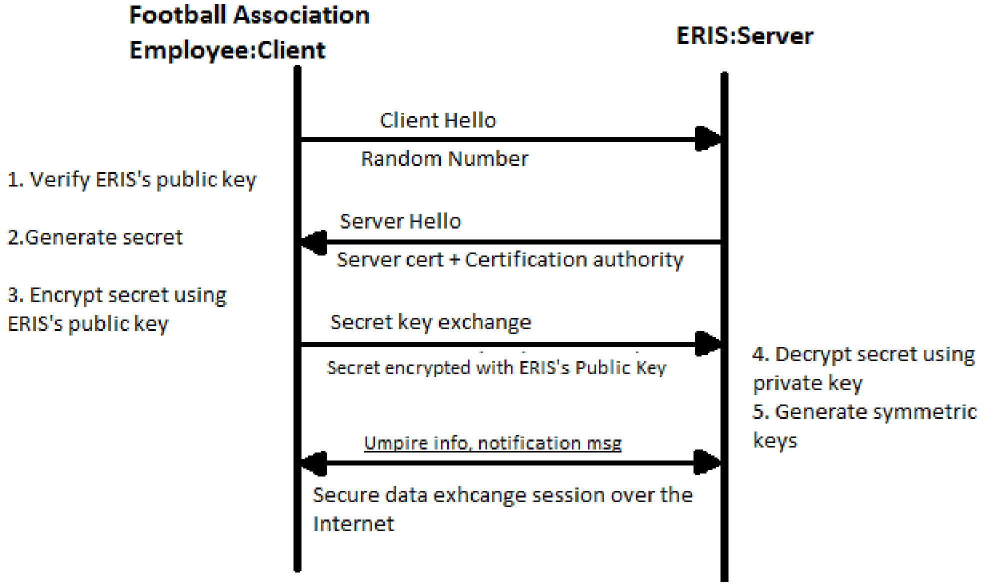

Football Association Employee:Client
ERIS:Server
Client Hello
Random Number
1. Verify ERIS's public key
2.Generate secret
3. Encrypt secret using ERIS's public key
Server Hello
Server cert + Certification authority
Secret key exchange
Secret encrypted with ERIS's Public Key
4. Decrypt secret using private key
5. Generate symmetric keys
Umpire info, notification msg
Secure data exhcange session over the Internet

Figure A2 6 *TLS/SSL Protocol implementation, adapted from (Ahmed & Matulevičius, 2014)*

SRQ39: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQ40: Football Association employee should encrypt and sign the Umpire info (and notification messages) using the keys before sending it to ERIS.
SRQ41: Create Umpire interface should filter Umpire info.
SRQ42: Create Umpire interface should sanitize the Umpire info to transform it to the required format.
SRQ43: Create Umpire interface should canonicalize the Umpire info to verify it against its canonical representation.

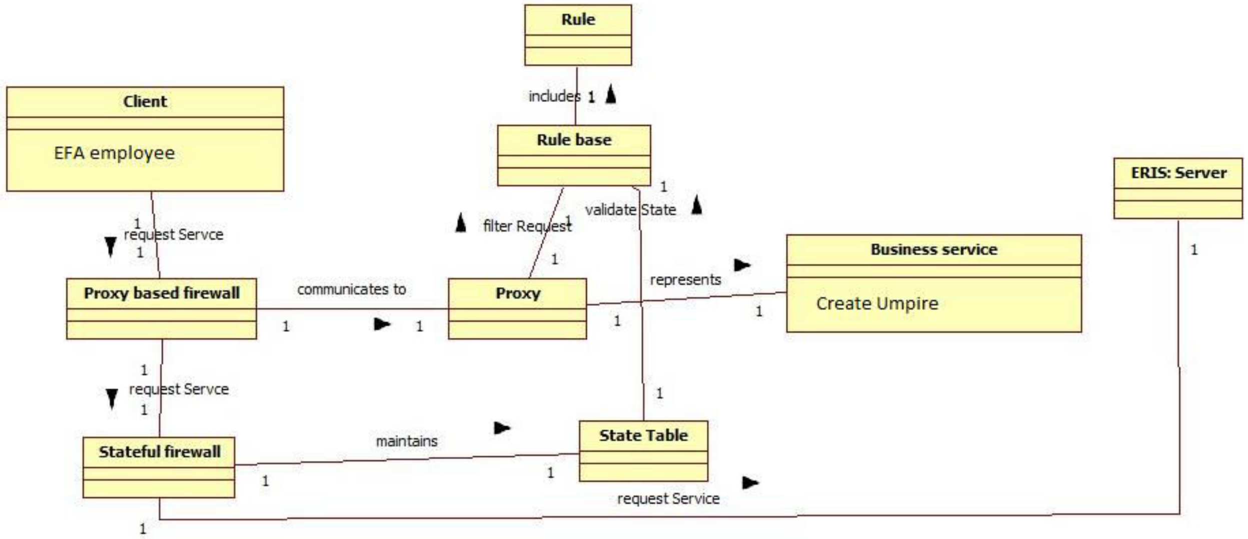


Figure A2 7 *Register Umpire Network infrastructure model*

SRQ44: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQ45: Proxy based firewall should communicate to the proxy, which represents the Create Umpire, to determine the validity of the Umpire info received from the Football Association employee
SRQ46: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQ47: ERIS should block all default incoming ports by default until these ports are explicitly opened.

In most cases, the communication between the server and the business partners is bidirectional and similar security requirements must be taken into account when information is sent back from the server to the business partners. In the Register Umpire process, the server is assumed to be trusted and no requirements are thus elicited.

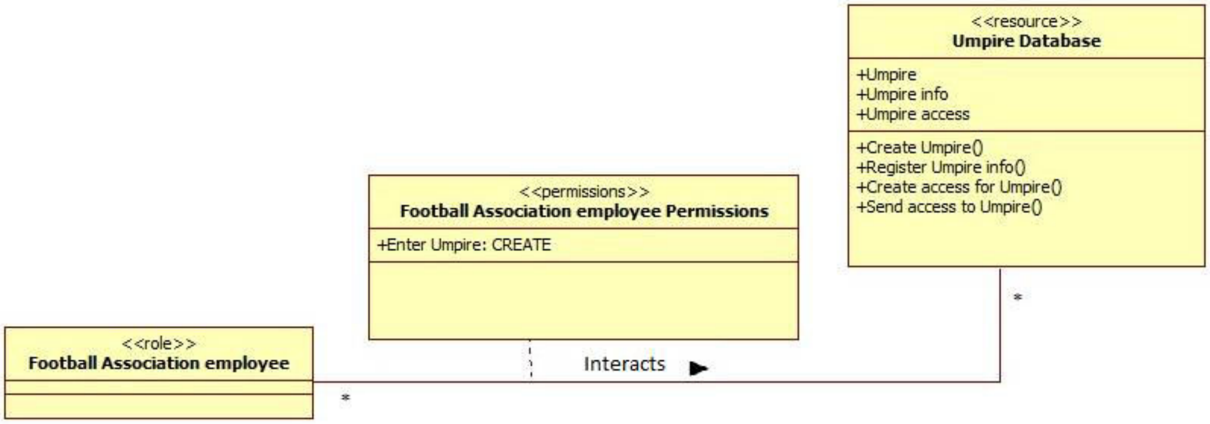


Figure A2 8 *Register Umpire Database RBAC model*

SRQ48: ERIS should audit the operations after the storage of Umpire, Umpire info and Umpire access to the Umpire Database.
SRQ49: ERIS should perform an operation to hide Umpire when it is stored in the Umpire Database.
SRQ50: ERIS should perform an operation to hide Umpire info when it is stored in the Umpire Database.
SRQ51: ERIS should perform an operation to hide Umpire access when it is stored in the Umpire Database.

Timetabling

The following represents the SREBP implementation on the Timetabling business process

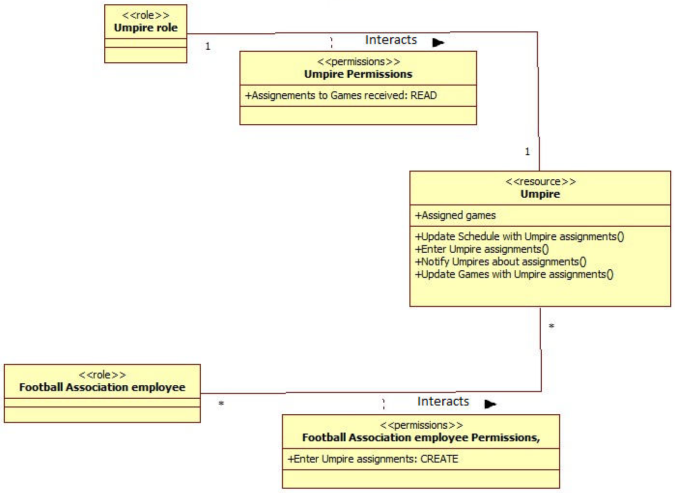

<<role>>
Umpire role
1
Interacts
<<permissions>>
Umpire Permissions
+Assignements to Games received: READ
1
<<resource>>
Umpire
+Assigned games
+Update Schedule with Umpire assignments()
+Enter Umpire assignments()
+Notify Umpires about assignments()
+Update Games with Umpire assignments()
*
<<role>>
Football Association employee
*
Interacts
<<permissions>>
Football Association employee Permissions,
+Enter Umpire assignments: CREATE

Figure A2 9 *Timetabling: Umpire RBAC model*

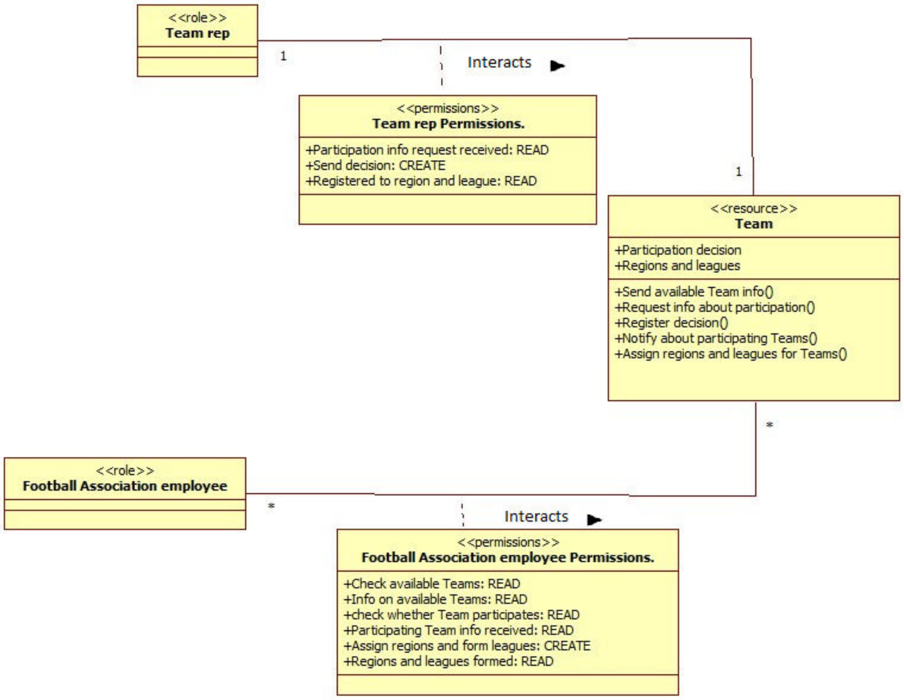

<<role>>
Team rep
1
Interacts
<<permissions>>
Team rep Permissions.
+Participation info request received: READ
+Send decision: CREATE
+Registered to region and league: READ
1
<<resource>>
Team
+Participation decision
+Regions and leagues
+Send available Team info()
+Request info about participation()
+Register decision()
+Notify about participating Teams()
+Assign regions and leagues for Teams()
*
<<role>>
Football Association employee
*
Interacts
<<permissions>>
Football Association employee Permissions.
+Check available Teams: READ
+Info on available Teams: READ
+check whether Team participates: READ
+Participating Team info received: READ
+Assign regions and form leagues: CREATE
+Regions and leagues formed: READ

Figure A2 10 *Timetabling, Team RBAC model*

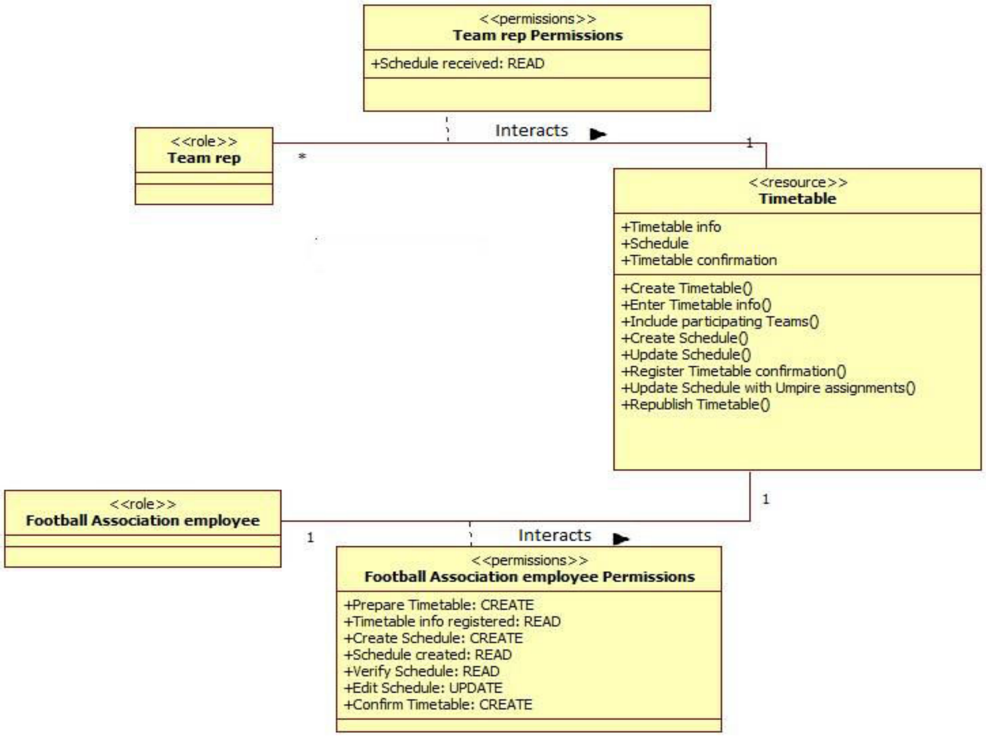


Figure A2 11 *Timetabling, Timetable RBAC model*

SRQ52: Football Association employee: should be able to: Create the Timetable, Schedule and Timetable confirmation.
SRQ53: Football Association employee: should be able to:
Read the Timetable info, Schedule and Timetable confirmation.
SRQ54: Football Association employee should be able to:
Update the Schedule.
SRQ55: Team representative should be able to:
Read the Schedule message.
SRQ56: Permission Prepare Timetable: CREATE should be given only to one user assigned to Football Association employee role. This user also receives the permissions Timetable info registered: READ, Create Schedule: CREATE, Schedule created: READ, Verify Schedule: READ, Edit Schedule: UPDATE and Confirm Timetable: CREATE.
SRQ57: Football Association employee: should be able to: Create the Regions and leagues.
SRQ58: Football Association employee: should be able to: Read the Participation decision and Regions and leagues.
SRQ59: Team rep should be able to: Create the Participation decision.
SRQ60: Team rep should be able to: Read the Participation decision and Regions and leagues.
SRQ61: Football Association employee: should be able to: Create the Assigned games.
SRQ62: The Umpire: should be able to:
Read the Assigned games.

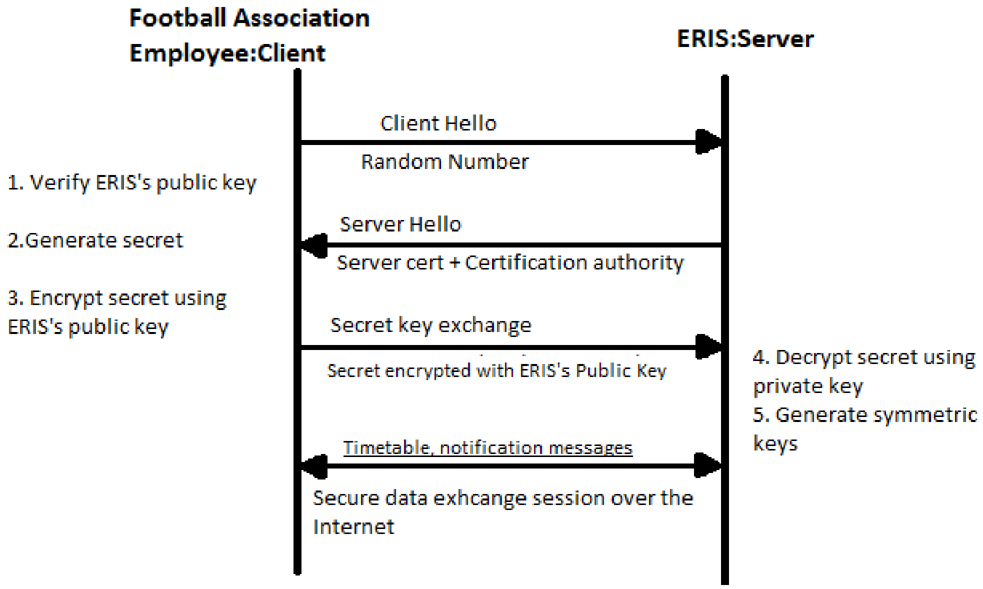

Football Association Employee:Client
ERIS:Server
Client Hello
Random Number
1. Verify ERIS's public key
2.Generate secret
3. Encrypt secret using ERIS's public key
Server Hello
Server cert + Certification authority
Secret key exchange
Secret encrypted with ERIS's Public Key
4. Decrypt secret using private key
5. Generate symmetric keys
Timetable, notification messages
Secure data exhcange session over the Internet

Figure A2 12 *TLS/SSL Protocol implementation, adapted from (Ahmed & Matulevičius, 2014)*

SRQ63: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority

SRQ64: Football Association employee should encrypt and sign the Timetable info, Schedule, Timetable confirmation, Regions and leagues and Umpire assignments (and notification messages) using the keys before sending it to ERIS.
SRQ65: Team rep should encrypt and sign the Participation decision (and notification messages) using the keys before sending it to ERIS.
SRQ66: Create Timetable interface should filter Timetable info and Schedule.
SRQ67: Create Timetable interface should sanitize the Timetable info and Schedule to transform it to the required format.
SRQ68: Create Timetable interface should canonicalize the Timetable info and Schedule to verify it against its canonical representation.
SRQ69: Send decision interface should filter Participation decision.
SRQ70: Send decision interface should sanitize the Participation decision to transform it to the required format.
SRQ71: Send decision interface should canonicalize the Participation decision to verify it against its canonical representation.
SRQ72: Enter Umpire assignments interface should filter Assigned games.
SRQ73: Enter Umpire assignments interface should sanitize the Assigned games to transform it to the required format.
SRQ74: Enter Umpire assignments interface should canonicalize the Assigned games to verify it against its canonical representation.

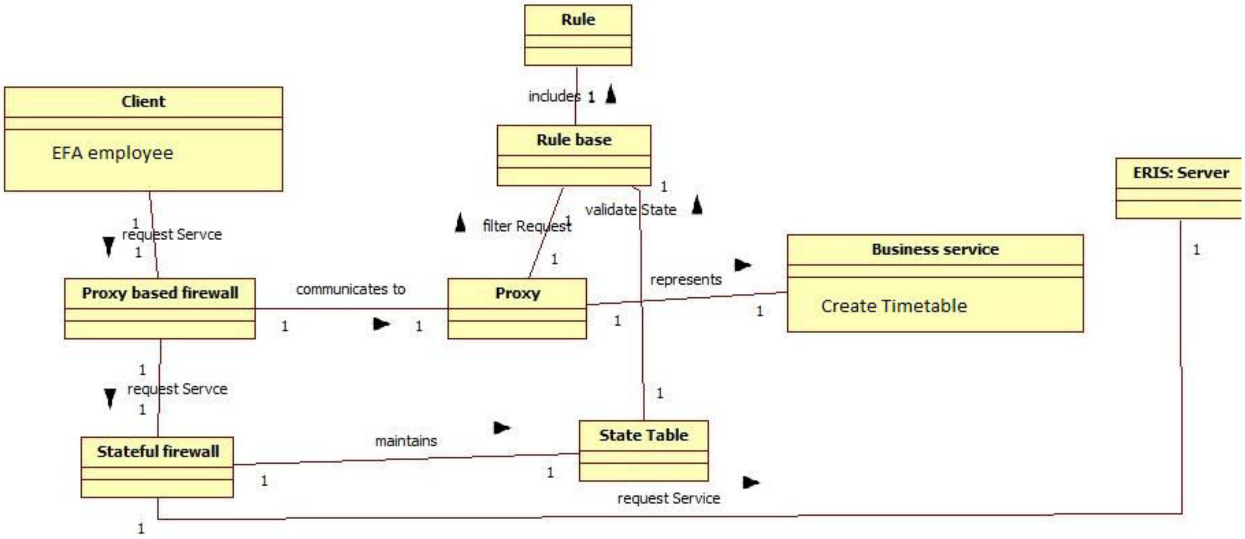


Figure A2 13 *Timetabling Network infrastructure model*

SRQ75: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQ76: Proxy based firewall should communicate to the proxy, which represents the Create

Timetable, to determine the validity of the Timetable info and Timetable confirmation received from the Football Association employee

SRQ77: Proxy based firewall should communicate to the proxy, which represents the Create Schedule, to determine the validity of the Schedule received from the Football Association employee.

SRQ88: Proxy based firewall should communicate to the proxy, which represents the Edit Schedule, to determine the validity of the Schedule received from the Football Association employee.

SRQ79: Proxy based firewall should communicate to the proxy, which represents the Confirm Timetable, to determine the validity of the Timetable confirmation received from the Football Association employee.

SRQ80: Proxy based firewall should communicate to the proxy, which represents the Assign regions and form leagues, to determine the validity of the Regions and leagues received from the Football Association employee.

SRQ81: Proxy based firewall should communicate to the proxy, which represents the Send decision, to determine the validity of the Participation decision received from the Team rep.

SRQ82: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.

SRQ83: Stateful firewall should maintain a state table to check the Team rep's requests for additional conditions of established communication.

SRQ84: ERIS should block all default incoming ports by default until these ports are explicitly opened.

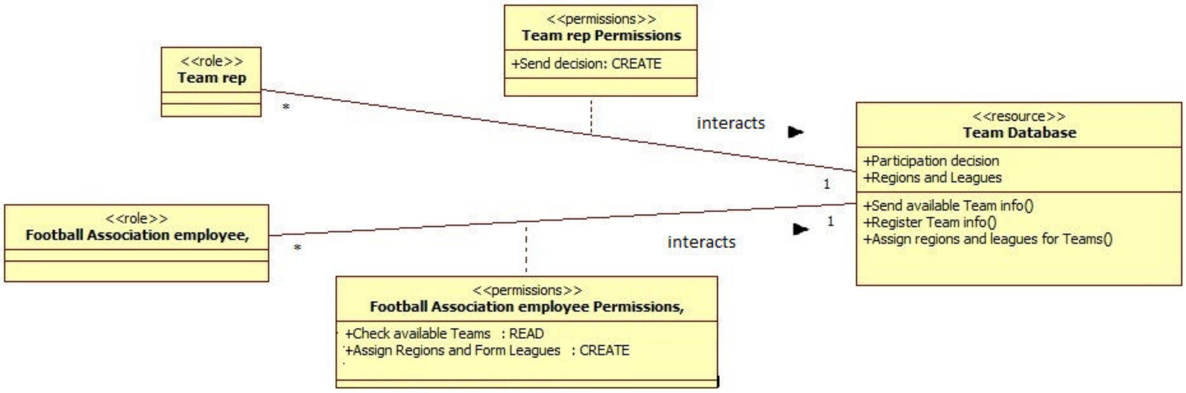

<<permissions>>
Team rep Permissions
+Send decision: CREATE
<<role>>
Team rep
*
interacts
<<resource>>
Team Database
+Participation decision
+Regions and Leagues
+Send available Team info()
+Register Team info()
+Assign regions and leagues for Teams()
1
1
<<role>>
Football Association employee,
*
interacts
<<permissions>>
Football Association employee Permissions,
+Check available Teams : READ
+Assign Regions and Form Leagues : CREATE

Figure A2 14 *Timetabling, Team Database RBAC model*

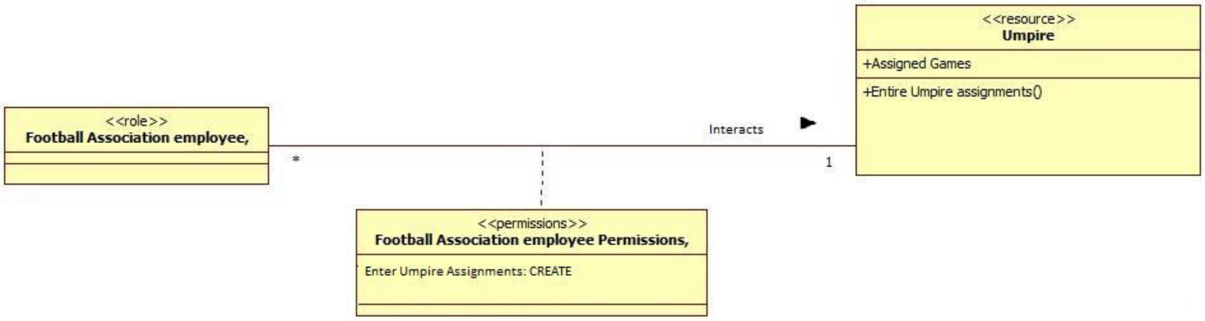

<<resource>>
Umpire
+Assigned Games
+Entire Umpire assignments()
<<role>>
Football Association employee,
Interacts
*
1
<<permissions>>
Football Association employee Permissions,
Enter Umpire Assignments: CREATE

Figure A2 15 *Timetabling, Umpire Database RBAC model*

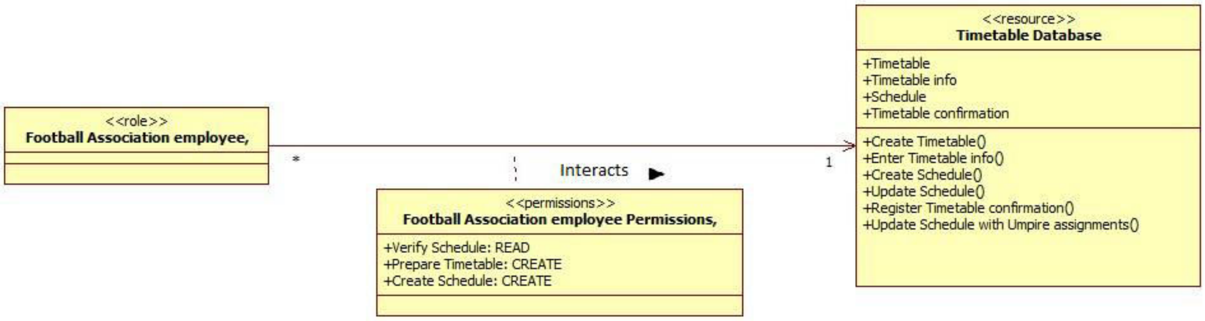


Figure A2 16 *Timetabling, Timetable Database RBAC model*

SRQ85: ERIS should audit the operations after the storage of Timetable, Timetable info, Schedule and Timetable confirmation in the Timetable Database.
SRQ86: ERIS should perform an operation to hide Timetable info when it is stored in the Timetable Database.
SRQ87: ERIS should perform an operation to hide Schedule when it is stored in the Timetable Database.

SRQ88: ERIS should perform an operation to hide Timetable confirmation when it is stored in the Timetable Database.
SRQ89: ERIS should audit the operations after the storage of Participation decision and Regions and leagues in the Team Database.
SRQ90: ERIS should perform an operation to hide Participation decision when it is stored in the Team Database.
SRQ91: ERIS should perform an operation to hide Regions and leagues when it is stored in the Team Database.
SRQ92: ERIS should audit the operations after the storage of Assigned games in the Umpire Database.
SRQ93: ERIS should perform an operation to hide Assigned games when it is stored in the Umpire Database.

Game report registration

The following represents the SREBP implementation on the Game report registration business process

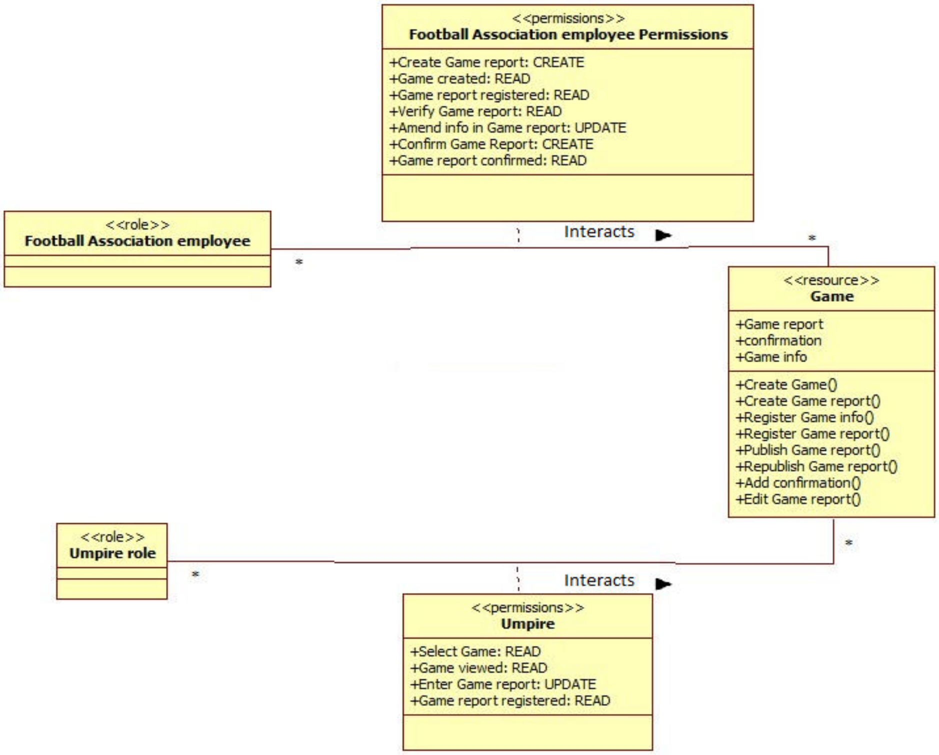


Figure A2 17 *Game report registration RBAC model*

SRQ94: Football Association employee: should be able to: Create the Game, Game report, Game confirmation, and Game info.
SRQ95: Football Association employee: should be able to: Read the Game, Game entry, Game

confirmation, Game report and Game info.
SRQ96: Umpire should be able to update the Game report.
SRQ97: Umpire should be able to read the Game report and Game info.
SRQ98: Permission Game report registered: READ should be given only to one user assigned to Football Association employee role. This user also receives the permissions Verify Game report: READ, Amend info in Game report: UPDATE, Confirm Game Report: CREATE and Game report confirmed: READ.
SRQ99: Permission Select Game: READ should be given only to one user assigned to Umpire role. This user also receives the permissions Game viewed: READ, Enter Game report: UPDATE and Game report

Registered: READ.

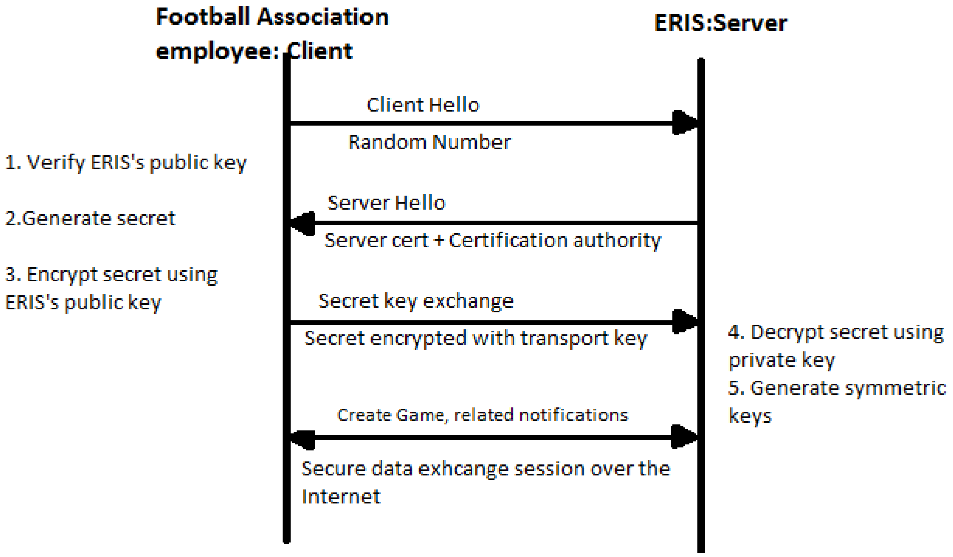

Football Association employee: Client
ERIS:Server
Client Hello
Random Number
1. Verify ERIS's public key
2.Generate secret
3. Encrypt secret using ERIS's public key
Server Hello
Server cert + Certification authority
Secret key exchange
Secret encrypted with transport key
4. Decrypt secret using private key
5. Generate symmetric keys
Create Game, related notifications
Secure data exhcange session over the Internet

Figure A2 18 *TLS/SSL Protocol implementation, adapted from (Ahmed & Matulevičius, 2014)*

SRQ100: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQ101: Football Association employee should encrypt and sign the Game, Game report, Confirmation and Game info (and notification messages) using the keys before sending it to ERIS.
SRQ102: Umpire should encrypt and sign the Game report (and notification messages) using the keys before sending it to ERIS.
SRQ103: Create Game interface should filter Game info, Confirmation and Game report.
SRQ104: Create Game interface should sanitize the Game info, Confirmation and Game report to transform it to the required format.
SRQ105: Create Game interface should canonicalize the Game info, Confirmation and Game report to verify it against its canonical representation.

SRQ106: Enter Game report interface should canonicalize the Game report to verify it against its canonical representation.
SRQ107: Enter Game interface should sanitize the Game report to transform it to the required format.
SRQ108: Enter Game interface should sanitize the Game report to transform it to the required format.

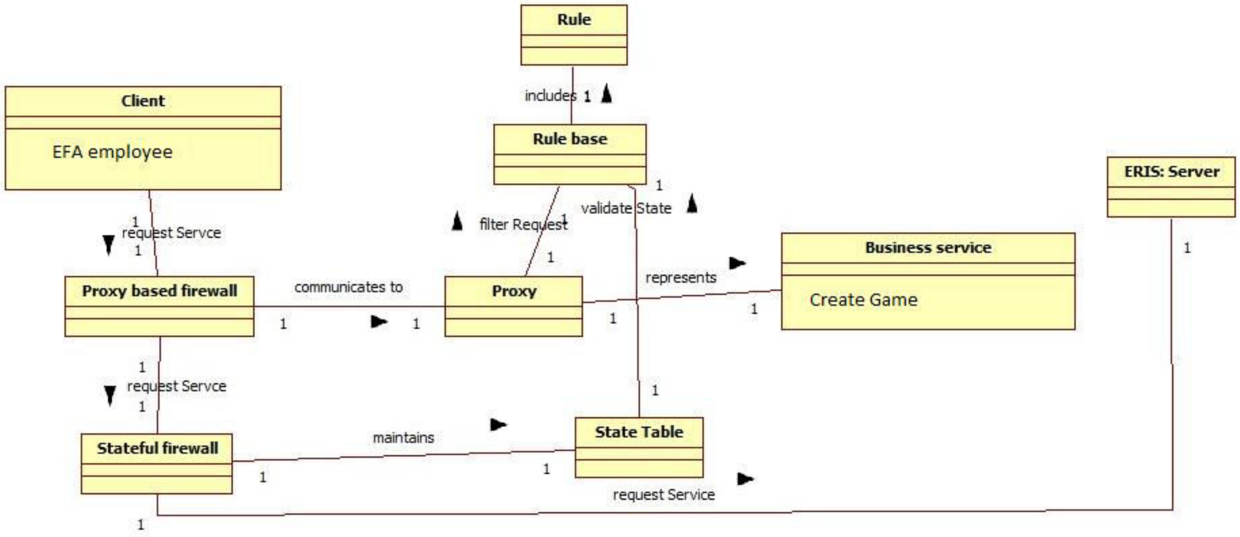


Figure A2 19 *Register game report Network infrastructure model*

SRQ109: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQ110: Proxy based firewall should communicate to the proxy, which represents the Create Game, to determine the validity of the Game info and Game report received from the Football Association employee
SRQ111: Proxy based firewall should communicate to the proxy, which represents the Enter Game report, to determine the validity of the Game report received from the Umpire.
SRQ112: Proxy based firewall should communicate to the proxy, which represents the Create Game report, to determine the validity of the Game report received from the Football Association employee.
SRQ113: Proxy based firewall should communicate to the proxy, which represents the Confirm Game report, to determine the validity of the Confirmation received from the Football Association employee.
SRQ114: Proxy based firewall should communicate to the proxy, which represents the Amend Game report, to determine the validity of the Game report received from the Football Association employee.

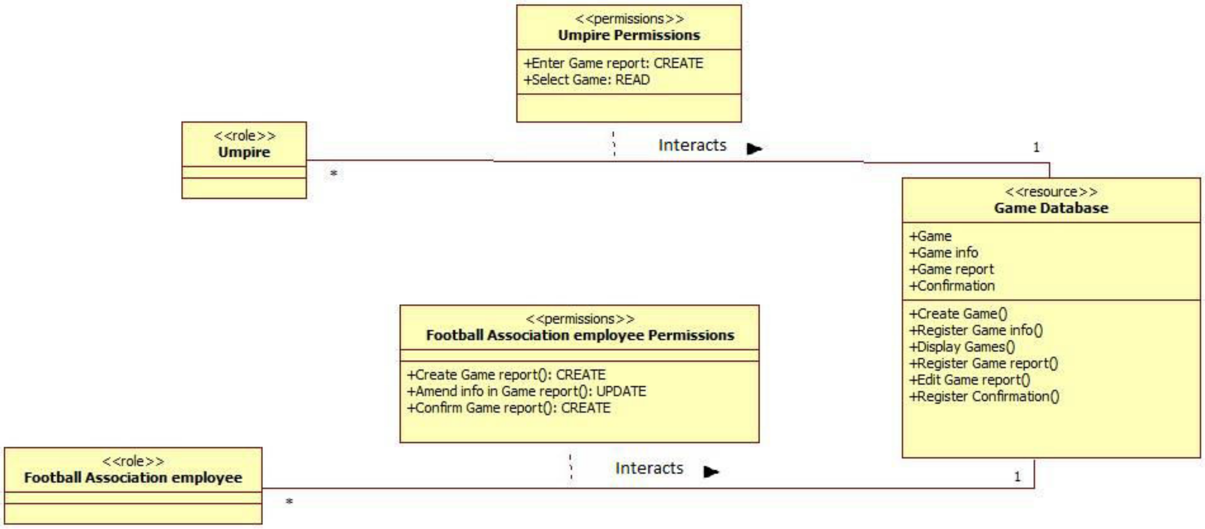


Figure A2 20 *Game report registration database RBAC model*

SRQ115: ERIS should audit the operations after the storage of Game, Game info, Game report and Confirmation.

SRQ116: ERIS should perform an operation to hide Game when it is stored in the Game Database.

SRQ117: ERIS should perform an operation to hide Game info when it is stored in the Game Database.

SRQ118: ERIS should perform an operation to hide Game report when it is stored in the Game Database.

SRQ119: ERIS should perform an operation to hide Confirmation when it is stored in the Game Database.

SRQ120: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.

SRQ121: Stateful firewall should maintain a state table to check the Umpire's requests for additional conditions of established communication.

SREBP security requirements categorization

The security requirements elicited in Appendix section A 2 were categorized and compiled into the following lists according to business assets.

Table A2 1: Player BA security requirements

Player	
SRQBA1:1	SRQ18: Football Association employee: should be able to Create the Player.
SRQBA1:2	SRQ19: Football Association employee: should be able to Read the Player info.
SRQBA1:3	SRQ20: The Player should be able to Read the Player info.
SRQBA1:4	SRQ21: The Team rep should be able to Read the Player info.
SRQBA1:5	SRQ22: Permission Info registered: READ should be given only to one user assigned to The Player role.
SRQBA1:6	SRQ23: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQBA1:7	SRQ24: Football Association employee should encrypt and sign the Player info (and notification messages) using the keys before sending it to ERIS.
SRQBA1:8	SRQ25: Create Player interface should filter Player info.
SRQBA1:9	SRQ26: Create Player interface should sanitize the Player info to transform it to the required format
SRQBA1:10	SRQ27: Create Player interface should canonicalize the Player info to verify it against its canonical representation.
SRQBA1:11	SRQ28: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQBA1:12	SRQ29: Proxy based firewall should communicate to the proxy, which represents the Create Player, to determine the validity of the Player info received from the Football Association employee
SRQBA1:13	SRQ30: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQBA1:14	SRQ31: ERIS should block all default incoming ports by default until these ports are explicitly opened.
SRQBA1:15	SRQ32: ERIS should audit the operations after the storage of Player and Player info to the Player Database.

SRQBA1:16	SRQ33: ERIS should perform an operation to hide Player when it is stored in the Player Database.
SRQBA1:17	SRQ34: ERIS should perform an operation to hide Player info when it is stored in the Player Database.
SRQBA1:18	SRQ34: ERIS should perform an operation to hide Player performance when it is stored in the Player Database.

Table A2 2: Team BA security requirements

Team	
SRQBA2:1	SRQ1: Football Association employee: should be able to: Create the Team
SRQBA2:2	SRQ2: Football Association employee: should be able to: Read the Team info and Team rep.
SRQBA2:3	SRQ3: Team representative should be able to: Read the Team info and Team rep.
SRQBA2:4	SRQ4: Permission Access to Team received: READ should be given only to one user assigned to Team Rep. This user also receives permission Update Team info: UPDATE.
SRQBA2:5	SRQ5: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQBA2:6	SRQ6: Football Association employee should encrypt and sign the Team info (and notification messages) using the keys before sending it to ERIS.
SRQBA2:7	SRQ7: Create Team interface should filter Team info.
SRQBA2:8	SRQ8: Create Team interface should sanitize the Team info to transform it to the required format
SRQBA2:9	SRQ9: Create Team interface should canonicalize the Team info to verify it against its canonical representation.
SRQBA2:10	SRQ10: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQBA2:11	SRQ11: Proxy based firewall should communicate to the proxy, which represents the Create Team, to determine the validity of the Team info received from the Football association employee
SRQBA2:12	SRQ12: Stateful firewall should maintain a state table to check the Football association employee's requests for additional conditions of established communication.
SRQBA2:13	SRQ13: ERIS should block all default incoming ports by default until these ports are explicitly opened.
SRQBA2:14	SRQ14: ERIS should audit the operations after the storage of Team,

	Team info and Team rep to the Team Database.
SRQBA2:15	SRQ15: ERIS should perform an operation to hide Team when it is stored in the Team Database.
SRQBA2:16	SRQ16: ERIS should perform an operation to hide Team info when it is stored in the Team Database.
SRQBA2:17	SRQ17: ERIS should perform an operation to hide Team rep when it is stored in the Team Database.
SRQBA2:18	SRQ57: Football Association employee: should be able to: Create the Regions and leagues.
SRQBA2:19	SRQ58: Football Association employee: should be able to: Read the Participation decision and Regions and leagues.
SRQBA2:20	SRQ59: Team rep should be able to: Create the Participation decision.
SRQBA2:21	SRQ60: Team rep should be able to: Read the Participation decision and Regions and leagues.
SRQBA2:22	SRQ64: Football Association employee should encrypt and sign the Timetable info, Schedule, Timetable confirmation, Regions and leagues and Umpire assignments (and notification messages) using the keys before sending it to ERIS.
SRQBA2:23	SRQ65: Team rep should encrypt and sign the Participation decision (and notification messages) using the keys before sending it to ERIS.
SRQBA2:24	SRQ69: Send decision interface should filter Participation decision.
SRQBA2:25	SRQ70: Send decision interface should sanitize the Participation decision to transform it to the required format.
SRQBA2:26	SRQ71: Send decision interface should canonicalize the Participation decision to verify it against its canonical representation.
SRQBA2:27	SRQ80: Proxy based firewall should communicate to the proxy, which represents the Assign regions and form leagues, to determine the validity of the Regions and leagues received from the Football Association employee.
SRQBA2:28	SRQ83: Stateful firewall should maintain a state table to check the Team rep's requests for additional conditions of established communication.
SRQBA2:29	SRQ81: Proxy based firewall should communicate to the proxy, which represents the Send decision, to determine the validity of the Participation decision received from the Team rep.
SRQBA2:30	SRQ89: ERIS should audit the operations after the storage of Participation decision and Regions and leagues in the Team Database.
SRQBA2:31	SRQ90: ERIS should perform an operation to hide Participation decision when it is stored in the Team Database.

SRQBA2:32	SRQ91: ERIS should perform an operation to hide Regions and leagues when it is stored in the Team Database.

Table A2 3: Umpire BA security requirements

Umpire	
SRQBA3:1	SRQ35: Football Association employee: should be able to: Create the Umpire .
SRQBA3:2	SRQ36: Football Association employee: should be able to: Read the Umpire info and Umpire access.
SRQBA3:3	SRQ37: Umpire should be able to: Read the Umpire info and Umpire info message.
SRQBA3:4	SRQ38: Permission Umpire access received: READ should be given only to one user assigned to The Umpire role.
SRQBA3:5	SRQ39: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQBA3:6	SRQ40: Football Association employee should encrypt and sign the Umpire info (and notification messages) using the keys before sending it to ERIS.
SRQBA3:7	SRQ41: Create Umpire interface should filter Umpire info.
SRQBA3:8	SRQ42: Create Umpire interface should sanitize the Umpire info to transform it to the required format.
SRQBA3:9	SRQ43: Create Umpire interface should canonicalize the Umpire info to verify it against its canonical representation.
SRQBA3:10	SRQ44: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQBA3:11	SRQ45: Proxy based firewall should communicate to the proxy, which represents the Create Umpire, to determine the validity of the Umpire info received from the Football Association employee
SRQBA3:12	SRQ46: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQBA3:13	SRQ47: ERIS should block all default incoming ports by default until these ports are explicitly opened.
SRQBA3:14	SRQ48: ERIS should audit the operations after the storage of Umpire, Umpire info and Umpire access to the Umpire Database.

SRQBA3:15	SRQ49: ERIS should perform an operation to hide Umpire when it is stored in the Umpire Database.
SRQBA3:16	SRQ50: ERIS should perform an operation to hide Umpire info when it is stored in the Umpire Database.
SRQBA3:17	SRQ51: ERIS should perform an operation to hide Umpire access when it is stored in the Umpire Database.
SRQBA3:18	SRQ61: Football Association employee: should be able to: Create the Assigned games.
SRQBA3:19	SRQ62: The Umpire: should be able to: Read the Assigned games.
SRQBA3:20	SRQ64: Football Association employee should encrypt and sign the Timetable info, Schedule, Timetable confirmation, Regions and leagues and Umpire assignments (and notification messages) using the keys before sending it to ERIS.
SRQBA3:21	SRQ72: Enter Umpire assignments interface should filter Assigned games.
SRQBA3:22	SRQ73: Enter Umpire assignments interface should sanitize the Assigned games to transform it to the required format.
SRQBA3:23	SRQ74: Enter Umpire assignments interface should canonicalize the Assigned games to verify it against its canonical representation.
SRQBA3:24	SRQ92: ERIS should audit the operations after the storage of Assigned games in the Umpire Database.
SRQBA3:25	SRQ93: ERIS should perform an operation to hide Assigned games when it is stored in the Umpire Database.

Table A2 4: Game BA security requirements

Game	
SRQBA4:1	SRQ94: Football Association employee: should be able to: Create the Game, Game report, Game confirmation, and Game info.
SRQBA4:2	SRQ95: Football Association employee: should be able to: Read the Game, Game entry, Game confirmation, Game report and Game info.
SRQBA4:3	SRQ96: Umpire should be able to update the Game report.
SRQBA4:4	SRQ97: Umpire should be able to read the Game report and Game info.
SRQBA4:5	SRQ98: Permission Game report registered: READ should be given only to one user assigned to Football Association employee role. This user also

	receives the permissions Verify Game report: READ, Amend info in Game report: UPDATE, Confirm Game Report: CREATE and Game report confirmed: READ.
SRQBA4: 6	SRQ99: Permission Select Game: READ should be given only to one user assigned to Umpire role. This user also receives the permissions Game viewed: READ, Enter Game report: UPDATE and Game report registered: READ.
SRQBA4: 7	SRQ100: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQBA4: 8	SRQ101: Football Association employee should encrypt and sign the Game, Game report, Confirmation and Game info (and notification messages) using the keys before sending it to ERIS.
SRQBA4: 9	SRQ102: Umpire should encrypt and sign the Game report (and notification messages) using the keys before sending it to ERIS.
SRQBA4: 10	SRQ103: Create Game interface should filter Game info, Confirmation and Game report.
SRQBA4: 11	SRQ104: Create Game interface should sanitize the Game info, Confirmation and Game report to transform it to the required format.
SRQBA4: 12	SRQ105: Create Game interface should canonicalize the Game info, Confirmation and Game report to verify it against its canonical representation.
SRQBA4: 13	SRQ106: Enter Game report interface should canonicalize the Game report to verify it against its canonical representation.
SRQBA4: 14	SRQ107: Enter Game interface should sanitize the Game report to transform it to the required format.
SRQBA4: 15	SRQ108: Enter Game interface should sanitize the Game report to transform it to the required format.
SRQBA4: 16	SRQ109: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQBA4: 17	SRQ110: Proxy based firewall should communicate to the proxy, which represents the Create Game, to determine the validity of the Game info and Game report received from the Football Association employee
SRQBA4: 18	SRQ111: Proxy based firewall should communicate to the proxy, which represents the Enter Game report, to determine the validity of the Game report received from the Umpire.
SRQBA4: 19	SRQ112: Proxy based firewall should communicate to the proxy, which represents the Create Game report, to determine the validity of the Game report received from the Football Association employee.
SRQBA4:	SRQ113: Proxy based firewall should communicate to the proxy, which

20	represents the Confirm Game report, to determine the validity of the Confirmation received from the Football Association employee.
SRQBA4: 21	SRQ114: Proxy based firewall should communicate to the proxy, which represents the Amend Game report, to determine the validity of the Game report received from the Football Association employee.
SRQBA4: 22	SRQ115: ERIS should audit the operations after the storage of Game, Game info, Game report and Confirmation.
SRQBA4: 23	SRQ116: ERIS should perform an operation to hide Game when it is stored in the Game Database.
SRQBA4: 24	SRQ117: ERIS should perform an operation to hide Game info when it is stored in the Game Database.
SRQBA4: 25	SRQ118: ERIS should perform an operation to hide Game report when it is stored in the Game Database.
SRQBA4: 26	SRQ119: ERIS should perform an operation to hide Confirmation when it is stored in the Game Database.
SRQBA4: 27	SRQ120: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQBA4: 28	SRQ121: Stateful firewall should maintain a state table to check the Umpire's requests for additional conditions of established communication.
SRQBA4: 29	SRQ47: ERIS should block all default incoming ports by default until these ports are explicitly opened.

Table A2 5: Timetable BA security requirements

Timetable	
SRQBA5: 1	SRQ52: Football Association employee: should be able to: Create the Timetable, Schedule and Timetable confirmation.
SRQBA5: 2	SRQ53: Football Association employee: should be able to: Read the Timetable info, Schedule and Timetable confirmation.
SRQBA5: 3	SRQ54: Football Association employee should be able to: Update the Schedule.
SRQBA5: 4	SRQ55: Team representative should be able to: Read the Schedule
SRQBA5: 5	SRQ56: Permission Prepare Timetable: CREATE should be given only to one user assigned to Football Association employee role. This user also receives the permissions Timetable info registered: READ, Create Schedule: CREATE, Schedule created: READ, Verify Schedule: READ, Edit

	Schedule: UPDATE and Confirm Timetable: CREATE.
SRQBA5: 6	SRQ63: ERIS should have a unique identity in the form of key pairs (public and private keys) certified by a certification authority
SRQBA5: 7	SRQ64: Football Association employee should encrypt and sign the Timetable info, Schedule, Timetable confirmation, Regions and leagues and Umpire assignments (and notification messages) using the keys before sending it to ERIS.
SRQBA5: 8	SRQ65: Team rep should encrypt and sign the Participation decision (and notification messages) using the keys before sending it to ERIS.
SRQBA5: 9	SRQ66: Create Timetable interface should filter Timetable info and Schedule.
SRQBA5: 10	SRQ67: Create Timetable interface should sanitize the Timetable info and Schedule to transform it to the required format.
SRQBA5: 11	SRQ68: Create Timetable interface should canonicalize the Timetable info and Schedule to verify it against its canonical representation.
SRQBA5: 12	SRQ75: ERIS should establish a rule base to communicate with business partners such as Football Association employee.
SRQBA5: 13	SRQ76: Proxy based firewall should communicate to the proxy, which represents the Create Timetable, to determine the validity of the Timetable info and Timetable confirmation received from the Football Association employee
SRQBA5: 14	SRQ77: Proxy based firewall should communicate to the proxy, which represents the Create Schedule, to determine the validity of the Schedule received from the Football Association employee.
SRQBA5: 15	SRQ78: Proxy based firewall should communicate to the proxy, which represents the Edit Schedule, to determine the validity of the Schedule received from the Football Association employee.
SRQBA5: 16	SRQ79: Proxy based firewall should communicate to the proxy, which represents the Confirm Timetable, to determine the validity of the Timetable confirmation received from the Football Association employee.
SRQBA5: 17	SRQ82: Stateful firewall should maintain a state table to check the Football Association employee's requests for additional conditions of established communication.
SRQBA5: 18	SRQ85: ERIS should audit the operations after the storage of Timetable, Timetable info, Schedule and Timetable confirmation in the Timetable Database.
SRQBA5: 19	SRQ86: ERIS should perform an operation to hide Timetable info when it is stored in the Timetable Database.
SRQBA5:	SRQ87: ERIS should perform an operation to hide Schedule when it is

20	stored in the Timetable Database.
SRQBA5: 21	SRQ88: ERIS should perform an operation to hide Timetable confirmation when it is stored in the Timetable Database.
SRQBA5: 22	SRQ47: ERIS should block all default incoming ports by default until these ports are explicitly opened.

Section A3: SQUARE implementation

This section covers the security requirements elicitation section for SQUARE

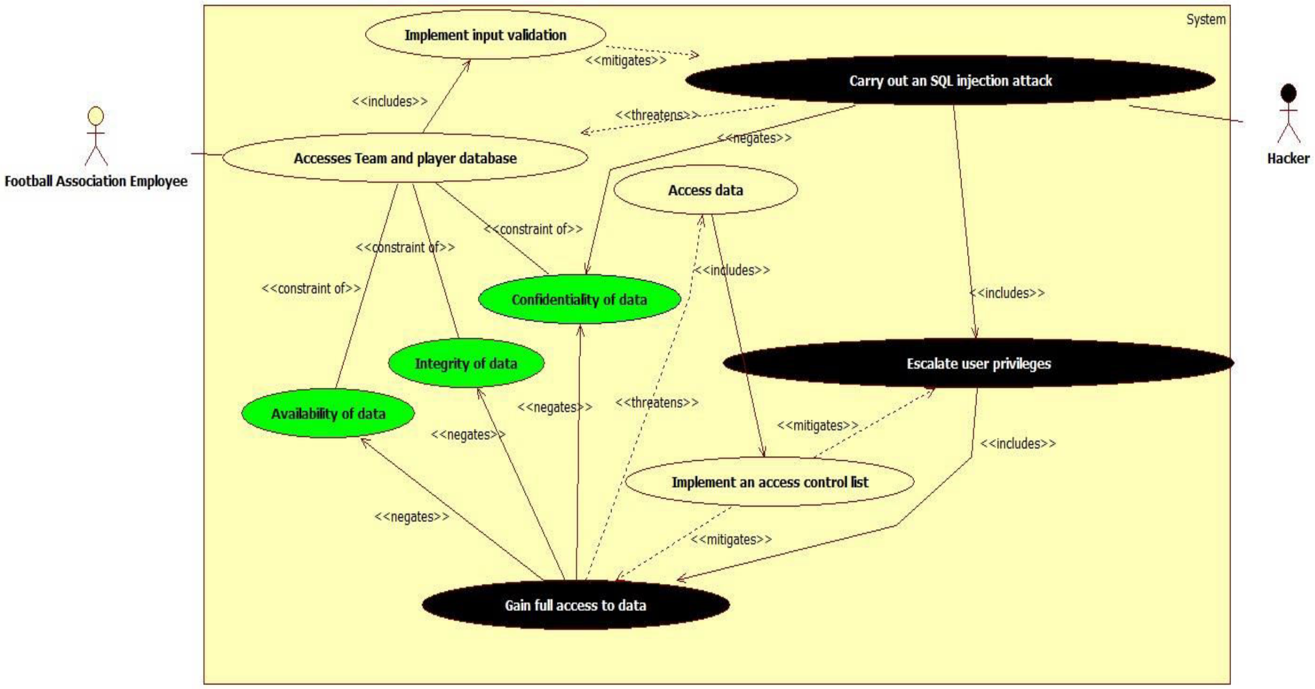


Figure A2 1: Misuse cases diagram for BA1 and BA2 – SQL and privilege escalation

Table A3 1 : SQL injection

Business asset	Player, Team, Game
	Asset related concepts
Risk ID	**R3**
IS Asset	**Team and player Database**
Security criterion	Confidentiality of the business assets
	Risk related concepts
Risk	Hacker carries out an SQL injection attack and gains access to the database thus negating the confidentiality of the business assets
Impact	Loss of confidentiality of the business assets
Event	Hacker carries out an SQL injection attack and is able to gain access to the database
Vulnerability	No input sanitization or canonicalization of inputs
Threat agent	Hacker
Threat	Hacker can carry out an SQL injection to gain access to the database
Attack method	SQL injection
	Risk Treatment related concepts
Security requirement	An access control list (ACL) should be implemented
Security requirement ID	**SRQ3**
Control	Implement an ACL.
Cost of control	**0-500 EUR**

Table A3 2: Escalation of privileges

Business asset	Player, Team,Game
	Asset related concepts
Risk ID	**R4**
IS Asset	**Team and player Database**
Security criterion	CIA of the business assets
	Risk related concepts
Risk	Hacker escalates their privileges on the database, thereby gaining full root access to the database, allowing them to access, view, modify and delete all the data and negate the CIA of the business assets.
Impact	Loss of CIA of the business assets
Event	Hacker escalates their privileges and gains full root access to the database due to no access control lists being in place
Vulnerability	No set access control lists.
Threat agent	Hacker
Threat	Hacker is able to escalate their privileges to gain full root access to the database
Attack method	Escalation of privileges

Risk Treatment related concepts	
Security requirement	Input sanitization, canonicalization and validation should be implemented.
Security requirement ID	**SRQ4**
Control	Implement input sanitization and canonicalization
Cost of control	**0-1000 EUR**

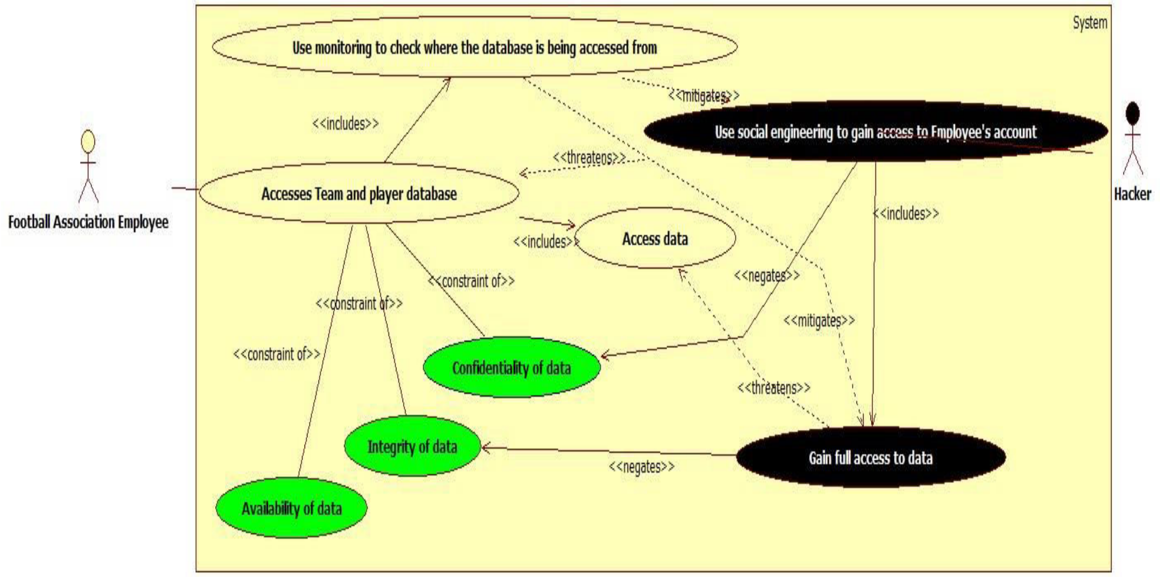


Figure A2 2: Misuse cases diagram for BA1 and BA2 – Social engineering

Table A3 3: Social engineering

Business asset	Player, Team, Game
	Asset related concepts
Risk ID	**R5**
IS Asset	**Team and player Database**
Security criterion	C and I of the business assets
	Risk related concepts
Risk	Hacker uses social engineering/phishing to gain access to the Football Association employee's computer as the employee has not been trained to detect social engineering attempts. The hacker is able to gain full access to the database through the Football Association employee's computer
Impact	Loss of C and I of the business assets
Event	Hacker uses social engineering (phishing for example) to gain access to their computer and thereby access the database
Vulnerability	No anti-social engineering training
Threat agent	Hacker
Threat	Hacker is able to use social engineering on one of the Football Association employees
Attack method	Social engineering
	Risk Treatment related concepts
Security requirement	social engineering training for employees should be implemented
Security requirement ID	**SRQ5**
Control	Implement social engineering awareness training for employees
Cost of control	**50 EUR per employee**

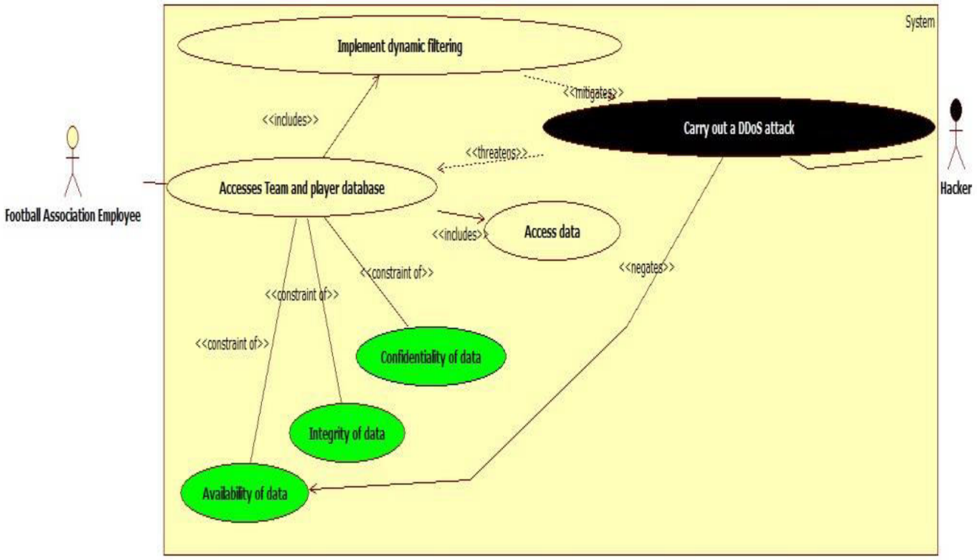


Figure A2 3: Misuse cases diagram for BA1 and BA2 – DDoS attack

Table A3 4: DDoS attack

Business asset	Player, Team, Game
	Asset related concepts
Risk ID	**R6**
IS Asset	**Team and player Database**
Security criterion	Availability of the business assets
	Risk related concepts
Risk	Hacker launches a DDoS attack against the databases as no countermeasures have been set up to mitigate this. This leads to the service being unavailable for the users.
Impact	Loss of availability of the data
Event	Hacker attacks the databases using DDoS as no ip address filtering is set in place
Vulnerability	No countermeasures set up, no ip address filtering.
Threat agent	Hacker with a botnet
Threat	A hacker launching a DDoS attack against the databases
Attack method	Distributed Denial of Service attack (DDoS)
	Risk Treatment related concepts
Security requirement	ACL and dynamic ip filtering should be implemented
Security requirement ID	**SRQ6**
Control	Implement an ACL
Cost of Control	**0 to 500 EUR**

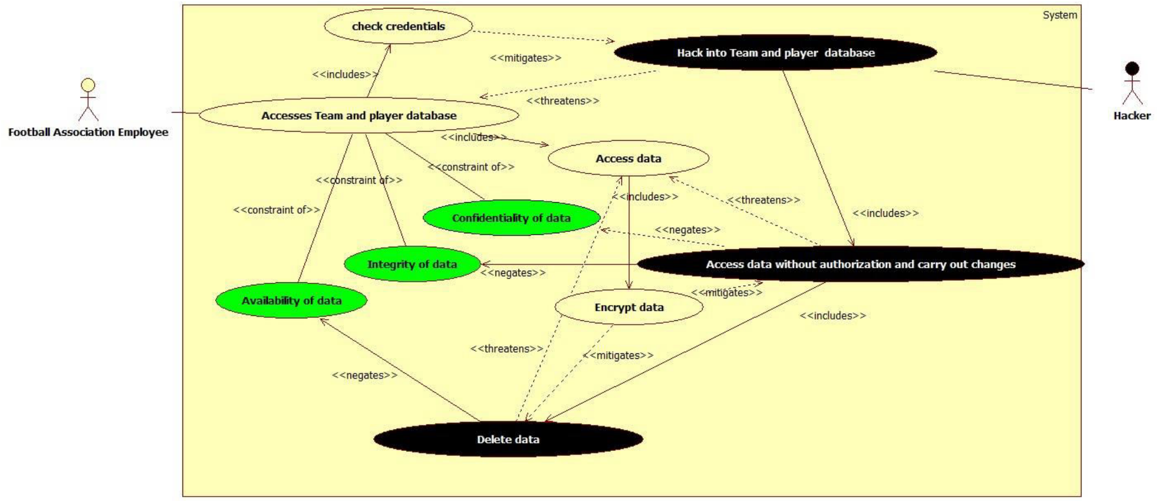


Figure A2 4: Misuse cases diagram for BA1 and BA2 – Unauthorized data manipulation

Table A3 5: Unauthorized data manipulation

Business asset	Player, Team, Game
	Asset related concepts
Risk ID	**R7**
IS Asset	**Team and player database**
Security criterion	CIA of the business assets
	Risk related concepts
Risk	Hacker hacks into the database and is able to access and view the unencrypted data which leads to the loss of CIA of the data.
Impact	Loss of CIA of the data
Event	Hacker hacks into the database and is able to read the data as it is saved in plaintext
Vulnerability	No encryption of data
Threat agent	Hacker
Threat	A hacker is able to hack into the database and freely read data
Attack method	Hacking into the database
	Risk Treatment related concepts
Security requirement	Data stored in the database should be encrypted
Security requirement ID	**SRQ7**
Control	Implement data encryption
Cost of Control	**0 EUR**

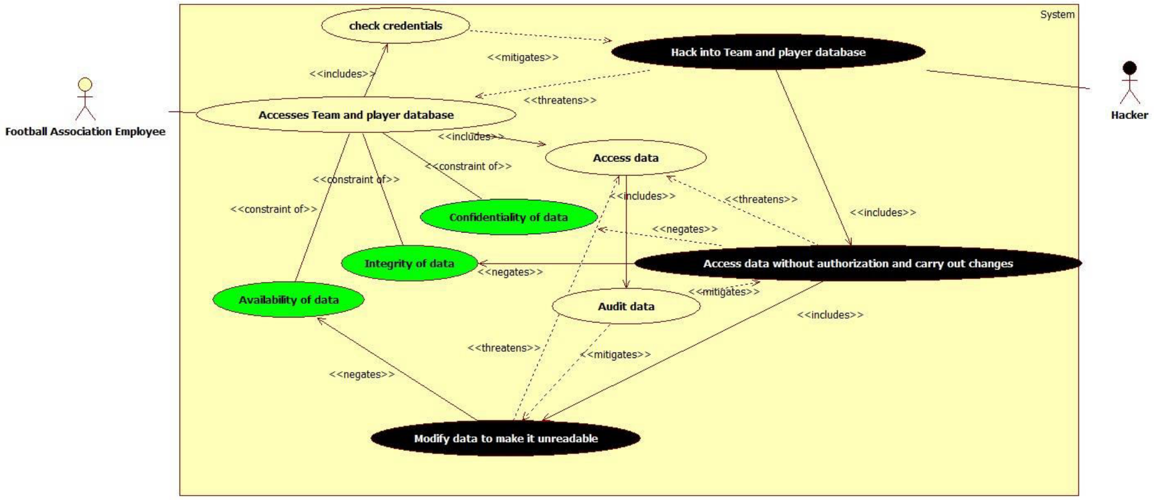


Figure A2 5: Misuse cases diagram for BA1 and BA2 – Unauthorized data manipulation

Table A3 6: Hacker changes team information before league entry is created.

Business asset	Player, Team, Game
	Asset related concepts
Risk ID	**R8**
IS Asset	**Team and player database**
Security criterion	Confidentiality of the makeup of the league, which teams will play etc. Integrity of the composition of the league.
	Risk related concepts
Risk	Hacker is able to hack the Team and player database and modify the data before league entries are created, resulting in incorrect league entries to be created which result in the loss of integrity of the data
Impact	Loss of integrity of the business asset.
Event	Hacker is able to access the database and change the data entry causing incorrect league entry to be created
Vulnerability	No auditing of the team information before league entry creation.
Threat agent	Hacker
Threat	Hacker is able to hack the Team and player database and modify data
Attack method	Hacking the Team and player database and modifying data
	Risk Treatment related concepts
Security requirement	The entries in the database should be audited regularly.
Security requirement ID	**SRQ8**
Control	Implement regular database auditing
Cost of control	**1000 – 5000 EUR**

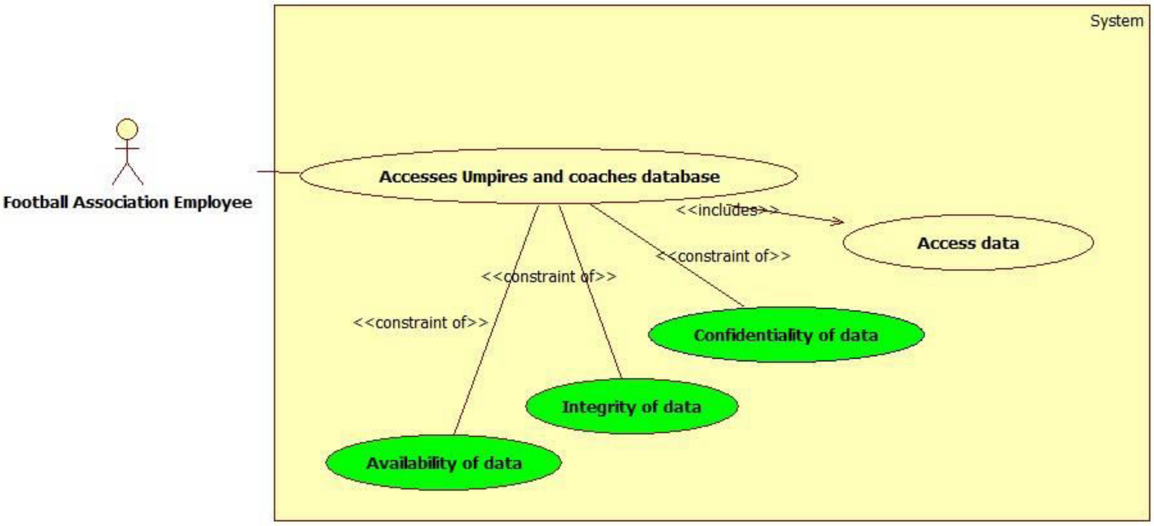


Figure A2 6: Use cases diagram for BA3

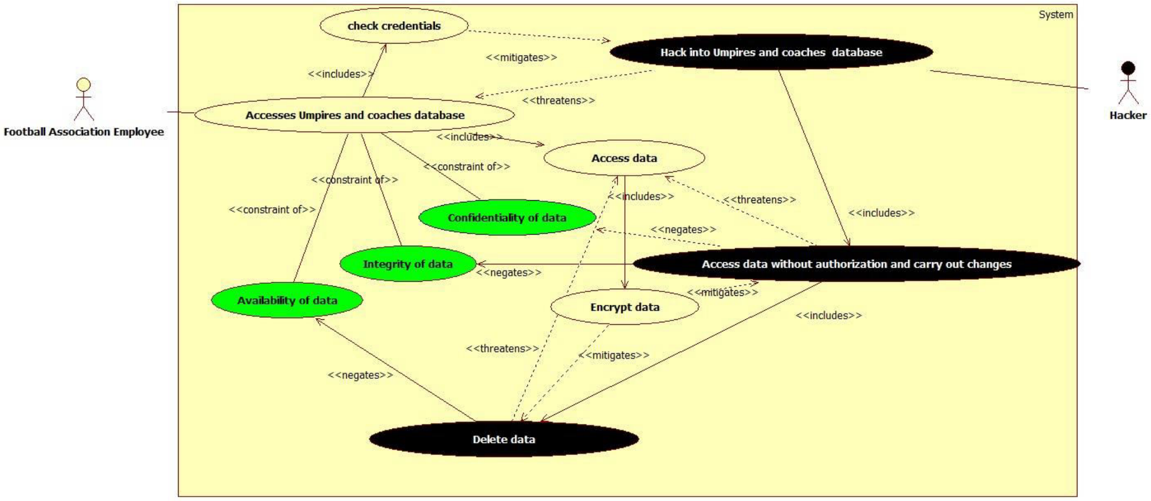


Figure A2 7: Misuse cases diagram for BA3 – Hacking and unauthorized data deletion

Table A3 7: Unauthorized data manipulation

Business asset	Umpire
	Asset related concepts
Risk ID	**R9**
IS Asset	**Umpires and coaches database**
Security criterion	CIA of the business assets
	Risk related concepts
Risk	Hacker hacks into the database and is able to access and view the unencrypted data which leads to the loss of CIA of the data.
Impact	Loss of CIA of the data
Event	Hacker hacks into the database and is able to read the data as it is saved in plaintext
Vulnerability	No encryption of data
Threat agent	Hacker
Threat	A hacker is able to hack into the database and freely read data
Attack method	Hacking into the database
	Risk Treatment related concepts
Security requirement	Data stored in the database should be encrypted
Security requirement ID	**SRQ9**
Control	Implement data encryption
Cost of Control	**0 EUR**

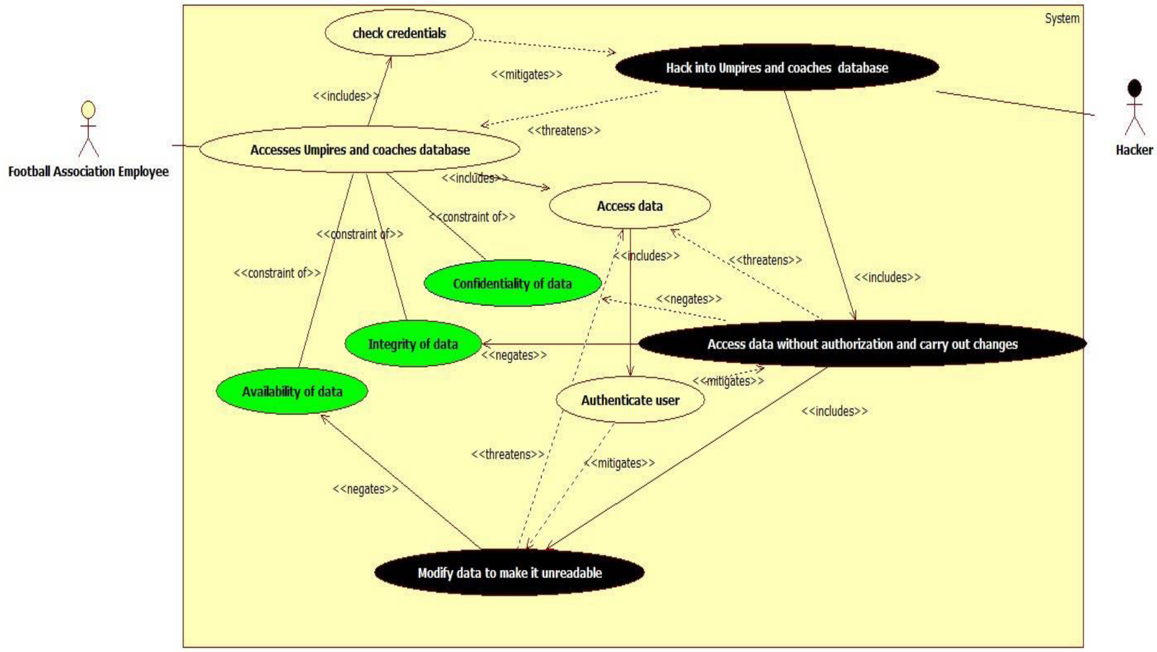


Figure A2 8: cases diagram for BA3– Hacking and unauthorized access

Table A3 8: Hacker accessing and modifying the Team and player database

Business asset	Umpire
	Asset related concepts
Risk ID	**R10**
IS Asset	**Umpire and coaches database**
Security criterion	Confidentiality of the Umpire’s personal information.
	Risk related concepts
Risk	Hacker hacks into the database thus negating the confidentiality of the data.
Impact	Loss of confidentiality of the business asset.
Event	Hacker hacks into the database due to user permissions not being checked when data is accessed
Vulnerability	User permissions are not checked when data is accessed.
Threat agent	Hacker
Threat	Hacker is able to hack into the database
Attack method	Hacking the Team and player database
	Risk Treatment related concepts
Security requirement	Only authorized personnel should be able to access the database. User credentials must be checked
Security requirement ID	**SRQ10**
Control	Implementation of Estonian national ID card authentication software
Cost of control	**500 EUR**

Table A3 9: Hacker hacks into the Umpire and coaches database to manipulate umpire's information.

Business asset	Umpire
	Asset related concepts
Risk ID	**R11**
IS Asset	**Umpire and coaches database**
Security criterion	Availability and integrity of the Umpire's information.
	Risk related concepts
Risk	Hacker hacks into the database and changes data thus negating the availability and integrity of the data.
Impact	Loss of availability and integrity of the business asset.
Event	Hacker hacks into the database and changes the data.
Vulnerability	User permissions are not checked when data is being modified.
Threat agent	Hacker
Threat	Hacker can hack into the database and change data.
Attack method	Hacking the Team and player database
	Risk Treatment related concepts
Security requirement	Authentication should be implemented when data is being modified.
Security requirement ID	**SRQ11**
Control	Implement authentication software
Cost of control	**0-1000 EUR**

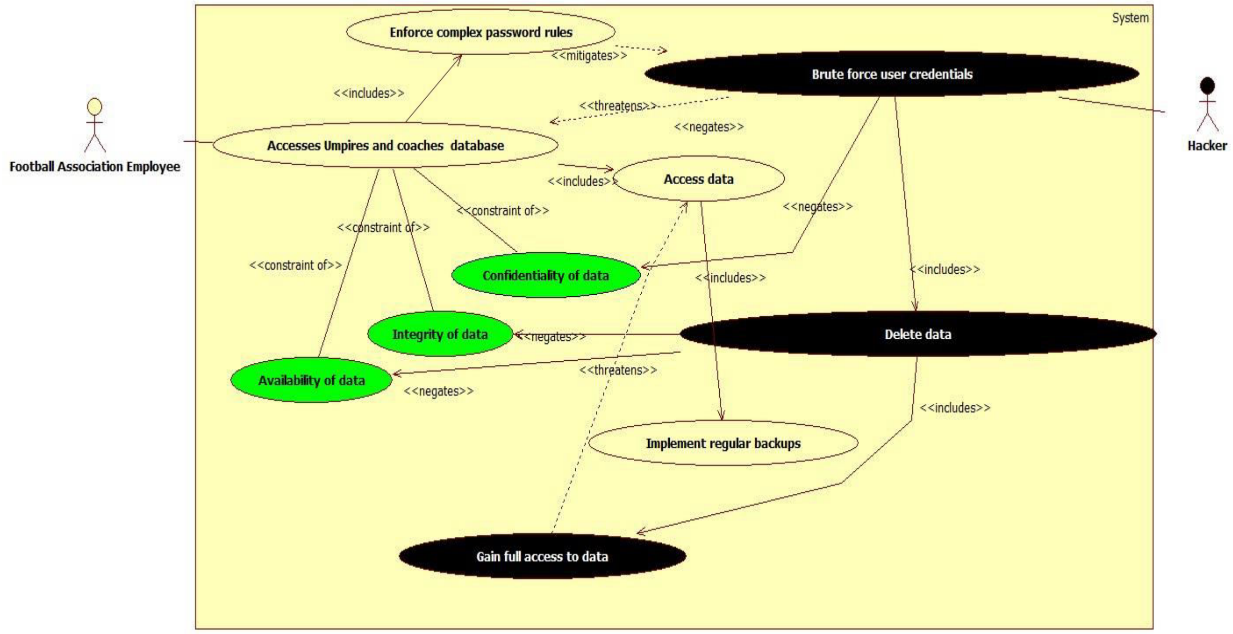


Figure A2 9: Misuse cases diagram for BA3 – SQL and privilege escalation

Table A3 10: SQL injection

Business asset	Umpire
	Asset related concepts
Risk ID	**R12**
IS Asset	**Umpire and coaches database**
Security criterion	Confidentiality of the business assets
	Risk related concepts
Risk	Hacker carries out an SQL injection attack and gains access to the database thus negating the confidentiality of the business assets
Impact	Loss of confidentiality of the business assets
Event	Hacker carries out an SQL injection attack and is able to gain access to the database
Vulnerability	No input sanitization or canonicalization of inputs
Threat agent	Hacker
Threat	Hacker can carry out an SQL injection to gain access to the database
Attack method	SQL injection
	Risk Treatment related concepts
Security requirement	Input sanitization, canonicalization and validation has to be implemented.
Security requirement ID	**SRQ12**

Table A3 11: Escalation of privileges

Business asset	Umpire
	Asset related concepts
Risk ID	**R13**
IS Asset	**Umpire and coaches database**
Security criterion	CIA of the business assets
	Risk related concepts
Risk	Hacker escalates their privileges on the database, thereby gaining full root access to the database, allowing them to access, view, modify and delete all the data and negate the CIA of the business assets.
Impact	Loss of CIA of the business assets
Event	Hacker escalates their privileges and gains full root access to the database due to no access control lists being in place
Vulnerability	No set access control lists.
Threat agent	Hacker
Threat	Hacker is able to escalate their privileges to gain full root access to the database
Attack method	Escalation of privileges
	Risk Treatment related concepts

Security requirement	An access control list (ACL) should be implemented
Security requirement ID	**SRQ13**
Control	Implement an ACL.
Cost of control	**0-500 EUR**
Security requirement	An access control list (ACL) should be implemented

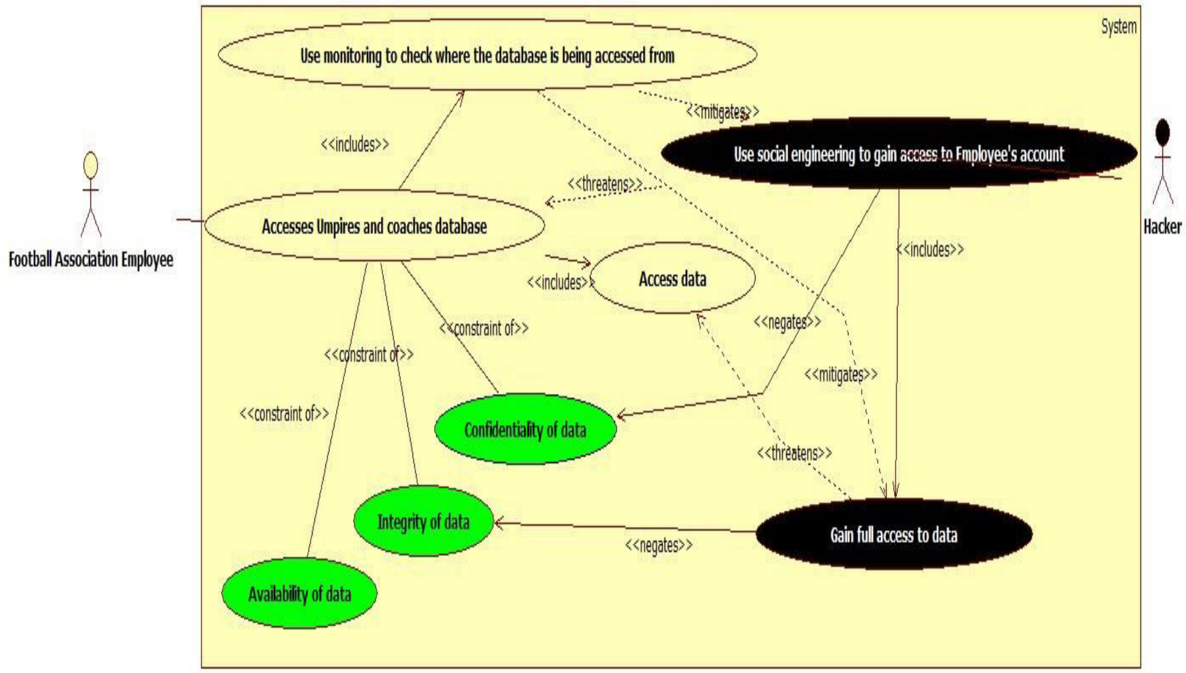


Figure A2 10: Misuse cases diagram for BA3 – Social engineering

Table A3 12: Social engineering

Business asset	Umpire
	Asset related concepts
Risk ID	**R14**
IS Asset	**Umpires and coaches database**
Security criterion	C and I of the business assets
	Risk related concepts
Risk	Hacker uses social engineering/phishing to gain access to the Football Association employee's computer as the employee has not been trained to detect social engineering attempts. The hacker is able to gain full access to the database through the Football Association employee's computer
Impact	Loss of C and I of the business assets
Event	Hacker uses social engineering (phishing for example) to gain

	access to their computer and thereby access the database
Vulnerability	No anti-social engineering training
Threat agent	Hacker
Threat	Hacker is able to use social engineering on one of the Football Association employees
Attack method	Social engineering
	Risk Treatment related concepts
Security requirement	Implement social engineering training for employees
Security requirement ID	**SRQ14**
Control	Implement social engineering awareness training for employees
Cost of control	**50 EUR per employee**

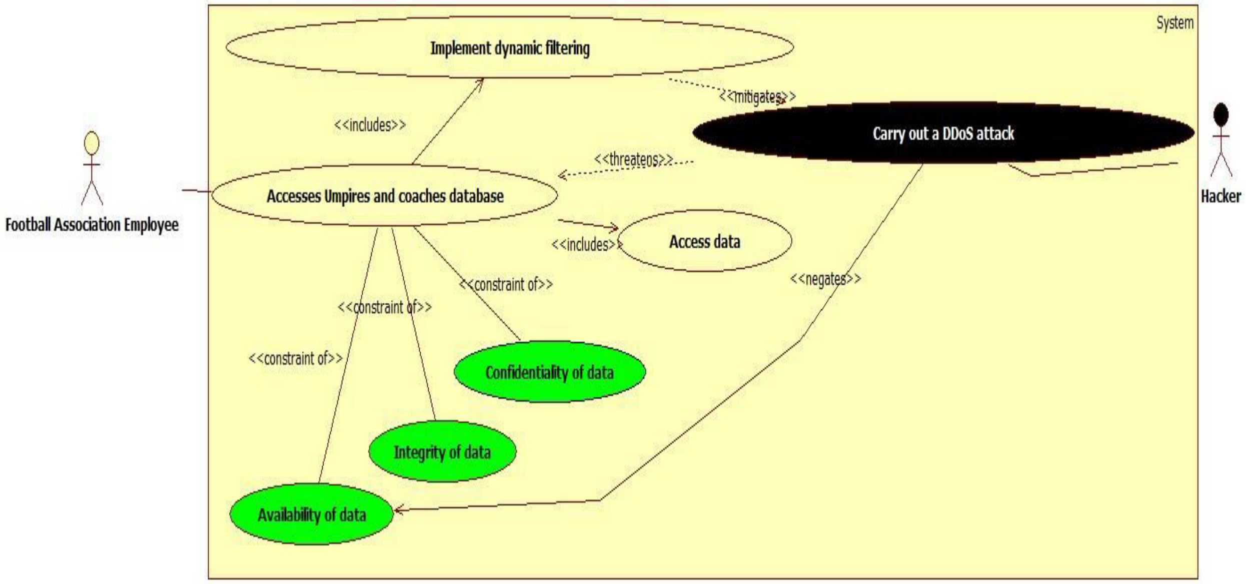


Figure A2 11: Misuse cases diagram for BA3 – DDoS attack

Table A3 13: DDoS attack

Business asset	Umpire
	Asset related concepts
Risk ID	**15**
IS Asset	**Umpires and coaches database**
Security criterion	Availability of the business assets
	Risk related concepts
Risk	Hacker launches a DDoS attack against the databases as no countermeasures have been set up to mitigate this. This leads to the

	service being unavailable for the users.
Impact	Loss of availability of the data
Event	Hacker attacks the databases using DDoS as no ip address filtering is set in place
Vulnerability	No countermeasures set up, no ip address filtering.
Threat agent	Hacker with a botnet
Threat	A hacker launching a DDoS attack against the databases
Attack method	Distributed Denial of Service attack (DDoS)
	Risk Treatment related concepts
Security requirement	ACL and dynamic ip filtering should be implemented
Security requirement ID	**SRQ15**
Control	Implement an ACL
Cost of Control	**0 to 500 EUR**

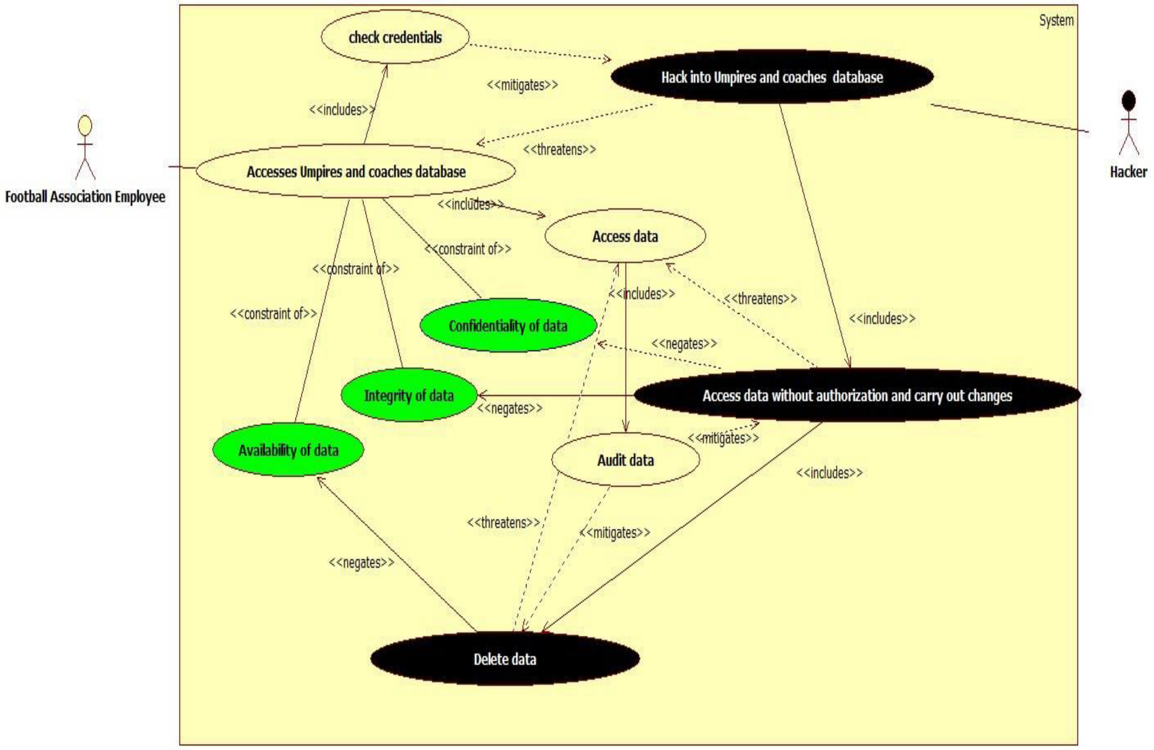


Figure A2 12: Misuse cases diagram for BA3: Unauthorized data manipulation

Table A3 14: Unauthorized data manipulation

Business asset	Game, Timetable
	Asset related concepts
Risk ID	**R16**
IS Asset	**Team and player database**
Security criterion	Confidentiality of the makeup of the league, which teams will play etc. Integrity of the composition of the league.
	Risk related concepts
Risk	Hacker is able to hack the Team and player database and modify the data before league entries are created, resulting in incorrect league entries to be created which result in the loss of integrity of the data
Impact	Loss of integrity of the business asset.
Event	Hacker is able to access the database and change the data entry causing incorrect league entry to be created
Vulnerability	No auditing of the team information before league entry creation.
Threat agent	Hacker
Threat	Hacker is able to hack the Team and player database and modify data
Attack method	Hacking the Team and player database and modifying data
	Risk Treatment related concepts
Security requirement	The entries in the database should be audited regularly.
Security requirement ID	**SRQ8**
Control	Implement regular database auditing
Cost of control	**1000 – 5000 EUR**

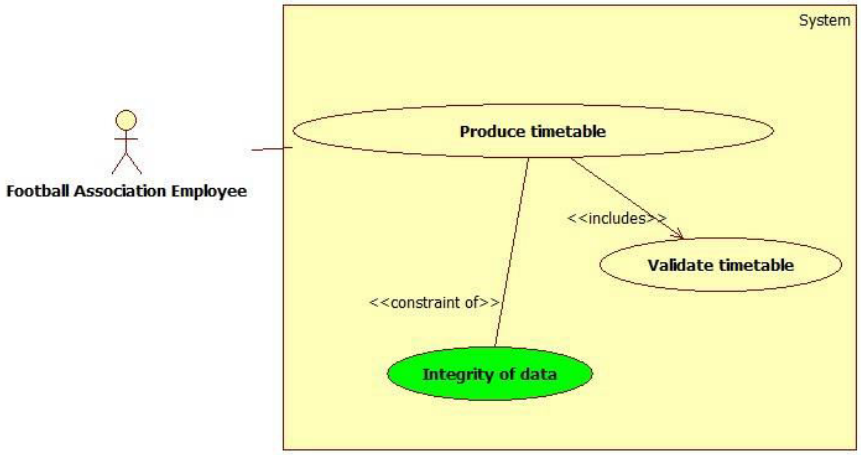


Figure A2 13: Use cases diagram for BA4 and BA5

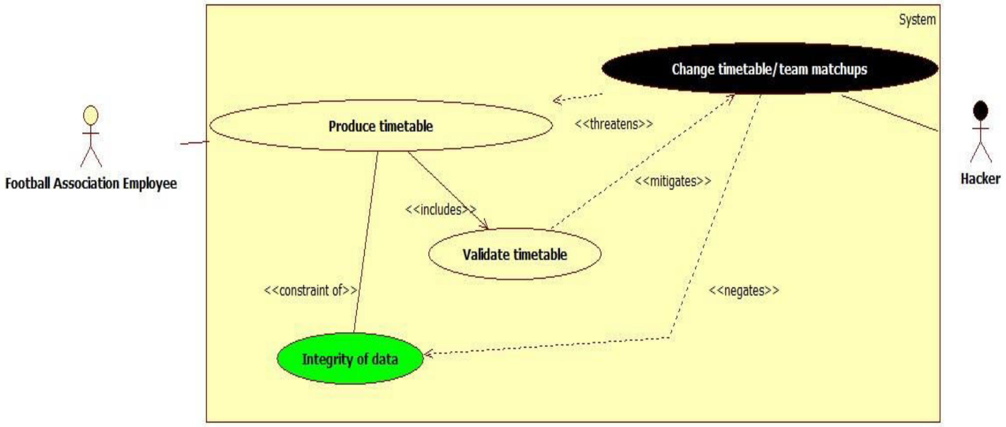


Figure A2 14: Misuse cases diagram for BA4 and BA5 – Unauthorized data manipulation

Table A3 15: Malicious user modifies the timetabling software output.

Business asset	Game
	Asset related concepts
Risk ID	**R17**
IS Asset	**Timetabling software**
Security criterion	Integrity of the timetable, the timetable has to meet the regulations set by UEFA/FIFA.
	Risk related concepts
Risk	Malicious user/disgruntled employee is able to change the team matchups manually due to no authentication/validation of the timetable in place resulting in the loss of integrity for the business asset.
Impact	The timetable has non-random matchups between teams, the integrity of the business asset is compromised
Event	Malicious user/disgruntled employee changes the team matchups manually without having to validate or authenticate the changes
Vulnerability	No system to validate and authenticate the timetable
Threat agent	Malicious user/disgruntled employee
Threat	Malicious user/disgruntled employee changes the team matchups manually
Attack method	The team matchups are changed manually
	Risk Treatment related concepts
Security requirement	The output of the software should be compared to the timetable input.
Security requirement ID	**SRQ17**
Control	Implement output comparison software
Cost of control	**0 to 500 EUR**

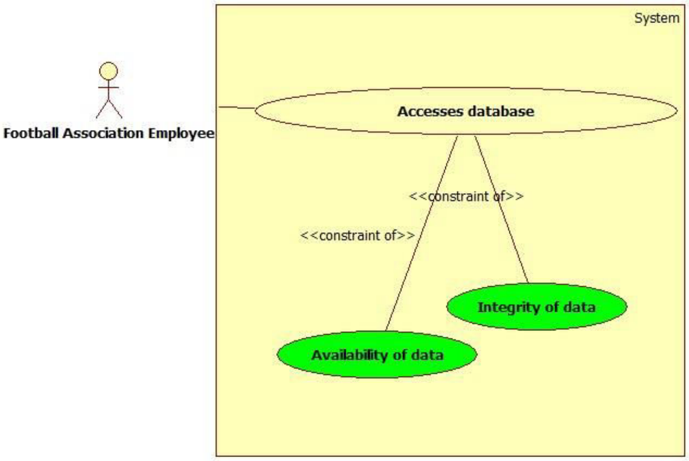


Figure A2 15: Use cases diagram for BA6 and BA7

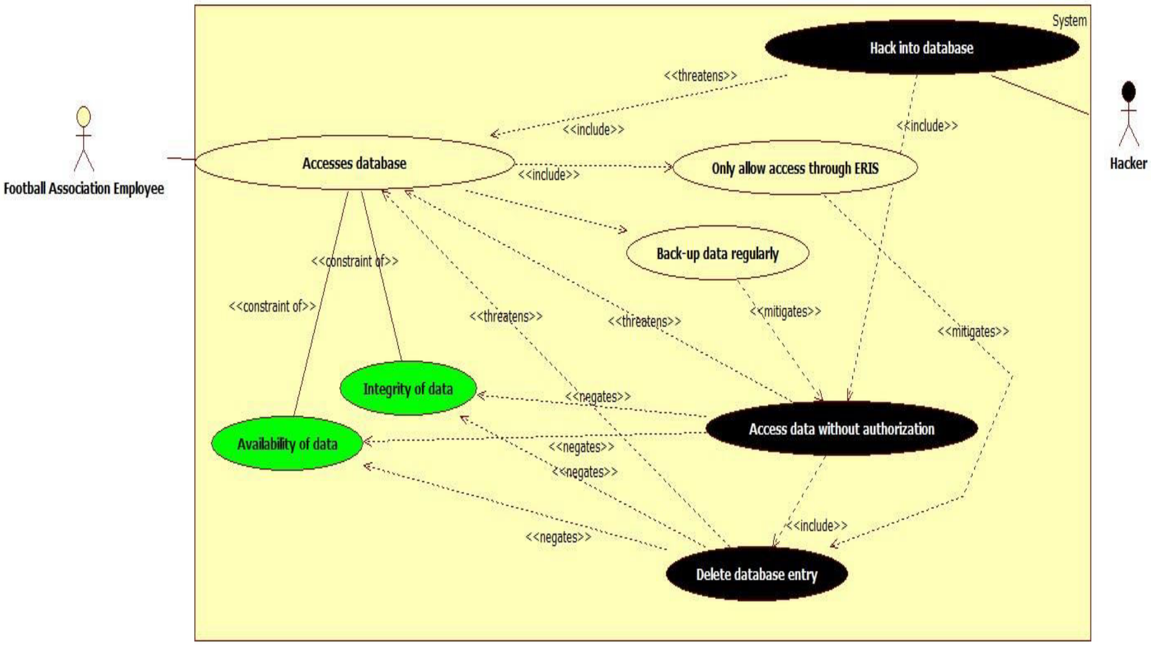


Figure A2 16: Misuse cases diagram for BA1, BA2 and BA3- Unauthorized file manipulation

Table A3 16: unauthorized data manipulation

Business asset	Database related BA
	Asset related concepts
Risk ID	**R18**
IS Asset	**Team and player database, Coaches and umpires database, Games database**
Security criterion	CIA of the business asset
	Risk related concepts
Risk	Hacker hacks the database and changes entries, leading to the loss of confidentiality, integrity and availability of the data.
Impact	Loss of CIA of the business asset.
Event	Hacker is able to hack the database and edit entries due to no controls being in place to check who can edit data
Vulnerability	No controls in place to determine who can edit data.
Threat agent	Hacker
Threat	Hacker is able to hack the database and edit entries
Attack method	Hacking the database and editing entries
	Risk Treatment related concepts
Security requirement	Data in the database should only be modifiable through ERIS after proper authentication.
Security requirement ID	**SRQ18**
Control	Only make the databases accessible through ERIS
Cost of control	**0 to 500 EUR**

Table A3 17: Attacker intentionally deletes umpire ID from the database.

Business asset	Database related BA
	Asset related concepts
Risk ID	**R19**
IS Asset	**Team and player database, Coaches and umpires database, Games database**
Security criterion	Integrity and availability of the database entries
	Risk related concepts
Risk	The attacker can delete entries in the databases and due to no backups, the entry cannot be recovered leading to the loss of integrity and availability of the business asset.
Impact	Loss of integrity and availability of the business asset.
Event	The attacker deletes the entry in the database which then cannot be recovered due to no backups of the database
Vulnerability	No backups for the entries in the user database
Threat agent	Malicious user
Threat	data being deleted from the database due to malicious activity.

Attack method	Accessing and deleting data entries from the database
	Risk Treatment related concepts
Security requirement	Regular backups of the databases should be introduced.
Security requirement ID	**SRQ19**
Control	Implement monthly backups
Cost of control	**0 to 500 EUR**

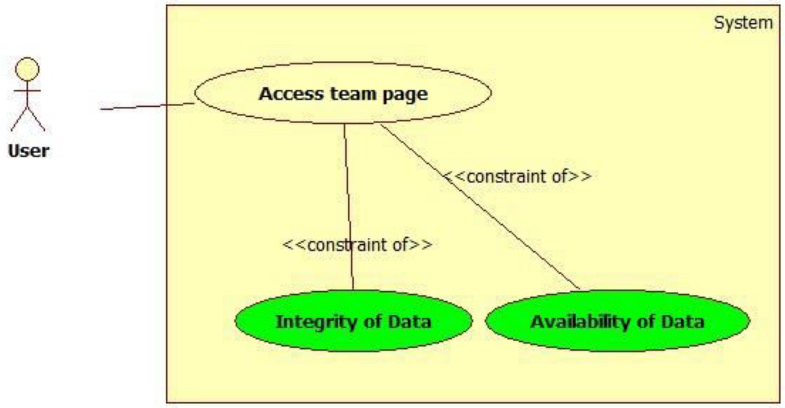


Figure A2 17: Use cases diagram for BA2

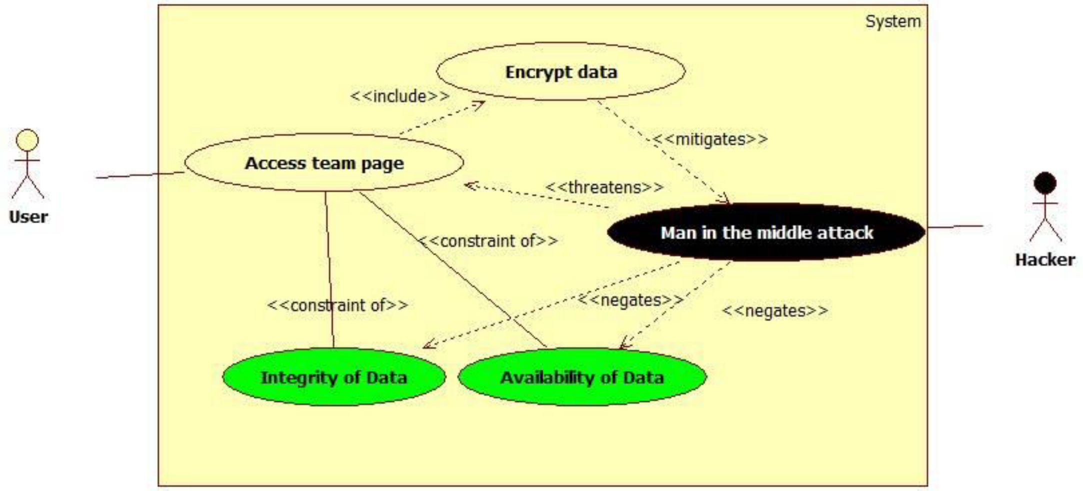


Figure A2 18: Misuse cases diagram forBA2– Man in the middle attack

Table A3 18: Session hijacking

Business asset	Team
	Asset related concepts
Risk ID	**R20**
IS Asset	**ERIS**
Security criterion	IA of the Business asset
	Risk related concepts
Risk	The attacker uses man in the middle attack to listen in on the data exchange leading to the loss of integrity and availability of the data
Impact	Loss of integrity and availability of the business asset. Loss of reliability of the medium of transportation.
Event	A hacker carries out a man in the middle attack due to no firewall being present
Vulnerability	No firewall in place to filter incoming and outgoing requests and data.
Threat agent	Hacker
Threat	Hacker carries out a man in the middle attack
Attack method	Listening in on the data traffic/man in the middle attack
	Risk Treatment related concepts
Security requirement	Any and all data exchange between the user and the server should be encrypted
Security requirement ID	**SRQ20**
Control	Implement data encryption whenever data is being transferred
Cost of control	**0 to 500 EUR**

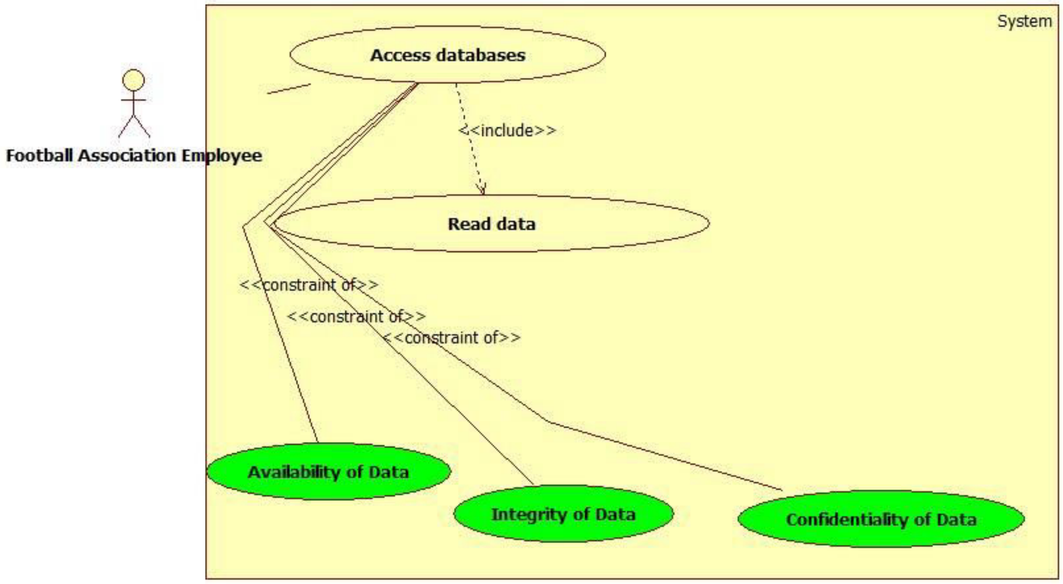


Figure A2 19: Use cases diagram for BA9

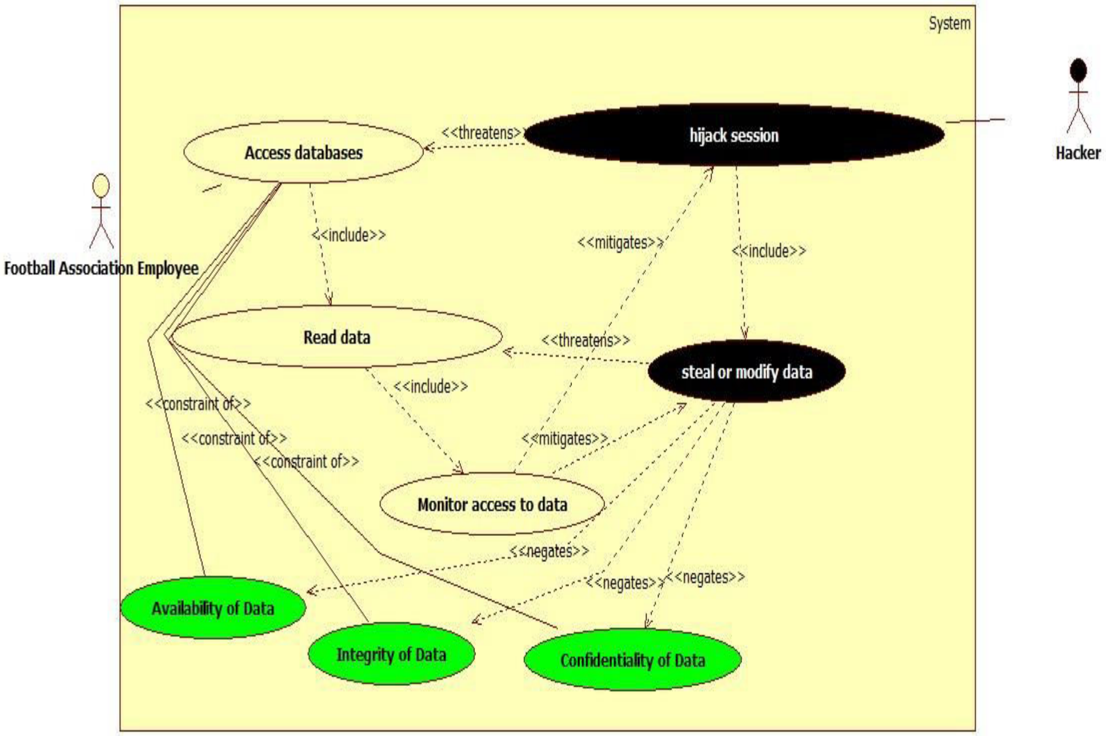


Figure A2 20: Misuse cases diagram for BA9 – session hijacking

Table A3 19: Unauthorized data modification

Business asset	Game
	Asset related concepts
Risk ID	**R21**
IS Asset	**Game database,**
Security criterion	CIA of the Game.
	Risk related concepts
Risk	Attacker is able to hijack the session used by an authorized user to access and/or modify confidential data without the risk of being caught due to no monitoring software being utilized thus compromising the CIA of the business asset.
Impact	Loss of integrity, confidentiality and availability of the business asset.
Event	The attacker hijacks an authorized user's session and is able to access the data for theft or modification without risk of being caught due to monitoring software.
Vulnerability	No monitoring software in place
Threat agent	Hacker

Threat	Hacker hijacks the session and steals and/or modifies data
Attack method	Session hijacking of authorized users or another way of gaining access to the databases to steal or modify data.
	Risk Treatment related concepts
Security requirement	Implement monitoring software to notify the administrator of any suspicious access/file modifications.
Security requirement ID	**SRQ21**
Control	Install monitoring software for the database
Cost of control	**0 to 500 EUR**

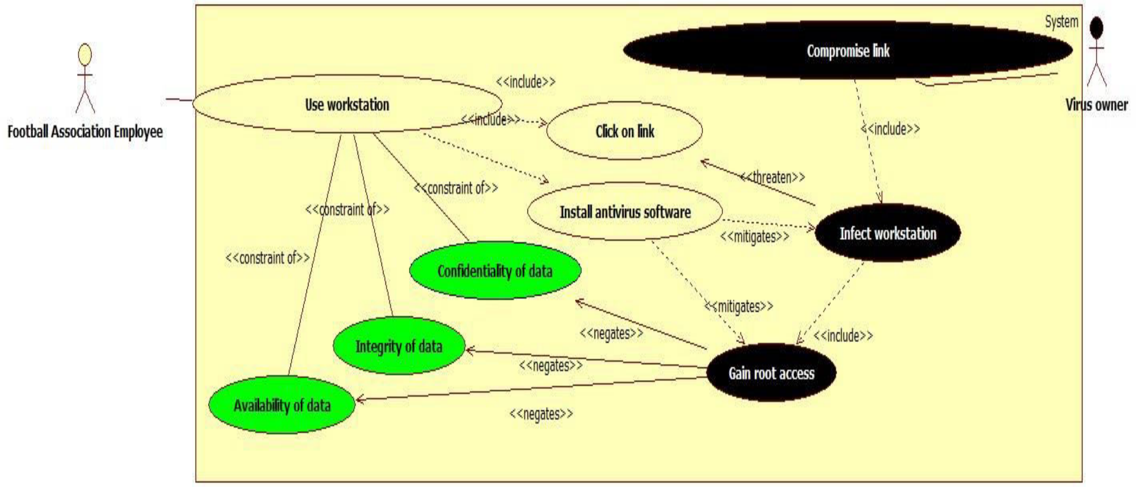


Figure A2 21: Misuse cases diagram for all BAs – virus infection

Table A3 20: Virus infection

Business asset	All
	Asset related concepts
Risk ID	**R22**
IS Asset	**ERIS**
Security criterion	CIA of the data
	Risk related concepts
Risk	Due to no antivirus software being installed, employees may inadvertently install viruses on their computers by clicking on infected links. The viruses can then infect the workstation and gain root access to the systems.
Impact	Loss of integrity, confidentiality and availability of the business asset.
Event	An employee clicks on a compromised link, downloading a virus to the workstation due to no antivirus software being present, this allows the virus to gain root access to the systems.

Vulnerability	No antivirus software is installed
Threat agent	Owner of the virus
Threat	Due to no antivirus software, the virus is able to infect workstations on ERIS and gain root access to the systems.
Attack method	Virus is able to infect workstations on ERIS and gain access to the systems.
	Risk Treatment related concepts
Security requirement	Antivirus software should be installed on all workstations
Security requirement ID	**SRQ22**
Control	Install antivirus software for workstations
Cost of control	**0 EUR to 5000 EUR/year**

SQUARE Requirements Categorization

The security requirements elicited using SQUARE are categorized below according to their BAs.

Table A3 21: BA1 – Player

SRQ ID	Player Business Asset SRQ Description
SRQ1.1	Only authorized personnel should be able to access the Player Business Asset. User credentials must be checked
SRQ2.1	Authentication should be implemented when data is being modified in the Player Business Asset
SRQ3.1	An access control list (ACL) should be implemented to access the Player Business Asset
SRQ4.1	Input sanitization, canonicalization and validation should be implemented for any inputs interfacing with the Player Business Asset
SRQ5	Social engineering training for employees should be implemented
SRQ6.1	ACL and dynamic ip filtering should be implemented when accessing the Player Business Asset
SRQ7.1	Data stored in the Player Business Asset should be encrypted
SRQ8.1	Data stored in the Player Business Asset should be audited regularly
SRQ10.1	Data in the Player Business Asset should only be modifiable through ERIS after proper authentication.
SRQ11.1	Regular backups of the Player Business Asset should be introduced.
SRQ12	Any and all data exchange between the user and the server should be encrypted
SRQ13.1	Implement monitoring software to notify the administrator of any suspicious access/file modifications in the Player Business Asset
SRQ14	Antivirus software should be installed on all workstations

Table A3 22: BA2 – Team

SRQ ID	Team Business Asset SRQ Description
SRQ1.2	Only authorized personnel should be able to access the Team Business Asset. User credentials must be checked
SRQ2.2	Authentication should be implemented when data is being modified in the Team Business Asset
SRQ3.2	An access control list (ACL) should be implemented to access the Team Business Asset
SRQ4.2	Input sanitization, canonicalization and validation should be implemented for any inputs interfacing with the Team Business Asset
SRQ5	Social engineering training for employees should be implemented
SRQ6.2	ACL and dynamic ip filtering should be implemented when accessing the Team Business Asset
SRQ7.2	Data stored in the Team Business Asset should be encrypted
SRQ8.2	Data stored in the Team Business Asset should be audited regularly
SRQ10.2	Data in the Team Business Asset should only be modifiable through ERIS after proper authentication.
SRQ11.2	Regular backups of the Team Business Asset should be introduced.
SRQ12	Any and all data exchange between the user and the server should be encrypted
SRQ13.2	Implement monitoring software to notify the administrator of any suspicious access/file modifications in the Team Business Asset
SRQ14	Antivirus software should be installed on all workstations

Table A3 23: BA3- Umpire

SRQ ID	Umpire Business Asset SRQ Description
SRQ1.3	Only authorized personnel should be able to access the Umpire Business Asset. User credentials must be checked
SRQ2.3	Authentication should be implemented when data is being modified in the Umpire Business Asset
SRQ3.3	An access control list (ACL) should be implemented to access the Umpire Business Asset
SRQ4.3	Input sanitization, canonicalization and validation should be implemented for any inputs interfacing with the Umpire Business Asset
SRQ5	Social engineering training for employees should be implemented
SRQ6.3	ACL and dynamic ip filtering should be implemented when accessing the Umpire Business Asset
SRQ7.3	Data stored in the Umpire Business Asset should be encrypted
SRQ8.3	Data stored in the Umpire Business Asset should be audited regularly
SRQ10.3	Data in the Umpire Business Asset should only be modifiable through ERIS after proper authentication.
SRQ11.3	Regular backups of the Umpire Business Asset should be introduced.

SRQ12	Any and all data exchange between the user and the server should be encrypted
SRQ13.3	Implement monitoring software to notify the administrator of any suspicious access/file modifications in the Umpire Business Asset
SRQ14	Antivirus software should be installed on all workstations

Table A3 24: BA4- Game

SRQ ID	Game Business Asset SRQ Description
SRQ1.4	Only authorized personnel should be able to access the Game Business Asset. User credentials must be checked
SRQ2.4	Authentication should be implemented when data is being modified in the Game Business Asset
SRQ3.4	An access control list (ACL) should be implemented to access the Game Business Asset
SRQ4.4	Input sanitization, canonicalization and validation should be implemented for any inputs interfacing with the Game Business Asset
SRQ5	Social engineering training for employees should be implemented
SRQ6.4	ACL and dynamic ip filtering should be implemented when accessing the Game Business Asset
SRQ7.4	Data stored in the Game Business Asset should be encrypted
SRQ8.4	Data stored in the Game Business Asset should be audited regularly
SRQ10.4	Data in the Game Business Asset should only be modifiable through ERIS after proper authentication.
SRQ11.4	Regular backups of the Game Business Asset should be introduced.
SRQ12	Any and all data exchange between the user and the server should be encrypted
SRQ13.4	Implement monitoring software to notify the administrator of any suspicious access/file modifications in the Game Business Asset
SRQ14	Antivirus software should be installed on all workstations

Table A3 25: BA5- Timetable

SRQ ID	Timetable Business Asset SRQ Description
SRQ1.5	Only authorized personnel should be able to access the Timetable Business Asset. User credentials must be checked
SRQ2.5	Authentication should be implemented when data is being modified in the Timetable Business Asset
SRQ3.5	An access control list (ACL) should be implemented to access the Timetable Business Asset
SRQ4.5	Input sanitization, canonicalization and validation should be implemented for any inputs interfacing with the Timetable Business Asset
SRQ5	Social engineering training for employees should be implemented
SRQ6.5	ACL and dynamic ip filtering should be implemented when accessing the Timetable Business Asset
SRQ7.5	Data stored in the Timetable Business Asset should be encrypted
SRQ8.5	Data stored in the Timetable Business Asset should be audited regularly

SRQ9	**The software output should be compared to the input when compiling the timetable**
SRQ10.5	**Data in the Timetable Business Asset should only be modifiable through ERIS after proper authentication.**
SRQ11.5	**Regular backups of the Timetable Business Asset should be introduced.**
SRQ12	**Any and all data exchange between the user and the server should be encrypted**
SRQ13.5	**Implement monitoring software to notify the administrator of any suspicious access/file modifications in the Timetable Business Asset**
SRQ14	**Antivirus software should be installed on all workstations**

Section A4: Results Comparison Tables

The tables below represent the comparison of completeness tables of the elicited security requirements.

Table A4 1: Player BA

Asset: Player										
Requirements Categorization			**Requirements (SREBP)**	**Coverage**				**Requirements (SQUARE)**	**Coverage**	
1. Identification	C	6.25	SRQBA1:5	75%	4.69	C	6.25	SRQ1.1	50%	3.13
	I	6.25	SRQBA1:5	75%	4.69	I	6.25		0%	-
	A	-				A	-			
2. Authentication	C	4.17	SRQBA1:5, SRQBA1:6, SRQBA1:11, SRQBA1:12, SRQBA1:13	100%	4.17	C	4.17	SRQ1.1, SRQ 3.1	75%	3.13
	I	4.17	SRQBA1:5, SRQBA1:6, SRQBA1:11, SRQBA1:12, SRQBA1:13	100%	4.17	I	4.17	SRQ2.1	50%	2.09
	A	4.17	SRQBA1:5, SRQBA1:11,	100%	4.17	A	4.17	SRQ2.1	50%	2.09
3. Authorization	C	4.17	SRQBA1:1, SRQBA1:2, SRQBA1:3, SRQBA1:4, SRQBA1:5,	100%	4.17	C	4.17	SRQ1.1, SRQ3.1	100%	4.17
	I	4.17	SRQBA1:1, SRQBA1:2, SRQBA1:3, SRQBA1:4, SRQBA1:5	100%	4.17	I	4.17	SRQ2.1	50%	2.09
	A	4.17	SRQBA1:11 SRQBA1:14	50%	2.085	A	4.17	SRQ6.1, SRQ2.1	25%	1.04
4. Accounting	C	4.17	SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:15	75%	3.1275	C	4.17	SRQ8.1, SRQ13.1	100%	4.17
	I	4.17	SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:15	75%	3.1275	I	4.17	SRQ8.1, SRQ13.1	100%	4.17
	A	4.17	SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:15	75%	3.1275	A	4.17	SRQ13.1	75%	3.13
5. Audit	C	4.17	SRQBA1:15	75%	3.1275	C	4.17		0%	-
	I	4.17	SRQBA1:15	75%	3.1275	I	4.17	SRQ13.1	25%	1.04
	A	4.17	SRQBA1:15	75%	3.1275	A	4.17		0%	0.00
6. Non repudiation	C	-				C	-			
	I	12.5	SRQBA1:15	75%	9.375	I	12.5			0.00
	A	-				A	-			
7. Immunity	C	4.17	SRQBA1:7, SRQBA1:8, SRQBA1:9, SRQBA1:10, SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:16, SRQBA1:17, SRQBA1:18	100%	4.17	C	4.17	SRQ4.1, SRQ14	75%	3.13
	I	4.17	SRQBA1:7, SRQBA1:8, SRQBA1:9, SRQBA1:10, SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:16, SRQBA1:17, SRQBA1:18	100%	4.17	I	4.17	SRQ4.1, SRQ14	75%	3.13
	A	4.17	SRQBA1:7, SRQBA1:8, SRQBA1:9, SRQBA1:10, SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14, SRQBA1:16, SRQBA1:17, SRQBA1:18	100%	4.17	A	4.17	SRQ4.1, SRQ14	75%	3.13
8. Data Exchange	C	4.17	SRQBA1:6, SRQBA1:7, SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14	100%	4.17	C	4.17	SRQ12	50%	2.09
	I	4.17	SRQBA1:6, SRQBA1:7, SRQBA1:11, SRQBA1:12, SRQBA1:13, SRQBA1:14	100%	4.17	I	4.17	SRQ12	50%	2.09
	A	4.17		0%	0	A	4.17	SRQ6.1, SRQ12	50%	2.09
					81.30					45.87

Table A4 2: Umpire BA

Asset: Umpire										
Requirements Categorization			**Requirements (SREBP)**	**Coverage**				**Requirements (SQUARE)**	**Coverage**	
1. Identification	C	6.25	SRQBA3:4	75%	4.69	C	6.25	SRQ1.3	50%	3.13
	I	6.25	SRQBA3:4	75%	4.69	I	6.25		0%	-
	A	-				A	-			
2. Authentication	C	4.17	SRQBA3:4, SRQBA3:5, SRQBA3:10, SRQBA3:11, SRQBA3:12	100%	4.17	C	4.17	SRQ1.3, SRQ 3.3	75%	3.13
	I	4.17	SRQBA3:4, SRQBA3:5, SRQBA3:10, SRQBA3:11, SRQBA3:12	100%	4.17	I	4.17	SRQ2.3	50%	2.09
	A	4.17	SRQBA3:5, SRQBA3:10	100%	4.17	A	4.17	SRQ2.3	50%	2.09
3. Authorization	C	4.17	SRQBA3:1, SRQBA3:2, SRQBA3:3, SRQBA3:4, SRQBA3:18, SRQBA3:19	100%	4.17	C	4.17	SRQ1.3, SRQ3.3	100%	4.17
	I	4.17	SRQBA3:1, SRQBA3:2, SRQBA3:3, SRQBA3:4, SRQBA3:18, SRQBA3:19	100%	4.17	I	4.17	SRQ2.3	50%	2.09
	A	4.17	SRQBA3:10, SRQBA3:13	50%	2.085	A	4.17	SRQ6.3, SRQ2.3	25%	1.04
4. Accounting	C	4.17	SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:14	100%	4.17	C	4.17	SRQ8.3, SRQ13.3	100%	4.17
	I	4.17	SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:14	100%	4.17	I	4.17	SRQ8.3, SRQ13.3	100%	4.17
	A	4.17	SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:14	100%	4.17	A	4.17	SRQ13.3	75%	3.13
5. Audit	C	4.17	SRQBA3:14, SRQBA3:24	75%	3.1275	C	4.17		0%	-
	I	4.17	SRQBA3:14, SRQBA3:24	75%	3.1275	I	4.17	SRQ13.3	25%	1.04
	A	4.17	SRQBA3:14, SRQBA3:24	75%	3.1275	A	4.17		0%	0.00
6. Non repudiation	C	-				C	-			
	I	12.5	SRQBA3:14, SRQBA3:24	75%	9.375	I	12.5		0%	0.00
	A	-				A	-			
7. Immunity	C	4.17	SRQBA3:5, SRQBA3:6, SRQBA3:7, SRQBA3:8, SRQBA3:9, SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:15, SRQBA3:16, SRQBA3:17, SRQBA3:20, SRQBA3:21, SRQBA3:22, SRQBA3:23, SRQBA3:25	100%	4.17	C	4.17	SRQ4.3, SRQ14	75%	3.13
	I	4.17	SRQBA3:5, SRQBA3:6, SRQBA3:7, SRQBA3:8, SRQBA3:9, SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:15, SRQBA3:16, SRQBA3:17, SRQBA3:20, SRQBA3:21, SRQBA3:22, SRQBA3:23, SRQBA3:25	100%	4.17	I	4.17	SRQ4.3, SRQ14	75%	3.13
	A	4.17	SRQBA3:5, SRQBA3:6, SRQBA3:7, SRQBA3:8, SRQBA3:9, SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:15, SRQBA3:16, SRQBA3:17, SRQBA3:20, SRQBA3:21, SRQBA3:22, SRQBA3:23, SRQBA3:25	100%	4.17	A	4.17	SRQ4.3, SRQ14	75%	3.13
8. Data Exchange	C	4.17	SRQBA3:5, SRQBA3:6, SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:20	100%	4.17	C	4.17	SRQ12	50%	2.09
	I	4.17	SRQBA3:5, SRQBA3:6, SRQBA3:10, SRQBA3:11, SRQBA3:12, SRQBA3:13, SRQBA3:20	100%	4.17	I	4.17	SRQ12	50%	2.09
	A	4.17		0%	0	A	4.17	SRQ6.3, SRQ12	50%	2.09
					84.43					45.87

Table A4 3: Game BA

Asset: Game										
Requirements Categorization			**Requirements (SREBP)**	**Coverage**				**Requirements (SQUARE)**	**Coverage**	
1. Identification	C	6.25	SRQBA4:5, SRQBA4:6	75%	4.69	C	6.25	SRQ1.4	50%	3.13
	I	6.25	SRQBA4:5, SRQBA4:6	75%	4.69	I	6.25		0%	-
	A	-				A	-			
2. Authentication	C	4.17	SRQBA4:5, SRQBA4:6, SRQBA4:7, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:27, SRQBA4:28	100%	4.17	C	4.17	SRQ1.4, SRQ 3.4	75%	3.13
	I	4.17	SRQBA4:5, SRQBA4:6, SRQBA4:7, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:27, SRQBA4:28	100%	4.17	I	4.17	SRQ2.4	50%	2.09
	A	4.17	SRQBA4:7, SRQBA4:16	100%	4.17	A	4.17	SRQ2.4	50%	2.09
3. Authorization	C	4.17	SRQBA4:1, SRQBA4:2, SRQBA4:3, SRQBA4:4, SRQBA4:5, SRQBA4:6	100%	4.17	C	4.17	SRQ1.4, SRQ3.4	100%	4.17
	I	4.17	SRQBA4:1, SRQBA4:2, SRQBA4:3, SRQBA4:4, SRQBA4:5, SRQBA4:6	100%	4.17	I	4.17	SRQ2.4	50%	2.09
	A	4.17	SRQBA4:16, SRQBA4:29	50%	2.085	A	4.17	SRQ6.4, SRQ2.4	25%	1.04
4. Accounting	C	4.17	SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:22, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	C	4.17	SRQ8.4, SRQ13.4	100%	4.17
	I	4.17	SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:22, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	I	4.17	SRQ8.4, SRQ13.4	100%	4.17
	A	4.17	SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:22, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	A	4.17	SRQ13.4	75%	3.13
5. Audit	C	4.17	SRQBA4:22	75%	3.1275	C	4.17		0%	-
	I	4.17	SRQBA4:22	75%	3.1275	I	4.17		0%	0.00
	A	4.17	SRQBA4:22	75%	3.1275	A	4.17		0%	0.00
6. Non repudiation	C	-		75%	9.375	C	-		25%	3.13
	I	12.5	SRQBA4:22			I	12.5	SRQ13.4		
	A	-				A	-			
7. Immunity	C	4.17	SRQBA4:7, SRQBA4:8, SRQBA4:9, SRQBA4:10, SRQBA4:11, SRQBA4:12, SRQBA4:13, SRQBA4:14, SRQBA4:15, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:23, SRQBA4:24, SRQBA4:25, SRQBA4:26, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	C	4.17	SRQ4.4, SRQ14	75%	3.13
	I	4.17	SRQBA4:7, SRQBA4:8, SRQBA4:9, SRQBA4:10, SRQBA4:11, SRQBA4:12, SRQBA4:13, SRQBA4:14, SRQBA4:15, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:23, SRQBA4:24, SRQBA4:25, SRQBA4:26, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	I	4.17	SRQ4.4, SRQ14	75%	3.13
	A	4.17	SRQBA4:7, SRQBA4:8, SRQBA4:9, SRQBA4:10, SRQBA4:11, SRQBA4:12, SRQBA4:13, SRQBA4:14, SRQBA4:15, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:23, SRQBA4:24, SRQBA4:25, SRQBA4:26, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	A	4.17	SRQ4.4, SRQ14	75%	3.13
8. Data Exchange	C	4.17	SRQBA4:7, SRQBA4:8, SRQBA4:9, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	C	4.17	SRQ12	50%	2.09
	I	4.17	SRQBA4:7, SRQBA4:8, SRQBA4:9, SRQBA4:16, SRQBA4:17, SRQBA4:18, SRQBA4:19, SRQBA4:20, SRQBA4:21, SRQBA4:27, SRQBA4:28, SRQBA4:29	100%	4.17	I	4.17	SRQ12	50%	2.09
	A	4.17		0%	0	A	4.17	SRQ6.4, SRQ12	50%	2.09
					84.43					47.95

Table A4 4: Timetable BA

Asset: Timetable Requirements Categorization			Requirements (SREBP)	Coverage				Requirements (SQUARE)	Coverage	
1. Identification	C	6.25	SRQBA5:5	75%	4.69	C	6.25	SRQ1.5	50%	3.13
	I	6.25	SRQBA5:5	75%	4.69	I	6.25		0%	-
	A	-				A	-			
2. Authentication	C	4.17	SRQBA5:4, SRQBA5:5, SRQBA5:6, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17	100%	4.17	C	4.17	SRQ1.5, SRQ 3.5	75%	3.13
	I	4.17	SRQBA5:4, SRQBA5:5, SRQBA5:6, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17	100%	4.17	I	4.17	SRQ2.5	50%	2.09
	A	4.17	SRQBA5:6, SRQBA5:12	100%	4.17	A	4.17	SRQ2.5	50%	2.09
3. Authorization	C	4.17	SRQBA5:1, SRQBA5:2, SRQBA5:3, SRQBA5:4, SRQBA5:5	100%	4.17	C	4.17	SRQ1.5, SRQ3.5	100%	4.17
	I	4.17	SRQBA5:1, SRQBA5:2, SRQBA5:3, SRQBA5:4, SRQBA5:5	100%	4.17	I	4.17	SRQ2.5	50%	2.09
	A	4.17	SRQBA5:12, SRQBA5:22	0%	0	A	4.17	SRQ6.5, SRQ2.5	25%	1.04
4. Accounting	C	4.17	SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:18	100%	4.17	C	4.17	SRQ8.5, SRQ13.5	100%	4.17
	I	4.17	SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:18	100%	4.17	I	4.17	SRQ8.5, SRQ13.5	100%	4.17
	A	4.17	SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:18	100%	4.17	A	4.17	SRQ13.5	75%	3.13
5. Audit	C	4.17	SRQBA5:18	75%	3.1275	C	4.17		0%	-
	I	4.17	SRQBA5:18	75%	3.1275	I	4.17	SRQ9, SRQ13.5	75%	3.13
	A	4.17	SRQBA5:18	75%	3.1275	A	4.17		0%	0.00
6. Non repudiation	C	-				C	-			
	I	12.5	SRQBA5:18	75%	9.375	I	12.5	SRQ13.5	25%	3.13
	A	-				A	-			
7. Immunity	C	4.17	SRQBA5:6, SRQBA5:7, SRQBA5:8, SRQBA5:9, SRQBA5:10, SRQBA5:11, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:19, SRQBA5:20, SRQBA5:21, SRQBA5:22	100%	4.17	C	4.17	SRQ4.5 SRQ14	75%	3.13
	I	4.17	SRQBA5:6, SRQBA5:7, SRQBA5:8, SRQBA5:9, SRQBA5:10, SRQBA5:11, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:19, SRQBA5:20, SRQBA5:21, SRQBA5:22	100%	4.17	I	4.17	SRQ4.5 SRQ14	75%	3.13
	A	4.17	SRQBA5:6, SRQBA5:7, SRQBA5:8, SRQBA5:9, SRQBA5:10, SRQBA5:11, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:19, SRQBA5:20, SRQBA5:21, SRQBA5:22	100%	4.17	A	4.17	SRQ4.5 SRQ14	75%	3.13
8. Data Exchange	C	4.17	SRQBA5:6, SRQBA5:7, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:22	100%	4.17	C	4.17	SRQ12	50%	2.09
	I	4.17	SRQBA5:6, SRQBA5:7, SRQBA5:12, SRQBA5:13, SRQBA5:14, SRQBA5:15, SRQBA5:16, SRQBA5:17, SRQBA5:22	100%	4.17	I	4.17	SRQ12	50%	2.09
	A	4.17		0%	0	A	4.17	SRQ6.5, SRQ12	50%	2.09
					82.34					51.08

Non-exclusive licence to reproduce thesis and make thesis public

I, **Karl Kolk**(date of birth: 20.04.1990),

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*An Empirical Comparison of Approaches for Security Requirements Elicitation*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, **05.02.2015**