CHALMERS

Security in Close Proximity Systems

A Technical Summary and Case Study of Security in NFC Systems

Bachelor's thesis in Computer Science and Engineering

SIMON HOLM
PONTUS JOHANSSON BERG
KIM KLING
JOHAN LARSSON HÖRKÉN
PONTUS MALM
CHRISTOFFER SANDLUND

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2015

BACHELOR'S THESIS

Security in Close Proximity Systems

A Technical Summary and Case Study of Security in NFC Systems

SIMON HOLM
PONTUS JOHANSSON BERG
KIM KLING
JOHAN LARSSON HÖRKÉN
PONTUS MALM
CHRISTOFFER SANDLUND

Department of Computer Science and Engineering
Computer Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden 2015

Security in Close Proximity Systems
A Technical Summary and Case Study of Security in NFC Systems
SIMON HOLM
PONTUS JOHANSSON BERG
KIM KLING
JOHAN LARSSON HÖRKÉN
PONTUS MALM
CHRISTOFFER SANDLUND

Examiner: Arne Linde

Bachelor's thesis 2015:34

Department of Computer Science and Engineering
Computer Engineering
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: +46 (0)31-772 1000

Chalmers Reproservice
Göteborg, Sweden 2015

Security in Close Proximity Systems

A Technical Summary and Case Study of Security in NFC Systems

SIMON HOLM
PONTUS JOHANSSON BERG
KIM KLING
JOHAN LARSSON HÖRKÉN
PONTUS MALM
CHRISTOFFER SANDLUND
Department of Computer Science and Engineering, Chalmers University of Technology

Bachelor's thesis

Abstract

This thesis investigates security in close proximity systems by conducting research about the close proximity technology and practically investigating two commonly used close proximity systems. In this thesis the systems are limited to those that use Near Field Communication (NFC), since NFC is commonly used in close proximity systems. NFC is a mean of communication using radio waves at the frequency of 13.56 MHz.

A case study of the security that is implemented in NFC applications is conducted in this thesis. The case study consist of an analysis in regards to an access control system and an investigation of Peer-to-Peer communication using the NFC technology. To fully understand the technology a research about the close proximity technology is undertaken. The first case study analyses the security of an access control system which is used by homeowners. A theoretical analysis of NFC Peer-to-Peer communication is performed in the second case, where only a limited amount of practical tests are performed.

The study revealed poor security in both the access control system and the Peer-to-Peer communication. In the discussion the security vulnerabilities that are revealed in the case studies, and the theoretical analysis of the NFC technology, are given possible security improvements. The improvements suggest both short and long term ways of increasing security.

The NFC standards does not address security, rather this is implemented at the application layer. However, not all NFC systems add adequate security, and non-secure systems are, unfortunately, available on the market.

Keywords: NFC, Security, Access control system, Peer-to-Peer communication, Mobile payments

Sammanfattning

Den här kandidatrapporten undersöker säkerheten i beröringsfria system genom att göra en grundlig undersökning av tekniken, samt praktiskt undersöka hur ett par vanligt använda beröringsfria system är implementerade. De undersökta systemen är avgränsade till sådana som använder Near Field Communication (NFC) då det är en teknik som är vanligt förekommande i beröringsfria system. NFC är en teknik som används för att kommunicera med radiovågor på frekvensen 13,56 MHz.

En fallstudie av den säkerhet som är implementerad i NFC-applikationer genomförs i den här rapporten. Fallstudien består av en analys kring ett NFC-baserat passersystem och en undersökning av NFC-tekniken i Peer-to-Peer-kommunikation. För att fullt ut förstå teknologin görs en efterforskning av den teknik som används i beröringsfria system. Den första fallstudien undersöker säkerheten i ett NFC-baserat passersystemen för hemmabruk. En teoretisk analys av NFCs användning inom Peer-to-Peer-kommunikation görs i den andra fallstudien, där endast ett fåtal praktiska test är utförda.

Undersökningen avslöjade en undermålig säkerhet i både passersystemet och i Peer-to-Peer-kommunikationen. I diskussionen ges förbättringsförslag till de säkerhetshål som avslöjades i fallstudien och i den teoretiska analysen av NFC-tekniken. Förbättringarna är ämnade att fungera både på kort och lång sikt.

Standarderna för NFC tillför ingen säkerhet, utan den får istället implementeras i applikationslagret. De undersökta NFC-systemen använder inte adekvat säkerhet, och osäkra system finns, tyvärr, på marknaden.

Acknowledgements

We want to give a special thanks to our supervisor Pierre Kleberger for his assiduous reading and correcting of this thesis, as well as being a sounding board. We would also like to thank our examiner Arne Linde for the investment in hardware which made the case studies possible.

List of Abbreviations

AES Advanced Encryption Standard.
ASK Amplitude Shift Keying.
ATQA Answer to request, Type A.

CPU Central Processing Unit.

DoS Denial of Service.

IEC International Electrotechnical Commission.
ISO International Organization for Standardization.
IV Initial Vector.

LFSR Linear-Feedback Shift Register.
LLCP Logical Link Control Protocol.

MFCUK MiFare Classic Universal toolKit.
MFOC Mifare Classic Offline Cracker.
MITM Man-In-The-Middle.

NDEF NFC Data Exchange Format.
NFC Near Field Communication.
NFCIP-1 Near Field Communication Interface and Protocol 1.
NIST U.S. National Institute of Standards and Technology.

P2P Peer-to-Peer.
PCD Proximity Coupling Device.
PICC Proximity Inductive Coupling Card.
PIN Personal Identification Number.
PKE Public Key Encryption.

RF Radio Frequency.
RFID Radio Frequency IDentification.

SoC System-on-a-Chip.

UID Unique IDentifier.

Contents

Abstract **i**

Sammanfattning **ii**

Acknowledgements **iii**

List of Abbreviations **iv**

List of Figures **viii**

List of Tables **ix**

1 Introduction **1**
1.1 Aim 1
1.2 Scope 1
1.3 Related Work 2
1.4 Structure of Thesis 2

2 Introduction to Computer Security **3**
2.1 Security Objectives 3
2.2 Breaching the Security Objectives 4
2.2.1 Spoof 4
2.2.2 Eavesdrop 4
2.2.3 Relay 5
2.2.4 Replay 5
2.2.5 Denial of Service 5
2.3 Number Generation 6
2.3.1 True Random Number Generation 6
2.3.2 Pseudo Random Number Generation 6
2.4 Encryption 8
2.4.1 Symmetric Encryption 8
2.4.2 Asymmetric Encryption 9
2.4.3 Secure Device Pairing 9
2.5 Man-In-The-Middle 9
2.6 System Architecture to Prevent Attacks 10
2.7 Security Through Obscurity 10
2.8 Secure Element 10
2.9 Temporary ID 10

3 Introduction to Close Proximity Systems **11**
3.1 Historical Overview 11
3.2 Components of a Close Proximity System 11
3.3 The NFC Protocol Stack 13
3.4 Communication Between NFC Compatible Devices - Coupling 13
3.4.1 Initialisation Process and Transport Protocoll in ISO/IEC 18092 14
3.4.2 Initialisation Process in ISO/IEC 14443-3 16
3.4.3 Differences in Coupling Between ISO/IEC 14443-3 and 18092 17
3.4.4 NFC Data Exchange Format 17

3.5 Translating and Transmitting Data - Modulation . . . 17
3.6 Security in NFC Protocols . . . 17

4 Implementations of Close Proximity Technology 19
4.1 Mifare Classic . . . 19
4.1.1 Memory Structure . . . 19
4.1.2 Other Mifare Technologies . . . 19
4.2 Access Control Systems . . . 20
4.3 Contactless Payments . . . 21
4.3.1 Smart Cards . . . 21
4.3.2 Mobile Payments . . . 21
4.4 Peer-to-Peer Communication . . . 22

5 Methodology and Laboratory Equipment 23
5.1 Methodology in Case Studies . . . 23
5.2 Hardware . . . 23
5.3 Software . . . 24

6 Case Studies 27
6.1 Case 1: Home Access Control Systems . . . 27
6.1.1 Attack Vectors . . . 27
6.1.2 Execution . . . 28
6.2 Case 2: Peer-to-Peer Communication . . . 28
6.2.1 Attack Vectors . . . 29
6.2.2 Execution . . . 29

7 Results of Case Studies 31
7.1 Case 1: Home Access Control Systems . . . 31
7.1.1 Spoof . . . 31
7.1.2 Relay . . . 31
7.1.3 Denial of Service . . . 31
7.2 Case 2: Peer-to-Peer Communication . . . 31
7.2.1 Eavesdrop . . . 32
7.2.2 Relay . . . 32
7.2.3 Android Beam . . . 32
7.3 Summary of Results . . . 32

8 Discussion and Future Work 33
8.1 General Discussion About the NFC Technology . . . 33
8.2 Discussion Regarding Case 1: Home Access Control System . . . 34
8.2.1 Mifare Classic . . . 34
8.2.2 Keys and Access Bits . . . 34
8.2.3 Entry Permissions . . . 35
8.2.4 Comparison of Electronic and Mechanical Access Control Systems . . . 35
8.3 Discussion Regarding Case 2: Peer-to-Peer Communication . . . 35
8.3.1 Secure Channel . . . 35
8.3.2 Replay and Random Number Generation . . . 35
8.3.3 Android Beam . . . 36
8.3.4 Mobile Access Control Systems . . . 36
8.4 Mobile Payments . . . 36
8.5 Environmental Concerns . . . 37
8.6 Reflection of the Work . . . 37
8.7 Future Work . . . 37
8.7.1 Security in Mobile Payments Using NFC . . . 37
8.7.2 Construction of a More Secure Access Control System . . . 38

9 Conclusion 39

References **41**

A Modulation Using Amplitude Shift Keying **45**

A.1 Modified Miller Modulation 46

A.2 Manchester Modulation 46

List of Figures

2.1 Security Objectives. . . . 3
2.2 Spoof attack 4
2.3 Eavesdropping attack 5
2.4 Relay attack 5
2.5 Replay attack 5
2.6 Denial of Service attack 6
2.7 State diagram of a 4 bit LFSR, state x 7
2.8 State diagram of a 4 bit LFSR, state x+1 7
2.9 A message is being encrypted and then deciphered 8
2.10 A message is being asymmetricaly encrypted and then deciphered 9
2.11 Man-in-the-Middle attack 10
3.1 Initiator and target in a close proximity system 12
3.2 Active NFC communication 13
3.3 Passive NFC communication 13
3.4 NFC Protocol Stack 14
3.5 Coupling process 15
3.6 Initialisation process 16
4.1 Memory structure of Mifare Classic 1K 20
4.2 Lock house and handle of an access control systems for personal use. 21
5.1 NFC module connected to a Raspberry Pi. 24
A.1 ASK of binary data using Modified Miller and Manchester method. 45

List of Tables

3.1 NFC-IP characteristics. 12
7.1 Summary of results. 32
A.1 Overview of which D corresponds to which transfer speed and thereby ASK method. 45

1

Introduction

Wireless communication is a technology that has become widely recognised and more commonly used the past years. Wi-Fi and Bluetooth are de facto standards for wireless communication for the home consumer and have made a huge impact on the computerised way of living. The fast technological development, together with an urge both from consumers and producers of a more simplified way of living, has led to a request of wireless applications available in areas such as payments, product tracking and access control systems.

These wireless applications exist today, but are fairly young. One of the most common technologies used when implementing these kind of services is called Radio Frequency IDentification (RFID), which is a contactless communication technology, using Radio Frequency (RF) fields [1].

A common frequency for close proximity communication is 13.56 MHz, which is called Near Field Communication (NFC) to distinguish communication at this specific frequency. NFC work in close proximity, somewhere around 10 cm according to Ernst Haselsteiner and Klemens Breitfuß. [2]

Since the NFC technology has been implemented in close proximity systems such as mobile payments, one may wonder if the close proximity is sufficient security to ensure secure payments. Does it exist any other security in the technology, preventing attackers from modifying valuable information in this close proximity communication? The security issue does not only exist in contactless payments, but also in applications such as access control systems, mobile communications and any other technology using close proximity communication at the NFC frequency. This thesis intend to give a technical overview of the close proximity systems as well as investigate the security of these systems.

One of the systems studied is an access control system for home use that is available on the market. This system is a good representation of a system that is utilising NFC technology for access verification. Due to the sensitivity of the research, the name of this particular access control system and its manufacturer, as well as specific details about how the attacks are performed, remains unmentioned. Beside the access control system, there are also be a study of how mobile payments and Peer-to-Peer (P2P) communication work over NFC.

1.1 Aim

The aim of this thesis is to assess how secure everyday close proximity systems truly are. As with all young technologies it may have a portion of flaws not yet found. It is in everyone's interest to eliminate these flaws as soon as possible and make the technology and their protocols more mature. This thesis also intend to clarify how the close proximity technology operates, by performing a technical research.

1.2 Scope

This thesis is limited to examining the security of the NFC technology. It focuses on security using affordable mobile devices and Proximity Inductive Coupling Cards (PICCs) (which are more commonly known as tags). A few different systems representative for the Swedish market are analysed in order to get an understanding of the overall security of the NFC technology.

This thesis examine the following two topics.

- The NFC technology, including some implementations and its embedded security.
- The possibility to bypass the security of systems using NFC.

1.3 Related Work

This thesis is strongly inspired by the thesis by Alm et al. [1] that focuses on different attack vectors on particular systems using the RFID and NFC technology. That thesis also give a good introduction to the close proximity technology and how to design attack vectors against commonly known close proximity systems. The thesis written by Alm et al. differs from this one in which systems that are investigated. The focus of this thesis is systems produced after the publication of the thesis by Alm et al. This thesis also intend to give a deeper understanding of the construction of close proximity systems, especially NFC systems.

One of the most commonly known papers regarding security in close proximity systems is written by Ernst Haselsteiner and Klemens Breitfuß [2]. Their thesis introduces the NFC technology in a short, clear and understandable way. Attack methods against close proximity communication are described. Many of the other works regarding attacks against NFC systems refer to the work by Ernst Haselsteiner and Klemens Breitfuß. In the end of their thesis, solutions and recommendations that would improve the security in the NFC technology are suggested. This thesis intend to practically demonstrate some of Haselsteiner and Breitfuß' theories about attack methods and further discuss counter measurements against these attacks.

Practical attacks against close proximity systems have been performed by Francis et al. [3], where it was shown that a relay attack can be performed in contactless transactions using only two NFC enabled mobile devices. Diakos et al. [4] shows that it is possible to eavesdrop on close proximity communication at the 13.56 MHz frequency from a distance of 20–90 cm. The variations in distance depend on the electrical field strength of the signals as well as the used equipment. This thesis intend to take inspiration from their work and try to apply such theories to different systems.

1.4 Structure of Thesis

Chapter 1 is an introduction to the rest of this thesis. It contains the aim of this thesis, which is further limited by a scope. At last, the chapter presents some related work.

Chapter 2 is the first of three chapters to introduce the reader to the NFC technology. It describes computer security and the general characteristics of a secure system, as well as how to achieve security. The chapter also describe how security is breached, and finally some security related technologies. Chapter 3, Introduction to Close Proximity Systems, present the close proximity technology, specifically the RFID and NFC technologies. It presents how the communication and protocols interact and the security of the NFC technology. Chapter 4 introduce common implementations of close proximity systems together with their security. The chapter will first present the Mifare Classic technology, followed by access control systems and contactless payments. Finally, P2P communication using NFC is described.

The method used in the analysis of this thesis is described in Chapter 5. In addition, it also describes the materials in the form of hardware and software. The actual study is described in Chapter 6. First, a home access control system is analysed, thereafter an investigation of P2P communication. Chapter 7 presents the result of the cases, which then are discussed in Chapter 8. The discussion also present the authors opinions about the technology as well as some countermeasurements that would make the close proximity technology more secure. Finally, a conclusion of the thesis is found in Chapter 9.

2

Introduction to Computer Security

Computer Security is a broad term. It covers areas such as application security, network security, cryptography, attack methods, but also soft topics such as social engineering and management. Since this thesis only treat cryptography and some technical attacks, the focus of this thesis is such technologies. The topics and technologies described are not limited to NFC and close proximity, but could be applied to many areas in computer science.

Risk management is very important in Computer Security. Risk is "An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result" [5, p. 16]. With that said, some vulnerabilities will therefore never be fixed, or set to a low priority due to very low risk and/or loss. This is important to have in mind when discussing computer security.

The majority of the concepts described below is based on two books, Computer Security - Principles and Practice by William Stallings and Lawrence Brown, and An Introduction to Computer Security: The NIST Handbook by Barbara Guttman and Edward A. Roback.

2.1 Security Objectives

There are three important security objectives to consider when securing a system. The following applies to information and services. The security objectives are *Confidentiality*, *Integrity* and *Availability* [5, p. 11]. See Figure 2.1 for a visual explanation.

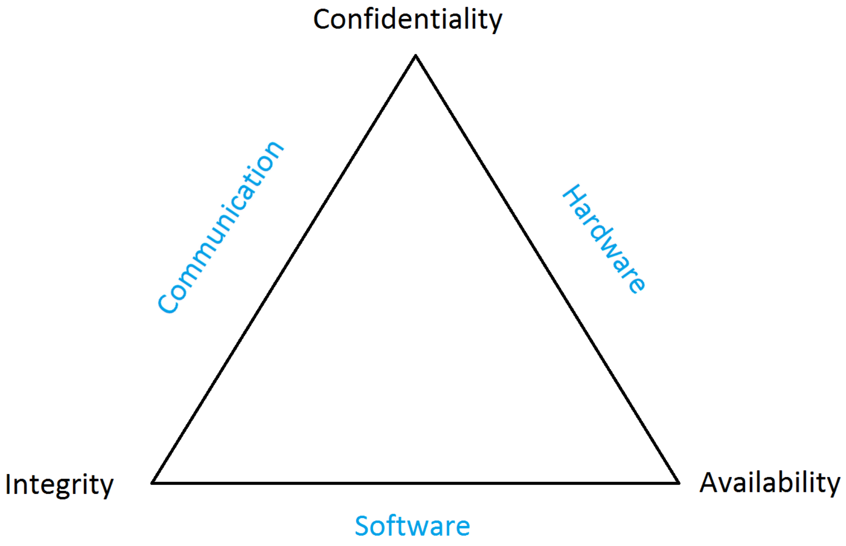


Figure 2.1: *Security Objectives.*

Confidentiality As defined by Stallings and Brown; "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information" [5, p. 12]. This means to protect the information from unauthorised access.

Integrity Securing the integrity protects information from being modified by an unauthorised entity. Stallings and Brown define integrity as: "Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information" [5, p. 12].

Availability Stallings and Brown define availability as: "Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system" [5, p. 12].

Responsibilities for the Security Objectives

To successfully fulfil the security objectives, the product or service needs to be architectured well. The communication is important to secure in order to ensure *Confidentiality* and *Integrity*. Encrypting and signing the communication is therefore needed.

The software in the system should be engineered to guarantee *Availability*, if it is required. It should also have an authentication mechanism to deliver high *Integrity*.

Hardware restrictions are important to prevent attacks on all of the Security Objectives, but mainly on *Confidentiality* and *Availability*. This is done by locking down the hardware from unauthorised access, and ensuring that the hardware have the ability to handle Denial of Service (DoS) attacks and common errors.

2.2 Breaching the Security Objectives

There are a few theoretical methods used to breach the Security Objectives. How it is performed practically depends on the system, but the desired result is to bypass one of the objectives and establish a breach. In all of these methods it is desired, but not required, that none of the communicating parties gain knowledge that they are being attacked.

2.2.1 Spoof

As stated by Howard and Longstaff, spoofing is defined as: "masquerade by assuming the appearance of a different entity in network communications" [6, p. 24]. This breaches the *Integrity* objective. A spoofing attack is shown in Figure 2.2.

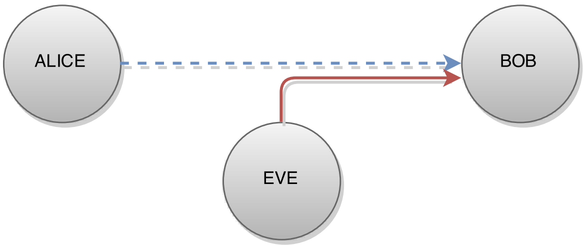


Figure 2.2: *Spoof attack where EVE use the privileges of ALICE to communicate with BOB.*

2.2.2 Eavesdrop

Eavesdropping is when an attacker gains access to a communication that is not intended for her. An eavesdrop could occur on any transportation media. This violates the *Confidentiality*. An eavesdropping attack is shown in Figure 2.3.

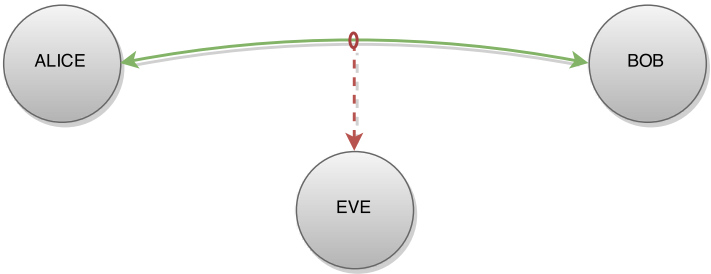


Figure 2.3: *Eavesdropping attack on ALICE's and BOB's communication, where EVE is eavesdropping.*

2.2.3 Relay

A relay attack is when an attacker initiates a communication with one out of two parties, and then relays the answer to the other party. If the communication goes both ways, the second party's messages is relayed back to the first party. A relay attack is shown in Figure 2.4.

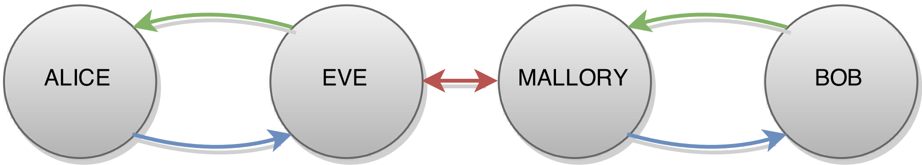


Figure 2.4: *Relay attack on ALICE and BOB, by EVE and MALLORY. EVE initiate the communication with ALICE, then forward the communication to MALLORY who transmit it to BOB, and vice versa.*

2.2.4 Replay

An attacker is listening to a communication between two parties and then replays selected message or messages to one of the parties. This attack method is often used in order to let the attacker authenticate as a trusted party. For example, a user sends credentials to a server, which then grants the user access. Meanwhile, the attacker have been listening and can later send the same credentials to the server in order to perform the same action as the user. A replay attack is shown in Figure 2.5.

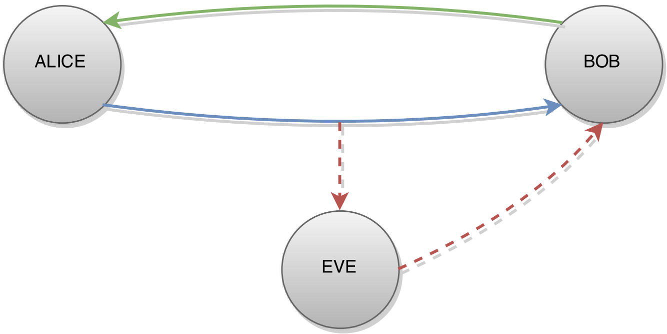


Figure 2.5: *Replay attack by EVE, on ALICE's and BOB's communication. EVE records messages from ALICE, then later replays them to BOB.*

2.2.5 Denial of Service

A Denial of Service (DoS) attack has the intention of breaching the *Availability* of a system. Howard and Longstaff defines it as: "intentional degradation or blocking of computer or network resources" [6, p. 22]. This could be done by performing actions to induce a system failure, disturb a communication or in any other way decrease an authorised users ability to access a system. A DoS attack is shown in Figure 2.6.

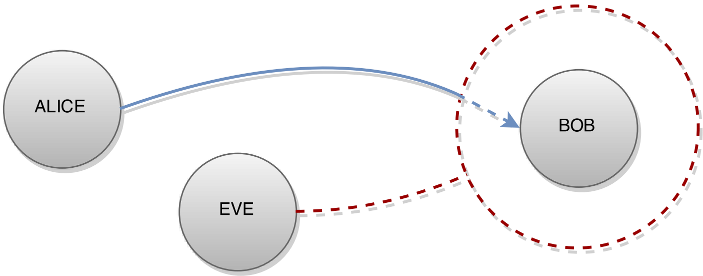


Figure 2.6: *DoS attack by EVE on BOB, resulting in ALICE being unable to talk to BOB.*

2.3 Number Generation

To securely use cryptography, random numbers are important. They are the foundation on which cryptography acts. If an attacker could predict random numbers, session keys or other secret types of data, secrets could be revealed and used to gain access to information. Therefore a good source of random numbers is needed. Devices with more computing power can use advanced algorithms or even dedicated devices that produce good random numbers. Devices with low computing power needs simpler and faster ways to generate random numbers, often by using algorithms to perform actions on allocated memory.

2.3.1 True Random Number Generation

To get true random numbers, information from multiple sources has to be gathered. These sources may include arbitrary factors such as noise in hardware, temperature, mouse- and keyboard clicks, milliseconds since boot or dedicated devices that measures cosmic background radiation or radioactive decay to generate random numbers. These methods provide a limited stream of entropy, and is often used as an Initial Vector (IV) in an algorithm that amplifies the limited entropy. For each request of random number, a new random IV is gathered and amplified to get a new random number.

2.3.2 Pseudo Random Number Generation

Devices with no ability to get good random numbers uses a pseudo random source. It is often algorithms where a number is used as an IV in order to produce a new number. The IV is then modified, based on the first value to create a new number. This approach may be vulnerable to prediction attacks where an attacker can predict a future random number based on earlier outcomes.

Linear-Feedback Shift Register

In order to create pseudo random numbers, a Linear-Feedback Shift Register (LFSR) is used on systems with low computing powers, such as DVD-players. At each new number generation, the register is shifted left. The tap sequence is what defines which bits that should be combined to provide the new rightmost bit. An LFSR is a periodic sequence with the size of $2^L - 1$, where L is the bit length of the register. All non-zero numbers are generated during a cycle. Since LFSRs are cyclic, an attacker with access to the tap sequence, register length and a generated number has the ability to predict all further generated numbers. Figure 2.7 and Figure 2.8 shows how a rightmost bit is calculated and used as input to get a new number. [7, p. 14-19]

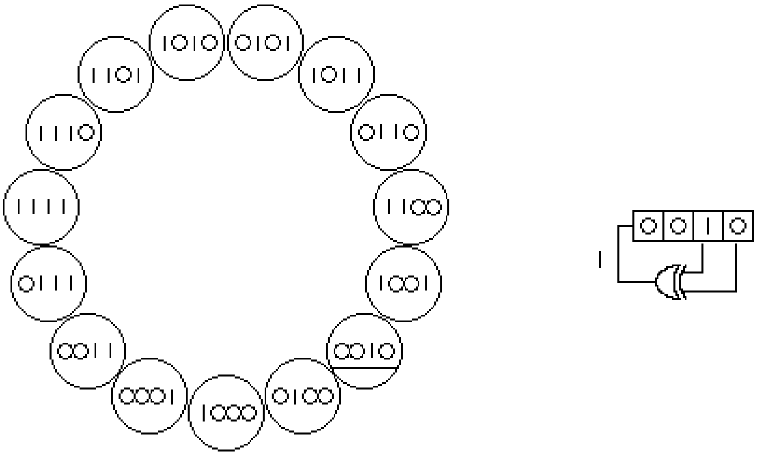


Figure 2.7: *State diagram of a 4 bit LFSR, state x. Remix of "State diagram 4-bit LFSR" by Cuddlyable3 on Wikimedia Commons. Licensed under CC BY-SA 3.0. [8]*

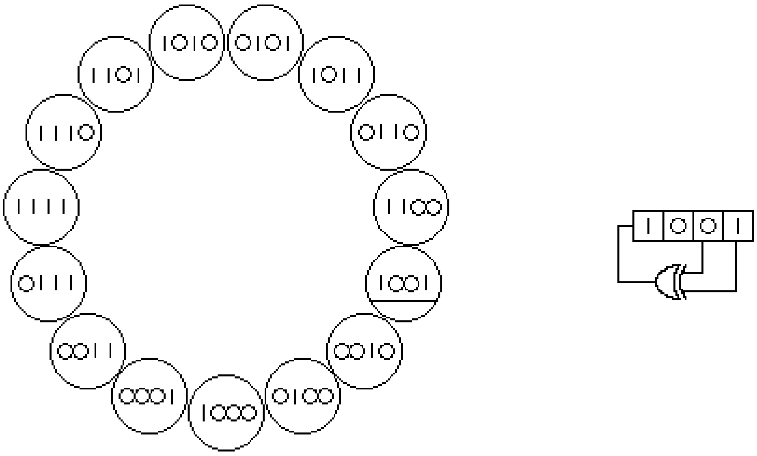


Figure 2.8: *State diagram of a 4 bit LFSR, state x+1. Remix of "State diagram 4-bit LFSR" by Cuddlyable3 on Wikimedia Commons. Licensed under CC BY-SA 3.0. [8]*

2.4 Encryption

Encryption is a way to make a message unreadable by an unauthorised user. This is done by scrambling the data with a predefined function, and using a key and the plaintext (the data that should be encrypted) as input.

There are two methods of encryption; symmetric and asymmetric. A symmetric encryption uses the same key for encryption and decryption. An asymmetric encryption uses one key for encrypting, and one for decryption. This is also called Public Key Encryption (PKE), since the key used for encryption is public and available to everyone, and the decryption key is kept private. There are numerous encryption schemes and algorithms used for encrypting and decrypting messages. Below is the important ones used in this thesis, grouped by method.

2.4.1 Symmetric Encryption

A symmetric encryption scheme uses the same secret key for encryption and decryption. This makes it reasonably fast and easy to use. It is important that the delivery of the secret key to the intended recipient is conducted using a secure channel. If N equals the number of people in a group, the required number of keys to be kept secure for a user is $N - 1$. For the group in total it is $\sum_{k=0}^{n-1} k$. This makes it hard to keep track of symmetric keys for many communications. A symmetric encryption process is shown in Figure 2.9. Below are examples of symmetric encryption schemes used in this thesis.

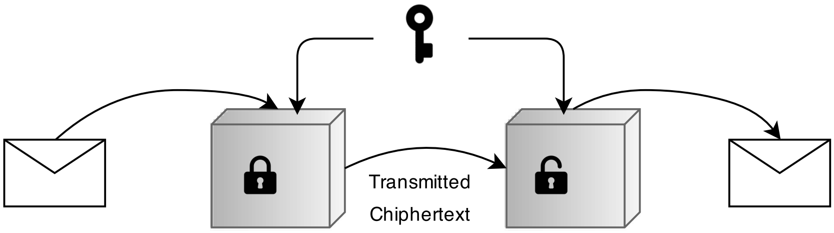


Figure 2.9: *A message is being encrypted and then deciphered. The message is encrypted and represented as the left box, and when the same decryption key is used to decipher the message in the right box, the message unfolds.*

AES

The Advanced Encryption Standard (AES) was standardised as a encryption scheme in 2001 by U.S. National Institute of Standards and Technology (NIST). Among 15 competing algorithms, the Rijndael algorithm was chosen as the used algorithm [5, p. 44]. AES is specified as a symmetric block cipher with length of 128 bits, using key sizes with lengths 128, 192 or 256 bits [5, p. 44]. There are no known practical attacks as of today, but there exist some theoretical attacks that decreases the schemes complexity or takes advantages of a side channel.

Crypto-1

The Crypto-1 encryption scheme is closed-source and owned by NXP Semiconductors. The technical specs for Crypto-1 was long a secret, but has been reverse engineered by Nohl et al. [9]. The report by Nohl et al. discovered that Crypto-1 consists of a single 48-bit LFSR, which is discussed in Section 2.3.2. Furthermore, Nohl et al. claims that Crypto-1 is using symmetric encipherment algorithms for its authentication mechanisms. Their thesis concluded that Crypto-1 is roughly following the ISO 9798-2 [10] specification, which is treating security techniques in information technology algorithms. On the same track, Sean O'Neil et al. concluded that the method used by Crypto-1 to grant security is substandard compared to other methods of encryption that exists [11]. Sean O'Neil et al. also claimed in their abstract: "We can recover the full 48-bit key of the [Crypto-1] algorithm in 200 seconds on a PC, given 1 known IV (from one single encryption). The security of this cipher is therefore close to zero" [11].

2.4.2 Asymmetric Encryption

Asymmetric schemes have separate encryption and decryption keys. The encryption key is public to allow others to encrypt with the same key. Therefore it is called the public key. This ensures that the recipient is the only party able to decipher the message. The decryption key is called the private key since it is not meant to be publicly disclosed. Access to the private key makes it possible to decrypt the information. [5, p 54-55]

The keys a user need to keep secure is only their own since all the encryption keys are public. PKE, or asymmetric encryption, is up to 1000 times slower than symmetric encryption because of the bigger numbers involved. Those keys therefore needs to be larger. An asymmetric encryption process is shown in Figure 2.10.

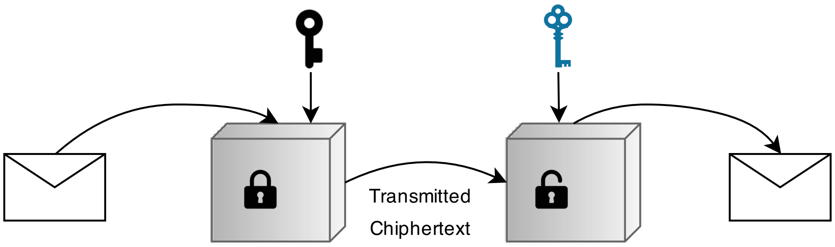


Figure 2.10: *A message is being asymmetricaly encrypted and then deciphered. The message is represented as the left box, and when the correct decryption key is used to decipher the message in the right box, the message unfolds.*

RSA

RSA is thoroughly described in Computer Security Principles and Practice (2nd edition) [5, ch. 21.3] as:

Quote 1. *One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978 [RIVE78]. The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n.*

There exist side-channel attacks on RSA that for example take advantage of the Central Processing Unit (CPU) or more correctly the voltage being sent to the CPU and analyse that information to break the cipher. Those are not practical to implement versus most of the systems since it requires hardware access which is rarely granted to an attacker.

2.4.3 Secure Device Pairing

This process is described by van Tilborg and Jajodia [12]:

Quote 2. *A classical way for two communication parties to establish a symmetric key without physical device contact is the Diffie–Hellman key agreement (DHKA). Denote the two communicating devices as A and B. The process of DHKA between A and B is sketched as follows: A and B both choose a common large prime p and a generator g, and each of them selects a random number a and b, respectively. Then they both publish their public numbers $X_a = g^a \mod p$ and $X_b = g^b \mod p$. Finally, A computes $(X_b)^a = g^{ab} \mod p$ and B computes $(X_b)^a = g^{ab} \mod p$ as the session key.*

This process makes it possible for two parties to agree on a key for a symmetrically encrypted communication using the same communication channel that previously needed an asymmetric encryption in order to be secure.

2.5 Man-In-The-Middle

A Man-In-The-Middle (MITM) attack is an attack on a communication between two parties. The attacker intercepts the messages and forwards it to the other party. This state can then be escalated by either getting the plaintext of the communication (violates *Confidentiality*) and/or modifying the plaintext or ciphertext (violates *Integrity*). A MITM attack can be followed by a spoofing attack, replay attack, relay attack and DoS attack. In a MITM attack neither of the parties is aware of the fact that they are not talking to each other directly, but through an attacker. A MITM attack is shown in Figure 2.11. [2, p. 6]

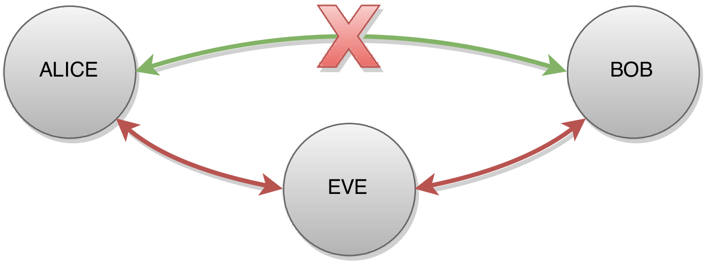


Figure 2.11: *MITM attack by EVE on the communication between ALICE and BOB.*

2.6 System Architecture to Prevent Attacks

To ensure the security of a system, security must be a part of its design. It can not be added after the implementation is completed, nor something an owner can save money on. If not prioritised, problems can occur. The cat and mouse game between the developers and the attackers is constantly in the attackers favour, since they only need to find one vulnerability to perform a successful attack. The developers, on the other hand, need to prevent all vulnerabilities in order to have a secure system. [5]

In modern software development a system is rarely an independent entity. It is usually dependent on functionality in the underlying operating system and correctly functioning hardware. Often third party code is used to speed up the development and reduce the cost for the client. The entire program is then used in environments which it have little or no control over. In order to keep the system secure, all links in this chain must be considered secure. A general advise is to never trust anyone using a system. A user may be someone with bad intent and must not be trusted. By validating and restricting input from the user, common problems such as buffer overflows and rounding errors can be prevented. All external communication need to be encrypted with well proven encryption schemes. This makes any data flow harder to either read or modify.

Even if actions have been taken to secure the communication, it is never advised to trust the communication, since a user can modify underlying software to establish a MITM. Every attack method needs to be thought about and, if possible, made harder to achieve.

2.7 Security Through Obscurity

Developers that relies on or uses secrecy of the system design, rather than a strong encryption scheme, as a layer of security is said to utilise security through obscurity. A system using security through obscurity relies on the possible security vulnerabilities remaining hidden or unknown rather than implementing a well known strong security scheme. [13]

2.8 Secure Element

A secure element is a hardware component which securely stores sensitive data, such as the decryption key for the devices public key [12]. It is stored in such way that not even the owner of the hardware could get hold of the data. Rather it is automatically utilised when sending and receiving data.

2.9 Temporary ID

A temporary ID is an identity token that is changed each time an entity is authenticated. This technique ensures that an attacker that has acquired the ID of a specific entity is incapable of using the ID for malicious reasons, due to the ID being changed each time it is used. The entity and the reader where the temporary ID is verified agrees upon a new temporary ID that is used the next time the entity tries to authenticate.

3

Introduction to Close Proximity Systems

This chapter presents general technical background about the RFID and NFC technologies as well as some more advanced technologies. The RFID and NFC technologies are presented together due to their close relation to each other. The beginning of this chapter presents a brief historical overview, followed by the general components and standards used in NFC technology. Then some specific techniques are presented, as well as some security considerations.

3.1 Historical Overview

The roots of the RFID technology can be traced to the Second World War, where radar was a common way of detecting aircrafts. The problem was that there were no way of distinguishing friend from foe. The Germans discovered that if the pilots returning to the home base barrel rolled their planes, the wings would create a change in the reflected radar signal, thus indicating that it was a friendly aircraft rather than an Allied spy plane. This was essentially the first RFID system. [14]

The founder of the radar, Sir Robert Alexander Watson-Watt, worked to improve this technique of detecting aircrafts by placing transmitters aboard British planes. When the transmitter received signals from the ground, they began broadcasting back that they were Brittish. The RFID technology works in the same manner. The initiator sends a signal that initiates a target, which then responds. [14]

An active RFID PICC with rewritable memory was first claimed as a patent in 1973 by Mario W. Cardullo, but it was not until Charles Walton filed a patent for a passive transponder the same year that the patent got recognised. The technology was then widely adapted by the industry, where it was most commonly used for identification of products. Later, the technology has been adapted to access control systems, payment systems, contactless smart cards and anti-theft devices, to name some of the applications. Companies commercialised the technology over time, using the 125 kHz frequency at first, then moving up to the higher frequency of 13.56 MHz which were unregulated and unused in most countries and provided much higher transfer rates. The RF communication taking part at the 13.56 MHz frequency later became known as NFC. It can therefore be said that NFC is a subset of the RFID technology with additions, and with the amendment that it operates at the specific frequency of 13.56 MHz. [14]

To make the technology usable, common standards has to be agreed upon, so that different parties may communicate using the same technology. The first specifications regarding NFC was agreed upon 2004 by Sony, Nokia and Philips who later formed the NFC Forum [15], though the vast majority of the specifications considering NFC has been made by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), which are recognized standard setting organisations. The ISO/IEC standards has later been further documented by European Computer Manufacturers Association (ECMA), even though they generally consist of the same information. The following technical information relies on information from these standards, such as ISO/IEC 13157 [16, 17], 14443 [18, 19, 20, 21], 18000 [22] and 18092 [23], and is referenced accordingly.

3.2 Components of a Close Proximity System

NFC communication is performed between an *initiator* and a *target.* Examples of initiators are access card readers, bus card payment stations, and payment stations at the supermarket. The targets are the access cards, bus cards and payment cards corresponding to those initiators, and in addition different types of mobile devices.

In order to activate the target, the initiator generates an electromagnetic field. The initiator is shown as ALICE and the target is shown as BOB in Figure 3.1. The induction is specified in the NFC specifications to work at the 13.56 MHz frequency [23], but may in the RFID case be ranged between many different frequencies [18, 19, 20, 21]. This field is later referred to as RF, even though it is a purely magnetic field [24].

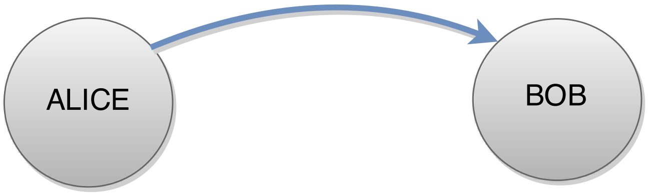


Figure 3.1: *The two most fundamental components of a close proximity system – initiator ALICE, and target BOB.*

It should be emphasised that the NFC technology is a subset of RFID characteristics with some additions, defined in e.g. ISO/IEC 14443 [18, 19, 20, 21], but have further restrictions and specifications. This thesis furthermost consider NFC specific implementations of the technology.

There are several differences between RFID and NFC. One of the specifications where the NFC technology differs from the RFID is the rules about how the initiator and target communicates, known as *coupling*, later discussed in Section 3.4. The standard for communication is called Near Field Communication Interface and Protocol 1 (NFCIP-1), further described in the ISO/IEC 18092 [23].

The components of an NFC system, compliant with the ISO/IEC 18092, should follow the characteristics shown in Table 3.1. The initiator shall generate a RF field at the frequency $\mathrm{f_c}$, with field strength between $\mathrm{H_{min}}$ and $\mathrm{H_{max}}$. Devices compatible with NFCIP-1 shall detect external RF fields with a strength higher than $\mathrm{H_{threshold}}$. [23]

Table 3.1: NFC-IP characteristics.

$f_c = 13,56$ MHz $\pm$ 7 kHz
$H_{\text{min}} = 1,5$ A/m (rms)
$H_{\text{max}} = 7,5$ A/m (rms)
$H_{\text{threshold}} = 0,1875$ A/m (rms)

There are two different types of communication – passive and active, with the most fundamental difference that passive communication consist of an unpowered target, while both initiator and target are powered in active communication.

In active communication mode both initiator and target use their own RF fields to communicate [23]. The initiator, e.g. ALICE, generates a RF field that activates the target, BOB, who then respond by creating its own RF field, as shown in Figure 3.2. The initiator and target takes turns in generating RF, clearly marking the end of a communication block, thus performing two way communication. Examples of an active communication mode are mobile payments and P2P communication between mobile devices using NFC, such as Android Beam [25].

To set up passive communication, the initiator, e.g. ALICE, generates an RF field that start the communication in passive communication mode. The target, BOB, responds by modulating the initiators RF field, as shown in Figure 3.3 this is referred to as load modulation [23].

The cheapest and most fundamental passive components are called PICCs. These have limited memory, almost no computing power and they get their power from the electromagnetic induction created by the receiver. PICCs can be implemented in different ways for different purposes. More information on PICCs are presented in Section 4.1, and can also be found in “Security in access control systems using RFID” [1].

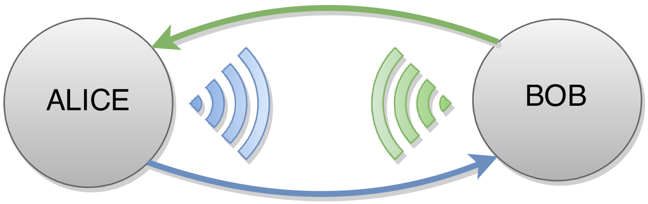


Figure 3.2: *Active communication with initiator ALICE, and target BOB. ALICE generates an RF field, BOB responds by generating his own RF field.*

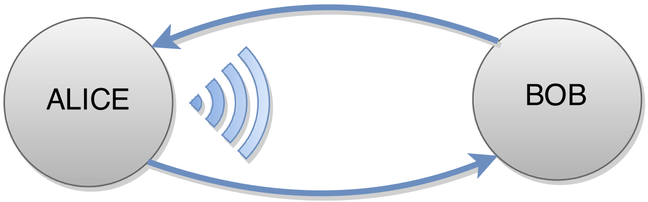


Figure 3.3: *Passive communication with initiator ALICE, and target BOB. ALICE generates an RF field, which BOB modulates.*

Both active and passive technology may be used in various different applications, for instance in prepaid solutions for public transportation and access control systems.

3.3 The NFC Protocol Stack

To make the NFC technology usable, common standards has to be agreed upon. In computer and networking context, these standards are often referred to as *protocols*. A *protocol stack* is therefore a representation of the different protocols regarding a specific technology and how these interact. Figure 3.4 shows the NFC protocol stack.

NFC is divided into the subcategories NFC-A, -B, -F and P2P, as shown in Figure 3.4. They have the same basic characteristics, as stated in 3.2. NFC-A and NFC-B are the most common technologies in passive communication. They are quite similar but differ for instance in the coupling mechanism initialisation and anticollision [23]. The NFC-F is only used by Sony in their FeliCa technology [27], and is not further considered throughout this thesis, since it is not as commonly used as the NFC-A and NFC-B technologies. Active communication mode is described by the P2P column in Figure 3.4. It has a specific component that makes it suited for P2P communication, namely the Logical Link Control Protocol (LLCP), which states a link layer standard for the communication, specified by the NFC Forum [28].

3.4 Communication Between NFC Compatible Devices - Coupling

According to Ernst Haselsteiner and Klemens Breitfuß [2], the coupling distance of NFC is theoretically somewhere around 10 cm, though it is hard to calculate the exact distance due to interferences and manufacturing differences in antenna windings and size. The coupling distance is in practice around 3-4 cm. This section describes the initialisation process of ISO/IEC 18092 and 14443, and the differences between them.

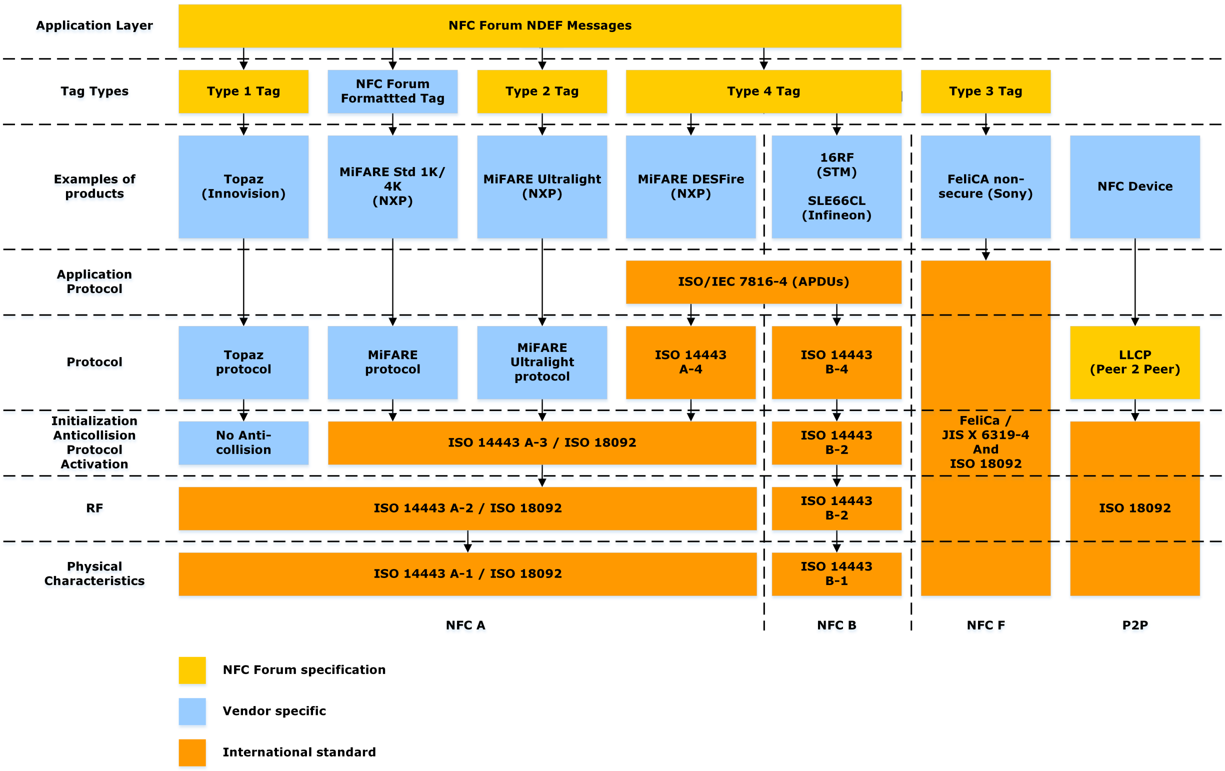


Figure 3.4: *"NFC Protocol Stack" by Erik Hubers - Own work. Licensed under CC BY-SA 4.0. [26]*

3.4.1 Initialisation Process and Transport Protocoll in ISO/IEC 18092

When an NFC device following the NFCIP-1 want to initiate communication, it should fulfil the following operations, according to the ISO/IEC 18092 [23]:

Quote 3. *The General Protocol flow between NFCIP-1 devices shall be conducted through the following consecutive operations:*

- *Any NFCIP-1 device shall be in Target mode initially and not generate an RF field, and shall wait for a command from an Initiator.*
- *The NFCIP-1 device may switch to Initiator mode and select either Active or Passive communication mode and transfer speed.*
- *Initiators shall test for external RF field presence and shall not activate their RF field if an external RF field is detected.*
- *If an external RF field is not detected, the Initiator shall activate its own RF field for the activation of Target.*
- *Exchange commands and responses in the same communication mode and the transfer speed.*

This tells us that an NFC device following the NFCIP-1 cannot generate a RF field, when another field at the same frequency f_c with magnetic field strength greater then $H_{threshold}$ is detected, with f_c and $H_{threshold}$ as given in Table 3.1. Thus making collision of communication for devices following the NFCIP-1 impossible.

The coupling process of devices following NFCIP-1 is shown in Figure 3.5. The first step in the initialisation process is to check for external RFs. If none detected, the initiator may chose either active or passive communication mode. This is where the initialisation process ends and the transport protocol starts. Protocol activation is generated by NFCID3, which is a random ID for transport protocol activation and the next step in the initialisation process. The initiator may switch parameters for the subsequent transport protocol using something called *parameter selection*. Then entering the data exchange protocol, which is where the exchange of information is performed. After the information exchange, the initiator sends a specific deactivation command, thus implying end of communication and the transaction is finished. This entire process is referred to as *coupling.* [23]

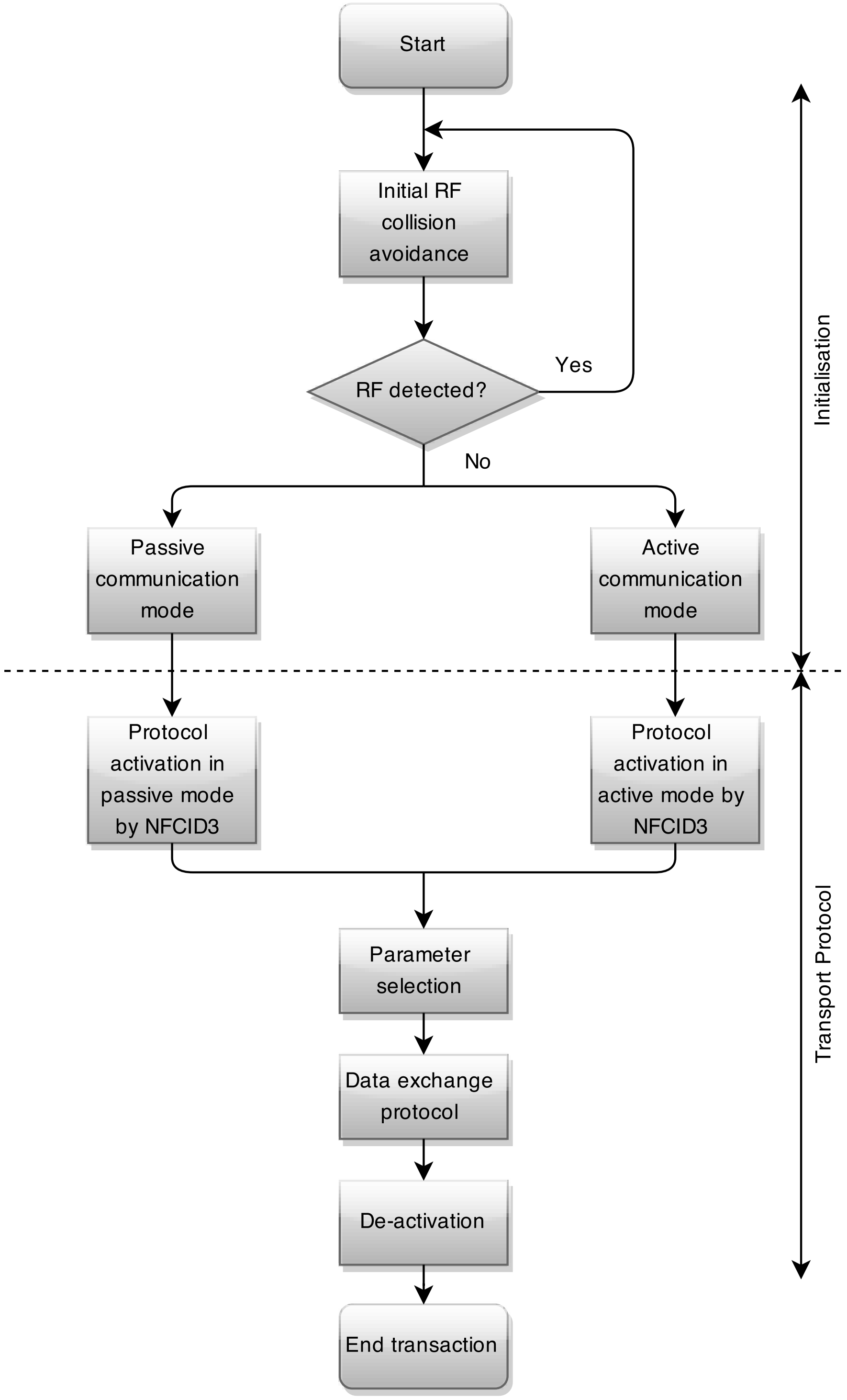

Start
Initial RF collision avoidance
RF detected?
Yes
No
Passive communication mode
Active communication mode
Protocol activation in passive mode by NFCID3
Protocol activation in active mode by NFCID3
Parameter selection
Data exchange protocol
De-activation
End transaction
Initialisation
Transport Protocol

Figure 3.5: *Coupling process of devices following the ISO/IEC 18092 protocol.*

3.4.2 Initialisation Process in ISO/IEC 14443-3

The initialisation process is divided into Type A and Type B, depending on the PICC, as seen in the NFC protocol stack in Figure 3.4. This thesis only consider Type A, due to its appearance in the later analyses. For more information about Type B, see ISO/IEC 14443-3, section 7 [20].

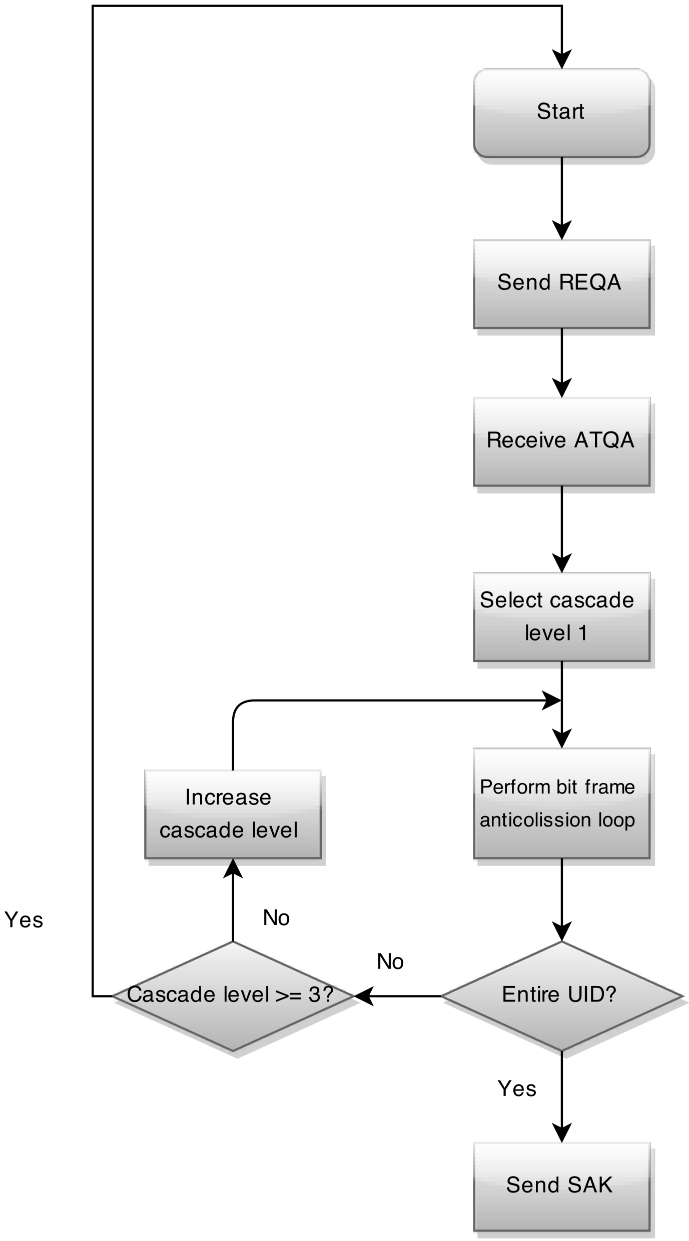


Figure 3.6: *Initialisation process for devices following the ISO/IEC 14443 standard.*

As seen in Figure 3.6, the request is started by a Proximity Coupling Device (PCD) (in this Section referred to as *initiator*) sending the Request command, Type A (REQA) to the PICC (in this Section referred to as *target*). This is the (request) command to read a PICC of type A. If a PICC of type A is found, it replies by sending Answer to request, Type A (ATQA). Cascade level is a variable related to the Unique IDentifier (UID) of the PICC. The cascade level can at most have the value three, meaning a maximum (triple) UID size of 10 bytes. After receiving ATQA the cascade level is set to one, and then an anticollision loop is entered where the PCD checks if the entire UID is received, as well as if more than one PICC responds. If not the entire UID is found and no other PICC is present, a jump back in the anticollision loop is performed and the cascade level is incremented to receive the rest of the UID. The PCD sends Select Acknowledge (SAK) if the entire UID was found. The PCD should then be paired with the PICC with said UID [20].

The anticollision loop is a mechanism that allows a PCD to handle many PICCs at the same time, which may be very valuable in some applications of the RFID technology, e.g. for scanning multiple products simultaneously in a warehouse.

3.4.3 Differences in Coupling Between ISO/IEC 14443-3 and 18092

The RFID and the NFC technologies are closely related. One of the greatest differences in the initialisation process of devices following the ISO/IEC 18092 [23] with devices following the ISO/IEC 14443-3 [20] is the ability of handling collisions. The ISO/IEC 18092 clearly states that *no* device following the protocol may generate RF-field while another RF is detected within close proximity. However the ISO/IEC 14443-3 has a function called anticollision loop and cascade levels, enabling devices following the ISO/IEC 14443-3 to handle more than one request at the same time. This may be applicable in, for example, warehousing applications and detection of multiple products at the same time. More information of the initialisation of RFID devices may be found in the ISO/IEC 14443-3 [20].

3.4.4 NFC Data Exchange Format

The NFC communication is transmitted using the Data Exchange Protocol defined in ISO/IEC 18092 [23] (Section 12.6). This protocol defines the format of the transmitted data and the protocol header for instance. Applications using the NFC P2P technology rely on the LLCP of the NFC forum, which in turn use the NFC Data Exchange Format (NDEF) [29] protocol for data exchange. The NDEF protocol is defined by the NFC forum, even though it is rather similar to the ISO/IEC 18092 standard.

3.5 Translating and Transmitting Data - Modulation

For NFC devices to be able to communicate with each other on the open RF, the digital information has to be converted into analogue signals and then transmitted. This process is called *modulation*. The reversed process, converting an analogue signal into a digital one, is known as *demodulation*.

Amplitude Shift Keying (ASK) defines how an analogue signal should be interpreted. It represents digital data as variations in the amplitude of an (RF) Carrier Wave, which is a waveform, usually in the form of a sinusoid, with purpose to convey information. There are two commonly used principles of implementing ASK, known as *Modified Miller* and *Manchester* encoding. These principles are further described by Bilginer and Ljunggren [24], and a brief description of the *Modified Miller* and *Manchester* encoding principles can be found in Appendix A.

3.6 Security in NFC Protocols

One of the problems with the NFC technology is that it does not support a common security standard for a secure channel and encryption of data. Attempts have been made to create a common standard for encryption by the ISO/IEC in their standards 13157-1 [16] and 13157-2 [17], but these has not yet been recognised and widely used.

The ISO/IEC 13157 standards states mechanisms of setting up so called Shared Secret Service (SSE) and Secure Channel Service (SCH) using the PKE technology (see Section 2.4.2). The ISO/IEC 13157-1 [16] and ISO/IEC 13157-2 [17] standards states different encryption theories used to ensure secure communication, containing some of the encryption theories presented in Section 2.4. These are widely recognised secure encryption standards, and a widespread usage of these would make the NFC communication more secure over all.

Referring to the NFC protocol stack, in Figure 3.4, it can be seen that none of the bottom layer standards contains any specification for secure channel, nor encryption of data. Since the NFC Forum clearly states that [28]:

Quote 4. *"The LLCP does not provide secure data transfer between any two service access points. Secure communication may be provided by the lower or upper layer protocols."*

Secure channel and encryption of data may only occur at the application layer of P2P communication. To conclude; the NFC technology does not by default support any security. Applications using NFC therefore explicitly have to utilise external security implementations.

4

Implementations of Close Proximity Technology

This chapter describes different implementations of the technology presented earlier in the Introduction to – Computer Security and – Close Proximity Systems chapters. First the implementation of passive communication named Mifare Classic is presented. The chapter also considers access control system implementations, contactless payments and finally P2P implementations.

4.1 Mifare Classic

Mifare is one of the cheapest and most widespread implementations of the PICC technologies. It holds up to 70% of the market shares in prepaid solutions for public transportation as of 2011 [30], and is eminent in various access control systems, electronic toll collection systems, school and campus cards, Internet cafés, car parking systems and employee cards. Mifare is created by NXP Semiconductors [31], and their most commonly used product is a PICC called Mifare Classic [32].

The general behaviour of the Mifare Classic PICC is the same as stated in Section 3.4.1, which is a very common implementation of the ISO/IEC 14443 standards [18, 19, 20, 21]. Still, the technology are compliant with various NFC applications, such as NFC PCD (see Section 3.4.3). Mifare Classic has some product specific implementations which are explained below.

Mifare Classic uses the proprietary cryptographic scheme Crypto-1, developed specfically for this PICC. As stated in Section 2.4.1, Crypto-1 does not provide any security since it is considered broken.

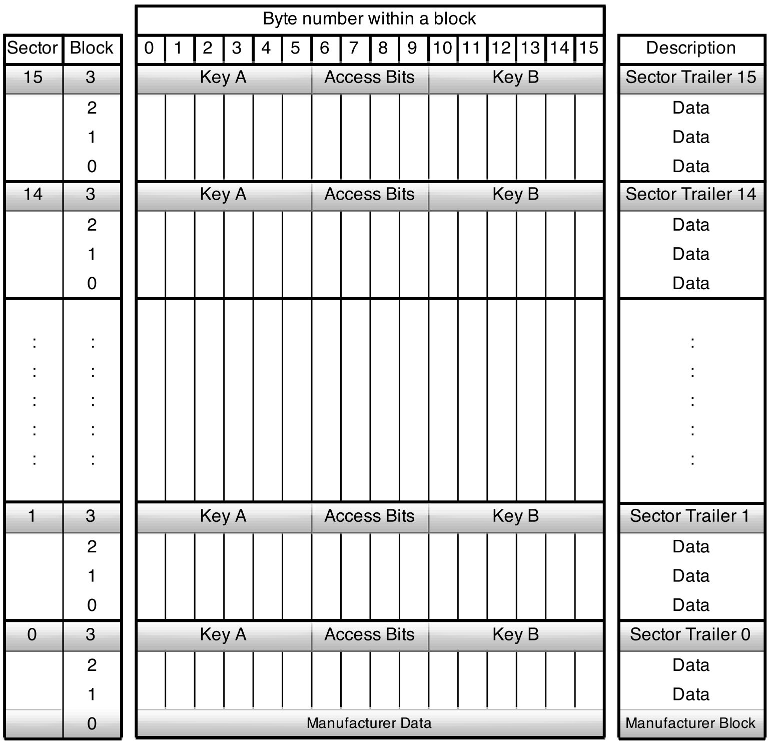
4.1.1 Memory Structure

Mifare Classic is available in 1K [33] and 4K [34], which refers to the amount of available storage on the PICC. The memory of the 1K model is 1 kB organised in 16 sectors of 4 blocks, whereas the 4K model contains 4 kB organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. Each block contains 16 bytes. Figure 4.1 shows the memory structure of the 1K model. The last block of each sector is called *trailer*, which contains two secret keys, refereed to as *A key* and *B key*. These keys may, when accessed properly, grant access for read, write or both read and write, for each block in the current sector. The trailer also contains *access bits*, which sets read and write permissions for the A and B keys. The access bits define permissions for each block individually. [33, 34]

Block zero, which is read-only, contains a UID that consists of either 4 or 7 bytes. This thesis refers to the blocks that are not trailers or block 0 as *data blocks*. The A and B keys are set to the hexadecimal value FFFFFFFFFFFF_{16} by default [33, p. 10].

4.1.2 Other Mifare Technologies

NXP Semiconductors does not only manufacture the Mifare Classic PICC, but also many other PICCs. Some of the other PICCs they produce are Mifare Plus and Mifare DESFire. These are considered more secure, since both of these use the secure symmetric encryption scheme AES [35, 36]. However, Mifare Classic is by far the most widespread PICC used today [37].



		Byte number within a block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	:
:	:																	:
:	:																	:
:	:																	:
:	:																	:
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0	Manufacturer Data																Manufacturer Block

Figure 4.1: *Memory structure of Mifare Classic 1K. The memory of the 1K model is 1 kB organised in 16 sectors of 4 blocks. Each block contains 16 bytes.*

4.2 Access Control Systems

Access control systems allows a selective access for a place or resource. Some of the traditional, most conventional ways of restricting access, is the use of keys and mechanical locks or the usage of physical guards. Nowadays, technology has increased the usage of electronic locks that use a unique identifier, which is confirmed by a database of authorised identifiers to granted access. These unique identifiers might for instance be a Personal Identification Number (PIN) accessed through a keypad, retinal scan, fingerprint reader or the use of a personal close proximity identifier. The combination of several of these unique identifiers simultaneously result in drastically increased security.

PICCs might be in the shape of a keyfob and they are often implemented to use passive communication. Many of the most common applications in access control systems using PICCs utilise the Mifare technology.

The most fundamental way of implementing an access control system using PICCs built upon Mifare technology, the person who wishes to access, e.g. Alice, presents the PICC to the PCD, e.g. Bob. After the initialisation process (see Figure 3.6), Bob knows the UID of Alice and can verify the UID against the access database. If a match is found, Bob gives access to Alice.

A study of an Access Control System

The access control system investigated in this thesis is using Mifare Classic PICCs for authentication. Such PICCs have got many vulnerabilities, some of them more severe [38]. One of the flaws with the implementation of this particular PICC is the fact that it uses the weak encryption Crypto-1. While investigating the security in home access control systems, one approach is – logically – to attempt to crack Crypto-1, and thus penetrate the home access control system. The attack study is explained in Chapter 6. A graphical representation of the access control system investigated in this thesis is shown in Figure 4.2

Figure 4.2: *Lock house and handle of an access control systems for personal use.*

4.3 Contactless Payments

A technology becoming more common is contactless payments. This is a technology that intends to simplify everyday payments by utilising close proximity communication to perform payments. There are different implementations of contactless payments, and this thesis presents two of them.

4.3.1 Smart Cards

This technology often use regular credit/debit cards with embedded RFID chips, often referred to as *smart cards*, to perform payments in payment stations supporting RF communication. The payment station work as initiator and the smart card as a target. The security in these systems is widely discussed and questioned. Dubinsky [39] shows some of the security flaws in these systems.

Another technology using smart cards is prepaid payment solutions, where instead of a credit/debit card, the smart card consists of a regular passive PICC. This technology is for instance used in public transportation. Common implementation of prepaid smart cards use the Mifare Classic technology, which makes the implementation vulnerable in many ways, for example due to its weak encryption.

4.3.2 Mobile Payments

There are different ways in which mobile devices are used to perform contactless payments, depending on the used application. In one of the most common applications the NFC technology is only used front-end to gain information about the current payment station. Then the application checks the payment station ID and performs the payment back-end. In this way no sensitive information is shared using NFC. [40]

Because of the fact that almost no sensitive information is transferred using NFC in close proximity payments almost no security is commonly applied in the NFC communication of the application. This creates vulnerabilities in the technology, e.g. relay and replay attacks, as shown by Roland et al. in their paper *Applying Relay Attacks to Google Wallet* [41]. To be able to perform a relay attack, one first need to intercept the information conveyed using NFC, thus implying that the technology also is vulnerable to the eavesdropping attack.

4.4 Peer-to-Peer Communication

A common implementation of the active communication mode is P2P communication. In this mode, the two communicating parties take turns to exchange information. The initiator start the communication while the target passively listen without generating its own RF field. The initiator clearly mark when the communication is finished, then enters passive mode to become the target of the other device's active communication [2]. A practical example of this is NFC communication between two mobile devices. NFC is supported in many of the modern mobile devices. Using for example the Android Beam technology [25], which is a technology using P2P communication between two mobile devices to share information, such as contacts, using NFC.

Since the NFC technology does not supply any embedded security by default, such as encryption of data, the security used in P2P has to be applied in the application layer of the NFC protocol stack. As seen in Figure 3.4, there is an empty block at the Application Layer of the P2P communication, thereby implying that the application independently has to provide standards. The security in P2P communication is varied depending on the used application.

Since both parts in the communication are powered, the application may use PKE to encrypt information in the P2P communication. If a secure element exists, the application may access the secure element as a decryption key for the asymmetric encryption. They may later agree on a symmetric encryption key for further secure communication.

5

Methodology and Laboratory Equipment

The foundation of this thesis is based upon a vast study of the close proximity technology and general computer security. The analysis is divided into cases chosen in such a way that they give a good general representation of the NFC technology. The goal of the cases is to cover different applications of NFC technology to get a good understanding of how the technology is used today, and the security risks that follows. Different attack methods are tested for both cases in order to breach the security constraints.

5.1 Methodology in Case Studies

A case study is a scientific way of setting up hypothesises and then testing those through e.g. laborations or experiments, summarise the results and present the work with a logical analysis. This process is described as highly iterative and tightly linked to empirical studies. [42]

Practical tests and a theoretical investigation are performed in order to assess the security in real world applications using NFC. The theoretical investigations also gives knowledge of today's systems even though no practical analysis is performed. This thesis contains two case studies, which are chosen in such a way that they give a wide representation of a variety of systems using NFC. The first case contains practical tests, while the second case has only got one small practical test. Instead, the second case contains more of a theoretical analysis.

Due to the sensitivity of the research, the name of the particular system analysed in Case 1 and its manufacturer, as well as specific details about how the attacks are performed, remains unmentioned.

5.2 Hardware

In order to perform practical tests for the attack methods, hardware is needed. The hardware that is utilised in the case studies is described in the following sections. Part of the laboration setup is shown in Figure 5.1.

Raspberry Pi The main component of the lab setup is three *Raspberry Pi B+* System-on-a-Chip (SoC) computers. This SoC is used because it has been thoroughly tested, is widely available and is relatively cheap. Due to the amount of interfaces on the Raspberry Pi B+, many different types of NFC expansion boards can be used.

NFC module Two different types of *PN532* NFC modules are used in Case 1: Home Access Control System. The first module is equipped with an NFC microcontroller connected via a Serial Peripheral Interface (SPI) to the Raspberry Pi's. The other module type is connected via USB to a laptop. The operating speed is greater when connected to a more powerful device; meaning that a modern laptop has greater performance than a Raspberry Pi.

Home Access Control System According to the manufacturer's specifications, the specific access control system investigated in this thesis utilises the Mifare Classic 1K technology for access control. One PICC can be used in six access control systems, and one access control system can have ten registered PICCs. Sector 0-6 of the PICC are allocated for the access control system. The remaining nine sectors (7-15) are left encrypted with standard keys, with the purpose of giving the user access to utilise them as he or she wants.

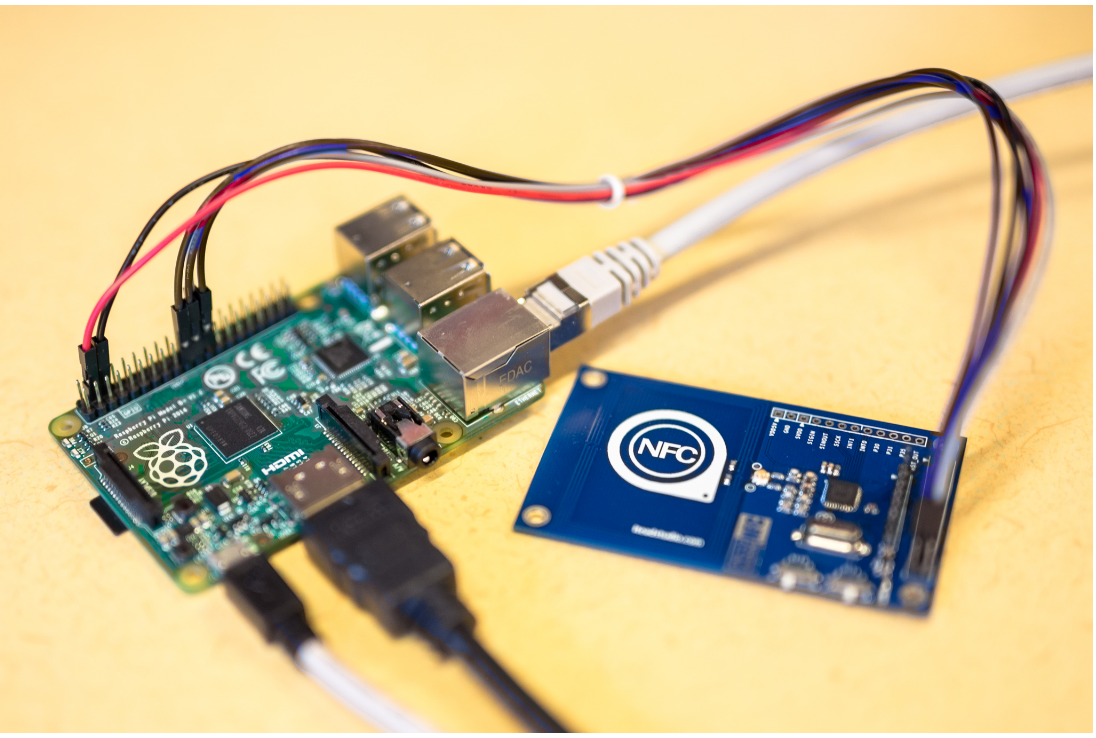


Figure 5.1: *NFC module connected to a Raspberry Pi.*

In order to achieve a higher level of security in the access control system each Mifare Classic 1K PICC has a Temporary ID (see Section 2.9). If an unauthorised PICC manages to get access through a system using temporary ID, the owner of the system notice on the next passage that an unauthorised passage has been made, and therefore has the ability to delete the intruders PICC from the system.

It is possible to use the access control system in more than one way; several settings are available for granting access. One of them, a numerical keypad, is found on the lock. This keypad could be used for authentication instead of the PICC. The owner of the access control system is entitled to choose if passage should be granted by introducing the right PICC to the reader on the lock, or if one should be allowed access by pressing the right personal code on the numerical keypad. This personal code is distributed by the owner of the access control system to someone that is allowed to enter. It is also possible to make both the PICC and the numerical code necessary for authentication. Thus, by further increasing the maximum number of combination patterns that could potentially allow access, the security of the electronic lock is enhanced.

The numerical keypad is used for one more reason – there is a six digit master code that invariably is granted access. If one has forgotten the personal code, or has lost the PICC, the master code grants access regardless of whom is using it.

Fully writable PICC As stated in chapter 4.1.1, the standard Mifare Classic PICC contains a memory block which cannot be changed or overwritten. An off-brand PICC without any write protected memory block is acquired to make a complete copy of a PICC. If the UID or the rest of block zero is used by a system to identify a card, full write access is needed to perform a successful copy of a PICC for that system.

Android Mobile Device Two mobile devices running Android version 5 are used in order to perform an analysis of the Android Beam application.

5.3 Software

Several open source softwares are used to perform the laborations in this thesis. Among many softwares, Raspbian, libnfc, MFOC and MFCUK are the most important. Added to these are scripts and code written by the authors.

Raspbian *Raspbian* is a *Linux* based operating system optimised to run on a Raspberry Pi. The advantage of using Raspbian is the large amount of software already included in the distribution. This ensures that as little configuration as possible is required. [43]

libnfc The software library *libnfc* make it easy to communicate to NFC PICCs by supplying an interface for the NFC module. All other software related to NFC used in this thesis uses functions and example code from this library. [44]

Mifare Classic Offline Cracker Mifare Classic Offline Cracker (MFOC) is an open source tool for finding encryption keys in Mifare Classic cards. MFOC utilises a weakness that requires at least one previously known key (A or B) [38]. Using this known key and the weakness in the Mifare Classic card all unknown keys are recovered relatively quickly [45] (see Section 2.4.1).

MiFare Classic Universal ToolKit MiFare Classic Universal toolKit (MFCUK) is an open source tool for finding encryption keys of Mifare Classic PICCs without any known keys. This tool uses notably more time per recovered key than MFOC and is therefore often used to recover only one key from a PICC. The remaining keys can then be recovered using MFOC. [46]

Android Beam Android mobile devices can communicate with each other with the help of an application called Android Beam. [47] This communication utilises NFC to establish a channel between the devices.

Custom Code and Scripts A bash script is created to simplify the process of finding encryption keys and creating copies of a PICC. This script reduces manual work and makes an attack against a home access control system an easier task.

6

Case Studies

The two investigated cases in this thesis are meant to examine different implementations of the NFC technology. The first case is focusing on the security of an access control system, and the second concentrates on mobile device communication. The first case undertakes a study of a spoofing attack and a DoS-attack, and in the second case there is a theoretical analysis of P2P communication. Both cases also determines whether it is possible or not to perform a relay attack in their respective area.

6.1 Case 1: Home Access Control Systems

Swedish insurance companies agree that all types of electronical locks does not fulfill the criterias needed to be classified as 'highly secure', thereby the system that is investigated in this case is not considered secure per se. [48]. However, in that classification, all types of electronical locks are merged into one. No consideration of which type of lock, or how it actually is implemented in reality is taken into account. The manufacturer of the access control system analysed in this case claims that their system is – if not the most secure – one of the most secure electronical locks there is. In this chapter a thorough investigation of the security of this home access control system is undertaken. This particular system uses NFC-technology for access verification.

6.1.1 Attack Vectors

This case involves three different type of intrusions; one that consists of spoofing, one that is utilising a DoS attack, and one relay attack. The following subsections describes the chosen attack vectors and their implementation in this project.

Spoof

The simplest way to spoof a Mifare Classic PICC is to read the original, authenticated PICC and then copy all of its data to another Mifare Classic PICC. Since block 0, containing the UID of Mifare Classic PICCs is read-only and cannot be written from one PICC to another, it is important when authenticating a Mifare Classic PICC to check if the UID is correct. This prevents spoofing using a standard Mifare Classic PICC as a fake PICC. There is however special Mifare PICCs where block 0 is writeable [49].

If one is trying to spoof a Mifare Classic PICC there are also several other different security aspects to consider. One concern is whether the A and B keys are specific to the system or if it uses standard keys, since a PICC with standard keys could be very easily read. If the keys are system specific, the next concern is to see whether all PICCs have the same keys, or if every PICC has its own key or set of keys. If every PICC of the system uses the same set of keys, an attacker would only need to crack one PICC in order to being able to easily copy every PICC used in the system. It is also important to examine if the access control system uses all following components when authenticating a PICC; the UID, the data contents of sectors 0-6 and the specific set of keys (if any) for sectors 0-6.

Relay

In access control systems it is very interesting to perform a relay-attack, since an attacker would not have to know anything about the information on the PICC in order to gain access to the facility. A relay attack could in theory be easily conducted with two NFC devices that can communicate with each other over distance, for example using mobile Internet.

Denial of Service

Finally it is of interest to determine whether a DoS is possible to perform and how easy it can be done. This can be performed in several different ways, for example by corrupting data on the Mifare Classic PICC or physically tampering with the access control system. Since this case focuses on NFC security the analysis of the DoS-attack only examines data corruption of the PICC. The complexity of performing a DoS depends on how the write access is implemented and the difficulty of obtaining the keys to the specific PICC, which is examined in the spoofing section.

6.1.2 Execution

Spoof

First of all an attempt to read the PICC is performed using the standard Mifare Classic key. If the PICC is not using the standard key, MFOC run on a Raspberry Pi is used to obtain the unknown keys. Once all unknown keys are obtained they are used in an attempt to read another PICC from the same system in order to determine if all PICCs in the system uses the same set of keys.

An attempt to spoof a PICC is performed using a Mifare Classic PICC with writable block 0. The entire content of the original PICC is copied to the false PICC in order to determine whether a spoofing attack is possible at all. In order to ascertain which components of the PICC that are used for authentication three more attempts are made to spoof the original PICC. To examine whether a component is used, it is overwritten with other data while the others are kept intact, and then an attempt to spoof is performed. The components checked are the UID, the data contents of sectors 0-6 and the specific set of keys (if any) for sectors 0-6.

Relay

This attack is tested in a laboratory environment consisting of a Raspberry Pi with two NFC boards and an instance of the access control system. The PICC is placed on one of the NFC readers connected to the Raspberry Pi. This reader is called a proxy reader. Further, the other NFC reader is placed on the access control system. This reader acts as a proxy PICC. The access control system then initiates communication with the proxy PICC, and this data stream is recorded and instantly sent to the PICC via the proxy reader. The response from the PICC is then recorded and sent to the access control system via the proxy PICC. If successful, this tricks both the access control system and the PICC that they are communicating directly to each other rather than through a third party. The data forwarding is repeated as long as the access control system and the PICC are communicating.

The library libnfc provides sample code to relay NFC communication between two NFC readers connected to the same device [50], in this case a Raspberry Pi. The sample code is rewritten to fit the purpose of this study. When the program is executed it presents the relayed data to the PICC that is placed on the proxy reader and the proxy PICC is presented to the access control system. All the data is then printed on the monitor.

Denial of Service

With all keys retrieved, it can be determined what information about the PICC that is needed to gain write access. Once write access is gained the content is modified in order to prevent the access control system from authenticating the PICC.

6.2 Case 2: Peer-to-Peer Communication

This case undertakes a theoretical approach rather than executing practical tests. However, a few practical tests are also performed. The case explores the vulnerabilities of the NFC P2P mode with respect to its use in mobile devices. Within the mobile device area, NFC and P2P is used for many different functions, and more come as the technology develops. Mobile devices equipped with NFC may use the technology for various purposes, such as transferring a file, performing mobile payments and as a supplement for various PICCs.

6.2.1 Attack Vectors

This case involves two different types of intrusions; one eavesdropping attack, and one relay attack. The following subsections describe the chosen attack vectors and their implementation in this project.

A study of the security behind the implementation of the Android Beam application is also undertaken. This analysis consists of an investigation of the security methods used by two Android mobile devices that are transmitting data to each others via Android Beam.

Eavesdrop

When utilising the P2P mode of NFC, the devices first set up a connection then communicate using NDEF (see Section 3.4.4). It is theoretically possible to eavesdrop on this communication, providing one is in possession of adequate equipment – such as antennas, amplifiers and software decoders further shown by Diakos et al. [4]. Even if the application being used implement a strong secure channel encryption on the communication it is still theoretically possible to eavesdrop. However, the extracted information does not make sense, but it could still be used for a replay attack.

Relay

To perform a relay attack against P2P NFC communication, two mobile devices can be used to relay the information between themselves. This can be done without the mobile devices being at the same location. The attacker can relay the information over e.g. Internet or any other communication medium. A relay attack could be used to relay credit card information from one person to a terminal, with purpose to use that information instead.

6.2.2 Execution

Eavesdrop

Eavesdropping on a connection over NFC P2P mode can be done with the use of an antenna and an oscilloscope [4]. The oscilloscope displays the electromagnetic waves from the connection as a sinusoidal. It is possible to convert those mathematical expressions to binary data with the right software and knowledge. A software program then interprets the binary data so the information is made readable.

Relay

Two mobile devices communicating with each other over NFC in P2P mode are exposed to a relay attack. This attack is performed by presenting two attacking mobile devices to the communication. When one of the victims devices initiate the communication, one of the attacking mobile devices intercepts that communication, and then relays it to the other attacking device using e.g. Internet. The second attacking device is then transmitting the communication to the target (the victims second device).

Android Beam

Using Android Beam, a mobile device can initiate communication with another mobile device. The NFC option as well as the Android Beam function need to be activated on both mobile devices in order to start the communication. The sender locate the directory where the wanted data is located, then tells the device to start to beam the data. Then, the device is moved in close proximity to the receivers device. The receiver needs to have the screen unlocked to be able to receive the data.

7

Results of Case Studies

The protocols that utilise NFC contains no embedded security. All the security in NFC systems is implemented at the application layer. In this chapter the results of each test case are presented. First, the results of Case 1 is presented, thereafter the results of Case 2 is presented, and both cases is summarised in a table.

7.1 Case 1: Home Access Control Systems

The outcome of each attack vector is presented under its respective caption. First, the results of the spoofing attack is presented, followed by the relay attack, and finally the DoS attack.

7.1.1 Spoof

Using the Mifare Classic standard key as A key for all sectors, an attempt was made to read the PICC. Access was not granted to sectors 0-6, which indicates that the A keys for sector 0-6 are different from the standard key. Using the standard key as B keys was however granted with read access. Once the B keys were obtained, MFOC was used to successfully acquire the previously unknown A keys. It was observed that all of the previously unknown keys were different from each other. The process of retrieving the keys took close to eight hours when a Raspberry Pi performed the calculations. The same process took under two minutes when a laptop with a Dual Core 2.6 Ghz CPU and a USB PCD was used. There were unsuccessful attempts at reading sectors 0-6 of the other PICCs belonging to the same system using the obtained A keys. This indicates that the PICCs have different sets of A keys for sector 0-6. All PICCs use the Mifare Classic standard key as B key.

When a spoof attack was performed using a complete copy of the original PICC, the access control system granted access to the false PICC. When attempts were made with any of the components – UID, data content or A keys – the modified access control system did not grant access, showing that it uses all three components to authenticate the PICC. This violates the confidentiality of the security objectives.

7.1.2 Relay

Unsuccessful attempts to perform a relay attack with two NFC readers connected to same Raspberry Pi was made. Access was not granted when one of the readers were presented with a PICC, while presenting the other reader to the system. It was seen that the communication started, but was then interrupted.

7.1.3 Denial of Service

It was seen that the access bits of sector 0-6 are set to factory default, which grants both read and write access using either the A or B key. Since all B keys of the PICCs are set to factory default, the data blocks could be overwritten, resulting in a successful DoS attack. The availability of the security objectives is thereby breached.

7.2 Case 2: Peer-to-Peer Communication

The outcome of each test vector is presented under its respective caption. The results of the eavesdropping attack is presented first, followed by the relay attack and finally the Android Beam analysis.

7.2.1 Eavesdrop

A successful eavesdropping attack on NFC communication has been made by Kortvedt et al. It gives the attacker full access to the information exchanged during the transmission [51]. Kortvedt et al. used an antenna and an oscilloscope to eavesdrop on the communication. The antenna used was the antenna from a Mifare PICC. Such antennas intercept the signals from the communication and displays them visually when connected to an oscilloscope.

7.2.2 Relay

As proved by Francis et al. it is possible to execute a relay attack against two mobile devices, thus breaking the confidentiallity of the security objectives. Francis et al. also states that the security in real world applications that are using NFC P2P communication can be circumvented. One thing that is emphasised is the fact that not only P2P communication using NFC could be exposed to a relay attack, but all kinds of NFC environments are in the danger zone. [52]

7.2.3 Android Beam

Successful attempts proved that when using Android Beam a receiver has no choice but to accept an incoming transmission. When two devices are trying to initiate a data transfer communication with Android Beam, given that the devices are in range of each other, the receiving device immediately starts to receive the incoming data stream, presuming the screen is unlocked. All the data is transmitted without giving the operator any choice of not accepting the transmission.

7.3 Summary of Results

The outcome of the performed attack vectors is summarised in Table 7.1.

Table 7.1: Summary of results.

Case 1	Spoof	✓
	Relay	✗
	Denial of Service	✓
Case 2	Eavesdrop	✓
	Relay	✓
	Android Beam	✓

8

Discussion and Future Work

This chapter intend to discuss the results of the case studies and the theoretical research together with suggestions of counter measurements and improvements of the technologies. The discussion illuminate both the weaknesses of the NFC technology that is analysed and the investigated applications. The authors opinions about the thesis, the general technology, and what effect it may have on the environment, is presented together with proposals on future research.

8.1 General Discussion About the NFC Technology

The main focus of this thesis has involved gathering information and understanding of the close proximity technologies RFID and NFC. Close proximity systems are a rather broad area of technology with many different applications who all make their own interpretation of the technology. Over all, the applications still have the same basic characteristics. An important finding in this thesis is that the NFC technology is a subset of RFID technology, with some additions. Other works vaguely imply the difference between the technologies, but we can after our research state that both the RFID and NFC technologies are a form of wireless communication technology, communicating using RF. RFID is ranged over a broad area of frequencies, and the NFC technology is restricted to communication at the 13.56 MHz frequency.

The next area of interest is how the communication is mediated. The standards describe that the communicating parties after an initiation process are *paired* to one another, and thereby can start exchanging data. The data is modulated from plaintext to radio waves by ASK. What the common standards do not tell are how one ought to know that no other than the intended target of the communication may intercept the radio waves. After the research and performed case studies, this thesis hereby states that the NFC communication at the frequency of 13.56 MHz is theoretically vulnerable for eavesdropping. This implies further vulnerabilities against other attacks, such as relay and replay.

Eavesdropped information is less useful if one cannot understand the meaning of the data. Therefore, the encryption of the communication at the NFC frequency is investigated. As stated in Section 3.6, the NFC technology itself does *not* contain any support for encryption of data. This implies that as long as one can intercept the communication it is also theoretically possible to understand it.

Encryption at the application level and usage of the NFC technology only as an identifier rather than a transfer medium, is the best way to make this technology even more secure in the future. The NFC technology can theoretically continue to be used in existing applications as long as the manufacturers using it are conscious of the flaws in the technology.

The attempt of standardise secure communication in the ISO/IEC 13157 is a good start towards a more secure technology. But to truly obtain secure close proximity communication this standard has to be widely recognised and implemented, for instance in the NFC protocol stack. This would generate secure communication independent of the used application. The standards has not reached that level of maturity yet since the technology is fairly young. Still, the NFC technology is over all very useful and it can be applied in various implementations. Even though it has flaws in the security and some lack of standardisation in the protocols, this could be overlooked with good implementations of the technology. Another approach that is highly recommended is to replace the weak encryption used by the Mifare Classic PICCs to an AES encryption. This results in a problem for Mifare Classic PICCs since it does not have the required computational power that AES encryption requires. A complete overhaul of systems using the Mifare Classic PICC is therefore suggested.

This concludes that the overall security of the NFC technology is rather flawed, but with awareness of these flaws, security can be achieved in the application layer rather than in the NFC communication. It is also important for developers to be aware of the security flaws in order to not use NFC for security sensitive applications.

8.2 Discussion Regarding Case 1: Home Access Control System

The NFC part of the access control system analysed in this thesis has got too many vulnerabilities to be labelled secure. The security in the PICCs used in the access control system is poor. Standard keys are used in the PICCs which simplifies an attack further. An explanation of were the NFC part of the electronic lock is inadequate is presented in the following subsections.

One of the attack vectors tested, the relay attack, did not succeed even though a relay attack is theoretically possible. When the relay code executes it can be seen that data is relayed, but that the communication then is interrupted. This is presumed to be due to timing issues. The timing issues could possibly be circumvented with the use of hardware that is able to relay the data faster. Thus, the relay attack performed in this thesis did not violate any of the security objectives.

8.2.1 Mifare Classic

It is revealed that the security of the Mifare Classic 1K PICC is deficient for use in NFC systems that are keen about security. The reasons to why Mifare Classic is inadequate in this area are several, where one of them being the conventionally weak encryption used; Crypto-1. To strengthen the security of the Mifare Classic PICC its encryption should be changed. The encryption method should be adjusted to one that is more advanced, e.g. 128-bit AES. This may be problematic to perform both since the Mifare Classic does not have enough computing power to use AES, and that Crypto-1 and the Mifare Classic PICC are widely established which complicates the change to better alternatives. If both Crypto-1 and the Mifare Classic PICCs would be replaced all the current Mifare Classic readers has to be replaced as well. This is due to the fact that all the settled readers are assembled in such a way that they only accept PICCs with the Crypto-1 encryption. So, in short, it is a question of keeping the expense at bay. Replacing all existing NFC-readers is very costly and time consuming.

In retrospect, the main issue with the Mifare Classic card is the use of hidden functions. Crypto-1 can be seen as a trade-off between security and the limited processing power in the PICC. The security relies on the weak function to stay secret, which is security through obscurity. Instead of hiding inadequate security fixes from the user, resources should be invested in finding a solid solution to the problem at hand.

8.2.2 Keys and Access Bits

In the system investigated it is discovered that all the B keys are the default keys, set from factory. The decision to use factory default keys is a huge security risk taken by the access control system manufacturer. That decision enables attacks using specialised software, such as MFOC. Further, one can argue that the Mifare Classic PICC should require a change of the standard keys in order for the PICCs to work in external systems. This would guarantee that every system that is using Mifare Classic PICCs is a bit more secure.

It can also be argued against the usage of factory default access bits in combination with factory default B keys. As the system is designed right now, this leads to the opportunity to read all data blocks without knowledge of the A keys. It is a serious security flaw that an intruder is given read/write access with only a factory default key, since it enables an attacker to easily perform a quick DoS attack. It should however be noted that a spoof cannot be performed with knowledge only about the B keys, since the access control system authenticates using the A keys, and a PICC with incorrect A keys does not authenticate. To conclude this paragraph, it is strongly recommended to not use factory default access bits in order to reduce the possibility of an attacker getting read and/or write access.

It seems as though the A keys for sector 0-6 are a derivate of the UID using some unknown function. It was seen in Section 6.1.2 that sectors 0-6 have different A keys, which are also different for different PICCs. None of the three PICCs included in the access control system had any corresponding keys. This implies that the access control system has information about the different keys of the different PICCs. Since the system can be used with PICCs acquired separately or from other systems, it does not seem reasonable that all keys are stored in its memory, but rather calculated in some way. If this unknown function were to be known, anyone could read and copy any PICC much more easily.

8.2.3 Entry Permissions

As was stated in Section 4.2 the access control system has three different settings for granting entry permission. The first setting requires that a valid PICC is presented to the reader. The second possible tuning is that a numerical code consisting of at least six digits is entered on the numerical keypad mounted on the access control system. The third setting requires that both a valid PICC is presented to the reader and that the correct numerical code is entered on the keypad, else the access control system does not grant passage. Due to several levels of security, the third setting of the lock is the most secure. As of now an operator can choose to bypass some degrees of security. The access control system would become more secure if it required both a numerical code and a PICC for granting access permission, instead of letting a user authenticate using only a PICC.

8.2.4 Comparison of Electronic and Mechanical Access Control Systems

If the analysed access control system is compared with a more conventional lock, using physical keys, some differences are noticed. If the electrical lock is set to only require a numerical code to allow passage, it is impossible to drop any physical key, since there is none to lose in the first place. However, one can still lose the ability to enter through the access control system by forgetting the numerical code. Misplacing a physical key is far worse than losing a PICC or forgetting a numerical code. That is because if a physical key is lost, the whole conventional lock system needs to be replaced in order to keep the security at the highest possible level. If, on the other hand, a PICC is lost, the owner can expel that particular PICC from granting passage by deleting it from the access control system. When a lost PICC is deleted from the system, the owner only has to buy a new PICC from the lock manufacturer, and then adjust that particular PICC into a new authorised one.

One aspect where the conventional lock is ahead of the electric lock comes with the scenario where a burglar want to grant himself passage through the access control system by copying a victims home access PICC or physical key. It is much easier to clone the homeowners PICC and write the data to an empty PICC than copy and clone a physical key. The PICC could, with the right hardware, be cloned in a matter of seconds, whereas the physical key takes more time to reproduce. The traditional key also require that an attacker has full physical access to the key in order for it to be copied – it cannot be copied while it lies in the victims pocket. The burglar could clone the victims PICC e.g. while sitting next to the person on a public transport, since the PICC could theoretically be read from an instance of up to 10 cm. By using such a strategy, the victim does not with great certainty notice anything out of the ordinary. But, in reality, his or hers home is now open for the burglar to access as he pleases.

8.3 Discussion Regarding Case 2: Peer-to-Peer Communication

An improvement of the general implementation of NFC technology within the P2P field is desirable. This would ensure that it is even harder to modify, or in any other way perform malicious actions against communication between two mobile devices using NFC P2P. The following subsections describes a few possible improvements to this area.

8.3.1 Secure Channel

To make NFC really secure on mobile devices the use of PKE is a possible approach. With the use of PKE, the devices can agree on a shared encryption key over a secure channel. The shared encryption key can then be used for further encryption of the communication. Even if someone eavesdropped on the communication no understandable information would be acquired – especially if a strong secure channel is established.

8.3.2 Replay and Random Number Generation

If an eavesdrop attack is done against a secure channel, it is still possible to have some use of the eavesdropped information. This is due to the fact that it can be used for a replay attack as described in Section 2.2.4. An example of such an attack would be to store the credit data from someone paying with P2P technology. When the data is stored it can be replayed so that an additional payment is registered. This means that the victim ends up paying more than once for the same product. One countermeasure against a replay attack is to implement a function that adds a random number to the transaction. This number can be generated as described in Section 2.3. The communication is protected against a replay attack if a reply from either the target or the initiator is based on a random number that is specific for each transmission.

8.3.3 Android Beam

As shown in Section 6.2.2 Android Beam does not grant the receiver any choice regarding if he or she want to accept the incoming transmission or not. This enables the possibility of transmitting harmful files without giving the receiver a chance of declining those files. Such files could appear innocent to the operator, but in the background malicious programs that influence the receivers mobile device in a harmful way might be executed. A solution to this flaw is to require a confirmation from the receiver before the transmission starts. In this way the receiver would not be exposed to potentially hazardous programs without knowledge.

8.3.4 Mobile Access Control Systems

As both mobile devices and access control systems nowadays might be connected to the Internet, new innovative ways to gain access is to be expected. Access could be granted through an online application on the mobile device, which is communicating with the access control system. If the mobile device is compatible with the NFC technology, the device may be used as a close proximity identifier to grant passage through access control systems. The mobile device might enable PICC emulator mode and access the systems using the unique identifier of its secure element (see Section 2.8). This would work in the same manner as the passive PICCs that are common in today's access control systems. Stronger security could be applied to this technology by requiring a PIN in the access control application of the mobile device.

Further applications of mobile access control systems are for instance distribution of temporary accesses. Temporary access identifiers may be sent using conventional means of communication, such as email or text messages, but also directly through NFC P2P communication or dedicated applications. This temporary access identifier should be generated in alliance with the access control system which the temporary identifier intend to access tentatively through a dedicated application connected to the access control system. In this way specifications regarding the number of times, or during which time the temporary identifier is valid, could be configured in accordance with the access control system. This temporary identifier could then be presented to the access control system by a mobile device that is emulating a PICC, or through a dedicated app. The device require technology that allows it to have NFC in card emulator mode.

8.4 Mobile Payments

Since most of the mobile payment systems are closed for external investigation, it is hard to grasp the functionally of these systems. All one might say is that some of these systems use NFC in some way. One might only speculate in how different applications uses the NFC technology. Hopefully, no mobile payment application are using NFC technology to transfer the actual payment, nor any sensitive information, such as the bank account number. Since the NFC technology is vulnerable to eavesdropping attacks in general, as shown in this thesis, any sensitive information transferred using NFC risk being intercepted by unauthorised parties.

The most convenient way to implement a mobile payment system is, except for encryption of all NFC communication, to merely use the NFC communication as an identifier for correct payment. To clarify, say that a costumer, Alice, want to buy an ice cream from a pay desk, Bob, using NFC. Alice would present her NFC enabled mobile device in active communication mode to the NFC payment terminal of Bob. Bob's payment terminal could then reply by sending a unique payment identifier regarding the current payment to Alice's mobile device. This unique identifier would then be matched back-end in a payment application. Then, the actual payment is performed using existing secure payment standards over the Internet. When the payment is performed both Alice's mobile Device, and Bob's payment terminal, should be notified about the successful transaction, thus indicating the completion of the payment. Alice can now walk away with her ice cream. In this way, no sensitive information would be transferred using NFC. Even if the unique payment identifier would be intercepted during the communication between Alice's and Bob's devices, a possible intruder would not have any use of that information – as long as he or she does not wish to pay for Alice's ice cream.

Using the above discussed unique payment identifier, no sensitive information would be transmitted using NFC, but it requires both of the communicating parties to have a stable Internet connection. In order to be able to perform a mobile payment in an environment where one or both of the communicating parties lack Internet connection, this technology would not work.

In an offline mobile payment system using NFC, sensitive information regarding either bank account number or prepaid currency, would have to be transmitted. This information has to be cached locally until connection to the Internet is found, thereby creating vulnerabilities by offline attacks on the devices. Such offline attacks could be deletion of the stored data or manipulation of the payment communication. This kind of payment exist, only not in the country where this thesis is performed. Still, it is strongly advised against this kind of payment – if not, a highly competent encryption algorithm for encrypting the communication is recommended, as well as secure storage of the payment information.

8.5 Environmental Concerns

By further extending the usage of NFC technology, developments in the environmental area could be achieved. If NFC payment terminals were to replace regular cash registers and bank card readers in stores a lot of paper and plastic could be saved. Mobile NFC devices would then be used for purchases instead of the more conventional method consisting of trading cash or paying with a bank card. The mobile device is then, in addition to its current applications, used for all kinds of payments. Extending this idea, the mobile device could potentially also replace PICCs in access control systems. If that where to become reality, resources would be conserved due to the fact that there would be no need to manufacture PICCs or physical keys.

Another consequence that arises with the removal of cash is that the transportation of physical currencies to resellers, cash dispensers, and between banks would diminish. This would save expenses for banks due to their decreased need of secure travels and maintenance charges. Furthermore, reducing the number of transports helps lowering the total amount of emissions. However, if cash where to be replaced by mobile devices, which probably should be connected to the Internet, it can be argued that people's privacy is being limited. That is because it is easier to control where and when someone has paid for something.

8.6 Reflection of the Work

The aim of this thesis was to assess how secure real world applications using NFC technology are. Another aim was to clarify how the NFC technology operates. With the knowledge gained in the technical study and the practical cases, the authors concludes that the aim is reached – both regarding the security analysis and how the technology functions.

The systems chosen for investigation were meant to give a good representation of today's NFC market. Something that could have been done differently is to assess the security of more systems. As it is now, the security has been investigated in only one access control system and one software application using NFC. It would also be interesting to analyse the security of an access control system not using Crypto-1, meaning that the Mifare Classic PICCs are replaced with, e.g. Mifare DESFire. The reason to why DESFire was not investigated in this thesis is due to the fact that Mifare Classic is by far the most common PICC used in access control systems.

Assembling an antenna that can eavesdrop on NFC communication at higher distances is something that was not performed in this thesis. However, it would have been good for the results if it where shown that the small range of NFC could be extended via an attack vector.

8.7 Future Work

The aim of this project was to assert how the security of everyday close proximity systems is implemented. This thesis was limited to systems communicating at the NFC frequency of 13.56 MHz, which is a rather large technology. Future works can specialise in a broader analysis of the RFID technology. Fields that are suitable for additional research are described in the following subsections.

8.7.1 Security in Mobile Payments Using NFC

It is interesting to further investigate the security of mobile payment systems in collaboration with the systems suppliers. It would then be possible to perform practical attacks against those systems in a closed lab environment. A look at the back-end technology of a system that is utilising NFC is intriguing in order to see how the technology is implemented. Then, an investigation of the logic presented in Section 8.4 might be undertaken.

8.7.2 Construction of a More Secure Access Control System

Construction of a new access control system that is not using the Mifare Classic PICC would be satisfying. This system could use the same basic technology found in existing access control systems, but it should be implemented in a much smarter way insomuch as avoiding the known security flaws. It would also be interesting to use the NFC technology that is implemented in almost all new mobile devices for access control as discussed in Section 8.3.4.

9

Conclusion

This thesis concludes that the Near Field Communication (NFC) technology is a subset of the Radio Frequency IDentification (RFID) technology, with additions. RFID ranges over a broad area of frequencies whilst the NFC technology is specified to communication at 13.56 MHz. Due to the fact that both technologies communicate using radio waves, it is possible to eavesdrop the Radio Frequency communication and use the information gained to perform further attacks. There is no embedded security regarding secure communication in the NFC protocol stack. Security in the communication therefore has to be applied at the application layer.

From the results and discussion about Case 1, this thesis concludes that the Mifare Classic technology uses a weak encryption algorithm called Crypto-1. This algorithm relies on security through obscurity and it can *not* be classified as secure. Case 1 studies a commonly used access control system that uses the Mifare Classic technology, implemented with standard keys to access the data blocks. This makes it easy to perform attacks against the access control system. This thesis successfully demonstrate spoofing and Denial of Service (DoS) attacks.

Case 2 shows that the NFC Peer-to-Peer (P2P) technology does not implement any embedded security in the NFC protocol stack. Secure encryption of communication has to be implemented at the application layer. Android Beam is a commonly used application that implement the NFC P2P technology. This application does not give the receiver any option to decline reception of incoming transmissions, assuming the receiver has both NFC and Android Beam activated.

A counter measurement against the vulnerabilities of the examined close proximity systems is to make the security of the NFC technology more robust. This can be done by using NFC communication to convey payment identifiers, and not the payment itself, in mobile payment systems using NFC. Another example is to diminish the use of Mifare Classic Proximity Inductive Coupling Cards (PICCs) in benefit for a more secure PICC in access control systems.

Mobile devices compliant with NFC may be used in modern access control systems, as well as in contactless payments. Assuming the security of such systems is implemented in an adequate way, this technology could result in a positive environmental impact due to decreased use of materials.

With the acquired knowledge from this thesis, the authors hope that the NFC technology matures and become more secure to use for sensitive applications. The tested access control system hopefully improves and new products on the market should use more secure technologies.

The close proximity systems investigated in this thesis are considered insecure, though they can be implemented in a secure way.

References

[1] Daniel Fallstrand Robin Karlsson Viktor Lindström Robert Stigsson David Alm Hannes Eriksson. "Security in access control systems using RFID". Bachelor Thesis. Department of Computer Science and Engineering, Chalmers University of Technology, 2013.

[2] Klemens Breitfuß Ernst Haselsteiner. Security in Near Field Communication (NFC). Strengths and Weaknesses (2006).

[3] Keith Mayes Konstantinos Markantonakis Lishoy Francis Gerhard Hancke. Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones (2005).

[4] Tim W. C. Brown Stephan Wesemeyer Thomas P. Diakos Johann A. Briffa. Eavesdropping near-field contactless payments: a quantitative analysis (2013).

[5] Lawrie Brown William Stallings. *Computer Security - Principles and Practice*. Pearson Education, 2012.

[6] Thomas A. Longstaff John D. Howard. A Common Language for Computer Security Incidents (1998).

[7] Katerina Mitrokotsa. *Stream ciphers and pseudorandom numbers*. URL: `http://www.cse.chalmers.se/edu/year/2014/course/TDA351/lectures/lect12.pdf` (visited on May 14, 2015).

[8] Cuddlyable3. *State diagram 4-bit LFSR*. URL: `http://commons.wikimedia.org/wiki/File:LFSR-F4.GIF` (visited on May 14, 2015).

[9] Starbug Starbug Henryk Plötz Karsten Nohl David Evans. Reverse-engineering a cryptographic RFID tag (2008).

[10] International Organization for Standardization, ed. *Information technology - Security techniques - Entity authentication. Part 2: Mechanisms using symmetric encipherment algoritms.*

[11] Sean O'Neil Nicolas T. Courtois Karsten Nohl. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards (N/A).

[12] Sushil Jajodia Henk C. A. van Tilborg. *Encyclopedia of Cryptography and Security*. Springer US, 2011.

[13] Jargon File. *Security through obscurity*. URL: `http://catb.org/jargon/html/S/security-through-obscurity.html` (visited on May 18, 2015).

[14] Mark Roberti. *The History of RFID Technology*. URL: `http://www.rfidjournal.com/articles/view?1338` (visited on Mar. 25, 2015).

[15] NearFieldCommunication.org. *History of Near Field Communication*. URL: `http://www.nearfieldcommunication.org/history-nfc.html` (visited on Feb. 13, 2015).

[16] International Organization for Standardization, ed. *Information technology — Telecommunications and information exchange between systems — NFC Security. NFC-SEC NFCIP-1 security services and protocol.*

[17] International Organization for Standardization, ed. *Information technology — Telecommunications and information exchange between systems — NFC Security. NFC-SEC cryptography standard using ECDH and AES.*

[18] International Organization for Standardization, ed. *Identification cards – Contactless integrated circuit cards – Proximity cards. Part 1: Physical characteristics.* ISO 14443-1. 2008.

[19] International Organization for Standardization, ed. *Identification cards – Contactless integrated circuit cards – Proximity cards. Part 2: Radio frequency power and signal interface.* ISO 14443-2. 2010.

[20] International Organization for Standardization, ed. *Identification cards – Contactless integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.* ISO 14443-3. 2011.

[21] International Organization for Standardization, ed. *Identification cards – Contactless integrated circuit cards – Proximity cards. Part 4: Transmission protocol.* ISO 14443-4. 2008.

[22] International Organization for Standardization, ed. *Information technology – Radio frequency identification for item management. Part 3: Parameters for air interface communications at 13,56 MHz.* ISO 18000-3. 2010.

[23] International Organization for Standardization, ed. *Information Technology – Telecommunications and information exchange between systems – Near Field Communication. Part 3: Interface and Protocol (NFCIP-1).*

[24] Paul-Luis Ljunggren Bekir Bilginer. Near Field Communication (2011).

[25] Android. *NFC Basics.* URL: `http://developer.android.com/guide/topics/connectivity/nfc/nfc.html` (visited on Mar. 30, 2015).

[26] Erik Hubers. *NFC Protocol Stack.* URL: `http://commons.wikimedia.org/wiki/File:NFC_Protocol_Stack.png` (visited on Mar. 30, 2015).

[27] Sony Corporation. *FeliCa.* URL: `http://www.sony.net/Products/felica/` (visited on Mar. 30, 2015).

[28] NFC Forum. NFC Logical Link Control Protocol (2014).

[29] NFC Forum, ed. *NFC Data Exchange Format (NDEF). Technical Specification.* NFCForum-TS-NDEF_1.0. 2006.

[30] RFID Blog Editing Team. *NXP Leads the Growing Contactless Ticketing Market.* URL: `http://www.rfid-blog.com/?p=729` (visited on Apr. 1, 2015).

[31] NXP Semiconductors. URL: `http://www.nxp.com/` (visited on Apr. 1, 2015).

[32] NXP Semiconductors. *NXP Mifare Classic.* URL: `http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_classic/` (visited on Mar. 20, 2015).

[33] NXP Semiconductors. *MIFARE Classic EV1 1K. Mainstream contactless smart card IC for fast and easy solution development.* NXP Semiconductors, 2014.

[34] NXP Semiconductors. *MIFARE Classic EV1 4K. Mainstream contactless smart card IC for fast and easy solution development.* NXP Semiconductors, 2014.

[35] NXP Semiconductors. *MIFARE Plus.* URL: `http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_plus/` (visited on Apr. 1, 2015).

[36] NXP Semiconductors. *MIFARE DESFire.* URL: `http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/` (visited on Apr. 1, 2015).

[37] Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OV-Chipkaart project (2008).

[38] Roel Verdult Ronny Wichers Schreur Flavio D. Garcia Peter van Rossum. Wirelessly Pickpocketing a Mifare Classic Card (2009).

[39] Zach Dubinsky. *New credit cards pose security problem.* URL: `http://www.cbc.ca/news/technology/new-credit-cards-pose-security-problem-1.904220` (visited on Apr. 1, 2015).

[40] Seamless. *The payment revolution.* URL: `http://seamless.se/products/seqr/` (visited on Apr. 3, 2015).

[41] Josef Scharinger Michael Roland Josef Langer. Applying Relay Attacks to Google Wallet (2013).

[42] Kathleen M. Eisenhardt. Building Theories from Case Study Research (1989).

[43] *Official homepage for the raspbian project.* URL: `https://raspbian.org` (visited on May 4, 2015).

[44] *libnfc source code and official repository.* URL: `https://github.com/nfc-tools/libnfc` (visited on May 4, 2015).

[45] *mfoc source code and official repository.* URL: `https://github.com/nfc-tools/mfoc` (visited on May 4, 2015).

[46] *mfcuk source code and official repository.* URL: `https://github.com/nfc-tools/mfcuk` (visited on May 4, 2015).

[47] Android. *NFC Basics.* URL: `http://developer.android.com/guide/topics/connectivity/nfc/nfc.html` (visited on May 15, 2015).

[48] dinbyggare.se. *Dörrlås - En dörr är aldrig bättre än dess låsanordning.* URL: `http://www.dinbyggare.se/documents/pageblank.aspx?id=6172#godkanda-dorrlas` (visited on Apr. 17, 2015).

[49] *Reseller of sector 0 writeable Mifare Classic cards.* URL: `http://www.clonemykey.com/uid-changeable-writable-mifare/` (visited on May 5, 2015).

[50] Dario Carluccio. *nfc-tools / libnfc.* URL: `https://github.com/nfc-tools/libnfc/tree/master/examples` (visited on May 13, 2015).

[51] Henning Kortvedt and S Mjolsnes. "Eavesdropping near field communication". *The Norwegian Information Security Conference (NISK).* 2009.

[52] *Practical NFC Peer-to-Peer Relay Attack using Mobile Phones.* URL: https://eprint.iacr.org/2010/228.pdf (visited on May 6, 2015).

A

Modulation Using Amplitude Shift Keying

Appendix A intend to briefly describe the Amplitude Shift Keying (ASK) principles known as *Modified Miller* and *Manchester* encoding.

The usage of the different principles depend on the bit duration b_{D}, which can be calculated using the following equation:

$$b_{\mathrm{D}} = \frac{128}{D \cdot f_{\mathrm{c}}} s \tag{A.1}$$

Where $\mathrm{f_c}$ is the carrier frequency from Equation 3.1 and the value of D is given by Table A.1 and depend on the bit rate.

Table A.1: Overview of which D corresponds to which transfer speed and thereby ASK method.

D	**kbps**	**Principle**
1	106	Modified Miller
2	212	Manchester
4	424	Manchester

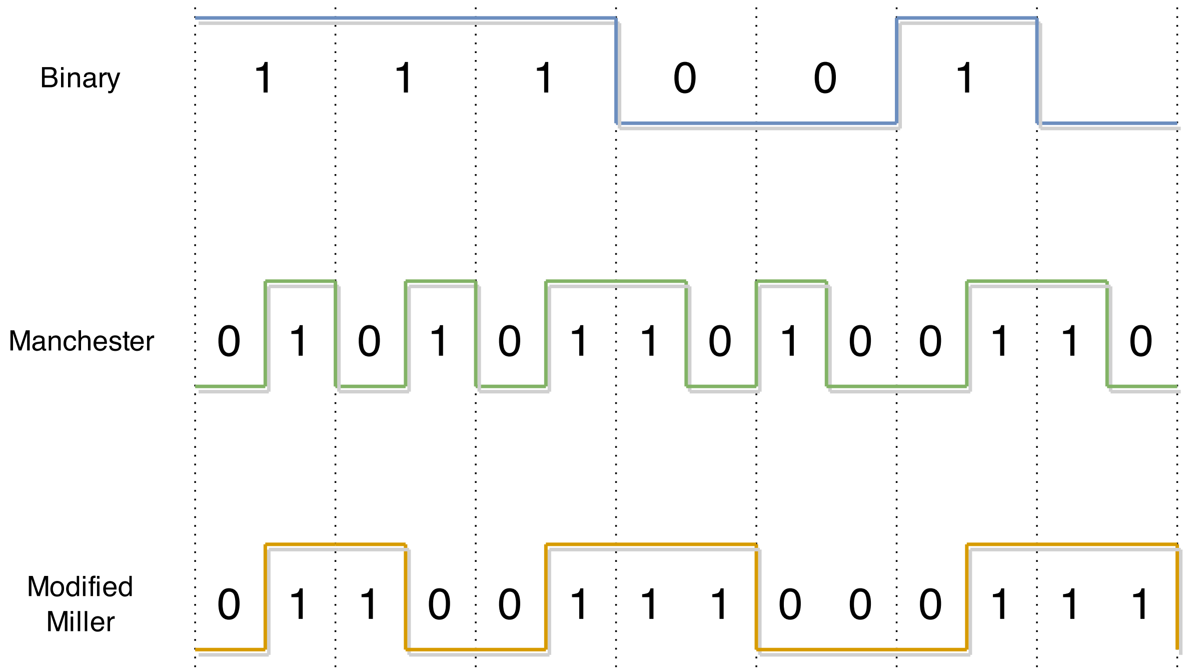


Figure A.1: *ASK of binary data using Modified Miller and Manchester method.*

A.1 Modified Miller Modulation

During 106 kbit/s transfer rate, Miller Coding with 100% ASK is used. This means the signal varies from no to full amplitude. Data can be changed from no signal to a signal with full strength, but doing it the other way around is practically impossible, further described by Bilginer and Ljunggren [24].

This principle interprets a change in signal over an oscillation, either from 0 to 1 or from 1 to 0 as a binary 1 . Subsequently it interprets the continuation of the career of either 1 or 0 over an oscillation as a binary 0, as shown in Figure 3.4.

A.2 Manchester Modulation

During higher bit rates, Manchester encoding is used with 10% ASK. Such a transmission varies between two amplitudes. Bilginer and Ljungren further describes the difference in the modulation scheme [24].

The Manchester encoding interprets a change in the signal from 0 to 1 as a binary one, and a binary 0 as the change in signal from 1 to 0 over an oscillation, as shown in Figure A.1.