NFC - Possibilities and Risks

Uwe Trottmann
Betreuer: Matthias Wachs
Seminar Future Internet WS2012
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: uwe.trottmann@tum.de

ABSTRACT
Near Field Communication (NFC) is an emerging close range, low bandwidth, induction based communication standard. It is already and will be more broadly integrated tightly with modern smartphones, devices and operating systems. Payment services, setup of high-bandwidth connections, information sharing and identity verification become possible by just touching two NFC devices together. This paper tries to give an overview over how NFC technology works, what some of its current and potential applications are and which risks and exploits come along with its simplicity.

Keywords
NFC, NDEF, SNEP, payments, ISIS, wallet, ticketing, RFID

1. INTRODUCTION
Near Field Communication (NFC) is a consumer-oriented wireless technology using magnetic fields and induction to communicate data over a distance of centimeters at low bandwidth. It is backed by the NFC Forum, consisting of more than 160 members including industry heavy-weights like Samsung, Sony and NXP. They push and certify integration of NFC technology in modern consumer electronics like smartphones and operating systems like Android and Windows 8. Current applications include payment and ticketing by just waving your phone, the setup of Bluetooth or Wi-Fi connections between devices by touching them together and embedding of information or device configurations in passive entities, so called NFC tags.

The following will give an overview over the history and technology behind NFC (2), showcase the breadth of current and future applications (3) as well as discuss risks, attack vectors and existing exploits (4).

2. HISTORY AND TECHNOLOGY
In 2004 ISO/IEC standard 18092 "Near Field Communication - Interface and Protocol (NFCIP-1)" [2] specified a technology for exchange of information and telecommunications. It is based on and expands on existing RFID standards for contactless cards by ISO/IEC (ISO/IEC 14443 [3]) and Sony (Felicity Card/FeliCa [4], based on JIS X 6319-4 [5]). Implementations and applications in various forms and devices based on this standard are backed and certified by the NFC Forum, an industry consortium which came to life the same year. The NFC Forum now includes more than 160 members like electronics manufacturers Samsung and Sony, chip providers NXP and Broadcom and even financial services companies Visa and Mastercard. Mid-2006 initial specifications for a data exchange format (NDEF, see 2.3) and record types - the first few instances being text, URIs and smart posters - were announced [6].

Both prior standards ISO/IEC 14443 and FeliCa differentiate between dedicated reading and writing devices and integrated circuit cards. The cards are mainly passive objects and do not have a power source of their own. The used fields operate in the globally available, unlicensed ISM[1] band of 13.56 MHz and require small distances in the range of centimeters between the reader and the contactless card.

According to the new ISO/IEC 18092 standard [2], NFC devices operate in the same ISM band of 13.56 MHz and are required to be compatible with ISO/IEC 14443 and FeliCa. Communication involves an active initiator device generating a magnetic field in close proximity to a passive target device, typically at about four centimeters or less. All devices by default are in target mode and wait for an incoming command by an initiator. If a field is noticed by a target device, it will manipulate it to transmit information back to the initiator. This mode is similar to the reader and card scheme in ISO/IEC 14443 and FeliCa and is called passive mode. One should note that using special resonant circuitry a passive target device may be built which does not require its own power source similar to existing contactless cards in various form factors. These are called tags and are discussed in more detail later on (see section 3.1).

In contrast to the previous standards, however, any NFC device may opt to become the active component, the initiator. This active mode enables both devices to take turns in generating their own fields while the other listens for data, effectively establishing a half-duplex connection.

Both the passive and active mode provide data rates of 106, 212 or 424 kbit/s using the Manchester coding scheme with amplitude shift keying for modulation for all mode and data rate combinations. Active mode at 106 kbit/s is an exception, it uses a form of Miller coding (both codings are described in [2]).

NFC connections as specified by ISO/IEC 18092 themselves

[1]Various frequency bands widely reserved for Industrial, Science and Medical use

doi: 10.2312/NET-2013-02-1_05

	NFC	ZigBee	Bluetooth (2.1)	WLAN (802.11ac)
Range	< 10cm	< 100m	< 100m	< 250m
Data rate	<424 kbit/s	<250 kbit/s	<2.1 Mbit/s	<866.7 Mbit/s
Network size	2	2**64	8	2007
Frequency band	13.56 MHz	868/915 MHz, 2.4 GHz	2.4 GHz	2.4/5 GHz

Table 1: NFC compared to other wireless technologies. [7]

do not require any form of encryption. It is of the discretion of the implementing applications to provide any layer of security, which might not be as reliable on a application-to-application basis compared to built-in security. In addition the application layer may be more prone to vulnerabilities and outside influences especially considering an active NFC device always listening and reacting to incoming commands as mentioned before. Serious privacy concerns may arise if personal information can simply be read from a NFC-equipped mobile phone due to sloppy applications handing out data without approval. Or even programs being executed resulting in the infection of the users device. Therefore the last chapter (4) will shed more light on possible and existing attacks.

2.1 Comparison

As Near Field Communication is based on RFID technology it shares similar properties. Taking a closer look at RFID, it is designed to read data from tags or cards via radio-frequency (RF) electromagnetic fields for the purposes of identification or tracking of objects or people. Tags and cards are always passive, only reading devices active. Communication, however, may occur on a wider variety of frequencies, including the 13.56 MHz ISM band NFC uses. More importantly RFID is capable of operating without line-of-sight making it feasible for different automation tasks, like the scanning of stacks of crates passing a RFID reader equipped warehouse gate. In comparison NFC is restricted to very short distances but allows devices to function either as, in RFID terms, a reader or tag/card. [8]

In the following multiple other existing wireless technologies, namely ZigBee, Bluetooth and WLAN are described and compared to NFC as listed in table 1.

ZigBee is a wireless technology designed to support significantly higher ranges with improved maximum data rates requiring only minimal hardware. Like RFID it is mainly used in commercial applications, but seldom in consumer products. ZigBee allows to interconnect devices into a mesh like network while consuming as little energy as possible. It extends the IEEE 802.15.4 standard, operating mainly on 2.4 GHz, and may support thousands of devices in one network, for example to report sensor measurements or automate devices through remote commands. [9]

Bluetooth, specified by the Bluetooth SIG[2], is similar to ZigBee. It, however, restricts the device architecture to one master and up to seven slave devices. More devices may be linked into this Personal Area Network, albeit in a passive, parked mode. The resulting piconet was supposed to get rid of cables required to connect computer accessories like printers or digital cameras. Nowadays, Bluetooth is included in pretty much every mobile handset and is commonly used for file transfers or spontaneous device networks with data rates significantly higher than NFC at a larger range in the ball bark of meters (see table1). However, setup is far more complicated and time consuming requiring pairing and the exchange of secrets. [10]

WLAN was designed to extend the range of LANs to mobile devices like laptops. It is specified as the IEEE 802.11 standard which has been extended numerous times to include more features, MIMO support and higher bandwidth. As the n extension is becoming the default in current mobile phones and access points, 802.11ac carries forward with even more supported antennas and even higher bandwidth (see table1) exceeding Bluetooth and NFC by orders of magnitude. With 802.11ac WLAN will transition completely to the 5 GHz band away from 2.4 GHz which has become somewhat crowded: Bluetooth, ZigBee and many other wireless technologies use it. Of all presented technologies WLAN has the highest possible range for consumer equipment in the realm of hundreds of meters. It also supports connection encryption out of the box. [10]

2.2 Operating modes

According to the NFC Forum there exist three basic modes of operation for NFC Forum devices: reader/writer mode, peer-to-peer mode and card emulation mode. In reader/writer mode a device is able to read or write NFC tags as specified by the NFC Forum. These include smart posters or tags with embedded text, URLs or signatures. This mode is conform with ISO/IEC 14443 and the FeliCa standard.

Peer-to-peer mode allows devices to exchange small chunks of data with each other, examples would be setup parameters for Bluetooth or Wi-Fi connections or virtual business cards. This behavior is newly specified by ISO/IEC standard 18092.

At last there is a card emulation mode which gives NFC devices the capability to emulate traditional, contactless, read-only RFID smart cards. This allows NFC devices to integrate with existing legacy RFID infrastructure, like ticketing systems in public transport, without any modifications of the legacy system.

2.3 NFC Data Exchange Format

To store and exchange information the NFC Forum has specified the NFC Data Exchange Format (NDEF, [11]). It is a binary message format allowing data exchange between NFC Forum devices or between a NFC Forum device and one of four NFC Forum tag types (type 1 through 4, [12]).

[2] `http://www.bluetooth.com`

doi: 10.2312/NET-2013-02-1_05

There exist NFC Forum Well-known Types, specified according to the NFC Forum Record Type Definition (RTD) specification [15]. These are simple URNs using the namespace identifier "nfc", prefixing "wkt" for well-known types or "ext" for self-defined types. A sample URN would be "urn:nfc:wkt:Sp" for the NFC Forum Smart Poster record type or "urn:nfc:ext:example.com:foo" for a self-defined type. The Smart Poster RTD [18] is based on the Text RTD [16] and URI RTD [17] in combination with actions that may trigger the launch of a web browser or sending of a SMS message. The Signature RTD [19] defines additional signature fields and suitable algorithms to allow verification of the authenticity and integrity of records inside a NDEF message, but employs no restrictions on the use of a certification architecture nor requires one at all. There also exists a Generic Control RTD [20], it is, however, deprecated and will be removed on or after August 9, 2012.

A NDEF message itself can include an unlimited amount of application-defined payloads in so called records. Each message is started with a record flagged as *MB* (Message Begin) and ends with a record flagged as *ME* (Message End). NDEF messages can be nested by including them inside a record of an existing NDEF message.

NDEF Message				
R_1, MB=1	...	R_i	...	R_n, ME=1

Figure 1: Example of an NDEF message with multiple records [11].

In addition to several flags providing support for chunking payloads over records (CF) or signaling very short records (SR), each record specifies the length of its payload as well as its type and an optional payload identifier which may be used to establish links between payloads in other records (see figure 2). Payload types may be formatted as NFC Forum specified Record Type Definitions as mentioned above, any MIME type as specified by RFC 2046 [13], URIs [14] and various others. When encoded in a NDEF message the namespace identifier and prefix of a Well-known type are dropped and represented by appropriate Type Name Format (TNF) field values in the record header. However, all types are understood as mere guidelines for overlying applications on how to parse payloads.

3. APPLICATIONS

According to the NFC Forum [1] NFC technology is or may be used in the areas of

- Access control,
- Consumer electronics,
- Healthcare,
- Information collection and exchange,
- Loyalty and coupons,
- Payments and
- Transport.

7	6	5	4	3	2	1	0
MB	ME	CF	SR	IL	TNF		
Type length							
Payload length 3							
Payload length 2							
Payload length 1							
Payload length 0							
ID length							
Type							
ID							
Payload							

Figure 2: NDEF Record layout. IL = ID length is present flag [11].

In general NFC is predestined to become a widely deployed technology as it requires only simple active hardware and can use cheap, easily mountable integrated circuit tags. Consumers will have NFC functionality embedded in their regular phones and setup and usage is as simple as bringing devices into close proximity of another. Applications on top may add value ranging from automation to payments.

As applications are endless we will focus on a few interesting areas: passive NFC tags (3.1), sharing between devices (3.2), financial services (3.3) - which will probably have the biggest (monetary) impact - as well as identification documents like tickets (3.4).

3.1 Tags

Storing pieces of information inside small, flexible circuitry embedded into stickers, little plastic shells or paper is one of the main visible use cases for NFC. These tags may be read by a NFC device, supporting the NFC Forum specified reader/writer mode, close to them and may contain simple text or URLs up to complex application specific data like configuration instructions. The NFC Forum specifies four different tag types, simply named NFC Forum Type 1 Tag through 4. Type 1 and 2 are based on the ISO/IEC 14443A contactless card standard [3] and are read- and re-writable. Type 1 tags store at minimum 96 bytes, Type 2 tags at minimum 48 bytes. Both at most 2 kbyte. Type 3 is basically the JIS X 6319-4 [5] contactless smart card standard used by FeliCa from Sony [4] which includes an additional read-only mode with available memory varying up to a maximum of 1 MByte while allowing multiple services on one card. Similarly Type 4 tags support multiple services, read-only mode and vary in memory size up to 32 KByte per service. However, they are based on the ISO/IEC 14443A/B standard.

Sony was the first company to offer its NFC tags, called Xperia SmartTags [21], as a consumer oriented accessory for their Android smartphones. Internet and some brick and mortar stores start to catch on to the trend and are offering tags with more memory in form factors ranging from stickers, classic card sizes and wrist bands to Sony

doi: 10.2312/NET-2013-02-1_05

SmartTags-like plastic badges[3]. Most of them make use of NXPs MIFARE chip series which are compatible with ISO/IEC 14443 [3], read- and writable by any NFC Forum device in reader/writer mode. Common use cases include mode or profile switching of a phone on touching a tag. For example putting your phone near a tag in your car may start the navigation app and enable Bluetooth pairing to the infotainment system. To write and react to the tags Sony provides a companion app, however there exist multiple free alternatives which support a wider range of tag types and commands[4][5].

3.2 Sharing

As the rise of Web 2.0 technology has shown social integration like sharing content between people is highly popular. Using NFC Forum devices in peer-to-peer mode enables a dead simple way of sharing content. Contact information, website URLs or small files are quickly passed on by a simple, intuitive action: touching devices together. For this particular purpose the NFC Forum defined a Simple NDEF Exchange Protocol (SNEP) [22] which uses the connection-oriented mode of the transport protocol Logical Link Control Protocol (LLCP) providing sequenced and guaranteed data delivery. It is also defined by the NFC Forum [23]. SNEP is a versioned request-response protocol between a client and a server. A client may send SNEP request messages to store (Put) or retrieve (Get) NDEF messages from a server over a LLCP data link connection.

Notably Android Beam [24], introduced by Google with Android 4.0 (Ice Cream Sandwich) in late 2011, is a peer-to-peer data exchange protocol for Android devices based on SNEP. It also supports Androids own, older NDEF Push protocol as a fallback. The sending user has to run the Android application he wants to share data from in the foreground, the receiving device needs to be unlocked and on its home screen. On touching the two devices together the sending device will show a "Touch to Beam" confirmation button allowing to transmit the desired information. Android Beam can be used by any application implementing its API. For example the built-in *People* app shares contacts, the *Browser* app shares URLs. Upon completion, the appropriate application will automatically be launched on the receiving device to handle the shared data.

To share bigger files like high-resolution photos or videos NFCs highest data rate of 424 kbit/s is barely sufficient. To work around this limitation, with Android 4.1, Google introduced establishing a separate, faster transport connection like Bluetooth via Android Beam taking over data transfers from NFC after successful connection[6]. The NFC Forum happens to have a specification of exactly this process titled Connection Handover [25], initially released in 2008, revised in 2010. In addition to a "Negotiated Handover" like Android Beam uses, it defines a "Static Handover" where parameters are stored and read off a passive tag.

Looking further back in time, Nokia was the first company to integrate NFC into a consumer purchasable phone in January 2007: the Nokia 6131. They showcased interaction with smart posters and sending images over to a digital picture frame[7]. In June 2011 they introduced their N9 smartphone [26] with the MeeGo operating system featuring tight integration with NFC in concert with a set of NFC-enabled wireless speakers (Nokia Play 360 [27]). By touching the phone to the speakers a Bluetooth connection would automatically be established and music would play on the speakers.

Meanwhile, in addition to Android and MeeGo, NFC peer-to-peer capability has been integrated into Microsoft's Windows Phone operating system as well as directly into Microsoft's new touch-focused tablet and desktop operating system Windows 8 [28]. In any case the focus has been on friction-less sharing between devices, on occasion handing over to a high-throughput connection when necessary to support larger data transfers.

3.3 Financial services

One of the biggest areas of interest, at least from an industries perspective, is financial services: paying with your phone acting as a digital wallet. As of 2012 there are three approaches on paying with NFC: you carry a NFC enabled banking or credit card, your phone includes a Secure SIM which handles encryption and authentication over the NFC interface, or you install an application which handles all payment processing.

There are currently two competing major application-based payment solutions: Google Wallet [29] and ISIS [30]. So far these are only available in the United States of America. Both require the installation of an application on your phone, then credit or debit cards have to be linked to their services to make them available for checking out within the app. On checkout the app is simply openend, unlocked with a PIN, and the phone placed on the merchants terminal to complete the transaction. Google Wallet tries to monetize their free service with Google Offers, displaying deals at the current shopping location. It works with any Mastercard PayPass [31] or Google Wallet enabled terminal with Mastercard claiming hundreds of thousands of supported locations world-wide. Non-partner credit cards may still be linked, but all transactions are handled through a virtual Mastercard. ISIS on the other hand is announced to support any NFC-enabled device of the three partners at&t, T-Mobile USA and Verizon launching in summer of 2012 and later. In contrast to Google Wallet, ISIS will only support some major cards directly, forcing users to rely on a prepaid card option, which can be charged in advance. However, ISIS is being backed by mobile phone providers which may come in as an advantage as Google Wallet is currently simply blocked on all Verizon phones while ISIS is readied for release [32]. ISIS is scheduled for a limited

[3]XDA developers, Where to Buy NFC Tags `http://forum.xda-developers.com/showthread.php?t=1662367`
[4]NFC Task Launcher `https://play.google.com/store/apps/details?id=com.jwsoft.nfcactionlauncher`
[5]NFC TagWriter by NXP `https://play.google.com/store/apps/details?id=com.nxp.nfc.tagwriter`
[6]Android 4.1 APIs `https://developer.android.com/about/versions/android-4.1.html#Connectivity`
[7]NFC in action `http://www.nearfield.org/2007/01/video-of-6131-nfc-phone-in-use`

doi: 10.2312/NET-2013-02-1_05

release on October 22nd 2012 [33].

Notably, as of September 2012 Mastercard has released an Android and BlackBerry SDK for their contactless payments product PayPass to enable any NFC-equipped device to pay through their service stepping into direct competition with Wallet and ISIS[8].

On the bright side, the competing standards for payment systems may soon be on the verge of getting unified or at least made compatible as the Electronic Transactions Association - a global trade association representing more than 500 companies including Google, ISIS, Visa and Mastercard - announced the launch of a Mobile Payments Committee on August 9, 2012 [34] including all four major US mobile carriers. At first, members promised to hold monthly meetings to update each other on their activities to slowly expand cooperation with the final goal of achieving industry wide solutions at some point.

Meanwhile as of April 2012, the Deutsche Kreditwirtschaft, a union of all major banks in Germany, has rolled out "girogo" [35]. A huge one-year pilot project covering the region of Hannover plus the cities of Braunschweig and Wolfsburg featuring NFC-enabled banking cards, the "girocard". It allows payments of up to 20 Euros with a swipe over a terminal without any PIN or signature. On the downside, the card has to be charged in advance with as much as 200 Euros via an ATM or a merchant checkout terminal secured by PIN. Single transactions will also not be visible on bank statements. The project has support from a big German grocery store, a gas company and various small retail chains totaling in a few hundred locations so far [36].

At last Microsoft announced [37] to integrate their payment solution in the upcoming Windows Phone 8 operating system. Their "Wallet" will require the phone to carry a Secure SIM element for paying, which is a conventional SIM packing additional functionality for encryption and authentication. It is handed out by the wireless carriers themselves. When transactions are triggered via the phones NFC interface further communication with a terminal will happen directly with the Secure SIM element avoiding the potentially less secure application environment of the phones operating system. "Wallet" will also have support for coupons, similar to Google Wallet, and store virtual boarding passes.

On a broader scale, the GSM Association announced its "Pay-Buy Mobile" initiative as early as 2007 [38] for embedding payment solutions inside SIM cards. Following years of trials, May 2010 saw the roll out of NFC services in Nice, France, for information access, public transport ticketing, coupons, loyalty programs and contactless payments in cooperation with major banks. More cities are planned. Similar undertakings made NFC services available in South Korea, Turkey, The United Kingdom and Tanzania. Mobile provider Orange is in the process of deploying NFC technology to various European countries. 2012 will see further projects by telecom providers KPN, T-Mobile and Vodafone in cooperation with banks in the Netherlands and as previously mentioned the release of ISIS in the US [39]. Several network operators like Deutsche Telekom, Orange and Telenor have promised through GSMA to launch NFC services throughout the world in 2012 [40].

[8] `http://www.mastercard.com/mobile/mobile-paypass.html`

3.4 Ticketing and Identification

Ticketing in public transport or sporting events, access control to restricted areas and embedding in identity documents are further applications for NFC technology. Public transport companies are already using or at least experimenting, access control and identity documents are mainly still promoted by the NFC Forum [41]. In both areas various RFID solutions, like Transport for London's Oyster[9], have been in use for several years using chips like NXPs MIFARE Classic smart card [42]. Biometric contactless readable passports are used in multiple countries around the world including the United States and Germany [43]. Moving public transport systems like Oyster over to NFC provides the freedom to freely exchange cards with customers phones. Due to security requirements, long standardization processes and small renewal cycles this will likely not happen for passports or other federal identity documents anytime soon. Similar concerns and missing standards hinder health care applications, like a virtual patient file linked in a personal NFC-enabled device which could provide relevant health data in a critical situation to speed up and reduce errors during care.

As for public transport, Deutsche Bahn offers their Touch&Travel program in Germany since November 2011. By scanning so called Touchpoints passengers can determine start and end of a journey and be automatically charged for the traveled distance. Showing the ticket to train personnel is realized via the passengers NFC phone interface in combination with an installable app [44]. Transport of London already trialed NFC phone replacements for its Oyster cards with high customer satisfaction, but to this date is waiting for Secure SIM based solutions to match the speed of the traditional Oyster, MIFARE Classic powered, smart card [45].

4. RISKS, ATTACK VECTORS AND EXPLOITS

As with many wireless communication technologies NFC is not invulnerable, despite its short range. Basic connections as specified by ISO/IEC 18092 using the NFCIP-1 protocol [2] are unencrypted and there are no checks for authenticity. Applications on top of NFC are expected to handle encryption and authentication by themselves. Notably, for authentication the NFC Forum already provides a Signature RTD specification [19] to embed signatures in NDEF messages.

4.1 Eavesdropping

As a wireless technology NFC is especially prone to eavesdropping. Despite connections occurring at a range of about four centimeters attackers might still exploit special circumstances and use specialized hardware to listen in on a connection. Similar attacks already exist for RFID contactless cards, in particular those using ISO/IEC 14443

[9] `https://oyster.tfl.gov.uk`

doi: 10.2312/NET-2013-02-1_05

implementations which NFC is also supporting [46]. When using active mode, so both devices are taking turns in generating their own fields, eavesdropping distances of up to 10m may be possible. In passive mode, where the target responds by modulating the initiators field, the range of attack drops significantly to around 1m [47].

4.2 Denial of Service

The simplest form of attack prohibits the use of the device or disturbs communication. As each device reacts to an incoming signal in some form, may it be a user interface requiring interaction, an attacker might spam the device with empty tag signals to make it unusable. The only solution is the inclusion of an off switch to disable NFC altogether [48]. Otherwise, communication might be prohibited by disturbing the data flow through transmitting at NFC frequencies with the correct timing. This would result in scrambled signals the receiving device is unable to decode. The attack just requires fitting hardware and sufficient knowledge of the used modulation and coding. However, NFC devices may easily detect such active corruptions as they require significantly more power on the attackers field [47].

4.3 Data modification

To actually modify data more thought has to be put in how the signals are modulated and coded so data still appears valid to the receiving device. Attacks occur on the bit level, switching single 1s to 0s and vice versa. When using the modified Miller coding only certain bits may be flipped. However, for almost all modes and data rates Manchester coding is used (see 2), allowing to modify any bit of the communication [47]. Prevention involves checking for third-party field influences and stopping communication on detecting any (which NFC devices do by default as specified by NFCIP-1), or using an encrypted channel on a higher layer. There exists an ISO/IEC standard describing NFC-SEC to already provide security on the data link layer complementing application layer security [49].

4.4 Relay attack

A relay attack is executed by sitting in the middle of two communicating parties and simply "relaying" requests and responses effectively making oneself invisible to either party (see figure 3). Relay attacks exist already for RFID systems and have been perfected to work with regular NFC phones by just installing specific pieces of software. An attacker would require two phones to act as proxies connected to each other with a high-speed link such as Bluetooth. One proxy device interfaces with the NFC token or device of a victim functioning as a proxy-reader. It forwards all messages over the high-speed link to the second proxy device imitating a NFC token to interface with the actual NFC reader, acting as proxy-token. Relaying even allows circumventing dynamic authentication on newer NFC card models as using the relay link introduces only small delays still accepted by current card readers. This attack concerns any ISO/IEC 14443 implementing contactless system, many, not NFC, of which are widely in use like the previously mentioned NXP MIFARE products. Possible countermeasures include aborting the communication if round trip times or the location of the pairing device are not as expected. For this purpose it has been suggested to tap into positioning via GPS or cellular networks as present in modern smartphones [50].

Figure 3: Schematic of a relay attack using a contactless smartcard, two NFC equipped phones and a reader terminal.

4.5 Others

Unlike technical attacks there still remains the risk of simply losing the NFC-enabled banking card or phone, with the phone being unencrypted or only secured via a weak PIN opening up abuse by third parties. Authentication should be handled by a separate factor to prevent any of those issues. Phishing by replacing original tags or readers with malicious units can be avoided by signing the content of exchanged messages [48], for example using the Signature RTD as specified by the NFC Forum [19]. Man-in-the-Middle attacks are practically impossible as either initiator or target are able to detect additional fields by a third party as mentioned before [47].

4.6 Implementation vulnerabilities

Attack surfaces do not only exist within the technology but also in implementations and attached services. Vulnerabilities in software handling or parsing NFC messages may open up access to sensitive data or a whole device. An example exploit was demonstrated by Charlie Miller at the Black Hat 2012 conference [51] which can take control of a Nokia N9 running MeeGo or a Galaxy Nexus running the Android 4.0 mobile operating system. Both operating systems accept incoming data beamed from the attackers device or tag and then automatically open a malicious web page or a modified file in a vulnerable app. Protective measures include modifying apps to let the user always confirm the triggered action before executing it.

5. CONCLUSION

Near Field Communication is on its way to become an essential part of our daily lives. It provides simple means of making information available by using NFC tags embeddable everywhere one can think, readable with the NFC-enabled mobile device in your pocket. Sharing of text, websites or setting up Bluetooth or Wi-Fi connections for large file transfers or advanced interaction is as far away as touching two devices. Waving your credit card or phone at checkout makes paying a new experience. However, certain risks are associated with mostly unencrypted data transfers, security holes in still young software libraries or by actual theft. Communication in the range of centimeters may appear to make exploitation difficult, but it is very much possible. As of 2015 every second smartphone may be equipped with the technology [52], standards for better security and interoperability will likely emerge. Near Field Communication is going mainstream, for the better or worse.

doi: 10.2312/NET-2013-02-1_05

6. REFERENCES

[1] *NFC Forum*, http://www.nfc-forum.org

[2] ISO/IEC 18092 *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, 2004

[3] ISO/IEC 14443 *Identification cards – Contactless integrated circuit cards – Proximity cards*, 2000

[4] *Sony Global - FeliCa*, http://www.sony.net/Products/felica

[5] JIS X 6319-4 *Specification of implementation for integrated circuit(s) cards – Part 4: High speed proximity cards*, 2005

[6] *NFC Forum Unveils Technology Architecture And Announces Initial Specifications And Mandatory Tag Format Support* http://www.nfc-forum.org/news/pr/view?item_key=0b210bbd23e9c1a07cb3d975e6317d1d650ed51f, June 5, 2006

[7] Jin-Shyan Lee, Yu-Wei Su, Chung-Chou Shen: *A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*, Industrial Electronics Society, 2007

[8] Ari Juels: *RFID Security and Privacy: A Research Survey*, IEEE Journal on Selected Areas in Communications, Volume 24 Issue 2, 381-394, February, 2006

[9] http://www.zigbee.org

[10] Erina Ferro, Francesco Potorti: *Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison*, IEEE Wireless Communications, February, 2005

[11] *NFC Data Exchange Format (NDEF) Technical Specification*, NDEF 1.0, NFC Forum, July 24, 2006

[12] *NFC Forum Tag Type Technical Specifications*, http://www.nfc-forum.org/specs/spec_list/#tagtypes

[13] N. Freed, N. Borenstein: *RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*, 1996

[14] T. Berners-Lee, R. Fielding, L. Masinter: *Uniform Resource Identifier (URI): Generic Syntax*, RFC 3986, January, 2005

[15] *NFC Record Type Definition (RTD) Technical Specification*, RTD 1.0, NFC Forum, July 24, 2006

[16] *Text Record Type Definition Technical Specification*, RTD-Text 1.0, NFC Forum, July 24, 2006

[17] *URI Record Type Definition Technical Specification*, RTD-URI 1.0, NFC Forum, July 24, 2006

[18] *Smart Poster Record Type Definition Technical Specification*, SPR 1.1, NFC Forum, July 24, 2006

[19] *Signature Record Type Definition Technical Specification*, SIGNATURE 1.0, NFC Forum, November 18, 2010

[20] *Generic Control Record Type Definition Technical Specification*, GC-RTD 1.0, NFC Forum, March 7, 2008

[21] *Sony Xperia SmartTags* http://www.sonymobile.com/gb/products/accessories/xperia-smarttags/

[22] *Simple NDEF Exchange Protocol Technical Specification*, SNEP 1.0, NFC Forum, August 31, 2011

[23] *Logical Link Control Protocol Technical Specification*, LLCP 1.1, NFC Forum, June 6, 2011

[24] *Beaming NDEF Messages to Other Devices*, Android Developers, http://developer.android.com/guide/topics/connectivity/nfc/nfc.html#p2p

[25] *Connection Handover Technical Specification*, Connection Handover 1.2, NFC Forum, July 7, 2010

[26] Heidi Lemmetyinen: *Introducing the Nokia N9: all it takes is a swipe!*, Conversations by Nokia, June 21, 2011, http://conversations.nokia.com/2011/06/21/introducing-the-nokia-n9-all-it-takes-is-a-swipe/

[27] Adam Fraser: *Nokia steps it up a gear, with new accessories*, Conversations by Nokia, June 21, 2011, http://conversations.nokia.com/2011/06/21/nokia-steps-it-up-a-gear-with-new-accessories/

[28] *Microsoft MSDN Windows.Networking.Proximity namespace*, http://msdn.microsoft.com/en-us/library/windows/apps/windows.networking.proximity

[29] *Google Wallet*, http://www.google.com/wallet/

[30] *ISIS*, http://www.paywithisis.com/

[31] *Mastercard PayPass*, http://www.paypass.com/

[32] Amir Efrati, Anton Troianovski: *War Over the Digital Wallet*, The Wall Street Journal, December 7, 2011, http://online.wsj.com/article/SB10001424052970204770404577081610232043208.html

[33] Nathan Ingraham: *ISIS confirms October 22nd launch in Salt Lake City and Austin*, The Verge, October 17, 2012, http://www.theverge.com/2012/10/17/3516778/isis-october-22nd-launch-salt-lake-city-austin

[34] *ETA Launches Committee To Guide Emerging Mobile Payments Industry*, August 9, 2012, http://www.electran.org/docs/releases/2012/ETALaunchesMobilePaymentsCommittee.pdf

[35] *Deutsche Kreditwirtschaft führt neues Markenzeichen girogo für das kontaktlose Bezahlen ein*, January 11, 2012, http://www.die-deutsche-kreditwirtschaft.de/dk/pressemitteilungen/volltext/backpid/26/article/deutsche-kreditwirtschaft-fuehrt-neues-markenzeichen-girogo-fuer-das-kontaktlose-bezahlen-ein.html

[36] *girogo*, http://girogo.de

[37] *Announcing Windows Phone 8*, June 20, 2012, http://windowsteamblog.com/windows_phone/b/windowsphone/archive/2012/06/20/announcing-windows-phone-8.aspx

[38] *GSM Association Aims For Global Point Of Sale Purchases by Mobile Phone*, GSMA, February 13, 2007, http://www.gsma.com/newsroom/gsm-association-aims-for-global-point-of-sale-purchases-by-mobile-phone/

[39] *NFC - Market by Market*, GSMA, http://www.gsma.com/mobilenfc/the-gsma-and-mobile-nfc/nfc-market-by-market/

[40] *World's Leading Mobile Operators Announce Commitment to NFC Technology*, GSMA, http://www.gsma.com/newsroom/worlds-leading-mobile-operators-announce-commitment-to-nfc-technology/

[41] *NFC as Technology Enabler*, http://www.nfc-

forum.org/aboutnfc/tech_enabler/

[42] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, Bart Jacobs: *Dismantling MIFARE Classic*, ESORICS 2008, LNCS 5283, pp. 97-114, 2008

[43] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, Ronny Wichers Schreur: *Crossing Borders: Security and Privacy Issues of the European e-Passport*, arXiv, January 25, 2008, http://arxiv.org/abs/0801.3930v1

[44] *Touch&Travel*, http://www.touchandtravel.de

[45] Dan Balaban: *London Oyster Card Chief: NFC Not Ready for Fast-Paced Fare Payment*, NFC Times, May 30, 2012, http://nfctimes.com/news/london-oyster-card-chief-nfc-not-ready-fast-paced-fare-payment

[46] G.P. Hancke: *Practical eavesdropping and skimming attacks on high-frequency RFID tokens*, Journal of Computer Security, Volume 19 Issue 2, 259-288, 2011

[47] Ernst Haselsteiner and Philips Semiconductors: *Security in Near Field Communication (NFC)*, Workshop on RFID Security RFIDSec, 2006

[48] Gerald Madlmayr, Josef Langer, Christian Kantner, Josef Scharinger: *NFC Devices: Security and Privacy*, Availability, Reliability and Security - IEEEARES, 642-647, 2008

[49] ISO/IEC 13157-1 *Information technology – Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security services and protocol*, 2010, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53430

[50] Lishoy Francis, Gerhard Hancke, Keith Mayes, Konstantinos Markantonakis: *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, 2011

[51] Charlie Miller: *Don't stand so close to me: an analysis of the NFC attack surface*, July 25, 2012, http://www.blackhat.com/usa/bh-us-12-briefings.html#Miller

[52] Peter Schüler: *Nichtöffentlicher Nahverkehr - Die Nahfunktechnik NFC in Smartphones und Chipkarten*, c't 2012, Heft 14, 140-143, 2012, http://www.heise.de/ct/inhalt/2012/14/140/

doi: 10.2312/NET-2013-02-1_05