TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Jürgen Niinre 190844TAF 191674IABM

DATA CENTRIC SMARTPHONE MESSAGING APPLICATION'S SECURITY EVALUATION

Master thesis

Supervisors: Tarmo Veskioja
PhD
Olaf Maennel
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Jürgen Niinre 190844TAF 191674IABM

ANDMETE KESKNE NUTITELEFONI SÕNUMIVAHETUSRAKENDUSE TURVAHINNANG

magistritöö

Juhendaja: Tarmo Veskioja
Doktorikraad

Olaf Maennel

Doktorikraad

Tallinn 2019

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: Jürgen Niinre

04.05.2019

Abstract

The goal of this thesis is to find out of what the smartphone messaging application security consists and how it would be possible to rank smartphone messaging application security vs. similar applications.

This thesis builds a risk evaluation model for smartphone messaging applications, using ISO/IEC 27005:2014 standard methodology. With the use of expert opinions and AHP modelling, the author of this thesis found out the biggest threats and important vulnerabilities for a smartphone.

Finally, author proposed a security ranking method for smartphone messaging application by taking into account different security tests in scientific literature.

It was found out that according to expert opinions, the messaging application only influences 2,9% of the total smartphone information security risk. Using expert opinions and performed security tests in literature, the best ranking messaging application in terms of security was WhatsApp, with Viber close in the second place.

This thesis is written in English and is 55 pages long, including 5 chapters, 18 figures and 10 tables.

Annotatsioon

Andmete keskne nutitelefoni sõnumivahetusrakenduse turvahinnang

Käesolev magistritöö pakub välja riski hindamise mudeli nutitelefoni sõnumivahetusrakendusele, kasutades ISO/IEC 27005:2014 metoodikat. Erinevad nutitelefoni turvariskid ja -nõrkused on leitud akadeemilisest kirjandusest ning turvaraportitest. Akadeemilisest kirjandusest pärinevad ka sõnumivahetusrakenduste turvatestid, mis annavad võimaluse sõnumivahetusrakenduste võrdlemiseks kasutades juba tehtud teste.

Selleks, et oleks võimalik erinevaid riske hinnata üksteise suhtes ning järjestada nutitelefonidele tehtud turvatestide olulisust, viis autor läbi küsitluse 6 erinevast ettevõttest või riigiasutusest pärineva turvaeksperdi vahel. Saadud andmetega sai hinnata nutitelefonidele mõjuvaid riske ning järjestada sõnumivahetusrakendusi turvalisuse vaates.

Küsitluse tulemusena selgus, et nutitelefoni sõnumivahetusrakendus mõjutab vaid 2,9% kõikidest nutitelefoni turvariskidest (pahavara, pahatahtlik sisu, võrgurünne, füüsiline kaotus, sotsiaalsed tehnikad). Lisaks selgus, et arvestades ekspertarvamusi ning akadeemilises kirjanduses tehtud turvateste, võib järeldada, et parima turvaskooriga olid peaaegu võrdselt sõnumivahetusrakendused WhatsApp ning Viber.

Tulemustele rakendati ka statistilist ning- tundlikkuse analüüsi ja peale ühe erisuse ei leitud statistiliselt olulisi muudatusi (98% tõenäosusega) lähteandmetes, mis mõjutaks lõpptulemust. Erisuseks oli statistiline võimalus nutitelefoni sõnumivahetuse rakenduse turvatesti tähtsuse muudatuseks mõne eksperdi poolt, samas töö autori hinnangul taolise turvatesti hinnangu muutmine sellisel määral ei olnud võimalik.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 55 leheküljel, 5 peatükki, 18 joonist, 5 tabelit.

List of abbreviations and terms

AHP	Analytic Hierarchy Process
Alternatives	Alternatives are for what the results are found in AHP analysis
App	(Smartphone) Application
Asset	Asset is anything that gives value to the organization and therefore requires protection
Attack	When Threat and Vulnerability exist, attack is possible.
Availability	Property of being accessible and usable upon demand by an authorized entity
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities or processes
Consistency ratio	Shows the quality of user input
CPU	Central Processing Unit
Criteria	Units that are compared to each other in AHP analysis
Data	Data – any data, that either stored locally in smartphone (contacts, message, voice logs, configuration, camera output), input by user (via keyboard), input from sensor or exchanged over communication network (messages, status information, voice data). For this thesis there is no distinction between different information types (Personal, Business, etc) or different Sources.
IEC	International Electrotechnical Commission
Integrity	Property of accuracy and completeness
IP	Internet protocol
ISO	International Standardisation Organisation
Layer	Grouping of criteria
MCDA	Multiple criteria decision analysis
MCDM	Multiple criteria decision making
Messaging application	By IP messaging (or in this thesis, just messaging) is usually meant Applications that use only the TCP/IP communication capabilities of smartphone for sending messages or making calls
OS	Operating system

Risk	Threat likelihood x Asset impact
Saaty scale	Scale of pairwise comparison values, from 1-9
Sensitivity analysis	Sensitivity analyses show how well the alternatives performed with respect to each of the objectives as well as how sensitive the alternatives are to changes in the importance of the objectives
Smartphone	A mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps
Threat	Threat or threat event has the potential to harm assets, such as information and therefore it can negatively impact organization
Vulnerability	Vulnerability does not cause harm in itself, as there needs to be a threat present that can exploit it

Table of contents

List of figures

List of tables

1 Introduction

There are several smartphone messaging applications available, each of which claiming to be more secure than the other. How to verify the security and really know which application is the most secure one?

This thesis contributes to the issue with the following topics:

- finding out a data centric security model for the smartphone messaging application and
- calculating data centric security ranking for the smartphone messaging application.

1.1 Context and background

The usage of smartphones in everyday communication is becoming widespread. In 2018 67% of the total world population used a mobile service and 60% of these users preferred to use a smartphone [1, p. 8].

Due to the widespread usage and constant connectivity, one of the issues related to the smartphone usage is keeping both private and company information secure.

It is quite difficult for a decision maker in an organization to decide which external (messaging) application employees should or could use for communication with each other.

Usually every company has their own e-mail server, however, it is very rare for a company to have their own messaging server infrastructure.

In practice employees use whatever messaging application they like or what their friends like [2, p. 156] but that might not be the best choice when looking into the protecting private- and company data.

1.2 Problem statement and objectives

General objective of this thesis is to find and evaluate a method for the smartphone messaging application information security assessment in an organization.

More fine-grained sub-goals are:

1. To establish a security model of a smartphone and - messaging application, to answer the question, “What the security is made of?”.
2. To measure the amount of security, either by expert opinions, statistics or other conducted research available, which is influenced by a messaging application.
3. To calculate the security ranking for a select smartphone messaging application, by using a well-established methodology.
4. To analyse the results, to see if the ranking scores are statistically meaningful.

1.3 Methodology

In this thesis the author uses ISO 27005:2014 [3] standard to build a smartphone security model. It is done by finding out smartphone assets, threats, vulnerabilities and risks.

To prioritize and get a final uniform risk score author performs AHP (Analytic Hierarchy Process) analysis on the list of risks with the help of expert opinions, according to [4] and [5].

AHP model is analysed, using standard AHP sensitivity analysis, according to [6], [7] and [8].

Web-HIPRE web tool [9] is used to visualize and present the AHP model. Weight calculations are done in Excel.

1.4 Work structure

In the first chapter the overview of the work is presented by describing the work background, objectives and methodology used.

In the second chapter the context is established for building a security model for smartphone messaging applications. ISO 27005:2014 standard [3] methodology is described and smartphone information security is defined. Afterwards overview of the messaging application is given.

In the third chapter, actual smartphone messaging application security model is being built, using available research and security reports.

In the fourth chapter main characteristics are explained on AHP methodology and sensitivity analysis.

In the fifth chapter a case study is performed by using the security model derived and AHP methodology with expert opinions, to find out ranking of a list of smartphone messaging applications and analyse the results.

In the sixth chapter the conclusions of the work are presented.

2 Security model context

To find out the security model for smartphone messaging applications, author of the thesis decided to rely on ISO 27000:2014 [10] methodology. Using this standard it is possible to methodologically approach the security and define the parts that both negate and contribute to it.

The basic building block for a security model is risk. In following subchapters author of the thesis finds out what risks are and how we could use risks to build a security model for smartphone messaging applications.

2.1 Information security in an organization

We can define information security based on ISO 27000:2014 [10]. This family of standards is created to keep organization's information assets secure. Information security is defined as the preservation of confidentiality, integrity and the availability of information [10, pp. 3-7]:

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes,
- Integrity is the property of accuracy and completeness,
- Availability is the property of being accessible and usable upon demand by an authorized entity.

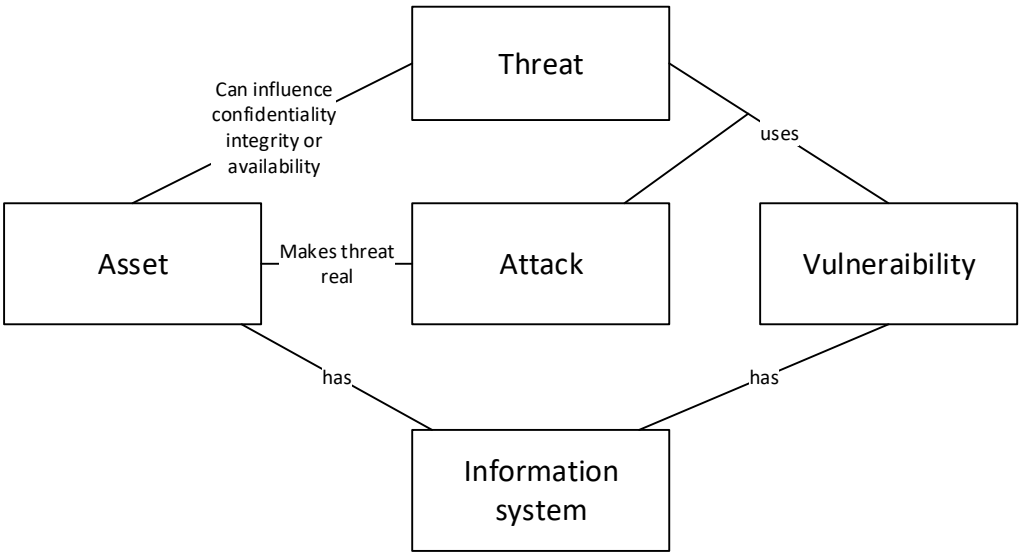

Figure 1. Information security base term relations

An asset is anything that gives value to the organization and therefore requires protection [3, p. 14]. This can be hardware, software, connections, data, processes, etc.

Threat or threat event has the potential to harm assets, such as information and therefore it can negatively impact organization [3, p. 14]. Because of the impact on the information system's availability, integrity and confidentiality, all possible threats should be identified. Threats can be further specified to be adversarial (humans) or non-adversarial (acts of nature and non-voluntary acts by humans) [11].

Because threats are not related to any particular information system and can be applied to any organization's information assets, there are already available sources where many threats are catalogued for easier assessment, in [3] and [12].

Vulnerability does not cause harm in itself, as there needs to be a threat present that can exploit it [3, p. 14]. When vulnerability is combined with a suitable threat, then a practical attack is possible by a threat source.

2.2 Smartphone information security

Most commonly smartphone is defined as „A mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps.“ [13]

Accordingly, smartphone can be viewed as a small information system that has the same qualities as a computer information system – it has its processor, data, communication facilities, etc. Therefore, it can be assumed that the same security assessment framework can be applied as for the information systems with computers. This has also been demonstrated by [14], [15] and [16].

There are also some differences between common computer system and smartphone in relation to security [16, pp. 19-20]:

- Mobility – mobile devices are mobile, they are not kept in secure premises and therefore might get stolen and physically tampered with.
- Strong personalization – mobile devices are not usually shared between users, while computers often are.
- Strong connectivity – many devices support multiple ways to connect to a network or the Internet.
- Technology convergence – current mobile devices combine many different technologies in a single device, like PDA, mobile phone, music player, camera.
- Reduced Capabilities - mobile devices are computers but lack many features that desktop computers have. For example, a mobile device does not have a full keyboard and has limited processing capabilities.

It is also harder to control mobile devices by organizations, because users are using their own private mobile devices to access corporate services, view corporate data and conduct business [17, pp. 1-2]. Due to that we have additional, private assets that are mixed with corporate assets in a single smartphone, thus increasing the number of threats that can be applied.

2.3 Messaging applications

The first widespread mobile messaging solution was SMS (Short Message System), introduced by GSM (Global System for Global Communications) standard in 1989 and the first SMS message was sent three years later [18]. Users could send texts, ringtones

and low level graphics. The initial value of the SMS service to users was that you could always get the message later even when you were temporarily out of coverage.

MMS (Multimedia Message System) was introduced in 2001 and is offering several advantages over SMS. While SMS could only contain text, MMS allows to use images, videos and audio [19].

According to the GSMA survey [1, p. 17] at least 80% of smartphone users engage monthly to use SMS/MMS. However, there is a new messaging solution that users engage in equal amount: IP messaging [1, p. 17].

By IP messaging (or in this thesis, just messaging) is usually meant Applications that use only the TCP/IP communication capabilities of smartphone for sending messages or making calls, while SMS/MMS also used some of the mobile network core features. Because of the nature of communications that IP messaging uses, these are sometimes also called Over the Top (OTT) - or Mobile Instant Messaging (MIM) applications [20, p. 352], because they rely on the TCP/IP service provided by mobile networks and they are considered more suitable for (instant)conversations in real time.

While cost significantly impacts people's frequency of usage, the social influence is one of the main reasons for today's migration to such MIM applications. The nature and intent of WhatsApp messages tend to be more social, informal and conversational in nature, while SMS is seen as more privacy preserving, more formal and generally more reliable. [20, p. 361]

2.4 Evaluating messaging application security

Knowing the procedures laid out in ISO 27005:2014 [3], handling the smartphone as an information system on its own and messaging application as a software installed in the smartphone, we can define a theoretical security model for further analysis below.

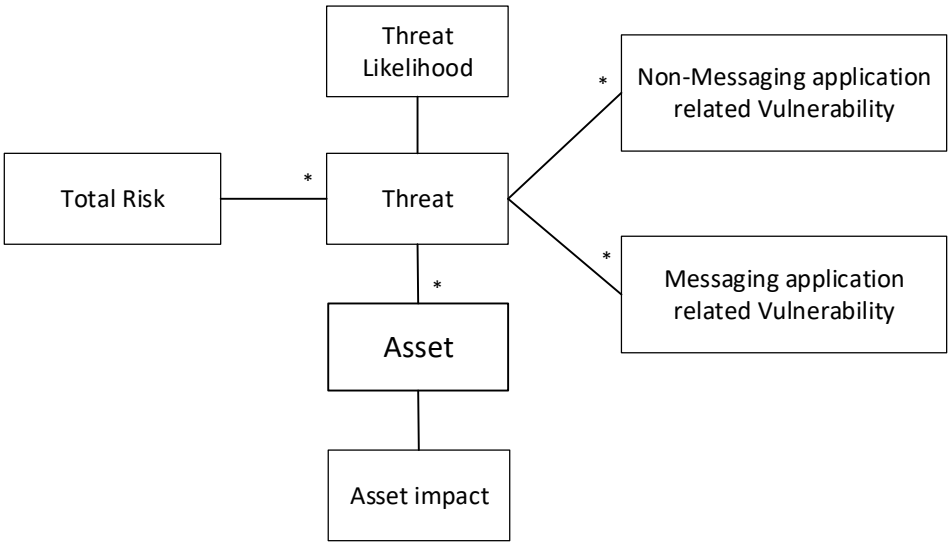

Figure 2. ISO/IEC 27000 model to evaluate messaging application related risks

$$TotalRisk = \sum ThreatLikelihood \times AssetImpact \quad (1)$$

Using the equation (1) we can calculate the total risk for the smartphone application containing a messaging application. For every threat we have a threat likelihood (measured in probability) and asset impact (measured as cost to replace) of related assets.

As there is now a way to measure risks, how can we rank the messaging application security? In this thesis the author has chosen to calculate a score for every messaging application vulnerability that has been countered either by implementing a security control or there is a proof about certain vulnerability not existing. The simplified view of such a model is shown in the figure below.

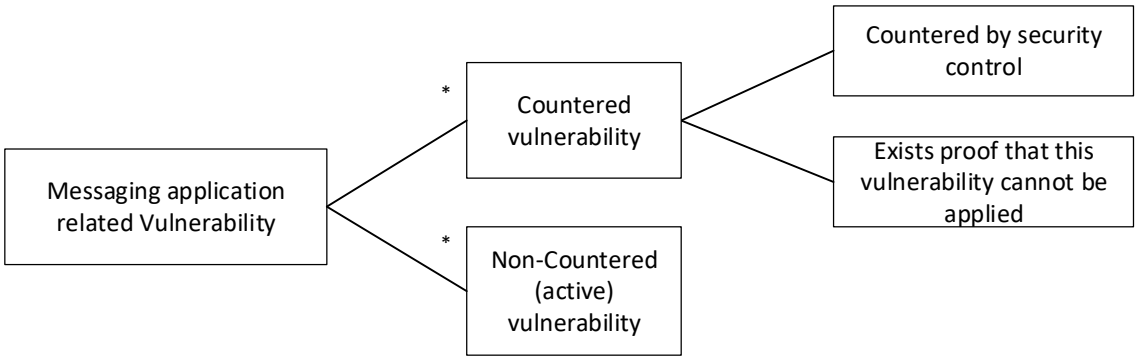

Figure 3. Classifying messaging application vulnerabilities

We can get a security score for every messaging application by counting up the countered vulnerabilities.

3 Messaging application security model

To find a security model for smartphone messaging applications, author of this thesis proposes to perform the following tasks with procedures established in [3] and subchapter 2.4:

A risk identification to be performed in the current chapter:

- To identify smartphone assets
- To identify smartphone threats
- To identify smartphone vulnerabilities
- To identify smartphone asset impact
- To identify messaging application specific vulnerabilities
- To identify messaging application specific security controls
- To establish a risk model, involving both smartphone and smartphone messaging application risks.

3.1 Smartphone assets

Below is a broad categorization of different assets for smartphone suggested by [14], [15], [21] and [22]:

- Data (Private Information, Personal Data, Corporate intellectual property, Financial assets, the Data that can endanger personal and political reputation, Network access data, Offline data, Data synchronization with PC, Documents, the Multimedia data stored on device, Configurations and other, Password storage, Confidential content, E-mail, Pictures, Contacts, Online storage)
- Hardware/Resources (Battery Power, Memory, CPU)

- Connectivity (Service availability and functionality, Voice communication, Messaging, Bluetooth/IR, Web access)

- Applications (Phone, SMS, E-mail, Banking, Social Media, Messaging, Business applications, etc)

According to [3, p. 14] and asset suggestions mentioned above, we can derive an asset definition for smartphone messaging applications: “Asset is anything that smartphone or messaging application has that gives value (and therefor can cause loss of value) to the organization”.

By using the definition, we can define the following assets to be further considered in the current thesis:

- Data – any data, that either stored locally (contacts, message, voice logs, configuration, camera output), input by a user (via keyboard), input from sensor or exchanged over communication network (messages, status information, voice data). For this thesis there is no distinction between different information types (Personal, Business, etc) or different Sources.

- Device hardware and software resources – including CPU (Central Processing Unit), screen, memory, battery, external memory, OS (Operating System). Sometimes an organization has a direct interest in a device as it has been purchased or subsidized for the user. Device hardware and software resources have to be protected also because if not working properly, a user cannot communicate at all.

- Device connectivity – it has been provided as a separate asset, because it is equally important (compared to device hardware and software resources) to the messaging application to work correctly.

- Messaging application – the binary code and initial configuration data that has been provided as a package to be downloaded from an application store. Once the application has been installed, the application data becomes part of the data asset. Messaging application code is important to be protected as not to contain backdoors or bugs that can lead to loss of data.

The assets mentioned above are depicted also in the figure below.

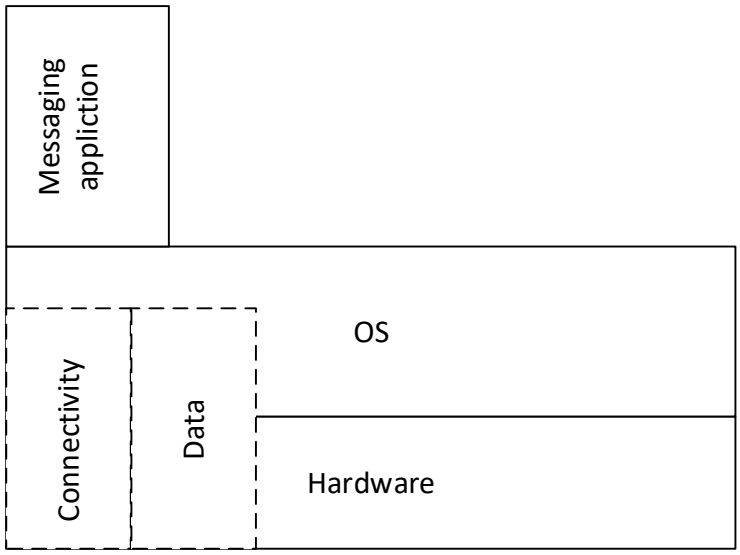

Figure 4. Asset model of smartphone messaging application

3.2 Smartphone vulnerabilities

Vulnerability can be exploited to cause harm to assets. [3] lists following common vulnerabilities:

- Hardware vulnerabilities (10 example vulnerabilities)
- Software (23 example vulnerabilities)
- Network (10 example vulnerabilities)
- Personnel (8 example vulnerabilities)
- Site (4 example vulnerabilities)
- Organization (30 example vulnerabilities)

There is a public database available that lists the vulnerabilities for common software products including smartphone OS-s [23]. When checking the most used smartphone OS platforms (Android and iOS), we can see the total of 3799 vulnerabilities listed from 2009 in the following categories [23]:

- Denial of Service (1167)
- Bypass Something (292)

- Execute Code (1223)
- Memory Corruption (870)
- Gain Information (567)
- Gain Privilege (354)
- Overflow (1235)
- Sql Injection (5)
- Directory Traversal (8)
- XSS (40)
- CSRF (1)

Another major security vulnerability is the (un)awareness of users. A survey was made [24, pp. 101-104], which analysed 510 respondents, examining the security awareness of smartphone users. The applicable categories by which users were evaluated were: user authentication, anti-virus applications, updates, permissions and data encryption.

- 84.5% of respondents reported using one or more authentication controls.
- Knowledge of malware and security software (e.g. anti-virus, anti-malware) was reported by 77.6 and 70.4% respectively.
- The majority of respondents auto-update applications (42.2 percent) or update at least once a month (34.7%).
- 96.9% of respondents download applications from an official repository.
- 58.8% read the permission requests on initial installation of an application. However, only 34.5% of respondents read permission requests when updating applications
- 25.5% of users are unaware of the data encryption.

By using [14], [21], [25] and [26], example vulnerabilities list in [3], user awareness studies above and software vulnerabilities described by CVE website [23], we can define the vulnerabilities for smartphone messaging application in the table below.

Table 1. Smartphone vulnerabilities analysed further in this thesis

Vulnerability type	**Description**
Hardware	Susceptibility to environment, can be stolen
Software	Implementation error (OS, Messaging application) - e.g. denial of service, bypass, arbitrary code execution, memory corruption, gain information, gain privilege, overflow, sql injection, Directory Traversal, XSS, CRSF
User unawareness	Lack of security controls Use of untrusted mobile devices (jailbreaking) Use of untrusted networks (Unsecured wifi) Use of untrusted applications (Use of applications from 3rd parties) Use of untrusted content Unaware use of location services Dismissing updates Not paying attention to requested permissions

3.3 Smartphone threats

The existence of threat shows that an attack is possible, given that there is a vulnerability and there is no security control applied to counter that threat.

The following example threat types are listed by [3]:

- Physical damage (6 example threats)
- Natural events (5 example threats)
- Loss of essential services (3 example treats)
- Disturbance due to radiation (3 example threats)

- Compromise of information (11 example threats)
- Technical failures (5 example threats)
- Unauthorized actions (5 example threats)
- Compromise of functions (5 example threats)

In this thesis, the author has chosen the following generic threats to smartphones that are compiled from [14], [15], [17], [22], [27] and [28]:

- Malicious application
- Malicious content
- Social engineering
- Network attack
- Physical loss/theft

3.3.1 Malicious application

Under the malicious application the author has included all threats that are related to a misbehaving application: Malware, Ransomware, Spyware, Disabling application, Abusing application, etc):

- Malware is the most frequently encountered cyberthreat and malware is considered as no 1 threat in 2018 cyber attacks [28, p. 26].
- The ransomware attacker gains ownership of files and/or various devices and blocks the real owner from accessing them. To return the ownership the attacker demands a ransom in cryptocurrency [28, p. 100]
- If the smartphone has spyware installed, allowing an attacker to access or infer personal data by spying on an individual. [21, p. 4]
- Disabling applications or the device by application, remotely exploiting a vulnerability or maliciously using the permissions granted by the owner at installation. [22, p. 43]

- Diallerware: an attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers. [21, p. 4]

- The Unauthorized collection of user (location) data [25, p. 6]

3.3.2 Malicious content

Malicious content web attacks have been described by [28, p. 33] as when the attacking website sends malformed network content to the victim's browser, causing the browser to run malicious logic of the attacker's choosing. Once the browser has been exploited, the malicious logic attempts to install malware on the system or steal confidential data that flows through the Web browser.

Malicious content attack can be realized also, by using unverified QR codes or NFC tags [25, p. 6]

3.3.3 Social engineering

Social engineering attacks in general are tricking the user into disclosing sensitive information. Social engineering attacks can also be used to entice a user to install malware on a mobile device. [17, p. 3]

Phishing is special form of social engineering, which uses the mechanism of crafting messages that use social engineering techniques so that the recipient will be lured and "take the bait". More specifically, phishers try to lure the recipients of phishing emails and messages to open a malicious attachment, click on an unsafe URL, hand over their credentials via legitimate looking phishing pages, wire money, etc. [28, p. 40]

3.3.4 Network attack

By network attack, an outside attacker is gaining access to a smartphone via an attack to phone software (OS/App) or server software using a network infrastructure (for example man in the middle attack).

The following particular threats have been identified by literature:

- By spoofing attacks is meant that an attacker deploys a rogue network access point and users connect to it. The attacker subsequently intercepts the user communication to carry out further attacks such as phishing. [21, p. 4]

- An attacker can risk availability of a smartphone to take denial of service attack to base station, wireless network, web server. An attacker can risk availability of a smartphone using radio interference. [14, p. 315]

- Network congestion: network resource overload due to a smartphone usage leading to the network unavailability for the end-user. [21, p. 4]

- Malicious activity against a network or network device (for example, sending spam, infecting other devices, sniffing or scanning). [21, p. 4]

- Blocking, modifying, or eavesdropping on the device's communication network when connected to an unreliable network. [22, p. 41]

3.3.5 Physical loss and theft

This threat category deals with a possibility of malicious third part getting access to the smartphone device.

Following sub-threats have been identified by [21, p. 3]:

- Data leakage: a stolen or lost phone with unprotected memory allows an attacker to access the data on it.

- Improper decommissioning: the phone is disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it.

3.4 Smartphone asset impact analysis

In order to evaluate asset impact, we can come to the following conclusions listed in the table below.

Table 2. The smartphone asset impact analysis

Asset	**Impact**
Data	Data loss can be extremely high value to an organization, because it can result in a loss of reputation that in some cases can be unrecoverable. Impact can be extreme.

Device	Replacing a device has a cost attached that can range up to 1599€ for the most expensive devices. [29]
Connectivity	Connectivity is also quite easily replaceable, if for example wi-fi is not available a mobile network can be used, so the impact is 0.
Messaging application	Value exists for an organization to facilitate communication between employees, but it is easily replaceable, so the impact is 0

In this thesis we only take into account data as an asset, mainly because it can have high value to an organization [21, p. 50] and other asset impacts when compared to business critical data loss are not as high (for example smartphone hardware).

To simplify the final model, in this thesis an assumption is made that any threat could get an access and leak all the data in a smartphone.

3.5 Vulnerabilities and security controls on smartphone messaging applications

Regarding vulnerabilities and security controls found in messaging applications:

- [26] performed vulnerability tests on 17 different messaging applications.
- [30] compared the implementations of instant messaging protocols (Off the Record, Signal and Matrix) and performed tests on 6 messaging applications. Authors found out 20 distinct security controls in these tests that could hinder the network based threats.

By combining the vulnerabilities and security controls found in the papers mentioned above, we can list the tests available in the following table.

Table 3. Security tests applied on smartphone messaging applications

Test	**Type**	**Year tested**
Registration tests		
Account hijack	vulnerability	2014

Access to SMS Inbox (for reading registration code)	vulnerability	2018
Registration with phone number	security control	2018
Registration with email	security control	2018
Registration verification with SMS	security control	2018
Registration verification with call	security control	2018
Registration verification with e-mail	security control	2018
Key handling and verification tests		
Trust other user with its (encryption) keys automatically without verification	vulnerability	2018
No notification about user (encryption) key changes on other side	vulnerability	2018
No blocking of messages when (encryption) keys of other user have changed	vulnerability	2018
Notification About E2E Encryption	security control	2018
User (encryption) key verification: via QR-code	security control	2018
User (encryption) key verification: via Phone call	security control	2018
User (encryption) key Verification: out of band (e.g PGP)	security control	2018
UI Display Verified check on User (encryption) key verification	security control	2018
Server side tests		
Contact list leak via server	vulnerability	2014

A more through description of each vulnerability/security control is given in the Appendix 1.

3.6 Building risk model

By taking into account the results from previous subchapters:

- smartphone threats
- smartphone vulnerabilities

- smartphone asset impact
- messaging application specific vulnerabilities and security controls

It is possible to formulate a final risk model for smartphones, containing a messaging application using the figure below.

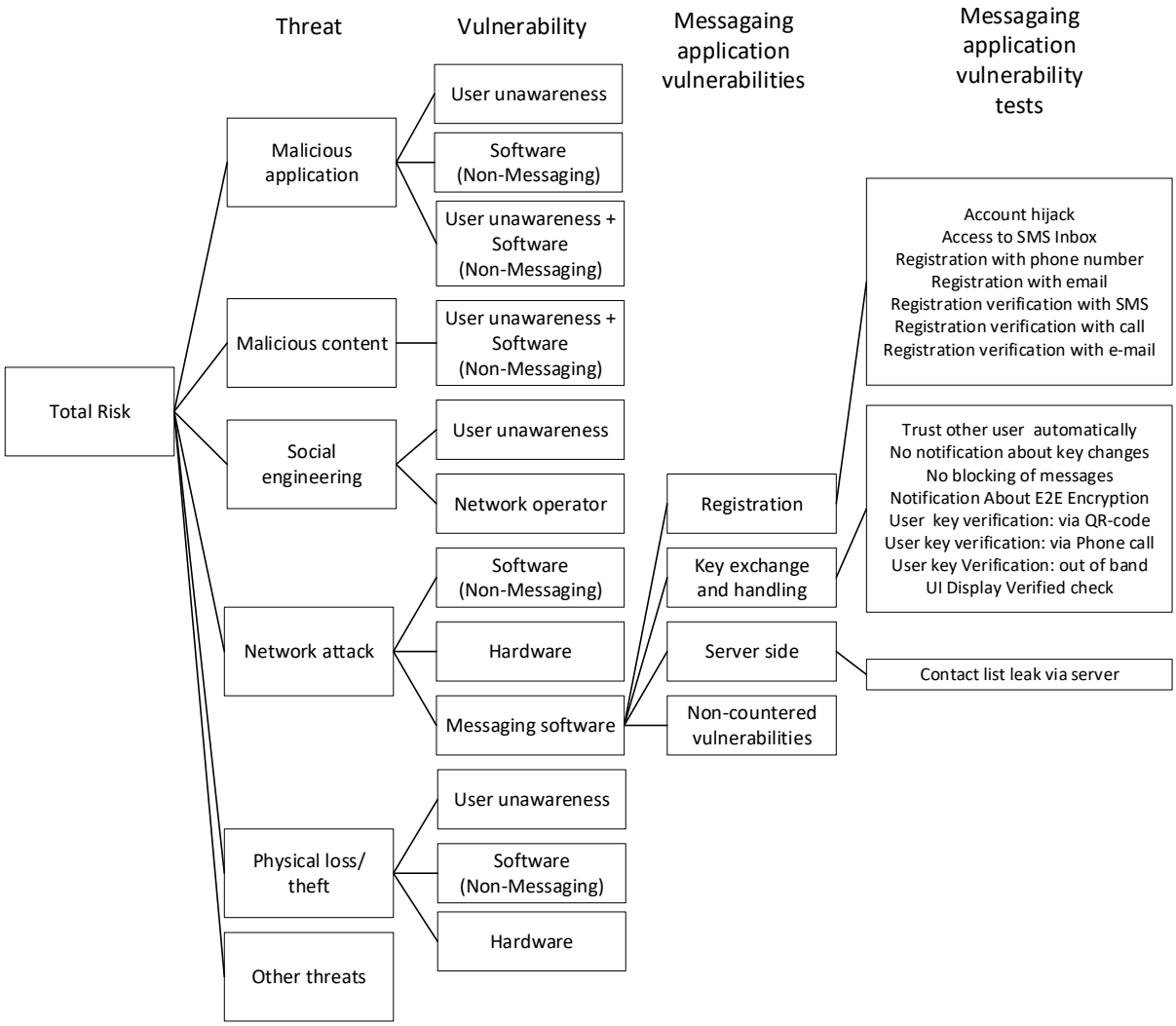

Figure 5. General risk model for smartphones with a messaging application installed

The description of threats and vulnerabilities in the above model are given in the table below.

Table 4. Risk model attack descriptions

Threat	**Vulnerability**	**Attack Description (threat + vulnerability)**
Malicious application	User Unawareness + Non-messaging software	Malicious application installation that takes advantage of user's unawareness and software vulnerability to get access to data
	Non-messaging software	Malicious application that is installed from a legitimate source gaining access to data by a software flaw/bug
	User unawareness	Malicious application getting location data knowingly from a user, with the user's acceptance/ignorance
Malicious content	User unawareness + Non-messaging software	Malicious content gaining control of a smartphone and/or access to data because of user action (NFC/QR/infected web page/) and software flaw
Social engineering	User unawareness	An Attacker gaining data via Phishing/Unintentional data disclosure
	Network (operator)	An Attacker gaining user's mobile identity by performing social engineering attack on a Network operator
Network attack	Non-messaging software	An Outside attacker gaining access to data via an attack on network infrastructure and /or man in the middle attack
	Hardware	An Attacker using aging technology to eavesdrop (for example 2G)
	Messaging application software, account registration	An Attacker hijacking an account
	Messaging application software, key handling and verification	An Attacker impersonating another user
	Messaging server software	An Attacker gaining a list of user's contacts
Physical loss of phone	User unawareness	An Attacker gaining access to data because of the missing protection or encryption
	Non messaging software	An Attacker gaining access to data because of the flaw in the smartphone OS
	Hardware	An Attacker gaining access to data because of the flaw in the smartphone's hardware

According to formula (1) we can calculate the total risk. Because in this thesis the author has chosen to study threats to a single asset – data -, we can assume that TotalRisk equals Data loss recovery cost, because sum of ThreatLikelihood is 1:

$$TotalRisk = DataLossRecoveryCost * \sum ThreatLikelihood = DataLossRecoveryCost \quad (2)$$

According to the model then we can assume that performed tests on messaging application can reduce the total risk by a certain per-centage amount.

What are the threat likelihoods and how much risk the messaging application in total can contribute and how much risk the tests performed on messaging application can reduce are evaluated in the next chapters, using expert opinions.

4 Description of AHP

One way to perform qualitative risk analysis and to find out how big ratios different smartphone and smartphone messaging application risks have from total risk is to ask expert opinion.

In this chapter author of the thesis gives a short overview of AHP (Analytic Hierarchy process) that can take subjective opinions of experts and calculate a final numerical result.

4.1 MCDA and MDCM

Multiple-criteria decision-making (MCDM) or multiple-criteria decision analysis (MCDA) is a sub-discipline of operations research that explicitly evaluates multiple conflicting criteria in decision making [31].

Multi criteria decision making has been applied in many domains. MCDM method helps to choose the best alternatives where many criteria have come into existence, the best one can be obtained by analysing the different scope for the criteria, weights for the criteria and to choose the optimum ones using any multi criteria decision making techniques. [32]

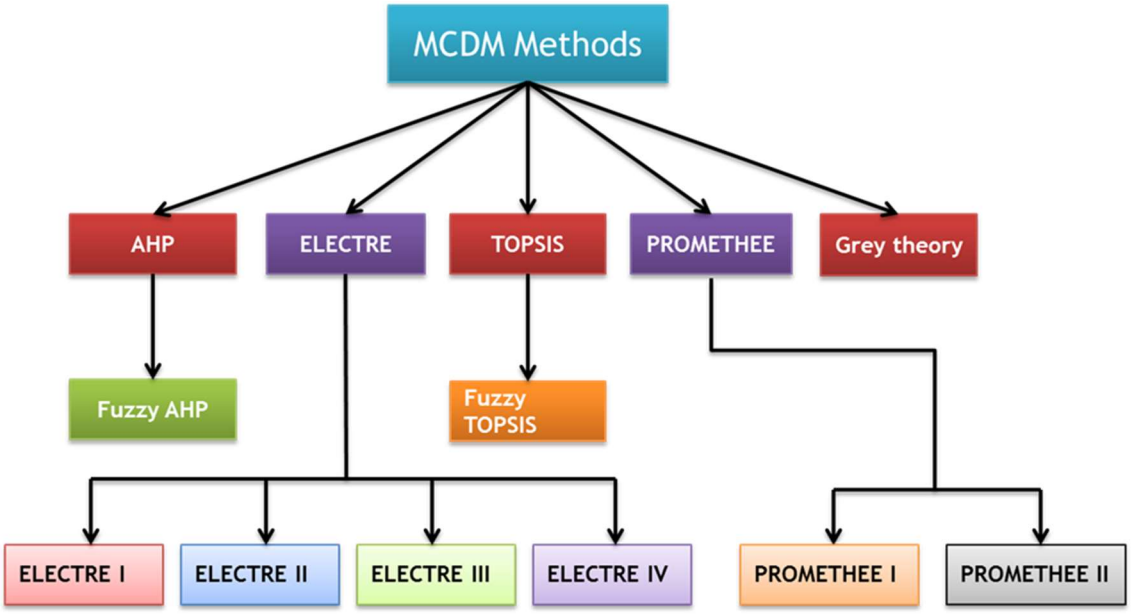

Figure 6. Overview of MCDM methods

4.2 AHP

Analytic Hierarchy Process (AHP) is a decision method, created by Thomas L. Saaty [4]. The main benefit of this method is that a subjective input can be used to find an objective solution to a problem.

AHP model consists of group of decision elements: one group is a set of alternatives, another group might be a set of criteria or sub-criteria, yet another group might be a set of scenarios and another group might be a set of decision-makers. The classical 3-layer AHP model consists of goal element, in the 1st layer, alternatives in the 3rd layer and criteria in the 2nd layer. Pairs of alternatives are usually compared to each other based on one criterion at a time, these pairwise comparisons form a comparison matrix. Similarly, pairs of criteria are compared to each other with respect to the goal, forming a comparison matrix of criteria. [5, p. 13]

According to the security model, established before in chapter 3.6, we can create an initial AHP model, in figure below.

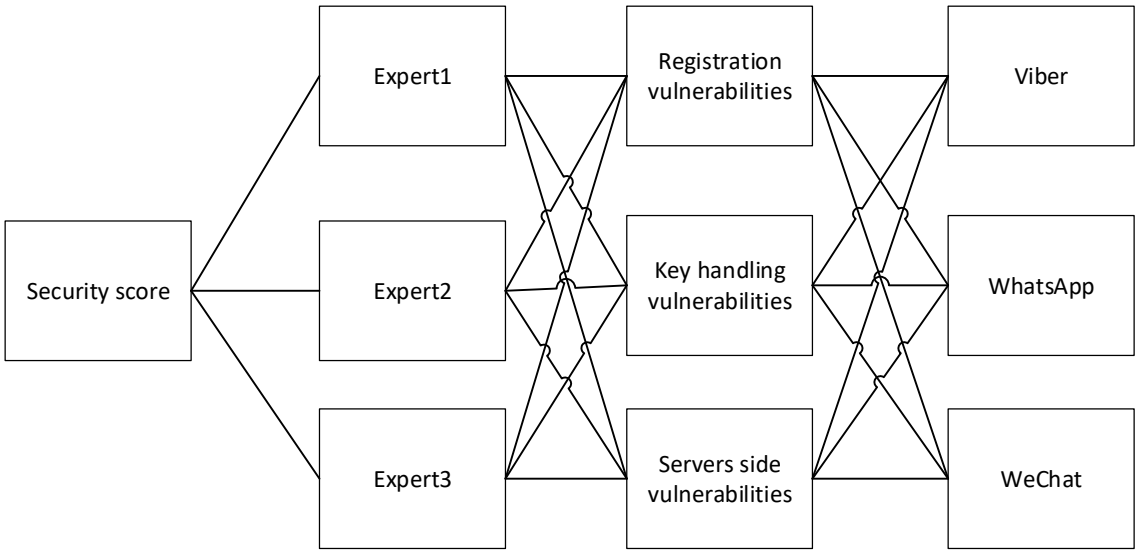

Figure 7. Initial AHP model

If there is a complicated problem, which depends on many criteria, it is quite difficult to make the right final choice between alternatives. If we define and group the criteria and evaluate the alternatives against the criteria and criteria against each other, it is easier to get the end result.

In the figure above experts decide on a most critical vulnerability for a messaging application and each vulnerability relates to an alternative (by tests performed). In the end

we would get a score for every alternative, where the tests are performed and expert opinion is weighted in.

The whole decision process is quite subjective: criteria-criteria and sometimes criteria-alternative relations are subjectively valued on a Saaty scale.

Table 5. Saaty scale [5, p. 9]

Intensity	**Definition**	**Description**
1	Equally important	Two activities contribute equally to the objective
3	Weak importance	Experience and judgement slightly favor one activity over another
5	Strong importance	One of the activities is strongly favored
7	Demonstrated importance	One of the activities is strongly favored, confirmed in practice
9	Absolute importance	One of the activities has the highest possible order of affirmation
2,4,6,8	Compromise choices	

After the pairwise criterion-criterion or criterion-alternative decisions have been made, we can have a comparison matrix for each group. The example is set in the table below.

Table 6. Sample comparison matrix

	Registration	**Key handling**	**Server side**
Registration	1	5	7
Key Handling	1/5	1	1/3
Server side	1/7	3	1

The table above shows that Registration vulnerabilities are deemed the most critical because it has been evaluated 5 : 1/5 against key handling and 7 : 1/7 against server side vulnerabilities.

To find the weights for the expert1 comparison matrix, given above, we have to find an eigenvector for the matrix. In this thesis, author used approximation method (geometric mean) to eigenvector calculations, as suggested by [5, p. 10]. The reason for choosing approximation was, that it was easier to use, and in two cases out of four the criteria

matrix was 3x3 where the approximation would equal the eigenvector. In one case the decision matrixes were automatically generated, and therefor consistent, what also constituted for approximation to be the same as eigenvector. In one case (5x5 matrix) the approximation would differ from eigenvector, but as author also performed statistical and sensitivity analysis later, the usage of approximation would be considered acceptable.

To find out if the choices were consistent, we can calculate a consistency index using maximum eigenvalue (λ) and rows (n) of the matrix [5, p. 12].

$$CI = \frac{\lambda_{max} - n}{n-1} \tag{3}$$

Consistency ratio is calculated from consistency index and random consistency index as [5, p. 12]:

$$CR = \frac{CI}{RI} \tag{4}$$

Random consistency index is pre-calculated and is dependent on the size of the matrix and to a lesser degree also on the eigenvector method and on the numerical Saaty scale [5, p. 12], [33]:

Table 7. Random consistency index for the geometric mean eigenvector method

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RI	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

If the consistency ratio (CR) is below 0.1, the matrix is considered stable, if the matrix is larger, also up to 0.2 is considered acceptable [5, p. 12], [33]. However even larger CR can be considered acceptable if the possible impact of inconsistent comparisons has been studied in the sensitivity analysis.

4.3 Statistical analysis with unchanged pool of experts

With the statistical analysis we can find out whether the grouped results of experts are statistically reliable with respect to the pairwise comparisons made by the experts, e.g. how likely it is for a certain weight to change that can cause end results of the model to change if we assume that the set of experts remains the same but the comparison values given by the experts might change.

For every comparison in the matrix we can derive an error factor. This factor shows how much we must multiply the subjective comparison value to make the comparison consistent [33, p. 18].

$$error_{factor} = \frac{1}{\sqrt[no_{rows}-2]{Product(column(i)) * Product(row(j)) * c_{ij}^{no_{rows}}}} \quad (5)$$

Where no_{rows} is number of rows in the comparison matrix, cij is a comparison on row (i), column (j).

The above error factor can also be used to calculate the expert error factor, over all decisions in all the comparison matrixes, contributed by that particular expert. This is first done by log transforming error factors, summing together, dividing by the number of error factors and using it as exponent to e [34].

$$expert\ error_{factor} = e^{\frac{\sum \ln(error_{factor})}{n}} \quad (6)$$

Where n is the number of error factors.

Then we can derive a group error factor common to an average decisionmaker by using geometric mean over all expert error factors [34].

The reason behind using log transformation is that ratios on ratio scale are multiplicative to each other, not additive and in order to use normal distribution approaches one would have to first log transform the data, then do the computations with the normal distribution and finally transform the log scale data back to original scale [34].

When we need to get a particular probability for a change of a specific pairwise group comparison on group decision level, we need to log the expected change in group comparison *vs*. the group error factor [34].

$$change = abs\left(\frac{\ln\left(\frac{groupComparisonNewValue}{groupComparisonOldValue}\right)}{\ln(group\ error_{factor})}\right) \quad (7)$$

Then we can find the cumulative probability of the change inside normal distribution (with mean 0 and standard deviation 1) [34].

$$probability = (1 - norm.dist\ (change))^n \quad (8)$$

Where n is the number of experts and norm.dist is a function in Excel. With this probability we can estimate if a change by experts in a single comparison is probable or not.

4.4 Statistical analysis with changing pool of experts

Instead of assuming that the set of experts remains the same, one could assume that the set (sample) of experts might change and a consider a new set of experts from the same pool (population) of experts.

First, a deviation factor matrix is found by formula [34]:

$$deviation\ factor_{ij} = \frac{e^{stddev.s\left(\sum ln\left(c_{ij}\right)\right)}}{\sqrt{n}} \quad (9)$$

Where c_{ij} is one expert's comparison value, n is number of experts, stdev.s is excel function. The idea behind the denominator is that measuring error (i.e standard deviation) decreases as a square root of number of measurements [34].

When we need to get a particular probability for a change of a specific pairwise comparison on the group decision level, we need to log the expected change in group comparison *vs*. the deviation factor [34].

$$change_{ij} = abs\left(\frac{\ln\left(\frac{groupComparisonNewValue}{groupComparisonOldValue}\right)}{\ln(deviation\ factor_{ij})}\right) \quad (10)$$

After that we can find the probability [34]:

$$probability_{ij} = \left(1 - norm.dist\ (change_{\mathrm{ij}})\right) \quad (11)$$

Were norm.dist is a function in Excel. With this probability we can estimate whether a change by experts in a single comparison is probable or not.

4.5 Sensitivity analysis

Sensitivity analysis can be performed to see how well the alternatives performed with respect to each of the objectives as well as how sensitive the alternatives are to changes in the importance of the objectives. [35, p. 79]

Uses of sensitivity analysis have been also described by [7, p. 3]:

- How robust the optimal solution is in the face of different parameter (comparison) values.
- Under what circumstances would the optimal solution change.
- How the optimal solution would change in different circumstances.
- What is the cost of following an alternative strategy.

The reason for the analysis is to ensure that the model would be as stable as possible and so firm that these could be used to make real-life decisions.

Because the AHP model is based on subjective comparison values, we use sensitivity analysis to find out if the results can change, if we change some of the weights of the criteria or alternative. One way to do this is to calculate the sensitivity factor [8, p. 43]:

$$SensitivityFactor = \frac{\boldsymbol{NewWeight}}{1-\boldsymbol{NewWeight}} * \frac{1-\boldsymbol{OriginalWeight}}{\boldsymbol{OriginalWeight}} \quad (12)$$

By taking sensitivity factor into account, one can decide whether the change is probable or not. If changing the criteria weight has sensitivity factor as 10, the change is not likely, however, when it is up to 2 (two), the change might be more likely. We can also use the change probability calculated in the previous subchapters (4.3 and 4.4) to find out how probable is a certain change in comparison values (and therefore in weights).

5 Case study

In this chapter the author performs a case study of AHP model, made of threats and vulnerabilities of smartphone messaging application, mainly to:

- Measure the threat likelihood of smartphone messaging application.
- Find a ranking method for smartphone messaging applications, in terms of vulnerabilities proven to be missing or security controls found

5.1 Model set-up

The AHP model is set up by using the criteria from figure 5 and is concluded in the table below.

Table 8. AHP model criteria

Goal (TotalRisk)	**Criteria Layer 1 (Threat)**	**Criteria Layer 2 (Vulnerability)**	**Criteria Layer 3 (Messaging app. Vulnerability)**	**Criteria layer 4 (Tests)**
	Malicious application			
	Malicious content			
	Social engineering			
	Network attack			
		Messaging software		
			Registration	Tests(6)
			Key handling& verification	Tests(8)
			Server side	Tests(1)
		Non-Messagaing software		
		Hardware		
	Physical loss/theft			

The following alternatives are also evaluated in terms to the tests performed, as by research conducted [26] [30]:

- WeChat
- Viber
- Telegram
- WhatsApp
- Signal
- Wire
- Riot

The AHP model constructed is not a classical one, because not every criterion influences the alternatives. However, the first two layers are kept to find the distribution of weights of the general threats, so that we could find the answer to one our objectives ("Measure the threat likelihood (security) that is influenced by a messaging application").

There were 8 questionnaires sent out, 6 security experts from Telia, SK ID Solutions, Cybernetica, Guardtime and two separate Government institutions answered the questionnaire in Appendix 2.

Group results from different experts were calculated as geometric mean into a single comparison matrix and then entered into the AHP model.

Because there are many tests in criteria layer 3, it was not practically possible to make pairwise comparison by experts (in total 43 comparisons). Therefore, the author decided to let experts rank the severity of vulnerability or the importance of security control in a scale of 1-3.

For layer 3 the ranking given by experts were inserted into (consistent) Saaty matrix. The value for the comparison was derived using following formula [34]:

$$comparison_{ij} = 3^{(ranking_i - ranking_j)} \quad (13)$$

Where $ranking_i$ and $ranking_j$ were the rankings of two tests (the missing vulnerability of existing security control) compared against each other. Index i and j have values in the range from one to number of compared items in the ranking (including comparison vs itself where comparison result is 1). For example, if we have following rankings by an expert: Criteria 1 (1), Criteria 2 (3), Criteria 3 (2), we would get following consistent comparison matrix:

Table 9. Automatically generated comparison matrix from individual rankings

	Criteria 1	Criteria 2	Criteria 3
Criteria 1	3^(1-1) = 1	3^(1-3) = 1/9	3^(1-2) = 1/3
Criteria 2	3^(3-1) = 9	3^(3-3) = 1	3^(3-2) = 3
Criteria 3	3^(2-1) = 3	3^(2-3) = 1/3	3^(2-2) = 1

After finding the individual expert comparison matrixes, a group matrix was found by using geometric mean on individual expert comparisons. The resulting weights from group matrix were then adjusted by the time difference in years the tests were performed at and after that normalized again and were then entered directly to layer 2.

The values for alternatives for criteria layer 4 (tests) were automatically set as 0 (security control not found/vulnerability found by research) or 1 (security control found/vulnerability proven not found).

The numerical values for group results for different layers are given in the Appendix 3-Appendix 6.

5.2 AHP Model

The final AHP model is visualized, using the Web-Hipre tool [9], in the figure below.

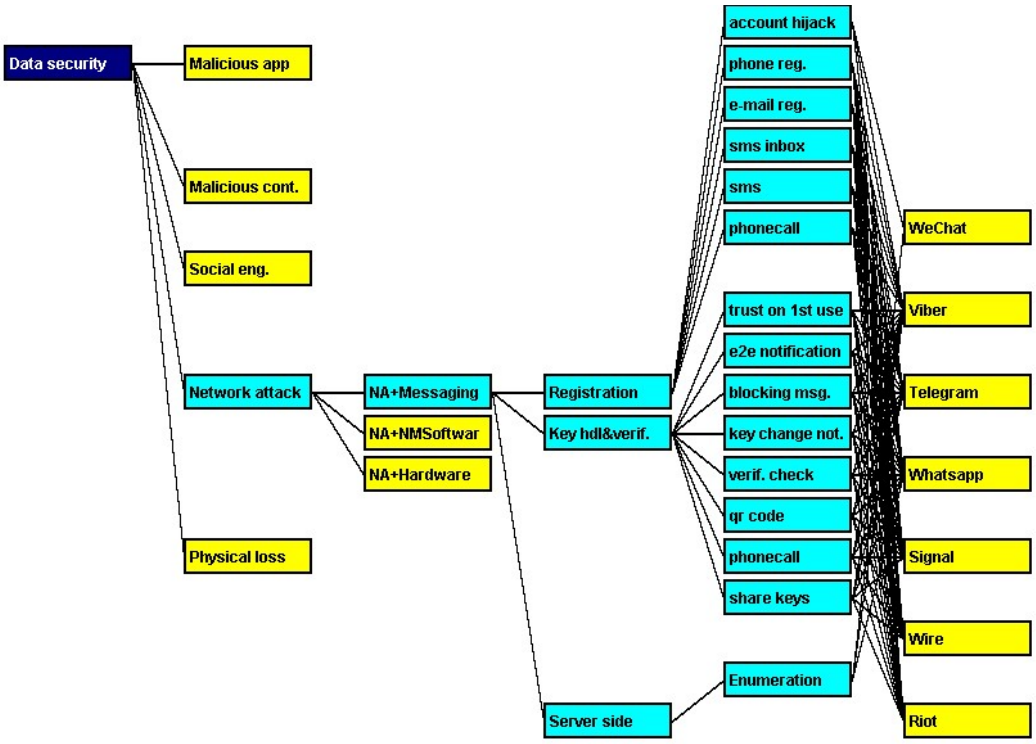

Figure 8. Final AHP model

5.3 Results for layer 1

Results on threat likelihood were achieved by entering the feedback from questionnaires (example questionnaire is given in Appendix 2).

According to IT security experts, only 6,2% of attacks to smartphones can be attributed to network attacks in general, according to the figure below.

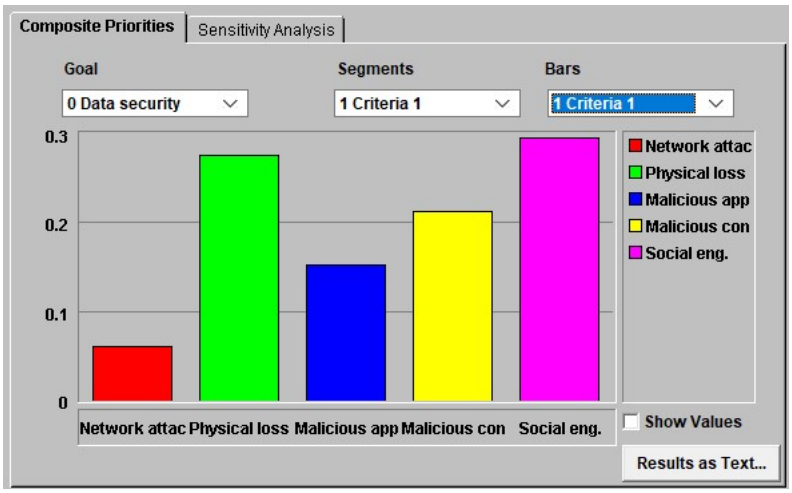

Figure 9. Group results for main threat likelihood for smartphone

When looking into the individual expert results for pairwise comparison of criteria in layer 1, we can find the following statistical results in the table below.

Table 10. Statistical results for expert responses

	CR	**Expert error factor (chapter 4.3)**
Expert1	0,26	2,62
Expert2	0,11	1,94
Expert3	0,24	2,8
Expert4	0,13	1,32
Expert5	0,11	2,36
Expert6	0,14	3,66

As can be seen from the statistical analysis, two experts did not have highly consistent results (CR>0.2). However, the author decided to keep these results because even when on its own the consistency is not adequate, these add value to a group decision.

When looking at error factors, it can be seen that single experts comparison results can change from average 1,32 times(Expert 4) to 3,66 times (Expert 6).

The author investigated further by testing the final result with different expert group combinations (total 63), the results are in the figure below.

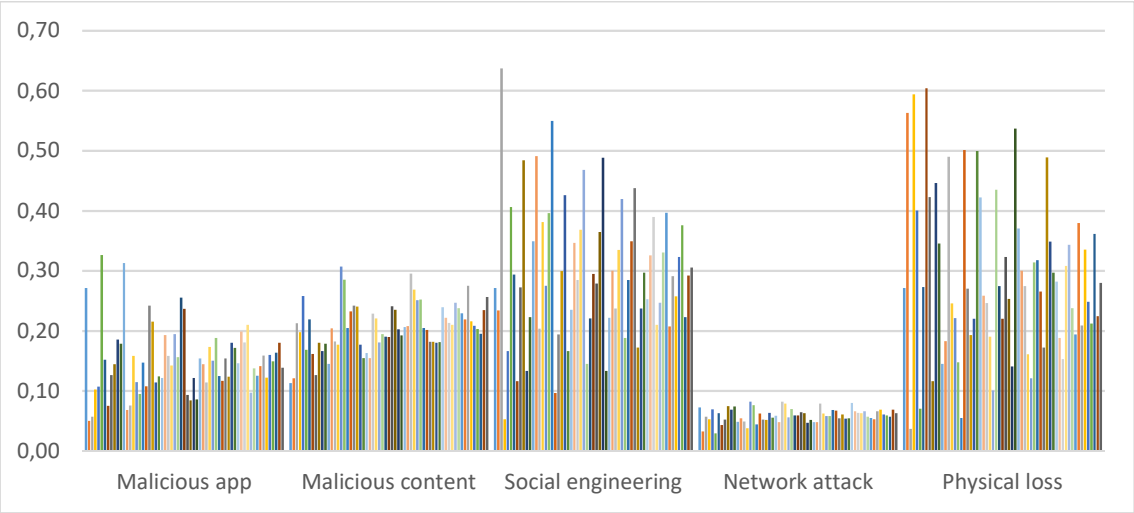

Figure 10. Threat likelihoods using different expert group combinations

When we combine the results into different group combinations, we can still see from the table above that for Network Attack, Malicious app and Malicious content, the results are quite stable. For Social engineering and Physical loss the results vary a little, but it can still be said that these seem to be the top threats by expert opinions. The individual calculations are given in Appendix 7.

Table 11. Statistical overview of weights for different expert group combinations

	Malicious app	**Malicious content**	**Social engineering**	**Network attack**	**Physical loss**
Minimum	0,05	0,11	0,05	0,03	0,04
Geometric mean	0,14	0,20	0,27	0,06	0,25
Median	0,15	0,20	0,29	0,06	0,27
Maximum	0,33	0,31	0,64	0,08	0,60

5.4 Results for layer 2

According to experts, 48% of all network attacks can be attributed to the messaging application when it is installed in a smartphone. All the answers were consistent (CR < 0.2). The results are presented in the following figure.

Figure 11. Network attack weight distribution

5.5 Results for layer 3 and 4

According to expert opinions, most of the attacks (67%) to messaging applications are attributable to registration vulnerabilities. All the answers were consistent (CR < 0.2), except one that was highly unstable (CR=2,21) and was left out from the results. The results are presented in the figure below.

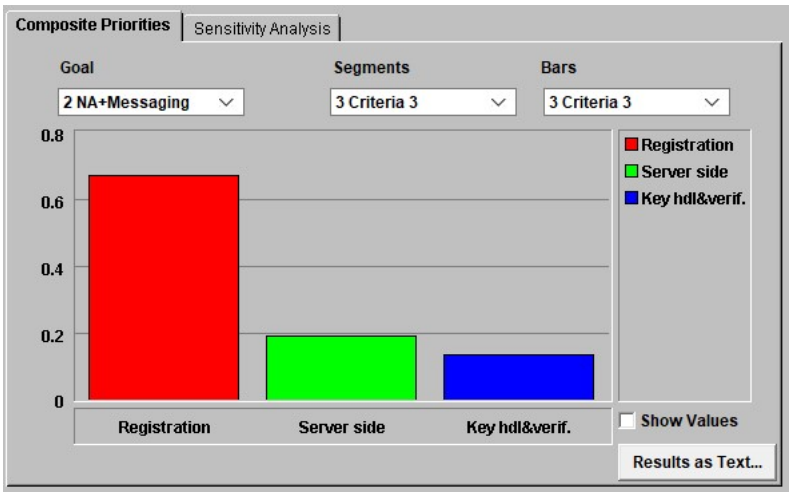

Figure 12. Important vulnerabilities for smartphone messaging application by expert opinions

By inserting the ranking data given by experts into AHP matrix, as discussed in the Chapter 5.1 and the formula (13), we get the following results:

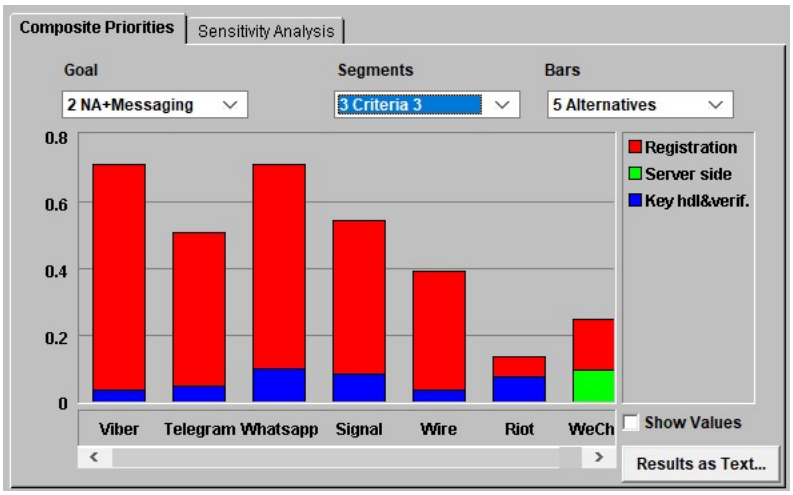

Figure 13. Final security ranking of smartphone messaging applications

According to the group decision results at layers 3 and 4 , WhatsApp is the most secured (71.3%/100%) and close to second position is Viber (71.0%/100%).

To give a more definite opinion on the ranking, we can perform a sensitivity analysis in the following chapter.

5.6 Sensitivity analysis

5.6.1 Sensitivity analysis of registration vulnerability

According to the graph below, the final order of apps changes if the registration vulnerabilities weight is increased from 0.67 to 0.68. The weight of registration vulnerabilities must be increased (0.68/(1-0.68)=2,15) / (0.67/(1-0.67)=2,03) = 1,05 times for it to change the final order (Viber).

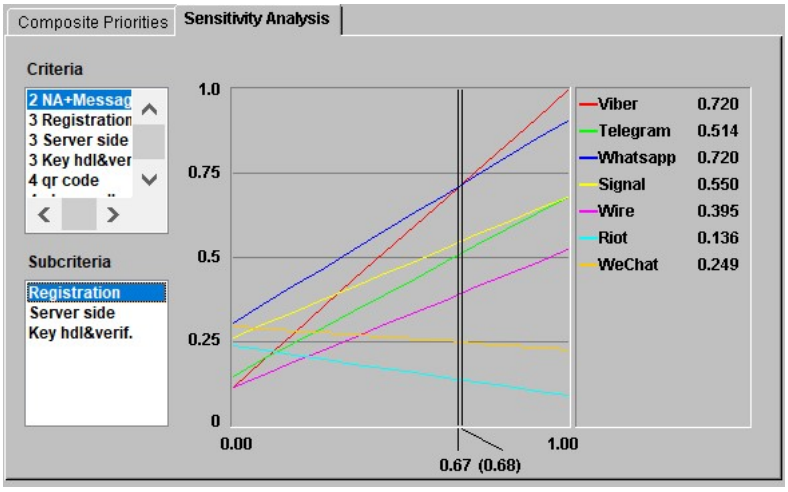

Figure 14. Sensitivity of registration vulnerability

To find out whether it is likely to change or not we are using the formulas derived in the subchapter 4.3. In order to increase the registration weight to 0,68, the experts would have to increase the registration comparison values. The biggest effect is given by increasing the registration *vs.* key handling and verification 1,03 times by all experts in average. The probability of this happening is 1,3%, so not very likely but it could happen.

5.6.2 Sensitivity analysis of key handling and verification vulnerability

According to the graph below, the final order of apps changes if key handling & verification vulnerabilities weight is decreased from 0.13 to 0.12. The weight of key handling & verification vulnerabilities must be decreased (0.13/(1-0.13)=0,15) / (0.12/(1-0.12)=0,13) = 1,13 times for it to change the final order (Viber).

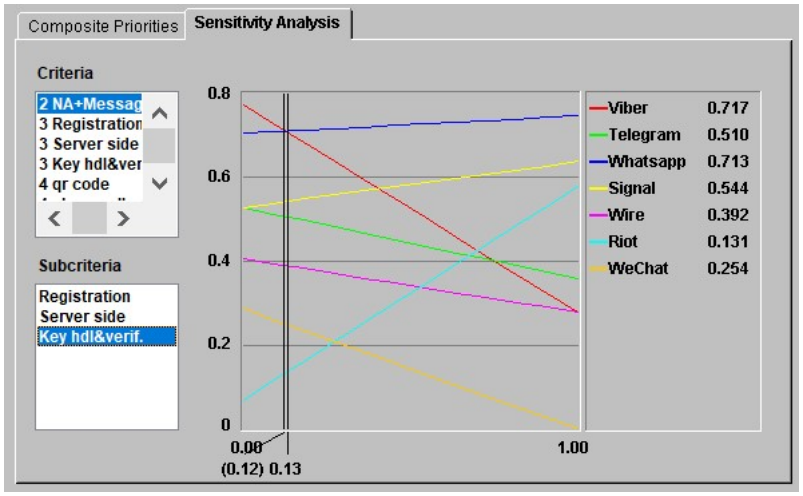

Figure 15. Sensitivity of key handling and verification vulnerability

To find out whether it is likely change or not we are using the formulas derived in the subchapter 4.3. In order to decrease the key handling and verification weight to 0,12 the experts would have to decrease the key handling and verification comparison values. The biggest effect is given by decreasing the key handling and verification *vs*. the registration comparison 1,15 times by all experts in average. The probability of this happening is 0,6%, so not very likely.

5.6.3 Sensitivity analysis of server side vulnerabilities

According to the graph below, the final order of apps changes if server side vulnerabilities weight is increased from 0.19 to 0.58. The weight of key server side attacks must be increased (0.58/(1-0.58)=1,38) / (0.19/(1-0.19)=0,23) = 6 times for it to change the final order (WeChat).

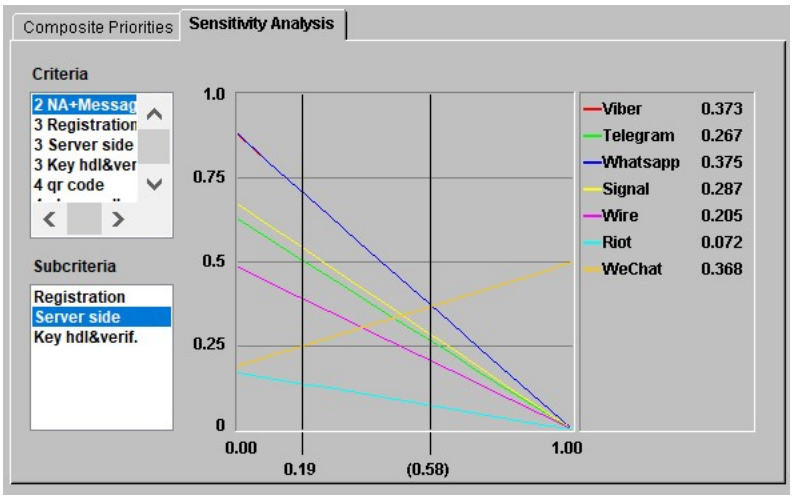

Figure 16. Sensitivity of server side vulnerabilities

To find out whether it is likely change or not we are using the formulas derived in the subchapter 4.3. In order to increase the server side weight to 0,58, the experts would have to increase the server side comparison values. The biggest effect is given by increasing the server side *vs.* registration comparison 25 times by all experts in average, that is not probable.

5.6.4 Sensitivity analysis for layer 4 tests

On layer 4 we analyse the rankings of different tests and verify which rankings must change and how much for the final order of apps to change.

In the sensitivity analysis graph below, we can see that, by changing the e-mail registration test weight from 0.09 to 0.1, we can change also the final ranking of apps.

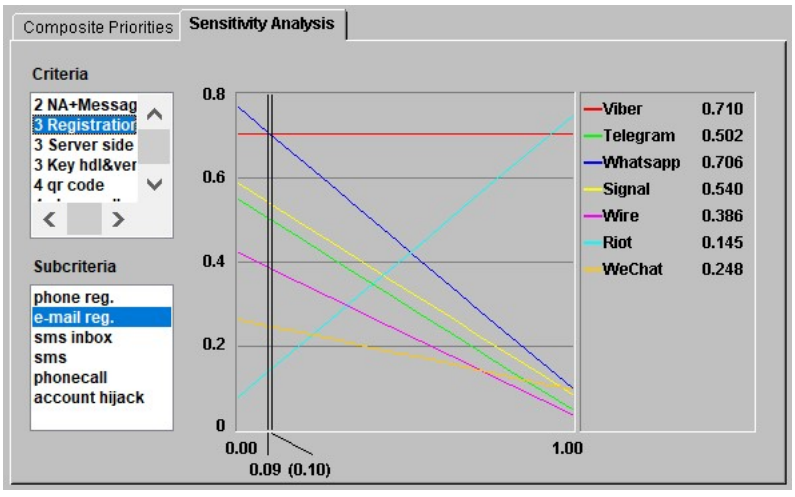

Figure 17. Sensitivity of e-mail registration test

For this change we must increase the e-mail registration weight ((0.09/(1-0.09)=0,098 / (0.1/(1-0.1)=0,11) = 1,13 times.

To calculate how probable this change is, we use formulas in paragraph 4.4, and find out that we have to change comparison of registration via phone number *vs*. registration via e-mail from 2.5 to 1,98. The probability of such change is 30%, and is statistically very likely. However, this change is not probable to be done by security experts, because e-mails are easier to take over than phone numbers. There are websites that have collected the e-mails and passwords for web services that have been breached. One of such website claims to have data for 7 billion accounts [36].

We can also monitor a similar possibility when looking into the changing key verification check test, on the figure below.

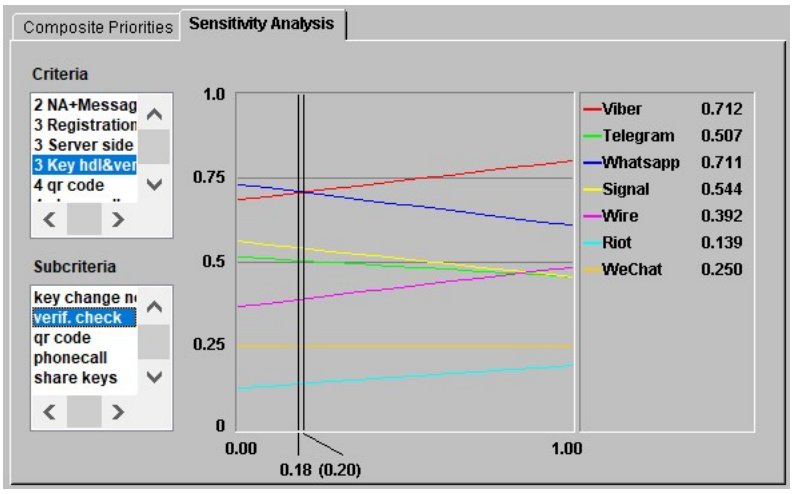

Figure 18. Sensitivity of key verification check test

In the above sensitivity analysis graph we can see that by changing the key verification check test weight from 0.18 to 0.20, we can change also the final ranking of apps.

For this change we must increase the key verification test weigh ((0.20/(1-0.20)=0,25 / (0.18/(1-0.18)=0,21) = 1,19 times.

To calculate how probable this change is, we use formulas in the paragraph 4.4, and find out that we have to change comparison of key check verification vs trust other users from 1,73 to 4,2. The probability of such change is 0,16% and is statistically not likely.

5.7 Sensitivity analysis results

The author sought into changing the weights of different criteria to see if the ranking order of the final model would change.

The author found one criteria (e-mail registration test) where increasing the likelihood *vs.* the phone number registration tests could lead to change on the ranking of the messaging applications in 30% statistical probability. However, when taking security into account this change is not likely.

On all other criteria changes tested, the statistical probability was lower than 2%:

- Increasing Registration vulnerabilities weight 0,67-0,68
- Decreasing Key handling and verification vulnerabilities weight 0,13-0,12
- Increasing server side vulnerabilities weigh 0,19-0,58
- Increasing Key verification check weight 0,18-0,20

Summary

The goal of this thesis is to find out of what the smartphone messaging application security consists and how it would be possible to rank smartphone messaging application security vs. similar applications. The goal and sub-goals of the thesis were achieved.

Theoretical framework, how to build a risk model for smartphone applications and how to rank security between applications, was established in the second chapter, using ISO 27000:2014 series of standards methodology.

Scientific literature and reports were used to generate a list of possible threats and vulnerabilities for a smartphone. Knowing the smartphone threats, vulnerabilities and also security tests done on alternative messaging applications, a complete security model was built in chapter 3.6.

To find out the weights-or ratios between different threats and vulnerabilities, the author investigated a methodology that could turn subjective valuations into objective results, AHP. 6 security experts answered to the questionnaire, that made it possible to find out the rankings between different threats, vulnerabilities, security tests done and on messaging applications.

The author of this thesis found out that according to expert opinions, messaging application only influences 2,9% of the total smartphone information security risk.

According to security tests completed and expert opinions, the best ranking messaging application was WhatsApp with Viber close in second place.

The results were statistically analysed and with one exception would hold with 98% accuracy. Exception that was found was related to a importance ranking of a smartphone messaging application test. It was statistically possible (30%) that changing the test ranking would also change the final ranking of the applications. However, by opinion of the author of thesis, this change was not possible to be done in the context of security.

References

[1] GSMA, "Mobile Economy," 2019. [Online]. Available: https://www.gsma.com/r/mobileeconomy/. [Accessed 4 May 2019].

[2] A. De Luca, S. Das, O. Martin, I. Iulia and L. Ben, "Expert and Non-Expert Attitudes towards (Secure) Instant Messaging," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, 2016.

[3] *Information technology - Security techniques - Information security risk management, ISO/IEC Standard 27005:2014,* 2014.

[4] T. L. Saaty, The Analytic Hierarchy Process, New York: McGraw-Hill, 1980.

[5] L. Võhandu, *Subjektiivsetest hinnangutest objektiivsete tulemusteni: loengukonspekt,* Tallinn: Tallinna Tehnikaülikooli trükikoda, 1998.

[6] A. Saltelli, "Sensitivity Analysis for Importance Assessment," *Risk Analysis,* vol. 22, no. 3, pp. 579-590, 2002.

[7] D. J. Pannell, "Sensitivity analysis of normative economic models: theoretical framework and practical strategies," *Agricultural Economics,* vol. 16, no. 2, pp. 139-152, 1997.

[8] O. Oidekivi, "Master thesis: The Development of an AHP Sensitivity Analysis Application based on the XMCDA 2.2.2 Standard," 2018. [Online]. Available: https://digi.lib.ttu.ee/i/?10617.

[9] J. Mustajoki and R. Hämäläinen, "Web-Hipre: Global Decision Support By Value Tree And AHP Analysis," *INFOR: Information Systems and Operational Research,* vol. 38, no. 3, pp. 208-220, 2000.

[10] *Information technology - Security techniques -Information security management systems - Overview and vocabulary, ISO/IEC Standard 27000:2014,* 2014.

[11] M. Nieles, K. Dempsey and V. Pillitteri, "An Introduction to Information Security, NIST Special Publication 800-12, Revision 1," 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[12] "Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1," 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed 03 May 2019].

[13] "Oxford Dictionary," Oxford University Press, [Online]. Available: https://en.oxforddictionaries.com/definition/smartphone. [Accessed 03 May 2019].

[14] W. Jeon, J. Kim, Y. Lee and D. Won, "A Practical Analysis of Smartphone Security," in *Human Interface and the Management of Information. Interacting with Information*, Orlando, 2011.

[15] M. Theoharidou, A. Mylonas and D. Gritzalis, "A Risk Assessment Method for Smartphones," in *Information Security and Privacy Research*, Heraklion, 2012.

[16] C. Mulliner, "Master Thesis: Security of Smart Phones," 2006. [Online]. Available: https://mulliner.org/mobilesecurity/2006_mulliner_MSThesis.pdf.

[17] C. Nachenberg, "A Window Into Mobile Device Security," 2011. [Online]. Available: https://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf. [Accessed 03 May 2019].

[18] GSMA, "History," [Online]. Available: https://www.gsma.com/aboutus/history. [Accessed 03 May 2019].

[19] M. Ghaderi and S. Keshav, "Multimedia messaging service: system description and performance analysis," in *First International Conference on Wireless Internet (WICON'05)*, Budapest, 2005.

[20] K. Church and R. Oliveira, "What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS," in *MobileHCI '13 Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, Munich, 2013.

[21] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," 2010. [Online]. Available: https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users. [Accessed 03 May 2019].

[22] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev and C. Glezer, "Google Android: A Comprehensive Security Assessment," *IEEE Security & Privacy,* vol. 8, no. 2, pp. 35 - 44, 2010.

[23] CVE Details, "CVE Details," [Online]. Available: https://www.cvedetails.com/. [Accessed 03 May 2019].

[24] F. Parker, J. Ophoff, J. Van Belle and K. R, "Security awareness and adoption of security controls by smartphone users," in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Cape Town, 2015.

[25] M. Souppaya and K. Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124 Revision 1," 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. [Accessed 03 May 2019].

[26] R. Mueller, S. Schrittwieser, P. Fruehwirt, P. Kieseberg and E. Weippl, "Security and privacy of smartphone messaging applications," *International Journal of Pervasive Computing and Communications,* vol. 11, no. 2, pp. 132-150, 2015.

[27] T. Lederm and N. Clarke, "Risk Assessment for Mobile Devices," in *Trust, Privacy and Security in Digital Business*, Tolouse, 2011.

[28] ENISA, "ENISA Threat Landscape Report 2018," 2018. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape. [Accessed 03 May 2019].

[29] Telia, "Telia online store," [Online]. Available: (https://pood.telia.ee/nutitelefonid?type=list&page=1&sort=ExpensiveFirst). [Accessed 03 May 2019].

[30] C. Johansen, A. Mujaj, H. Arshad and J. Noll, "The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications (authors' version)," 2018. [Online]. Available: https://arxiv.org/abs/1807.07952v1.

[31] Wikipedia, "Multiple criteria decision analysis," [Online]. Available: https://en.wikipedia.org/wiki/Multiple-criteria_decision_analysis. [Accessed 03 May 2019].

[32] M. Aruldoss, M. Lakshmi and V. Venkatesan, "A Survey on Multi Criteria Decision Making Methods and Its Applications," *American Journal of Information Systems,* vol. 1, no. 1, pp. 31-43, 2013.

[33] A. Kitsik, "Improving the sensitivity analysis of the Analytic Hierarchy Process," 2007. [Online]. Available: https://maurus.ttu.ee/ained/IDN5120/doc/16/Ahti_Kitsik_magt66_2007.pdf. [Accessed 03 May 2019].

[34] T. Veskioja, "Re: _magistritöö,_viimane_versioon," Personali email (03.05.2019).

[35] E. Forman and M. Selly, "Decision By Objectives," 1996. [Online]. Available: http://professorforman.com/decisionbyobjectives/dbo.pdf. [Accessed 05 May 2019].

[36] "';--have i been pwned?," [Online]. Available: https://haveibeenpwned.com/. [Accessed 06 May 2019].

Appendix 1 – Messaging application vulnerability and security control tests

Account hijacking: Most applications prompt the user to enter their phone number first and then send a SMS to that number containing an (usually 4 to 6-digit) authentication code which the user has to enter. In some cases, it was possible to emulate the code sending or receiving in such a way that it was possible to hijack a particular account related to a mobile subscription.

Sender ID spoofing/Message manipulation: This vulnerability class deals with an attacker manipulating or forging messages and sender information without hijacking the entire account. This usually involves creating and sending messages with a fake (spoofed) sender ID by bypassing user-identification mechanisms inside the application.

Unrequested SMS/phone calls. As most applications use passive SMS/call-based varication during sign-up, it is possible to generate unwanted messages or even phone calls to arbitrary phone numbers.

Enumeration. Nearly/Pretty much all applications allow the user to upload their phone book to identify other registered users. The server usually replies with a list of contacts that are also registered or the service. By uploading specific phone numbers an attacker can gain knowledge about whether the targeted person uses the service. This information can potentially be used for further attacks such as impersonation or spoofing attacks.

Setup and registration tests: The setup and registration process are the first a user needs to go through after installing an application. This test checks how the applications handle the registration process, what the user needs to do to register a new account and whether there are multiple ways to register or only with a phone number.

- Phone registration: Register account with a phone number
- E-mail registration: Register account with an e-mail address

- SMS verification: Receive verification code through SMS
- Phone call verification: Receive verification code through a phone call
- Access SMS inbox: App requires access to SMS Inbox in order to read the verification code automatically
- Contact list upload: App requires to upload contacts to see if others are using the same application.

Initial contact : This test scenario is a part of each of the other scenarios where two users have a conversation. When Bob sends to Alice a message, tests look how the application handles the first message sent to the other participant and whether the participants are informed of the secure messaging capabilities or whether the application shows how the cryptographic keys are used.

- Trust-On-First-Use: Automatically verify each other's keys on conversation initiation (in comparison with other apps, where users have to manually verify each other)
- Notification About E2E Encryption: Does the app present notifications to explain to the user that messages are end-to-end encrypted?
- Message after key change: This scenario tests how the application handles changes of cryptographic keys after Bob deletes the application in the middle of a conversation with Alice. After Bob has reinstalled his application, Alice sends him a new message and examines if the application gives Alice any information about the key changes.
- Notification about key changes: Notifies Alice that Bob has changed cryptographic keys.
- Blocking message: Blocks new message from being sent until Alice and Bob verify each other.

Verification process: In a conversation, Alice and Bob want to verify each other, to ensure that they are having a conversation with honest participants. This test scenarios look at

how the verification process works and if it is a secure and usable method of doing the verification between participants.

- QR-code: Verify each other through a QR-code (each messaging app can scan other users QR code)
- Verify by Phone call: Call each other with E2E-encrypted phone call and read keys out loud.
- Share keys through 3rd party: Share the keys through other applications (e.g PGP)
- Verified check: Users can check later if a specific user is already verified.

Other Security Implementations

- Passphrase/code: Add a passphrase/code that only the user knows and enters it to gain access to the application.
- Two-step verification: When registering after a reinstall or new device, then a second, passphrase/code is needed which only the specific user knows.
- Screen security: The user is not allowed to screenshot within the application.
- Clear trusted contacts: Clear all the contacts the user has verified, which means the user needs to verify each contact once again.
- Delete devices from account: If the application allows multiple devices, then there should be an option to delete devices which are not in use anymore.

Appendix 2 – Questionnaire

Background: Users use smartphones for both private and company use. They mostly use messaging apps (like Viber, Telegram, Signal, Riot, Wire or WhatsApp) for messaging or calling with friends or colleagues.

Question: In your opinion, which security threats to user data are more likely to happen?

By data it is meant any data, that is either stored locally in a smartphone (contacts, message, voice logs, configuration, camera output), input by a user (via keyboard), input from sensor, exchanged over communication network (messages, status information, voice data) or stored in external servers.

Particular threats in in this questionnaire are:

Threat to user data	**Example attacks using threat**
Malicious Application (includes, Malware, Ransomware, Spyware, etc)	Malicious application using the User's unawareness to install and software vulnerability to get access to data Malicious application that is installed from legitimate source gaining access to data by a software flaw/bug Malicious application getting data knowingly from user, with user acceptance/ignorance
Malicious content	Malicious content gaining control of a smartphone and/or access to data because of user's action (NFC/QR/infected web page/) and software flaw
Social engineering	An Attacker gaining data via Phishing/Uninentional data disclosure An Attacker gaining users mobile identity by performing social engineering attack on Network operator
Network attack	An Outside attacker gaining access to data via an attack to phone software (OS/App) or Application server software using network infrastructure (for example man in the middle attack), An Attacker using aging hardware of technology to eavesdrop (for example 2G)
Physical loss or theft of a phone	An Attacker gaining access to data because of the missing or weak protection (e.g. screen lock or memory encryption)

	An Attacker gaining access to data because of flaw in the smartphone's OS An Attacker gaining access to data because of the flaw in the smartphone's hardware

Which threats on a smartphone in your opinion are more likely to happen on/with? User's data?
NB Please put one check per line.

Malicious Application	☐	☐	☐	☐	☐	Malicious content
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Malicious Application	☐	☐	☐	☐	☐	Social engineering
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Malicious Application	☐	☐	☐	☐	☐	Network attack
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Malicious Application	☐	☐	☐	☐	☐	Physical loss/theft of phone
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Malicious content	☐	☐	☐	☐	☐	Social engineering
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Malicious content	☐	☐	☐	☐	☐	Network attack
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	

Malicious content	☐	☐	☐	☐	☐	Physical loss/theft of phone
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Social engineering	☐	☐	☐	☐	☐	Network attack
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Social engineering	☐	☐	☐	☐	☐	Physical loss/theft of phone
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Network attack	☐	☐	☐	☐	☐	Physical loss/theft of phone
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	

When looking into network attacks, which attack is more likely to happen when users use smartphone messaging apps?

Network attack on Messaging App	☐	☐	☐	☐	☐	Network attack on Non-Messaging Software (OS/Another App)
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Network attack on Messaging App	☐	☐	☐	☐	☐	Network attack on Phone hardware
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Network attack on Non-Messaging	☐	☐	☐	☐	☐	Network attack on Phone hardware

Software (OS/Another App)	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	

When looking into network attacks to smartphone messaging app/server, which attack is more likely to happen?

Attack	**Description**
Registration	Attack on registration procedure (account hijack using fake calls/SMS)
Key handling&verification	Attacks on key exchange, how keys are generated, presented and verified for users
Server side	Attacks on messagaing application server

Registration	☐	☐	☐	☐	☐	Key handling& verfication
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Registration	☐	☐	☐	☐	☐	Server side
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	
Key handling& verfication	☐	☐	☐	☐	☐	Server side
	Highly more likely <-	More likely <-	Equal	More Likely ->	Highly more likely ->	

Please rank a severity of vulnerability in messaging application (3-major, 2-normal, 1 minor):

Account hijack	
Access to SMS Inbox (for reading registration code)	
Trust other user with its (encryption) keys automatically without verification	
No notification about user (encryption) key changes on other side	

No blocking of messages when (encryption) keys of other user have changed	
Spamming other user with SMS/calls	
Contact list leak via server	

Please rank importance of security control in messaging application (3-very important, 2-important, 1 not important):

Registration with phone number	
Registration with email	
Registration verification with SMS	
Registration verification with call	
Registration verification with e-mail	
Notification About E2E Encryption	
User (encryption) key verification: via QR-code	
User (encryption) key verification: via Phone call	
User (encryption) key Verification: out of band (e.g PGP)	
UI Display Verified check on User (encryption) key verification	
Other Security: Additional Messaging App Screenlock Passphrase	
Other Security: Two step verification on account recovery	
Other Security: Screenshot prohibited on secure conversations	

Appendix 3 - Layer 1 weights calculation

Group_1	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	3,00	0,33[1]	3,00	3,00	1,55	0,27
Malicious content	0,33	1,00	0,33	3,00	0,33	0,64	0,11
Social engineering	3,00	3,00	1,00	3,00	0,33	1,55	0,27
Network attack	0,33	0,33	0,33	1,00	0,33	0,42	0,07
Physical loss	0,33	3,00	3,00	3,00	1,00	1,55	0,27
Sum	5,00	10,33	5,00	13,00	5,00	5,72	1,00
Group_2	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	0,33	0,11	3,00	0,11	0,42	0,05
Malicious content	3,00	1,00	1,00	3,00	0,11	1,00	0,12
Social engineering	9,00	1,00	1,00	9,00	0,33	1,93	0,23
Network attack	0,33	0,33	0,11	1,00	0,11	0,27	0,03
Physical loss	9,00	9,00	3,00	9,00	1,00	4,66	0,56
Sum	22,33	11,67	5,22	25,00	1,67	8,27	1,00
Group_3	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	0,33	0,11	0,33	3,00	0,52	0,06
Malicious content	3,00	1,00	0,11[2]	9,00	9,00	1,93	0,21
Social engineering	9,00	9,00	1,00	9,00	9,00	5,80	0,64
Network attack	3,00	0,11	0,11	1,00	1,00	0,52	0,06
Physical loss	0,33	0,11	0,11	1,00	1,00	0,33	0,04
Sum	16,33	10,56	1,44	20,33	23,00	9,10	1,00

[1] Expert likely entered this comparison wrongly and it should be 3 instead of 1/3 because 3 would make the matrix consistent, the value was not changed by author of thesis

[2] Using 1 here would make the matrix consistent, however the initial value was not changed by the author of theses

Group_4	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	0,33	3,00	3,00	0,11	0,80	0,10
Malicious content	3,00	1,00	3,00	3,00	0,33	1,55	0,20
Social engineering	0,33	0,33	1,00	1,00	0,11	0,42	0,05
Network attack	0,33	0,33	1,00	1,00	0,11	0,42	0,05
Physical loss	9,00	3,00	9,00	9,00	1,00	4,66	0,59
Sum	13,67	5,00	17,00	17,00	1,67	7,84	1,00
Group_5	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	0,33	0,33	3,00	0,33	0,64	0,11
Malicious content	3,00	1,00	3,00	3,00	0,33	1,55	0,26
Social engineering	3,00	0,33	1,00	3,00	0,33	1,00	0,17
Network attack	0,33	0,33	0,33	1,00	0,33	0,42	0,07
Physical loss	3,00	3,00	3,00	3,00	1,00	2,41	0,40
Sum	10,33	5,00	7,67	13,00	2,33	6,02	1,00
Group_6	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	3,00	0,33	9,00	9,00	2,41	0,33
Malicious content	0,33	1,00	0,33	9,00	3,00	1,25	0,17
Social engineering	3,00	3,00	1,00	9,00	3,00	3,00	0,41
Network attack	0,11	0,11	0,11	1,00	0,33	0,21	0,03
Physical loss	0,11	0,33	0,33	3,00	1,00	0,52	0,07
Sum	4,56	7,44	2,11	31,00	16,33	7,39	1,00
Group_123456	Malicious app	Malicious content	Social engineering	Network attack	Physical loss	Geomean	Weights
Malicious app	1,00	0,69	0,33	2,50	0,83	0,86	0,15
Malicious content	1,44	1,00	0,69	4,33	0,69	1,25	0,22
Social engineering	3,00	1,44	1,00	4,33	0,69	1,67	0,29
Network attack	0,40	0,23	0,23	1,00	0,28	0,36	0,06
Physical loss	1,20	1,44	1,44	3,60	1,00	1,55	0,27
Sum	7,04	4,81	3,70	15,75	3,50	5,69	1,00

Appendix 4 – Layer 2 weights calculation

Group1	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	0,33	0,33	0,48	0,14
Messaging software	3,00	1,00	3,00	2,08	0,58
Other software	3,00	0,33	1,00	1,00	0,28
Sum	7,00	1,67	4,33	3,56	1,00
Group2	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	0,11	0,33	0,33	0,06
Messaging software	9,00	1,00	9,00	4,33	0,81
Other software	3,00	0,11	1,00	0,69	0,13
Sum	13,00	1,22	10,33	5,35	1,00
Group3	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	0,33	0,33	0,48	0,14
Messaging software	3,00	1,00	3,00	2,08	0,58
Other software	3,00	0,33	1,00	1,00	0,28
Sum	7,00	1,67	4,33	3,56	1,00
Group4	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	0,11	0,33	0,33	0,08
Messaging software	9,00	1,00	3,00	3,00	0,69
Other software	3,00	0,33	1,00	1,00	0,23
Sum	13,00	1,44	4,33	4,33	1,00
Product	27,00	0,04	1,00		
Group5	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	3,00	0,33	1,00	0,28
Messaging software	0,33	1,00	0,33	0,48	0,14

Other software	3,00	3,00	1,00	2,08	0,58
Sum	4,33	7,00	1,67	3,56	1,00
Group6	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	1,00	0,33	0,69	0,20
Messaging software	1,00	1,00	0,33	0,69	0,20
Other software	3,00	3,00	1,00	2,08	0,60
Sum	5,00	5,00	1,67	3,47	1,00
Group_123456	Hardware	Messaging software	Other software	Geomean	Weights
Hardware	1,00	0,40	0,33	0,51	0,15
Messaging software	2,50	1,00	1,73	1,63	0,49
Other software	3,00	0,58	1,00	1,20	0,36
Sum	6,50	1,98	3,07	3,34	1,00

Appendix 5 – Layer 3 weights calculation

Group1	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1	3	3	2,08	0,58
Server side	0,33	1	3	1,00	0,28
Key handling&verif.	0,33	0,33	1	0,48	0,14
Sum	1,67	4,33	7,00	3,56	1,00
Group2	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1	1	9	2,08	0,47
Server side	1	1	9	2,08	0,47
Key handling&verif.	0,11	0,11	1	0,23	0,05
Sum	2,11	2,11	19,00	4,39	1,00
Group3	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1	9	9	4,33	0,81
Server side	0,11	1	0,33	0,33	0,06
Key handling&verif.	0,11	3	1	0,69	0,13
Sum	1,22	13,00	10,33	5,35	1,00
Group4	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1,00	9,00	3,00	3,00	0,69
Server side	0,11	1,00	0,33	0,33	0,08
Key handling&verif.	0,33	3,00	1,00	1,00	0,23
Sum	1,44	13,00	4,33	4,33	1,00
Group5	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1,00	3,00	3,00	2,08	0,58
Server side	0,33	1,00	3,00	1,00	0,28
Key handling&verif.	0,33	0,33	1,00	0,48	0,14
Sum	1,67	4,33	7,00	3,56	1,00

Group6	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1,00	0,33	9,00	1,44	0,46
Server side	3,00	1,00	0,33	1,00	0,32
Key handling&verif.	0,11	3,00	1,00	0,69	0,22
Sum	4,11	4,33	10,33	3,14	1,00
Group_123456	Registration	Server side	Key handling&verif.	Geomean	Weights
Registration	1,00	3,74	4,66	2,59	0,67
Server side	0,27	1,00	1,55	0,75	0,19
Key handling&verif.	0,21	0,64	1,00	0,52	0,13
Sum	1,48	5,38	7,21	3,85	1,00

Appendix 6 – Layer 4 tests ranking by experts

	Year tested	Group 1	Group2	Group3	Group4	Group5	Group6
Vulnerabilities							
Account hijack	2014	3,00	3,00	3,00	3,00	3,00	3,00
Access to SMS Inbox (for reading registration code)	2018	2,00	2,00	3,00	1,00	2,00	3,00
Trust other user with its (encryption) keys automatically without verification	2018	2,00	1,00	2,00	1,00	3,00	2,00
No notification about user (encryption) key changes on other side	2018	3,00	1,00	2,00	1,00	3,00	2,00
No blocking of messages when (encryption) keys of other user have changed	2018	2,00	1,00	2,00	1,00	2,00	1,00
Contact list leak via server	2014	1,00	2,00	3,00	3,00	3,00	3,00
Security controls							
Registration with phone number	2018	2,00	2,00	3,00	3,00	3,00	2,00
Registration with email	2018	1,00	1,00	2,00	2,00	2,00	2,00
Registration verification with SMS	2018	2,00	1,00	3,00	3,00	3,00	2,00
Registration verification with call	2018	2,00	1,00	1,00	3,00	3,00	1,00
Registration verification with e-mail	2018	1,00	2,00	2,00	2,00	2,00	1,00
Notification About E2E Encryption	2018	2,00	2,00	3,00	3,00	2,00	2,00
User (encryption) key verification: via QR-code	2018	2,00	2,00	3,00	2,00	3,00	2,00
User (encryption) key verification: via Phone call	2018	2,00	1,00	2,00	2,00	3,00	1,00

User (encryption) key Verification: out of band (e.g PGP)	2018	2,00	1,00	1,00	2,00	2,00	1,00
UI Display Verified check on User (encryption) key verification	2018	2,00	1,00	3,00	2,00	3,00	3,00

Appendix 7 – Calculations for Layer1 for different groups of experts

	Malicious app	Malicious content	Social engineering	Network attack	Physical loss
Group_1	0,27	0,11	0,27	0,07	0,27
Group_2	0,05	0,12	0,23	0,03	0,56
Group_3	0,06	0,21	0,64	0,06	0,04
Group_4	0,10	0,20	0,05	0,05	0,59
Group_5	0,11	0,26	0,17	0,07	0,40
Group_6	0,33	0,17	0,41	0,03	0,07
Group_123456	0,15	0,22	0,29	0,06	0,27
Group_24	0,07	0,16	0,12	0,04	0,60
Group_12	0,13	0,13	0,27	0,05	0,42
Group_13	0,14	0,18	0,48	0,07	0,12
Group_14	0,19	0,17	0,13	0,07	0,45
Group_15	0,18	0,18	0,22	0,07	0,35
Group_16	0,31	0,14	0,35	0,05	0,14
Group_23	0,07	0,20	0,49	0,05	0,18
Group_25	0,08	0,18	0,20	0,05	0,49
Group_26	0,16	0,18	0,38	0,04	0,25
Group_34	0,11	0,31	0,28	0,08	0,22
Group_35	0,10	0,29	0,40	0,08	0,15
Group_36	0,15	0,20	0,55	0,04	0,05
Group_45	0,11	0,23	0,10	0,06	0,50
Group_46	0,24	0,24	0,19	0,05	0,27
Group_56	0,22	0,24	0,30	0,05	0,19
Group_123	0,11	0,18	0,43	0,06	0,22
Group_124	0,12	0,15	0,17	0,06	0,50
Group_125	0,12	0,16	0,23	0,06	0,42

Group_126	0,19	0,15	0,35	0,05	0,26
Group_134	0,16	0,23	0,28	0,08	0,25
Group_135	0,14	0,22	0,37	0,08	0,19
Group_136	0,19	0,18	0,47	0,06	0,10
Group_145	0,16	0,19	0,14	0,07	0,43
Group_146	0,26	0,19	0,22	0,06	0,27
Group_156	0,24	0,19	0,29	0,06	0,22
Group_234	0,09	0,24	0,28	0,06	0,32
Group_235	0,08	0,24	0,36	0,06	0,25
Group_236	0,12	0,20	0,49	0,05	0,14
Group_245	0,09	0,19	0,13	0,05	0,54
Group_246	0,15	0,21	0,22	0,05	0,37
Group_256	0,14	0,21	0,30	0,05	0,30
Group_345	0,11	0,30	0,24	0,08	0,27
Group_346	0,17	0,27	0,33	0,06	0,16
Group_356	0,15	0,25	0,42	0,06	0,12
Group_456	0,19	0,25	0,19	0,06	0,31
Group_1234	0,12	0,20	0,28	0,07	0,32
Group_1235	0,12	0,20	0,35	0,07	0,27
Group_1236	0,15	0,18	0,44	0,05	0,17
Group_1245	0,12	0,18	0,17	0,06	0,49
Group_1246	0,18	0,18	0,24	0,05	0,35
Group_1256	0,17	0,18	0,30	0,05	0,30
Group_1345	0,15	0,24	0,25	0,08	0,28
Group_1346	0,20	0,22	0,33	0,07	0,19
Group_1356	0,18	0,21	0,39	0,06	0,15
Group_1456	0,21	0,21	0,21	0,06	0,31
Group_2345	0,10	0,25	0,25	0,07	0,34
Group_2346	0,14	0,24	0,33	0,06	0,24
Group_2356	0,13	0,23	0,40	0,05	0,19
Group_2456	0,14	0,22	0,21	0,05	0,38
Group_3456	0,16	0,28	0,29	0,07	0,21
Group_12345	0,12	0,22	0,26	0,07	0,34

Group_12346	0,16	0,21	0,32	0,06	0,25
Group_12356	0,15	0,20	0,38	0,06	0,21
Group_12456	0,16	0,20	0,22	0,06	0,36
Group_13456	0,18	0,23	0,29	0,07	0,22
Group_23456	0,14	0,26	0,31	0,06	0,28
min	0,05	0,11	0,05	0,03	0,04
geomean	0,14	0,20	0,27	0,06	0,25
median	0,15	0,20	0,29	0,06	0,27
max	0,33	0,31	0,64	0,08	0,60