State of the Art for Near Field Communication: security and privacy within the field

Liam Church and Maria Moloney

Escher Group Ltd, Ireland

Liam.Church@eschergroup.com,

Maria.Moloney@echergroup.com

Third draft: May 10th, 2012,

Abstract

This paper provides an overview of near field communication (NFC) technology, from the perspective of security and privacy. Firstly, the paper starts with an explanation of what NCF is and how it works. This is followed by some examples in use of the technology today, in particular NFC mobile payments. The paper then goes on to look at the security and privacy challenges it currently faces and suggests some possible solutions to these challenges.

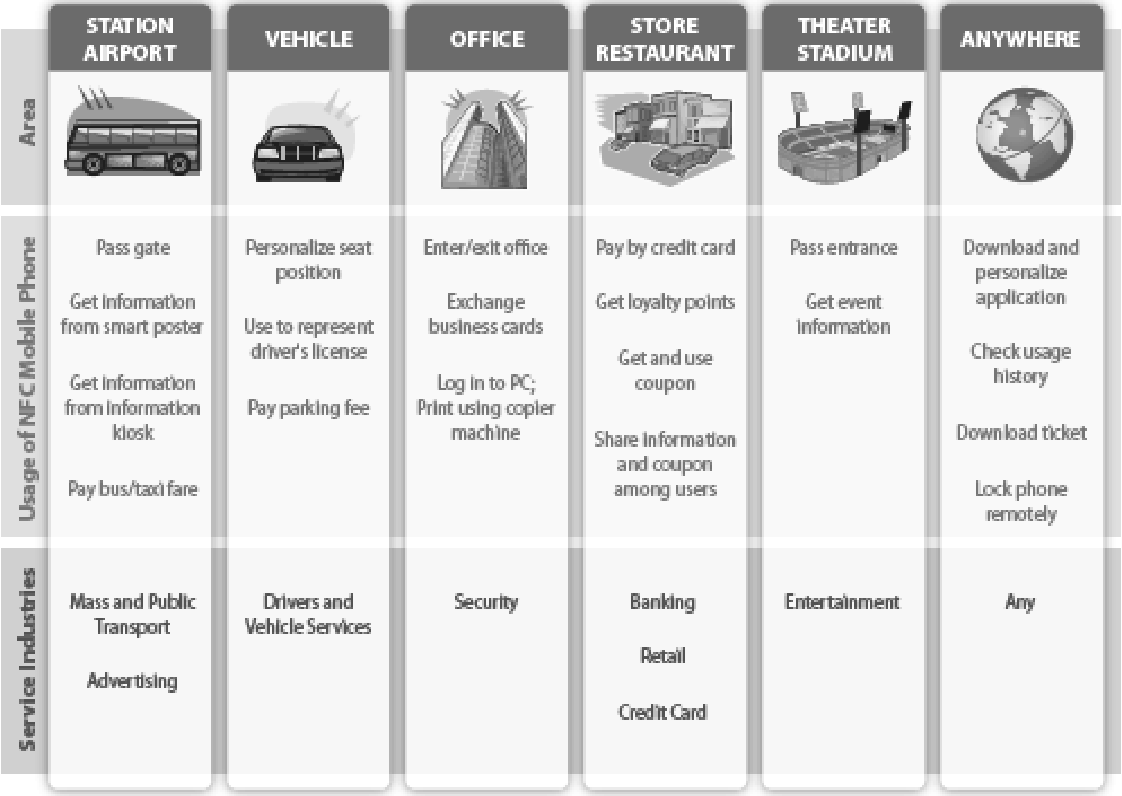
Introduction

NFC is a Radio Frequency (RF) technology for short-range communication that exchanges data between a reader, such as a phone or sensor, and a target, such as another reader or a microchip embedded in a device. The specification details of NFC can be found in ISO 18092 [1]. It is a follow-on technology from Radio Frequency Identification (RFID). The history of RFID can be traced back to the Second World War, where the British Air force tagged their planes with suitcase-sized devices to establish a friend-enemy detection system. The first commercial release of the technology came in the 1960's in the form of a 1 bit RFID for securing goods in shops, which is still widely used. In the 1990's RFID became more and more common for use in admission control systems and toll road systems [2].

In 2002, NFC was developed by NXP Semiconductors and Sony. In general, because NFC is an evolution of RFID and smartcard technology [3], it is compatible with most existing RFID and contactless smartcard systems, but its architecture is different in principle. While RFID and contactless smartcards have a reader/tag structure, an NFC device can be both reader and transmitter. An NFC Data Exchange Format (NDEF) was specified to ensure RFID tags and contactless smartcards are compatible with NFC applications. A key characteristic of NFC is that its wireless communication interface usually has a working distance limit of about 10cm.

In 2004, the NFC forum was founded by Philips, Nokia and Sony. The vision of the NFC Forum is to enable users to access content and services in an intuitive way, leading to a world of secure universal commerce and connectivity in which consumers can access and pay for physical and digital services anywhere, at any time, using any device. Its mission is to advance the use of NFC technology by developing standards-based specifications that ensure interoperability between devices and services, encouraging the development of products using NFC Forum specifications, educating the market globally about NFC technology, and ensuring that products claiming NFC capabilities comply with NFC Forum specifications [4].

By adding the functions of a mobile phone to those of a contactless NFC card, a new intelligent device or an “NFC Mobile Phone,” was defined. This newly defined device is an intelligent mobile network-enabled device that can connect with other NFC devices in close proximity. This unique combination of both mobile and NFC technology enables users to enjoy innovative services. Users can access myriad NFC services in their daily lives by having an all-in-one personal device that provides them with a highly personalized and interactive environment [5]. A specific use for NFC devices was pioneered in Japan and has since been introduced to the US market, which enables a suitably equipped mobile phone or tablet to act as either an NFC payment card or payment terminal or both [6]. An interesting example of this technology is the Google Wallet, which is discussed in more detail at a later stage in this paper. Figure 1 gives various examples of how an NFC mobile phone can be used:



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

Figure 1 Potential uses of NFC mobile phones, taken from [5]

NFC Operation Modes

The interface operates in several modes. The modes are decided by whether a device can create its own RF field or whether it retrieves power from the RF field generated by another device. If the device generates its own RF field it is called an *active* device, if it does not, it is called a *passive* device. Active devices usually have a power supply; passive devices, such as contactless smart cards, usually do not. The way data is transmitted from device A to device B indicates whether the transmitting device is in active or passive mode [7].

Three different communication modes for NFC devices are possible, 1) peer to peer mode, 2) reader/writer mode, and 3) card emulation mode [8]. Peer to peer mode enables communication between two NFC devices. The device which starts the communication is called the *initiator* the other is called the *target*. Device A sends a message to device B and device B sends a reply. Device B cannot send any data to device A without first receiving data from device A. This protocol, which handles the initiator and target configuration in peer to peer mode ensures a smooth establishment of communication, and is called the *Logical Link Control Protocol* (LLCP). The main difference of this mode is the difference in energy consumption of the initiator and the 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 [8].

The second mode is the reader/writer mode, which allows the NFC devices to communicate with NFC forum tags. These tags are typically passive components. 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 either information, such as Internet addresses or perform actions on the device, such as connecting to a wireless network [8].

The third and final mode is the optional card emulation mode. This allows the NFC device to communicate with well known RFID readers. The device, therefore, can emulate one or more RFID smartcard(s). With this mode it is possible to use existing contactless infrastructure such as for payment or admission control.

The emulation of the smartcard[1] can be done either in the application layer or in a so called *Secure Element*. A Secure Element is a device, similar to a real smartcard that uses an interface to the NFC device to transfer its data. In combination with the reader/writer mode, it is possible to implement a similar but simpler mode to the peer to peer mode, which with the correct hardware implementation makes it possible to use the NFC device when it is switched off or is short of energy [12]. Figure 1 shows the three operation modes for NFC.

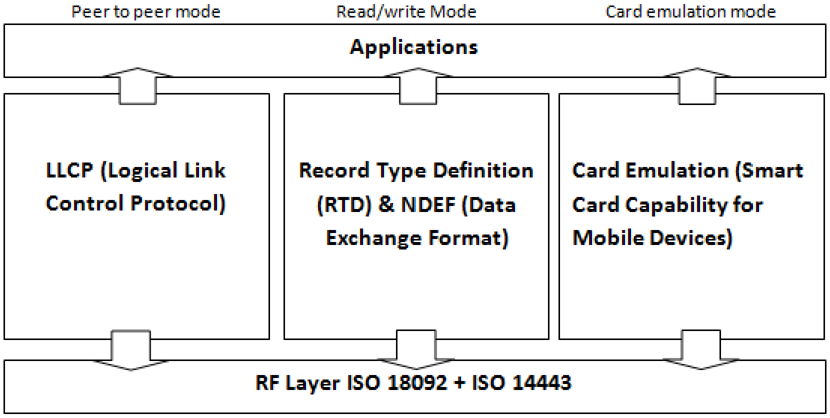

Peer to peer mode
Read/write Mode
Card emulation mode
Applications
LLCP (Logical Link Control Protocol)
Record Type Definition (RTD) & NDEF (Data Exchange Format)
Card Emulation (Smart Card Capability for Mobile Devices)
RF Layer ISO 18092 + ISO 14443

Figure 2 NFC operation modes, taken from [9]

[1] A smart card is any pocket-sized card with embedded integrated circuits. It is usually made of plastic and contains volatile memory and microprocessor components. Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations. Its benefits include the provision of identification, authentication, data storage and application processing [18].

NFC communication is not limited to a simple pair of devices. In fact, one initiator device can talk to multiple target devices. In such a scenario, all target devices are enabled at the same time, but before sending a message, the initiator device selects a receiving device. The message is then ignored by all non selected target devices. Only the selected target device is allowed to reply to the received data. It is not possible to send data to more than one device at the same time, i.e. broadcasting messages are not supported.

Hardware Architecture

Hardware architecture comprises a system's physical components and their interrelationships. The main components of the NFC hardware architecture are [8]:

1. The Host-Controller: Application Execution Environment (AEE), the environment where the application rests, such as the mobile phone;
2. The Secure Element: Trusted Execution Environment (TEE), the secure environment where sensitive information such as debit card data is stored, stored within the host controller;
3. The NFC-Controller: Contactless Front-end (CLF), the link between the host and NFC, with an interface to the Secure Element;
4. NFC-Antenna: simply put this is simply loops of wire, occupying as much surface area as the device allows.

Here we will discuss in detail the two central components from the list above that of the secure element and the NFC controller. Figure 3 shows the NFC elements within a mobile device.

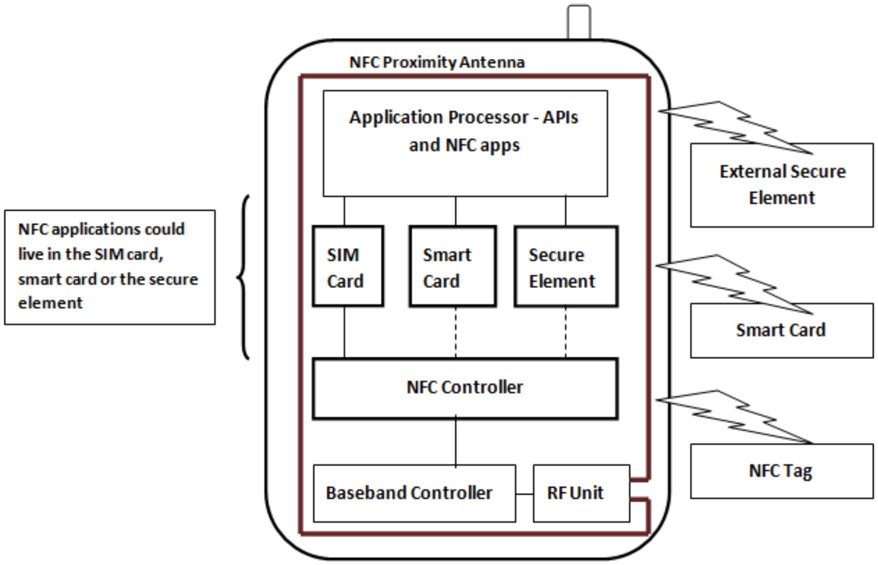


Figure 3 A description of the NFC related elements in mobile devices, adapted from [10]

NFC Controller

The NFC-Controller is the link between the air interface[2], the host-controller and the secure element. The Host-Controller is most likely a mobile device like a mobile phone, or a smart car key. There are various interfaces between the host controller and the NFC controller such as the serial peripheral

[2] In mobile or wireless communication, the air interface is the radio-based communication link between the mobile station and the active base station.

interface (SPI), and universal serial bus (USB). 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 a modulator/demodulator between the analogue 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.

Secure Element

On most mobile devices, such as mobile phones, there is no way to store secure data directly. For most NFC applications, i.e. payment and authentication solutions, secure storage systems are essential. For sensitive data, the storage needs to be resistant to manipulation and it must be able to execute cryptographic functions and to execute security-relevant software. Smartcards usually implement these requirements [8]. To implement such secure elements, there are different possibilities, each with its own advantages and disadvantages [12]:

1. **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.

2. **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. 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.

3. **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 was introduced by European Telecommunication Standards Institute (ETSI). While the SMC is usually owned by the user, which allows him/her to change his/her data independently, the SIM card of a mobile phone is owned by the network provider and, thus, the network provider must cooperate with the secure service provider.

An NFC system implementing a Secure Element is often abbreviated as *Secure NFC*, this is misleading because only the data stored on the secure element is secured, not the whole NFC communication [7]. Figure 4 shows possible solutions for the location of the Secure Element.

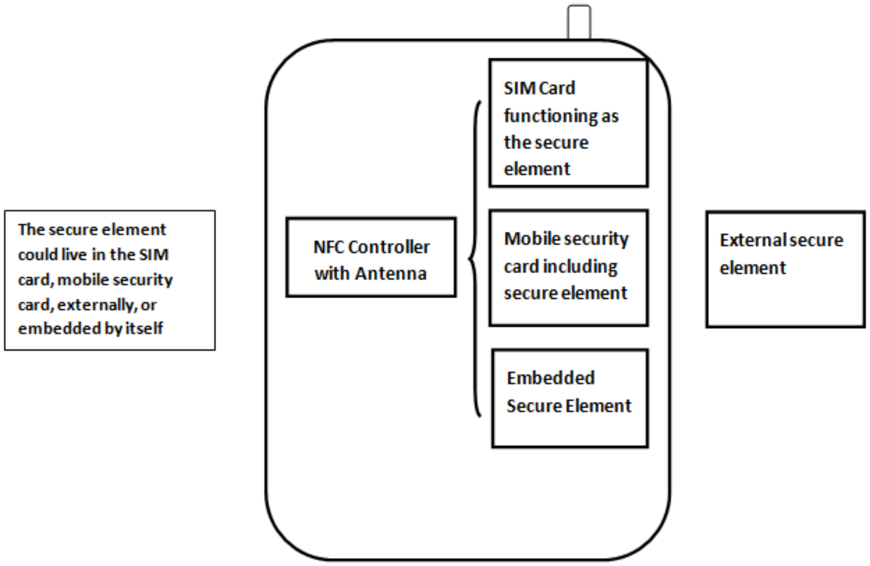

The secure element could live in the SIM card, mobile security card, externally, or embedded by itself
NFC Controller with Antenna
SIM Card functioning as the secure element
Mobile security card including secure element
Embedded Secure Element
External secure element

Figure 4 Possible secure element solutions

NFC Data Formats

To ensure compatibility between all the NFC and RFID devices, the data exchange formats used in both NFC and RFID were standardized.

The NFC Forum Tags

These tags are an important part of NFC technology. They implement the passive storage devices such as smart-posters, and other areas where small amounts of data can be stored and transferred to active NFC devices. Data can be retrieved from these passive tags by touching it with an NFC device. For example, the live area of the poster can be used as a touch point for the active NFC device. The stored data on the NFC tag may contain any form of data, but common applications are for storing URLs from where the NFC device may find further information. In view of this only small amounts of data are usually possible.

The NFC Data Exchange Format

The NFC Data Exchange Format (NDEF) [11] 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 [8].

NFC Record Type Definition

The NFC record type definition 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: this contains simple Text, and no specific application is assigned.

- URI Record Type: this contains a Uniform Resource Identifier (URI), which could be e-mail, web addresses, telephone numbers or other identification codes.
- Smart Poster Record Type: this 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: this provides a structure for any control activity.
- Signature Record Type: this contains a signature, which is provided to certify the correctness of the data.
- Connection Handover: this provides handover of an NFC connection to another communication technology with higher data throughput (e.g. Bluetooth).

NFC and Mobile Payments (Google Wallet)

As previously discussed, an interesting example of NFC mobile payments technology is the Google Wallet. This is a software app for the new NFC Android phones that supports NFC payments and enables other phone apps to interface to the payment system. Such phones contain a Secure Element (SE), a smartcard chip mounted in a tamper-resistant package with an NFC chip and antenna. A bank can load a payment card into the SE chip in the form of a signed Java card applet; the user can then select it using the phone's screen and use it to pay, whether by tapping it against a payment terminal in a physical store, or by an online transaction [5]. The wallet and its associated infrastructure deal with tedious and time consuming problems for the user, such as provisioning the phone with the right cards, revoking them should the phone be lost or stolen, and logging transactions to resolve disputes. Figure 5 shows an image of the payments process taken from the Google website used for Google Wallet transactions:

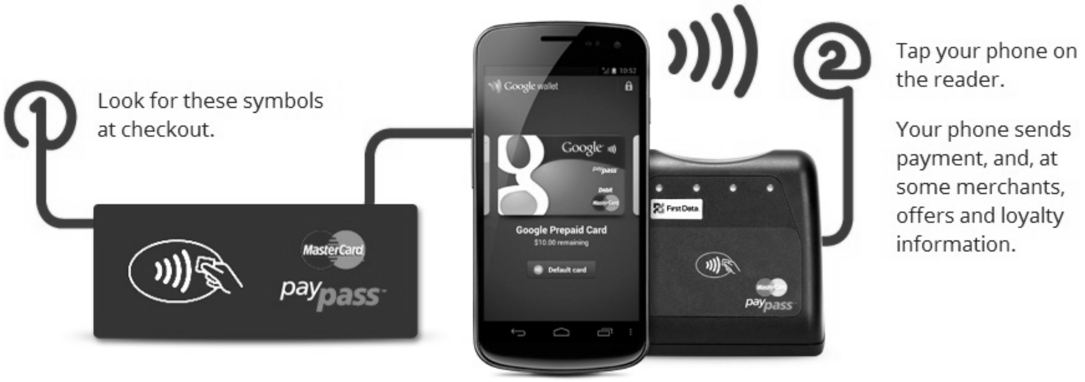

1
Look for these symbols at checkout.
MasterCard
paypass
Google wallet
Google
Google Prepaid Card
$10.00 remaining
Default card
FirstData
2
Tap your phone on the reader.
Your phone sends payment, and, at some merchants, offers and loyalty information.

Figure 5 Google Wallet 'Instore' use [12]

NFC Safety and Security

This section discusses the safety and security measures available for NFC. Initially, it looks at general security and privacy within the NFC field. This is followed by a discussion of security with an NFC mobile payment scheme and uses the Google Wallet as an example.

General NFC Safety and Security

For a communication system, *safety can be defined as the provision of a guaranteed transfer of the data and in the event of a disturbance that there is a safe state where no catastrophic consequences* *can occur*. Security for a communication system is *the prevention of unauthorized access and unauthorized manipulation of data*. Security is categorized into three principles (CIA for short):

- ***C**onfidentiality* is the principle whereby only those with sufficient privileges and a demonstrated need may access certain information. When unauthorised individuals or systems can view information, confidentiality is breached.
- ***I**ntegrity* is the principle of ensuring information is maintained in a complete and uncorrupted state. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being entered, stored or transmitted.
- ***A**vailability* is the principle that allows entities to access information in a usable format without interference or obstruction. An entity may be a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorised users.

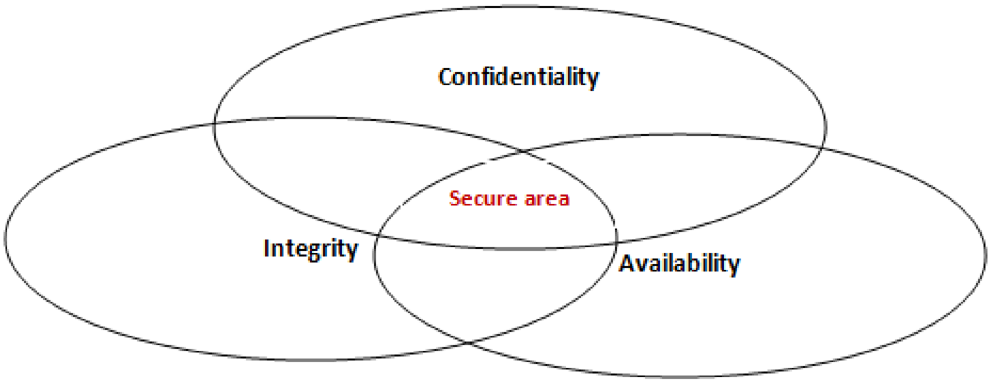


Figure 6 Creating security in a system

Figure 5 outlines how security is created using the principles of confidentiality, integrity and availability. There are many ways to break the security of a system. The majority of attacks fall under four threat headings:

- Spying: unauthorised access to information;
- Deception: deceive through wrong information;
- Denial of service (DOS): compromise the availability of the NFC system;
- Protection of privacy: ensuring all sensitive information transferred and stored within the NFC system is protected.

All types of wireless communication are vulnerable to these threats. It is easy to listen into a wireless channel and the intended signal can easily be disturbed by other signals. The problem with radio transmission is that malicious users can access the communication channel undetected. Without any protection, it is possible to pick up messages, alter information in live communication and store messages with the intention to replay them with the same or altered content at a later time [13]. To overcome the threats, the system needs to implement authentication, integrity checks, confidentiality and replay protection. The level of security needed is defined by the application itself. Whenever money is involved, an application will attract potential malicious users. Private content sharing on the other hand may not require the same level of security. MasterCard and VISA are big actors in this arena and various equipment vendors implement different security solutions in this field. Some of the work of these companies is public, but specific technical specifications are kept within the companies and their trusted partners. The passive communication mode seems like a good solution for transfer of sensitive data, as this mode seems harder to eavesdrop upon compared to the active communication mode [13].

Three key elements within NFC security are discussed here, namely, attacks: over the air interface of NFC, via the NFC tag, and/or via the NFC device [8].

Attacks over the air interface

As a result of the air interface being contactless, attacks can be performed without physical access. That means that there are many possibilities for the attacker to conceal his attacks. Known attacks to the air interface are:

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 easy, however. The attacker has to increase the energy of the high frequency field, use an optimised antenna and handle the increasing noise in the communication.

Jamming: here a sender blocks the NFC system by sending a disturbance signal on its frequency. This sender must be either placed near the NFC system or use appropriate antennas and power rates. This attack compromises the availability of the NFC system.

Denial of service: as there could be more than one NFC device/tag in range, an anti-collision algorithm has to be performed to select the individual device, with which to communicate. 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 this attack two parties are tricked into a three party communication, without their knowledge. Instead of directly communicating 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 confidentiality and integrity of an NFC system.

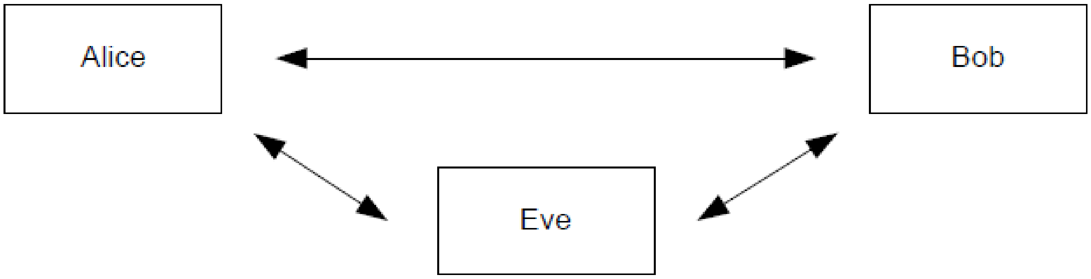
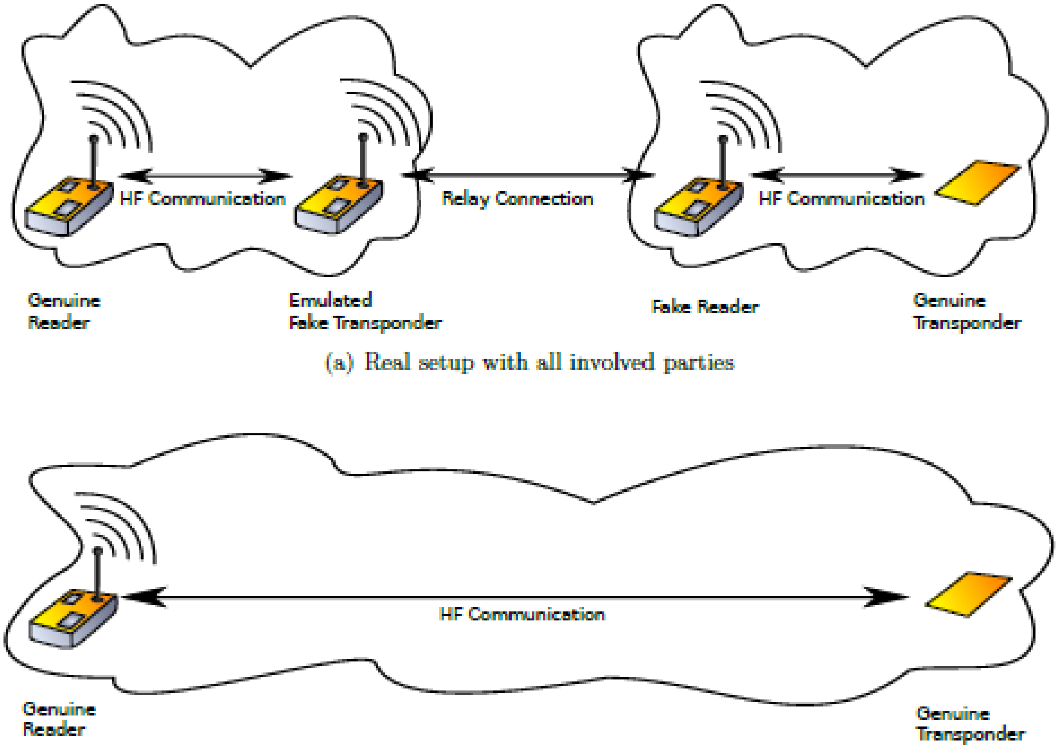


Figure 7 Man in the middle setup

Eavesdropping: since NFC systems communicate 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 is able to amplify weak signals received over a distance up to 30 - 40cm [13,14]. In [13] it is demonstrated that producing such eavesdropping equipment can be done at relatively low coast. This attack compromises the confidentiality of an NFC system [8].

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.



(a) Real setup with all involved parties

(b) Virtual setup seen by the reader and the transponder

Figure 8 relay attack on NFC devices, taken from [15]

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 cannot 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.

Attacks on the NFC Tag

The attacks that can be performed on the NFC tag are as follows:

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 mechanically, for example by cutting the connection to its antenna. Another way to destroy the tag is an overpowered electrical field on the tag's 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 anti-collision (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.

Attacks on the NFC Device

An NFC device is often a complex and powerful device such as a mobile phone. Such devices are valuable to attackers and, thus, there is a high risk of attack. An example of an attack on the device is hacking into an application which uses the NFC interface. Attacks on NFC devices are performed either with the knowledge of the user i.e. the user is the attacker, or without the user's knowledge i.e. the hacker accesses the device through an internet connection.

Security Measures Against Attacks in NFC

Since NFC devices have become popular for payment and ticketing solutions, security has become a high priority. Most of the attacks listed above can be prevented by using authentication and encryption methods [8]. MIFARE technologies[3], which are manufactured by NXP Semiconductors,

[3] MIFARE is the NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards and proximity cards.

have introduced ISO/IEC 14443 compliant solutions with support for 3DES, AES, RSA encryption protocols [13]. Their first attempt to implement security was Crypto-1, an NXP proprietary stream cipher with 48 bit key made for MIFARE Classic. Because of low cost and good reliability, this version has been heavily deployed in electronic wallet, public transportation and ticketing applications. Several publications during 2007 and 2008 describe how to break this cipher, one of them with a secret key recovery time down to 40 ms on a laptop [13]. The latest solutions from both MIFARE and FeliCa are approved at minimum Common Criteria (CC) assurance level EAL4, and the hardware of MIFARE SmartMX has passed EAL5+ evaluation. CC is standardized in ISO/IEC 15408, which is a certification standard for IT security. EAL4 is the highest EAL-level which is expected to be economically feasible while implementing the security in an existing product line. EAL5 is applicable for systems requiring high level of independently assured security in a planned development. The design process is rigorous, but should keep the cost related to security specialists at a reasonable level. In their RC-S860 chip, FeliCa has implemented mutual authentication using 3DES and data encryption by a transaction key generated in the authentication procedure. FeliCa claims in the product description that the features make forgery and card fraud nearly impossible [13].

A more challenging attack to perform is the *Man in the Middle attack*. For this to occur, three devices have to be in a single range in order to 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 results 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 [7].

Experiments show that a passive eavesdropping attack can occur up to a distance of 30 - 40cm, which limits the possibilities for an attacker to hide either himself or his equipment [16]. However, in certain situations like a crowded underground train at rush hour, the attacking equipment can be placed in a bag to avoid suspicion and the owners of the NFC devices would, thus, be unaware that their device is being surreptitiously read from a passerby. To avoid this type of attack, the host device would need an application, which asks for permission, i.e. 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 off the NFC functionality would then prevent an attacker from skimming the NFC data while walking by [17].

Safety and Security in NFC Mobile Payment Systems

It has been predicted that mobile wallets will, in future, be the mediator between the payment mechanism of a mobile device and the apps (being) downloaded on that mobile device seeking payment. The reason for this is to avoid untrustworthy apps having access to payment information of users. In the absence of a wallet app, rogue or subversive apps could phish the user by requesting him/her to enter their pin in exchange for payment of a game costing, let us say, €2.50, while actually initiating payment for a much larger transaction in the background. By providing a trustworthy logging mechanism and user interface, the wallet can create a payment platform that supports secure innovation [6].

Governance over an NFC payments system is a challenge as the system usually involves hundreds and thousands of vendors, banks and merchants, each one wishing to cut costs and customise their own systems, both of which can seriously undermine security. When a serious security breach actually does occur nobody wants to take responsibility or pay the costs. Additionally, as users sign up to the system, it invariably involves more and more stakeholders and becomes increasingly more complex, making governance even harder.

Another challenge for NFC payment systems is that crimes that were difficult to achieve on traditional chip and pin devices, suddenly become feasible. Take for example the following scenario outlined in [6], which explains that at present, it is possible to connect a false chip and pin terminal remotely to a false chip and pin card, so that when the victim buys coffee from a vending machine upon which the false terminal has been fixed, a crook can steal money from an ATM hundreds of miles away using the false card. With conventional chip and pin systems, this requires specialist equipment, so it has not been industrialised at any scale. But once mobile phones contain NFC technology, a criminal can program one phone to act as a false terminal, and another to act as a false card. An attack that once required serious engineering is now just a software application. Unfortunately, crimes can be pirated just as easily as music. Once a card cloning scam gets into widespread use, the question arises as to who is capable of stopping it, and how [6].

The strategic risk for companies investing in NFC technology for mobile payments is that of an attack that makes fraud so easy that the mobile platform or channel that they are developing becomes unviable. A nightmare scenario for Google wallet engineers, for example, is that malware on a mobile phone might take over the device so comprehensively that a remote software attack becomes possible. If malware can infect a phone to such an extent that large amount of money can be defrauded, while it sits quietly in the user’s pocket, then its viability as a mobile payments platform is threatened. Hardware security devices such as the Secure Element are designed to reduce such risks, but it is always possible that design error or governance failure could lead to such a catastrophe [6].

Conclusions

In this paper a review of near field technology was conducted. Specific aspects of the technology were chosen for the review, namely, introducing the technology, the various operation modes of the technology, its hardware architecture, data formats and the security built around the technology to prevent breaches. It then discusses current potential security attacks that can be launched on the technology and the measures taken to prevent these attacks.

This paper is a work in progress and will be updated as the technology changes.

Bibliography

1. INFORMATION technology - Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1). **International Organisation for Standardisation**, 2004. ISSN ISO/IEC 18092. Disponivel em: <http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578>. Acesso em: 29 March 2012.

2. ROBERTI, M. The History of RFID Technology. **RFID Journal**. Disponivel em: <http://www.rfidjournal.com/article/view/1338/1>. Acesso em: 29 March 2012.

3. VAZQUEZ-BRISENO, M. et al. Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World. In: DELIYANNIS, I. **Interactive Multimedia**. Janeza Trdine: InTech, 2012.

4. PREUSS, P. NFC Forum: NFC Use Cases. **NFC Forum**, 2009. Disponivel em: <http://www.nfc-forum.org/events/oulu_spotlight/Forum_and_Use_Cases.pdf>. Acesso em: 10 May 2012.

5. NFC FORUM. Essentials for Successful NFC Mobile Ecosystems. **NFC Forum**, 2008. Disponivel em: <http://www.nfc-forum.org/resources/white_papers/NFC_Forum_Mobile_NFC_Ecosystem_White_Paper.pdf>. Acesso em: 26th April 2012.

6. ANDERSON, R. **Risk and Privacy Implications of Consumer Payment Innovation**. Consumer Payment Innovation in the Connected Age Conference. Kansas City, Kansas, United States: [s.n.]. 2012.

7. BREITFUSS, E. H. A. K. **Security in Near Field Communications**. Workshop on RFID Security. Graz, AUSTRIA: [s.n.]. 2006. http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.

8. KERSCHBERGER, M. Near Field Communication A survey of safety and security measures. **Institute of Computer Aided Automation**, 2011. Disponivel em: <https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf>. Acesso em: 29 March 2012.

9. LAZARRI, T. D. Near Field Communication (Slideshare Presentation). **Slideshare**, 2008. Disponivel em: <http://www.slideshare.net/tdelazzari/near-field-communication-presentation>. Acesso em: 26th April 2012.

10. JAN KREMER CONSULTING SERVICES. NFC Near field Communication WHite Paper. **Jan Kremer Consulting Services**, 2010. Disponivel em: <http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf>. Acesso em: 26th April 2012.

11. NFC Data Exchange Format (NDEF) - Technical Specification. **NFC Forum Technical Specifications**, 2006. Disponivel em: <http://www.nfc-forum.org/specs/spec_list/>. Acesso em: 29 March 2012.

12. GOOGLE.COM. How it works: Use-it-instore. **Google**, 2012. Disponivel em: <http://www.google.com/wallet/how-it-works.html#in-store>. Acesso em: 10 May 2012.

13. KORTVEDT, H. S. Securing Near Field Communication. **Master's thesis**, Norwegian University of

. Science and Technology, 2009.

14 KFIR, Z.; WOOL, A. **Picking Virtual Pockets using Relay Attacks on Contactless**. First International
. Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). Washington, DC, USA : [s.n.]. 2005. p. 47-58.

15 WEISS, M. Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile
. Equipment. **FAKULT AT F UR INFORMATIK DER TECHNISCHEN UNIVERSIT AT M UNCHEN**, 2010. Disponivel em: <http://www.sec.in.tum.de/assets/studentwork/finished/Weiss2010.pdf>. Acesso em: 26 April 2012.

16 KFIR, Z.; WOOL, A. **Picking Virtual Pockets using Relay Attacks on Contactless Smartcard**. First
. International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). [S.l.]: IEEE Computer Society. 2005. p. 47–58.

17 MADLMAYR, G. et al. **NFC Devices:** Security and Privacy. Third International Conference on
. Availability, Reliability and Security, 2008, (ARES 08).. Barcelona , Spain: [s.n.]. 2008. p. 642 - 647.

18 WIKIPEDIA.COM. Smart card. **Wikipedia.com**, 2012. Disponivel em:
. <http://en.wikipedia.org/wiki/SmartCard>. Acesso em: 10 May 2012.