Independent project (degree project), 15 credits, for the degree of Bachelor of Science (180 credits) with a major in Computer Science
Spring Semester 2020
Faculty of Natural Sciences

Near Field Communication

Security concerns & applicable security in Android

Filip Bengtsson
Matteo Madrusan

Authors
Filip Bengtsson, Matteo Madrusan

Title
Near Field Communication - Security concerns & applicable security in Android

Supervisor
Eric Chen

Examiner
Qinghua Wang

Abstract
Near Field Communication (NFC) is being used more frequent in smart devices, this raises security concerns whether the users information is secure from attackers. The thesis examines the threats that NFC on Android smartphones are exposed to, its countermeasures, as well as existing protocols that ensures the integrity and confidentiality of the users data. The results were achieved by a literature study, a questionnaire sent to companies that create products related to the subject as well as an experiment that was divided into two parts. The first part examined what information can be extracted from a debit card stored on an Android smartphone. The second part included a relay attack in which a purchase would be made with a victim's debit card by using Android smartphones. The results shows that it is difficult to conduct any attack on the smart devices because of the limited range of NFC as well as the protocols available for making purchases with debit cards stored on smart devices disallows unauthorized applications and hardware to attack cards stored in smart devices.

Keywords
Near Field Communication, Active NFC, Security Protocol, Security Exploit, Standard Security Protocol, NFC Attack Countermeasures

Table of Content

1. Introduction

1.1 Background

Near Field Communication (NFC) is a technique that has become popular to use on a daily basis for people around the world. There are several different ways in which NFC can be used, the most common way being payments from smartphones, physical contactless credit cards and tags for unlocking doors. Smartphones using NFC technology are called active devices as they can both read and exchange data with other compatible devices, while cards and tags are passive NFC devices as they can only be read from by other NFC devices [1]. NFC is a technology that is built upon the older Radio-Frequency Identification (RFID) technology, both uses radio frequency in order to transmit data to the receiving device. However, NFC is better suited for mobile devices than RFID [2]. In a survey conducted by Internetstiftelsen, together with banks such as Länsförsäkringar and Skandinaviska Enskilda Banken in 2017, 1000 people in Sweden were asked how often they use certain payment methods. While the majority of participants used a credit- or debit card on weekly basis, a quarter of the participants also used mobile payment methods [3]. However, 2017 was the year both Samsung Pay and Apple Pay was introduced in Sweden, which shows that mobile payments caught on quickly and according to the survey, the trend shows that it is steadily increasing. Although NFC is widely used in different contexts, the devices that uses NFC might be exposed to several threats and attacks since there is an absence of a standardized security protocol [4]. Wang [5] argues that a high-level protocol might endanger the user's information, in Wangs findings he refer the problem with a high level protocol being that it could be used by criminals in order to generate breakthroughs. Another thesis, conducted by Malmberg and Söderberg [6], researched which information can be extracted from credit card that uses NFC. [2]

However, the thesis only studied the passive form of NFC devices. The major difference between the active and passive devices is that the active are always usually connected to the Internet which exposes the active devices to different threats than the passive. This thesis will therefore focus on the active NFC devices such as smartphones, as the devices

can store several different credit cards and tags on it. The work will also on whether it is possible to extract the same information on active devices as to their passive counterparts and exploit it.

1.2 Current Payment Standard

There is currently a standard used for contactless payments which both active and passive devices must follow. This standard is called Payment Card Industry Data Security Standard (PCI DDS) [7]. This standard is enforced and businesses that stores, transmits, accepts and processes cardholder data must follow PCI DDS. For active NFC devices, this means that the full card information is never directly stored in the devices but tokenized which means that the credit card information is always verified by the cardholder's bank.

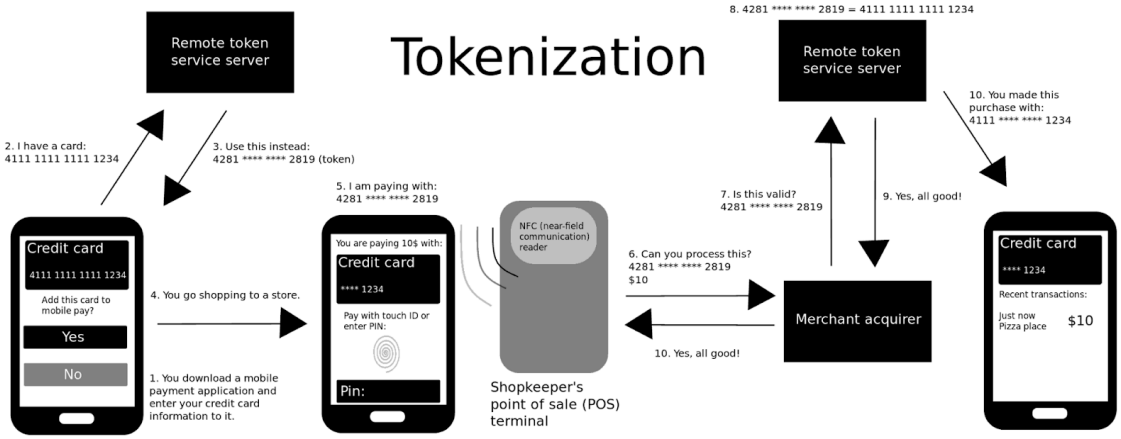

Figure 1. *Simplified version of mobile payment tokenization* [8].

As seen in Fig 1. the active NFC devices does not hold the actual cardholders card information but a token of it. However, the danger lies in whether the attacker can still use this token and exploit it to harm the confidentiality of the cardholder's card.

1.3 Problem Statement

As the availability and usage of NFC tags and cards increase, users are seeking out for solutions to hold these passive devices in an efficient and practical way. Some have even resorted to planting a chip into their body [9] [10]. Even though this is possible, the availability of creating applications that can store different NFC tags and cards has also

increased which reaches the natural conclusion that in a near future, more tags will be stored on mobile devices for the sake of practicality. Therefore, this thesis will focus on what could be extracted from an active NFC device such as a smartphone in which a passive card is stored, in this case a debit card. As the card should hold a high standard of security, the purpose is to examine if this still can be exploited, as well as researching the different security threats that active NFC devices are exposed to. Ultimately, creating a picture of how vulnerable the integrity and confidentiality of the user's information is in active NFC devices.

1.4 Research Questions

The three research questions below are the focus of this thesis.

Question 1: What information can be extracted from the communication between two active NFC devices?

When two active NFC devices exchanges information, what information can be extracted and is there a way for attackers to exploit the information for personal gain

Question 2: What threats and attacks are active NFC devices exposed to and are there any countermeasures for them?

Even though active NFC devices has the possibility to implement their own security, they are still exposed to threats when doing the data transmission between each other. What threats and attacks are the devices exposed to and how can they protect the integrity and confidentiality of the data?

Question 3: Are there any current protocols to ensure the integrity and confidentiality of the data being transmitted between active NFC devices?

Integrity and confidentiality are important within the area of data security. This is to protect the users from their personal information to be exploited. Is there any current protocol that ensures this, if yes, how is it secured or if no, why does not a protocol as such exists?

1.5 Limitations

There are some restraints and limitations for the thesis. Firstly, both authors have never dealt with NFC previously on a technical level such as programming as well as researching it before this. However, the authors will conduct this research as their degree thesis to receive a bachelor's in computer science and therefore has previous experience with conducting a thorough research on this topic. Time is of the essence and therefore the thesis will not be able to go into depth as there is a time plan to follow with crucial deadlines. This is the greatest limitation as there is a need for an in-depth research of active NFC devices and its security. This work also focuses on the security amongst active NFC devices such as smartphones, the reason for this is that the experiment that will be conducted during the thesis is based on phones that have access to NFC to be able to understand what information what that can be extracted from the communication between two devices and sent over to a third party using a relay attack. This removes the research that can be conducted on passive devices which currently is most of the NFC devices used and therefore limits the depth of the thesis.

2. Methodology

There will be three different methods to extract as much information as possible. It will have a theoretical part which revolves around a literature review in which different academical sources will be used to better understand the implications of some of the current threats. This will be completed together with a questionnaire in which different companies that creates NFC solutions will answer a couple of questions about NFC implementation and protocols. Lastly, a practical part will also be used in the form of an experiment. This will allow the authors to understand what information can be extracted from active NFC devices.

2.1 Literature review

The purpose of this method is to be able to answer research questions 2 and 3. The literature study is important to have in this work in order to gain knowledge and better understand NFC and how it is implemented in different ways and the different threats that can occur. Using the literature review, the areas in how different strategies for security work or do not can be studied. This means that the literature study can be used in answering all three research questions presented above, making it the most important methodology which will be highly focused in order to understand NFC.

The strategy for the literature research is to find scientific articles and works that gives a deeper understanding in the subject of NFC and the way the protocols are built. There is also an importance in the articles and work being peer reviewed to make sure the authenticity of the references in the work to make sure there are no errors in the work. The articles gathered has been taken from ACM Digital Library which has been accessed through Kristianstad University (HKR) website and Google Scholar. The keywords being used when searching for the articles have been NFC, Near Field Communication, security, standard, protocol, exploit, active.

2.2 Questionnaire

The questionnaire will be used by the authors to be able to gather information from different companies that sells and creates different NFC solutions. This will create a broader understanding of how these companies handles the security surrounding the technology and if there are any specific protocols that they may or may not follow. The questionnaire will complement the answer in research question 2 as well as answering question 3. It consists of six questions:

1. What precautions do [company] take to ensure the security of the customers that uses NFC devices?

2. How do [company] implement NFC in their devices and what protocols do they follow?

3. What is the general idea behind [company]'s NFC solution?

4. What differs [company]'s solution from other competitors and what makes your product the superior?

5. How do [company] develop its security protocols for NFC?

6. Is there any reason to collaborate with other companies to develop a standardized security protocol?

2.2.1 Question Motivations & Design

The reasoning behind the questions is to allow the companies, that are willing to participate, to thoroughly explain how they process the possible security threats that the NFC devices the company is dealing with. By this, the authors will hopefully be able to answer the whether or not they ensure that the users information is secure. This by both expecting threats that can cause the integrity and confidentiality of the NFC devices to be intact. Furthermore, it might also answer as to why Wang's [3] conclusion that a high-level protocol could do more harm than good and the best way to protect the device from threats is through low-level security.

The general idea behind the design of the questionnaire is to give more insight on companies that provide NFC solutions are implementing security into their devices and solutions as well as actively ensuring that their devices are secure and able to countermeasure some attacks.

2.2.2 Ethical Perspective

The questionnaire will be sent to a couple of companies that the authors seem fit in the context of the subject. An inquiry is first sent to the companies that if they are interested and willing to participate. The context of the questionnaire is explained in the inquiry and the companies are aware that the questions will be used in a thesis. If the company want to participate, they will be sent the questions. The questions above can be difficult to answer for some businesses as the questions can give an incentive to include sensitive information that the company does not want to be spread outside of itself. Therefore, when the company receives the questions, they are freely to not answer those questions that they do not seem to be fit to answer.

2.3 Experiment

The experiment will be divided into two different parts. The first will handle the extraction of information between two active NFC devices, this will allow the authors to answer research question 2. This will be done by a smartphone reading a digital card stored in another smartphone. This is to identify what information can be extracted and comparing the result with the thesis previously conducted by Söderberg and Malmberg [6].

This part of the experiment will include:

- Two Android smartphones
- A computer running Android studio
- A USB cable

As seen in the list above, the experiment itself is a modification on the tests previously done by Söderberg and Malmberg [6]. However, this will include the tokenized version of the card uses that is stored in the smartphone following the PCI DDS.

The second part of the experiment includes whether an attacker is able to read a victim's card and purchase something with the information extracted from the victim's card. This will firstly be tested with active NFC devices but will also tested with passive ones. Below is a simplified figure of how the attack would be conducted.

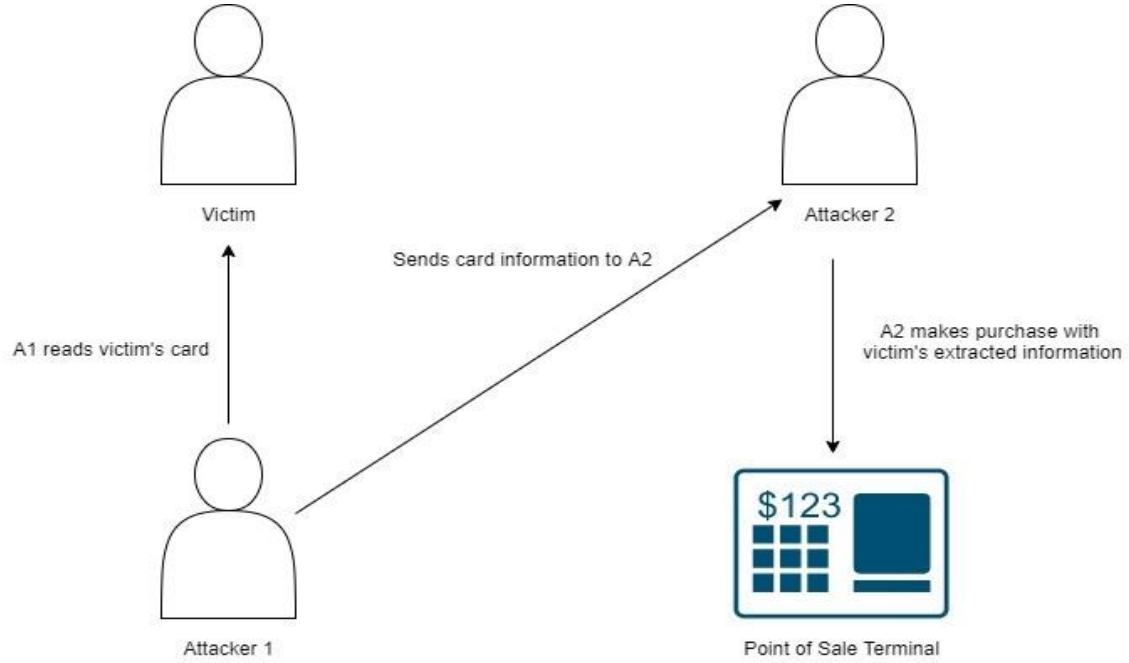

Figure 2. *Simplified figure of how the relay attack will be conducted.*

This part of the experiment will include the following:

- Three smart devices
    - 2 amongst them must be Android smartphones which will be the attacker's devices
- A computer running a Java server for the communication between the attacker's devices
- A credit-or debit card
- A Point of Sale Terminal

To further explain how the attack will be conducted. The victim in this case will have his or her card available through the smart device, which will have all authentication removed and the card will be in a passive mode which attacker 1 (A1) can read. A1 will then send the extracted information through the server to attacker 2 (A2), using simple packet forwarding, in which A2 will then try to make a small purchase with the extracted information.

2.3.1 Ethical Conundrum

The first part of the experiment does not have any ethical issues itself except from not allowing the information of the victim's card information to be used in any public setting except from verifying the result in comparison with Söderberg and Malmberg [6]. However, the second part of the experiment can have greater ethical issues if the result would show that it is possible to exploit the victim's cards in a relay attack. Therefore, if the experiment is somewhat successful, the source will not be available to the public as it can issue great consequences for users of different NFC devices. However, the dilemma lies in the result of the experiment as the authors should verify that there is a possibility to execute a relay attack but not in such a manner that someone can use it to exploit users of NFC devices in the future.

3. Literature Study

3.1 Basics of Near Field Communication

NFC is a communication technique that has gained popularity during the recent years. NFC can be seen in smartphones or other devices such as tags and credit cards. NFC operates at 13.56 megahertz and can transmit between 106 kilobits per second and 424 kilobits per second. The NFC technology has a very limited range in which it can operate which is normally up to maximum 10 cm. There are two different types of NFC devices, these are the passive, such as tags, and active, which are often smart devices. Two passive NFC devices cannot communicate with each other since the passive devices do not have power supply on their own, while the active devices have their own power supply and can create a Radio Frequency (RF) field on which the passive devices can get powered by in order to work. Having a smartphone as an active device means that it can also work as an passive device as well switching in between reading or writing data [4]. The passive device can be read by any active device.

The NFC technique allows three different types of communication between the devices which can depend on how the device is programmed. The active NFC device can use all three communications when operating. The first one is when the active device is acting as a credit card, it takes on the role of a passive device and does not produce a RF field on its own and instead awaits data from an active device and then sends back the response as a normal credit card would which has NFC implemented.

The second type of communication is when the device is active and is looking for passive devices in which it can send data to.

The last form of communication is called peer-to-peer, this is when two active NFC devices that can switch between active and passive work together. one of the devices will go into the active mode while the other is in the passive, they then alternate between the modes in order to send the data. The device that first initiated the connection is called the initiator and the receiving device is called the target [4].

3.1.1 Application Layer Data Protocol

When two different NFC devices communicate, whether they are active or passive, the devices follow the same protocol, Application Protocol Data Units (APDU), to identify what the data units represents. APDU consists of two different types of data units, command, and response. When two devices communicate, one of the devices must send an APDU command to be able to receive any data from the other device, in form of a response. The figure below explains the structure of a command:

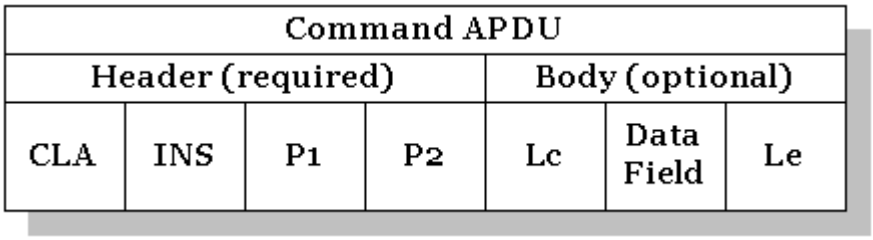

Figure 3. *APDU command data unit.* [11].

The header is divided into four parts and the body three. Further specifications on the APDU command:

- CLA
  - Class byte
  - 1 byte
  - Indicates the type of command
    - Interindustry (ISO 7816-4)
    - Proprietary
- INS
  - Instruction byte
    - Specifies which specific command will be used
  - 1 byte
- P1 and P2
  - Command specific parameters
  - 2 bytes
    - 1 byte each
- Lc
  - Specifies N length of command payload
  - 0 - 3 bytes

- Data Field
    - Command payload
    - Length specified as N in Lc
- Le
    - Specifies N length of APDU response
    - 0 - 3 bytes

To further explain the class byte (CLA), it can contain interindustry specific classes in compliance with ISO 7816-4. However, proprietary classes are used in specific cases depending on the implementation. The APDU response is structured as such:

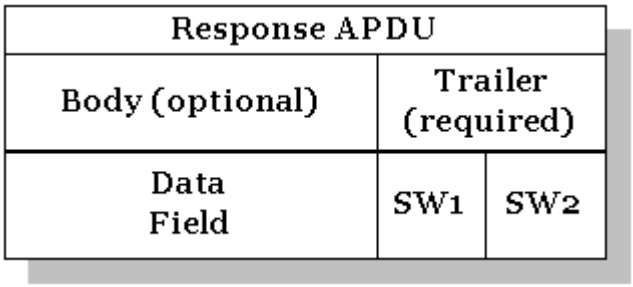

Figure 4. *APDU response data unit.* [11].

As shown in Fig 4. the response is divided into two different parts. Further explanation of the APDU response:

- Data Field:
    - Data returned depending on the INS
    - Length specified in Lc in APDU command
- SW1 and SW2
    - Status word
        - Return status on whether the command was successful or other statuses depending on different circumstances
    - 2 bytes
        - 1 byte each

3.2 Security Threats

3.2.1 Man in the Middle

The man in the middle attack is when an attacker manages to intercept the messages being sent between the devices being targeted. In order for the man in the middle to work the attacker cannot be seen by any of the targets. This makes the devices to believe that they are communication with each other when they are not. When the devices then set up their encryption the attacker will be in the middle receiving all the keys. Both devices targeted believes that they are talking with each other when in fact they are both communicating with the attacker that is now in control of the entire communication [4].

The man in the middle attack is however weak against NFC devices since it is very difficult to make it successful. The attacker needs to be close enough to receive the messages that are sent from the devices which means that the attacker needs to get very close the targets because of the way NFC operates. This fact makes the man in the middle attack incredible hard to pull off making it a low threat for NFC devices [4].

3.2.2 Eavesdropping

NFC is a communication that is contactless, this means that it can be targeted by malicious attackers in order to try to get what information is being sent between devices, radio frequency waves are being used when two NFC devices are trying to send data between each other which gives an attacker the opportunity to listen in on the transmission using a receiver like an antenna [5]. Since there is no built-in protection against the eavesdropping attack, data that is being sent needs to be encrypted on an application-level to be able to add security. This means however that the security protocols towards eavesdropping might vary highly depending on the groups of developers implementing the protocols [4].

Since it is difficult to execute a man in the middle attack against NFC devices it makes encryption more secure than it can be on other platforms, it is important however that the developers for the programs using NFC have knowledge on the fact that NFC does not have an implemented encryption and therefore implement a secure system to ensure safety for the users so that eavesdropping becomes less of a threat. The protection against

eavesdropping is also stronger for communication between passive and active NFC devices. This is due to the fact that the passive tags do not transmit and instead awaits the transmission from the active device giving the eavesdropping the range of about a meter. For the communication between the active to active NFC devices the range for eavesdropping is up to about 10 meters. The range for eavesdropping can however vary for different reason like the equipment of the attacker, signal strength of the NFC devices and the way the attacker's antenna used for the eavesdropping [4].

.

3.2.3 Transmission Interference

Transmission interference can occur when information is being transported, during this time the data might be picked up or corrupted. This means that transmission loses efficiency when sending the data to the receiving device. In order for the an attacker to interfere with the original signal the interference signal should be sent on the same broadcasting channel as the communication is being sent on [12]. This can lead to that the interference signal getting added to the correct transmission data resulting in exceptions being thrown on the devices communicating [5].

3.2.4 Data Modification

Data modification is in the same category of attacks as data corruption, but it has the big difference of the data still being able to be read by the NFC devices while the data corruption cannot be read. This is an incredible difficult attack to be able to succeed with since it requires the attacker to manage to transmit a RF signal that perfectly overlaps the receiver of the NFC device that initially was used for the communication. This makes the attack almost impossible since the requirements for the attack to succeed would require that the attacker and NFC device that sends data would have their transmissions reach the receiving NFC device at the exact same time giving the attacker a waveform that the attacker then needs to be able to calculate in order to be able to send their own message to the device and this message needs to be sent almost at the same time as the first transmissions reach the receiver in order for the attacker to create a pause in the communication [4] [12].

The best way to avoid the data modification attack would be to establish a secure channel. The reason for this is since NFC works by being in very close proximity of each other making the man in the middle attack almost impossible to achieve. Haselsteiner and Breitfuß [12] mentioned the unauthenticated version of Diffie-Hellman (DH) works perfectly for this purpose. The DH is a way to exchange session keys with each other over a public channel, the DH was the first algorithm that was shared using public-keys [13]. It can be seen as one of the main foundations for the theory and practice of cryptography. DH has a downside of not being very secure about man-in-the-middle attacks [14], however for the purpose of security for the avoidance of data modification on NFC devices, it would be sufficient for the reason that man-in-the-middle is near impossible to achieve on NFC devices. The key that gets created and shared can function to obtain a symmetric key for Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). With this key a secure channel can be established which can provide confidentiality, integrity, and authenticity to the data being transmitted between the devices [12].

3.2.5 Relay Attacks

Even as NFC devices are limited in their practical range of communication, they do however suffer from being exposed from relay attacks. As previously mentioned, the relay attack must include three parties: a victim and two attackers. The first attacker will read the victim's card from a close proximity, this attacker is also known as a mole [15]. The second attacker will receive transaction details from a Point of Sale (POS) terminal and forward it to the victim's NFC device through the mole. The response generated by the victim's device is read by the mole and forwarded to the second attacker, which then makes a purchase on the POS terminal [15].

However, for most active NFC devices, such as Android and Apple smartphones, the security measures are extended beyond the card emulation application. Manufacturers of the smart devices usually apply different types of security to large parts of their software. Secure technology such fingerprint scanning and face recognition are applied as well as passwords and pin numbers. Therefore, for most active NFC devices there are multiple layers of security that locks the tokenized cards which minimizes the possibility of a relay attack. However, the scenario still stands if a mole has access to an NFC device with open

tokenized cards, the relay attack can be used to exploit said card. This has previously been tested and deemed successful [16].

3.2.6 Point of Sale Security Risks

POS systems are usually built as any other general-purpose computers and the operating systems (OS) are usually based on general purpose OS such as Windows or, if Unix based, Linux [17]. Therefore, the POS systems are exposed to the same threats as the OS it is based on. As there is an array of attacks that such systems can be exploited by, the one that can do the most harm to users are attacks which steals payment card information from POS terminal through keylogging Trojans to extract password-hash, replaying login sequences or by using brute force [17] [18].

Other attacks that may be a threat POS system are packet-sniffing software as well as infiltration with database injections [17]. The infiltration attack uses injections through the external systems of a corporation to be able to reach a device within the corporate web server. This way, the attacker gains access to different parts of the network and could then exploit it by using packet-sniffing software as well as other malicious software [17]. The attacker could also orchestrate a spear-phishing attack towards different people within the corporate network to install malicious backdoor software on the victim's computer [17]. Furthermore, packet-sniffing could also expose secret personal information if the point to point encryption is weak in the POS system. The data transmission is protected using secure sockets (SSL), which encrypts the packet on the network level [17]. However, if the SSL cipher is weak, the packet's payload may be picked up by a packet-sniffer and having the data exposed to the attacker. Which break the confidentiality of the users data. To countermeasure this, the POS terminal does need to take the same security measures as other computers such as malware identification software amongst other measures. Therefore, the measures do not need to be more advanced as the terminals is another type of a computer.

3.3 Current Security Protocols

NFC does not have a standard security protocol to be used whenever and wherever implementation of it takes place, there are however protocols that are being used as standard on different devices for payment when it comes to NFC. One of these standards is the PCI DDS standard that was mentioned above in section 1.2, this is a standard that is used for smartphone payments using NFC and not any physical cards [7]. The experiment conducted in this thesis that has the goal of testing whether a relay attack could be possible to be able to extract information from a smartphone and be used by the attackers to make a purchase is going through this specific protocol since it is the standard for smartphones.

Another standard that is being used for another set of devices is the Europay, Mastercard, and Visa (EMV) protocol. This standard is used for credit and debit cards and can be used for contactless payment at an NFC device. It was developed by EMVCo which was established by several of the biggest companies within credit cards such as Visa, Mastercard and American Express. The goal for EMV was to create a standard way around the world to make transactions secure when using payment cards that were chip-based as well as point-of-sale, the standard is built upon the ISE/IEC 14443 standard [19].

Upon these protocols, EMVCo oversees all devices and application that is compatible with EMV cards. This is done by applying for a certificate in which EMV tests the product. If the product testing is successful, the company applying for a certificate must then pay for the certificate which then has to be renewed every year or every other year. Below is a figure how the acceptance process works for Kernel IDs:

Figure 5. *EMV certificate process* [20].

This allows the application to publish its ID to the EMVCo database to allow EMV accepted POS terminals to communicate with the application. EMV provides specifications for APDU commands and responses as well as specifications for encrypted communication. This allows the POS terminals and other EMV certified hardware to disallow communication with uncertified applications and hardware. This enhances the security for smart cards stored in Android devices which as all information stored that is not public cannot be access by an uncertified application or hardware.

4. Result

4.1 Literature Study Result

The literature study has been able to provide insight into the function of the NFC devices and how they work, the literature review helped answering research question 2 and 3. It also gave the information about how some protocols are implemented and the differences on how the three different ways the NFC devices communicate which are card emulation mode, reader/writer mode and peer-to-peer. In answering research question 2:
What threats and attacks are active NFC devices exposed to and are there any countermeasures for them?

During the literature review it can be found that there exist several types of attacks against active NFC devices that can be utilized by people with malicious intent. But it is also learnt that some of these attacks are not very strong against NFC, thanks to the nature of the way NFC operates, one example of this is the man-in-the-middle attack, this attack has little ground to be of any major threat towards NFC and as such makes it easier to create security against other types of attacks since the man-in-the-middle being a very low threat. It is discovered that one of the best approaches towards security on NFC is encryption and since NFC does not have encryption implemented on its own it is up to each developer to make sure that a good algorithm for this is used.

Eavesdropping is another attack that needs to be taken into consideration, while NFC communicates via short distances up to 10 cm, someone could actually stand farther away and listen into the communication using an antenna which could be performed depending on gear up to 10 meters away when communication is done between active to active NFC devices, it is however much shorter for communication between passive to active around 1 m since the passive device gets powered by the active once it is close enough. Since the range for eavesdropping can be so far it is important to encrypt the data so that if someone is eavesdropping the attacker should not be able to know the content of the data.

An attacker does not need to try to read the data sent between the devices in order to be a threat, if the attacker decides to try and disturb the communication a transmission

interference attack could be performed. This is a try to send signals on the same broadcasting channel as the original transmission and might corrupt the data so that errors occur and the data being unreadable.

The data modification attack is an attack where the attacker wants to change the content of the data but it is still readable by the NFC devices, this attack was found out to be incredibly difficult to pull off since it requires precise timing from the attackers side in such a way that the attackers data reach the receiving NFC device at the same time as the original data does so. In order to create additional security in the matter it is proposed by Haselsteiner and Breitfuß [12] to use a public-key algorithm called Deffie-Hellman to create a secure channel on which communication is performed.

The relay attack can have devastating consequences for the victim if not proper security has been implemented. Protocols such as PCI DDS as well as the certification process and specifications provided by EMV. These protocols do increase the integrity and confidentiality of the data being transferred with NFC. However, without proper security implementation, the relay attack can cause much damage towards the victim such as leaking personal information. The possibility to set up such an attack does not take much preparations as the attacker does not need to properly understand the data being transferred but the what the purpose of the data is.

POS terminals have the same type of security risks as regular personal computers (PC). Therefore, it can be affected by a large array of attacks. However, similar countermeasures that are implemented on OS for PC can be implemented on POS terminals as they are often based on Windows or Unix which already has countermeasures available.

However, most of these attacks can be countered with the EMV. EMV provides security specifications and certificate for each application and hardware model, which disallows uncertified hardware or applications to gains access to the communication channels used. The acceptance process includes testing in which the product reaches the security criteria set by EMV. This ensures that the product can withstand the previously mentioned attacks.

Research question 3:

Are there any current protocols to ensure the integrity and confidentiality of the data being transmitted between active NFC devices?

It was discovered early during the thesis that NFC devices does not have any built in layer of protection on its own and that it is instead up to the developers for the applications that are using the NFC devices to implement their own security like encryption and establishing secure channels where data can be transferred in a secure way and that there is no standard protocol for how this is implemented. It was however also discovered that there are in fact two standard protocols for payment transactions, PCI DDS and EMV.

The PCI DDS protocol is used in order to make sure that the physical card is not stored on the device and instead stores the card information on a remote server, this server gives the user a token that is connected to the credit card and when performing payments that token is then used by the POS terminal to see if it is valid by checking with the server. If the token is valid the transaction continues. The token that is generated will also change between each payment session giving it high security. The token only contains public card information, it can still be discussed whether that might be sensitive information if an attacker would be able to get a hold of it.

EMV provides a great layer of security for hardware and applications. Each hardware model and each application are provided with its own certificate which has to be reapplied for and renewed every other year. This ensures that the products security is always up to date. Furthermore, EMV provides the products with security specifications which states how the secure messaging should be set up and used. This provides the a proprietary CLA byte in the APDU command to ensure that the data and channel is secure. Therefore, the confidentiality of the data is secured by the security specifications provided by EMV. The confidentiality as well as the integrity is then further secured by disallowing uncertified products to communicate with certified products.

4.2 Experiment Result

4.2.1 Data Extraction from Active NFC Devices

The first part of the experiment tried to extract information from an active NFC device. It was also meant to answer research question 1:

What information can be extracted from the communication between two active NFC devices?

This part of the experiment was successful. An active NFC device in form of an Android smartphone was able to read data from a debit card stored in a different Android smartphone. However, the data that could be read was only the public data that can be accessed such as the debit card manufacturer, which in this case was Visa. The command used for the experiment was a hex string which was converted to a byte array upon transmission, it was structured as such:

Table 1. APDU command used for the experiment.

CLA	INS	P1	P1	Lc	Payload	Le
00	A4	04	00	07	A0000000031010	00

Further explanation on the specific parts of the command:

- CLA
  - Indicates that there is not any secure messaging involved.
- INS
  - Select file command
- P1
  - Select file name stated in payload
- P2
  - Return first record by payload name
- Lc
  - Length of payload
- Payload
  - Name of file to be found

        - In this case, the named if specified for Visa cards
            - For Mastercard cards: A0000000041010
- Le
    - Length of response
        - Left empty to receive a response with a non-specific length

The response from the command in Table 1:

Table 2. APDU response received.

Response Body	SW1	SW2
6F718407A0000000031010A566500A5669736120446562697487019F38369F66049F02069F03069F1A0295055F2A029A039C019F37049F01069F09029F15029F160F9F1C089F1E089F33039F35019F39019F4E205F2D027376BF0C169F5A053107520752BF6304DF2001809F0A0400010101	90	00

Further explanation of the key words in the response, which are highlighted in red and blue:

- 6F – File Control Information (FCI) Template
    - 84 – Dedicated File Name
        - A0000000031010 – Name of file
    - A5 – FCI Proprietary Template
        - 50 – Application Label
            - 0A56697361204465626974 – V i s a D e b i t
        - 87 – Application Priority Indicator
        - 9F38 – Processing Options Data Object List (PDOL)
        - 5F2D – Language Preferences
            - 7376 – s v (Swedish)
        - BF0C – FCI Issuer Discretionary Data
            - 9F5A - Unknown Tag
            - BF63 – Unknown Tag
            - 9F0A – Unknown Tag

The response only shows public information that can be accessed through the card, however, the data that is being read from the smartphone is different from the actual card. The first reason is that the card being stored in the smartphone is only a token of the physical card. Secondly, the card token is reset after every purchase. Which results in if the card on the smartphone was read, used for a payment and then read again, the read result would be different each time except for the some of the bytes such as file name among other. The APDU response is structured in the same way as explained in Malmberg and Söderberg [5], in which a physical card was used instead. The public information can be accessed, and the response includes the same public information, however, the public information differs on the smartphone as it depends if the card was read between purchases. As seen in the list, the response includes public information such as template used for the response, the preferred language as well as the what application will be used. PDOL includes other public information such as amount for a transaction, transaction date amongst other variables that are necessary for a transaction without displaying any actual card information.

4.2.2 Relay Attack

The second part of the experiment was not as successful as the first part. The tests were not successful in the context of the execution as the experiment could not be properly executed, however, it demonstrated the security measures taken by EMV certified products. Initially, the communication between the two different smartphones was set up and tested in the same way as in the first part. The smart device which read the card was successfully able to send data to the second device through a remote server. However, the purpose of this experiment was to test it on an EMV certified POS terminal, which it was tested on. When including the EMV certified POS terminal, A2s smartphone was not able to receive any data from the POS terminal. An explanation for this is that the application used for the attack was not EMV certified and did not include an ID that the POS could recognize and therefore did not send any information to A2s smartphone. The communication was able to be set up and worked properly, however, the APDU command that A2 in Fig 2. should have sent to A1 was never received. Therefore, A1 was never able to extract the data from the victim’s card application. The security of EMV certified products disallowed the relay attack to exploit the victim's card. Even though previous experiments [16] has shown that this sort of attack is possible, the EMV security standard

has developed since then, showing that a certification is necessary for such of an attack to be successful. Therefore, the experiment was successful in the sense that it showed the security implemented in EMV systems and the difficulty of exploiting it.

4.3 Questionnaire Result

The questionnaire was sent to 5 different companies, in which one was willing to take part of the questions. However, answers on the questions was never received. Therefore, there questionnaire does not have any results which the thesis can take part of.

5. Discussion

5.1 Result Discussion

As the results show in the experiment, an NFC reader or smartphone devices with NFC can easily extract the public information from a card stored on a smart device. However, the results also showed that the line drawn there as it is not possible for an uncertified application to exploit sensitive card information. This is ensured by the certification provided by EMVCo and their security specifications that gives the product manufacturers to implement secure communication channels as well as secure messaging. This allows the product to withstand attacks such as relay attacks as the application used to attack has to be certified by EMV, in which by moral standards, would not accept such an application which could ultimately harm their users in form of Visa and Mastercard cards. This was further showed in the second part of the experiment which a relay attack was unsuccessful. As stated in the literature study, the reason for this was that the application used to receive the data from the POS was not EMV certified while the POS terminal was, otherwise, the POS would not be able to make purchases with Visa and Mastercard cards. The communication security between a POS terminal and an active NFC is also secured by the EMV specifications. However, this leaves the idea whether such of an attack would be possible if both the POS terminal and the card application are certified by EMV. This would work as other known applications such as Google Pay, however, it is then up for discussion if such an application would be pass the EMV certification process as the intention of such an application is to do harm.

The POS terminal itself has other security threats that are similar to PCs, however, the OS used is often based on either Windows or Unix. This allows the terminals to implement available tools common to these OSs to counter major types of attacks. However, as the terminal is connected to the internet, it is exposed to packet-sniffing as well as DDOS attacks.

Some of the attacks performed against the NFC devices were proven to be difficult to be successful with especially the man-in-the-middle attack since NFC devices operates in very close proximity from each other. Since this attack is a low threat developer can then use different forms of security that otherwise might have been exposed to this attack to counter other attack types on NFC.

The eavesdropping attack is something that can be used to access sensitive data and it is recommended to have encryption so that no sensitive information can be read by an attacker. Even though NFC operates in short distances like 10 cm an eavesdropper could be able to listen into the transmission up to 10 m away depending on the type of communication between the devices using an antenna.

Transmission interference a possibility for the attacker to disrupt the signal that is sent and might be used by an attacker to create difficulty in sending and receiving information from the NFC devices since the attackers signal interfere on the same broadcasting channel as the original transmission.

Data modification is one of the more difficult attacks to pull off since it required the precise timing of the attacker to be able to add the attacker's own data to the transmission data. Establishing secure channels helped in preventing this type of attack.

5.2 Future Work

The experiment conducted in this thesis has only been limited to relay attacks against the active NFC devices, however it would be interesting to see whether a more technically difficult attack would be able to succeed with a good rate of succession. It is clear from the results that the data modification attack is hard to execute, creating a scenario where the transmission data from the NFC devices get modified and then read on the other end would be very interesting in seeing how and which data in the transmission can be changed and manage the attack so that it would result in a data modification. For easier achievement this could be done using an application that does not use any encryption and would not necessarily have to perform any sort of payment since the EMV protocol would make the data modification difficult to execute.

6. Conclusion

The thesis finds that it is possible to extract the same data from a card stored on a smart device as the physical card. The card information extracted from the smart device is a token of the physical card, this follows the guidelines set by PCI DDS which are a requirement by the banks that issues the debit/credit cards. Upon a purchase, the token is then restored and a new one is stored in the smart device. The NFC security for Android smartphones are dependent on the security applied to the application using it as a form of communication. For purchases with the most common card manufacturers such as Visa and Mastercard, the product that want to be able to read and use such cards must be certified and follow the security specifications provided by EMVCo. The NFC on Android devices is secure in the sense that it is difficult to execute any kind of attack as the limited distance for NFC to react to readers or writers allows the communication to be secure.

In conclusion, NFC communication on Android devices as well as on other smart devices is secure which makes it difficult for attackers to exploit sensitive information transmission in any way using NFC.

7. References

1. Square, Inc. *How NFC Works*. [Online].; 2015 [cited 2020 Mars 23]. Available from: http://nearfieldcommunication.org/how-it-works.html.

2. Broll G, Keck S, Holleis P, Butz A. Improving the accessibility of NFC/RFID-based mobile interaction through learnability and guidance. In *MobileHCI '09: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*; 2009; Bonn. p. 1-10.

3. Insight Intelligence AB. *Sverige Betalar 2017*. [Online].; 2017 [cited 2020 Mars 22]. Available from: https://internetstiftelsen.se/docs/sverige-betalar-2017.pdf.

4. Nelson D, Qiao M, Carpenter A. Security of the near field communication protocol: an overview. *Journal of Computing Sciences in Colleges*. 2013 December: p. 94-104.

5. Wang Z. Information Security Vulnerabilities of NFC Technology and Improvement Programs. In *ICISS '18: Proceedings of the 2018 International Conference on Information Science and System*; 2018; Jeju. p. 196-199.

6. Malmberg A, Söderberg S. *Security of Contactless Payment Cards*. Kristianstad: Högskolan Kristianstad, Faculty of Natrual Science; 2019.

7. Visa. *PCI DSS compliance*. [Online].; 2020 [cited 2020 Mars 20]. Available from: https://www.visa.se/partner-with-us/pci-dss-compliance-information.html.

8. Keministi. *Tokenization (data security)*. [Online].; 2018 [cited 2020 Mars 20]. Available from: https://en.wikipedia.org/wiki/Tokenization_(data_security)#/media/File:How_mobile_payment_tokenization_works.png.

9. Mårtensson R. *Ökat intresse för att sätta in mikrochip i handen*. [Online].; 2018 [cited 2020 Mars 20]. Available from: https://www.svt.se/nyheter/inrikes/stort-intresse-for-att-chippa-sig-i-handen.

10. CHIPSTER. *Chip i handen*. [Online].; 2020 [cited 2020 Mars 20]. Available from: https://chipster.nu/artiklar/chip-i-handen.

11. Ortiz EC. *An Introduction to Java Card Technology*. [Online].; 2003 [cited 2020 May 06]. Available from: https://www.oracle.com/technetwork/articles/java/javacard1-139251.html?printOnly=1.

12. Hasensteiner E, Breitfuß K. Security in Near Field Communication (NFC). In *Workshop on RFID Security 14 Jul 2006 conference*; 2006; Graz.

13. Adrian D, Bhargavan K, Durumeric Z, Gaudry P, Green M, Halderman JA. Imperfect forward secrecy: how Diffie-Hellman fails in practice. *Communications of the ACM*. 2018 December: p. 5-17.

14. Yao ACC, Zhao Y. OAKE: a new family of implicitly authenticated diffie-hellman protocols. In *CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*; 2013; Berlin. p. 1113–1128.

15. Li P, Fang H, Liu X, Yang B. A countermeasure against relay attack in NFC payment. In *ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*; 2017; Cambridge City. p. 1-5.

16. Vila J, Rodriguez RJ. Practical Experiences on NFC Relay Attacks. In *Radio Frequency Identification: 11th International Workshop*; 2015; New York. p. 87-103.

17. Symantec. *Attacks on point-of-sales systems*. [Online].; 2014 [cited 2020 Mars 22]. Available from: https://docs.broadcom.com/docs/attacks-on-point-of-sale-systems-en.

18. Kaspersky. *Point of Threat or Point of Sale*. [Online].; 2017 [cited 2020 Mars 22]. Available from: https://media.kaspersky.com/en/business-security/enterprise/kess-pos-threats-whitepaper-white.pdf.

19. Akinyokun N, Teague V. Security and Privacy Implications of NFC-enabled Contactless Payment Systems. In *ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security*; 2017; Reggio Calabria. p. 1-10.

20. EMVCo. *Kernel ID*. [Online].; 2020 [cited 2020 May 06]. Available from: https://www.emvco.com/processes-forms/registration-services/kernel/.