Near Field Communication

A survey of safety and security measures

Bachelorarbeit

Sommersemester 2011

Martin Kerschberger
0825780
martin.kerschberger@student.tuwien.ac.at

Betreuung
Ao. Univ. Prof. Dr. Wolfgang Kastner

Vienna, July 17, 2011

Declaration

Hereby I declare that this work has been written autonomously, that all used sources and utilities are denoted accordingly and that these points of the work - including tables and figures - which where taken from other creations or the Internet have been marked as borrowing by quoting the original sources. This document will not be submitted to any other course.

Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen und Abbildungen -, die anderen Werken oder dem Internet in Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe. Diese Arbeit wird in keiner anderen Lehrveranstaltung zur Bewertung eingereicht.

Contents

List of Figures

List of Tables

Abbreviations

ABM	Asynchronous Balanced Mode
AEE	Application Execution Environment
AES	Advanced Encryption Standard
ATM	Automatic Teller Machine
CLF	Contactless Front-end
CRC	Cylic Redundancy Check
DOS	Denial of Service
ECDH	Elliptic Curves Diffie-Hellman
ECMA	European Computer Manufacturers Association
ETSI	European Telecommunication Standards Institute
HCI	Host Control Interface
HDLC	High Level Data Link Control
HF	High Frequency
IEC	International Electrotechnical Commission
I^{2}C	Inter-Integrated Circuit
ISO	International Organization for Standardization
LLC	Logical Link Control
LLCP	Logical Link Control Protocol
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP-1	Near Field Communication Interface and Protocol
NFCIP-2	Near Field Communication Interface and Protocol - 2
NFC-WI	NFC Wired Interface
PDU	Protocol Data Unit
PIN	Personal Identification Number
RF	Radio Frequency
RFID	Radio Frequency Identification
RTD	NFC Record Type Definition
SCH	Secure Channel Service
SIM	Subscriber Identity Module
SMC	Secure Memory Card
SMS	Short Message Service
SPI	Serial Peripheral Interface
SSE	Shared Secret Service
TEE	Trusted Execution Environment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
USB	Universal Serial Bus

Abstract

This paper gives a general overview of Near Field Communication (NFC) technology with a special focus on safety and security.

First, an introduction is provided on how NFC works. The associated hardware structure, standard communication methods, and the relevant international standards for NFC are discussed.

In the main section, this work examines the security and safety risks of NFC, summarizes built-in measures regarding security and safety and also suggests a principal protocol for safety integrated communication with NFC.

Finally, this work shows some applications, with focus given to aid organizations, which would benefit greatly from the use of NFC technology.

1 Introduction

NFC is a Radio Frequency (RF) technology for communication over short distances up to about 10cm.

It is mainly a logical advancement of Radio Frequency Identification (RFID). The history of RFID reaches back to the Second World War, where the British Air force tagged their planes with suitcase-sized devices to establish a friend-enemy-detection. The first commercial release came in the 1960's: 1 bit RFID for securing goods in shops, which is still widely used. In the 1990's RFID became more and more common e.g. for admission control systems or toll systems [37].

In 2002, NFC was developed by *NXP Semiconductors* and *Sony*. In general, NFC is compatible with existing RFID systems, but its architecture is different in principle. While RFID has only a reader - tag structure, an NFC device can be both reader and transmitter. In 2004, for better standardization the *NFC-Forum* was founded by the two developing companies. The forum now has about 140 members [17]. After this, the most NFC relevant standards were released as European Computer Manufacturers Association (ECMA) standards before becoming an ISO/IEC standard, by a procedure called *Fast-Track* [12].

The first NFC-compatible mobile phones were distributed by Samsung and Nokia in 2005. In the same year the first field trials in payment with NFC started in France [12]. The world's first commercial rollout of NFC was in Austria. *Mobilkom Austria*, *OEBB* and *Wiener Linien* placed about 450 NFC tags at vending machines to support the customer, in buying tickets for the railway and underground via SMS [39].

For the near future, commercial use of NFC technology is expected to increase. This is due to the fact that three smart phone operating system / device manufacturers Apple (iPhone), Google (Android) and RIM (Blackberry) have announced plans to include NFC in their next products. Additionally, *MasterCard*, an international debit card company, is about to start its *PayPass*, an NFC based payment solution [15].

1.1 Operation Modes

The most important NFC standards, in relation to the operation modes, are ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1) [23] and ECMA-352: Near Field Communication Interface and Protocol - 2 (NFCIP-2) [24].

NFCIP-1 combines the two RFID communication protocols: MIFARE (ISO/IEC 14443 Type A [31]) and FeliCa (JIS X 6319-4 [35]), and extends them with new communication possibilities and a new transport protocol. NFCIP-2 combines NFC with the functionality of RFID readers. This way NFC is compatible with most RFID devices [12].

Where RFID has strictly one or more passive components (tags) and one active component (reader), NFC breaks this up. For NFC devices it is possible to communicate with each other, acting as tag or as reader / writer. To ensure this, the *NFC-Forum* defines the following operation modes [18]: *Peer to Peer Mode, Reader / Writer Mode* and *Card Emulation Mode*. A systematic overview is given in Figure 1. Parts of the algorithms to determine which mode is used and to get knowledge of other NFC devices in range are defined in NFCIP-2.

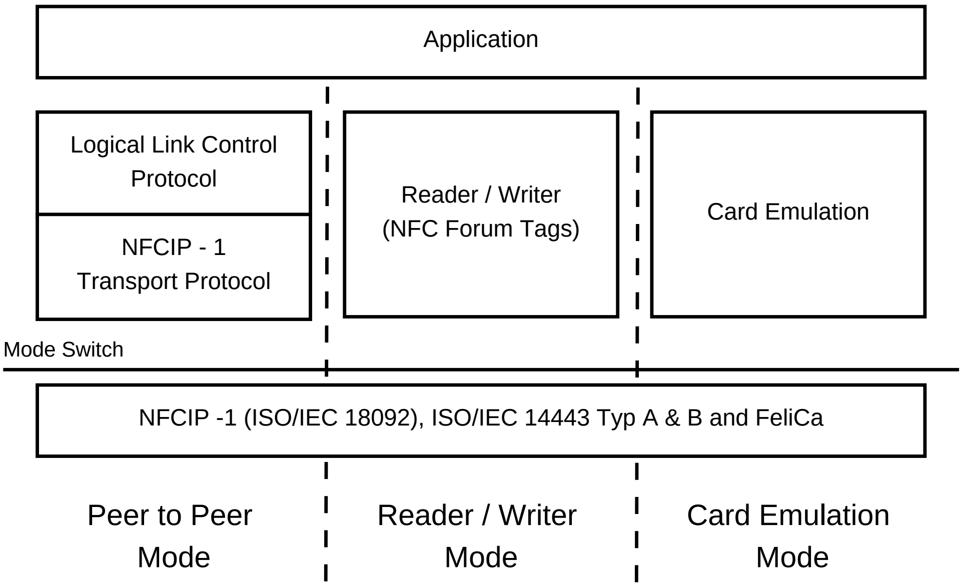
Application
Logical Link Control Protocol
NFCIP - 1 Transport Protocol
Reader / Writer (NFC Forum Tags)
Card Emulation
Mode Switch
NFCIP -1 (ISO/IEC 18092), ISO/IEC 14443 Typ A & B and FeliCa
Peer to Peer Mode
Reader / Writer Mode
Card Emulation Mode

Figure 1: Overview of the *NFC-Forum* operation modes [12]

Whereas most RFID readers are designed to be the only active devices in range, for NFC devices this assumption is not possible, therefore a collision avoidance is used. Also the recognition speed of devices in range should stay beyond 200ms, for proper usability. Many NFC devices are mobile and therefore have a narrow power capacity, since higher recognition speed requires more energy. There will be always a compromise between the detection speed and the energy consumption [12].

1.1.1 Peer to Peer Mode

Peer to Peer Mode enables communication between two NFC devices. The device which starts the communication is called Initiator, the other is called Target.

The *Peer to Peer Modes* protocol stack is organized similar to the *OSI Reference Model*, but has only 4 Layers: Physical, Media Access Control (MAC), Logical Link Control (LLC) and Application. Physical and Application Layers are equal to the *OSI Reference Model*, MAC and LLC build the Data Link Layer of the *OSI*

Reference Model, as shown in Figure 2. The Physical- and MAC Layer are specified by NFCIP-1; the LLC is specified by the *NFC Forum - Logical Link Control Protocol (LLCP) - Technical Specification* [21].

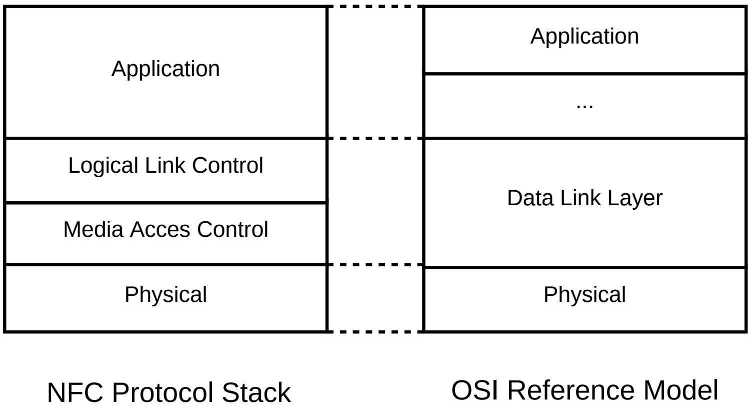

Figure 2: NFC Peer to Peer Protocol Stack versus OSI Reference Model [12, 21]

NFCIP-1 differs between an Active and a Passive communication mode:

"In the Active communication mode, both the Initiator and the Target shall use their own RF field to enable communication. The Initiator starts the NFCIP-1 communication. The Target responds to an Initiator command in the Active communication mode using self-generated modulation of self- generated the RF field."

"In the Passive communication mode, the Initiator generates the RF field and starts the communication. The Target responds to an Initiator command in the Passive communication mode using a load modulation scheme."

The main difference in these modes is the energy consumption of Initiator and Target. In the Active communication mode the power required for generating the RF field is shared by Initiator and Target, whereas in Passive communication mode the Initiator has to supply the power required for the field generation.

To ensure proper communication, NFCIP-1 defines the following protocol flow: All devices should stay in Target mode and don't generate an RF field as default. A device switches only to Initiator mode if it is required by the application, and the application defines the use of Active or Passive communication mode. Before activating the RF field the Initiator has to check against another active sender so no other communication is disturbed. If no other RF field is detected the Initiator starts communication and tells the Target to use Active or Passive communication mode and transmission speed. After communication, both devices switch back to Target mode and deactivate their RF fields [23].

In the MAC Layer only the Initiator can start a data transmission, the LLCP enables Asynchronous Balanced Mode (ABM) where additionally the Target is able to start a data transfer and error recovery is possible. LLCP is also capable of managing multiple application's access at the same time by multiplexing. It delivers a Connectionless Transport Protocol with a minimum of protocol overhead, for use when a higher level protocol uses flow control mechanisms. A connection-oriented transport protocol is also provided, which ensures a guaranteed and sequenced delivery of the data units. LLCP does not provide a secure data transfer mode [21].

1.1.2 Reader / Writer Mode

Reader / Writer Mode allows the NFC devices to communicate with *NFC Forum Tags*. These tags are typically passive components (see Chapter 1.3.1). Thus, this mode is also known as *Passive Mode*.

The tags can be placed in posters or other places and by touching the tag with the NFC device, the stored information is transmitted to the device. They can contain only information (e.g. Internet addresses) or perform actions on the device (e.g. connect to a Wireless Network).

This mode is fully compatible with the ISO/IEC 14443 and FeliCa technology and because of this, NFC devices can be used as readers / writers in existing RFID infrastructures. The *NFC Forum* does not include Vicinity systems (ISO/IEC 15693 [32]) to the *Reader / Writer Mode*, but NFCIP-2 does [12].

1.1.3 Card Emulation Mode

The optional *Card Emulation Mode* allows the NFC device to communicate with well known RFID readers. The device therefore can emulate one or more RFID smartcards. With this mode it is possible to use the existing contactless infrastructure e.g. for payment or admission control.

The emulation of the smartcard can be done either in application or in a so called *Secure Element* (see Chapter 1.2). A *Secure Element* is a device, similar to a real smartcard but uses an interface to the NFC device to transfer its data.

In combination with the *Reader / Writer Mode*, it is possible to implement a mode similar to the *Peer to Peer Mode*, but it is simpler because the protocol stack defined in *Peer to Peer Mode* is not needed. With the correct hardware implementation it is possible to use this mode even when the NFC device is switched off or is short of energy [12].

1.2 Hardware Architecture

NFC is an inductive coupled technology, the frequency of the RF field is 13.56 MHz. The specified data rates (106kBit/s, 202kBit/s and 404kBit/s) are a consequence of the compatibility with the MIFARE (ISO/IEC 14443 Type A [31]) and FeliCa (JIS X 6319-4 [35]) RFID standards.

The main components of the NFC environment are [12]:

- *Host-Controller*

  Application Execution Environment (AEE), the environment where the application rests e.g. mobile phone,

- *Secure Element*

  Trusted Execution Environment (TEE), the secure environment where e.g. debit card data are stored,

- *NFC-Controller*

  Contactless Front-end (CLF), the link between Host and NFC, with an interface to the *Secure Element*,

- *NFC-Antenna*.

1.2.1 NFC-Controller

The *NFC-Controller* is the link between *Air Interface*, *Host-Controller* and *Secure Element*. The *Host-Controller* is most likely a mobile device (e.g. a mobile phone, or a *smart car key* [38]). Between *Host*- and *NFC-Controller* there are interfaces like Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I^2C) and Universal Serial Bus (USB) in use. For the communication with the *Secure Element* there are typically smartcard interfaces, the *NFC Wired Interface* or the *Single Wire Protocol* in use. The Controller works as modulator / demodulator between the analog *Air Interface* and other digital interfaces. The *NFC-Controllers* have integrated microcontrollers, which implement the low level services, so the exchange with the *Host-Controller* is limited to the application Data and some control commands [5, 12].

In some cases (e.g. *Card Emulation Mode* for payment applications with mobile phones) the *NFC-Controller* and the *Secure Element* should still work when the host is turned off or the battery is empty. For such cases, the interface between NFC-Controller and *Secure Element* needs the possibility to power the *Secure Element* with the energy the *NFC-Controller* retrieves from the *Air Interface*. The *NFC-Controller* can be connected to more than one *Secure Element* [12].

1.2.2 Secure Element

On most mobile devices (such as mobile phones) there is no way to store secure data directly. But for most NFC applications (e.g. payment and authentication solutions) such a storage system is essential. For such data, the storage needs to be secured from manipulation. Thus, it must be able to execute cryptographic functions and to implement a secure environment to execute security-relevant software. Smartcards usually implements these requirements [12].

To implement such a *Secure Element*, there are different possibilities, each with its own advantages and disadvantages [12]:

- *Software without secure hardware.*

  Software is the most flexible and independent solution, but software could not be optimally secured without the hardware as there is always the possibility that the unsecured hardware is manipulated.

- *Device integrated hardware.*

  This is the most host dependent, but most reliable solution. The *Secure Element* is either a part of the host or is built in as its own chip. The communication with the element and the *NFC-Controller* works like a smartcard or over the *NFC Wired Interface* (see Section 1.2.3). The biggest disadvantage of this solution is, if the user changes the device, the provider of the secure service has to remove the data from the old device and to put it on the new one.

- *Changeable hardware.*

  In most cases, this would be the best compromise between reliability, usability and costs. Because a hardware interface is needed to plug in the removable *Secure Element*, the production costs of the host device are higher. Such removable devices could be a Secure Memory Card (SMC), which combines the secure smartcard functions with a usual memory card function, or a Universal Integrated Circuit Card (UICC); for example in a mobile phone this is the Subscriber Identity Module (SIM) card. On actual SIM cards there is only one out of 8 connectors free for use, so the *Single Wire Protocol* (see Section 1.2.4) was introduced by European Telecommunication Standards Institute (ETSI). While the SMC is usually owned by the user (he can change his data by himself), the SIM card of a mobile phone is owned by the network provider (the network provider must cooperate with the secure service provider).

An NFC system implementing a *Secure Element* is often called shortly *Secure NFC*, this is misleading because only the data stored on the *Secure Element* is secured, not the whole NFC communication [7].

1.2.3 NFC Wired Interface

The *NFC Wired Interface (NFC-WI)* (by NXP Semiconductors also called S^{2}C- Interface) is a two wire interface for data exchange between an *NFC-Controller* and the *Secure Element* and is standardized in ECMA-373: Near Field Communication Wired Interface (NFC-WI) [25]. It is shown in Figure 3.

It has two wires (Signal-In and Signal-Out) over which the NFC HF data is transferred directly. In this Interface the *NFC-Controller* is only the gateway between the *Secure Element* and the Air Interface. It is mostly used for *Card Emulation Mode*. Due to the direct NFC data transfer, this interface works on the NFC standard frequency of 13,56MHz and with the standard datarates: 106kBit/s, 202kBit/s and 404kBit/s [5, 12].

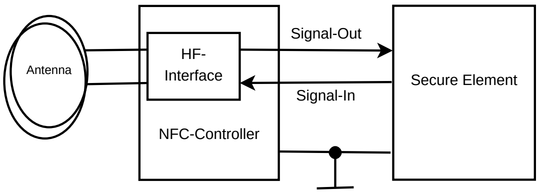

Figure 3: NFC Wired Interface [5]

1.2.4 Single Wire Protocol

The *Single Wire Protocol* is standardized in the ETSI TS 102 613: UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics [30] norm. It is shown in Figure 4.

It is a one wire interface over which the data and the energy is transferred. It was introduced, for the case when there is only one free connector on the usual 8 connector SIM cards. It is a Master-Slave-Interface, where the *NFC-Controller* is the master and the *Secure Element* is the slave. There is no connection between the *Secure Element* and the host, so all the data transfer must go trough the *NFC-Controller* by the use of Host Control Interface (HCI). The data transfer is managed by a High Level Data Link Control (HDLC) Protocol. Because the *Secure Element* drains its power from the *NFC-Controller* the *Single Wire Protocol* is an optimal solution for NFC-Services which have to work even if the battery of the device is empty [5, 12].

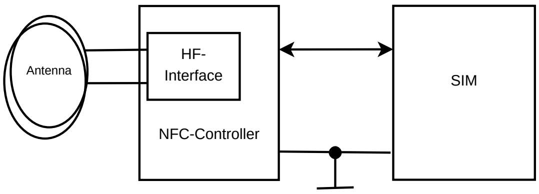

Figure 4: Single Wire Protocol [5]

1.3 Data formats

To gain compatibility between all the NFC and RFID devices from the different manufacturers the data exchange formats had to be standardized.

1.3.1 NFC Forum Tags

The *NFC Forum Tags* are an important part of NFC technology. They implement the passive storage devices which are used to build e.g. *smart-posters*, from which you can receive data by touching with an NFC device.

From the *NFC Forum*, there are currently four types defined, each device which implements the *Reader / Writer Mode* has to be compatible with them. Type 1 - 3 are based on existing RFID tags, but Type 4 consists of the existing smartcard standards. An overview is given in Table 1. The given limits of the memory size are a consequence of the addressing methods. Type 1 has only a collision detection but no collision avoidance, so there could be at most one tag in range. Type 2, 3 and 4 also implement a collision avoidance mechanism, so there could be more than one chip in range, at Type 4 the parallel use of them is also possible. A high priority point at specification of the *NFC Froum Tags* was that for communication and production of the tags no secret technology is needed, so everyone can produce them [12].

Tag type	Technology	Manufacturer	Standard	Size
Type 1	Topaz	Innovision	ISO/IEC 14443 A	$\leq$ 2048 Byte
Type 2	MIFARE Ultralight	NXP	ISO/IEC 14443 A	$\leq$ 2048 Byte
Type 3	FeliCa	Sony	JIS X 6319-4	$<$ 1 MB
Type 4	Smartcard	-	ISO/IEC 14443, ISO/IEC 7816-4	$<$ 512 MB

Table 1: *NFC Forum Tags* overview [12]

1.3.2 NFC Data Exchange Format

The *NFC Data Exchange Format* (NDEF) [19] defines a message encapsulation to provide communication between two NFC devices or an NFC device and an *NFC Forum Tag*. Because of this, data management in NFC devices is simplified. It guarantees a consistent format for data exchange in NFC applications.

"*NDEF is a simple binary data format, which encapsulates application payload. The reliable and secure transport of the data, is the charge of the protocol stack beneath, or the application layer above.*" [12]

An NDEF message consists of one or more NDEF Records. A single Record consists of a Header and a Payload field. The length of the payload is variable and is defined in the header. To determine the message length and organization, there are flags (e.g. for start message and end message) in the NDEF Record. There are also values to define the record type and the payload length in the header. [19, 12]

1.3.3 NFC Record Type Definition

NDEF Records provide the transport of data, but do not specify a guideline for usage or representation of the data, nor does the use of Multipurpose Internet Mail Extensions (MIME) types.

But in case of the manufacturer requesting overlapping compatibility guidelines like the *NFC Record Type Definition* (RTD) [20] are required. The RTD defines the principal semantics of the record types and each type has is its own specification. To give other organizations the possibility to specify their own types independently from the *NFC Forum* there is a classification in *NFC Forum External Types* and *NFC Forum Well-Known Types*.

The *NFC Forum Well-Known Types* are standardized by the technical specifications of the *NFC Forum*, which provide the guideline for processing and representing the data. They are:

- *Text Record Type*

  Simple Text, no specific application is assigned.

- *URI Record Type*

  Uniform Resource Identifier (URI) could be e-mail, web addresses, telephone numbers or other identification codes.

- *Smart Poster Record Type*

  is an extension of the *URI Record Type*, it provides extra information about the URI such as Icons or recommended actions.

- *Generic Control Record Type*

  provides a structure for any control activity.

- *Signature Record Type*

  a signature is provided to certify the correctness of the data (see Section 2.2.3).

- *Connection Handover*

  provides handover of an NFC connection to another communication technology with higher data throughput (e.g. Bluetooth).

1.4 Standards

Due to the high compatibility with RFID and other smartcard systems NFC consists of a lot of standards. Some of the most relevant are listed in Table 2.

Standard		Name
ISO/IEC 18092	ECMA-340 [23]	Near Field Communication Interface and Protocol (NFCIP-1)
ISO/IEC 21481	ECMA-352 [24]	Near Field Communication Interface and Protocol - 2 (NFCIP-2)
ISO/IEC 28361	ECMA-373 [25]	Near Field Communication Wired Interface (NFC-WI)
ISO/IEC 13157-1	ECMA-385 [26]	NFC-SEC: NFCIP-1 Security Services and Protocol
ISO/IEC 13157-2	ECMA-386 [27]	NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES Reference
ECMA-390 [28]		Front-End Configuration Command for NFC-WI (NFC-FEC)
ECMA-391 [29]		Memory-Spot Interface and Protocol (MSIP-1)
ISO/IEC 14443 [31]		Identification cards - Contactless integrated circuit(s) cards - Proximity cards
ISO/IEC 7816		Identification cards - Integrated circuit cards
ISO/IEC 15693 [32]		Identification cards - Contactless integrated circuit cards - Vicinity cards
JIS X 6319-4 [35]		Specification of implementation for integrated circuit(s) cards - Part 4: High Speed proximity cards
ETSI TS 102 613 [30]		UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics

Table 2: Listing of NFC and RFID standards

2 Safety and Security

In the previous chapter we showed the principles of NFC. In this chapter we will discuss the safety and security measures of NFC.

Safety is reliability regarding failures or an abstraction of avoidance of catastrophic consequences. Such consequences could be either physical injury of people or the damage of machinery. A quantitative definition can be given as the probability that the system will not exhibit a specified undesired behavior throughout a period of time [9, 36]. "*Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.*" [33] For a communication system, safety means that there is a guaranteed transfer of the data and given any disturbances there is a safe state where no catastrophic consequences can occur.

Security is the prevention of unauthorized access and unauthorized manipulation of data. There is no quantitative definition possible. *Security* is categorized in three sections [36]:

- *Secrecy*: the measurements to prevent data from unauthorized access,
- *Integrity*: the measurements to prevent data from unauthorized changes,
- *Availability*: the percentage of time for which the data is accessible.

There are many ways to break the security of a system. However, in our further considerations we mainly concentrate on the risks given by the *Air Interface* of NFC.

2.1 Attacks on NFC systems

Figure 5 gives an overview of the possible attacks on a *NFC Reader / Writer* environment. In the other communication modes the situation is similar. The *Air Interface* is always the same and the participating NFC devices can always be manipulated either by the owner / user himself or without the owner's knowledge by a hacker.

Based on the motivation these attacks can be classified in four categories [2]:

- *Spying*: unauthorized access to information,
- *Deception*: deceive through wrong information,
- *Denial of Service* (DOS): compromise the availability of the NFC system,
- *Protection of privacy*:

  "*Because the attacker believes that his privacy is threatened by the RFID system, he protects himself by attacking the system.*" [2]

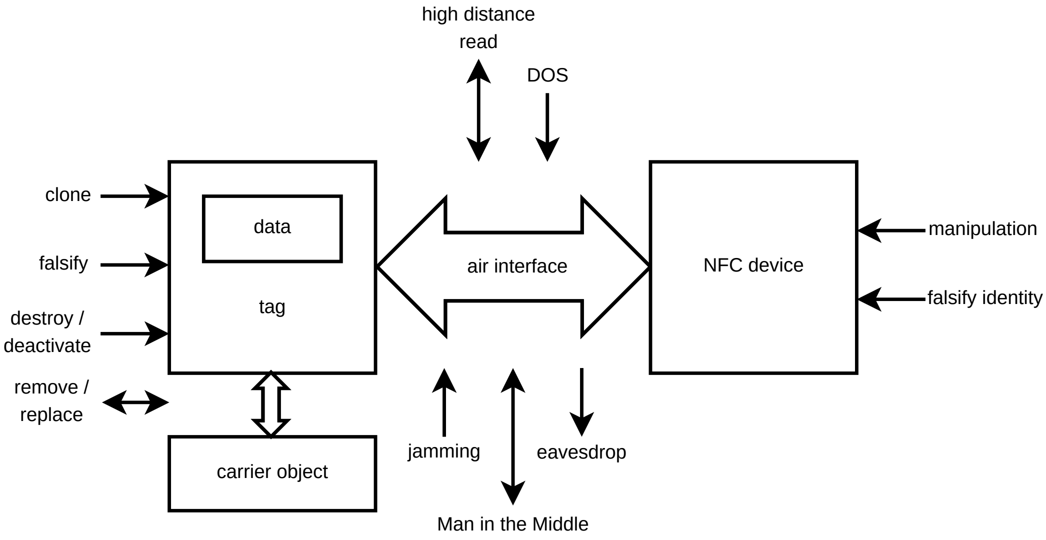

Figure 5: Schematic overview of the attacks on a NFC System [5, 2]

Attacks on the backend of NFC devices (e.g. a network connection to verify secure keys) would enlarge this work too much, so they are of no concern in our further discussion. For an introduction into these themes, refer to [14].

2.1.1 Attacks on the tag

The attacks which could be performed on the Tag are [5, 13, 2]:

- *Destroy*:

  This is the simplest attack which could be used. Afterwards the tag is not able to communicate any longer with an NFC device. It could be destroyed mechanical, for example by cutting the connection to its antenna. Another way to destroy the tag is an overpowered electrical field on the tags working frequency, so that the electrical components would overload. Destroying the electrical circuits of the tag could also be done by placing the tag into a microwave oven.

  This attack would compromise the *availability* of an NFC system.

- *Remove*:

  In this attack, the tag is removed from the carrier object. The motivation for this could be a thief, who wants to smuggle the carrier object through the security checks without recognition.

  This attack would compromise the *availability* of an NFC system.

- *Shield*:

  This attack is only temporary and it could be done by placing the tag inside a metal box or a wrapping it in tinfoil. The inductive coupling is disturbed by high losses caused by eddy current induction inside the metal. This method could be used, for example, to pass automated toll checkpoints without recognition. The tag is not destroyed permanently.

  This attack would compromise the *availability* of an NFC system.

- *Clone*:

  In this attack the original tag is read and an exact copy is created. The complexity of this attack depends on the tag. A read-only tag which stores only a simple numeric ID can be cloned very easily. There are also simple solutions possible where the ID can be changed. The reader can not decide if it is the original or the cloned tag. If some kind of certification is used, this attack would get more complex.

  This attack compromises the *secrecy* of an NFC system.

- *Falsify / Replace*:

  This attack overwrites the data of a tag or physically replaces it. Overwriting can be done easily if the original tag is a writeable tag without any security measures (or these measures are broken). The aim of this attack is to falsify the original tag, e.g. for phishing purposes.

  This attack compromises the *integrity* of an NFC system.

- *Tracking*:

  If a tag always uses the same unique ID for anticollision (or is a simple read only tag with a numeric ID) an attacker could track the tag easily. If the tag is always carried by the user, his movements could be tracked.

  This attack compromises the *secrecy* of an NFC system.

2.1.2 Attacks over the Air Interface

Due to the fact that the *Air Interface* is contactless, the attacks could be performed without physical access. That means that there are many possibilities for the attacker (or his equipment) to conceal his attacks.

The actual known attacks over the *Air Interface* are [5, 7, 13]:

- *High distance read*:

  The attacker modifies an NFC device, to increase its range, so he can read tags from a safe distance. This is not as easy as it sounds at first. The attacker has to increase the energy of the High Frequency (HF) field, use an optimized antenna and handle the increasing noise in the communication.

This attack compromises the *secrecy* of an NFC system.

- *Jamming*:

  At *jamming* a sender blocks the NFC system by sending a disturbance signal on its frequency (13.56 MHz). This sender must be either placed near the NFC system or use appropriate antennas and power rates.

  This attack compromises the *availability* of an NFC system.

- Denial of Service:

  As there could be more than one NFC device / tag in range, an anticollision algorithm has to be performed to select the individual device to communicate with. The attacker generates collisions / answers for every possible device address and simulates the existence of a high amount of devices in range of the reader. The reader will now try to reach each of the simulated devices to disable them and communicate with the desired device. But in the case that the reader can never reach the simulated devices, the desired communication is blocked.

  This attack compromises the *availability* of an NFC system.

- *Man in the Middle*:

  In a *Man in the Middle* attack two parties are tricked into a three party communication, without their knowledge. Instead of directly communication with each other they communicate through a third participant, who intercepts the messages between the other two. Thus he is able to modify data before sending it to the original receiver. An authentication system would not help, because the attacker can also intercept and set up one secure channel to the first party and a second secure channel to the second one.

  This attack compromises the *secrecy* and *integrity* of an NFC system.

- *Eavesdrop*:

  Since NFC systems communicates over an open (accessible) medium (air) with electromagnetic waves, eavesdropping is a logical attack. Because the receiver of the attacker does not need the power of the active part of the communication for answering, he would be able to amplify weak signals received over a distance up to 30 - 40cm [8, 10]. [10] shows that producing such a eavesdrop equipment can be done at relatively low coast.

  This attack would compromise the *secrecy* of an NFC system.

- *Relay Attack*:

  In this attack the invader uses another communication channel (relay) as an intermediary to increase the range. The attacker needs no physical access to the device, but only an antenna and the relay in reading range. The other, perhaps more conspicuous, devices could be far away.

  This attack would compromise the *secrecy* of an NFC system.

- *Data Modification*:

  The attacker utilizes modulation of the signal to provide the receiver a valid but manipulated message. The feasibility of this attack depends highly on the coding mechanism for the modulation, and the data can not be changed arbitrary but only to dominant states.

  This attack compromises the *integrity* of an NFC system.

- *Data Insertion*:

  If the answering device needs a long time for its answer, the attacker could insert a message into the communication. This would be only successful if the transmission is finished, before the answering device starts with its answer. Otherwise the message would be corrupted.

  This attack compromises the *integrity* of an NFC system.

2.1.3 Attacks on the NFC device

An NFC device could be a complex and powerful device (e.g. a mobile phone), so there is a high potential of possible attacks, for example hacking into an application which uses the NFC interface. The attacks on the NFC device could be performed either with the knowledge of the user (he is the attacker) or without the user's knowledge (e.g. a hacker accesses the device through an internet connection).

At the device level nearly anything could be done to compromise the NFC system (e.g. falsify data, or gain a stolen ID). The mainly targeted classes would be *integrity* and *secrecy* but *availability* is also possible (e.g. the device is used to perform a DOS attack).

2.2 Security measures in NFC

At the beginning of NFC there was no real focus on security measures due to its short range. Since there are concepts and plans to use NFC for payment and ticketing solutions, security became a high priority topic.

2.2.1 Measures against attacks

Most of the listed attacks could be prevented by using authentication and encryption methods. For example, eavesdropping would be possible, but if the data is encrypted, the attacker would not have use of it until he is able to decrypt it.

A difficult attack to perform is the *Man in the Middle* attack. All three devices, have to be in one range, and so will disturb each other. To get a stable working communication, the attacker in the middle has to shield the connection between the other two devices. This would result in an attack if one of the parties is removed and replaced. Such an attack could be prevented by the use of authentication through a common, independent, trusted certification provider [12, 7].

Experiments [8, 10] show that a passive eavesdropping attack is possible up to a distance of 30 - 40cm. This limits the possibilities for an attacker to hide (himself or his equipment). But in a crowded scene like a full underground train at rush hour, the equipment placed in a bag would not be suspicious and the owners would not notice that their device has been read from a person walking by. To prevent data stored on the NFC device from unnoticed read by an attacker, it would be necessary to have an application on the host device which asks for permission (e.g. by entering a PIN code) before granting access to the data. As there are cases where the NFC function should also work even when the host device is short of energy or is switched off, there should also be the possibility to disable the NFC function. A simple mechanical switch would solve this requirement. Switching of the device would then prevent an attacker from skimming the NFC data while walking by [13].

In [7] Haselsteiner et al. suggest, an encryption algorithm for NFC, which works with a low amount of computational power. After a synchronization phase both communication devices send randomized logical zeros and ones. Because NFC uses Amplitude Shift Keying Modulation, an eavesdropper would only know that both devices sent either a one or a zero at the same time or both have sent a different sign, but would not be able to determine which party has sent which sign. Each active communication party could retrieve the sign sent by the other one, knowing which randomized sign was sent by himself. This algorithm would work well, as long as the eavesdropper does not overhear the synchronization phase.

On the NFC device the connection between *Secure Element* and host controller (application) should also be secured. This is needed to provide the security for the PIN and other codes which have to be transferred between them. Lastly, the user interaction should be done in a way which is not possible to intercept or clone by another application [12].

2.2.2 NFC Security standard series

The NFC-SEC: NFCIP-1 Security Services and Protocol [26] and NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES Reference [27] were released in their first version in 2009 and are the standardized answer to the increasing requirement for security solutions in NFC systems.

NFC-SEC is the first part of the *NFC Security standard series*, and defines the common framework. This framework was created for securing the data exchange in *Peer to Peer Mode* and is placed above *NFCIP-1* (Physical and MAC layers) and below higher level protocols. It defines the necessary extensions to *NFCIP-1*: sequence protocols and other basic conditions.

There are two services: the *Shared Secret Service* (SSE), which defines methods for establishing a shared secret (key) with application specific encryption methods, and the *Secure Channel Service* (SCH), which not only provides the connection set up, but also the establishing of a secure, encrypted communication path for the data messages [12, 26].

The other parts of the *NFC Security standard series*: *NFC-SEC-XX* define specific cryptographic mechanisms. Together they define algorithms for *secure key exchange*, encoding and securing the data integrity and the sequence of the messages.

Currently only *NFC-SEC-01* is officially available, which specifies the *Elliptic Curves Diffie-Hellman* (ECDH) algorithm for secure key exchange and the *Advanced Encryption Standard* (AES) (defined in ISO/IEC 1803-3) for encrypting the data. It addresses NFC communications which should be secured, and where no key is shared a priori [12, 27].

2.2.3 Signature Record Type

NFC-SEC is targeted on two NFC devices communicating with each other in *Peer to Peer Mode*, so it gives no protection for an NFC device communicating with an NFC Forum Tag. This is where the Signature Record Type comes in. It gives the possibility to prove the authenticity of an NDEF record / message.

NFC Forum Tags do not have significant security protection, they only have a write protection against overwriting with falsified data. Because usually they should be commonly readable, an encrypted data transfer would be an overkill. But they need a protection against replacing the tag (e.g. for phishing purposes), so the use of signatures would be necessary [13].

"However, a malicious third party could delete the signature record from the NDEF message or attach a new signature record to prevent the user from noticing any malicious change of content. It must be understood that the verification is only as trustworthy as the tools (signature algorithm, certificate, etc.) and processes (e.g.,

security policies) that are being used. These risks, along with the use of the Signature record, should be taken into consideration in the development of applications." [22]

The *Signature Record Type* provides such a possibility to verify the integrity and authenticity of data through signatures. It is possible to sign one or more NDEF records inside an NDEF message with a *Signature Record*. The payload of the *Signature Record* consists of three fields [22]:

- *Version field*:

  Currently there is only one version of the record, so devices which implement the NFC Forums *Signature Record Type Definition - Technical Specification* [22], have to ignore any version other than 1 (0x01).

- *Signature field*:

  This contains either the actual signature or a URI which points to the signature. The *Signature Record* always certifies the previous NDEF records of other type; if previous records should not be certified, an empty *Signature Record* has to be inserted.

- *Certificate Chain field*:

  Finally, this contains the certificates necessary to authenticate the *Signature Record*. It contains a chain of up to 15 certificates, where the first one certifies the signature and the following certify the authenticity of up to 14 records.

2.3 Functional Safety and NFC

All of the above listed attacks which compromise the *integrity* and the *availability* could also be a problem for the safety of a system, but in a *functional safe* system, such errors should be recognized and there have to be measures against it.

2.3.1 Requirements and measures for functional safety

The standard ISO/IEC 61784-3-1: Functional safety fieldbuses [34] defines the requirements and measures to establish a functional safe communication. The standard defines the real communication path as a black channel, around which a safe protocol is set up, which implements the following requirements [34]:

- Support for a publisher/subscriber and client/server connection.
- Prevention from interference through non-safety related devices.
- Protection against unintended or non-authorized configuration changes.

- Measures against explicitly defined faults. These faults and the measures against are listed in Table 3.
- Possibility to calculate the reaction time for the application.

Communication errors	Safety measures						
	Sequence number	Time stamp	Time expectation	Connection authentication	Data integrity assurance	Redundancy with cross checking	Different data integrity assurances Systems
Corruption					X	X	
Unintended repetition	X	X					
Incorrect sequence	X	X					
Loss	X						
Unacceptable delay		X	X				
Insertion	X						
Masquerade							X
Addressing				X			

Table 3: Possible communication errors and safety measures against them [34].

The measures *sequence number*, *time stamp* and *time expectation* could all be realized through incrementing a number at message generation. For *time expectation* there must an additional timer which checks if the messages are in time.

The *connection authentication* has to be done by signing each message.

Data integrity assurance, *redundancy with cross checking* and *different data integrity assurance systems* use Cylic Redundancy Check (CRC) to verify the data integrity. At *redundancy with cross checking* the data must send duplicates for cross checking. *Different data integrity assurance systems* means that, the protocol must use different CRCs then the channel transporting it [34].

2.3.2 Safety measures in NFC

NFC was not explicitly designed for use in safety relevant applications, so not all of the above listed measures are an implicit part of the NFC standards. Since *functional safe* data transfers would most likely be a two way communication, *Peer to Peer Mode* would be the mode of choice.

In *Peer to Peer Mode* we have four layers (refer to Figure 2) where the measures could be placed. In NFC (lower three layers) there are two functions already integrated which could be used for creating a safe connection. The rest of the measures have to get implemented as a protocol in the application layer.

The first NFC function which could be used is the *sequence integrity* of the *NFC-SEC* [26] standard. It is situated among the MAC and the LLC layer. It provides a consistent sequence numbering where the sequence number is also secured to make changes in the numbering detectable. If the sequence of the messages is not correct the incorrect messages are rejected and not provided to the layers above. Upon this *time expectation* could be realized in the protocol.

The second NFC function, could be the *connection-oriented Transport* of the LLCP [21]. It is situated in the LLC layer. The *connection-oriented Transport* provides a sequenced message transport with guaranteed delivery through acknowledgment. This is done by numbering the data packets and sending back a Protocol Data Unit (PDU) for each message received. If sent messages are not acknowledged, an unexpected link disruption could be assumed. Once a connection is established, the LLCP manages state information and receive buffers independently of other connections. The number of unacknowledged messages in the receive buffers before an unexpected link disruption is sensed could be configured.

These two functions already allowing *sequence numbering*, and *time expectation* could easily be implemented on them. With these measures most of the errors defined in ISO/IEC 61784-3-1 are covered. There are three errors left to cover: *Corruption*, *Masquerade* and *Addressing*. Using a protocol which implements the *NFC-SEC-01* standards, would also cover the *Corruption*- (through encryption where a data integrity check is included) and the *Addressing*- (by establishing a secure connection with authentication) errors. So there is only the *Masquerade* error left by now, against whom the protection is the use of different redundancy checks in the channel and the protocol. Using a secured connection would provide the checks in the channel, so in the application protocol an additional data redundancy check needs to be implemented.

By building measures against the defined errors most of the requirements for a *functional safe* communication are covered. Securing the channel would prevent unintended or unauthorized reconfiguration of the devices over the air. Prevention from interference could be assured with the use of LLCP, where established connections are independent from others. The calculation of the reaction time could go along with the measures for *time expectation*.

The usage of *Peer to Peer Mode* and the *connection-oriented Transport* provides the publisher/subscriber and client/server connection. But the application protocol still needs to implement a check for the actual connection state. In case of a disrupted connection it must switch back to the fail safe state (not connected). The LLCP state information and the *time expectation* measure should be helpful in implementing these connection checks.

Finally, it should be possible to create a *functional safe* connection, with an application specific protocol implementing these extensions.

3 NFC Applications

Through the simple and intuitive usage, there is an high potential for different applications where the usability would benefit from NFC technology. In this chapter, we will focus only on some of them.

3.1 Payment solutions

In payment solutions, the biggest benefit would be that it is possible to integrate NFC technology in other devices which are always carried with the owner (e.g. car key or mobile phone). There are big commercial roll outs planned where NFC systems are used for payment.

In New York, Google is already testing their NFC payment solution for Android powered mobile phones, called *Google Wallet*. This happens in cooperation with the MasterCard *PayPass* system [15, 6].

In Germany the *Sparkasse* bank wants to start in the end of 2011 with the delivery of NFC ATM cards. Their plans are that by 2015 each of their customers will have such a card [40].

But not only the ATM cards need to be changed; all the terminals have to be upgraded to provide the NFC functionality. The payment companies are willing to take the upgrade costs because of forecasts that a lot of the customers will use their mobile phone with NFC payment solutions and thus the costs of the card production will decrease. The purchasers hope that the usage of these wireless systems will speed up the payment transactions and so they could save money with each costumer [16].

3.2 Healthcare

In healthcare, everything has to be documented exactly. Doing so is not always easy and the usual weary life in a hospital would not make it easier. NFC systems could help here saving time and increasing the safety.

In the usual medication scheme, a nurse has to find out which medication is required, fetch it, check if its the right, give it to the patient and document it. By the use of an NFC enabled system in the hospital, the personnel could get a medication list, for all of their patients on their mobile devices, and at the pharmacy an automated medication dispenser could provide the correct medications. In the next step the nurse gives the medication to the patients, checking each first by touching the patients ID, it would show which medication is required. Touching next the medication would perform the check and give an alarm if there is anything wrong. If its the right medicine in the right dosage, it will document that it has been given to the patient. Such a system would decrease the problems of medication errors, this would save money and time, and increase the patient's safety [11].

NFC could also be a benefit in the care of the elderly or Alzheimer's patients. Elderly people usually have problems interacting with new technologies. Since NFC is very simple and natural to use, the inhibition would be very low. For example, on the market there are a lot of Bluetooth enabled sensors for collection of vital values available. Combining them with NFC tags it would be easy for the people to connect them with a mobile device, which could utilize them. By placing this technology well in the daily routine of the people a lot of money for care giving could be saved while increasing the patient's safety at the same time [1].

3.3 Rescue organizations

There could be a great benefit in using NFC technologies in rescue organizations (e.g. paramedic services, fire fighters).

As there are studies for Germany, that 70% of health-realted emergencies happens at home and about 23% of the population lives alone, there would no one be able to give the paramedics information about medical history of the patient. For such cases, there are concepts to use NFC in combination with the *German electronic Health Card*, where the medical history could be stored. Dünnebeil et al. [3] suggest the placement of NFC tags containing the medical identity near the front door of the residence of people who live alone. In emergency situations a paramedic or doctor could read the tag with their mobile phone, connect over a secure connection to the health care database and retrieve the required information. For the privacy of the patients there have to be strict limitations regarding who has when access to the medical information [3].

The increasing safety design of vehicles makes it more and more difficult for rescue personal to evacuate people from crashed vehicles. Thus the *FIA Foundation* initiated a project called *Rescue Sheet* [4], where in the vehicles, A4 sized standardized information papers are placed. The placement of this paper is recommended behind the driver's sun visor, but it could be different for each car manufacturer or the paper could be removed by the owner of a vehicle. Usually the existence of such a card is shown by a sticker in the windshield of the vehicle. Combining this sticker with an NFC tag where the safety information is stored, there would be no need for the emergency personal to search for the paper. Additionally the emergency personal could automatically receive updates of this information over the air (with a mobile internet connection).

NFC tags could also help fire fighters. For large buildings there have to be alarm plans, with information the fire fighters need in emergency cases. These plans are usually bulky maps stored in security closets. In an emergency case, they have to be fetched from the closet and if there are more squads in action, there are often too few maps. By placing NFC tags in the building at strategic positions, each squad could fetch the information on their mobile device, with localized information about the section of the building where they are, and they do not need to search in the bulky maps for their actual location. In case of smart buildings far more functions could be realized. For example, switching of electricity or gas tubes by connecting with buildings controls.

Another possibility for the use of NFC could be for rescue or security organizations on an alarm to simply touch an NFC sender to retrieve the order information on the own mobile device and acknowledge the application of the order. At an NFC system this would be possible within milliseconds, where most other wireless systems need seconds to minutes to establish a connection. Such an extension could also be a benefit for the *Warn- und Alarm System Anzeige im Einsatzfahrzeug* project, because then there would be no need for a constant connection to the mission control equipment. This would result in a higher flexibility and a lower power consumption.

4 Conclusion

This thesis presented an overview of NFC technologies and possible underlying applications. In Chapter 1, NFC and RFID techniques are discussed. Also, the principal hardware design and the need for a *Secure Element* to store data are presented. Finally, the chapter gives an overview of the most relevant NFC standards.

Next, Chapter 2, examines the possible risks and attacks NFC systems are exposed to. Along necessary security measures are shown. In parallel, NFC is analyzed in relation to functional safety. In principle, NFC was not designed to provide safe communication. However, with help of underlying security measures and an application specific protocol also a functional safe communication according to ISO/IEC 61784-3-1 could be established.

Finally, Chapter 3 presents some possible future application domains which would benefit when using NFC systems. Besides payment solutions and applications within the area of ambient assisted living (e.g. tele-care and monitoring), emergency systems have been identified as future targets of interest for NFC technology.

References

[1] Jose Bravo, Diego López-de Ipiña, Carmen Fuentes, Ramón Hervás, Rocío Peña, Marcos Vergara, and Gregorio Casero. *Enabling NFC Technology for Supporting Chronic Diseases: A Proposal for Alzheimer Caregivers*, volume 5355 of *Lecture Notes in Computer Science*, book part (with own title) 8, pages 109–125. Springer Berlin / Heidelberg, 2008.

[2] Deutsches Bundesamt für Sicherheit in der Informationstechnik. Risiken und Chancen des Einsatzes von RFID-Systemen. Technical report, 2004.

[3] Sebastian Dunnebeil, Felix Kobler, Philip Koene, Jan Marco Leimeister, and Helmut Krcmar. Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure. pages 50–55, Hagenberg, Austria, February 2011.

[4] FIA Foundation. Rescue sheet. `http://www.rescue-sheet.info/`, (viewed June 2011).

[5] Klaus Finkenzeller. *RFID Handbuch*. Carl Hanser Verlag, München, 2008.

[6] Google. Google wallet. `http://www.google.com/wallet`, (viewed June 2011).

[7] Ernst Haselsteiner and Klemens Breitfuß. Security in Near Field Communication (NFC) - Strengths and Weaknesses. *RFIDSec*, 2006.

[8] Z. Kfir and A. Wool. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 47–58.

[9] Hermann Kopetz. *REAL-TIME SYSTEMS, Design Principles for Distributed Embedded Applications*. Kluwer Academic Publishers, 2002.

[10] Henning Siitonen Kortvedt. Securing Near Field Communication. Master's thesis, Norwegian University of Science and Technology, 2009.

[11] Antti Lahtela, Marko Hassinen, and Virpi Jylha. RFID and NFC in healthcare: Safety of hospitals medication care. pages 241–244, Tampere, Finland, January 2008.

[12] Josef Langer and Michael Roland. *Anwendungen und Technik von Near Field Communication (NFC)*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[13] Gerald Madlmayr, Josef Langer, Christian Kantner, and Josef Scharinger. NFC Devices: Security and Privacy. pages 642–647, March 2008.

[14] Gerald Madlmayr, Josef Langer, Christian Kantner, Josef Scharinger, and Ingrid Schaumuller-Bichl. Risk Analysis of Over-the-Air Transactions in an NFC Ecosystem. pages 87–92, Hagenberg, Austria, February 2009.

[15] MasterCard. Paypass. `http://www.mastercard.com/us/paypass/phonetrial/index.html`, (viewed May 2011).

[16] Renee Montes. Examining the technology, security, and applications of Near-Field communications, and evaluating the possible success of Near-Field communication applications in U.S. markets. Master's thesis, Bowie State University, 2009.

[17] NFC Forum. About the NFC forum. `http://www.nfc-forum.org/aboutus/`, (viewed April 2011).

[18] NFC Forum. NFC frequently asked questions. `http://www.nfc-forum.org/resources/faqs`, (viewed May 2011).

[19] NFC Forum. NFC Data Exchange Format (NDEF) - Technical Specification, 2006.

[20] NFC Forum. NFC Record Type Definition (RTD) - Technical Specification, 2006.

[21] NFC Forum. Logical Link Control Protocol - Technical Specification, 2009.

[22] NFC Forum. Signature Record Type Definition - Technical Specification, 2010.

[23] Norm ECMA-340. Near Field Communication Interface and Protocol (NFCIP-1), 2004.

[24] Norm ECMA-352. Near Field Communication Interface and Protocol -2 (NFCIP-2), 2010.

[25] Norm ECMA-373. Near Field Communication Wired Interface (NFC-WI), 2006.

[26] Norm ECMA-385. NFC-SEC: NFCIP-1 Security Services and Protocol, 2010.

[27] Norm ECMA-386. NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES Reference, 2010.

[28] Norm ECMA-390. Front-End Configuration Command for NFC-WI (NFC-FEC), 2009.

[29] Norm ECMA-391. Memory-Spot Interface and Protocol (MSIP-1), 2009.

[30] Norm ETSI TS 102 613. Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7), 2009.

[31] Norm ISO/IEC 14443. Identification cards - Contactless integrated circuit(s) cards - Proximity cards, 2001.

[32] Norm ISO/IEC 15693. Identification cards - Contactless integrated circuit cards - Vicinity cards, 2000.

[33] Norm ISO/IEC 61508. Functional safety of electric / electronic / prgrammable electronic safety-related systems., 1998.

[34] Norm ISO/IEC 61784-3-1. Functional safety fieldbuses - Additional specifications for CPF 1, 2008.

[35] Norm JIS X 6319-4. Specification of implementation for integrated circuit(s) cards - Part 4: High Speed proximity cards, 2005.

[36] Stefan Poledna. Course Slides: Dependable Systems, 2007.

[37] RFID Journal. History of RFID. `http://www.rfid-journal.de/rfid-geschichte.html`, (viewed April 2011).

[38] Rainer Steffen, Jörg Preiß inger, Tobias Schöllermann, Armin Müller, and Ingo Schnabel. Near Field Communication (NFC) in an Automotive Environment. pages 15–20, Monaco, Monaco, 2010.

[39] NFC Times. Austria: "rollout" uses NFC reader mode to sell tickets and snacks. `http://www.nfctimes.com/project/austria-rollout-uses-nfc-reader-mode-sell-tickets-and-snacks`, (viewed: April 2011).

[40] Welt Online. Sparkasse will 45 Millionen EC-Karten austauschen. `http://www.welt.de/finanzen/article13437240/Sparkasse-will-45-Millionen-EC-Karten-austauschen.html`, (viewed June 2011).