TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Computer Science
Centre for Digital Forensics and Cyber Security

ITC70LT

Juan Manuel Rodríguez López 144935IVCM

SECURITY RISK ASSESSMENT TO THE USE OF DIGITAL CHARTING IN COLOMBIA

Master's thesis

Supervisor: Alexander Horst Norta
PhD

Chair of Software Engineering

Tallinn 2016

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Arvutiteaduse instituut
Küberkriminalistika ja küberjulgeoleku keskus

ITC70LT
Juan Manuel Rodríguez López 144935IVCM

TURVALISUSE RISKIANALÜÜS DIGITAALSE SKEEMIDE KASUTAMISEL KOLUMBIAS.

Magistritöö Lõputöö

Juhendaja: Alexander Horst
Norta
PhD

tarkvaratehnika
õppetool

Tallinn 2016

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Juan Manuel Rodríguez López

25.05.2016

Acknowledgments

I am very grateful for all the support given by my academic supervisor Alexander Norta, PhD, throughout this process. His recommendations and permanent disposal, allowed me to find the right way to conduct this research.

Abstract

The paperless cockpit concept is a current trend in the aviation business, its aim is to avoid the use of operating manuals and paper chart in flight deck. The advantage of eliminating this weight is that fuel costs in air operations would be reduced. Electronic Flight Bags are used worldwide; however, there is a lack of information security studies about the operation of these devices.

This thesis develops a security risk assessment to the use of digital charting. A case study of the Colombian aviation is performed, considering military organization and commercial airline that conduct their operations in this country. The framework is the Information System Security Risk Management (ISSRM) methodology, to develop it six security risk oriented patterns are applied and the business processes are modelled using Business Process Modeling Notation (BPMN). Finally, for thesis evaluation, the Security Attribute Evaluation Method (SAEM) is performed.

This thesis is written in English and is 67 pages long, including 7 chapters, 30 figures and 12 tables.

Kokkuvõtte

Turvalisuse riskianalüüs digitaalse skeemide kasutamisel Kolumbias.

Paberivaba kabiini mõiste on praegune trend lennunduses, selle eesmärgiks on kasutusjuhendite ja paberi diagrammide kabiinidest eemaldamine. Edemusek on see, et kabiini mass on sellega vähenenud järelikult kaa kütuse hind. Elektroonilisi lennukotte kasutatakse ülemaailmas, kuid turvalisuse uuringutes on veel vähe informatsiooni selle kohta kuidas selliseid konstruktioone kasutada.

See uuringutöö arendab turvalisuse riskianalüüsi, edendamas digitaalse kaardistamise kasutamist. Juhtimisanalüüs kasutab Kolumbia näidet, arvestades lennuvägiga ja kaubandus lennufirmadega, mis viivad läbi oma tegevust selles riigis. Selle uuringu raamistik on infosüsteemide turvalisuse riskihalduse (ISSRM) metoodika, selle arendamiseks kasutatakse kuus turvariski orienteeritud mustreid. Äriprotsessi moelleerimiseks kasutatakse BPMN äriprotsesside modellerimiskeelt. Lõpputöö hindamiseks kasutatakse Security Attribute Evaluation meetodi (SAEM).

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 67 leheküljel, 7 peatükki, 30 joonist, 12 tabelit.

List of abbreviations and terms

AEROCIVIL	*Aeronáutica Civil* (Civilian Aeronautical)
BPMN	Business Process Modeling Notation
CA	Certification Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CEA	*Centro de Estudios de Ciencias Aeronauticas (*Aeronautical Sciences Studies Center)
CERT	Computer Emergency Readiness Team
CGI	Common Gateway Interface
CWE	Common Weakness Enumeration
DoS	Denial of Service
EASA	European Aviation Safety Agency
EFB	Electronic Flight Bag
FAA	Federal Aviation Administration
FCOM	Flight Crew Operations Manual
ICAO	International Civil Aviation Organization.
ILS	Instrument Landing System
IP	Internet Protocol
IS	Information System
ISSRM	Information System Security Risk Management
IT	Information Technology
LPC	Less Paper Cockpit
OWASP	Open Web Application Security Project
RAC	*Reglamentos Aeronáuticos de Colombia* (Colombian Aeronautical Regulations)
SAEM	Security Attribute Evaluation Method
SaaS	Software as a Service
SQL	Structured Query Language
SRP	Security Risk-oriented Patterns

Table of Contents

List of Figures

List of Tables

1 Introduction

The implementation of paperless cockpit concept has had a huge development in the aviation business; governments and private sector have put their efforts to generate new technologies and achieve standardization of processes. However, security should also be considered in the initial stages of business process design. This thesis proposes a method to secure business process to the use of digital charting in cockpit.

1.1 Motivation

During the last decade the aviation industry has been making innovations in its processes and services, especially on issues related to safety and improvement of the procedures in cockpit. One of these is the air navigation using digital charting, a trend that has become almost standard in global aviation. The designers of commercial aviation flight decks have been pursuing ways to reduce or eliminate the use of paper documents in flight operations to generate higher yields and savings in fuel consumption [34].

With the use of new products, it is necessary to have tools available to identify new vulnerabilities in its operation, to ensure the confidentiality, integrity and availability of the information. The security risk assessment is a necessary method for identifying possible attacks and pose control measures to mitigate these threats.

By being an active member of the Colombian Air Force, my intention is to ensure that the knowledge learned during these two years is applied in real cases and generate a positive impact within the organization. Therefore the case study is Colombia, as the security and risk studies are still very scarce, is relevant for investigating state-of-the-art scientific problems in this field.

1.2 State of the Art

During the last twenty years the aircraft manufacturers have driven the project of Less Paper Cockpit (LPC), one of the aims of this project is the implementation of the Flight Crew Operations Manual (FCOM) and the navigation system in electronic devices [17]. The following chapter describes the beginnings of this project in the civil and military aviation, the regulatory entities that were created to generate a control framework and the difficulties encountered by the industry with this new development.

1.2.1 The beginning of the digital maps

They started using electronic flight-bag devices in the cockpit around early 1990s when individual pilots perform functions as weight and balance calculations using their personal laptops and common software [57]. Subsequently, the airlines gave a new step by converting all of its operational documentation to electronic format in the mid-1990s [46], and finally with the development of new software, on December 2011, American Airlines became the first airline in the world to be fully Federal Aviation Administration (FAA approved) to use iPads during all phases of flight [11].

1.2.2 Previous studies

The concern about using digital maps in aviation is not new; US military forces have studied and developed the topic since over 20 years, in these studies it is evident that the greatest obstacle is to achieve a standard that satisfies all the staff related to aviation. This is because, regardless of the type of aircraft flying or mission they perform, the cockpit procedures are very systematic [53] [57].

Within military aviation there are many differences between pilots of different aircraft, while the pilots of fighter jets are more open to the implementation of new technologies and optimization of resources within their small cabin space. On the other hand, the pilots of transport aircraft seek to always have backup resources and tend not to abandon the classical methods of air navigation [33].

1.2.3 Regulatory entities

The Colombian aviation regulations of aeronautical charts are defined in the Colombian Aeronautical Regulations 90 (RAC 90), dealing with aeronautical charts for air

navigation, this Colombian standard clarifies everything related to symbols and defines the technical characteristics that must have both physical and digital charting, but it does not define exactly the application of these types of elements within aircraft cabins or dictate guidelines for the proper use of them [1] and in the international scope the Federal aviation Administration (FAA) has the FAA Aeronautical Chart User's Guide in its 12th edition and the INFO 11011 which determines the authorization process for the use of the iPads and Electronic Flight-Bags (EFBs) by the aeronautical authority [25].

In Europe, the regulation authority is the European Aviation Safety Agency (EASA) and in the International level the International Civil Aviation Organization (ICAO) is the organization that determines the rules to be followed by all countries [6]. The International Civil Aviation Organization (ICAO) is a specialized agency that depends from the United Nations, it was established in 1944 and its main function is manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention)[1].

[1] ICAO webpage consulted in 2/03/2016 http://www.icao.int/about-icao/Pages/default.aspx [29]

1.2.4 Previous events

In April 2015, two events related to information technology security were presented. In the first one, hackers broke down the customer´s database of the German airline company Lufthansa, getting access with fake identities, making purchases and obtaining benefits in an unauthorized manner[2]. In the second one, American Airlines had a delay of flights that include the Ronald Reagan International Airport which serves the city of Washington DC due to a single Instrument Landing System (ILS) duplicated chart at the Reagan National Airport, in American's database[3].

These events alerted the information technology security experts allowing that the studies related to information security will increase, as can be seen in figure 1. This has generated that the integrity of the information digital maps be equally important as their availability and new developments seeking to be safer [18].

Outcome	Total	EFB Primary Factor	EFB Contributing Factor
Spatial Deviation	22	12	10
Runway Incursion	4	—	4
Incorrect weight and balance computation	3	2	1
Expired database	2	2	—
Altitude confusion without violation	2	—	2
Deviation from company policy	1	—	1
Aborted takeoff	1	1	—
Incorrect take-off speed, tail strike on rotation	1	1	—
Altitude deviation during declared emergency	1	—	1
Total	**37**	**18**	**19**

Figure 1. Incidents related to the use of EFB occurred until 2009 [18].

1.3 Research Methodology and research questions

For the development of the thesis, a methodology that will help obtain concrete results and easy understanding has been chosen. Similarly, the research questions proposed are intended to cover as many aspects as possible, to serve as a basis for future research.

[2] Dw. consulted in 2/03/2016 http://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698 [23]

[3] Avionics magazine consulted in 2/03/2016 http://www.aviationtoday.com/av/commercial/American-Airlines-Jeppesen-Comment-on-EFB-Crash-that-Grounded-Flights_84925.html#.VvqciOagUZM [9]

1.3.1 Design science framework

To meet the objectives set for this thesis the Design Science Research Method will be used according to [28]. The method is a problem solving process which has seven guidelines as expressed in figure 2.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Figure 2. Design-science research guidelines [28].

The description of how the guidelines in figure 2 are applied in the thesis is the following:

- Design as an Artifact: The aim of the thesis is to produce a collaboration model between the entities that are involved in the air navigation system with digital charts.

- Problem Relevance: There is currently no security-related modeling in this particular subject. The previous studies have been based on statistical data and have used other methods to perform the security risk assessment.

- Design Evaluation: The aviation related workflows are evaluated using the Security Attribute Evaluation Method (SAEM) [14].

- Research Contributions: The modeling of this process along with the collaborations of the different participants will allow to understand in a way more agile the IT risks to which they are exposed and generate effective measures to control them.

• Research Rigor: The use of the collaboration tool of the BPMN framework in order to have a better understanding of the relations between all the participants involved in the process. To perform the security risk assessment the method of Information System Security Risk management will be used (ISSRM) [22].

• Design as a search process: For the implementation of the workflows related to the aviation, the doctrine applied by the Colombian Air Force to all their pilots, will be taken into account. Especially as it regards the use of instruments in the cockpit and the procedures for the flight, also established standards for civilian pilots and air traffic controllers when dealing with the use of digital charts.

• Communication of Research: The results and recommendations of this work could be applied in the ground training that received periodically all the pilots of the Colombian Air Force.

The aim of the thesis is to create a new and innovative model that will represent the relations that occur between the different business models analyzed; Identify risks and threats, and finally propose measures to mitigate the risks found.

1.3.2 Research questions

The main research objective for this thesis is the following:

How to conduct a security risk assessment for digital charting solutions in military aviation?

To achieve this objective, the security risk assessment should be developed taking in consideration the following criteria.

- RQ1: How to develop a security risk assessment for the use of the digital charting in the Colombian aviation?

With the results obtained in the previous step, an analysis is performed in order to verify whether the proposed measures actually meet the objectives.

- RQ2: How to apply the security risk-oriented patterns in the business process?

Finally a strategy must be created to effectively communicate the new procedures to all members of the organization

- RQ3: How to communicate the new security requirements to the employees?

1.4 Thesis structure

The structure of the thesis is the following:

Chapter 2 defines the background of Colombian aviation industry, analysing military and civilian entities that compose it. Subsequently, the modelling tool Business Process Modelling Notation (BPMN) and the method of Information System Security Risk Management (ISSRM) are described.

Chapter 3 develops the security risk assessment to the use of the digital charting in military and civilian aviation entities in Colombia. To demonstrate it, the Security Risk-oriented Patterns (SRP) are used.

Chapter 4 describes the application of the Security Risk-oriented Patterns in the business process, using the method proposed by [5].

Chapter 5 defines the method of communication of the new security requirements to avoid new information security incidents. The type of instruction and the hourly intensity for each entity are proposed.

Chapter 6 performs the evaluations of the proposed solutions that were made, using the Security Attribute Evaluation Method (SAEM) [14].

Chapter 7 draws conclusions based on the findings and discussion of the previous chapters. Then, the research questions in this thesis are answered. Also, an outlook for further research is provided.

2 Background

Colombia, like other South American countries, knowing the experiences of World War I on the use of aviation as a combat weapon, decided the creation of independent air forces, or embedded within the army or navy [41]. This military development that occurred since 1920 in most of the countries, has enabled a rapid growth of its warfighting capabilities, however, these organizations are currently concerned by standardizing its processes according to quality standards, allowing a more effective identification to new threats that they face.

In this chapter the evolution of the aviation industry in Colombia is analysed, taking into account the main representatives of this business model [35]. Subsequently, the modeling tool called Business Process Modeling Notation (BPMN) is studied, and finally, the method of Information System Security Risk Management (ISSRM) is described.

2.1 Aviation industry in Colombia

The Colombian Air Force is a military organization that depends from the Ministry of Defense, it has the ISO 9001 certification in all their processes and follow clear guidelines to maintain high levels of quality in performance. Currently the Colombian Air Force is in the process of modernizing the avionics of its aircraft, one of this, is a strategic plan for the use of iPads by pilots, they serve to set flight routes, navigation and check weather information [26].

At the level of commercial airlines in Colombia the only one with the implementation of fully digital charting on all its aircraft is EASYFLY, a small airline with 20 regional destinations and a very small participation market, with approximately 1 million passengers transported during the year 2015[4].

[4] EASYFLY webpage consulted in 2/03/2016 http://www.easyfly.com.co/px [24]

For the study, the processes developed by the company AVIANCA (*Aerovías del Continente Americano)*, which is the airline leader in the Colombian market[5], with its modern fleet of 180 short, medium, and long haul aircraft. That serve more than 100 direct destinations in 28 countries throughout the American and European continents[6], will be taken into account.

In the relations between the private and the public sector there have always been professional jealousy, the information shared is scarce and mutual aid are practically non-existent. However, when dealing with air navigation, there are strict standards that all the institutions are following, due to the risk involved in their operation. This kind of relationship between all the statements related to the air navigation is the center of study of the thesis, and the aim is to establish how vulnerable the entities are to different IT related attacks.

In Colombia there are around 581 aerodromes, 71 of which are controlled by the aviation authority and eight of them are fully for military operations, the other ones are private owned and territorial entities[7]. The civilian air traffic controller are trained and certified by AEROCIVIL and the military ones receive training both nationally and internationally. The communications and procedures are governed by international standards [25].

2.2 Business Process Modeling Notation (BPMN)

BBMN is an increasingly important standard for process modeling and has enjoyed high levels of attention due the widespread support. This modeling language is popular both in business and IT communities and allows the use of different tools according to the needs of each user [42].

---

5 AEROCIVIL webpage consulted in 2/03/2016 http://www.aerocivil.gov.co/AAeronautica/Estadisticas/Paginas/Inicio2.aspx [2]

6 AVIANCA webpage consulted in 2/05/2016 http://www.avianca.com/en-eu/our-company/corporate-information/corporate-profile.aspx [8]

7 AEROCIVIL webpage consulted in 2/03/2016 http://www.aerocivil.gov.co/Aerodromos/Aeropuertos/Paginas/Inicio.aspx [3]

2.2.1 Basic concepts

The Business Process Modeling Notation (BPMN) is a standard that provides a notation that is readily understandable by all business users. Is made up of a set of graphical elements that are distinguishable from each other [56]. The modeling language is based on the concept of extensibility layers, like the collaboration layer that will be used in this thesis, around basic series of simple core elements [36].

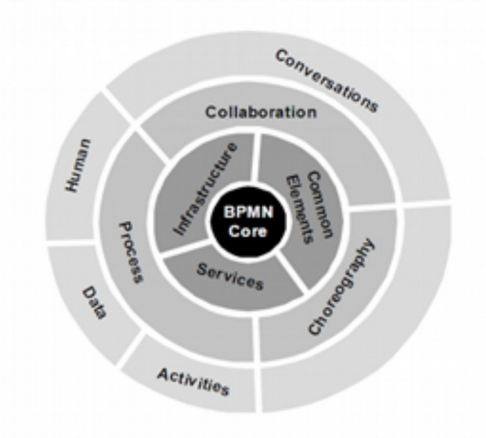

Figure 3. BPMN core and layer structure [36].

2.2.2 Collaborations

Collaborations is a package of the BPMN where the interactions between the participants are shown by message flows, and the participants are represented in two or more pools. When collaboration is defined it is contained in Definitions [36]. Figure 4 shows an example of this type of modeling.

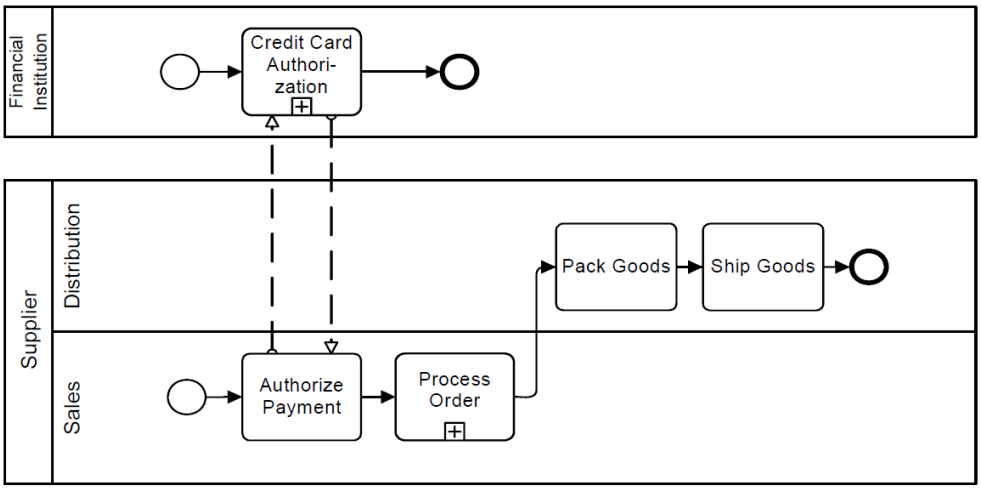

Figure 4. Example of collaboration Model [36].

2.3 Information System Security Risk Management (ISSRM)

ISSRM is a methodological tool that helps to identify easily and implement security requirements in a cost-effective manner for the business process analyzed [22]. Among its many advantages, is that it can be used with various modeling languages and has already been performed in several studies.

In the methodology are proposed three groups of concepts, which they differ by colours as seen in Figure 3. The first group is represented by yellow and are the asset-related concepts, the second one identified by the orange color are the risk-related concepts and finally the last one highlighted by green are the risk treatment-related concepts.

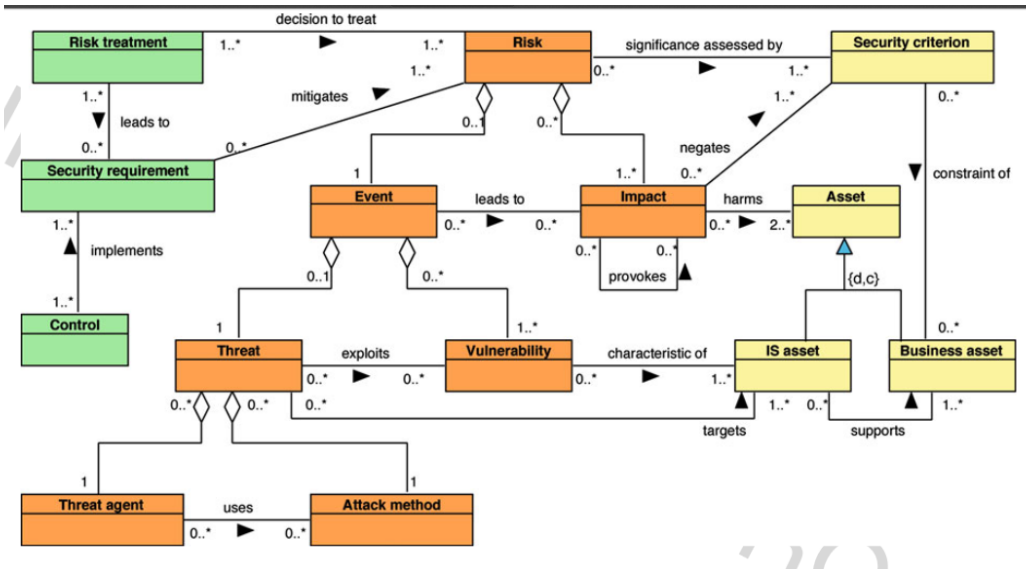

Figure 5. ISSRM Domain Model [22].

In the first group, the important assets are identified and classified into two types, business assets and information system assets. It also is determines the security criterion (Confidentiality, Integrity and Availability) that characterise the security needs of the asset.

For the group represented by the orange color is identified the Threat agent that uses an Attack Method to become a Threat to the asset. By exploiting a Vulnerability in the process this Threat causes an Event that leads to an Impact, Finally, by knowing the Impact and the Event, the Risk that the business asset is exposed to can be determined.

The last group will be the decisions to treat the risk identified, the categories of risk treatment are: avoidance, reduction, transfer and retention. The risk treatment is accomplished by applying a security requirement, that is based on the implementation of a Control [31].

3 Security Risk Assessment

The aim of this chapter is to develop a security risk assessment to the business process. This is achieved by answering the given research question:

- RQ1: How to develop a security risk assessment for the use of the digital charting in the Colombian aviation?

The research question is divided into three sub-questions allowing develop in stages the security risk assessment:

  - Rq1.1: What methods can be used to define the business process model?
  - Rq1.2: What information can be exchanged between collaborating systems?
  - Rq1.3: What level of trust exists between collaborating systems?

To answer the first sub-question, the Security Risk-oriented Patterns (SRP) are used. A pattern can be characterized as a solution to a problem that arises within a specific context [58]. This method allows introducing security requirements to the business processes through the collaboration between business and security analysts [5]. For the textual description the Security Risk-oriented Pattern Template proposed by [5] is used. When it comes to the use of patterns, various aspects are considered; the aim is to avoid the overlaps between them, taking into account the domain concepts of security: confidentiality, integrity and availability [27].

The second and third sub-questions are developed through performance of the security risk modelling with BPMN and the BPMN extensions proposed by [7]. In first instance each pattern is represented by the asset-related concepts that allow the identification of the business asset, information system asset and the security criterion. Later, the risks-related concepts are exposed; the diagrams show the impact generated by the occurrence of the event which affects the security criterion. Finally, the controls implemented to mitigate the risk are illustrated in the risk treatment-related concepts diagram.

3.1 SRP1: Secure the integrity of data transmitted between business entities

The first pattern is to secure the integrity of the communication between two business entities [10]. For this study, the pilot is considered as the client who is using an EFB and requesting a digital map file to perform the air navigation of a flight. The company or the supplier is the business entity providing this service.

Table 1. SRP1: Secure the integrity of data transmitted between business entities

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Secure the integrity of data transmitted between business entities
Pattern Description	This pattern secures the integrity of the data transmitted between the business entities.
Related Pattern(s)	No related patterns.
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	Digital map file.
Information System Asset	Electronic Flight Bag.
Security Criteria	Integrity of digital map file.
RISK ANALYSIS & ASSESSMENT	
Risk	The client faces loss of the integrity of the digital map file due an attacker send malicious file to client after intercept the communications using man-in-the-middle attack.
Impact	Loss of integrity of the digital map file.
Event	An attacker sends malicious file to client after intercepting the communications using man-in-the-middle attack[8].
Threat	An attacker sends malicious file to client
Vulnerability	Client does not verify hashes from downloaded digital map files.
Threat Agent	An attacker who intercepts communications using man-in-the-middle attack.
Attack Method	Using man-in-the-middle attack to send malicious digital map file.
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk avoidance
Security Requirement	Verify the authenticity of the file received
Control	- Compare the hash given by the company with the one obained from the received file. -Verify digital signature

[8] CWE webpage consulted in 8/04/2016 http://cwe.mitre.org/data/definitions/300.html [20]

In figure 6, a client requests a digital map file in order to perform a flight, via this application, the company demands the proper credentials, and after verifying them, sends the digital map file that was requested by the client.

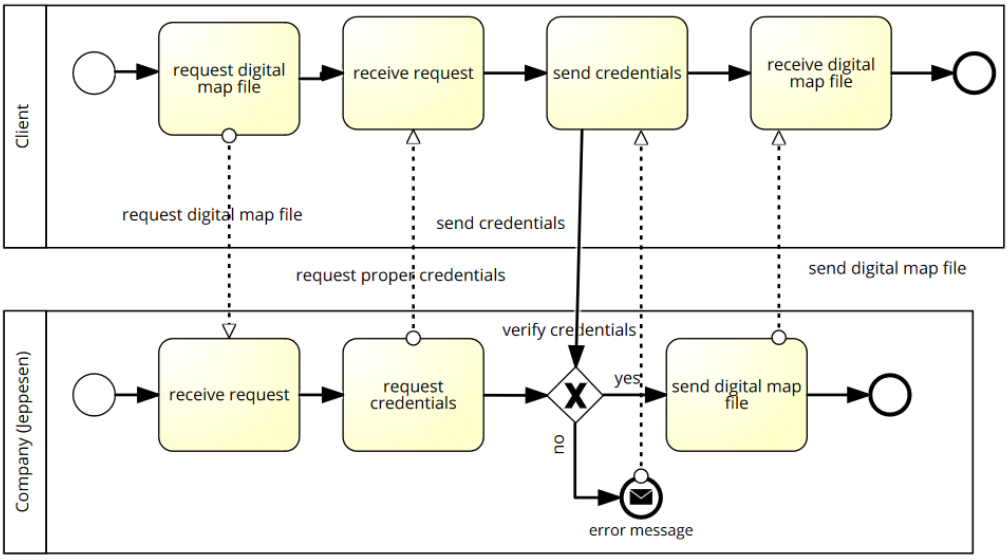

Figure 6. SRP1: Asset-related concepts

The figure 7 describes the risk that faces the business process, due the vulnerability that occurs when one does not verify the hashes of the received file. When this event happens, the integrity of the digital map file is compromised.

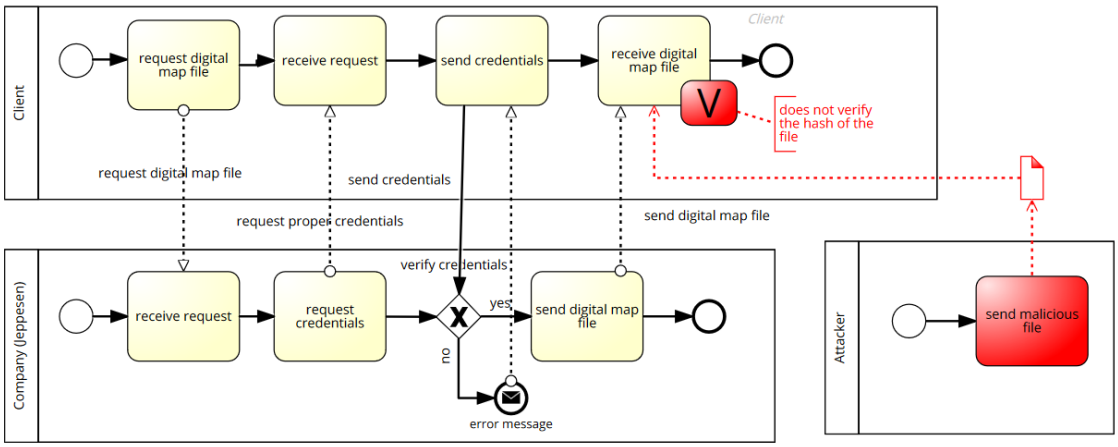

Figure 7. SRP1: Risk-related concepts

Figure 8 is representing the control applied to avoid the risk of loss the integrity of the file when the attacker sends a malicious file.

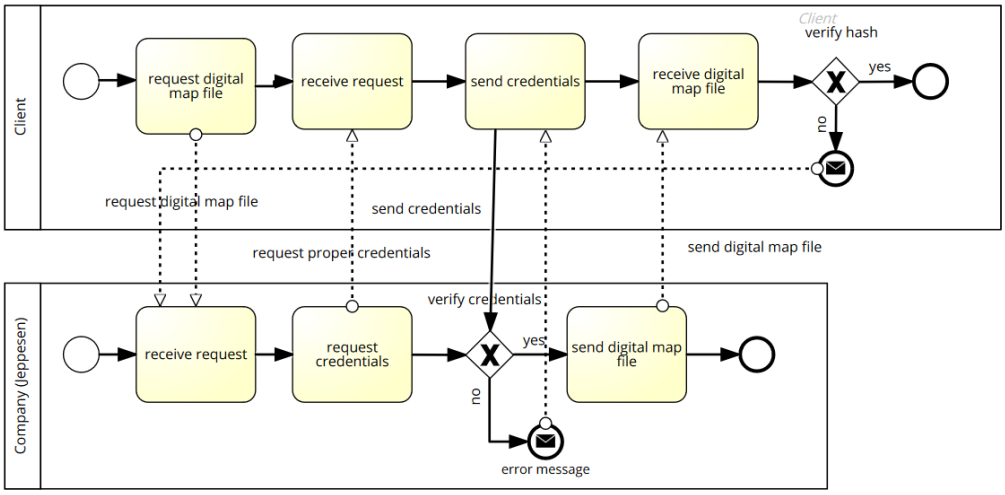

Figure 8. SRP1: Risk treatment-related concepts

3.2 SRP2: Secure the confidentiality of data transmitted between business entities

The second pattern is to secure the confidentiality of the communication between two business entities [55]. In this scenario, due the characteristics of the transmission medium, the data could be manipulated, affecting the confidentiality of the digital map file sent by the company.

Table 2. SRP2: Secure the confidentiality of data transmitted between business entities

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Secure the confidentiality of data transmitted between business entities
Pattern Description	This pattern secures the confidentiality of the data transmitted between the business entities.
Related Pattern(s)	No related patterns.
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	Digital map file.
Information System Asset	Electronic Flight Bag.
Security Criteria	Confidentiality of the digital map file.
RISK ANALYSIS & ASSESSMENT	

Risk	Attacker intercepts transmission medium and manipulate the data, due is not sent encrypted leading the loss of confidentiality of the digital map file.
Impact	Loss of confidentiality of the digital map file.
Event	Attacker intercepts transmission medium and manipulate the data due is not sent encrypted.
Threat	Attacker intercepts transmission medium to manipulate the data.
Vulnerability	The data is not sent encrypted.
Threat Agent	An attacker who intercepts transmission by establishing a proxy.
Attack Method	Intercept transmission medium by establishing a proxy between input interface and company[9].
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk Reduction.
Security Requirement	Make data unreadable to attacker.
Control	Cryptographic algorithm.

The figure 9 represents the collaboration between the business entities. The asset (digital map file) is sent from the company to the client, using a transmission medium.

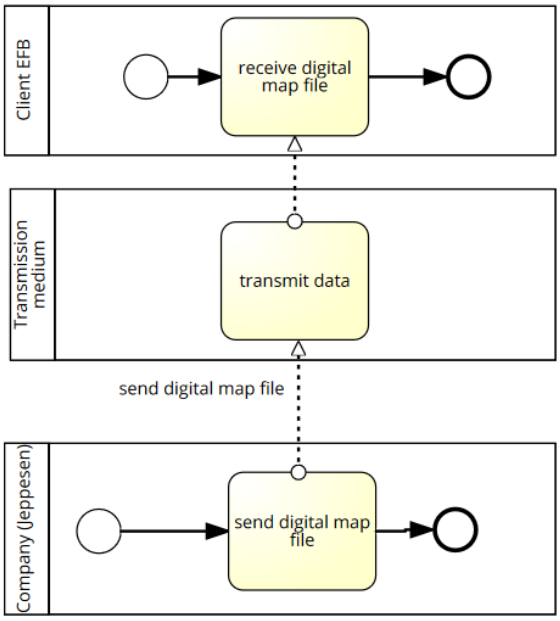

Figure 9. SRP2: Asset-related concepts

[9] CAPEC webpage consulted in 8/04/2016 http://capec.mitre.org/data/definitions/94.html [15]

Figure 8 demonstrates the risk that faces the confidentiality of the data when transmitted unencrypted. The attacker takes advantage of this vulnerability and can get the data.

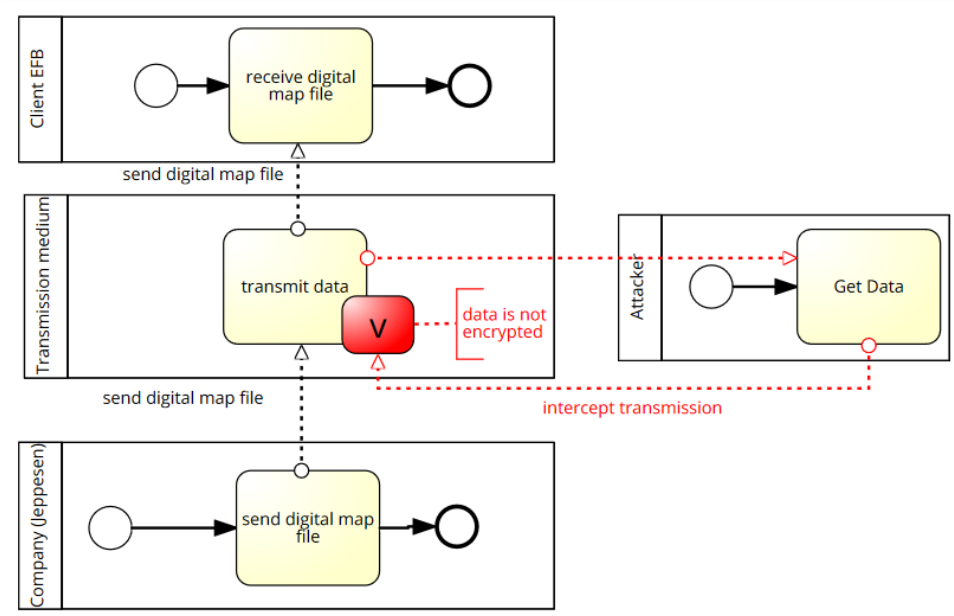

Figure 10. SRP2: Risk-related concepts

As may become evident from the figure 11, a control is applied to fulfill the security requirement to make the data unreadable to the attacker, ensuring the confidentiality of the transmitted digital map file.

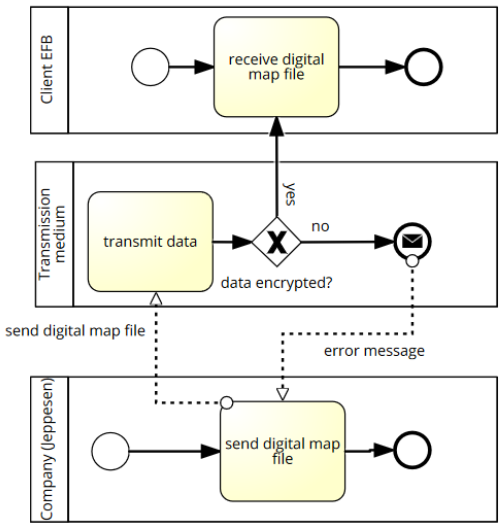

Figure 11. SRP2: Risk treatment-related concepts

3.3 SRP3: Protecting information system (IS) from Denial of Service (DoS) attack

To ensure that client's business process is in order, the company must permanently be available with its service. This SRP analyses a kind of a DoS attack [32].

Table 3. SRP3: Protecting IS from DoS Attack.

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Protecting IS from DoS Attack.
Pattern Description	This pattern ensures the availability of the digital maps downloads of the company.
Related Pattern(s)	No related pattern
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	Service of digital maps downloads.
Information System Asset	Server.
Security Criteria	Availability of the service.
RISK ANALYSIS & ASSESSMENT	
Risk	An attacker causes the loss of the availability of the service of digital maps downloads because the server crashes when consuming all resources by sending a large number of TCP SYN packets to the server port which allows unlimited number of connections.
Impact	Loss of the availability of the service of digital maps downloads because the server crashes when consuming all the resources.
Event	Attacker sends a large number of TCP SYN packets to the server port which allows unlimited number of connections.
Threat	Attacker can consume all the resources of the server with a large number of requests.
Vulnerability	The server allows unlimited number of connections [31]
Threat Agent	An attacker with the capability to initiate new connections in a faster rate than the server can fulfil the pending connections.
Attack Method	Attacker sends a large number of TCP SYN packets to the server port [19].
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk reduction
Security Requirement	Filter the incoming packets from the same IP address.
Control	Router configuration

Figure 12 represents the collaboration between the business entities, and the service provided by the company of digital maps.

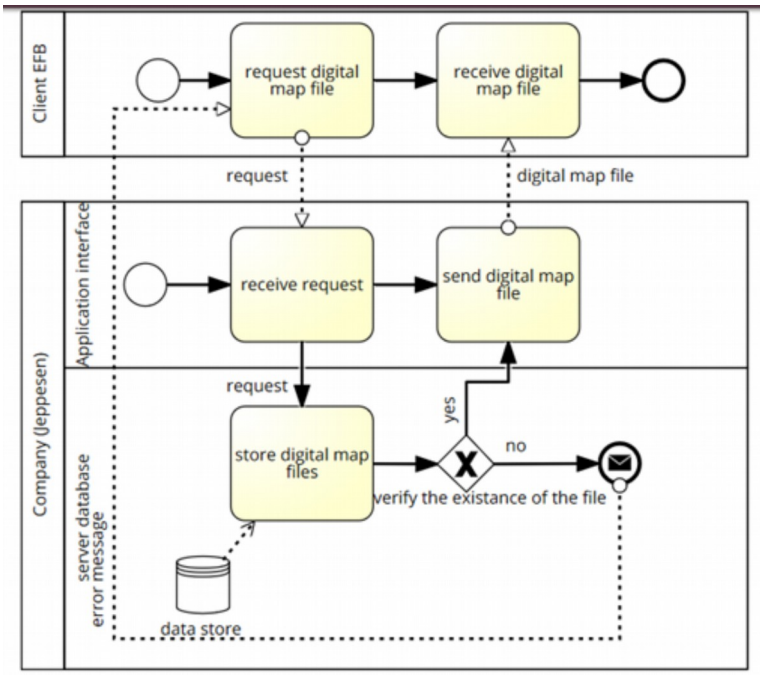

Figure 12. SRP3: Asset-related concepts

The figure 13 highlights the attack method developed by the attacker to the server port. By sending TCP SYN packets request, the server crashes when consuming all resources. The exploited vulnerability is that this port allows unlimited TCP connections.

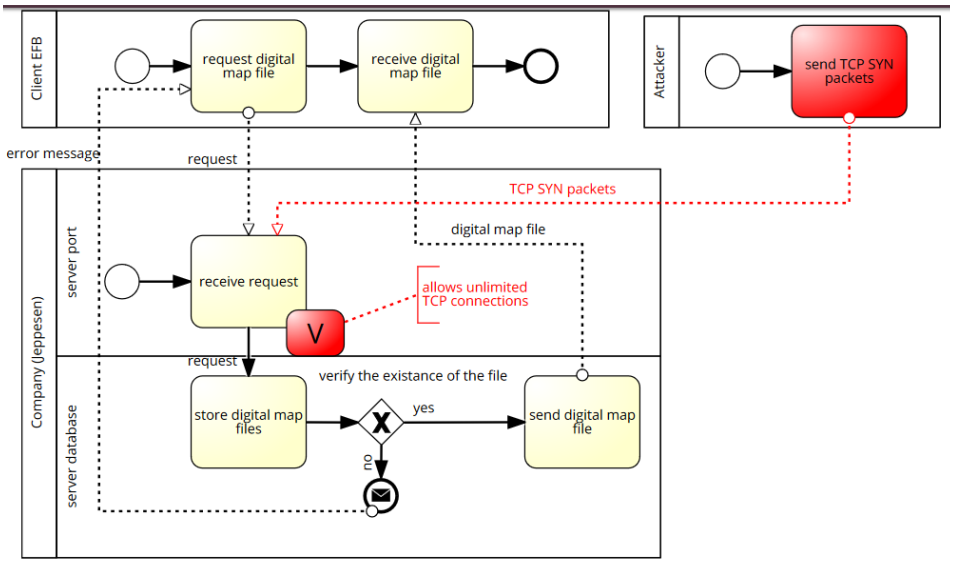

Figure 13.SRP3: Risk-related concepts

Proper router configuration is the control established, as can be seen in figure 15, thus, the risk of an attack is mitigated meeting the security requirement proposed.

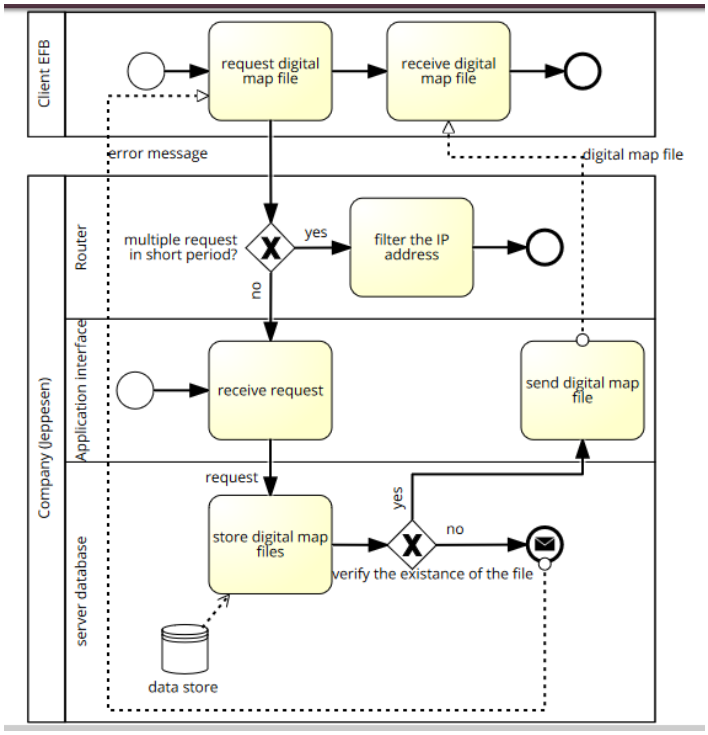

Figure 14. SRP3: Risk treatment-related concepts

3.4 SRP4: Preventing digital maps files leakage

The exclusive possession of digital maps is one of the main assets of the companies providing the service of electronic charts [57]. For this reason, protect the confidentiality of these elements is critical to their business model, the following pattern describes the necessary steps to do it.

Table 4. SRP4: Preventing digital maps files leakage.

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Preventing digital maps files leakage
Pattern Description	How to protect the confidentiality of the data in the server from attacker when an exception is raised in the system.
Related Pattern(s)	No related pattern
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	digital maps files

Information System Asset	Server database
Security Criteria	Confidentiality of digital maps files
RISK ANALYSIS & ASSESSMENT	
Risk	An attacker causes loss of confidentiality of the digital maps files after generating exception by providing invalid inputs to the server that is absence of exception handling techniques.
Impact	Loss of confidentiality of the digital maps files
Event	An attacker gets digital maps files after generating exception by providing invalid inputs to the server that is absence of exception handling techniques.
Threat	An attacker generates exception by providing invalid inputs.
Vulnerability	Absence of exception handling techniques[10]
Threat Agent	An attacker who wants digital maps files
Attack Method	Tries to generate exception by providing invalid inputs [31].
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk reduction
Security Requirement	Address error to stop the process
Control	The source code should implement adequate unexpected exception handling [31].

Figure 15 represents the relationship between the client and the company business process, to a request a digital map file is sent.

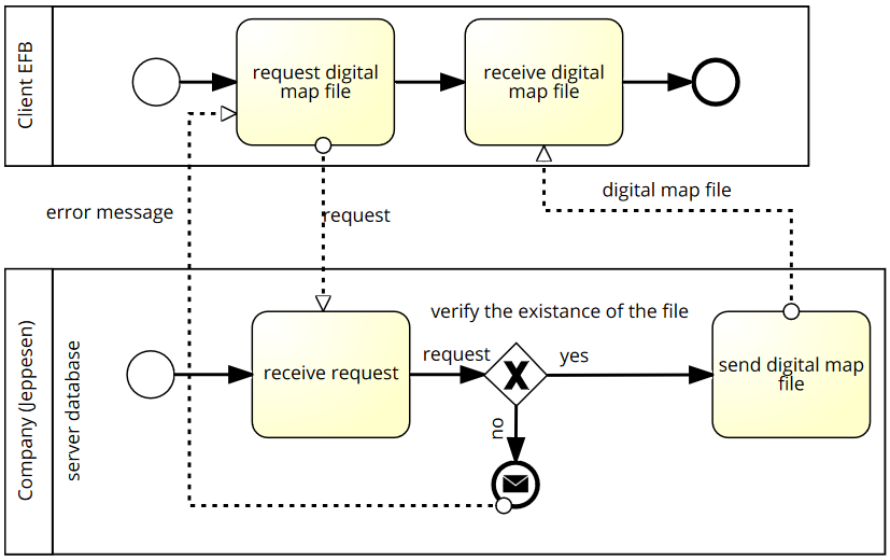

Figure 15. SRP4: Asset-related concepts

[10] OWASP webpage consulted in 15/04/2016 https://www.owasp.org/index.php/Exception_handling_techniques [38]

The figure 16 describes the vulnerability of the server database, which takes place due the absence of exception handling techniques; they allow invalid requests and send the file to the attacker, causing loss of confidentiality of the information stored in the server.

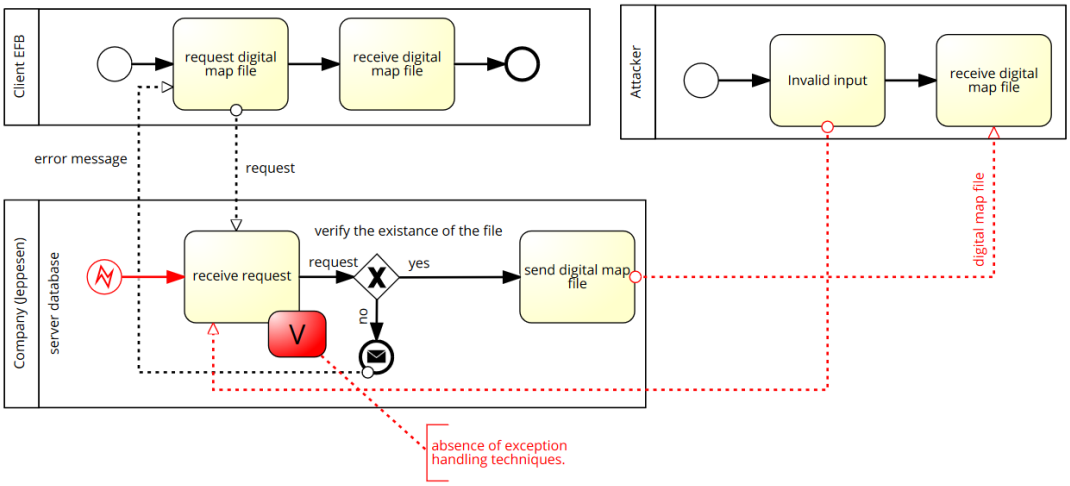

Figure 16. SRP4: Risk-related concepts

A proper source code is implemented as a control to ensure that when an error occurs, the process stops. Figure 17 represents how the security requirement is accomplished.

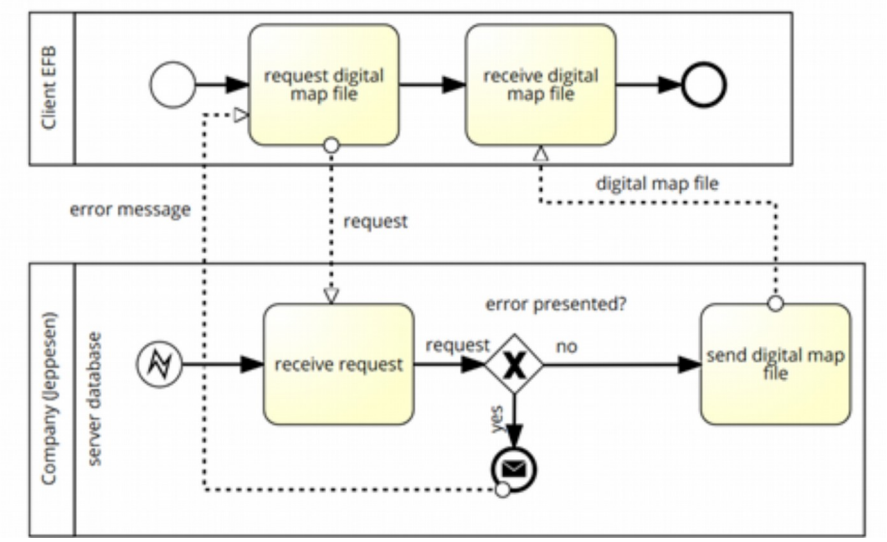

Figure 17. SRP4: Risk treatment-related concepts.

3.5 SRP5: Preventing information leakage due to SQL injection.

Injecting SQL code into a web application requires little effort by those, who understand both the semantics of the SQL language and CGI scripts [13]. This is the reason why this pattern is taken into account, and must follow the security requirements to avoid the loss of confidentiality of the digital maps files.

Table 5. SRP5: Preventing information leakage due to SQL injection.

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Preventing information leakage due to SQL injection.
Pattern Description	The pattern describes how to prevent the leakage of information when the attacker uses SQL injection to get access to server database.
Related Pattern(s)	No related pattern
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	Digital maps files
Information System Asset	Server database
Security Criteria	Confidentiality of digital maps files
RISK ANALYSIS & ASSESSMENT	
Risk	An attacker generates loss of confidentiality of the digital maps files after getting access by using SQL injection to the server due the user interface input is not filtering escape characters.
Impact	Loss of confidentiality of the digital maps files
Event	An attacker gets digital maps files after getting access with SQL injection due the user interface input is not filtering escape characters.
Threat	An attacker tries to get the digital maps using SQL injection
Vulnerability	User interface input is not filtering escape characters.
Threat Agent	An attacker who wants digital maps files
Attack Method	Use SQL injection for getting access and obtain digital maps files[11].
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk reduction.
Security Requirement	Avoid the input of escape characters.
Control	Use of prepared statements.

[11] OWASP webpage consulted in 15/04/2016 https://www.owasp.org/index.php/SQL_Injection [39]

Figure 18 identifies the business asset and the security criterion that should be protected.

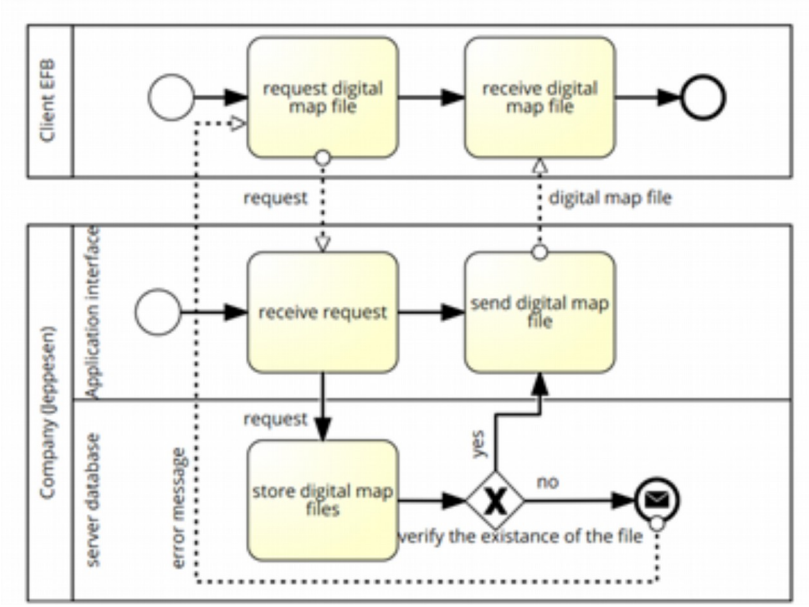

Figure 18. SRP5: Asset-related concepts

The vulnerability of the user interface is exploited by the attacker, who gets an access to the server database, as can be seen in figure 19.

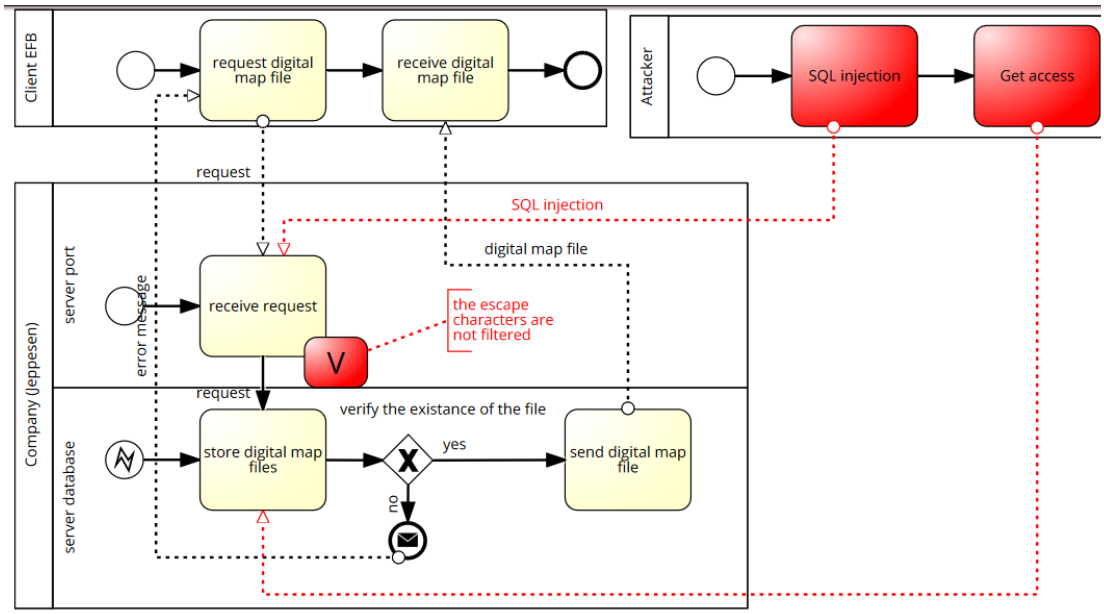

Figure 19. SRP5: Risk-related concepts

The control applied is to accept only prepared statement in the user interface query, which is represented in figure 20.

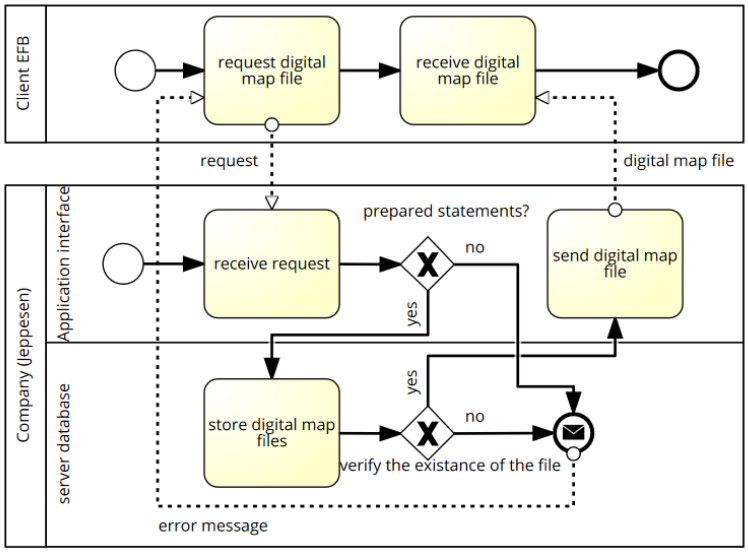

Figure 20. SRP5: Risk treatment-related concepts

3.6 SRP6: Mitigating Software-as-a-Service (SaaS) user request forgery.

In SaaS, the client has to depend on the provider for proper security measures [51]. Nevertheless, a user may have a previously installed malicious application and execute it, while authenticating to the SaaS application. The following pattern mitigates this risk that affects the business process.

Table 6. SRP6: Avoiding SaaS user request forgery.

ORGANISATIONAL SCENARIO & SECURITY CONTEXT IDENTIFICATION	
Pattern Name	Mitigating Software-as-a-Service (SaaS) user request forgery.
Pattern Description	The pattern mitigates the risk of execute a malicious application into the provider system, when a user is unaware that has a threat in its system.
Related Pattern(s)	No related pattern
ASSET IDENTIFICATION & SECURITY OBJECTIVE DETERMINATION	
Business Asset	Authentication process

Information System Asset	Web application interface
Security Criteria	Integrity of the authentication process
RISK ANALYSIS & ASSESSMENT	
Risk	An attacker generates loss of integrity of the authentication process after executes a malicious application into the server of the provider due it believes that is only interacting with the trusted user.
Impact	Loss of integrity of the authentication process.
Event	An attacker who wants to install a malicious application into the server of the provider due it believes that is only interacting with the trusted user.
Threat	An attacker installs a malicious application into the server of the provider.
Vulnerability	The provider believes that is only interacting with the trusted user.
Threat Agent	An attacker who wants to install a malicious application into the server of the provider
Attack Method	An attacker installs malicious application into the user's system and convinces the user to execute it while authenticated to the provider's application[12].
RISK TREATMENT & SECURITY REQUIREMENTS	
Risk Treatment	Risk reduction.
Security Requirement	Secure the communications between users and provider
Control	Use secure proxy service

Figure 21 represents the normal process when a user is requesting access to the provider.

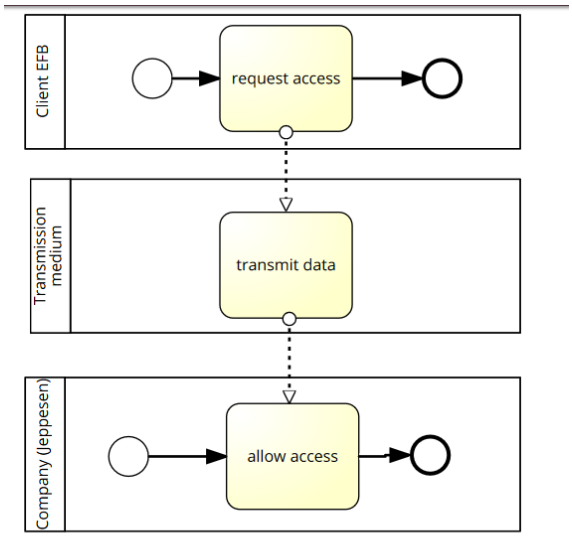

Figure 21. SRP6: Asset-related concepts

[12] CAPEC webpage consulted in 8/04/2016 http://capec.mitre.org/data/definitions/510.html [16]

The vulnerability that the provider trusts that is only interacting with the user is exploited by the attacker, it allows to execute a malicious program into the system of the provider, as can be seen in figure 22.

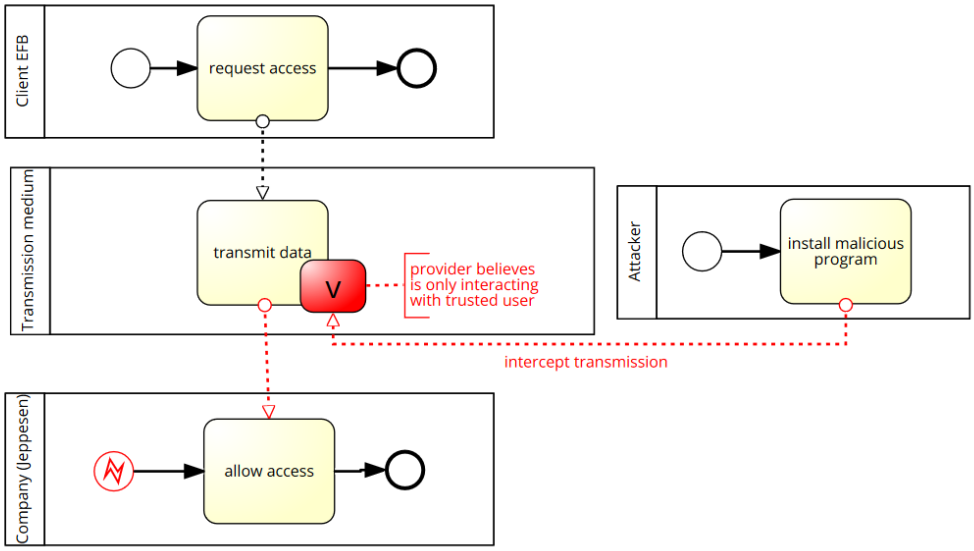

Figure 22. SRP6: Risk-related concepts

To mitigates the risk is implemented a control, allows the use only through a secure proxy service. Figure 23 represents this security requirement.

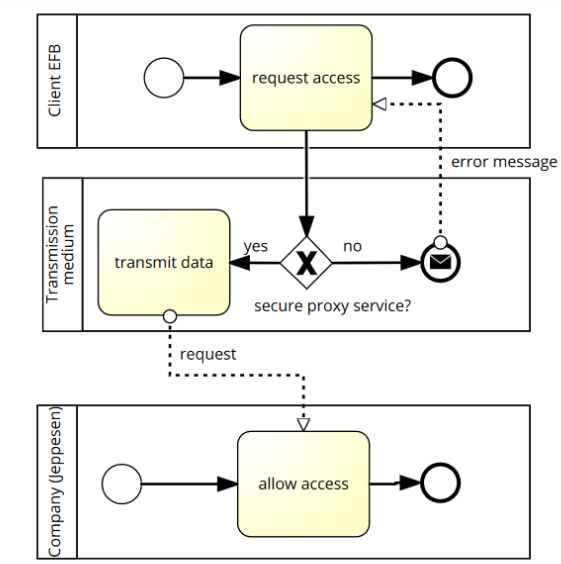

Figure 23. SRP6: Risk treatment-related concepts

3.7 Conclusions

In this chapter, six Security Risk-oriented Patterns (SRP) were described. To represent them, the Business Process Modeling Notation (BPMN) modeling tool was used. The method allows identifying all assets and risks of the business model; likewise, the relationships between entities were represented using the tool Collaborations of BPMN. Finally, security requirements were established.

In order to perform a security risk assessment to the use of the digital charting in the Colombian aviation the following research questions were presented:

- RQ1: How to develop a security risk assessment for the use of the digital charting in the Colombian aviation?
    - Rq1.1: What methods can be used to define the business process model?
    - Rq1.2: What information can be exchanged between collaborating systems?
    - Rq1.3: What level of trust exists between collaborating systems?

The first sub-question was solved by using the method of SRP and modeling by BPM. The graphical representation simplifies the identification of the risks that the business process model faces, therefore, security requirements that mitigate the risks were proposed. The main limitation of the application of this method is that there is a lack of theoretical support while choosing the controls that meet the security requirements. Such election is made subjectively based on experience of the business model analyst.

The second and third sub-questions were answered using the tool Collaborations of BPMN, this allowed the graphical representation of the relationships between entities. However, the process was difficult to perform, because of the complexity for determining the trust between entities with different objectives and business model.

This first step leads to the next chapter, where detailed discussion of security controls proposed is made, in order to meet the security requirements.

4 Pattern application

In previous chapter, six (6) Security Risk-oriented Patterns (SRP) were described. However, these patterns have not yet been implemented to secure the business process. Therefore, in this chapter the following research question is developed:

- RQ2: How to apply the security risk-oriented patterns in the business process?

The research question is broken down into two sub-questions in order to have a clear criterion about the best choice:

  - Rq2.1: What methodology should be used to apply the security risk-oriented patterns in the business process?
  - Rq2.2: Which is the best criterion to choose the security controls?

The first sub-question is acknowledged when the method proposed by [5] is applied, like the extended BPMN using padlocks to annotate business processes with security requirements proposed by [43]. The guidelines consist of seven (7) steps, as described in figure 24.

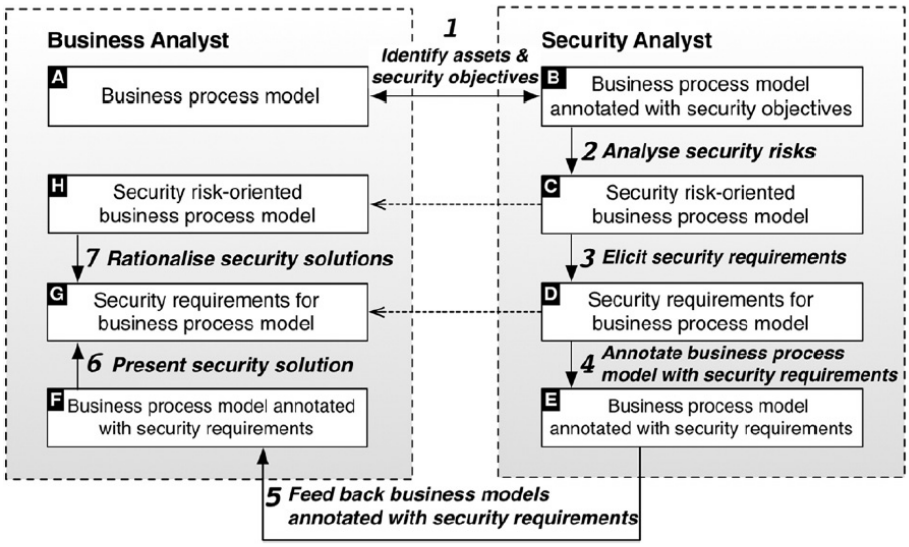

Figure 24. Steps of the method to secure business processes [5].

Taking into account the suggested steps, the following workflows are obtained. Applying them on the visualisation made in the previous chapter, allows determining the cost of the security requirements, based on the overall risk level. These measures justify the security solution that should be implemented into the security control [5] in response to the second sub-question.

4.1 SRP1

For the first pattern the identifying business asset is the digital map file; the risk that it faces is the loss of integrity, which appears when the attacker sends a malicious file, after he/she has intercepted the communications with the provider. The following step is to identify the security criterion, for this case, it is the integrity of the digital map file. Later, the security requirement that must be accomplished is identified. To achieve this requirement, two controls are proposed. Verifying the digital signature and checking that the hash of the file obtained matches with the one that provides the company.

With these results, a rasionalisation about the security requirements is made. The cost that is required for its implementation is minimal, the two can be achieved by establishing strict policies on handling EFBs devices. The compliance of these controls will prevent that the risk appears again. These steps are expressed in figure 25.

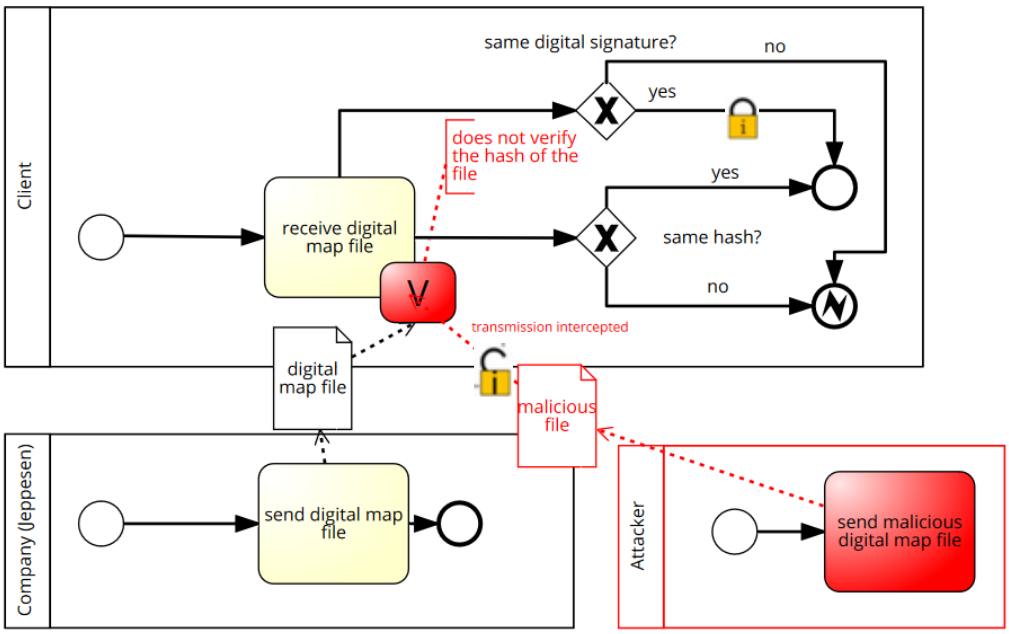

Figure 25. Applied SRP1.

4.2 SRP2

The second pattern is to ensure the confidentiality of data when it is transmitted, in first instance, the business and information system assets are identified. Later, the risk that faces the transmission medium is exposed, that risk occurs when the data is not encrypted. There is a need of a security requirement that will allow mitigating this risk and making the data unreadable to the attacker. To achieve this, three security controls could be applied; the first one, use a public key signed by a Certification Authority (CA), then, the use of a crypto algorithm is proposed, and final option is to exchange public keys using a secure channel.

The cost / benefit relation between the controls is different, however, the use of the crypto algorithm is the control that best mitigates the risk and ensures to keep the confidentiality of the digital maps files transmitted through the medium.Figure 26 represents this rationalisation.

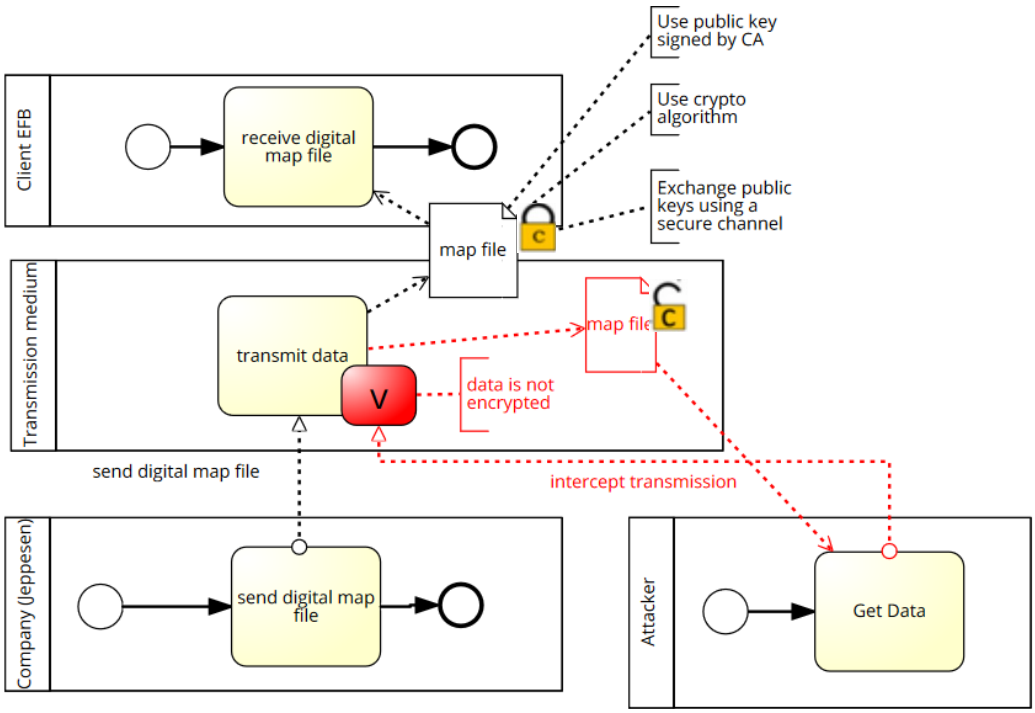

Figure 26. Applied SRP2.

4.3 SRP3

The service availability of downloading the digital maps is the security criterion that harms the risk, which is presented in this pattern. The attacker uses an attack method of sending multiple TCP SYN packets in a short period of time, causing the server running out of resources, thus, this attack can be done because it is exploiting not having proper configuration. The portal service for downloading the digital maps files is the identifying business asset, to protect it, the security requirement of filtering the incoming packets from the same IP address in a short period of time, must be achieved.

A security control in the server configuration is established, when multiple requests are presented in a short period of time, the IP address that makes the request is filtered, allowing to maintain service availability for legitimate users. These steps are represented in the figure 27.

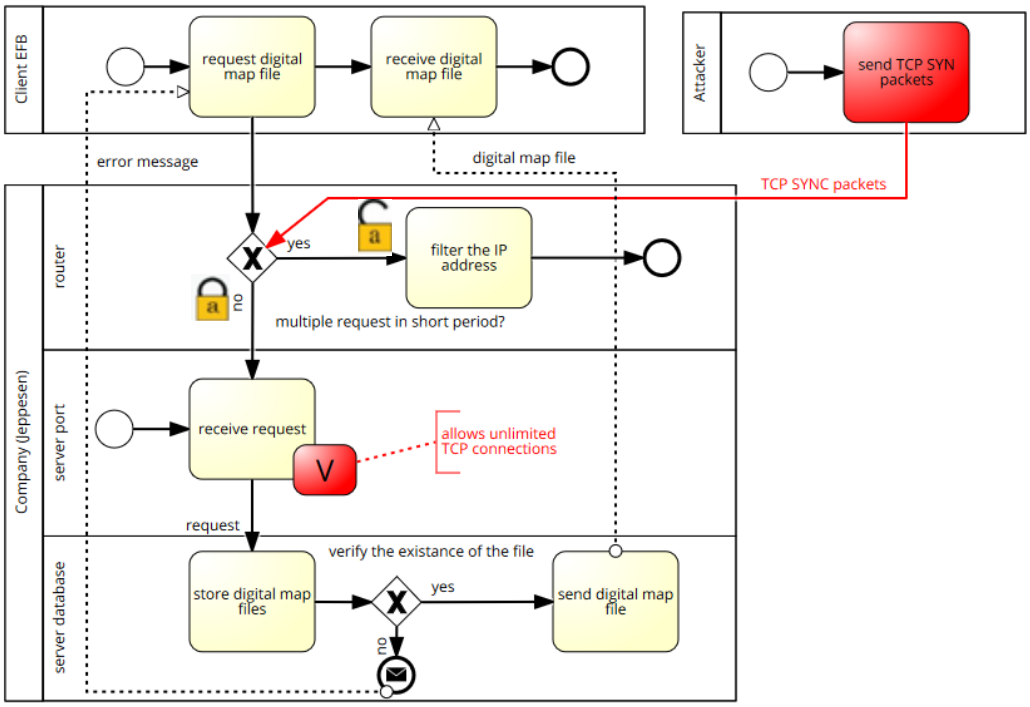

Figure 27. Applied SRP3.

4.4 SRP4

The business asset that is identified by studying the applicability of this pattern, are the digital maps files. The confidentiality of the asset is the security criterion which is being harmed when the risk occurs. As there is absence of exception handling techniques, the attacker exploits this vulnerability by sending multiple invalid inputs. To mitigate this risk, a security requirement of stopping the process when an error occurs should be implemented.

Proper programming of the source code is the security control proposed, this measure does not require additional costs in hardware implementation and allows accomplishing the security requirement. Figure 28 exposes all the steps previously mentioned.

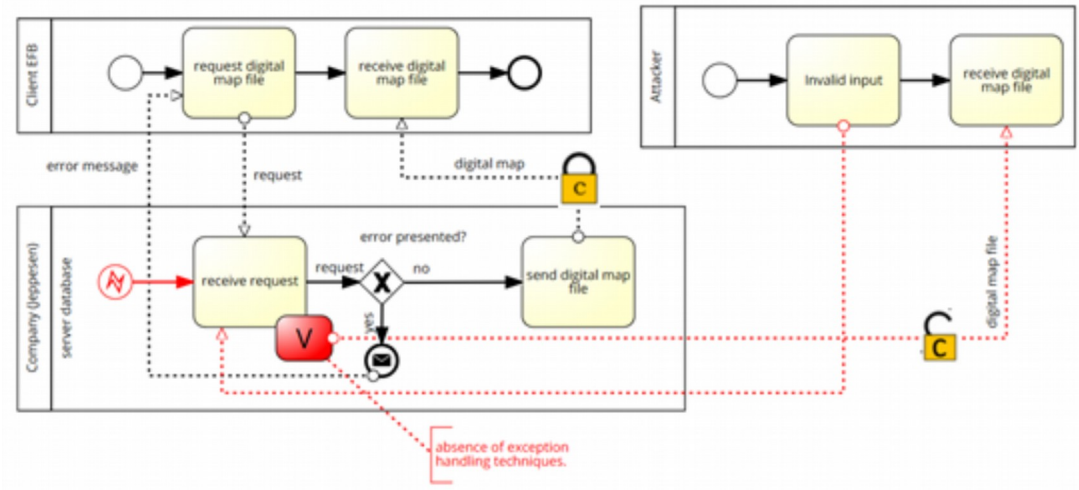

Figure 28. Applied SRP4.

4.5 SRP5

This pattern identifies the security criterion that should be protected, which is the confidentiality of the digital maps files that are stored in the server of the provider. In this case the attacker uses a SQL injection attack in the company's interface input; this generates an unwanted access to the system, because the escape characters are not filtered in the interface. A security requirement that avoids the input of the escape characters should be implemented.

There are two security controls that could be established. The first, using proper configuration of the user interface which will be allow just to use prepared statements. The second, which is graphically represented in the figure 29; it detects when dynamic SQL is happening, stops the process and sends an alert that allows warning the company when these kind of attacks affects it.

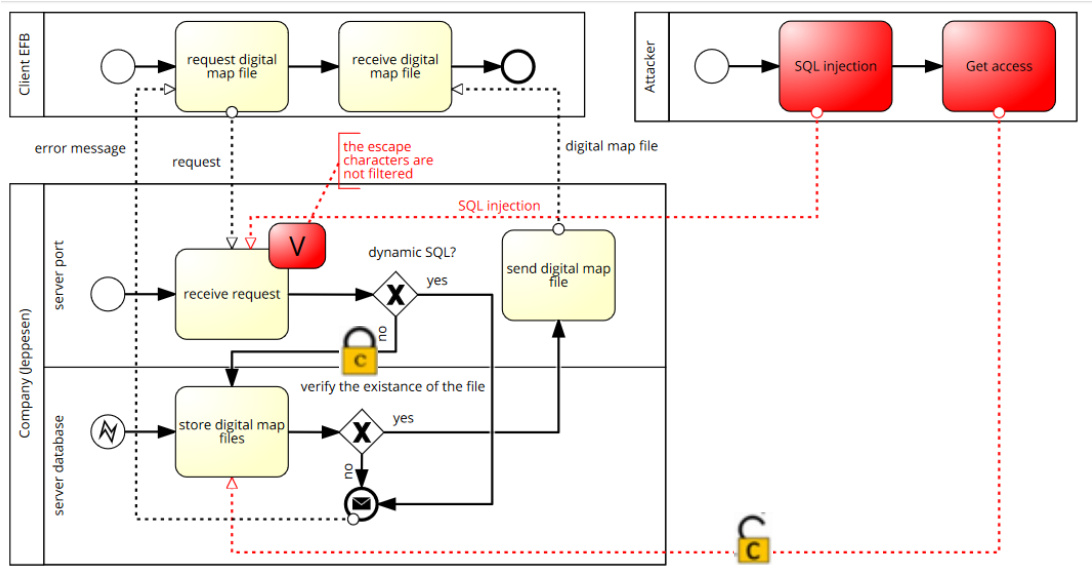

Figure 29. Applied SRP5.

4.6 SRP6

The first step is to identify the business asset, which in this pattern is the authentication process. The integrity of the asset is harmed when an attacker intercepts the transmission and executes a malicious program, because the transmission medium is not protected and the provider believes that is only interacting with a trusted user.

Later, a security requirement that mitigates this risk is set forth. To ensure that the communications between the user and the provider are secure, several security controls can be implemented. One of them, which has a better relation cost / benefit, is to develop a proxy between the user and the provider, avoiding that the communications could be intercepted. These steps are represented in the figure 30.

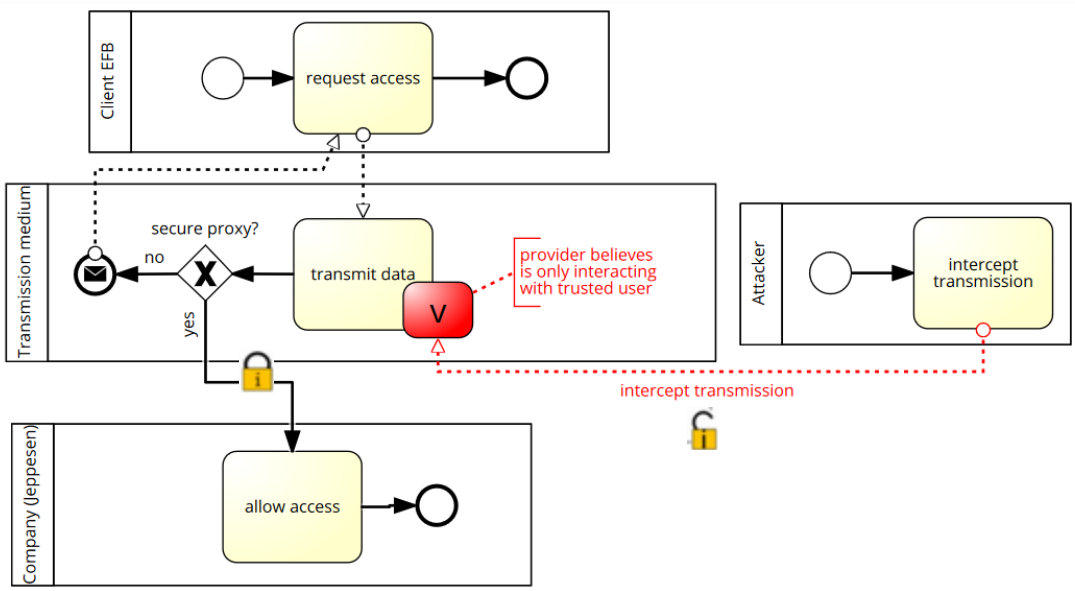

Figure 30. Applied SRP6.

4.7 Conclusions

The security risk-oriented patterns in the business process were applied in this chapter, considering giving answer to the following research questions:

- RQ2: How to apply the security risk-oriented patterns in the business process?
    - Rq2.1: What methodology should be used to apply the security risk-oriented patterns in the business process?
    - Rq2.2: Which is the best criterion to choose the security controls?

To respond the first sub-question, the aforementioned security patterns were applied using the method of securing the business process proposed by [5]. With this study the security controls that mitigate the risk faced by the business model were obtained, they were compared, and the security controls with the best cost-benefit ratio were proposed.

This method simplifies the analysis, allowing the easy identification of the vulnerabilities exploited by the attackers and generates faster security countermeasures to face it. The graphical representation provides an overview of the business model, allowing that the comparison of security controls is made based on objective criteria of the nature of business.

It was determined the cost-benefit ratio as the criterion to choose the security controls, thereby responding to the second sub-question. The limitation of this approach is that it must have an abundance of sources of information to avoid subjectivity when evaluating.

The measures to be applied should be properly communicated to all members of the organization, in the next chapter the best way to transmit these requirements is studied.

5 Communication within the organization

Given the results obtained in the previous two chapters, the following research question is developed:

- RQ3: How to communicate the new security requirements to the employees?

In this chapter the given research question is answered, dividing it into two sub-questions to analyze different approaches:

  - Rq3.1: Which is the most effective method for communicating the information?

  - Rq3.2: What level of security should be handled when transmitting information?

To answer the first sub-question one must take into account that during their entire career, pilots receive constant preparation; this ongoing training is the best scenario to communicate the new measures proposed in the previous chapters, to all members involved, for two reasons mainly. First, these instructions are mandatory, and secondly, pedagogy is based on very strict standards that are similar to the lessons offered by other training centers.

The following chapter describes a proposal for transmitting a secure communication for different entities, considering their business model, their capabilities and the current resources. In this way, the second sub-question is answered. Firstly, the training model for the Colombian Air Force is described, later, the educational model of Avianca is related, and finally, the instruction of the Air Traffic Controllers (ATC) is taken into discussion.

5.1 Training in Colombian Air Force

The pilot training is divided into three phases, in each one of them the apprentices acquire new skills, which allows them to perform in different aircrafts. The lessons are given by active members and retired pilots, taking into account the strict procedures and rules set forth by the educational institution manual [26].

5.1.1 Primary flight training

It is the initial phase of pilot training, the total programme of study is eighty (80) hours, divided into thirty five (35) theoretical and forty five (45) practical. The proposal is included within the academic plan one (1) hour for recognition and use of Electronic Flight-bags or iPads. In the practical part no instructions are proposed, due to the characteristics of the aircraft flown and type of missions performed.

5.1.2 Basic pilot training

During this phase, the pilots have already had contact with the aircraft and have developed some flight hours. They may choose one of the following kinds of aircrafts: fixed wing (airplane) or rotary wing (helicopter), however, the study programme is the same for both. The course has total of one hundred (100) hours, thirty (30) of them theoretical and the other seventy (70) practical.

For this period, it is proposed to include three (3) theoretical hours, which would be: interpretation of digital charts, handling of EFBs and information security vulnerabilities for this equipment. For the practical part, five (5) hours of actual operation of the device are proposed, allowing pilots to face real problems in the operation of the equipment.

5.1.3 Changing aircraft training

Every time a pilot is assigned to another type of aircraft, he/she must perform this training, which consist in eighty (80) hours, divided into twenty (20) theoretical and sixty (60) practical, this instruction updates the trainee with the aircraft capabilities, similarly to the threats that he/she may face. Therefore, it is the proper slot to give two (2) theoretical hours and one (1) practical hour of new information security threats in the navigation system through digital charts.

5.2 Training in Avianca

Avianca has a training school that allows all staff to be trained and kept up to date through new equipment and regulations courses [44]. Unlike other schools, to become a member of this organization, pilots should have prior training flight and a certain number of hours of flying duly certified.

5.2.1 Basic training

Once inside the company, pilots should take one hundred and fifty four (154) theoretical hours of basic subjects. The proposal is that at least eight (8) hours, will develop skills in use and handling of EFBs, interpretation of digital charting, information security threats and information security best practices. The practical training focuses on the proper use of the cockpit equipment; therefore, the only recommendation is to deepen in the handling of EFBs.

5.2.2 Changing aircraft and annual training

When the change of aircraft model is performed, a theoretical training of forty nine (49) hours must be done. Although, in this airline all EFBs are the same regardless the type of aircraft, at least one (1) practical hour should provide pilots with new information about security vulnerabilities and threats.

Each year a twenty eight (28) hours of theoretical review is performed by all staff members, allowing updating the personal on new technologies and procedures, review cases of incidents that affect safety, and apply new guidelines ordered by the company.

5.3 Training for air traffic controllers (ATC)

In Colombia the only authorized training centre for air traffic controllers depends on the AEROCIVIL, is called Aeronautical Sciences Studies Centre (*Centro de Estudios de Ciencias Aeronauticos* - CEA)[13]. The course lasts for seven months, which in total offers one thousand and two hundred (1200) theoretical hours. Although, the ATCs does not handle the EFBs, it is necessary to instruct them at least twenty (20) hours in digital cartography, symbolism and aeronautical communications [30].

[13] AEROCIVIL webpage consulted in 27/04/2016 http://www.aerocivil.gov.co/Educacion/CEA/Paginas/Inicio.aspx [4]

To keep the personal updated on new information security threats and vulnerabilities, one (1) hour of annual training is proposed.

5.4 Conclusions

This chapter established the best method to communicate the new requirements in the aviation industry, giving response to the following research questions:

- RQ3: How to communicate the new security requirements to the employees?
    - Rq3.1: Which is the most effective method for communicating the information?
    - Rq3.2: What level of security should be handled when transmitting information?

Table 7 summarizes the proposed instructions hours to achieve an effective communication within the organization solving the first sub-question. Permanent updates and immediate corrections to the detection of new threats should be one of the guidelines to ensure the continuity of the business process. The aviation business is even more complex, although, it is standardized that all communications must be in English, a stressful and multicultural work environment, it makes the task of achieving an optimal communication within the organization more complicated.

Table 7. Proposed instruction hours.

Entity	Primary Training	Basic Training	Change of Aircraft	Annual Training
Colombian Air Force	(1) theoretical	(3) theoretical (5) practical	(2) theoretical (1) practical	N/A
Avianca	N/A	(8) theoretical	(1) practical	(1) practical
ATC	(20) theoretical	N/A	N/A	(1) theoretical

An important limitation of the instructions is to establish a proper academic content of the subjects taught; therefore, the experience and knowledge of instructors and the technological means that classrooms have must be taken into account. Even more,

organizations are seeking every day an effective information system for their business model, especially in multidisciplinary environments.

When performing the instructions within the organization the risk of data loss is reduced, with this argument is given answer to the second sub-question. However, organizations should have strong privacy policies in order to keep confidentiality of their vital information assets.

6 Evaluation

To evaluate the results obtained, the method proposed by [14] is used. The purpose of the Security Attribute Evaluation Method (SAEM) is to provide a structured cost-benefit process to evaluate alternative security designs. This process involves four steps, which will be studied in this chapter: benefit assessment, threat index evaluation, coverage assessment and cost analysis.

6.1 Benefit assessment

The benefit assessment measures how well the technology mitigates the risk. For that purpose, three stages are developed. First, a list of the security technology categories is made. Later, the benefits that the implementation of these technologies can bring are established. Finally, the effectiveness of the countermeasures is quantified.

6.1.1 Security technology categories

At this stage the security controls are categorized according to the criteria proposed by [52]. Table 8 lists all the security controls and categorizes them into protection, detection and recovery.

Table 8. Technology categories

Protection	Detection	Recovery
· Use crypto algorithm · Exchange public keys using a secure channel. · Use public key signed by CA. · Secure proxy service.	· Verify digital signature. · Check the hash of the file. · Filter IP addresses. · Stop the process when dynamic SQL is happening.	·Stop the process when an error occurs.

6.1.2 Relevant security technology benefits

After the classification, the next step is to identify which technologies mitigate each of the threats. The benefits that bring the implementation of the controls are set against the major threats presented.

Table 9. Relevant technology benefits

Risk	Security Technologies
DoS	· Filter IP addresses
Scanning	· Use crypto algorithm · Exchange public keys using a secure channel. · Use public key signed by CA. · Secure proxy service.
Procedural Violation	· Stop the process when dynamic SQL is happening. · Stop the process when an error occurs.
Data Modification	· Verify digital signature. · Check the hash of the file.

6.1.3 Benefit estimation

In this last step, the effectiveness of countermeasures is quantified. The values according to the experience of security experts with the management of these technologies are estimated.

Table 10. Benefit estimation

Technology/Threats	DoS	Scanning	Procedural Violation	Data Modification
Filter IP addresses	50%[14]			25%
Use crypto algorithm		75%[15]		
Exchange public keys using a secure channel.		50%[16]		
Use public key signed by certification authority.		50%		

[14] OWASP webpage consulted in 1/05/2016 https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks [40]

[15] CWE webpage consulted in 1/05/2016 https://cwe.mitre.org/data/definitions/327.html [21]

[16] Security-in-a-box webpage consulted in 3/05/2016 https://securityinabox.org/en/guide/secure-communication [45]

Secure proxy service.		90%[17]		
Stop the process when dynamic SQL is happening.			80%[18]	
Stop the process when an error occurs.			75%[19]	
Verify digital signature.				75%[20]
Check the hash of the file.				100%[21]

6.2 Threat index evaluation

The second stage of the method evaluates the effects that security technology has while mitigating each risk. Previously obtained benefit assessment is applied to the threat frequencies, thus, the overall threat index is acquired. Considering previously mentioned criteria, several security controls that mitigate the same risk are exposed in table 11, in order to choose the one that gives greater benefit.

Table 11. Security controls that mitigate the same risk.

Confidentiality of digital map file	**Integrity of digital map file**
• Use crypto algorithm • Exchange public keys using a secure channel. • Use public key signed by CA.	• Verify digital signature. • Check the hash of the file.

In first scenario, the use of crypto algorithm is chosen, because, it has bigger effectiveness and is also the first step that must be taken to implement the other two

17 Stack exchange webpage consulted in 3/05/2016 http://security.stackexchange.com/questions/8145/does-https-prevent-man-in-the-middle-attacks-by-proxy-server [48]

18 ORACLE webpage consulted in 4/05/2016 https://docs.oracle.com/cd/B19306_01/appdev.102/b14261/dynamic.htm [37]

19 Erland Sommarskog webpage consulted in 4/05/2016 http://www.sommarskog.se/error-handling-II.html [47]

20 Stack exchange webpage consulted in 3/05/2016 http://security.stackexchange.com/questions/8034/how-digital-signature-verification-process-works

21 Stack exchange webpage consulted in 4/05/2016 [49] http://security.stackexchange.com/questions/33154/what-security-purpose-do-hashes-of-files-serve [50]

controls. For the second case, although both controls meet the security requirement, the integrity is guaranteed only when the hash of the file has been checked.

6.3 Security architecture coverage

The decision to select one technology over another might be based on engineering design principles rather than strictly an effectiveness evaluation [52]. However, in this step the principle of selection is based on technology category. Table 12 lists the remaining security controls and compares between the risk that mitigates and technology category.

Table 12. Security architecture coverage.

Risk	Security Technologies	Technology category
DoS	Filter IP addresses	Detection
Scanning	Use crypto algorithm	Protection
	Secure proxy service.	Protection
Procedural Violation	Stop the process when dynamic SQL is happening.	Detection
	Stop the process when an error occurs.	Recovery
Fake Authentication	Check the hash of the file.	Detection

There are only two security controls that are matching categories and mitigate the same risk. For the same reasons as in the previous step the use of crypto algorithm is chosen over the secure proxy service.

6.4 Cost

To determine the cost of security technology purchase, training, maintenance and installation costs are taken into account. However, the technology costs are highly dependent on system architectures, for this reason the manager makes decisions based on the best option for a specific design.

In the study case there are two technologies that appear to provide similar benefits and mitigate the risk of procedural violation. The implementations of both controls are based on source code programming; however, sending an alert when dynamic SQL happens is cheaper than program an error handling code.

6.5 Conclusions

The method applied is a cost-benefit analysis technique that allows evaluating the selection of security controls. Proposed security requirements were analyzed in four steps. As a result the security controls that should be implemented were obtained.

The success of the method depends on the prioritized list of the risks and the estimation of effectiveness of the security technologies. The conclusions are very similar to the results achieved in Chapters 3 and 4, allowing positive assessment of the research done before.

7 Conclusions

This chapter summarizes the assumptions made throughout the thesis. First, general conclusions are exposed. Then, the research questions are answered. Later, the constraints encountered in the development of thesis are named. Finally, the future work to be done is proposed.

7.1 General conclusions

In this thesis a security risk assessment to the use of digital charting was made, using as an example the Colombian aviation case. As a result of this work recommendations are given to improve the information security in the use of digital charting. Conclusions obtained in this thesis are following:

With the use of the Business Process Modeling Notation (BPMN) [36] an easy identification of the business assets and the risk is achieved. The modelling allows security analysts to have a general concept of the business model and comprehend the value of business assets of the company.

The framework for this research was the Information System Security Risk Management (ISSRM) [22]. By applying six security patterns to the business model, the business process and security analysts have an effective tool for identifying vulnerabilities and establishing security requirements. The model was well suited for secure business model related to aviation.

The method to secure business processes offered by [5], allows proposing security controls to achieve the security requirements. The criterion for choosing security controls have depended on cost-benefit ratio, taking into account current infrastructure and staff training.

By nature of the business aviation, the most effective way to communicate new policies within the organization, it is through the constant training that their members received.

Therefore, the proposed instructions within those workouts, become a direct communication tool between managers and all member of the company.

The companies that provide the service of digital charting should take into account the experiences of users with the handling of the information requested. This feedback is vital to design friendlier user interfaces, but at the same time increase security of information.

7.2 Answer to research questions

- RQ1: How to develop a security risk assessment for the use of the digital charting in the Colombian aviation?

Answer: To perform the security risk assessment the method of Information System Security Risk Management (ISSRM) [22] was used, this method allows the business process analysts to have a framework about the business model. Graphical representation of the business process was made using Business Process Modeling Notation (BPMN) [36], facilitating identification of assets and the risk that it faces.

In the research six security patterns were applied, protecting the confidentiality, integrity and availability of business model. Finally, by applying all steps of the method, the security controls with the best cost-benefit ratio were obtained.

- RQ2: How to apply the security risk-oriented patterns in the business process?

Answer: The Security Attribute Evaluation Method (SAEM) [14] was used to apply the security patterns in the business process. In this method, these four steps were following: benefit assessment, threat index evaluation, coverage assessment and cost analysis. To obtain the security controls, criteria from several security analysts were followed.

- RQ3: How to communicate the new security requirements to their employees?

Answer: Taking advantage of the constant training that aviation personal performs, theoretical and practical instructions are proposed. The lessons will update the staff on new information security threats and security controls to mitigate those. Continuous

training in this subject is the most effective tool to prevent damage to the business model.

7.3 Limitations

The limitations encountered during the development of the thesis were as follows:

- Academic studies on this specific subject were not found, security incidents that have occurred are very recent and technical information regarding that is not available.
- While evaluating the benefits of the security controls proposed, certain level of subjectivity is presented. In order to mitigate this subjectivity, criteria from different security analyst were taken into account.
- Initially it was planned to make a qualitative analysis to evaluate the results obtained. However, the method was changed because most of the pilots in Colombia were not aware of security information when using electronic flight bags.
- There is a lack of theoretical support while choosing the controls that meet the security requirements.

7.4 Further Research

This research is an initial step to continue studying this topic in Colombian aviation. Although there have not been major security incidents, entities should consider security requirements with the implementation of new applications and use of the devices in the cockpit. The topics for the further investigation are following:

- Raise the security awareness of members of the organization must be the primary objective of the instructions given. This communication method is very effective and should be exploited to create a strong security culture.
- Create a method that will not be paper-based to validate this study, evaluations in the field allow avoiding subjectivity of security analyst.

- Strengthen relations between the private sector and governments, using secure communication channels and sharing experiences through computer emergency readiness team (CERT) in each country.

References

[1] AEROCIVIL, Unidad Administrativa Especial de Aeronáutica Civil (2015, May). Cartas Aeronáuticas para la Navegación Aérea RAC 90. In Diario Oficial 49527. AEROCIVIL

[2] AEROCIVIL [Online] Available at: http://www.aerocivil.gov.co/AAeronautica/Estadisticas/Paginas/Inicio2.aspx

[3] AEROCIVIL [Online] Available at: http://www.aerocivil.gov.co/Aerodromos/Aeropuertos/Paginas/Inicio.aspx

[4] AEROCIVIL [Online] Available at: http://www.aerocivil.gov.co/Educacion/CEA/Paginas/Inicio.aspx

[5] Ahmed, N., & Matulevičius, R. (2014). Securing business processes using security risk-oriented patterns. Computer Standards & Interfaces, 36(4), 723-733.

[6] AIRCRAFT, C. O. B. International Civil Aviation Organization.

[7] Altuhhova, O., Matulevičius, R., & Ahmed, N. (2012, June). Towards definition of secure business processes. In Advanced Information Systems Engineering Workshops (pp. 1-15). Springer Berlin Heidelberg.

[8] Avianca [Online] Available at: http://www.avianca.com/en-eu/our-company/corporate-information/corporate-profile.aspx

[9] Avionics magazine. [Online] Available at: http://www.aviationtoday.com/av/commercial/American-Airlines-Jeppesen-Comment-on-EFB-Crash-that-Grounded-Flights_84925.html#.VvqciOagUZM

[10] Avoine, G., & Oechslin, P. (2005, March). A scalable and provably secure hash-based RFID protocol. In Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on (pp. 110-114). IEEE.

[11] Barstow, D. (2012). The aviation iPad revolution. Journal of Air Traffic Control, 54(2), 4.

[12] Bellardo, J., & Savage, S. (2003, August). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In USENIX security (pp. 15-28).

[13] Boyd, S. W., & Keromytis, A. D. (2004, June). SQLrand: Preventing SQL injection attacks. In Applied Cryptography and Network Security (pp. 292-302). Springer Berlin Heidelberg.

[14] Butler, S. A. (2002, May). Security attribute evaluation method: a cost-benefit approach. In Proceedings of the 24th international conference on Software engineering (pp. 232-240). ACM.

[15] CAPEC [Online] Available at: http://capec.mitre.org/data/definitions/94.html

[16] CAPEC [Online] Available at: http://capec.mitre.org/data/definitions/510.html

[17] Carreño Moreno, P. (2014). Hacia una fase digital.

[18] Chandra, D. C., & Kendra, A. J. (2010). Review of Safety Reports Involving Electronic Flight Bags. Air Traffic Organization Operations Planning, Human Factors Research and Engineering Group.

[19] Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: a tutorial. Communications Magazine, IEEE, 40(10), 42-51.

[20] CWE. [Online] Available at: http://cwe.mitre.org/data/definitions/300.html

[21] CWE. [Online] Available at: https://cwe.mitre.org/data/definitions/327.html

[22] 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). Springer Berlin Heidelberg.

[23] DW magazine. [Online] Available at: http://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698

[24] EASYFLY [Online] Available at: http://www.easyfly.com.co/px

[25] FAA, Federal Aviation Administration (2011). The Apple iPad and Other Suitable Tablet Computing Devices as Electronic Flight Bags (EFB). AFS-200 Guidelines for the Certification, Airworthiness, and Operational Use of Portable Electronic Flight Bags

[26] FAC, Fuerza Aérea Colombiana. (2007). Manual de Calidad Fuerza Aérea Colombiana. Bogotá: Departamento de Planeación Estratégica FAC.

[27] Hafiz, M., Adamczyk, P., & Johnson, R. E. (2007). Organizing security patterns. IEEE software, 24(4), 52.

[28] Hevner Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 28(1), 75-105.

[29] ICAO. [Online] Available at: http://www.icao.int/about-icao/Pages/default.aspxl

[30] Jarrin, J. A. (2015). Cartografía Aeronáutica.

[31] Khan, N. H. (2012). A Pattern-Based development of secure business processes.

[32] Loukas, G., & Öke, G. (2009). Protection against denial of service attacks: A survey. The Computer Journal, bxp078.

[33] Merickova, J., & Vilšer, J. Spatial Knowledge and Information CANADA: New Technologies in Air Navigation of the Czech Air Force.

[34] Nomura, S., Hutchins, E., & Holder, B. E. (2006, November). The uses of paper in commercial airline flight operations. In Proceedings of the 2006 20th

anniversary conference on Computer supported cooperative work (pp. 249-258). ACM.

[35] Nõukas, R. (2015). Service brokering environment for an airline.

[36] OMG, Business Process Model and Notation Version 2.0, 2011. [Online] Available at: http://www.bpmn.org/

[37] ORACLE. [Online] Available at: https://docs.oracle.com/cd/B19306_01/appdev.102/b14261/dynamic.htm/

[38] OWASP. [Online] Available at: https://www.owasp.org/index.php/Exception_handling_techniques

[39] OWASP. [Online] Available at: https://www.owasp.org/index.php/SQL_Injection

[40] OWASP. [Online] Available at: https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

[41] Peña Ortíz, Y. H. (2015). De la subordinación a la autonomía: la profesionalización militar en la construcción de la aviación militar colombiana, 1920-1936.

[42] Recker, J. C. (2008). BPMN modeling–who, where, how and why. BPTrends, 5(3), 1-8.

[43] Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2007). A BPMN extension for the modeling of security requirements in business processes. IEICE transactions on information and systems, 90(4), 745-752.

[44] Romero-Gutiérrez, W. R. (2015). Plan de negocio del proyecto de sistematización de procesos para la escuela de entrenamiento de la aerolínea avianca.

[45] Security-in-a-box [Online] Available at: https://securityinabox.org/en/guide/secure-communication

[46] Skaves, P. (2011, October). Electronic flight bag (EFB) policy and guidance. In Digital Avionics Systems Conference (DASC), 2011 IEEE/AIAA 30th (pp. 8D1-1). IEEE.

[47] Sommarskog, Erland. [Online] Available at: http://www.sommarskog.se/error-handling-II.html

[48] Stack exchange [Online] Available at: http://security.stackexchange.com/questions/8145/does-https-prevent-man-in-the-middle-attacks-by-proxy-server

[49] Stack exchange [Online] Available at: http://security.stackexchange.com/questions/8034/how-digital-signature-verification-process-works

[50] Stack exchange [Online] Available at: Stack exchange webpage consulted in 4/05/2016 http://security.stackexchange.com/questions/33154/what-security-purpose-do-hashes-of-files-serve

[51] Stamp, J., Dillinger, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories.

[52] Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

[53] Shaw, K. B., Kuder, S., Carter, S. V., Coughlan, S. D., & Richard, J. P. (1995). A Comprehensive Analysis of Navy and Marine Corps Digital Mapping, Charting, and Geodesy Requirements for Modeling and Simulation (No. NRL/FR/7441--93-9435). Naval research lab Stennis space center ms.

[54] tsipenyuk, K., Chess, B., & McGraw, G. (2005). Seven pernicious kingdoms: A taxonomy of software security errors. Security & Privacy, IEEE, 3(6), 81-84.

[55] Velmurugan, M. S. (2009). Security and trust in e-business: problems and prospects. International journal of electronic business management, 7(3), 151-158.

[56] White, S. A. (2004). Introduction to BPMN. IBM Cooperation, 2(0), 0.

[57] Yeh, M., Riley, V., & Mangold, S. J. (2003). Human Factors Considerations in the Design and Evaluation of Electronic Flight Bags (EFBs): Version 2 (No. DOT-VNTSC-FAA-03-07,). Office of Aviation Research.

[58] Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. Progress in informatics, 5(5), 35-47.