A Survey on Near Field Communication Attacks

Vasanth S[1], Arun Raj L[2]

[1]Department of CSE, B.S. Abdur Rahman University, CHENNAI-48
[2]Department of CSE, B.S. Abdur Rahman University, CHENNAI-48

Abstract— *Near Field Communication (NFC) is one of the emerging technologies nowadays which are used between two NFC enabled devices for faster and easier communication. As it operates at a frequency of 13.56 MHz, it is more secure and used for special transactions. Although it operates on a very low frequency several attacks are possible to exploit it. Here we deal with a list of NFC attacks like eavesdropping, data corruption and manipulation, data insertion, man-in-middle for which possible solutions are given to tackle those attacks. A secure channel for NFC is the best way to deal with the above attacks.*

Keywords— Eavesdropping, Man-in-middle, Near Field Communication, Secure channel for NFC.

I. INTRODUCTION

Near Field Communication or NFC is a short-range wireless communication method where the antenna used is much smaller than the wavelength of the carrier signal. NFC communicates either by modulated magnetic or electric field. It is a low- speed and a low-power device making it easier to setup and is based on inductive-coupling. It works using magnetic induction between two antenna loops located within each other's near field. NFC operates at a frequency of 13.56 MHz, corresponding to its wavelength of 22.11m and mostly used in mobiles phone [1]. This operates at a very close range rather than other communication devices like the Bluetooth so many attacks cannot possibly take place. NFC allows two-way communication and builds upon RFID. There are several modes in which the NFC interface operates. They are called active and passive devices. Active devices are the ones where the device generates its own field and the other is called passive device. Active devices works on power supply whereas passive devices don't (e.g. contactless smartcard). Once two NFC devices starts to communicate several configurations are possible.

The way data is transmitted depends on whether the transmitting device is in active or passive mode which is described in Table 1.1.

Table 1.1

Device A	Device B	Description
Active	Active	RF Field is alternatively generated by Device A and B
Active	Passive	Device A generated RF field
Passive	Active	Device B generates RF field

Table 1.2 shows a comparison between several aspects of NFC and Bluetooth communication methods.

Table 1.2

ASPECT	**NFC**	**BLUETOOTH**
Range	Up to 10cm	Up to 5 m
Frequency	13.56MHz	2.4 – 2.5 GHz
Transfer rate	424 kbit/s	2.1 mbit/s
Set-up time	< 0.1 s	< 6s
Power consumption	< 15 mA	Varies with class

NFC has several applications and are classified into three categories. They are

- Touch and Go
- Touch and Confirm
- Touch and Connect

1.1 Touch and Go

Access control or event ticketing is where the user needs to bring the access code or ticket close to the reader to gain access.

1.2 Touch and Confirm

Mobile payments applications where the user needs to enter a password to confirm that the user has accepted the transaction.

1.3 Touch and Connect

Linking two NFC based devices for enabling peer-to-peer data transfer such as downloading music or pictures.

II. ATTACKS

2.1. Eavesdropping

Eavesdropping attack is possible in most of the wireless communications. NFC can also be eavesdropped [2]. NFC uses RF waves for communication. An attacker could use a rouge antenna to capture the data that is being sent through the NFC enabled devices. The attacker could get the data from the RF. The Fig 2.1. shows an eavesdropping attack where an antenna can be used to capture the data from both the near field communication devices.

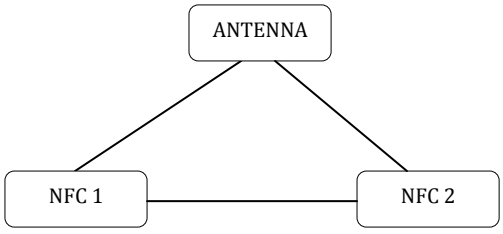

Fig 2.1. Eavesdropping attack

The NFC communicates between a close proximity of approximately 10 cm. The question is how close the attacker needs to be for getting those RF signals. There are several parameters that determine the answer. They are

- Antenna geometry, the environment , shielding effect
- Characteristics of the attackers antenna
- Quality of receivers antenna
- Quality of attacker's RF decoder
- Power of NFC
- Location of attack

The above parameters determine the eavesdropping nature of the attacker. If any of the value is found accurately there are high possibilities that the attacker could gain access to the data [3]. There is also major importance given to the mode in which the NFC data is operating i.e. if it is an active device the NFC devices generates its own RF field whereas in passive it is generated by other device. Both these communication uses different ways of communicating the data and its harder to eavesdrop in passive devices where the RF signal is not appropriate.

2.2. Data corruption and manipulation

Data corruption and manipulation occurs when an attacker disturbs the communication by sending data that may be valid, or even block the data so that it may be corrupted. This attack is like a denial of service attack.

For this the attacker need not decode the data being sent. He just needs to disturb the communication. This state is achieved by sending valid frequencies of the data spectrum at specific time. The correct time can be calculated if the attacker knows how to use the modulation scheme and coding techniques. The attack is not too complicated, since the attacker cannot manipulate the data.

2.3. Data insertion

Attacker inserts messages into the data exchange between two devices. This is possible only if the answering device takes a very long time to answer. The attacker could then send his data earlier than the valid receiver. The attack will be possible only if the inserted data are transmitted before the original device starts to answer. If the data streams overlap, the data will be corrupted. These types of attack are not possible when the device accepts the incoming file soon, whenever there is a time delay the attacker could insert some messages into the communication.

2.4. Man in the middle- attack

Man in the middle attack issues involves two party communications being intercepted by the third party [4]. The third party acts as a relay, by modifying the information received to achieve their aim. This must be achieved without knowing that there is an interceptor between the two devices.

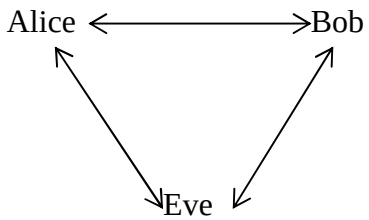

Fig 2.2. Man in the middle attack

As shown above in Fig. 2.2, Assume that Alice and Bob are two NFC users and Eve is the attacker. Assuming Alice uses active mode and Bob in passive mode. Alice generates the RF and sends to Bob, if Eve is close enough she can eavesdrop the data being sent by Alice. Eve must continuously disturb Alice to make sure that Bob doesn't receive the data that is being sent by Alice. In case Alice finds that she is being disturbed, Alice will stop the data that is being transmitted. Let's assume that Alice does not find the disturbance and the transmission continuous. In the next step, Eve needs to send the data to Bob, which is

a problem since the RF field generated by Alice is still there and Eve needs to generate a second RF field. This causes two RF field to be active at the same time and it is impossible to align the two RF fields perfectly. Therefore, it is practically impossible for Bob to understand the data that is sent by Eve. Because of this Man-in-the-Middle attack is not possible. This attack is possible if both Alice and Bob are both in active modes.

NFC device could now be sniffing your credit card without your knowledge. There is also a risk around malicious applications being downloaded onto NFC devices. The application could read any nearby NFC tag and send the data to the attacker. Mitigation for this risk requires user awareness.

Mobile malware are also one of the developing problems. These malwares could steal the credit card information which is stored or used by the NFC device and send it to the attacker through the web or NFC channel.

Another risk which is recently emerged is 'Android Beam' which is used to pass information between devices or from a tag to a device. The information that can be passed includes applications contacts, URLs, etc. There is no confirmation required on the receiving side.. This opens a whole new can of worms as you could transfer malicious applications to devices without the user requiring confirming the transfer. You could also transfer a malicious URL and either trick the user into clicking it or exploit a browser bug to visit the malicious website and download malicious content.

2.5 Relay attack

A relay attack is NFC is where the attacker has to forward the request to the reader (victim) and relay back its answer to the reader in real time in order to carry out a task by pretending to be the owner of the victim's smart card. The access victim system will not able to detect the attack because it will think a card is actually in front of it.

For example the attacker could hold the NFC reader near the victim's card and relays the data over another communication channel to a second NFC reader placed in proximity to the original reader that will emulate the victim's card. Timing is a main constrain for this attack as the distance will be longer and the relay time also increase with the distance for receiving the packets.

2.6 Spoofing

NFC spoofing attack is where a third party pretends to be another entity an induce the user to tap the tag so that it could force to execute a malicious code, aided by the fact that the mobile devices are configured to execute the commands of the NFC tag automatically.

III. POSSIBLE SOLUTIONS

3.1 Eavesdropping

NFC itself cannot protect itself against eavesdropping attack [5]. It is important to notes that the data being transmitted in passive mode is relatively hard to be eavesdropped on rather than the active mode, but just using passive mode is not sufficient for most applications while transmitting sensitive data.

The only solution possible for solving the attack is by creating a secure channel which will be outlined later.

3.2 Data corruption and manipulation

NFC devices can overcome the attack as it can check the RF field while they are transmitting. The power needed to corrupt the data is significantly larger than the power being sent while the data transfers. If NFC device finds this, it can detect the attack. The power output is actually larger than the original power needed for data transfer. The NFC devices identify it before in hand to know that there is an attacker and do not send the data to the corresponding device.

3.3. Data insertion

There are three possible methods the overcome this attack.

- Answering device answer with no delay. The attacker cannot be faster than the correct device [6]. The attacker can be fast as correct device only when two device answers at the same time no correct data is received.
- Listening by the answering device to the channel during the transmission. The device could then detect the attacker, who wants to insert the data.
- Secure channel between two devices.

3.4. Man-in-the-Middle

It is nearly impossible to do a man-in-the-middle attack [7]. It is recommended to use active-passive communication mode so that RF field is continuously generated by one of the valid party. Additionally, the active device should listen to the RF field while sending data so that it can detect any disturbance caused during the transmission.

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.

3.5. Secure channel for NFC

Establishing a secure connection between two NFC devices is the best way to protect from any kind of NFC related attacks. A secure connection might include a AES algorithm of 128 bit key so that the algorithm is more secure and it takes years to decrypt a single possible key.

A standard key agreement protocol like Diffie-Hellman based on RSA or Elliptic Curves could be used to establish a secret shared key between two NFC users.
The shared secret key can then be used to derive a symmetric key like the AES for providing confidentiality, integrity and authenticity of the data transmitted.

IV. CONCLUSION

Near field technology will have a meaningful impact on the usability of mobile devices in various contexts; on one hand, it will facilitate a user's experience by making it possible to access infinite services with a single devices, but as a side effect it also has a potentially dramatic impact on users' privacy. NFC operates in close range of 13.56 Mhz. Even though NFC have the shortest range among radio frequency technologies, combining them with existing technologies like Bluetooth or Infrared can increase its range of applications. So to deal with the attack of close proximity is nearly impossible. NFC itself cannot provide security against the attack like eavesdropping, data corruption or data insertion. The only solution to overcome these attacks is to establish a secure connection between to NFC device users to make the communication more secure. We can also use a 128 bit AES algorithm to encrypt the data so that the data being sent will be more secure than normal file transfer. We can also establish key agreement protocols without authentication to provide a standard secure channel.

REFERENCES

[1] Marcos J. Lopez Fernandez, Jorge Guzan Fernandez, Sergio Ríos Aguilar, Blanca Salazar Selvi, Ruben Gonzalez Crespo "Control of attendance applied in higher education through mobile NFC technologies" Journal of Future Generation Computer Systems, Volume 29, Issue 10, page no: 4478–4489 September 2013.

[2] Lai-Ying Leong ,Teck-Soon Hew, Garry Wei-Han Tan , Keng-Boon Ooi "Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach", International Conference on Embedded Systems, page no:5604–5620, May 2012

[3] Soon-Nyean Cheong , Huo-Chong Ling , Pei-Lee teh "Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system" , IEEE International Conference on Social Networks, Page no: 433-440, June 2011.

[4] Gregor Broll, Eduard Vodicka , Sebastian Boring "Exploring multi-user interactions with dynamic NFC-displays" Pervasive and Mobile Computing, Volume 9, page no 242–257, May 2013.

[5] Wolfgang Apolinarski , Marcus Handte, Muhammad Umer Iqbal, Pedro Jose Marron "Secure interaction with piggybacked key-exchange" Pervasive and Mobile Computing, Volume 10, page no:22–33, 2014.

[6] J. M. León-Coca, D. G. Reina, S. L. Toral, F. Barrero, N. Bessis "Authentication Systems Using ID Cards over NFC Links: the Spanish Experience using DNIe" The 4th International Conference on Emerging ubiquitous Systems and Pervasive Networks ,Page no:12-20, EUSPN-2013.

[7] Fahad Mehmood, Mohammad Hassannezhad, Tahir Abbas "Analytical investigation of mobile NFC adaption with SWOT-AHP approach: A case of Italian Telecom" The 7th International Journal on Interdisciplinary in Engineering, Volume 10, Issue 5, Page no :322-330, INTER-ENG 2013.