

Safety and Confidentiality Measures in Near Field Communication (NFC)

Harshalee D. Korde

PG Student, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Mumbai University, Maharashtra, India

ABSTRACT: This paper gives overview of Near Field Communication technology with its safety and confidentiality measures of the technology, namely, introduction to the technology, communication modes, operation modes of the technology, and the resolution to it. The paper lists functioning of NFC with examples. The paper persists to probable security threats that can be launched on the technology and the solution to avert these attacks.

KEYWORDS: NFC; Operation modes; communication modes; threats.

I. INTRODUCTION

Near field communication (NFC) is a set of standards or Smartphone and similar devices for short-range communication with each other by touching them together or bringing them into secure proximity, about 10 centimeters. It exchanges data connecting a reader, like a phone or sensor, and a target, like a microchip or another reader. With just a touch, NFC enables effortless use of the devices and gadgets we use daily.







	STATION AIRPORT	VEHICLE	OFFICE	STORE RESTAURANT	THEATER STADIUM	ANYWHERE
Area						
Usage of NFC Mobile Phone	<ul style="list-style-type: none"> Pass gate Get information from smart poster Get information from information kiosk Pay bus/taxi fare 	<ul style="list-style-type: none"> Personalize seat position Use to represent driver's license Pay parking fee 	<ul style="list-style-type: none"> Enter/exit office Exchange business cards Log in to PC; Print using copier machine 	<ul style="list-style-type: none"> Pay by credit card Get loyalty points Get and use coupon Share information and coupon among users 	<ul style="list-style-type: none"> Pass entrance Get event information 	<ul style="list-style-type: none"> Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	<ul style="list-style-type: none"> Mass and Public Transport Advertising 	<ul style="list-style-type: none"> Drivers and Vehicle Services 	<ul style="list-style-type: none"> Security 	<ul style="list-style-type: none"> Banking Retail Credit Card 	<ul style="list-style-type: none"> Entertainment 	<ul style="list-style-type: none"> Any

Fig. 1. Potential uses of NFC mobile phones

Here are some probable uses of NFC mobile phones [14]:

- Using a smart poster to download music or video.
- Trade business cards with another phone.
- Disburse bus or train fare.
- Print an image on a printer.
- Boarding a flight using a Smartphone as a ticket.
- Reward discounts and concessions through smart NFC posters



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

- Secure identification

II. MODES OF OPERATION

Based on whether NFC uses self-powered devices or powerless devices. The way data is transmitted from device A to device B specifies whether the transferring device is in active or passive mode [7]. NFC supports two modes of operation

- Passive Mode
- Active Mode

1.1. Passive Mode

In the passive mode, the NFC device acts as a target. All NFC tags operate in passive mode. Passive mode is for individual devices which do not have their own power source. These devices depend on the initiator (the reader or the smart phone) to get power. In the reader or writer mode, NFC tags work in the passive mode of operation [4] [6] [10]. If the device does not produce its own RF field it is called a passive device. Passive devices, like contactless smart cards usually do not have power supply.

1.2. Active Mode

This mode of operation applies to those NFC devices which have their power source. Smartphone and NFC readers are devices which operate in the active mode. If the device produces its own RF field it is called an active device. Active devices usually have a power supply. During P2P communication, both the device is active devices [4] [10].

To ensure proper communication following flow is followed:

- All devices should stay in Target mode and not generate an RF field as default.
- A device shifts to Initiator mode simply if it is required by the application.
- 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 sets the transmission speed. After communication, both devices switch back to Target mode and deactivate their RF fields [6].

III. MODES OF COMMUNICATION

Based on how devices interact with each other, NFC supports three modes of communication.

- Peer to peer mode
- Reader/writer mode

3.1. Card Emulation Mode Peer to Peer Mode:

In this mode, communication takes place between two active NFC devices. . Initiator is the device which starts the communication and the other is called the target. Device A sends a data to device B and device B sends a reply. Until any data is received from Device A, Device B cannot send any data. Smart phones such as Google Nexus S, Samsung Galaxy Nexus and a few other phones come equipped with NFC. By tapping these phones beside each other data can be swapped efficiently and with insignificant time delay. The data can be a business card, a music playlist. What data is to be sent is determined by the application [8].

3.2. Reader/writer mode:

This mode of communication involves a NFC device like a smart phone and a NFC tag. NFC tags have limited bytes of memory which can be transcribed onto. The tags can be located in posters or other places and by moving the tag with closer to the NFC device, the stored information is transmitted to the device. It contains information, such as Internet addresses or actions on the device, such as connecting to a wireless network [8]. The NFC enabled Smartphone transcribes to this NFC tag via a writing application. For writing data onto a tag, the NFC device must touch or bang the tag. Unlike way, the NFC device can even read from a tag. This can be used to perform simple operations such as switching Wi-Fi, setting up Bluetooth or even opening an application [4] [8].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

3.3. Card emulation mode:

This mode makes an NFC device such as a Smartphone emulate a smartcard. A smart card is any pocket-sized card with implanted integrated circuits. It is typically made of plastic and contains volatile memory and microprocessor components. Its benefits include the provision of identification, authentication, data storage and application processing [18]. In this mode, the device will stop emitting RF waves and become passive. Only familiar Radio-frequency identification (RFID) readers can communicate with NFC device. The device can emulate one or more than one smartcards if a reader is transported nearby this Smartphone, it can read data off the phone [8].

IV. SECURITY THREATS TO NFC

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 [11].

a. 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:

5.1.1. Denial of service:

This attack compromises the availability of an NFC system. Anti-collision algorithm has to be performed to select the individual device because there are possibilities of more than one NFC device/tag in range. The attacker generates collisions/answers for every possible device address and simulates the existence 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.

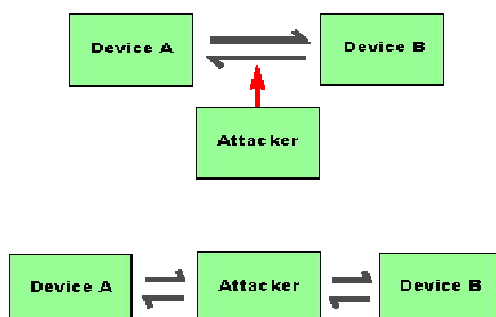


Fig. 4. Denial of Service attack

5.1.2. Man in the middle:

This attack compromises the confidentiality and integrity of an NFC system. In the classical Man-in-the-Middle Attack, two parties which want to talk to each other, called Alice and Bob, are tricked into a three party conversation by an attacker Eve.

A man-in-the-middle (MITM) attack is a form of eavesdropping where communication among two users is supervised and revised by an unauthorized party. Generally, the attacker dynamically eavesdrops by interrupting a public key message exchange and retransmits the message while replacing the requested key with his own.

In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication.

5.1.3. Eavesdropping:

This attack compromises the confidentiality of an NFC system [8]. Because NFC is a wireless communication interface it is obvious that eavesdropping is an important issue. When two devices interconnect via NFC they practice RF waves to converse to each other. An attacker can of course use an antenna to also obtain the conveyed signals. Whichever by investigating or by literature research the attacker can have the required information on how to abstract the conveyed data out of the acknowledged RF signal. Also the equipment mandatory to obtain the RF signal as well as

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

the equipment to decrypt the RF signal must be presumed to be obtainable to an attacker as there is no unusual equipment essential.

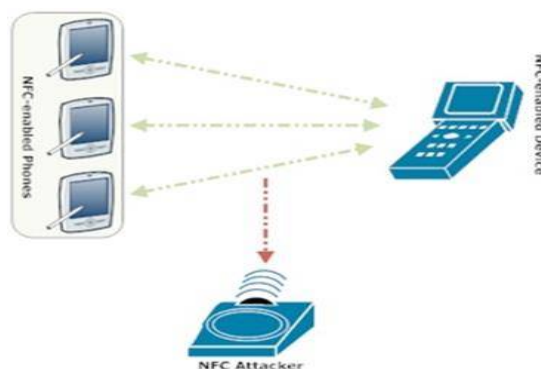


Fig. 6.Eavesdropping

The NFC communication is typically done between two devices in adjacent proximity. This means they are not further than 10 cm (typically less) away from each other. The foremost question is how close an attacker needs to be to be able to recover an operational RF signal. Unfortunately, there is no precise answer to this question. The motive for that is the enormous number of parameters which control the answer. For example the distance determined by on the following parameters, and there are many more.

- RF field characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)
- Characteristic of the attacker's antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.

5.1.4. Relay Attack:

In a relay attack an opposition acts as a man-in-the-middle. An adversarial device or another communication channel is placed secretly between a legitimate tag and reader to interrupt the communications between tag and reader and to increase the range. Tag and reader are fooled into thinking that they are communicating directly with each other. A large distance between a tag and reader can be bridged by using two devices: one for the communication with the reader and one for the communication with the tag.

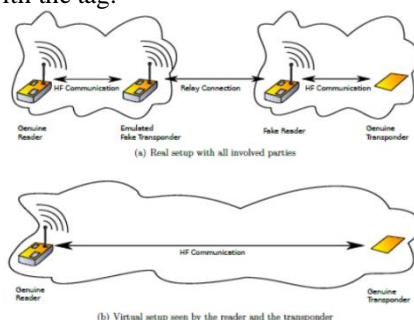


Fig. 7. Relay attack on NFC devices

5.1.5. Data Insertion:

This attack compromises the integrity of an NFC system. This means that the attacker enclosures messages



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

into the data exchange between two devices. But this is only probable, in case the answering device requires a much extended time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be positive, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.

5.1.6. Data Corruption:

Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device.

Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.

5.1.7. Data Modification:

This attack compromises the integrity of an NFC system. In data modification the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption.

The feasibility of this attack highly depends on the applied strength of the amplitude modulation. This is because the decoding of the signal is different for 100% and 10% modulation.

5.1.8. 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 optimized antenna and handle the increasing noise in the communication.

5.1.9. Jamming:

This attack compromises the availability of the NFC system. Tags listen randomly to every radio signal within their range. NFC system can be broken by sender to interrupt communication by purposefully causing electromagnetic interference via a radio signal in the same range or by using appropriate antennas and power rates.

b. Attacks on the NFC Tag

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

5.2.1. Clone:

This attack compromises the secrecy of an NFC system. 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 cannot decide if it is the original or the cloned tag. If some kind of certification is used, this attack would get more complex.

5.2.2. Remove:

This attack would compromise the availability of an NFC system. Considering the poor physical security that tags present, they can be easily removed from the associated items if they are not strongly attached to or implanted in them. Tag removal is a serious threat that can be easily deployed without the need of exceptional technical skills. It is a risk that leads to undetectable objects and suggests a significant security problem. Luckily, this kind of attack cannot be launched on a massive scale. Readers may also be removed if they are situated in unattended places. However, their size decides this attack hard to deploy. The inspiration for this could be a thief, who wants to smuggle the any item through the security checks without recognition.

5.2.3. Destroy:

This attack would compromise the availability of an NFC system. 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



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

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.

5.2.4. Shield:

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

5.2.5. Falsify/Replace:

This attack compromises the integrity of an NFC system. 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.

5.2.6. Tracking:

This attack compromises the secrecy of an NFC system. 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.

V. SOLUTIONS AND RECOMMENDATIONS

5.1 Eavesdropping

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 [14]. 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 passer-by. 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 [13].

NFC by itself cannot protect against eavesdropping. It is important to note that data transmitted in passive mode is considerably tough to be eavesdropped on, but just using the passive mode is probably not sufficient for most applications which convey profound data. The only real solution to eavesdropping is to establish a secure channel.

5.2 Data Corruption

NFC devices can counter this attack because they can check the RF field, while they are transmitting data. If NFC devices do this, it will be able to detect the attack. The power which is needed to corrupt the data is considerably larger, than the power which can be detected by the NFC device. Thus, every such attack should be detectable.

5.3 Data Modification

Protection against data modification can be achieved in various ways. By using 106k Baud in active mode gets impossible for an attacker to modify all the data transmitted via the RF link. This means that for both directions active mode would be needed to defend against data modification. While this is possible, this has the foremost weakness, that this mode is most defenseless to eavesdropping. Also, the protection against modification is not flawless, as even at 106k Baud some bits can be improved. The two other options might therefore be preferred.

NFC devices can check the RF field while transferring. This means the sending device could continuously check for such an attack and could stop the data transmission then an attack is detected.

The third and probably best solution would be a secure channel.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

5.4 Data Insertion

There are three possible countermeasures. One is that the answering device answers no delay. In this case the attacker cannot be faster than the correct device. The attacker can be as fast as the correct device, but if two devices response at the same time no precise data is received.

The second possible counter measure is eavesdropping by the answering device to the channel throughout the time, it is open and the starting point of the transmission. The device could then sense an attacker, who wants to inset data.

The third option again is a secure channel between the two devices.

5.5 Man-in-the-Middle-Attack

It is practically impossible to do a Man-in-the-Middle Attack on an NFC link. The commendation is to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties. Furthermore, the active party should listen to the RF filed while sending data to be able to identify any conflicts triggered by a possible attacker.

Such an attack could be prevented by the use of authentication through a common, independent, trusted certification provider [7].

VI. CONCLUSION

In this paper analysis of near field technology was conducted. Specific aspects of the technology were chosen for the analysis, namely, introducing the technology, the various modes of operation, various modes of communication of the technology, and the solution to it. It then discusses current probable security threats that can be launched on the technology and the solution to prevent these attacks.

REFERENCES

1. Liam Church, Maria Moloney Escher, "State of the Art for Near Field Communication: security and privacy within the field", Escher Group Ltd, 2012.
2. Gauthier Van Damme, Karel Wouters, "Practical Experiences with NFC Security on mobile Phones", Katholieke Universities Leuven.
3. Asawari Dudwadkar, Akhil Gore, Tushar Nachnani, Harshil Sabhnani, "Near Field Communication in Mobile Phones", International Journal of Engineering and Advanced Technology (IJEAT), Volume-3, Issue-1, 2013.
4. "Near field communication white paper", ECMA International, <http://www.ecmainternational.org/activities/Communications/tc32-tg19-2005-012.pdf>
5. Aikaterini Mitrokotsa, Michael Beye, Pedro Peris –opez, "Classification of RFID Threats based on Security", Delft University of Technology (TU Delft), Vol. 4833, LNCS, pp. 68-87.
6. Hussein Ahmad Al-Ofeishat et al. "Near field communication(NFC)", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, 2012.
7. Breitfuss, E. H. A. K., "Security in Near Field Communications. Workshop on RFID Security", <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20%20Security%20in%20NFC.pdf>, 2006.
8. "SET Labs Briefings", Infosys, <http://www.infosys.com/infosyslabs/ublications/Documents/winning-it.pdf>
9. Kerschberger, M., "Near Field Communication A survey of safety and security measures" Institute of Computer Aided Automation, https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf, 2012.
10. "NFC usage and working principles", http://developer.nokia.com/Community/Wiki/Inside_NFC:_Usages_and_Working_Principle
11. Ernst Haselsteiner, Klemens Breitfuß Philips, "Security in Near Field Communication (NFC) Strengths and Weaknesses".
12. Madlmayr, G. et al., "NFC Devices: Security and privacy" Third International Conference on Availability, Reliability and Security, p. 642 – 647, 2008.
13. Kfir Z., Wool A., "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard", IEEE Computer Society, p. 47–58, 2005.
14. "NFC FORUM: Essentials for Successful NFC Mobile Ecosystems", http://www.nfcforum.org/resources/white_papers/NFC_Foum_Mobile_NFC_Ecosystem_White_Paper.pdf, 2012.
15. "Smart card", <http://en.wikipedia.org/wiki/SmartCard>, 2012.