

Abstract

Nowadays, smartphones are the latest technology of mobile devices and they are used massively. They combine the functionality of many devices and present a variety of different capabilities. Their portability is another reason that they are preferred by users. During the years, many applications have been created in order to satisfy the needs of users and new technologies have been added in the platforms.

One emerging category of applications is mobile payments. There are different methods for mobile commerce and users have begun using their mobile devices for their purchases. A new promising technology for mobile commerce has been developed and it is called contactless payments. The protocol used for proximity transactions and communication is called Near Field Communication (NFC). NFC has not yet been implemented in all the mobile phones and smartphones, but many researchers have been interested in it. Smartphones in combination with NFC can create a new evolutionary application, the mobile wallet; a virtual wallet, which is designed to replace the wallet.

However, before this idea is feasible there are several issues that need consideration. Applications using NFC require storage for essential information and during payment transactions a part of the information is sent to a reader. Thus, many questions have been created considering how secure this new technology is. The aim of this project is to identify the possible risks and propose the security mechanisms that should be implemented in the protocol.

This project is an investigatory project (Type II). It is motivated by a real world issue and includes some research in order to produce an assessment about conducting contactless payments using a mobile phone/smartphone integrated with the NFC technology. The methodology that is used is product engineering, because we investigate a subject that requires possible solutions. The difference between the final thesis and the interim report is that the interim report presented smartphones and their threats in general and the final thesis focuses on a more specific subject.

This project presents a research on the relevant background and a risk assessment is conducted in order to identify the risks of using NFC for payments and communication. The most urgent risks are identified and security mechanisms are proposed based on the research that has already been done in the area.

- Research was conducted to gain more knowledge about Smartphones, Mobile Commerce, Contactless Payments and Near Field Communication (NFC).
- Presentation of the components that are required by NFC and presentation of possible scenarios when making a payment or establishing a communication.
- The possible risks and threats were identified.
- Quantitative Risk Assessment was used to evaluate the risks.
- Solutions and security mechanisms were proposed.

Acknowledgements

I would like to thank my supervisor, Dr. Theodore Tryfonas for his continuous guidance and support throughout my thesis. His advice and feedback have been proved invaluable.

I would also like to thank my family and my closest friends for the support and understanding they have shown during my studies.

Contents

Abstract	1
Acknowledgements	2
Contents.....	3
1. Introduction.....	5
1.1 Aims and Objectives.....	5
1.2 Structure	5
2. Background	6
2.1 Overview.....	6
2.2 Smartphones	6
2.2.1 Operating System and Security Mechanisms.....	8
2.3 Mobile Payments.....	14
2.4 Contactless Payments.....	16
2.5 Near Field Communication	17
2.6 Radio Frequency Identification.....	22
2.7 Wallet Applications	23
2.7.1 Osaifu-Keitai.....	23
2.7.2 Google Wallet.....	24
2.8 Security Concerns.....	25
2.8.1 Malicious Software.....	26
2.9 Consumer Perspective.....	27
3. Risk Assessment.....	29
3.1 Overview.....	29
3.2 Methodology.....	29
3.3 Quantitative Risk Analysis.....	31
3.3.1 Definition of context.....	31
3.3.2 Identify and Analyze the Risks.....	36

3.4 Classification of Risk.....	40
4. Results and Solutions	42
4.1 Overview.....	42
4.2 Security Objectives.....	43
4.3 Encryption Schemes.....	43
4.4 Security model.....	46
5. Discussion.....	48
6. Future Work.....	50
6.1 Risk Assessment on Smartphones.....	50
6.2 Creation of a more robust protocol.....	50
References	51

1. Introduction

This chapter presents the aims and objectives of this project and then explains the structure of the project and how each chapter is organized.

1.1 Aims and Objectives

The aim of this project is to assess the security of mobile phones and smartphones. The project focuses on one specific field; the Near Field Communication technology when integrated into a mobile phone or smartphone. The technology is added in mobile phones / smartphones for communication and for performing payments. However, because it is a novel technology, it not yet widely used and mobile operating systems have not started using it. The project examines how secure this technology is.

The project has two different objectives. The first objective is to present the background information in order to introduce the concepts that are used in the project. The second objective is to conduct a risk assessment to specify the levels of protection the NFC protocol integrates. The risk assessment has different stages. First, we define the context and components that interact with the protocol when performing payment or when they want to communicate with another user. The NFC protocol can be used in a variety of possible activities. Then, the proposed scenarios should be examined in order to investigate the existence of possible risks. The risks can be classified, specifying which are the most urgent. Finally, the last stage is to propose solutions for the found risks in order to reduce them.

1.2 Structure

The project is organized in 6 different chapters. The second chapter presents some background information. The smartphone and the most famous operating systems of smartphones are presented. Then, the mobile payments are explained and we focus on the contactless payments and on the capabilities of NFC. The chapter ends specifying some security concerns. The third chapter refers to the risk assessment. The methodology is explained and we present some scenarios of enabled mobile phones with NFC when performing payments. The scenarios are examined and the risks are presented based on possible threats. The risks are evaluated and the most urgent risks can be found. In chapter four, solutions are suggested based on previous research, it is checked if the solutions can be applicable and a more general security model is presented. Chapter 5 evaluates the work of this project and chapter 6 proposes future work.

2. Background

2.1 Overview

In this chapter, we present information in order to introduce the concepts that are going to be examined in the next chapters. We begin by explaining what smartphones are, their features and the operating systems that were implemented for smartphones with their security mechanisms. We proceed with introducing what mobile payments are and we emphasize on contactless payments and Near Field Communication. The technology is presented and RFID technology. Finally, security concerns are presented.

2.2 Smartphones

Mobile phones are the most massively used mobile devices (Satyanarayanan, 2005). Researchers and designers are always searching for new functionalities to include in mobile phones in order to make them more useful in everyday life (Satyanarayanan, 2005). Satyanarayanan (2005) poses the question about whether a mobile device should be characterized as a Swiss army knife or as a wallet. This characterization aims to emphasize if the added functionality to a mobile phone can be used to provide personalized services to a user or not (Satyanarayanan, 2005). Through the years, mobile phones have evolved into programmable and networked mobile devices (Töyssy and Helenius, 2006) and thus, the need to carry a number of different devices is reduced (Ortiz, 2006). This constant evolvement of mobile phones has led to the introduction of smartphones.

Smartphones are the newest technology of mobile phones and are already used by a great proportion of people. They have appeared a few years ago, but they have known a rapid expansion, mainly because their primary goal is to be used as communication tools (Lessard and Kessler, 2010). When they appeared, they had a low percentage in the mobile market, but as it was expected this situation was altered (Chang et al., 2008). It was announced that in the U.S.A by the end of 2009, 46.3% of mobile phones were smartphones (Lessard and Kessler, 2010).

On their first appearance, they were using 2G (second generation) technology but they have evolved to the 3G (third generation) technology (Chang et al., 2008). Smartphones seem to be able to combine much functionality of different devices in just one. More specifically, there is a convergence between the features of a regular mobile phone and the features of a personal digital assistant (PDA) (Töyssy and Helenius, 2006). A smartphone has also operations of other devices such as an audio player, a digital camera, a GPS receiver (Schmidt and Albayrak, 2008). As a result, this technology can attract different sets of users (Barton et al., 2006).

Smartphones have some characteristics of the latest technology. They have fast CPUs, large amounts of RAM, high-speed data connection, Bluetooth and Infrared for small range connections and wireless LAN (Local Area Network) (Schmidt and Albayrak, 2008). The different types of connectivity allow users to browse the web, to read and send emails, to send instant messages and to play online multi-user games. (Schmidt and Albayrak, 2008). They also have some other capabilities using different types of sensors. An example of sensing is positioning and many location-based applications have been implemented (Raento et al., 2009).

The most important feature of smartphones is the wide range of applications that has been created in order to satisfy the needs of a user (Varshney, 2002). There are 2 different kinds of applications; the applications that are needed for the functionality of the device and the applications that provide communication, information and entertainment (Barrera and Van Oorschot, 2011). The applications developed for the second category are mainly third-party applications. Many platforms encourage the development of third-party applications by providing the application programming interfaces (APIs), emulators and tools (Barrera and Van Oorschot, 2011). Third- party applications can be installed on a platform easily based on the policy of the platform.

Many researchers have proposed different features that a user should expect to find in a smartphone. A smartphone platform is considered to be successful when it provides ease of use, its appearance is appealing and it is not heavy (Chang et al., 2008). Chang et al. (2008) recommend some features that should be integrated in a smartphone; eleven must-have features and eight desirable features. These features are described below.

Must-have features:

1. “Multi-tasking operating system” (Chang et al., 2008: 741): The operating system of a smartphone should be able to execute simultaneously more than one task in order to correspond to the many applications that exist on it.
2. Powerful Processor: The processor that is embodied in a smartphone should offer 3 different functions; communication function, signal processing, device and data handling.
3. QWERTY keyboard for writing functions
4. Large displays with high screen resolution
5. High speed internet access: Internet access is needed for web browsing, sending and receiving emails and audio-video streaming.
6. “Business Productivity Tool” (Chang et al., 2008: 741): Smartphones should have the ability to support business actions and offer the appropriate software.
7. E-mail, SMS, MMS, IM services
8. Personal Information Management: A user should to be able to store personal information on the device such as phone numbers and appointments.
9. Host synchronization: Smartphones should have the ability to synchronize with other devices, either a computer or another smartphone in order to share data between them.
10. Voice communication and voice-mail: The main function of a smartphone is the ability to conduct phone calls.
11. WiFi and Bluetooth: Wireless technologies for connection to the Internet and communication with other devices

Desirable features:

1. Gaming: Users are interested in playing games while traveling or waiting for an appointment, because it is a relaxing activity. This feature eliminates the need of an extra device.
2. Camera: Users have engaged the addition of cameras in mobile phones and they have shown that it is a useful feature. Thus, it is expected that smartphones include this feature as well.
3. File management and manipulation of the files that are stored on the device
4. Video/audio streaming

5. Music player and mobile TV: This feature is used for the entertainment of users and it can also replace mobile devices such as MP3 players.
6. GPS and navigation: This feature extends the usage of a smartphone and it can be helpful for people.
7. Open standard Input/output communication and storage expansion: The architecture design of smartphones enables users to add more memory in the device. The extra slot of memory is able to communicate with the device and the user can access the data stored in it.
8. Radio Frequency Identification (RFID) and biometric features: This feature is desirable in order to enhance the security of the mobile device. Biometric features (fingerprints or voice recognition) can be used for authentication. Moreover, the ability to read RFID tags expands the functionality of the device.

In general, a smartphone has the properties of a mobile phone but also has many properties of a computer (Töyssy and Helenius, 2006). However, it is difficult to make a precise distinction between smartphones and computer, because they exchange some of their features (Töyssy and Helenius, 2006). On the other hand, smartphones cannot reach the capabilities of a personal computer on certain domains because of their complexity (Barton et al., 2006). Many researchers have expressed the opinion that smartphones have evolved quickly from their first appearance and are more powerful than desktop computers where 10 years ago (Barrera and Van Oorschot, 2011).

Smartphones are preferred by the majority of people. The main reason is their small size and the ability to carry them everywhere. Thus, people use smartphones for their everyday activities and store great amounts of personal data (Barrera and Van Oorschot, 2011). They access the internet, they access their bank accounts, they save personal information, such as passwords, appointments, things they want to remember. A smartphone can describe the character of its owner.

Although, smartphones present a new kind of technology and are part of introducing ubiquitous computing in our lives, they pose many challenges because of their nature. One of them is security (Barton et al., 2006). Users should be reassured that their personal information will not be accessed by third parties and their privacy will be preserved (Barton et al., 2006).

2.2.1 Operating Systems and Security Mechanisms

During the years many operating systems for smartphones have appeared. However, there is not a standard design for a unified platform in smartphones (Chang et al, 2008). Some operating systems were designed for Personal Digital Assistants (PDAs) and others for exclusive use in smartphones. Each operating system is not designed for a particular brand of smartphones. A handheld maker company can use many different operating systems to different models of smartphones. However, Blackberry and iPhone design and use their own operating systems.

2.2.1.1 Symbian OS

The Symbian Operating System (OS) was the dominant operating system of mobile devices and it was the first operating system that was created exclusively for smartphones (Vaughan-Nichols, 2003). First, it was known as EPOC and was developed for Psion Series 5 PDA

(James, 2004). In 1996, the company was split and in 1998, Symbian Ltd introduced the Symbian OS to the public. The company is constituted by different handset companies, such as Ericsson, Motorola, Nokia, Panasonic, Samsung Electronics, Psion, Siemens and Sony Ericsson.

According to James (2004), the devices with Symbian OS were using ARM and StrongARM processors, something that continues until today. Flash memory is used for storing programs, while the operating system is stored in flash ROM. Smartphones that implement Symbian can store a large amount of data and can serve multiple threads simultaneously (Töyssy and Helenius, 2006). Symbian also offers Bluetooth connectivity and uses some other open standards like Java and SyncML. Furthermore, Symbian OS offers features that are expected from a smartphone. Some of the features are video - camera, audio, instant messaging, organizer. (Vaughan-Nichols, 2003)

The design of Symbian OS is focused on good functionality and not on compatibility with other platforms. As a result, this operating system focuses on security. Symbian-specific libraries and frameworks were developed in order to provide device security and avoid buffer overflow attacks. A cleanup mechanism that manages resources is responsible to make sure that denial of service will not appear (James, 2004).

Security at the application layer is managed by assuring that each application is a different process and does not have access to the memory stack of another process neither can access the memory of the operating system. The security of Symbian OS is based on 3 different ways; capabilities, installation file signing and data caging. Capabilities define access to APIs (Application Programming Interface). Installation file signing refers to signed applications. Each application, in order to be considered valid and to be able to be installed on Symbian OS must be signed. During the signing process, certificates are produced that define one of the three levels of limitation where on the highest level is full device and network access. These are all contained in installation packages, which are referred to as SIS(Symbian OS Installation System) files. Data caging is responsible for permitting access to the file system. Based on the SIS files and certificates each application has certain privileges. (Schmidt and Albayrak, 2008).

Unfortunately, the security mechanisms that Symbian OS implements are not sufficient against attacks. The procedure for signing applications is expensive, so the application developers do not prefer it. However, a user is informed when they are trying to install an unregistered application in order to prevent the installation of a malicious package (James, 2004). The applications that offer services to users can be signed by their creators, but if the applications require to modify the settings of the system files then a signing process from Symbian is required (Barrera and Van Oorschot, 2011). Another drawback of Symbian OS is the lack of an encryption algorithm for the user data. This means that an attacker can have access to essential information (James, 2004).

2.2.1.2 Palm OS

The Palm OS was initially developed for PDAs and was released in 1998 by PalmSource. The first version of Palm OS was designed for the first PDA, Palm Pilot. Schmidt and Albayrak (2008) and Vaughan-Nichols (2003) mention that after several different versions of Palm OS, there have been made some adjustments in the operating system with the addition of some APIs, in order to be used in smartphones. Specifically, version 5 and 6 were able to

support the high demands of a smartphone. Consequently, the Palm OS is able to execute multiple tasks such as time management, audio playback and using Wireless Connectivity, web browsing, email and instant messaging. It has also the ability to support the features of a mobile phone (Vaughan-Nichols, 2003).

The early versions of Palm OS did not have any specific security features. However, they used the application signing and only applications with privileges could be executed (Schmidt and Albayrak, 2008). The lack of security features was because Palm OS had not been a target from attackers (Töyssy and Helenius, 2006). Later versions of Palm OS included more security features. Palm OS was empowered with 128-bit secure sockets layer encryption technology and with virtual private networking software (Vaughan-Nichols, 2003).

2.2.1.3 Windows Phone 7

Windows Phone 7 is the current operating system of the company Microsoft and is the successor of Windows Mobile. Microsoft has presented different operating systems over the years. The first operating system of Microsoft that could be used on mobile phones was the Microsoft Pocket PC Phone Edition (Töyssy and Helenius, 2006). Other operating systems that have been created before the appearance of Windows Phone 7 are Microsoft Smartphone 2002 and Windows Mobile with different versions such as Windows Mobile 2003, Windows Mobile 5 etc. The previous versions of Windows Phone 7, were not only targeting the mobile phone market, but could also be used in PDAs. The company was most interested in the needs of enterprises, but with Windows Phone 7, Microsoft focuses on consumers.

During the years that Symbian OS was the dominant operating system among smartphones, Microsoft's Smartphone 2002 was also used by a large proportion of users (Vaughan-Nichols, 2003). Smartphone 2002 offered a wide range of features except telephone functionality, but it did not offer touch-screen capabilities in order for users to use only the one hand (Vaughan-Nichols, 2003). On the other hand, Windows Mobile offered more features and included some security measures that focus on security roles, security policies and application signing (Schmidt and Albayrak, 2008). Security roles specify the rights of a user or a group of users, while security policies give permission for the execution of certain actions. Finally, the application signing is the procedure of identifying that an application does not carry any malware, as it was described to previous sections (Schmidt and Albayrak, 2008).

Mobile Phone 7 supports the above security measures. However, due to the large number of applications, the procedure of application signing is time-consuming and difficult. Therefore, many applications are not checked whether they contain malicious code or not or whether they access data or resources that are not entitled. In case the smartphone is lost, the operating system supports an application that the user can use in order to track the location of the smartphone, erase their data or lock the phone (Microsoft, 2011). Furthermore, there are not any encryption mechanisms on the device (Walker, 2010).

2.2.1.4 Blackberry

Blackberry is mostly designed as a business tool and is owned by the company Research In Motion (RIM) (Schmidt and Albayrak, 2008). Blackberry devices use their own operating

system in order to support the needs of their customers, who belong mostly in the business world.

Security is a crucial matter for Blackberry devices and is considered during the design of the smartphone (Walker, 2010). Other smartphones do not follow the same policy and add security levels after (Lambert, 2005). In order to gain the trust of their customers and ensure the security of data, RIM uses different features of security that are implemented in the smartphone and in the Blackberry Enterprise Server (BES) (Lambert, 2005).

To begin with, Blackberry implements encryption algorithms; Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) in order to protect data that travels between the device and the BES (Blackberry 2011). Each device is assigned with unique encryption keys that are created in a secure environment and are sent to the device. The keys are stored in the device and in the user's enterprise account. (Blackberry, 2011). With the first generation of keys the devices are also activated. (Lambert, 2005).

In order for the BES to send information to the appropriate Blackberry device the encryption key and the Personal Identification Number (PIN) are used to identify the device (Lambert, 2005). The BES sends data to a user which is encrypted with their private key from their private account. The encrypted data are decrypted with the private key stored in the device (Blackberry, 2011).

In contrast to other smartphones, Blackberry disables direct device-to-device communications, in order to ensure that all communications pass from the BES gateway (Lambert, 2005). However, no decryption takes place between the BES gateway and the device to eliminate the possibility of leakage of information to eavesdroppers (Blackberry, 2011). In addition, communications that can be decrypted with a valid key can take place in public networks. To increase the security of the device, outbound-initiated connections must be authenticated through the port 3101 of the firewall. Inbound traffic must be from the device or from the email server, so that they are authorized (Blackberry, 2011).

The contents of a Blackberry device are secured with different ways. The user can interact with the device by using a password to authenticate their selves. There is a certain number of attempts that the user can enter a password and if it is incorrect, the memory of the device is deleted. Data that are stored in the device are also secure with the use of encryption. The AES encryption algorithm is used to protect saved passwords. Thus, applications cannot have access to essential information. (Blackberry, 2011)

Furthermore, each application that is designed with the BlackBerry® Java™ Development Environment (JDE) should be signed by the RIM, so that it can be installed and have access to data stored in the device. Signed applications can be found in AppWorld, an application designed to inform users about the available applications (Barrera and Van Oorschot, 2011). On the other hand, distribution of non-signed applications is not restricted and they can be found on the developers' sites (Barrera and Van Oorschot, 2011). Third party applications can be installed on a Blackberry smartphone, however they are sandboxed and the execution is restricted only to their directory (Barrera and Van Oorschot, 2011). Each application should use a trusted certificate authority (CA) or a generated certificate, which should be made using the Public Key Infrastructure (X.509) standard (Blackberry, 2011).

Finally, system administrators regularly check the security of the device based on the enterprise policy so that the device fills the security policy (Lambert, 2005). Security settings are sent via BES to ensure that all the Blackberry devices are adjusted to the most recent

security policy. Therefore, the protection of a Blackberry device is not left entirely to the user (Lambert, 2005).

If the Blackberry device is lost, the user has the ability to erase remotely the data that are stored in the device. The data are not lost and the user can retrieve them through another device. The device can be set to erase the data automatically, if it is not connected to the network for a pre-defined period of time (Walker, 2010).

2.2.1.5 iOS

The iOS is the operating system designed for the Apple iPhone and the version that is currently used is 4. Version 5 is expected later in 2011. It was presented to the public with the name iPhoneOS and it was renamed to iOS in July 2010 (Barrera and Van Oorschot, 2011). When the iPhone was first appeared in June 2007 until today, it has known a huge success. Due to its appearance and style, and the big variety of applications it offers, iPhone has a large percentage in sales (Pandya, 2008). It is preferred by companies, because of its interface and the ability to execute simultaneously many applications. However, companies are adviced to increase the security of the smartphone with the addition of extra authentication measures (Walker, 2010).

The iOS is basically a modified version of the Mac OS X operating system that was adapted in order to satisfy the needs of a smartphone. The iOS runs on ARM processors, which are more suitable for smartphones due to low consumption power (Miller et al, 2007). Some of the applications of the iOS are applications of Mac OS X which are adjusted, such as MobileSafari and MobileMail (Miller et al, 2007). Moreover, iOS presents several layers of abstraction in order to support a variety of applications (Barrera and Van Oorschot, 2011).

The iOS implements different security features. Firstly, it offers hardware encryption and encrypts network communications. The 4-digit password required can be altered to satisfy the security needs of each user (Walker, 2010). In order to protect privacy issues, applications that need the location of the user, must have the consent of the user (Apple Inc, 2011). According to Miller et al (2007), write access is restricted in a specific area in the file system called sandbox and installation of third-party applications is restricted. This is done in order to eliminate “the attack surface of device” (Miller et al, 2007: 3) or “the device’s exposure to vulnerabilities” (Miller et al, 2007: 3). Third-party applications are only able to read and write data in their own directory and they require a signing process in order to be distributed to the public (Barrera and Van Oorschot, 2011). In addition, several features were removed from WebSafari and only certain file types can be downloaded to the device (Miller et al, 2007).

The iOS has the ability of erasing the stored data when the device is lost or stolen. This is achieved remotely, but it requires the existence of the original SIM and it must be connected to a network (Walker, 2010). The memory can also be erased after a number of unsuccessful attempts to unlock the phone (Apple Inc, 2011).

The iOS is concerned to have a lot of vulnerabilities. Every key stroke is saved in a file with a capture of the homepage when the user unlocks the phone. Thus, an attacker may gain access to this file (Walker, 2010). Furthermore, an attacker can gain control of the device, because processes that send and receive data over the network use the user’s id (Miller et al, 2007).

Address Space Layout Randomization (ASLR) and non-executable heap are also not used and these flaws can be exploited by attackers (Pandya, 2008).

2.2.1.6 Android

The Android operating system is owned by Google and has been one of the most significant operating systems over the past few years. “Android is an application execution environment for mobile devices that includes an operating system, application framework and core applications” (Shabtai et al, 2009: 5).

The Android operating system architecture has four different layers; Linux Kernel, Android Runtime Libraries, Application framework and Application layer (Shabtai et al, 2010). The Android Linux Kernel is based on Linux version 2.6, which implements features such as security, memory management, process management, network stack, and driver model (Android Developers, 2011). The Application layer consists of the applications that are installed on the device (Shabtai et al, 2010).

Mechanism	Description	Security Issue
Linux mechanisms		
POSIX users	Each application is associated with a different user ID (or UID).	Prevents one application from disturbing another
File access	The application's directory is only available to the application.	Prevents one application from accessing another's files
Environmental features		
Memory management unit (MMU)	Each process is running in its own address space.	Prevents privilege escalation, information disclosure, and denial of service
Type safety	Type safety enforces variable content to adhere to a specific format, both in compiling time and runtime.	Prevents buffer overflows and stack smashing
Mobile carrier security features	Smart phones use SIM cards to authenticate and authorize user identity.	Prevents phone call theft
Android-specific mechanisms		
Application permissions	Each application declares which permission it requires at install time.	Limits application abilities to perform malicious behavior
Component encapsulation	Each component in an application (such as an activity or service) has a visibility level that regulates access to it from other applications (for example, binding to a service).	Prevents one application from disturbing another, or accessing private components or APIs
Signing applications	The developer signs application .apk files, and the package manager verifies them.	Matches and verifies that two applications are from the same source
Dalvik virtual machine	Each application runs in its own virtual machine.	Prevents buffer overflows, remote code execution, and stack smashing

Table 2.1: Security Mechanisms incorporated in Android (Shabtai, 2010). This picture is copied from (Shabtai, 2010)

Android presents several security measures which are built in the operating system. There are 3 different categories of mechanisms. First, it adopts 2 security mechanisms from the Linux operating system; the Portable Operating System Interface (POSIX) users and file access. It presents further mechanisms which are called environmental features and are distinguished in

Memory Management Unit, Type Safety and Mobile Carrier security features. It also implements some security mechanisms that are designed specifically for Android which are Application Permissions, Component encapsulation and signing applications (Shabtai et al, 2010). The table 1 above presents the security mechanisms that can be found in Android, describes them and cites the protection they offer.

Shabtai et al. (2009) presents a security analysis of Android examining many elements. Among the elements that were examined are application-level permissions, installing applications, web-browser, sql injection, connectivity and communication and many others. The analysis had satisfactory results. Android provided adequate level of protection when the device is in normal state. The components of the operating system may be modified if there is a vulnerability found in the kernel or in one of the libraries it uses. However, it is expected that any vulnerabilities will be eliminated at some point in the future. Furthermore, Android can be attacked easily with local host-based exploitations attempts and an attacker can send malware using a Web browser. Attacks through Bluetooth and using sql injections are difficult to occurred, since there are protection mechanisms.

Barrera and Van Oorschot (2011) state that the applications, which are designed for Android are stored in “Android Market”. Applications can be downloaded from there or from the site of the developer of the application (Barrera and Van Oorschot, 2011). Google does not involve in the upload process of new applications (Barrera and Van Oorschot, 2011) thus, the application permissions may be altered by a malicious program and the user may not notice it (Shabtai et al, 2009), (Shabtai et al, 2010).

2.3 Mobile Payments

Mobile Payments are an emerging field which was designed in order to provide a wide range of services. Heikkinen (2009) states that mobile payments will be the “most efficient means of payment” (Heikkinen, 2009: 3). Mobile payments are defined by Pernet-Lubrano (2010) “as the act of paying for goods or services with a mobile device”. Mobile payments are different from other kinds of payments that can be made by using a computer, because they can only be done by a mobile device (Heikkinen, 2009).

When referring to a mobile device, it does not only reflect to mobile phones, but it can refer to anything that it can be carried by a person (Heikkinen, 2009). However, our main concern when mentioning mobile payments would be about mobile phones. Moreover, other technologies can be integrated in a mobile device in order to make a mobile payment feasible. Heikkinen (2009) indicates that a mobile device could be a “carrier of various mobile instruments” (Heikkinen, 2009: 6) and also proposes a different definition of mobile payments. “Mobile payments mean the use of payment services, other than Internet banking, be using a mobile handset, its keyboard and display” (Heikkinen, 2009: 10).

More and more schemes are designed in order to make payments simpler and quicker and can be distinguished to different categories. One distinction is presented by Pernet-Lubrano (2010) and it is on the location of the user and the location of the merchant.

The categories cited by Pernet-Lubrano (2010) are the following:

1. Remote payment over the mobile: It refers to purchases of digital or physical goods and services that can be made from a distance. Payments can be charged on the user’s bill directly or after sending an SMS message. Another way of remotely paying is by

entering a bank account number to a website. In order to protect the details of a bank account, a user can also register to a merchant's website or have an electronic wallet (PayPal, Amazon Checkout).

2. Proximity payment using the mobile terminal: Proximity payment basically refers to contactless payments that can take place when the mobile phone is waved or tapped on a receiving terminal, at a specified distance. Payments can be done for small amounts of money and for larger amounts as well with the requirement of entering a password. The information concerning the transaction is held within a secure component. In a different section, we explore the contactless payment in more depth. We analyze how feasible is the adaptation of this technology in mobile phones, examples of implementation and how secure it is.
3. Receiving money over the mobile: The mobile phone can read payment cards with the use of an external device which can be attached to it. An example of this technology is a product that Apple has developed which is called "Square" and can read the magnetic stripe of a card.

Heikkinen (2009) also presents a similar classification of mobile payments and also suggest that the time of payment should be considered. The applications could be prepaid, real-time or post-paid.

Varshney (2002) distinguishes mobile commerce in payments that can be charged on the bill of a user or on credit account and to payments that can be made using "mobile money". "Mobile money" can be stored in mobile phone using an application which reflects an electronic wallet. "Mobile money" can be granted from another user over a local area network or via a prepaid or postpaid service (Varshney, 2002). "Mobile money" is an early definition that can describe the today wallet applications that are implemented in smartphones.

Varshney (2002) presents the mobile scenarios with the following figure.

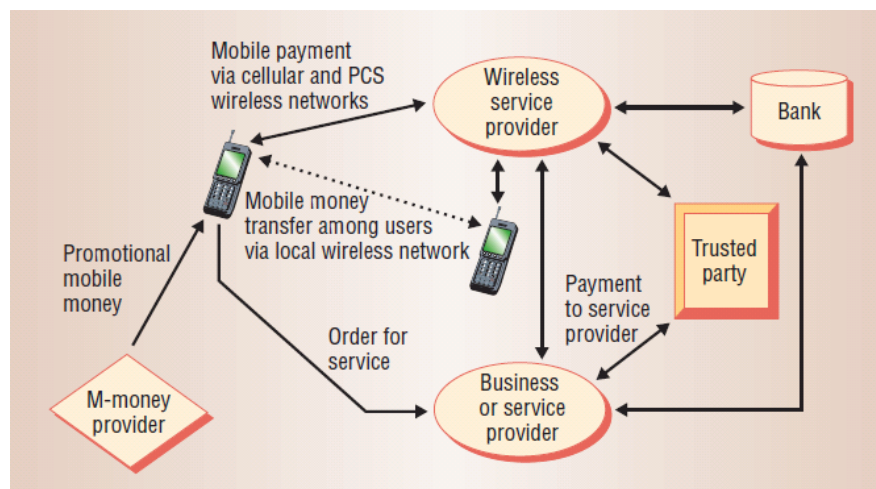


Figure 2.1. Mobile Scenarios. This figure is copied from (Varshney, 2002).

Chang et al. (2008) specifies the need of a standard that can be used for mobile commerce. This need is also highlighted by Linck et al. (2006) who state that the standardization and the

existence of specific procedures will facilitate the adaptation of users to this new technology and the users will find it easier to learn how to use it and trust it.

2.4 Contactless Payments

Contactless payments as presented in the previous sector belong to the category of proximity transactions of mobile commerce. They are a new trend in mobile phones and smartphones, but the introduction of contactless payments was made by the card industry. Bradford (2005) states that the card industry has always been searching for new ways to increase the use of card payments. Contactless payments can be defined as “traditional” payments that utilize microchips and radio frequency identification or near field communication to effect transactions without physical contact between the payment device and the point of sale (POS) terminal” (Bradford, 2005: 1). A POS is also referred as a reader.

This technology is added in cards and purchases can be made from a small distance. The action indicates waving or tapping the card over a POS terminal and the spent amount is subtracted from the account of the user. The technology used for the secure process of payments is the Visa technology used for the Chip and PIN transactions (Barclays, 2011). They are considered to be faster than magnetic-stripe and cash payments (Bradford, 2005) and this is mainly because in most cases the need for entering a Personal Identification Number (PIN) or waiting for change is eliminated (Olsen, 2008). Olsen (2008) also reports other advantages that contactless payments can offer. Using contactless card for payments can also reduce the possibility of error when manually handling money and the risk of theft.

The use of contactless payments focused mainly on micropayments. Micropayments refer on small purchases which are under the amount of £10 or £15. A significant number of people tend to use their payment cards for micropayments which sometimes is not possible because a limitation of a minimum amount spent may exist. Contactless payments aim to provide speed and convenience in places where this is essential (Olsen, 2008) and the user does have to enter a PIN (Personal Identification Number) to authorize the transaction (Pasquet, 2008). However, in order to provide a level of protection the user is asked to enter their Personal Identification Number after a certain number of transactions (Barclays, 2011). The user may also be asked to enter his PIN code when their purchase is referred to as macro payment (Pasquet, 2008). The user will have to wave their mobile phone over the POS, enter their PIN and then wave their mobile phone for a second time (Pasquet, 2008). Macro payments require authentication because the transactions regard a larger amount of money.

The following figures represent the signs of contactless payments. The first sign indicates that a card is able to conduct contactless payments and the second one can be found on a POS terminal in retail stores that accept this kind of payment.



Figure 2.2. Sign on cards. This picture is copied from (Barclays, 2011).



Figure 2.3. Sign on the POS terminal. This picture is copied from (Barclays, 2011).

Through the years, there have been several efforts for the deployment of contactless payments by the card industry. In 2003, American Express and MasterCard presented ExpressPay and PayPass respectively and in 2004, Visa launched Visa Wave (Bradford, 2005). Initially, most bank companies were reluctant to deploy this new technology (Bradford, 2005). After some time, different banks such as HSBC, Citibank, JPMorgan Chase and Key Bank have used the above products to introduce contactless technology to the public and different retailers have begun accepting contactless payments (Bradford, 2005). Furthermore, banks have thought of extending the use of this technology and adding it to mobile devices (Bradford, 2005).

In UK, the first attempt for contactless cards was made by Royal Bank of Scotland (RBS) in 2006 in association with MasterCard (Olsen, 2008). Barclays followed this initiation and in 2007, Barclays launched the OnePulse card which contained 3 different functionalities; Visa Wave and Pay for micropayments, the standard Chip and PIN card for macro payments and the Oyster fare application (Olsen, 2008). The efforts made by major banks added a new perspective into the future of contactless technology. More and more retailers in UK began trials on contactless payments, although they were concerned that this change would be a financial burden (Olsen, 2008).

Another different approach for adapting contactless technology in everyday life is the use of prepaid cards. Prepaid cards can have the same characteristics as a prepaid SIM card (Orsen, 2008). This would mainly attract people who do not have bank accounts. People can top-up their card in the same way they do with a pay as you go SIM card and then use it as a credit card (Orsen, 2008). This option also provides some level of protection, because prepaid cards are not connected to a person's bank account.

Contactless technology was considered promising from its first appearance. Thoughts were made that the future of this technology was the integration of cards in the mobile phones with the development of the appropriate software (Orsen, 2008). As a result, the mobile phone would be responsible for conducting payments. Research also presented that different kinds of mobile devices, such as keys, watches and mobile phones could be used. These thoughts became a reality and different applications for the mobile phones that were using Near Field Communication protocol have been presented.

3.5 Near Field Communication

Near Field Communication (NFC) is a new protocol that was developed for contactless communication within a short-range. It is vastly used by the cell phone industry, because it merges wireless networks with the contactless card technology. It was developed in order to create a new generation of mobile phones presenting more capabilities than ever (Fischer, 2009). Consequently, a single device can present the maximum level of functionality and Near Field Technology can be defined as a first step into context aware smart environments and to ubiquitous computing (Chang et al., 2009).

Firstly, we present the characteristics of NFC. The NFC protocol was designed and developed by the companies Philips and Sony in 2002 in order to provide contactless communication (Ortiz, 2006) and the standards of the protocol can be found in ISO/IEC 18092 (ISO, 2004). In the same year the forum of NFC was created by the two companies and Nokia to provide information about the new technology (NFC Forum, 2011). The protocol uses the standards of contactless cards as they are described in ISO/IEC 14443

(Madlmayr et al., 2008b). NFC is an advancement of the Radio Frequency Identification (RFID) and both technologies have many similarities (Madlmayr et al., 2008b). RFID is going to be described in a different sector.

In addition, NFC supports contactless communication in a distance of less than 10 centimeters with the use of electromagnetic waves (Madlmayr et al., 2008b). Other sources present that the distance should be 4 centimeters or less (NFC Forum, 2011). The radio frequency used by NFC to produce waves is located at 13.56MHz (Ortiz, 2006). The communication capabilities of NFC can reach 424 kbps (ISO, 2004).

Based on the characteristics we presented above, the NFC protocol presents some limitations on the distance that the two communicating devices should have between them and on the transfer data rate. The NFC protocol can send data within a small range and can only transfer certain data types (Ortiz, 2006). The following figure presents the data rate and the distance that NFC transfers data in comparison with other wireless technologies that are integrated into a mobile phone. The figure shows that the NFC technology requires the minimum possible distance for two devices to communicate and its data rate is one of the smallest.

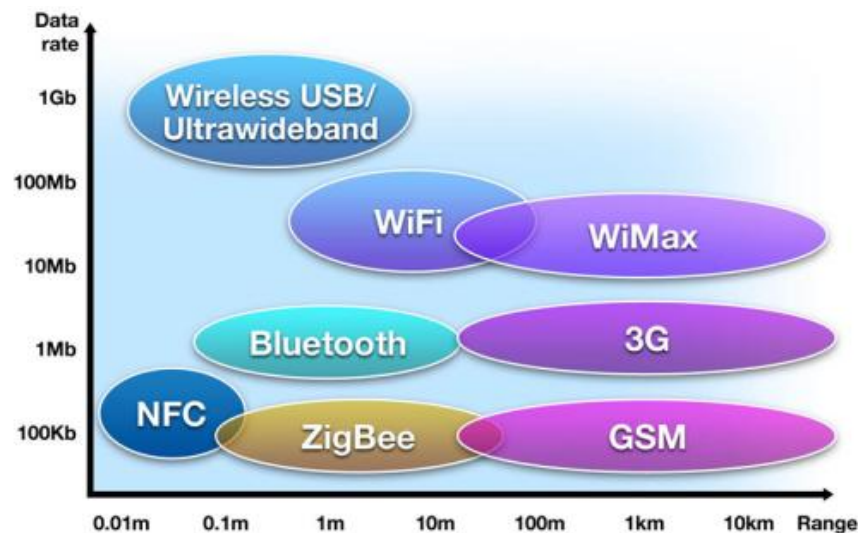


Figure 2.4. Comparison of different wireless technologies. This picture is copied from (NFC Forum, 2011)

A NFC device can be in active or passive mode (ISO, 2004) and all the devices can use both of them (Chang et al., 2009). The device is active if it generates the Radio Frequency field (RF) from a power supply or passive if it uses the power that an active device has generated (Haselsteiner and Breitfuß, 2006). Ortiz (2006) states an opinion in his article that the two modes provide a benefit that is not possible in any other contactless technology. The following table presents the three different cases of communication configuration between two devices.

Device A	Device B	Description
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF field is generated by Device B only

Table 2.2. Communication configuration (Haselsteiner and Breitfuß, 2006). This table is copied from (Haselsteiner and Breitfuß, 2006).

The two different modes presented above have the appropriate role when two devices with the NFC technology communicate. When the device is active, it can initiate the communication and also accept the data sent by other devices. When the device is passive, it must first receive data from an active device in order to be able to send data. An active device can be called an initiator and a target while a passive device can only be called a target (Haselsteiner and Breitfuß, 2006). The communication of NFC devices can be a one-to-many relationship. However, the initiator should specify from which device it expects an answer and the other devices should ignore the sent data (Haselsteiner and Breitfuß, 2006).

NFC can easily be integrated in any system. The most important component of a NFC system is the secure element. The secure element consists of the essential information that is needed for the communication and transactions (Francis et al., 2009). An antenna exists to send and receive data (Ortiz, 2006) and it should be large enough to provide a reliable communication between the tag and the device (Edwards, 2010). The existence of the NFC controller is also crucial. The NFC controller handles the function of the protocol, converts the analog signal to digital and vice versa and has access to the secure element (Madlmayr et al., 2008b). Additionally, the protocol of NFC is equipped to avoid collisions in the RF field (ISO, 2004). An RF-level detector is implemented in order to identify if another NFC device is transmitting (Ortiz, 2006). A card-mode detector exists to define the type of technology that is going to be used (Ortiz, 2006). The architecture of NFC when added to a mobile device will be examined in more detail in chapter 3.

Furthermore, NFC enabled devices have three different operating modes; peer-to-peer mode, reader/writer mode and tag emulation mode. These modes are described by Madlmayr et al. (2007) and by Madlmayr et al. (2008b):

- **Peer-to-peer Mode (Near Field Communication, NFC):** This mode refers to the communication that can be established between two devices that are using NFC. The devices have a two-way communication and can exchange data with a maximum speed of 424 kbps. Both devices can be in active mode, but there is still the need for an initiator and a target (Fischer, 2009).
- **Reader/Writer Mode (Proximity Coupling Device, PCD):** The device is able to initiate communication with a passive tag or smartcard for a certain operation (Fischer, 2009). The device is active and initiates the communication by generating a RF field and can read or modify the data of the passive tag.

- Tag Emulation Mode (Proximity Inductive Coupling Card, PICC): The device can change its mode to act as a smartcard, which is complied with the ISO 14443 standard in order to conduct payments or other similar actions that are included in the electronic wallet (Fischer, 2009). When the device is in this mode, an external reader cannot specify whether it is a NFC enabled device or a smartcard. This mode also benefits the industries, because there is no need to replace the existing technology that is used for contactless cards.

NFC was integrated into mobile phones, mainly smartphones in order to provide a wide range of contactless services (Francis et al, 2009). Ortiz (2006) quotes the opinion by Kay Irwin (inCode Consultancy) that in a few years time “NFC will be a standard feature in most cell phones”. Android has already adapted the NFC technology for communication purposes (Android Developers, 2011). It also uses NFC for the Google Wallet, an application that we will be described below.

Fischer (2009) characterizes a mobile phone with NFC as a magic wand, because depending on where the device points to, it can be interpreted to a specific function. The basic operation of NFC in smartphones is conducting contactless payments. However, smartphones can be used for the development of a variety of applications except payments. NFC tags can be used to provide interoperability between different applications. The NFC forum (2011) presents some of the areas where the NFC technology can be deployed. Examples of areas as stated in the NFC Forum (2011) are access control, consumer electronics, healthcare, information collection and exchange and transport. Among the different facilities, NFC can be used for communication; mobile devices can connect to each other (Francis et al, 2009). Furthermore, the NFC technology can be used for configuring other wireless technologies (Bluetooth, WiFi) by exchanging the appropriate settings (NFC Forum, 2011). Thus, this function eliminates the need for manual setup (Ortiz, 2006).

The applications that use contactless technology can be distinguished in four categories as stated by (Pasquet et al., 2008).

- Touch and Go: Consumer can wave or tap the device over a POS (Point of Sale) to conduct a payment without the need for authorization. This type of payments is called micropayments.
- Touch and Confirm: The user is asked to accept the transaction by entering a password.
- Touch and Connect: This category refers to connections between two devices in order to exchange data. This can also be done in order to transfer money from one device to another.
- Touch and Explore: The user has the ability of choosing one action between a list of functionalities.

The following figure presents the possible capabilities of a mobile phone with integrated NFC technology. The figure shows the areas where the technology is applicable, what activities and services it can offer and which industries can be involved.







Area	STATION AIRPORT	VEHICLE	OFFICE	STORE RESTAURANT	THEATER STADIUM	ANYWHERE
						
Usage of NFC Mobile Phone	Pass gate Get information from smart poster Get information from information kiosk Pay bus/taxi fare	Adjust seat position Open door Pay parking fee	Enter/exit office Exchange business cards Log in to PC; Print using copier machine	Pay by credit card Get loyalty point Get and use coupon Share information and coupon among users	Pass entrance Get event information	Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	Mass Transport Advertising	Public Transport	Security	Banking Retail Credit Card	Entertainment	Any

Figure 2.5. Possible use of mobile phones with NFC. This picture is copied from (NFC Forum, 2011).

These services can be managed by one application on the smartphone, the mobile or electronic wallet.

Mobile wallet is an application that represents an electronic version of a wallet (Shin, 2009). A mobile wallet includes all the information that is needed in order to conduct a mobile transaction. It also can store personal and essential information that can be found in a wallet such as credit card information, PIN codes, and details about online accounts (Shin, 2009). The personal data can be stored on the component which is responsible for conducting the contactless payment on an embedded chip which can be used for the storing of the personal information (Shin, 2009). The mobile wallet application emulates the functionality of a wallet and expands its functionality (Shin, 2009). The most challenging part of the electronic wallet is the combination of different payment cards and services that are available in the application (Fischer, 2009). The data stored in the phone should be distinguished based on the service they provide and they should be in different data cells. (Fischer, 2009). It is considered to be a revolutionary technology for the mobile commerce, because it is easy to use and quicker than other mobile commerce applications.

Although the mobile wallet application can offer many new benefits, it is not widely used yet. Shin (2009) outlines some of the reasons that mobile wallet and contactless are not widely used. The reasons given are also expressed by a variety of articles. Fischer (2009) states the need that the electronic wallet must implemented security to provide protection against electronic pickpockets or loss.

In addition to the electronic wallet, a variety of other applications were developed in order to ease the everyday life. As it is mentioned, in the above figure, information can be obtained

from a smart poster. A simple approach of this service is the addition of tags in advertising posters. When the user sees the advertisement, they can have access to more information through a website by simply waving the phone over the poster (Fischer, 2009). This approach can be used in different scenarios.

Other examples of applications using the NFC are the peer-to-peer transfer of business cards and a phone based reader/writer application that helps the elderly (Fischer, 2009). The first application is used for the exchange of business cards by taping two devices together while the use the peer-to-peer mode (Fischer, 2009). The second application can be used to replace the dial or the speed-dial when calling a person (Fisher, 2009). Tags that contain the phone number of people can be added on photos of them and when the user desires to call them, they can simply tap or wave to call them (Edwards, 2010).

Anokwa et al. (2007) address a problem that is visible in all the applications. The majority of NFC enabled applications is not designed based on a general interaction model. Thus, Anokwa et al. (2007) propose a user model so that when a mobile phone scans an item, the phone has all the properties and information about the scanned item. This procedure is called transformation. For example, the model presents all the available options that a user has when interacting with the poster based on its subject offering them all the information that the user may need.

Most of the NFC applications that have been implemented for mobile phones are not designed to control. Chang et al. (2009) present a more ambitious approach; an architecture model towards a NFC phone driven context-aware smart environment. A NFC enabled mobile phone can be used in order to control the home appliances using the Generic Control Record Type Definition (GCRTD). The user can personalize their NFC mobile phone with the settings they want for the control of home appliances.

2.6 Radio Frequency Identification (RFID)

Near Field Communication derives from Radio Frequency Identification (RFID). The protocol of NFC was created in order to enhance the functionality of RFID. Consequently, they present many similarities, but also they have some differences. RFID is used for identification, while the main use of NFC is two-way communication (Juels, 2005).

Radio Frequency Identification is defined as a technology whose main function is the unique identification of an object or a person (Juels, 2005). It is also known as an Electronic Product Code (EPC) tag (Juels, 2005). It is implemented with a very small microchip and an antenna. The microchip is used to transmit data wirelessly. The majority of the tags are passive and they do not have any source of power. However, when in the range of a reader, they gain power in order to transmit their information (Juels, 2005). The distance of the transmission depends on the frequency band that the reader uses (Juels, 2005).

RFID tags were introduced in the everyday life and they can provide many possibilities for the future by empowering the vision of ubiquitous computing. They can be integrated in home appliances and are used to provide access to buildings and to public transportation (Juels, 2005). They are also used for performing payments and they are known as contactless cards (Venkataramani and Gopalan, 2007).

Although, RFID tags are used widely there are security issues that cannot be ignored. RFID tags raise privacy issues. A person who uses an RFID tag sends a unique ID, which “betrays”

their location (Juel, 2005). There are also other issues, such as relay and cloning attacks (Juel, 2005). The security issues that were described were inherited to the NFC protocol as well and there are many concerns about the integration of the technology in mobile phones.

2.7 Wallet applications

Throughout the years different wallet applications made their appearance. All of them have a common target; the implementation of a convenient tool that offers security.

2.7.1 Osaifu-Keitai

NTT DoCoMo, the largest cell phone provider in Japan, has introduced one of the first mobile wallet, Osaifu-Keitai, in 2004 which serves a wallet within the phone (Pernet-Lubrano, 2010). Its implementation is based on the wireless smart card chip, FeliCa. FeliCa is a wireless smart card and was developed by Sony Corp. and Royal Philips Electronics in 1995 and is designed for proximity transactions. The two companies were the first to introduce the Near Field Communication protocol as it was mentioned above (Boyd, 2005).

DoCoMo's wallet phone uses the FeliCa smart card as a wireless prepaid cash card. Each user can register for the e-wallet service and load money in the card (Boyd, 2005). The top-up process can be made with two different ways, either inserting money in top-up machines or transferring money from a bank account using their phone, after they have inserted an identification number to authenticate themselves (Boyd, 2005). Furthermore, the user can be informed about the current balance and about previous transactions, because the information can be visible (Boyd, 2005). The wallet phone can be used to make different kinds of transactions, such as payments, identification and can also be used as a ticket or a boarding pass. For these transactions, it is necessary a FeliCa reader (Boyd, 2005).

The figure below summarizes the services the Osaifu-Keitai provides. The Osaifu-Keitai can replace a wallet, because all the information that can be found in a wallet is stored in the mobile device and it can also be used to conduct different activities.



Figure 2.6. Services available on Osaifu-Keitai. This picture is copied from (NTT DOCOMO Inc., 2011).

In order to provide certain levels of security the DoCoMo's wallet phones have adapted certain mechanisms (Boyd, 2005). The data of the application needed for the proximity transactions are stored in the files separated than the other files of the phone. During the communication between the smart card and the reader/writer, there is a mutual authentication which is based on an encryption scheme with random generated numbers (Boyd, 2005). Before any transaction, the user has the option of entering a personal identification number (PIN) in order to authenticate the transaction (Boyd, 2005). In the case that the mobile phone is lost, the user can lock it by informing the customer support of DoCoMo (Boyd, 2005).

DoCoMo's wallet phone has become an example for the design and deployment of other wallet phones (Shin, 2009). After its appearance other companies in Japan were interested in developing similar applications using the FeliCa smart card (Boyd, 2005).

2.7.2 Google Wallet



Figure 2.7. Sprint Nexus S 4G (Google, 2011)

In May 2011, Google released its wallet, the Google Wallet. The Google Wallet is an application that can be implemented on Sprint Nexus S 4G, but Google is ambitious and hopes that other phones will soon adapt this new technology (Google, 2011). With NFC integrated, a user can tap its phone to a POS (point of sale) to pay for buying goods (Google, 2011). Two different cards are supported which can be used in order to perform payments; Citi® MasterCard® credit cards and the Google Prepaid Card (Google, 2011). The Google Prepaid Card is a virtual card that can be topped up with any of the user's bank account and the user will not be charged with any fees (Google, 2011). The Google Prepaid Card was created and is supported by MasterCard® and Money Network® (Google, 2011). If a user has a Citi® MasterCard®, they can link their account with the card on the phone by entering their account information (Google, 2011). The details of the account are then stored in the secure element for future purchases (Google, 2011).

Google (2011) indicates that the security mechanisms that are implemented in Google Wallet ensure safe payments. The Google Wallet requires the setup of a PIN (Personal Identification Number) which will be entered before each purchase (Google, 2011). This feature is not applicable in other NFC payment schemes. Usually, the payments are made without requiring the insertion of a PIN. Furthermore, the bank account information that is stored in the secure element is protected with encryption (Google, 2011). The secure element is integrated as a separate component and only certain applications are able to access it (Google, 2011). During the payment process, the essential information is secure with the encryption technology that MasterCard PayPass provides (Google, 2011).

2.8 Security Concerns

Smartphones are more vulnerable to attacks than computers. This is based on the fact that smartphones are open, networked devices that can be programmed (Shabtai et al., 2009). In addition, the attackers are more experienced, because they have gained knowledge using the computer and the Internet. They already know the vulnerabilities that may exist in a device, so it is easier for them to write malicious code. As it is mentioned by Shabtai et al. (2009), ‘two years of smartphone evolution are equivalent to twenty years of work in computer viruses’ (Shabtai et al., 2009: 1).

Furthermore, users are making the mistake of trusting the security that a smartphone may have and as a result, they store more and more personal data in them (Chen and Peikari, 2008). The first years, smartphones were becoming popular there were not implemented many security mechanisms and the first smartphones had many holes and vulnerabilities. (Leavitt, 2005), (Chen and Peikari, 2008). Protection mechanisms like intrusion detection tools and antivirus programs are not present in smartphones because of their limited processing capabilities. (Chen and Peikari, 2008). Specifically, smartphones did not have as a primary goal the protection.

Smartphones are an attractive target for attackers. One of the main reasons is the existence of vulnerabilities. Moreover, smartphones are expanding around the world rapidly so the damage can be bigger and they contain a large amount of essential information (Shabtai et al., 2009). Smartphones are also well connected to different types of networks. They have internet access through wireless networks and can also use Personal networking using Bluetooth or ad-hoc networks (Chen and Peikari, 2008).

Although, many families of malware have been reported in the different operating systems of smartphones (Leavitt, 2005), the percentage of infected devices has been limited over the past years due to the fact that the overall number of smartphones was limited (Shabtai et al, 2009). Other reasons that malware was not a severe threat for smartphones is because there are a variety of mobile platforms and an attacker should create different malicious code for each one of them (Leavitt, 2005). Furthermore, smartphones are not continuously connected to the internet in order to save power, so the spreading procedure is delayed and Bluetooth attacks should happen in short range and this poses some restrictions (Chen and Peikari, 2008). However, it is estimated that until 2013, the number of smartphones will be 5 times bigger (Shabtai et al, 2009).

Smartphones consist of a large amount of personal data because of extensive use. This increases the possibility that a third person has unauthorized access to private data. This is considered a severe compromise of privacy (Tomlinson et al, 2010).

Some applications require access to data that are considered sensitive. Sensitive data can be defined as the data that may reveal personal information about the user such as their location, the applications they use, data they exchange with other people etc (Tomlinson et al, 2010). This also can be considered as a violation of privacy.

The next section presents a definition of malicious software.

2.8.1 Malicious Software

When we are referring to malicious software or malware, we mean one the three categories, virus, worm, Trojan. These three categories have many characteristics in common and their distinction is based on some details.

A virus can be defined as ‘a piece of software code (set of instructions but not a complete program) attached to a normal program or file’(Chen and Peikari, 2008 : 2). A virus is dependable on the program that is attached to and during the execution it takes the control and makes copies of itself to programs and files in the operating system.

A worm is an independent program. It propagates through the network and makes copies of itself on computers with vulnerabilities (Chen and Peikari, 2008).

A Trojan horse is presented as a legitimate program, but has a malicious function. Trojan horses are used to retrieve essential data such as passwords or are used to install other malicious programs (Chen and Peikari, 2008).

There are other types of malicious programs that have hidden functions, such as bots and spyware. ‘Bots are covertly installed software that secretly listen for remote commands, usually sent through Internet relay chat (IRC) channels, and execute them on compromised computers.’ (Chen and Peikari, 2008 : 2).

‘Spyware collects personal user information from a victim computer and transmits the data across the network, often for advertising purposes but possibly for data theft.’ (Chen and Peikari, 2008 : 2).

The image below presents the taxonomy of malicious software and the table presents the basic characteristics of a virus, a worm and a Trojan horse.

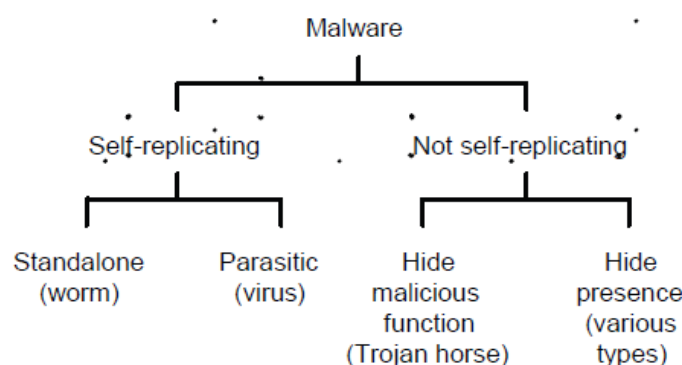


Figure 2.8. Malicious Software Taxonomy. This picture is copied from (Chen and Peikari, 2008)

	Appearance	User Interact.	Vector	Payload
Virus	needs a host-ing medium	usually needed	file transport, file injection, exploit	several, e.g. replication, modification
Worm	independent program	usually not needed	exploit	several, e.g. replication, remote access
Trojan Horse	malicious functionalities disguised	usually needed	file transport, exploits	several, e.g. remote access, destructive functionalities

Table 2.3. Malicious Software Taxonomy. This picture is copied from (Schmidt and Albayrak, 2008).

Malicious programs can cause a lot of problems to a smartphone. First, they can harm the device by making it unusable. They can steal personal and essential information, they can modify data and can charge the user by sending unwanted phone calls and messages (Shabtai et al., 2009). The majority of the malware that was created targeted the Symbian OS (Töyssy and Helenius, 2006).

In addition to these fears, the new NFC technology presents more challenges. Procedures that communicate with other entities require a high level of security in order to protect the essential information that is stored in a mobile device (Fischer, 2009). Even, the simplest services that are not involved with payments should provide security measures (Fischer, 2009). Furthermore,

2.9 Consumer Perspective

The widespread use of contactless payments conducted by payment cards and mobile phones depends on the acceptance of users. The most important obstacle that may delay the distribution of this technology is security issues (Smart Card Alliance, 2006).

A survey that is presented by Smart Card Alliance (2006) shows that from the percentage of people that used contactless payments, the majority believes that it is easy to use and fast. Smart Card Alliance (2006) denotes that a challenge is posed by consumers who are not familiar with this new technology. Users do not feel comfortable using this new technology, because they are not informed about how it works and is not part of everyday life (Ortiz, 2006). Education and experience will eliminate any hesitations about contactless payments (Smart Card Alliance, 2006). Edwards (2010) presents an opinion that the users will accept contactless technology, after they become comfortable with mobile payments. Furthermore, the results from the survey by Smart Card Alliance (2006) show that a significant proportion of users wants to use this technology, because contactless payments are easy to use and there is the possibility of carrying fewer items.

Although this new technology has its advantages, it has also many challenges that should be addressed (Pernet-Lubrano, 2010). There are fears that attackers will have a new mean to use for their own benefit (Francis et al, 2009). People are concerned about the security and

privacy issues of the NFC technology. Many different approaches have been presented in order to specify the security mechanisms that should be integrated in a mobile payment scheme.

Linck et al (2006) have presented how users perceive security and what are their concerns. This research can be used as a guideline to use the appropriate security mechanisms, so users can trust mobile payments.

3. Risk Assessment

3.1 Overview

In this chapter we focus on assessing the NFC functionality when it is integrated into a mobile phone/ smartphone. The main objection is to identify the vulnerabilities risks when using the mobile phone/smartphone to make a contactless payment and provide some possible solutions in order to enhance the security provided by the NFC protocol and eliminate possible threats. An improved version of the protocol will gain the trust of users and they will fill more comfortable using this technology to conduct their payments.

As it was mentioned on the previous chapter, NFC derives from RFID, which over the years has presented a number of security issues. Thus, the examination of whether those security issues were inherited in the NFC protocol is essential. Many articles and the NFC Forum declare that the NFC protocol has inherent security. The opinion is expressed based on the fact that the communication between two devices is done in a short-range distance. However, this does not necessarily mean that the NFC protocol is completely safe and further investigations are needed.

The acknowledgment of the vulnerabilities and risks is done through a quantitative risk assessment. First, we analyze the methodology used in order to observe how the protocol works and in order to characterize the potential risks. Furthermore, we present the architecture model of mobile device with NFC and through some use case scenarios we comprehend the entities and functions that are involved. We also provide information about threats that have been identified by researchers. At the end of the chapter, we present the possible risks that can occur to each different mobile operating system based on the implemented security mechanisms. Solutions are proposed in Chapter 4.

3.2 Methodology

The methodology used in order to evaluate the NFC protocol when it is used to conduct contactless payments with a mobile phone / smartphone is called Quantitative Risk Assessment (QRA). This type of analysis is chosen in order to identify the risks that could cause tremendous consequences in the system and the security mechanisms that should be applied to avoid them (Meritt, 2011). The objective of QRA is to present which of the risks are more dangerous and should be addressed first in order to eliminate them (Crocker, 2003). The risks are assigned with values which represent their significance, from urgent to non-important (Crocker, 2003).

A quantitative risk analysis can offer many advantages. It is a tool that is used for management in the industry and the analysis is objective (Tan, 2002). The analysis is made based on the needs of the industry, which can be declared and the recommended solutions reflect the recognized risks (Tan, 2002). Finally, the proposed solutions consider the cost and the benefits that a company will have (Tan, 2002).

To begin with, we present the definitions of risk and threat. A risk is called something that may harm or reduce the performance of a computational system. A threat can occur in a system and present a risk (Meritt, 2011).

The following points present the different stages of a Quantitative Risk Assessment as they are described by Croker (2003) and Tan (2002)

- Definition of the context. The components and the operational area of the concept should be presented.
- Identification of the risks: The risks should be identified and the conditions that contribute to their appearance should be presented.
- Determination of the severity of a risk. What are the consequences of each risk to the system? – Consequence (C).
- Specification of how frequent each risk can appear - Likelihood (L).
- Specification of how possible is the exposure of the system to each risk – Exposure (E).
- Classification of risks: $\text{Risk} = C \times L \times E$
- Identify the most urgent risks which have the highest value based on the above calculation.
- The most dangerous risks are analyzed.
- Solutions are proposed to address and eliminate the identified risks.

The following figure presents schematically the above procedure which is an alteration of the figure presented by Crocker (2003).

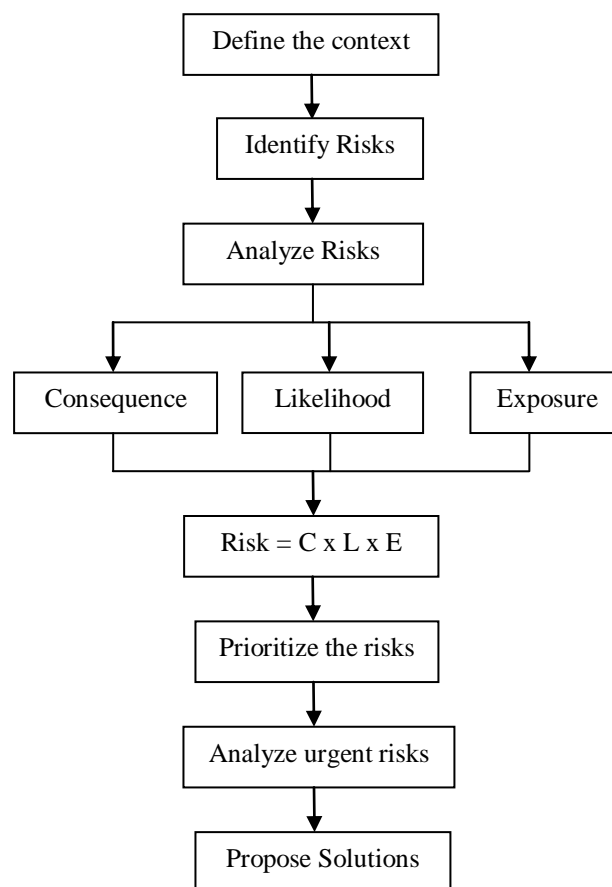


Figure 3.1. Quantitative Risk Assessment

3.3 Quantitative Risk Assessment

This section presents the Quantitative Risk Assessment that was made in order to identify the risks that may appear by using the NFC technology and which of these risks are the most crucial and need immediate actions.

3.3.1 Definition of Context

The first step of Quantitative Risk Assessment is the definition of the context. Thus, all the entities that participate in the technology and the processes that are needed must be defined. The most important and obvious entity that is needed, so that the protocol can work is the mobile phone / smartphone.

We show how a representative architecture model of a NFC enabled mobile phone works and then we proceed with the possible scenarios that occur when conducting payments.

3.3.1.1 Architecture Model

The following figures present the architecture model of a mobile phone / handset when it is integrated with the NFC technology.

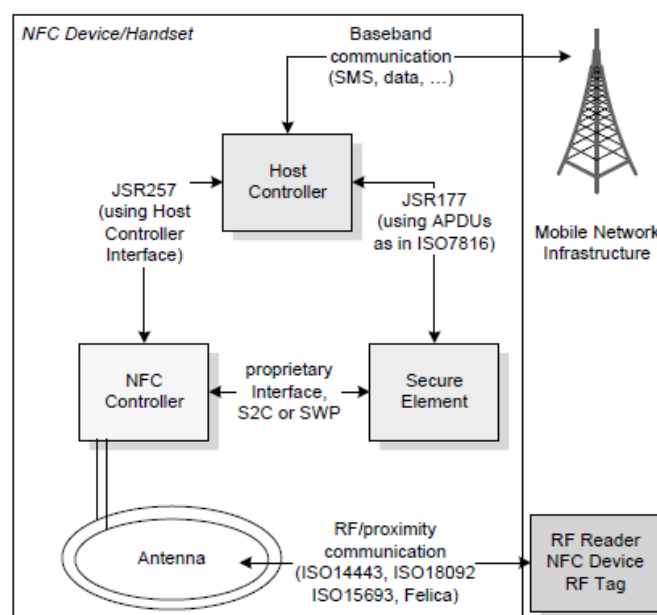


Figure 3.2. Architecture model of a NFC enabled mobile phone. This picture is copied from (Madlmayr et al., 2008b)

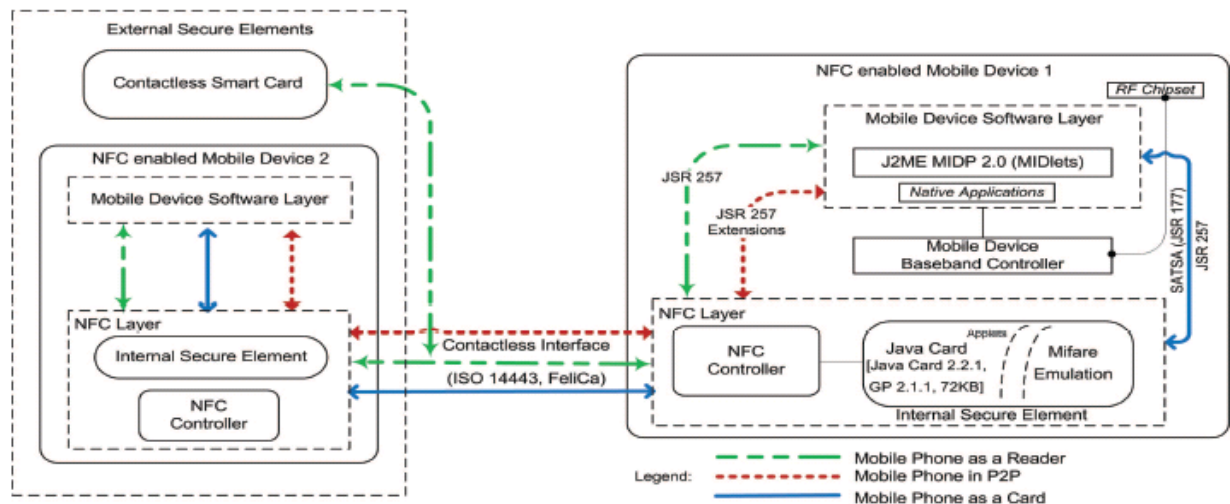


Figure 3.3. Architecture model of a NFC enabled mobile phone with operational modes when interacting with other devices. This picture is copied from (Francis et al., 2009).

The above pictures show the components that were described in the second chapter. However, in this section we will present them with more detail emphasizing the importance of the secure element.

The secure element is the most important component of the infrastructure (Francis et al., 2009). Choudhary and Risikko () define the secure element as “a dynamic environment, where applications are downloaded, personalized, managed and removed independent of each other with varying life cycles” (Choudhary and Risikko, :3). It consists all the essential information that is used for the transactions and the communication (Francis et al., 2009).

The content of the secure element can be modified by the appropriate applications installed on the mobile phone / smartphone (Madlmayr et al., 2008a). The applications are executed on the host controller which is responsible for the communication of the handset with the secure element (Madlmayr et al., 2008a). The host controller and the NFC controller have access to the data stored in the secure element. The NFC controller has access to data in the secure element that are going to be sent through an NFC communication (Madlmayr et al., 2008b). Additionally, the NFC controller is responsible for the conversion of the analog signal to digital and vice versa (Madlmayr et al., 2008b).

Based on the three modes, which a device can have and which were presented in chapter 2, a NFC enabled device can act as a contactless card and as Reader (Francis et al., 2009). When the device is in any of the three modes, the secure element communicates with the application layer through the host controller and with an external device with NFC controller (Francis et al., 2009). If the device acts as contactless card, it has a unique ID as it is indicated by the ISO 14443 (Madlmayr et al., 2008a) and can act as a passive contactless token (Francis et al., 2009). The ID is 4, 7 or 10 bytes long (Madlmayr et al., 2008a). This ID is used for identification in order to avoid collision issues during the process of contactless reading (Madlmayr et al., 2008a).

During the case that the device acts as a Reader, the device can communicate with other devices using JSR 257 API (Application Programming Interface) and the Host Controller. An example is that the device can initiate a communication with a smart object (NFC Data Exchange Format). (Francis et al, 2009).

The implementation of the secure element can be made using different architectures (Madlmayr et al., 2007). There are 3 major categories stated by Choudhary and Risikko ():

- **Removable Hardware:**
 - SIM card: The SIM card can be implemented easily and it is cost efficient (Madlmayr et al., 2007). Every cell phone needs a SIM card to make phone calls, thus it is easy to use it as a secure element as well (Madlmayr et al., 2007).
 - Advanced secure USB (Choudhary and Risikko,).
 - Secure Memory Card: It combines the functionalities of a smartcard and a memory card (Choudhary and Risikko,). It can store a large amount of information and can remain to its position from the beginning (Choudhary and Risikko,). The data stored are independently from other data on the device.
 - Universal Integrated Circuit Card (UICC): It has the properties of a smartcard and many applications can be stored on it Reveilhac and Pasquet, 2009).
- **Non-Removable Hardware:** An embedded chip or a baseband processor can be used (Reveilhac and Pasquet, 2009).
 - Baseband processor: The addition of extra hardware is not necessary. The secure element is part of the memory of the baseband (Reveilhac and Pasquet, 2009).
 - Embedded chip: A smartcard is added in the device and cannot be removed. The level of security provided is the one supported by the smartcard (Reveilhac and Pasquet, 2009). After purchase, the user should personalized it (Choudhary and Risikko,).
- **Software:** Software secure elements are considered in many areas (Choudhary and Risikko,).

Madlmayr et al. (2007) state that the cost of using an embedded secure element is less than a removable one. However, an embedded chip requires more attention. Although, there are many options, there is not a standardization about the architecture that it should be used (Reveilhac and Pasquet, 2009).

3.3.1.2 Scenarios

There are different scenarios when conducting a contactless payment and they can be divided based on their characteristics. Madlmayr et al. (2008b) proposes the following classification for mobile payment:

- Amount of money spent: micropayment or macro payment
- Point of Sale: Local or remote payment
- Clearing and Settlement: prepaid, post-paid, in-time paid
- Operation method: online or offline

In the scenarios described below we only use three of the above characteristics. All the payments are made locally. Because the NFC technology is a new technology for performing payments, it is not used by mobile phones or smartphones. All the scenarios described are results from various researches.

Scenario 1:

The first scenario is based on an idea proposed by Madlmayr et al. (2008b) for micropayments. The scenario presents a prepaid payment system which implements 3 different processes; top-up process, payment process and clearing and settlement.

A wallet application is needed to intervene between the secure element and the user and between the secure element and the server during the top up process. The wallet application informs the user about the available money on the phone and holds information about previous transactions. During the payment and top-up process, the wallet application updates the amount of money stored in the SVA (stored value amount), which is located in the secure element.

The following figure summarizes the different processes of the proposed payment system that are explained below.

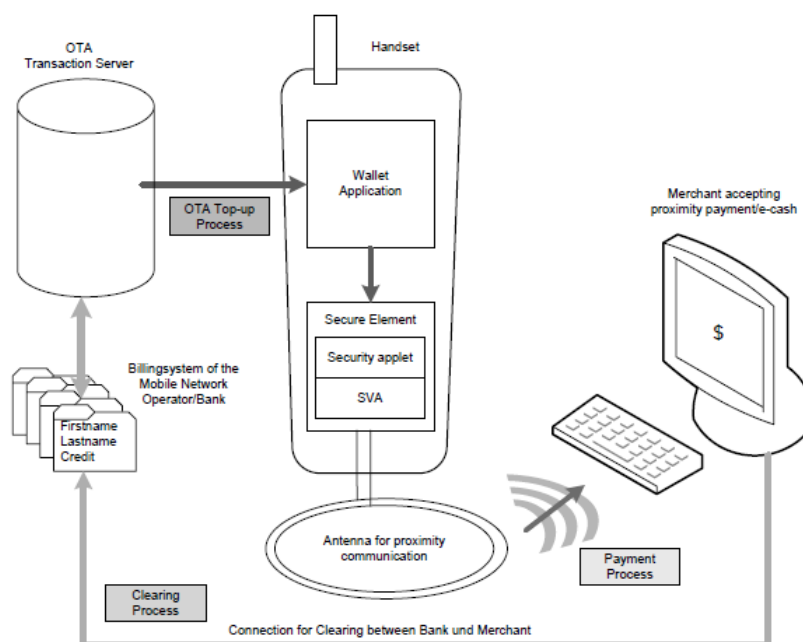


Figure 3. . Processes of the payment system. This picture is copied from (Madlmayr et al., 2008b)

- Top-up Process: The top-up process is made Over-The-Air within seconds. This procedure is called over the air because it can be made anywhere and at anytime.

The user initiates the process by selecting the appropriate option from the wallet application. Then, the wallet application requests the amount of money from the SVA. The user is informed about the available balance and they select the amount to be added. The wallet application creates an IP connection with the transaction server and sends the request of the user. The transaction server matches the user's mobile subscriber ISDN number with the IP address of the received package. The transaction server checks the account balance of the user and a positive answer is sent if the transaction can be made. The wallet application receives the packet and updates the SVA and the information are visible to the user. This process can be completed in 10 seconds.

- **Payment Process:** During the payment process the device should be in tag emulation mode. The user waves the device at a POS and the wallet application deducts the due amount from the SVA in some milliseconds.
- **Clearing and Settlement Process:** The transaction server can be informed with various ways. If the terminal operates online, the transaction server is informed immediately. If the terminal operates offline, it receives data after a predefined period of time. The transaction is cleared after some time and the money are received by the merchant.

Scenario 2:

A similar scenario can be made with in-time paid or post-paid cards. The top-up process is not needed and the clearing and settlement process of the above scenario can be used.

The difference is apparent during the payment process. The secure element contains all the information about the user's account. During the payment process, the device must be in tag emulation mode. The user waves the device at a POS and the wallet application initiates an IP connection with the transaction server and sends the request of the user. The transaction server matches the user's mobile subscriber ISDN number with the IP address of the received package. The transaction server checks the account balance of the user, it deducts the specified amount from their account and the transaction is completed. The wallet application can then be informed if the transaction was successful. The wallet application may also contain the available balance of the user's account and can inform them.

Scenario 3:

Pasquet et al. (2008) proposes a scenario that was used in a trial in France and it belongs to the category Touch and Confirm application. This scenario presents the actions that are requested by the user. We assume that the processes running at lower layers are the same with the above scenarios, but the difference is that the user is asked to enter a PIN code.

The user wants to make a purchase. The application that regards the payment can be chosen manually by the user or automatically. If the payment application is chosen manually, the user must select the appropriate application from a list. If it is selected automatically, the user waves the mobile phone at the POS and the technology recognizes the application that is needed for the payment. The application asks the user to enter their PIN code and the input is validated. If the PIN code is correct, the user is asked to wave the handset at the POS and the transaction is performed. Finally, the user is informed by a message that his transaction has been completed.

Scenario 4:

This scenario is presented by Haselsteiner and Breitfuß (2006). Two NFC devices can be used in order to exchange data. However, because of the low bandwidth only certain data types can be transferred (Ortiz, 2006). Thus, two devices cannot exchange music or video files, but these files can be exchanged using different technologies such as Bluetooth or WiFi. The NFC technology can be used, so the devices will exchange the settings in order to initiate the communication with the other technologies.

The above scenarios presented the components of communication and contactless payments and the processes that can be executed. We can summarize them in a small list below:

- Mobile phone integrated with NFC technology
- Secure element
- Contactless card properties / Payment Process
- Payment – Top-up processes
- Communication between 2 devices

In the next section, the risks that can threaten the above list are presented and explained.

3.3.2 Identify and Analyze the Risks

For each of the above points, we present the possible threats and risks. We also investigate if each risk is applicable in the Operating systems of smartphones that were described in chapter 2 based on the security mechanisms they use.

Hardware

To begin with we present one of the simplest threats. Because of the small size of the mobile phone, a mobile phone or a smartphone can be lost or stolen easily. As a result, all the data that are stored in the mobile phone / smartphone can be read by unauthorized people. Attackers can also have access to the secure element which contains information about bank accounts. Moreover, because the secure element may belong in the category of removable hardware it can be also lost or stolen. Other device may be able to read the contents stored on it.

The leakage of information of information can create some privacy issues as well. The secure element contains information about previous payment transactions. If an unauthorized person has access to this data, they can find information about the owner of the mobile device and about their location.

Another hardware component that is threatened and many attacks have been implemented is the unique ID of the contactless tag based on ISO14443 (Madlmayr et al., 2008a). This unique ID is used for identification and to avoid collisions, as it was mentioned in a previous chapter (Jara et al., 2010). The unique ID when it is transmitted it does not use an encryption algorithm and the reading device is not asked to authenticate itself (Madlmayr et al., 2008a). Thus, this situation encapsulates many risks.

There is the risk that the ID is leaked and then it can be used by another card which can lead to cloning (Jara et al, 2010). Moreover, there are privacy violations. Each ID is unique, so when it is leaked, the location of person is leaked as well.

Application Layer

Each mobile phone / smartphone has many applications installed on its platform. Some of them are applications developed by third parties. Although, most operating systems do not allow applications to run outside their directory, there are many ways to bypass these restrictions (Schroder et al., 2011). These applications can have access to the secure element. There are also other applications in the secure element that support the functionality of NFC (Madlmayr et al., 2008a). If other applications have access on them there is the risk of data modification, data insertion and there are issues that concern the privacy of the user as well.

Furthermore, third-party applications may consist malware. Many Operating Systems do not have a strict policy about the signing of third-party applications and the user must decide if they want to install the application or not. If an application consists of a Trojan horse then information from the secure element can be leaked to attackers and they can use it in order to impersonate the legitimate user. The existence of malware on a handset poses many other threats. Applications may be executed without the knowledge of the user and they can withhold the resources of the system. Threats are also present for the Host controller and the NFC controller. If they are modified then the NFC technology cannot work properly (Madlmayr et al., 2008a). “Processes initialized by the NFC controller that are executed on the Host controller can be blocked, modified or eavesdropped” (Madlmayr et al., 2008a:645). This can also happen to the NFC controller (Madlmayr et al., 2008a). Finally, a user may modify the properties of NFC or Host controller and can cause problems to the technology.

Contactless card properties / Payment Process

During the payment process, the mobile phone is turned on the tag emulation mode. This mode refers to contactless cards of the ISO 14443. This technology refers to RFID tags, which as it was mentioned above have many security issues. ISO 18092 and ISO 14443 do not implement any security for the contactless communication (Madlmayr et al., 2008a). Thus, the vulnerabilities, which were recognised in contactless cards, have been transferred to the NFC protocol.

The attacks can lead to information leakage, cloning, impersonating and to privacy violations. Moreover, some attacks can charge the account of a user with purchases that they have not committed. The possible attacks are presented below:

- Eavesdropping: Without any encryption schemes, an attacker can collect the data that are sent by the tag during a transaction (Jara, 2010).
- Spoofing Attack: The data that are stored in the tag can be duplicated and can be used to another reader (Jara, 2010).
- Cloning Attack: It is similar with spoofing attack, but with the difference that the duplicated data are store in another tag (Madlmayr et al., 2008a). Francis et al. (2009) presents a cloning attack can be done very easily with the use of another NFC enabled mobile phone and with the appropriate software. After the attack, the new contactless card is considered legitimate.
- Relay Attack: Most relay attacks focus on ISO 14443. In relay attacks the attacker retransmits the data send by the token and the reader in the time of the transaction (Hancke, 2009).

Payment / Top – up processes

In this section, we refer to the procedures that need an internet connection in order to communicate with a server. Other procedures involved are analyzed in other sections.

During the internet connection between the mobile phone / smartphone and the back-end server, there are fears of possible threats and attacks. In the network where the connection is made, there is the possibility that an attacker exists. If the information is sent without any

protection, attacks such as Data Modification, Data Insertion, Data Corruption and Man-in-the-Middle attack and Eavesdropping can be easily created.

These attacks are crucial because the attacker modifies data causing several problems and essential information concerning account details is leaked. This information can be used by the attacker in order to conduct payments using the user's account. Furthermore, the attacker can learn personal details about the user, which is a privacy breach.

Communication between two devices

There is a variety of attacks that can be done when two devices communicate with each other. Haselsteiner and Breitfuß (2006) present some of the possible attacks.

- **Eavesdropping:** The NFC protocol requires RF field in order for two devices to be able to communicate. An attacker can also receive the signals with the appropriate knowledge. The communication must be made in a small range distance, which is usually 4 cm. However, based on certain factors an attacker can listen to the communication from a certain distance. A combination of some parameters is sufficient for an attacker to eavesdrop. Some parameters are the attacker's antenna, the attacker's receiver and in what mode does the device transmits data. If the sender is in active mode then the distance is bigger at about 10m, but if the sender is in a passive mode, then the distance is reduced to about 1m. During eavesdropping, information can be leaked to the attacker.
- **Data Corruption:** This attack can also act as a Denial of Service, because the attacker cannot modify the sent data. However, if they are aware of the modulation and the coding used then the attacker can send valid packets of data.
- **Data Modification:** This attack is depended on the amplitude of modulation. The NFC protocol uses different coding schemes based on the value of baudrate. If the baudrate of an active is 106kBaud then the modified Miller coding scheme is used with 100% modulation. If the baudrate is greater, then the Manchester coding is used and the modulation is 10%. If the device is passive, then the Manchester coding is used. This information can be found on the ISO18092 (ISO, 2004).

The data modification can only be applied in certain bits of the modified Miller coding. If the Manchester coding scheme is used, then the attack can be applied for all bits. The attacker sends a signal, which must overlap the original signal and the decoder will decode the opposite value of the bit that was sent. The modification of data can lead to tremendous consequences.

- **Data Insertion:** Data insertion attack can be accomplished only if the response time for the answering device is long enough for the attacker to insert their data. The attacker must transmit the data before the response begins transmitting, otherwise the two messages will be conflicted.
- **Relay Attack:** (Francis et al., 2010) have shown that a peer-to-peer relay attack is possible between two devices that communicate with NFC technology. An attacker can create and introduce proxies. During the communication of two mobile phones, the proxies can interact between them using a Bluetooth connection. Mobile phone A believes that it receives messages from Proxy B and mobile phone B believes that it

communicates with Proxy A. However, the messages are sent from phone A and phone B. The proxy phones are only involved in order to relay the messages.

The following table summarizes the risks that were identified in this section. It presents the risks that can appear when certain threats are present. It also shows the consequences of each risk. Each threat has number indicating the possibility of the threat to appear and each consequence an number indicating the severity of the consequence.

Risk	Threat	Consequence
Information Leakage	1. Stolen or lost mobile phone (5%) 2. Stolen or lost secure element (removable) (5%) 3. Unauthorized or unsigned applications have access to secure element (30%) 4. Malware – Trojan horse (15%) 5. Eavesdropping (20%) 6. Man-in-the-Middle Attack (15%)	1. Privacy Violations (8) 2. An adversary can use the data for their own benefit – Impersonating (8)
Leakage of ID	1. Eavesdropping (20%)	1. Privacy Violations (8) 2. Clone creation (7)
Stored Data are modified	1. Malware (15%) 2. Data Modification (20%) 3. Data Insertion (20%)	1. Malfunction of the protocol (6) 2. Inconsistency (7)
Host or NFC controller compromised	1. Malware (15%) 2. Mistake by the user (5%)	1. Malfunction of the protocol (6)
Applications run without the user knowledge	1. Malware (15%)	1. System resources are withheld (5)
RFID tag information leaked	1. Eavesdropping (20%) 2. Cloning Attack (20%) 3. Spoofing Attack (20%) 4. Relay Attack (20%)	1. Clone creation (7) 2. Overcharged account (8) 3. Privacy Violations (8)

Table 3.1 Risk Identification

3.4 Classification of risk

In this section the risk will be classified. The above table will be used in order to assign values to consequence, likelihood and exposure.

The values of each element are:

- Consequence Range: 1 – 10 with 1 indicating not urgent and 10 urgent
The average is taken from the assigned values in the table.
- Likelihood Range: 0 – 100%
The percentage is summed.
- Exposure Range: 0 – 100%

In order to estimate the exposure factor we can use some of the questions as they were presented by Tan (2002):

1. Does the system under attack have any redundancies/ backups/copies?
Subtract 30% if the answer is YES
2. Is the attack from outside?
Subtract 15% if the answer is YES
Subtract 15% if the answer is NO
Subtract 10% if the answer is both YES and NO
3. What is the likelihood that the attack will go undetected in time for a full recovery?
Subtract 10% if the probability of being undetected is less than 20%
Subtract 30% if the probability of being undetected is less than 10%
4. How soon can a countermeasure be implemented in time if at all?
Subtract 30% if the countermeasure can be implemented within ½ hour
Subtract 20% if the countermeasure can be implemented within 1 hour
Subtract 10% if the countermeasure can be implemented within 2 hours

Risk	C	L	E	R
Information Leakage	90%	8	70%	5.04
Leakage of ID	20%	7.5	65%	0.975
Stored Data are modified	55%	6.5	50%	1.7875
Host or NFC controller compromised	20%	6	45%	0.54
Applications run without the user knowledge	15%	5	65%	0.4875
RFID tag information leaked	80%	7.66	55%	3.3704

Table 3.2. Risk Classification

The above table classified the threats and presents the most urgent ones. It is obvious that the most urgent risk is the information leakage with a risk value 5.04 and the least urgent risk is the compromise of the Host or the NFC controller.

The following table is ordered in order to examine the risks and their significance more closely.

Risk	C	L	E	R
Information Leakage	90%	8	70%	5.04
RFID tag information leaked	80%	7.66	55%	3.3704
Stored Data are modified	55%	6.5	50%	1.7875
Leakage of ID	20%	7.5	65%	0.975
Host or NFC controller compromised	20%	6	45%	0.54
Applications run without the user knowledge	15%	5	65%	0.4875

Table 3.3. Ordered Risks

The risks with high values presented a large percentage of likelihood and they are more likely to happen. The leakage of information for example, is a major risk that was presented in all of our scenarios. Different threats can lead to this result and the consequences are considered serious. An adversary has access to essential data that may represent bank accounts. As a result, they can use this information to impersonate the user and perform payments. Furthermore, the privacy of the user is violated. An adversary can learn more about the personal life of the user.

The information from the RFID tag can also be leaked to a third party. This will have the same consequences as the information leakage. An adversary can use the retrieved information to create a clone contactless card, which can be used for payments. Moreover, if the stored data are modified, the user then will not know the correct balance of their account or they want be able to use their phone to make contactless payments.

The other risks that were presented are not insignificant and solutions should be found as well. However, they cannot be classified as urgent, because there is a small possibility of appearance and their results are not tremendous.

4. Results & Solutions

4.1 Overview

The previous chapter presented the context of the NFC protocol when it is integrated into a mobile device / smartphone. This risk analysis targeted mobile payments and presented the risks that may appear. The risks were also valuated to discover which of them require immediate solutions in order to avoid tremendous consequences.

In this chapter we continue with the last step of our risk assessment. We propose some indicative solutions in order to ensure that contactless payments with NFC and peer-to-peer communication can be performed without risks. Furthermore, we evaluate how feasible is the implementation of each measure and the alternatives solutions that should be considered. For each of the identified risks, there is a list of solutions.

4.2 Security Objectives

The security measures that are adapted should satisfy certain objectives. The security objectives can be found on the table below.

Security objective	Definition	Enabling concept/technique
Confidentiality	Property that ensures that transaction information cannot be viewed by unauthorized persons	Encryption
Authentication	Property that the transaction information actually originates from the presumed transaction partner	Possession (e.g. of a mobile phone), knowledge (e.g. of a PIN) und property (e.g. biometric property)
Integrity	Property that the transaction information remains intact during transmission and cannot be altered	Digital signatures
Authorization	Property that parties involved must be able to verify if everyone involved in a transaction is allowed to make the transaction	Digital certificates
Non-repudiation	Property that no one should be able to claim that the transaction on his/her behalf was made without their knowledge	Digital signatures

Table 4.1. Security Objectives. This table is copied form (Linck et al., 2006)

4.3 Encryption Schemes

In this section we present briefly some of the cryptographic schemes that are used for confidentiality. Digital Signatures are used for integrity or non-repudiation, hash functions for authentication and digital certificates for authorization (Linck et al., 2006).

Cryptographic schemes are distinguished in symmetric and asymmetric schemes.

Asymmetric Schemes: A message can be encrypted using the public key but it can only be decrypted by the entity that holds the secret key.

- Diffie-Hellman Key exchange: It is the one of the first public-key algorithms. Two entities can exchange a key securely, which will be used for the encryption of messages. The algorithm uses computing discrete logarithms (Stallings, 2005: 298). However, it is not robust against the man-in-the-middle attack (Stallings, 2005: 298).
- RSA: “The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n for some n . A typical size for n is 1024 bits, n is less than 21024.” (Stallings, 2005: 268).

Symmetric Schemes: The two entities share a secret key and only the two entities know it. The data is exchange using that secret key for encryption and decryption. An asymmetric scheme should be used for the exchange of the secret key (Jara et al., 2010).

- AES: A cipher whose block length and key length can be specified to be 128, 192, or 256 bits (Stallings, 2005: 140). It was designed to replace the DES algorithm.
- Triple DES: The Triple DES with 3 keys is more secure than the other versions of DES algorithm (Stallings, 2005: 180). The DES algorithm is described: “Data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.” (Stallings, 2005: 72).

Hash Functions: Hash functions are used for the authentication of a message. A hash value h is generated with the use of a function H , which is applied on the message. They do not implement security, so the hash value must be protected (Stallings, 2005: 334).

Digital Signatures: They are used for message authentication. It offers protection to two entities that communicate with each other for a third-party. However, digital signatures do not provide protection to the entities for each other (Stallings, 2005: 378).

4.4 Security Measures

Hardware

When the mobile phone / smartphone is stolen or lost there are mechanisms, so that the memory of the phone can be erased remotely by the user or the user can report the phone as stolen and lock it. With these measures, the person, who has the mobile phone and they are not the legitimate owner, cannot have access to the wallet application or at the information that are stored in the secure element (Apple Inc., 2011).

As it was mentioned in the previous chapter, the secure element can be implemented with various architectures. A safe solution could be a secure element embedded in the mobile phone / smartphone or a removable component that implements a level of security, so that if it gets lost or stolen, it would be difficult for an adversary to have access to the stored data.

To protect the ID of the tag and eliminate the risk of cloning attacks a random algorithm can be used. This random algorithm can produce different ID each time. The random ID can be used for avoiding collisions and then the tag can be use the unique ID for further actions. (Jara et al., 2010). This measure is used with e-passports as well, but an adversary can find out if the tag represents a NFC device or a smartcard (Madlmayr et al., 2008a).

Application Layer

The secure element should be implemented in order to provide security as its name indicates. Essential data are stored in the secure element thus, it should be tamper resistant. If the secure element is a SIM card then there may be a level of security. Many SIM cards require a PIN code to authenticate the identity of a user.

Cryptographic functions should be applied to protect the data when they are transferred from and to the secure element and the applications stored in the secure element should be executed safely (Madlmayr et al., 2007). Moreover, application that need access to the secure element should be authorized and authenticated (Madlmayr et al., 2008a). All the applications installed on the mobile phone / smartphone and on the secure element should be signed. Not signed applications should not be distributed in order to avoid malware.

Madlmayr et al. (2008b) proposes a payment system which implements different levels of security. The secure element has a security applet stored in it. The application wallet does not have direct access to the secure element. The secure applet is responsible for all the information that leaves and enters the secure element. The information is encrypted.

Another approach is the addition of a trusted hardware component, which will control the system. This component controls the execution of applications. Only the applications, which are included in a list can be executed (Schroder et al., 2011).

Finally, a piece of hardware could be added in the device that contains the cryptographic algorithms that are needed for the encryption of the data that are stored in the device. The algorithms will run on the additional component and the device will not be overloaded with extra functionality.

Communication / Payment / Top – up process

The above processes present the same risks and the threats, thus the measures that can be applied on them are the same.

Madlmayr et al. (2008b) during the presentation of the payment system, they propose several security mechanisms that could be applied. During the top-up process, the security applet communicates with the transaction server using session keys in order to avoid relay and cloning attacks. The data are encrypted using the AES encryption scheme and signed using the RSA. The keys that are needed are stored in the security applet. The signing procedure is

used for non-repudiation and certificates are also used for authentication against the transaction server.

Haselsteiner and Breitfuß (2006) state that a secure channel eliminates the possibility of an attack. They propose a different scheme for peer-to-peer communication. They believe that the key agreement Diffie-Hellman can be used for the exchange of the secret key and then Triple DES or AES can be used for the exchange of data. This security measures can only be used for peer-to-peer NFC communication, because the Man-in-the-middle attack cannot be implemented (Haselsteiner and Breitfuß, 2006). For an internet connection, another asymmetric scheme should be used for the exchange of the public key.

In order to have a secure communication with devices the NFC protocol can adapt some security mechanisms that are in certain mobile operating systems. The encryption schemes, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) that are used by RIM in Blackberry when the device communicates with the BES can be used for the payment and top-up processes (Blackberry, 2011). Jara et al. (2010) present similar solutions for secure communication. They present a three level security architecture, which is summarized on the table below.

Security level	Security technique		Actors
First level	No security		An active and a passive device
Second level	Symmetric cryptography	3DES, AES	An active and a passive device
Third level	Asymmetric cryptography	RSA, ECC	Two active devices (P2P communication)

Table 4.2. Security Levels. This picture is copies from (Jara, 2010).

The three-level architecture is designed in order to satisfy each scenario. In the first level, there is no need for security; it concerns scenarios that simple tags need identification (Jara, 2010). The second level regards the payment process. The symmetric cryptography is used because it is faster than RSA. RSA add an extra overload to the communication because of its complexity. In addition DesFire is used to provide security to the RFID tags (Jara, 2010). MiFare is not used because many attacks can be implemented (Kasper et al., 2010). The third level was defined in order to provide authenticity, digital signature, confidentiality and integrity. It can be used for the key agreement that is needed at level 2 (Jara, 2010).

The above measures do not provide a solution for relay attacks because it is difficult to be protected against them. The main reason is because they can bypass the cryptography schemes that are implemented on the application layer (Hancke et al., 2009). However, there are other countermeasures that should be taken into account. Hanck et al. (2009) explores three different measures; timing constraints, distance bounding and additional verification.

- **Timing constraints:** The procedure of relaying a message needs some time. Thus, a specific period of time can be implemented in order to detect a late message which may be an attack. This measure has been adopted from the ISO 14443 standard.

However, it is no effective, because the time needed from the attacker's device to produce a relay message is much less than the time-outs. Another solution would be to eliminate the time-out values, but this would cause problems to the communication and legitimate messages could be rejected. The time that is needed from a device to generate a response message is likely to be larger than the time-out value. Consequently, the solution is not feasible and cannot be implemented.

- Distance Bounding: The maximum physical distance between two entities is calculated based on the Round-Trip-Time (RTT) of cryptographic challenge response pairs. These protocols can detect the delay that is cause by a relay attack.
- Additional Verification: Relay attacks could be reduced if more checking procedures were implemented. Authentication procedures such as face recognition or PIN codes so that they legitimate user could be verified. A check could be done to see if a proxy device is used. However, these measures increase the transaction time and are not preferred. Another solution is an additional device which can monitor the transaction and can recognize suspicious transactions.

The above measures were presented by various authors, who try to reduce the risks that exist within the NFC technology and they were identified during their research. However, they were not applied a representative number of devices.

4.5 Security Model

A more general model that can be applied in any mobile payment scheme is presented by (Taghiloo et al., 2010). The model tries to satisfy the objectives as they were presented in section 4.2. The following figures present the security mechanisms from the sender and receiver side.

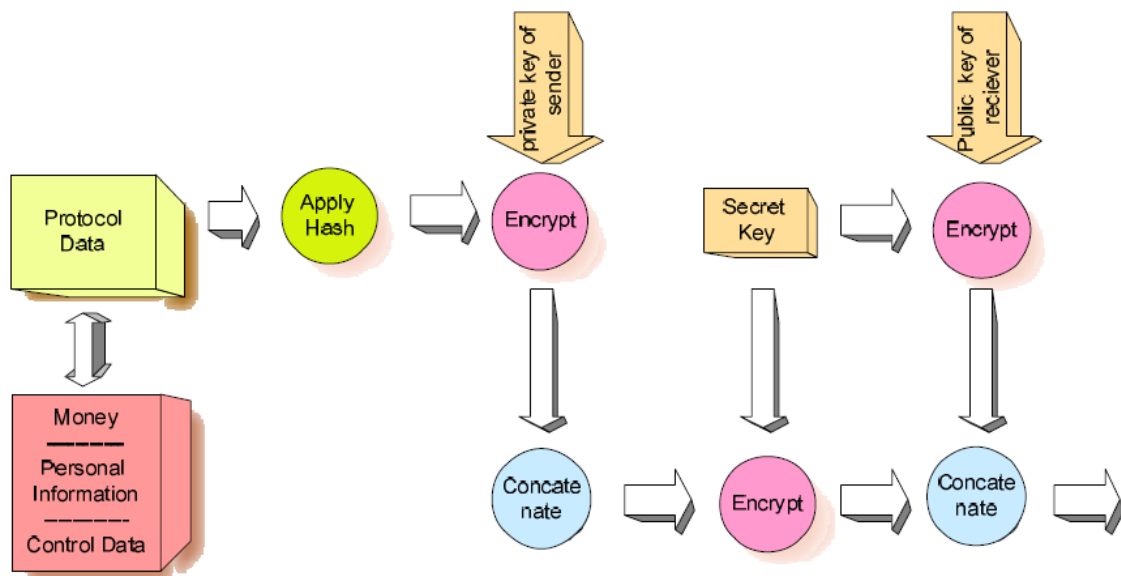


Figure 4.1 Security mechanisms of sender. This figure is copied from (Taghiloo et al., 2010).

The sender applies a hash function to the message and the result of the hash function is encrypted and concatenate with the original data. Then the result is encrypted with a secret key and the secret key is encrypted with the public key of the receiver. Finally, the two encrypted messages or concatenate.

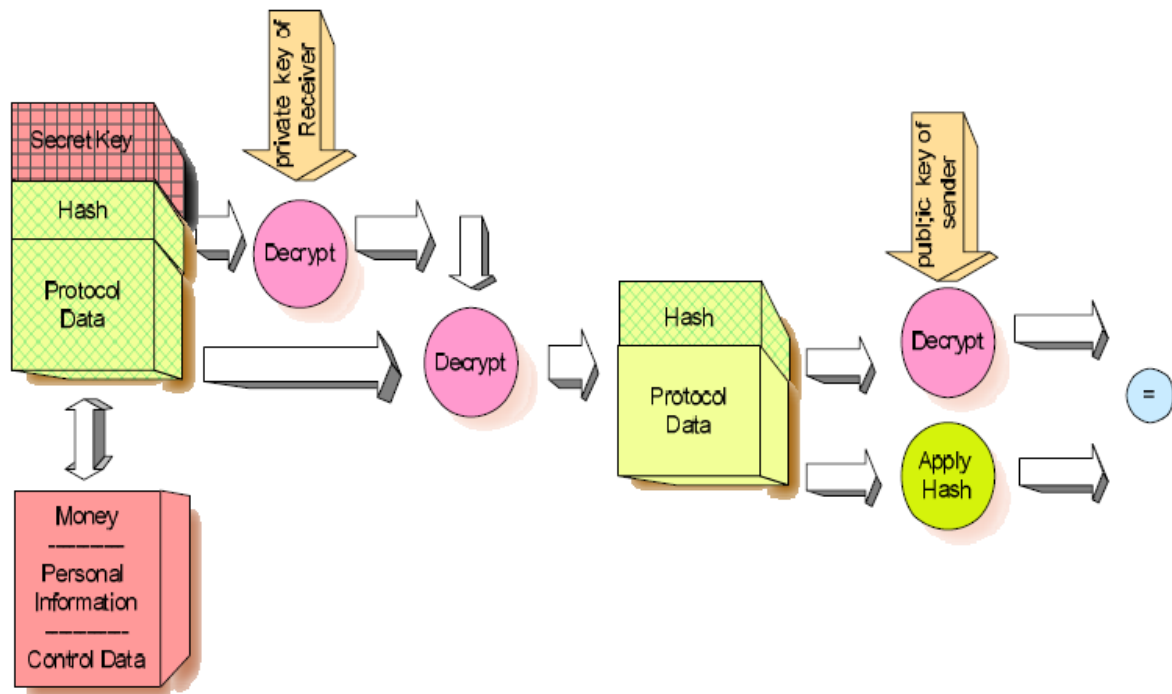


Figure 4.2 Security mechanisms of receiver. This figure is copied from (Taghiloo et al., 2010).

The receiver extracts the secret key from the sent data and decrypts it by using their private key. The message is decrypted with the secret key and then the hash is decrypted with the use of the sender's public key. The hash is applied to the remainder data. The decrypted hash and the remainder data are compared. If they are equal, then the data were sent securely.

5. Discussion

The aim of this project was the assessment of the security mechanisms that are implemented on mobile phones and smartphones. Smartphones present a variety of different technologies that can be investigated, so we decided to focus on contactless payments and on the Near Field Communication protocol when it is integrated in a mobile phone / smartphone.

The NFC protocol is relatively new and can offer new capabilities to a mobile phone /smartphone. Wallet applications can be designed and the user has the ability to choose between a variety of services. However, these new applications need to have access to essential data and bank accounts. As a result, people do not trust this technology and are not comfortable using it.

Our research aimed to find possible vulnerabilities and risks in order to reduce the percentage of attacks that can be implemented. Furthermore, we presented solutions and security mechanisms that should be added in the NFC technology, so that people will feel safer. Our research was not focused in one platform or on one operating system, because the NFC technology is not integrated yet in many mobile phones and smartphones. We examine the technology and its capabilities at a more abstract level.

Chapter 2 presented a background research on the relevant topics. The smartphones were presented and the most famous operating systems with the security mechanisms they use. Moreover, mobile payments were introduced and their categories and we focused on contactless payments. Near Field Communication was presented with a variety of details about its functionality and its capabilities. The term wallet application was explained and two applications were presented as an example. Chapter 2 concludes with explaining why people feel so reluctant about using this new technology. The main reason is because they feel threatened from the various types of attacks and because smartphones are considered an easy target by an adversary.

In chapter 3, a risk analysis was performed. The method of the risk assessment was chosen in order to create a more comprehensive and completed image about the NFC technology. A quantitative risk assessment was chosen in order to prioritize which of the found risks must be encountered first and which of the proposed solutions are the most appropriate.

The risk assessment was divided in several steps. First, the context of the protocol should be specified. We presented the most important component of the protocol, which is the secure element and we explained how the information flows in a representative architecture model. Then, we presented possible scenarios of the technology when the user wants to perform a payment or communicate with another device. The scenarios were needed in order to understand how the protocol interacts with the mobile phone/smartphone and with the environment.

The next step of the assessment was to identify any possible risks that may appear during the scenarios. The risks were identified from a series of different attacks. It is obvious that the NFC technology does not implement security mechanisms in order to protect its assets. This is mainly because the technology derived from RFID, which was proved that has a variety of security and privacy issues. After the identification of the risks we examined which of the presented risks were the most urgent using three different parameters; exposure, likelihood and consequence.

In chapter 4, security measures were proposed in order to enhance the protection of NFC protocol and reduce the risks. The security measures that are proposed are result of a research. Each measure was evaluated based on its performance and if there is a better solution, it is specified. Although, the proposed solutions seem to present a more secure protocol, it is expected that other possible solutions can be considered in further investigations.

This project evaluated the NFC protocol and identified some of the risks and threats that can occur when certain scenarios are executed. A different selection of scenarios could result different risks. Although, the NFC protocol adds new functionality to mobile phones, it has much vulnerability that should be addressed. The users will need security assurance in order to trust the NFC technology and add it to their everyday activities.

6. Future Work

NFC is still considered to be a new technology and it is expected that sometime in the future it will be adapted by all mobile phones and smartphones. However, there many issues that should be considered. The security mechanisms that are provided by the Near Field Communication protocol are inadequate and research should be carried out in order to find solution to reduce the risks and protect the assets of users. There are many different aspects of smartphones and Near Field Communication payments that can be examined.

6.1 Risk Assessment on Smartphones

The most used operating systems of smartphones, such Android, iOS and Blackberry have begun integrating NFC in the smartphones. Assessments should be performed in order to evaluate the addition of the new technology in each platform. Each operating system uses different technologies and security mechanisms.

As a result, when the NFC technology is integrated in the mobile platform, the risks would be different. Risk assessments are needed to indicate which components or processes need protection.

6.2 Creation of a more robust protocol

Near Field Communication is a protocol that explains how contactless communication is performed. However, ISO 18092, which presents the protocol, focuses on the communication and does not include security mechanisms for the protection of the protocol's participants and components. There are many risks that should be addressed and security mechanisms should be implemented. These security mechanisms can be included into a new standardization based on the existing technology of NFC.

However, a better and more preferred solution is the creation of a new protocol that will be designed with consideration for the possible risks. Thus, the security mechanisms will be integrated in the protocol. The new protocol will implement contactless communication with protection to users and to the components of the architecture model.

References

- Android Developers, (2011), What is Android? – Android Developers [Online] Available: <http://developer.android.com/guide/basics/what-is-android.html> Accessed: September 2011.
- Anokwa, Y., Borriello, G., Pering, T., and Want, R., (2007), “A User Interaction Model for NFC Enabled Applications”, *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07, 5th Annual IEEE International Conference*, New York, USA, pp. 357-361.
- Apple Inc., (2011), Apple-iPhone [Online] Available: <http://www.apple.com/uk/iphone/ios4/> Accessed: September 2011.
- Barclays (2011), Barclays contactless debit cards – Barclays [Online] Available: <http://www.barclays.co.uk/Helpsupport/Barclayscontactlessdebitcards/P1242561764200> Accessed: September 2011.
- Barrera, D. and Van Oorschot, P., (2011), “Secure Software Installation on Smartphones,” *Security & Privacy, IEEE*, vol. 9, May, pp. 42 - 48.
- Blackberry, (2011), Blackberry Security Features [Online] Available: <http://uk.blackberry.com/atagance/security/features.jsp> Accessed: September 2011.
- Barton, J.J., Shumin, Z. and Cousins, S.B., (2006), “Mobile phones will become the primary personal computing devices”, *7th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA'06)*, pp. 3-9.
- Boyd, J., (2005), “Here Comes The Wallet Phone”. *IEEE Spectrum Online*.
- Bradford Terri, (2005), “Contactless: The Next Payment Wave?,” *Payment System Research Briefing*, Federal Reserve Bank of Kansas City.
- Chang, Y.F., Chen, C.S., and Zhou, H., (2009) "Smart phone for mobile commerce", *Computer Standards & Interfaces*, vol.31, no. 4, pp. 740-747.
- Chen, T., and Peikari, C, (2008), “Malicious Software in Mobile Devices”. *Handbook of Research on Wireless Security*, pp. 1
- Choudhary B. and Risikko J, (2005), “Mobile Device Security Element”, *Key Findings from Technical Analysis v. 1.0, Mobey Forum*.
- Crooker, J, (2003), “Quantitative Risk Assessment: An Outline to being Realistically Prepared”, [Online] Available: <http://www.clermiston.com.au/Documents/Quantitative%20Risk%20Assessment.pdf> Accessed: September 2011.
- Edwards C., (2010), “Touch me I electric”, *Engineering & Technology*, pp.63-65
- Fischer, J. (2009), ‘NFC in Cell Phones: The New Paradigm for an Interactive World,’ *IEEE Communications Magazine*, vol. 47, no. 6, pp. 22-28.

Francis, L., Hancke, G.P., Mayes, K.E., and Markantonakis, K. (2009), "Potential Misuse of NFC Enabled Mobile Handsets with Embedded Security Elements as Contactless Attack Platforms.", *Proceedings of the 1st Workshop on RFID Security and Cryptography (RISC 2009), in conjunction with the International Conference for Internet Technology and Secured Transactions (ICITST 2009)*, pp. 1–8

Francis L., Hancke G., Mayes K., and Markantonakis K., (2010), "Practical NFC Peer-to-Peer Relay Attack using Mobile Phones", *Workshop on RFID Security*

Hancke, G., Mayes K., and Markantonakis K., (2009), Confidence in Smart Token Proximity: Relay Attacks Revisited. *Computers & Security*.

Haselsteiner E., Breitfuß K., (2006), "Security in near field communication (NFC)", Workshop on *RFID security*, Graz, Austria

Heikkinen, P. (2009), "A framework for evaluating mobile payments", Financial Markets and Statistics, Bank of Finland.

International Organization for Standardization, (2004), *ISO/IEC 18092 Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)*, ISO.

James, G., (2004), "Malicious threats to Smartphone", *Network Security*, vol. 2004, pp. 5-7.

Jara, A., J., Alcolea, A., F., Zamora, M. A. and Skarmeta, A. F. G., (2010), "Evaluation of the security capabilities on NFC-powered devices", *Smart Objects: Systems, Technologies and Applications (RFID Sys Tech), 2010 European Workshop*, pp.1-9, Spain.

Juels, A., "RFID Security and Privacy: A Research Survey", *To Appear in the Proceedings of IEEE JSAC'06*.

Kasper T., Silbermann M., and C. Paar., (2010) "All You Can Eat or Breaking a Real-World Contactless Payment System," *Financial Cryptography and Data Security*, vol. 6052, pp. 343-350.

Lambert, M. (2005), "Blackberry Security", *Network Security*, vol.2005, no.6, pp. 18-20

Lessard, J. and Kessler, G.C., (2010), "Android Forensics: Simplifying Cell Phone Examinations", *Small Scale Device Forensics Journal*, vol. 4, no. 1

Linck, K., Pousttchi, K., Wiedemann, D.G, (2006), "Security issues in mobile payment from the customer viewpoint, *Proceedings of the 14th European Conference on Information Systems (ECIS)*, Goteborg, Sweden.

Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C., and Scharinger, J. (2007) "The benefit of using SIM application toolkit in the context of near field communication applications", *International Conference on the Management of Mobile Business, ICMB*.

Madlmayr, G., Langer, J., Schaffer, C., Scharinger, J. (2008a), "NFC Devices: Security and Privacy", *Proceedings of the 3rd International Conference on Availability, Reliability and Security*, Barcelona

Madlmayr, G., Langer, J., Scharinger J. (2008b), “A Secure Near Field Communication based Mobile Payment System”, *Proceedings der 3. Konferenz Mobilität und Mobile Informationssysteme*, München

Meritt J.W, “A Method for Quantitative Risk Analysis”, [Online] Available <http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf> Accessed: September 2011

Microsoft, (2011), Windows Phone 7 [Online] Available: <http://www.microsoft.com/windowsphone/en-us/default.aspx> Accessed: September 2011.

Miller, C., Honoroff J., Mason J., “Security Evaluation of Apple’s iPhone”, *Independent Security Evaluators* [Online] <http://securityevaluators.com/files/papers/exploitingiphone.pdf> Accessed: September 2011.

NFC Forum, (2011), NFC Forum [Online] Available: <http://www.nfc-forum.org/aboutnfc/> Accessed: September 2011.

NTT DOCOMO Inc., (2011), Osaifu-Keitai – Services – NTT DOCOMO Global [Online] Available: <http://www.nttdocomo.com/services/osaifu/index.html> Accessed: September 2011.

Olsen, C, (2008), “Is contactless payment a reality for the retail industry?”, *Card Technology Today*, vol. 20, pp. 10-11

Ortiz S. Jr., (2006), “Is Near-Field Communication Close to Success?”, *IEEE Computer*, vol. 39, no. 3, pp. 18-20.

Pandya, V.R. (2008), “iPhone security analysis”, Project Report, Department of Computer Science, San Jose State University

Pasquet M., Reynaud J., Rosenberger C., (2008), “Secure payment with NFC mobile phone in the smarttouch project”, *Proceedings of the 2008 international symposium on Collaborative Technologies and Systems. IEEE*, pp. 95–98.

Pernet-Lubrano, S., (2010), “Mobile Payments: Moving Towards a Wallet in the Cloud?”, *Communications and Strategies*, No. 79, pp. 63-71.

Raento, M., Oulasvirta, A., and Eagle, N., (2009), “Smartphones: an emerging tool for social scientists,” *Sociological Methods & Research*, vol. 37, no. 3, pp. 426.

Reveilhac, M. and Pasquet, M., (2009), “Promising Secure Element Alternatives for NFC Technology”, *Proceedings of the 1st International Workshop on Near Field Communication*, Hagenberg, Austria, pp.75-80.

Satyanarayanan, M., (2003), “Swiss Army Knife or Wallet”, *Pervasive Computing*, pp.3.

Schmidt, A. and Albayrak, S., (2008), “Malicious software for smartphones”, Technical Report TUB-DAI 02/08-01, Technische Universität Berlin, DAI-Labor.

Schroder M.S. , Junge F. and Heer J., (2011), “Security through Sandboxing? - Towards more secure smartphone platforms”

- Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., and Dolev, S., (2009), “Google Android: A state-of-the-art review of security mechanisms”, *CoRR*, abs/0912.5101.
- Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., and Dolev, S., (2010), “Google Android: A comprehensive security assessment”, *IEEE Security and Privacy*, vol. 8, no.2 pp.35-44.
- Shin, D.(2009)., “Towards an understanding of the consumer acceptance of mobile wallet.”, *Computers in Human Behavior*, vol.25, no. 6, pp. 1343–1354.
- Smart Card Alliance, (2006), “Contactless Payments: Consumer Attitudes and Acceptance in the United States”, *A Smart Card Alliance and Javelin Strategy and Research Report*, [Online] <http://www.smartcardalliance.org/pages/publications-contactless-payments-attitudes-acceptance/>, Last accessed: 15 September 2011.
- Stallings W., (2005), “Cryptography and Network Security Principles and Practices”, Fourth Edition: Prentice Hall
- Tan S., (2002), “Quantitative Risk Analysis Step-By-Step”, [Online] Available: http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849 Accessed: September 2011
- Tangiloo M., Mohammad A.A., and Mohammad R.R, (2010), “Mobile Based Secure Digital Wallet for Peer to Peer Payment System”, *International Journal of UbiComp*, vol.1, no.4.
- Tomlinson, A., Yau P.W., MacDonald J.A, (2010), “Privacy threats in a mobile enterprise social network”, *Information Security Technical Report*, vol. 15, no. 2, p. 57-66
- Töyssy, S. and Helenius, M., (2006), “About malicious software in smartphones,” *Journal in Computer Virology*, vol. 2, no. 2, pp.109-119.
- Varshney U., Mobile payments, *IEEE Computer*, vol.35, no.12, pp. 120–121.
- Vaughan-Nichols, S. J., (2003), “OSs battle in the smart-phone market”, *Computer*, vol. 36, no. 6, pp. 10-12.
- Venkataramani, G. and Gopalan S., (2007), “Mobile phone based RFID architecture for secure electronic payments using RFID credit cards”, *Proceedings of International Conference on Availability, Reliability and Security*, pp. 610–620, Vienna, Austria, 2007.
- Walker, W., (2010), “Mobile telephony security compromises”, *Information Security Technical Report*, vol. 5, no.3, p. 134-136.