Remote relay attack on RFID access control systems using NFC enabled devices

Wouter van Dullink Pieter Westein
University of Amsterdam

February 12, 2013

Abstract

RFID and NFC are frequently used technologies in access control systems. Despite the use of cryptology used in access control systems, they are often still vulnerable for relay attacks. These attacks circumvent the security layer and cannot be prevented by cryptographic countermeasures. When preform a relay attack remotely, timing issues can occur due to the introduction of delay. In this paper, we present a practical relay attack on systems using the ISO/IEC 14443 standard. Here, two NFC enabled devices are used that can forward RFID communication over a network channel. This papers shows that a relay attack is possible, and we discuss a value that can be exploited to increase the chance for a successful attack. Also recommendations are given how manufacturers and users of the standard can protect them self against relay attacks.

Acknowledgments

We would like to thank our supervisors, Bart Roos and Jop van der Lelie, for their support and feedback during this research. We are also grateful to the acces control company that provided us equipment for our test environment and the companies that invited us to test their RFID system.

Last, we want to thank all of the peer reviewers who gave their feedback on draft versions of this report.

Contents

1 Introduction

To keep unauthorized personnel out of their building, companies have implemented access control systems. They usually give their employees an access badge with a Radio Frequency IDentification (RFID) chip in it. This technique uses electromagnetic fields to exchange data from a tag (like a smartcard) to an object (a reader) for the purpose of authentication, identification or tracking.

RFID is a general name but has a lot of variants. There are differences in frequency, range, power[1][2], proprietary variants and how the chip is implemented.[1] These differences have in common the fact, that they all use a wireless non-contact system in combination with radio frequency. This is shown more clearly, in table 1.

Frequency Range	**Frequencies**	**Passive Read Distance**
Low Frequency (LF)	125 - 134 KHz	10 - 20 CM
High Frequency (HF)	13.86 MHz	10 - 20 CM
Ultra-High Frequency (UHF)	868 - 928 MHz	3 meters
Microwave	2.45 and 5.8 GHz	3 meters
Ultra-Wide Band (UWB)	3.1 - 10.6 GHz	10 meters

Table 1: Overview RFID operating frequencies

This study will focus on the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) 14443 standard[2]. A part of the ISO 14443 standard will be examined within this research, to theoretically perform a relay attack at a greater distance. This means to extend the passive read distance, as show in table 1. With a relay attack, the adversary does not tamper with the data being sent over, but instead performs a Man-in-the-Middle attack between the smartcard and the reader.

Chapter 2 describes an introduction into RFID versus NFC, the standard ISO/IEC 14443 and the cards used for access control. Chapter 2.5 will explain the structure of relay attacks and will explain any timing issues that occur. Chapter 3 will explain the experiments that are conducted during this research. A scenario will be described that theoretically can be used to perform a remote relay attack. In chapter 4, the results will be shown. Here it will be clear whether the scenario was possible and what results were found in regard to remote relay attacks.

[1]Passive mode means that the card has a build in battery and can broadcast his own channel

[2]Active mode means there is no powersupply in the card but gets his power when coupling with a reader

1.1 Motivation

RFID and NFC are widely used and will become even more popular in the next few years, because NFC is becoming a standard in mobile phones.[3] This research originates from the National Cyber Security Centre (NCSC). The reason behind this project is shared with the NCSC, and can be seen in their mission statement:

> To help increase the resilience of Dutch society in the digital domain and, by doing so, help to create a safe, open and stable information society[4].

1.2 Research Questions

The focus of this research project is to minimize timing issues that occur during relay attacks, and to translate this into a practical relay-attack scenario. This attack will be demonstrated with two Near Field Communication (NFC) enabled devices, between the RFID reader and the smartcard. The following research question is stated:

How can you perform a practical relay-attack, using a network channel, between two NFC enabled devices?

In this paper, the landscape of a relay attack will be investigated. There are various requirements before a relay attack is actually possible. To answer the research question, we defined the following subquestions:

1. How NFC devices communicate with each other?
2. What measurements are taken to provide security for RFID cards?
3. Are there timing issues when performing a relay-attack over a large distance?
4. Which fields in a frame can be used to minimize timing issues, in such a way, that a relay-attack is still possible?

[3] http://www.rcrwireless.com: Mobile NFC The hype and the potential
[4] https://www.ncsc.nl/english/organisation/about-the-ncsc.html

1.3 Related work

This study expands on the paper written by Gerhard Hancke[3]. In this paper an attack is illustrated, which effectively allows an attacker to borrow the victims card for a short period without requiring physical access to the victim's card. In this paper the terms, proxy and mole are introduced. This paper also uses this terms. The term proxy indicate that this NFC device is used to communicate with a reader. Where the term mole is used to declare, the NFC device that communicates with a card. A second study illustrates a peer-to-peer attack, with the help of mobile phones.[4, 5]

A technique to prevent relay attacks is a distance bounding protocol. They calculate the delay between sending out challenge bits and the corresponding response bits. Because electromagnetic waves travel close to the speed of light, the distance can be calculated. Other research, that are related to relay attack, try to detect relay attacks[6, 7] or propose new distance bounding protocols[8], where the SwissKnife solution claims to solve every security problem.[9]

Issovits et al. proved that the ISO 14443 standard can be exploited, to obtain more time. In this paper they explain how to exploit the Waiting Time eXtension (WTXM) field. They developed an attack to monitor the time during the challenge response pairs, and send out WTX packets when they need more time.[10]

The practical side of this research will be based on the work that has been done by the LibNFC community. They have written a program that performs the relay attack at USB level. They also describe how to utilize this with two laptops, connected through a network channel.[11]

2 Background

As stated in the previous chapter, there are a lot of variants of RFID. The International Standard Organization (ISO) published a standard, to which these systems need to be compliant. After RFID is briefly explained, the ISO 14443 standard will be examined. Next, relay attacks are described, together with the timing issues that occur. Last, the timing values used within the standard are presented.

2.1 Radio frequency techniques

RFID is a contactless communication technique that is widely used for different purposes. The basic concept of a RFID implementation is the following:

There is a reader, referred to as a Proximity Coupling Device (PCD), and a contactless card, reffered to as a Proximity Integrated Circuit Card (PICC). The reader has an electromagnetic field that scans for cards that operate on the same frequency. Once a card is inside the electromagnetic field it can communicate with the reader. In the case of an access control system, the purpose is to grant access to a resource.

NFC is a short-range radio frequency technology that is based on RFID. NFC allows for two-way communication between endpoints, where users are able to read (and write) small amounts of data from tags and to communicate with other devices. The usage is the same as RFID, but the difference is that the passive reading range is limited to a maximum of 10 CM, where RFID can also use other frequencies, stated in table 1.

2.2 The ISO/IEC 14443 standard

The standard is split into four parts. The first part describes the physical characteristics of the cards[12]. The second part describes the characteristics of the fields to be provided for power and bidirectional communication between the reader and the card[13]. The third part describes the polling for cards entering the field of the reader, the byte format and framing, the content of the initial commands, methods to detect and communicate with multiple cards and other parameters required to initialize communication[14]. The fourth part describes a half-duplex block transmission protocol and defines the activation and deactivation sequence of the protocol[15].

The third and fourth part of the standard are applicable to this research. In the following two paragraphs, they will be further examined.

ISO 14443-3

Part three of the standard specifies the basic communication of an RFID, between a reader and a card. This is shown more clearly in appendix 8.1. The reader will constantly send out Request Commands (REQ) to scan for cards. A reader accepts both type A and B cards, so the corresponding REQ will be either REQA or REQB. This is known as polling. When a card is exposed to an electromagnetic field, it will receive either a REQA or REQB. The card answers this REQ with an Answer to Request(ATQ), appropriate to the card type. If there is a situation with multiple cards, collisions will occur during the multiple ATQ's. The standard specifies a routine that will be followed, but this is not used within this research. The coding of the ATQ is shown in figure 1.

b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1
RFU								UID size bit frame		RFU	Bit frame anticollision				

Figure 1: Coding of the ATQ

The Unique Identification Number size (UID size) is mostly set to 00, which indicates a single UID. It can be either 01 or 11, representing double or triple UID's respectively. The anti-collision is, as described above, used when multiple cards are presented within the electromagnetic field of the reader. In this research, this part is not examined.

After receiving the corresponding ATQ, the reader will send another frame, containing a Select (SEL) and a Number of Valid Bits (NVB) field. The NVB field will have an initial value of 20, saying all the cards inside the electromagnetic field have to send their Unique Identifier (UID). With no collisions, there will be only one UID received by the reader.
Then the reader will send out another SEL and NVB, following all 40 bits of the UID and a checksum correlated with the card's type. The NVB is set to 70 here, indicating that the reader will transmit the complete UID.
The card, that matches the UID, will respond to this message with a Select Acknowledge (SAK). The SAK contains 8 bits, which indicate whether the UID is complete and if the card supports the transmission protocol described in part four of the standard, or if the card supports another specific protocol. The communication process is shown in figure 2.

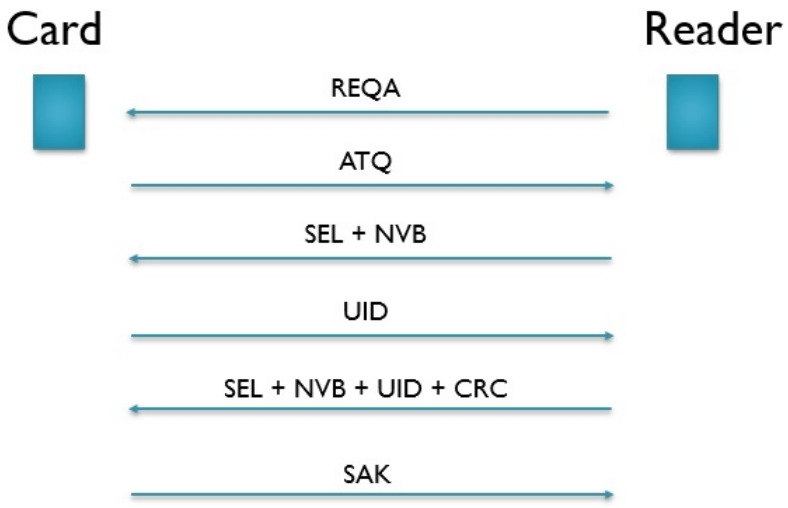

Figure 2: Communication between the card and the reader

ISO 14443-4
Part four of the standard specifies a transmission protocol. This protocol is capable of transferring application protocol data units, as defined in ISO/IEC 7816-4[16]. This protocol is only used when the SAK of the card is set on 20. In case of other values, the card uses a different transmission protocol. This protocol describes an addition to the normal procedure, and how blocks and frames are generated.

The addition to the normal procedure, is an Answer To Select (ATS). When the reader sees the SAK at value 20, it will send out a Request Answer To Select (RATS). The RATS is shown in figure 3. The parameter field consists of two parts:

1. The Frame Size for Device Integer (FSDI) codes the Frame Size for Device (FSD). The FSD defines the maximum size of a frame that the reader is able to receive.

2. The Card IDentifier (CID) defines a unique identifier for every card.

The card will respond to the RATS with an ATS. The ATS is shown in figure 3. The ATS is used to define parameters, to set how the exchange of data happens. The most important field is the TB(1) field, which codes the Frame Waiting Integer(FWI). This value is further examined in chapter 2.4. If the card supports any changeable parameters in the ATS, the reader may use a Protocol and Parameter Selection (PPS) request to change these parameters. This is not applicable to this research, so it will not be further examined.

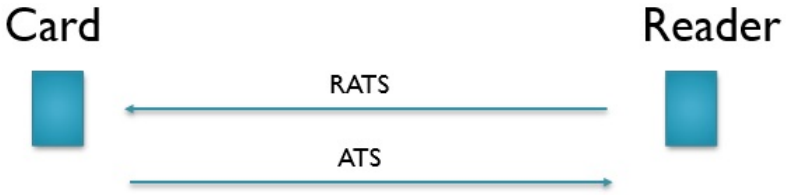

Figure 3: Transmission protocol in the standard

After receiving the ATS, the reader will start with the first challenge-response pair that is part of the access control application. The challenge-response pair is described in the ISO 7816-3 standard.[16]

After the challenge-response sequence ends and a certain limit of pairs is reached, the reader will deactivate the card. With this action the reader will send a DESELECT frame to the card containing the appropriate CID and the UID. The card will send an acknowledgement response back, based on this request.

2.3 Card types

Like the techniques in RFID systems, there are many variants in the implementation of contactless cards. For the ISO 14443, there are two types: Type A and Type B. The main differences between these types concern modulation methods, coding schemes[13] and protocol initialization procedures[14]. Both Type A and Type B cards use the same transmission protocol described in part 4 of the standard[15]. The transmission protocol specifies data block exchange and related mechanisms:

- Data block chaining
- Waiting time extension
- Multi-activation

Cards that are of type A, have fixed fields. These fields are shown in table 2 in more detail.

Card	**ATQA**	**SAK**	**ATS**	**UID length**
MIFARE Mini	00 04	09	-	4 bytes
MIFARE Classic 1k	00 04	08	-	4 bytes
MIFARE Classic 4k	00 02	18	-	4 bytes
MIFARE Ultralight	00 44	00	-	7 bytes
MIFARE DESFire	03 44	20	75 77 81 02 80	7 bytes
MIFARE DESFire EV1	03 44	20	75 77 81 02 80	7 bytes

Table 2: MIFARE card details

These are the MIFARE cards developed by NXP[5]. The cards are mostly based on the ISO 14443 standard, but some slighty differ according to their own version of the implementation of the transmission protocol. Looking at the tables above, the first observation here is that the first four cards do not have an ATS defined. As described in chapter 2.2, the ATS is used to define the FWT. If the transmission protocol in part four of the standard, and therefor the ATS, there might be a proprietary protocol in use.

[5]http://www.nxp.com/

2.4 Timing values

Part four of the ISO 14443 standard describes two timing values, that are used as parameters for communication between the card and the reader. This chapter describes both values, which are the Frame Waiting Time (FWT) and the Waiting Time Extension (WTX).

2.4.1 Frame Waiting Time

The first timing value within the standard, is the Frame Waiting Time (FWT). The FWT is the allowed time between a request and a response. The FWT is set in the ATS during the initialization phase. Each time a challenge and response sequence is sent and received by the reader, it will calculate the difference by means of the timestamps of the frame.

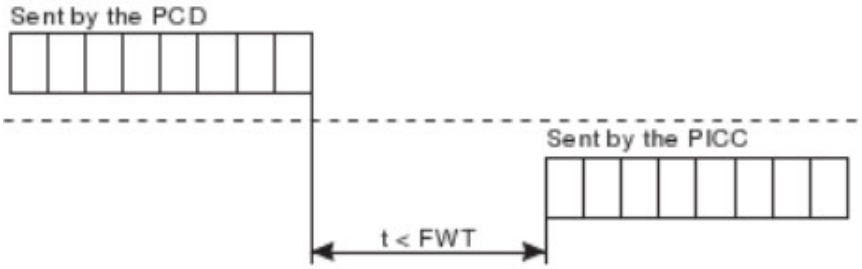

Figure 4: Overview Frame Waiting Time

If the difference between the request and the response is greater than the FWT, the reader will try to resend the challenge, since a transmission error could have occurred. When the difference in the retry is also greater than the FWT, the reader will close the communication with the card.

The reader calculates the FWT by means of the Frame Waiting Integer (FWI). The FWI is a four bit field inside the ATS packet.

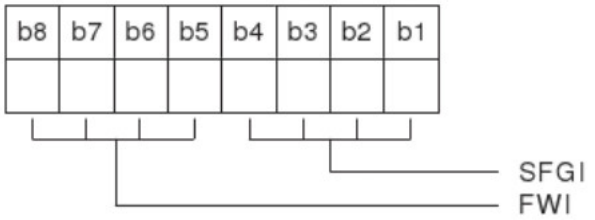

Figure 5: Overview Frame Waiting Integer field

Once the ATS is received by the reader, it will calculate the FWT with the following formula:

$FWT = (256x16/fc)x2^{FWI}$

The calculated FWT can not exceed the minimum and maximum of the FWT, as specified in the ISO/IEC 14443 standard[2]. When there is no value specified, the default FWT is used:

$FWT_{min} =\sim 302\mu sec$
$FWT_{max} =\sim 4949msec$
$FWT_{default} =\sim 4833\mu sec$

2.4.2 Waiting Time Extension

It can happen that during the challenge response sequence, the card needs more computation time. The protocol described in part four of the standard specifies that the card can use the Waiting Time Extension (WTX) in such a case. The WTX is set by creating a frame with an S-Block format, shown in figure 6.

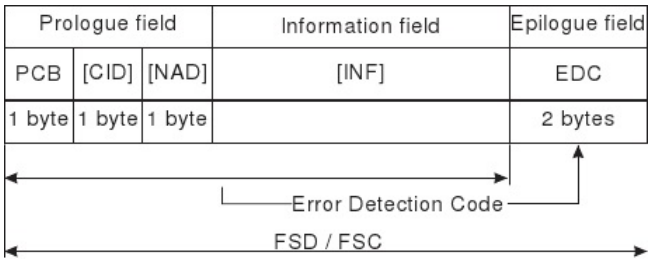

Figure 6: S Block Format

As stated in the standard, the S-Block will contain an Information field (INF), in the case of a WTX frame. This INF field is shown in figure 7.

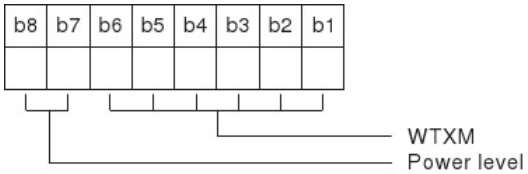

Figure 7: Details Information (INF) field

Within this INF field the first part will set the power level. This will indicate whether the card has enough power to process large command sets. The second part will set the Waiting Time Extension Multiplier (WTXM). The WTXM codes a 6 bit value that will be used to create the temporarily FWT used for that specific challenge-response pair. The representation of this bit will be in the range of 1 to 59. The formula that is used for calculate the temporarily FWT is the following:

$FWT_{temp} = FWTxWTXM$

When the card sends the WTX request, the reader will respond to it with an acknowledgement containing the same information as the request. Both the card and the reader will then calculate the temporary FWT.

Depending on the FWT that is being used by the RFID system, it is possible that the FWT_{temp} will be higher than the FWT_{max}. If this happens, the RFID system will use the FWT_{max} instead of the FWT_{temp}.

2.5 Relay attack

A RFID system can be subjected to many types of attacks, where this study will focus on relay attacks. This attack focuses on extending the range between the card and the reader and makes use of two NFC enabled devices, one acting as a reader and one acting as a card emulator. The access control system will not notice such an attack because it will think a card is actually in front of it.

An attacker can hold the NFC reader near the card of a victim and relay the data over another communication channel to a second NFC reader. The second reader will be placed in proximity to the original reader and will emulate the victim's card. This setup is shown, in more depth, in figure 8.

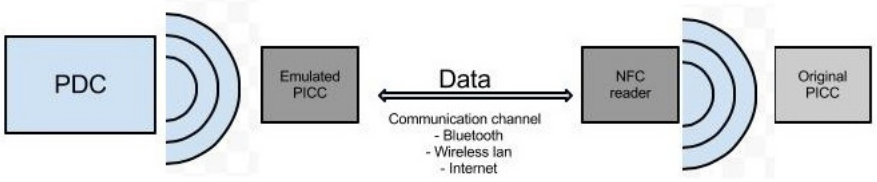

Figure 8: Overview relay attack

2.5.1 Timing issues

In telecommunication, delays are very common[17]. The term is used to explain the time a packet needs to travel from one node to another node. The delay is not only caused by propagation delay (how far the packet needs to travel or the distance it needs to accomplish), but also the processing delay, (the time a router needs to process a packet). Two elements of processing delay are queuing time (the time a packet is in the routing queue) and the transmission queue(the time it takes to push the packets on the link). For this research, the main focus will be on the distance and the delay that it causes.

If you increase the physical distance between the two NFC devices, the packets that are relayed will take longer to travel. Because a RFID system has a certain FWT, the time between a challenge and response will causes problems because it will be higher than the maximum allowed FWT.

3 Test setup

In this chapter the test setup will be described. First, the test environment will be examined and the attack scenario will be described. A program is developed to change the FWT bit in the ATS phase, in order to gain more time between the challenge-response pair. At the end of this chapter additional environments will be mentioned. These environments are real life situations, where the experiments will also be performed.

3.1 Environment

To test the attack scenario, a test environment was built. This test environment was made with components that was provided by an access control manufacturer, and consists of:

1. A wallreader
2. Software to manage the access control on doors
3. Empty proximity cards

With these components, a replica of a company implementation was built, to test our attack scenario. The software to manage access control was installed on a laptop. With the laptop and the other components connected in a Local Area Network (LAN), it was possible to simulate a working test environment.

The empty cards were of two types:

- MIFARE Classic
- MIFARE DESFire

3.2 Network setup

The relay attack layout was build within a test network. The network in this project is shown in figure 9.

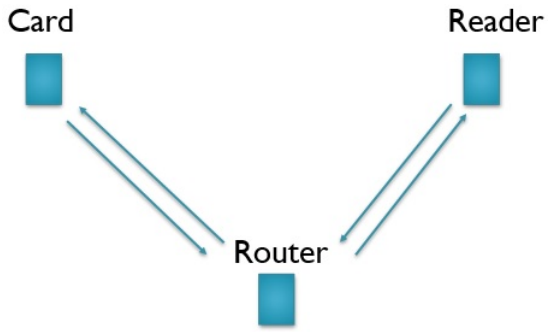

Figure 9: Network setup overview

The two NFC readers were each connected to a laptop by USB. The laptops were connected to a switch and each had a separate LAN. The router connected the two LANs. During the relay attack, the laptops used an open source program called Socat[6] to initialize a TCP connection. Once this TCP connection is active, the challenge-response sequence will be transported over this channel.

The readers that were connected to a laptop either performed the relay attack in initiator mode or in target mode. In initiator mode, the reader had the card in proximity, close enough to read the tag that was present on the card. It then connected to a target machine that sent the tag, where the target could emulate it. In target mode, the reader received a tag from the initiator, and emulated this on its NFC chip. The script is explained in more detail in the next paragraph.

[6]Socat is a command line based utility that established two bidirectional byte streams and transfers data between them

Script
The script that was used in this setup was developed by LibNFC[11]. The purpose of the script was to connect to a reader, opens it in either target or initiator mode, and use it during the relay attack. The working of the script is as follows:

1. Scan for NFC devices
   The script scans for attached USB devices, and checks whether they are in the list of supported NFC devices. If not, the script will return with an error, mentioning that it is missing a NFC device. If attached, the script will use this or these NFC device(s) and will mount them.

2. Pick one of the three modes
   Depending on the called mode, the script will initialize differently. There are three types of modes:

   - Initiator
   - Target
   - Local USB mode

   In the initiator mode, the script will mount the NFC device as a reader, and expect a card to be present on top of it. It then reads out the tag of the card and will forward it towards the target. The target will reside on another machine and both machines will be coupled together by means of a data channel.

   In target mode, the script will mount the NFC device as a emulator, and will wait for a card tag to be presented by the initiator. The target and the initiator will be coupled together by means of a data channel. When received, the tag will be loaded into the NFC device and it will wait until it is placed within the electromagnetic field of a reader.

   In local USB mode the script will mount two NFC devices as initiator and target. It expects a card to be present on the initiator and will place the tag onto the target. It then waits for the target to be placed within the electromagnetic field of a reader.

3. Depending on the mode, perform the relay attack
   Once the target, both in target and local mode, is placed within the electromagnetic field of a reader, it will relay all the data through the data channel back and forth.

3.3 Attack scenario

This attack scenario exploits the FWI bit in the ATS frame, explained in chapter 2.2. By changing the FWI in the ATS, both the reader and the card will use a higher FWT for each challenge-response pair, which will result in a practical remote relay attack.

In order to achieve this, the router in the test setup will execute a script that modifies the ATS response packet of the card, and change the FWI bit to a higher value. The script executes the following steps:

1. Scan for ATS response and place it in a queue:
   The ATS response has a specific data section that is unique for this message type. Scanning for this specific data section is done with an IPtables command. This command scans for a specific string in the raw data of every packet that flows through the interface. Once such packet is found, the command will place this packet in a queue.

2. Read the queue and capture each packet individually:
   Reading of the created queue in step 1 is done by a simple Python script. Each packet is processed individually.

3. Modify the raw data of the packet, changing the FWI bit:
   When the packet is captured, the raw data field is retrieved. This field contains the ATS. This step retrieves the original string, changes the FWI bit, and places the modified string back into the packet.

4. Resend the packet, keeping the source and destination address:
   Once the raw data field is modified, the packet is resent to its original destination.

The script that is used for this attack scenario, can be downloaded here[7].

[7] https://github.com/Pwestein/RP1-Scripts.git

3.4 Timing

Added delay can occur by adding an extra channel between the standard RFID setup. The communication between the reader and the first NFC device, and the card and the second NFC device, is not part of the additional delay, because this is the normal situation without extending the range.

The additional delay that is caused can be found in the following hardware.

1. Proxy delay
2. Mole delay
3. Relay channel delay

For the tests extra delay will be added to simulate more distance. Adding delay can be done with the Traffic Control (TC) [8] command.

The linux command is:
sudo tc qdisc add dev eth0 root netem delay 10ms

During the tests, each time 10 miliseconds of delay were added, to test if the relay attack was still possible. Simulating one milisecond increase could not be achieved in this research, so this will be stated for further work.

3.5 Additional environments

During this study, several companies were approached to look at different implementations of a RFID access control system. Within these environments, the following steps were followed in order to see if their system was vulnerable for relay attacks. These steps are:

1. Scan their card to see if they support the ISO/IEC 14443-4 standard.
2. Perform a USB relay attack with one laptop.
3. Perform a TCP relay attack with two laptops.
4. Perform a TCP relay attack with a delay, greater than the set FWI.
5. Perform a TCP relay attack with a delay, greater than the set FWI and changing the FWI bit in the ATS response.

The choice of steps differs from the tests in our own environment. Since our attack was focussed on the transmission protocol, described in part four of the standard[15], it was needed that the card used in the environment was compliant to it. Results inside these additional environments are explained in the next chapter.

[8] TC is used to configure Traffic Control in the Linux kernel.

4 Results

The results acquired during this research are divided into three categories:

1. Attack scenario
2. Relay attack limitations
3. Impact analysis

Attack scenario
During this research, we chose to adapt the ATS packet, when it was sent over the data channel between two NFC devices. Adapting the packet could be done, so theoretically, changing the FWT inside the ATS packet is possible. Also, delay was introduces into the network setup, to show that the attack works, even with delay that results in a higher FWT than allowed.

However, testing this in the RFID system was not possible because the hardware that was used, could not emulate the adapted packet. The chip inside the NFC device, has a predefined ATS and it overwrites any incoming ATS. For further work, the attack would need to be executed with two NFC devices that dont replace the modified ATS. The percentage of affected readers, will be stated in further work.

Relay attack limitations
The FWT is bound to part four in the standard. Only when the transmission protocol from the standard is used, the FWT can theoretically be changed. When the standard's transmission protocol is not used, it is most likely replaced with a proprietary protocol that is vendor specific. Perhaps the proprietary protocol also uses timing values, but this is for further work.

Impact analysis
In this study, additional companies were approached to conduct an investigation to different implementations of RFID access control systems. In total, four companies were approached. Two of them used a tag that operated on another frequency (125 Mhz) so our readers were not capable of reading it. The other two companies used MIFARE Classic cards. These could be read, which gave the following results:

Name	**Card type**	**ISO14443-4 compatible**
Company 1	Type A	No
Company 2	Type A	No
Company 3	None (125 MHz used)	No
Company 4	None (125 MHz used)	No

Table 3: Impact analysis at four companies

In table 3, you can see that these cards are not compatible with part four of the ISO 14443 standard. This indicates that these cards support a different transmission protocol than the one described in the standard. This could mean a proprietary protocol is used, that uses different timing parameters. The percentage of affected cards, will be for further work

5 Countermeasures

In this chapter we describe various countermeasures that can be implemented to prevent relay attacks. Most of these countermeasures are not protocol improvements, but rather expansions for the card holder, or the door reader.

5.1 Faraday cages

A simple prevention measure against relay attacks can be found at the user side. Users can shield their cards with a box that is called the cage of faraday.

5.2 Distance Bounding Protocols

As mentioned in various papers, one of the countermeasures is the use of distance bounding protocol. These protocols add an additional security boundary to the RFID system, so that the reader knows whether the card is presented inside the electromagnetic field, or a relay attack is being performed.

5.3 Signing of the FWT

During this study various cards are examined how high the Frame Waiting Time was. The FWI is an unsigned integer, so signing this would result in more security. However, this depends on the conputational power of the cards, to be able to verify the signer.

6 Conclusion

During this project, the researchers have looked at relay attacks against RFID access control systems using two NFC enabled devices.

The initial results showed that performing a relay attack, using a network channel between two NFC enabled devices, can be done. The security of the access control system that was analyzed, already allowed a relay attack from a certain distance. In the test enviroment the door could be opened with a delay of 80ms. By analysing the ISO 14443 standard to find solutions for timing issues, the researchers found a way to obtain even more time, resulting in a greater relay attack.

With this attack, there are some limitations in the execution of it. One of the most important ones is that this attack relies on the implementation of the transmission protocol, described in part 4 of the standard[15]. When having part four of the standard implemented, the timing values that are present can be theoretically abused to obtain enough time for a remote relay attack. If another transmission protocol, mostly a proprietary one, is used, then this attack is no longer possible. The other limitation is the NFC hardware. During this project, one of the drawbacks was having the NFC hardware replacing the modified ATS by a predefined ATS.

Countermeasures can be implemented, to reduce the risk of being a victim of relay attacks. The faraday cage and the distance bounding protocols are the obvious two that are suggested, but implementing an improved version of part four of the standard would result in a more sofisticated way. The proposed solution would mean that the FWI bit will be signed, by the reader, and would need to be verified by the card.

7 Future Work

Improved hardware
An important future work aspect, is to test the attack scenario on hardware that doesn't replace the modified ATS. During this project, the researchers weren't able to obtain this kind of hardware.

Detailed impact analysis
As stated in the result section, some cards and readers are affected due to this attack. Further work should be done on this subject. This would be a analysis at every card and reader manufacturer, to see whether they are affected by it. An important fact here is to look at each implementation of the RFID access control system.

Transmission protocol on other standards/frequencies
Research is also needed to see if other transmission protocols have similarities with timing, compared to ISO 14443 Transmission protocol. The attack is theoretically proved but the impact would be much more if other protocols are vulnerable to.

References

[1] K. Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. Wiley, 2010.

[2] Identification cards contactless integrated circuit(s) cards proximity cards, 2000.

[3] G.P. Hancke. A practical relay attack on iso 14443 proximity cards. *Technical report, University of Cambridge Computer Laboratory*, 2005.

[4] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical nfc peer-to-peer relay attack using mobile phones. *Radio Frequency Identification: Security and Privacy Issues*, 2010.

[5] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones. *IACR ePrint Archive*, 2011.

[6] G.P. Hancke, KE Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 2009.

[7] J. Munilla and A. Peinado. Enhanced low-cost rfid protocol to detect relay attacks. *Wireless Communications and Mobile Computing*, 2010.

[8] S. Lee, J. Kim, and S. Hong. Distance bounding with delayed responses. 2012.

[9] C. Kim, G. Avoine, F. Koeune, F.X. Standaert, and O. Pereira. The swiss-knife rfid distance bounding protocol. *Information Security and Cryptology–ICISC 2008*, 2009.

[10] W. Issovits and M. Hutter. Weaknesses of the iso/iec 14443 protocol regarding relay attacks. In *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, pages 335–342. IEEE, 2011.

[11] Lib NFC. Lib nfc website.

[12] ISO 14443-Part 1: Physical characteristics, 2008.

[13] ISO 14443-Part 2: Radio frequency power and signal interface, 2010.

[14] ISO 14443-Part 3: Initialization and anticollision, 2011.

[15] ISO 14443-Part 4: Transmission protocol, 2008.

[16] Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, 2005.

[17] B. Zhang, TS Ng, A. Nandi, R. Riedi, P. Druschel, and G. Wang. Measurement based analysis, modeling, and synthesis of the internet delay space. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 85–98. ACM, 2006.

8 Appendixes

8.1 A - Activation Sequence

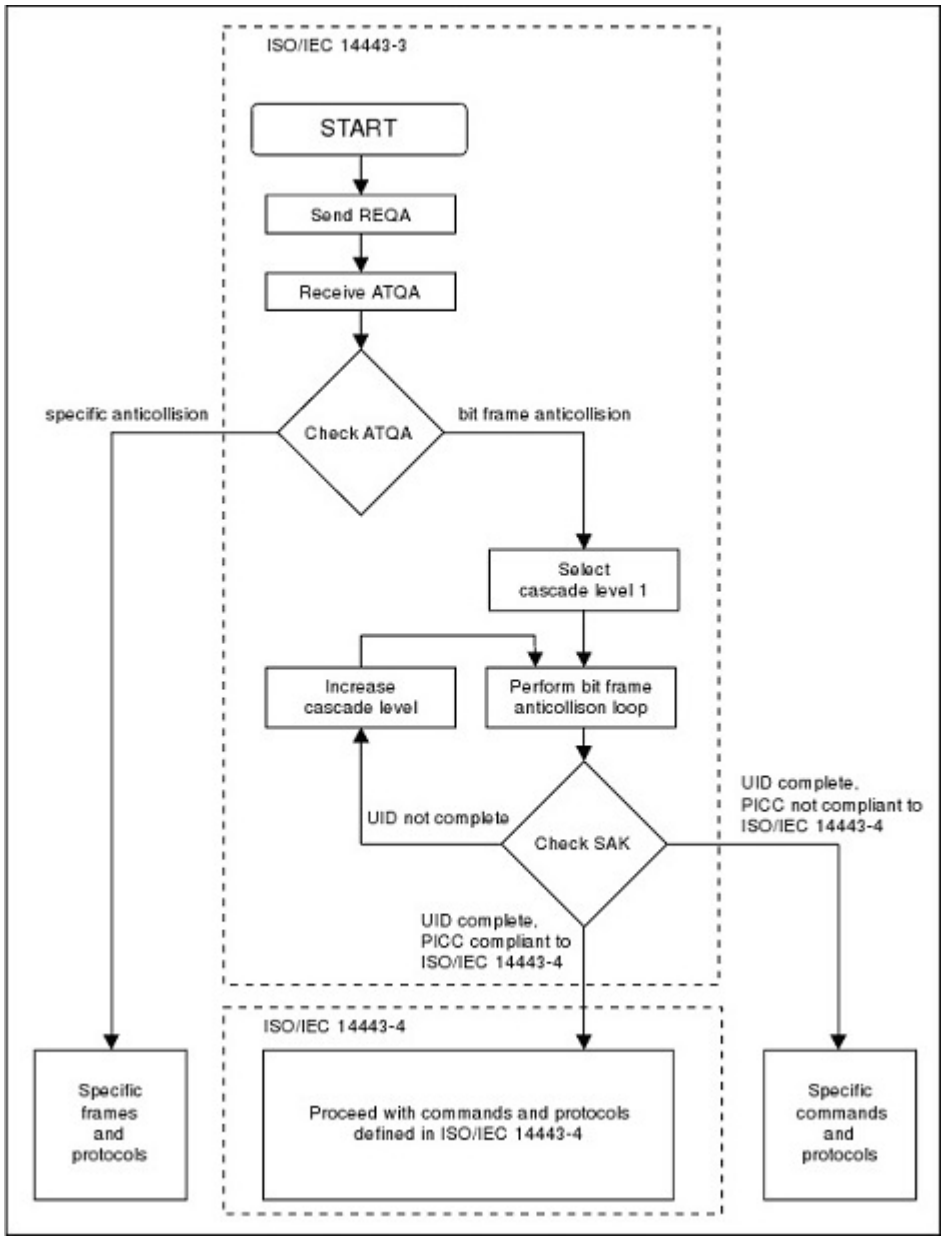

Figure 10: The initialization of proximity cards at the reader