Security Analysis of Near Field Communication

Nicklas Blomqvist Linus Blomquist
Email: {nicbl154,linbl758}@student.liu.se
Supervisor: Nahid Shahmehri, nahid.shahmehri@liu.se
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

This report presents the NFC technology and discusses the security issues. Common threats are presented and countermeasures against them are discussed. By reading papers in the area we have found that NFC has quite good security by design but needs complements like anti-virus programs in phones.

1. Introduction

The first application using NFC came out in 2006 [3] which means that this technology to communicate between two devices has been out for less than a decade. This leads to many questions regarding how secure NFC really is and what measurements are done to prevent possible attacks like denial-of-service- or man-in-the-middle attacks. Since NFC may be used in security critical environments, e.g. authorization method to access restricted areas, security is an important issue and needs to be considered.

This report starts with a presentation of the NFC communication and in what areas it can be used. After that comes a detailed presentation of the most common threats NFC faces and how to prevent those. Finally related work and our own solutions of this project will be presented.

2. NFC

To be able to discuss the security in NFC you need to understand how it works and the technology it uses. In this section we want to present NFC so that the threats can be discussed.

2.1 Introduction to NFC

NFC is a way to enable wireless communication between two electronic devices and builds on RFID technology with some key differences [4]. Firstly RFID has a transmission range of up to 100 meters compared to NFC that typically only has 4 centimeters [5]. Secondary RFID only enables one way communication instead of the two-way communication that NFC provides. This means that both devices using NFC can either receive or send messages in a communication. Finally, only one passive device can be scanned simultaniously instead of several. The standards that are used in NFC are ISO/IEC 14443 A&B and JIS-X 6319-4 [6] and it operates on the high frequency scale of RFID namely 13.56MHz.

The transmission range for NFC is a clear distinction to other similar wireless communication methods like Wi-Fi [5] or Bluetooth that have a far longer transmission range. Also the speed of the communication is relatively small and has a maximum speed of 424 kbps [5].

A NFC device could either be active or passive. If a device is passive it means that it includes data that can be read by another device but it can not read data from another device itself. In contrast can an active device both read data and send data to other devices [8].

To make a connection using NFC one device starts with emitting an electric current that creates a magnetic field that are used as a bridge between the devices. Passive devices then uses this energy to emit a response which removes their need of an own battery. This could for example be very useful when putting NFC tags on posters where there are no batteries available. Active devices on the other hand have their own power resources that they use [9]. This is another difference between NFC compared to Bluetooth and Wi-Fi that instead of using an electromagnetic radio field to communicate uses a radio transmissions instead [10].

NFC tags can be of different types that differ in memory space, communication speed and so on. This to adapt as good as possible to different business needs. These tags could have a read-only memory that prevents a possible attacker to change the data in the tag but could also have a rewrite-able memory [10].

2.2 Usage in reality

NFC could be used in several usage areas to enable wireless communication. Examples of these areas could be [11] [12]:

- Getting information from commercial posters
- Set-up a Bluetooth or Wi-Fi connection in a simple way
- Use your NFC device as a ticket or payment method
- Leave business cards
- As authorization method

Today, plastic cards using a magnetic strip or a chip are very frequently used but may in the future potentially be replaced by NFC devices such as cellphones. The reasons for this are because plastic cards have a limited lifetime compared to software in a NFC device, which has an infinite lifetime, which removes the cost of producing plastic cards [13]. If a cellphone gets broken you can simple move the NFC software to a new device.

2.3 Threats [14]

There will always be threats to systems and it's important to know about them in order to prevent them. Here we present an overview of the different attacks NFC faces in theory. We will in subsequent chapters go into more details of how these could be prevented.

2.3.1 Eavesdropping

In this type of attack the intruder only listens to the channel and tries to intercept messages in the NFC communication. In a payment scenario this could be about getting account details that enables the attacker to pretend being you at a later occasion and use your account as payment method.

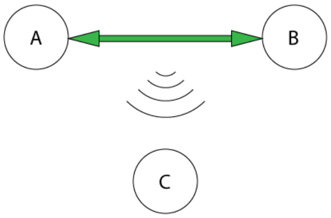

Figure 1. C is eavesdropping on communication between A and B.

Henning Siitonen Kortvedt showed in his master thesis 2009 that in a lab environment with the help of an antenna he could extend the transmission range from a passive NFC device to 29,2cm [13]. He also believes that it would be possible also in real life to eavesdrop complete NFC messages within a range of 30cm.

Gerhard Hancke is a research assistant at the university of London and have made some research regarding eavesdropping of RFID that as mentioned earlier is the technique NFC builds on. Using ISO/IEC 14443 (and ISO/IEC 15693) that NFC is also compatible with, he successfully completed an eavesdropping attack with equipment worth less than 50 pounds. It also seems like that the forwarding channel, the communication from the active device to the passive device, have a much longer transmission range than the backward channel [15], the communication from the passive device back to the active device, which make the backward channel safer from eavesdropping attacks.

2.3.2 Denial-of-service attack

This attacks happen when an attacker send interfering messages into a NFC communication channel that destroys legitimate messages. The interfering messages has to be on the same frequency as NFC and can be any random noise. This makes the service unavailable to be used by any user.

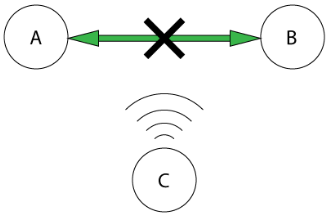

Figure 2. C is doing a Denial-of-service attack on A and B

Because a passive NFC tag lacks an own power resource it does not have the ability to remember who has scanned it and in which time. If you then use an active NFC device and keep it close to the tag at all time you deny all other users access to the tag by keep the tag occupied by handle requests from the same active device. Even an active NFC device can be attacked in a similar way by using an empty NFC tag that are kept close to the active NFC device. The active device will be kept occupied by giving error messages to the passive tag [23].

2.3.3 Man-in-the-middle attack

A Man-in-the-middle attack is a form of active eavesdropping where the attacker creates independent connections to the victims and relays the messages between them. The attacker act like a link between them but they think that they are communicating with each other. All this without neither the sending- or receiving device realizes that someone are currently listening to their communication. A regular eavesdrop can be stopped by encrypting the traffic between the devices.

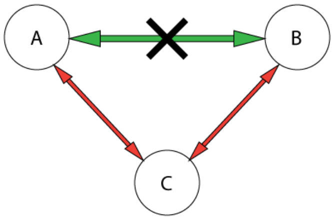

Figure 3. C is doing a Man-in-the-middle attack on A and B

The man-in-the-middle attack don't have the same problem because of the attackers connections to the victims and can set up correct encryption on this connections and still be able to read the traffic because all keys are known to the attacker.

Due to the short range of NFC the man-in-the-middle attack is practically impossible since the attacker needs to intercept the messages between the victims. NFC requires these to be close to each other, in order of centimeters, and therefore makes it really hard to intercept the messages and prevent them to reach their destination. The attacker's device also needs to be in range to establish connections to both victims, this makes the attack practically impossible to do without the victims noticing [2]. The attack then behaves like a Denial-of-service attack rather than a Man-in-the-middle.

By using a fake tag and a fake reader between a legitimate tag and a user Gerhard Hancke showed that, without the users' knowledge, this attack was possible on the ISO 14443A standard. The user places the card near the legitimate tag but got an answer from the fake reader and start communicates with this one instead. The fake reader the sends the private information to the fake tag that in turn communicates with the real legitimate reader [17].

2.3.4 Cloning of a passive device

Every device gets a unique unit id (uid) when it is manufactured. This is easy to count as a security feature and many uses these devices just by checking the uid. If a uid is stolen from someone and they can be able to construct a device with the same uid the attacker can be able to act like that device.

2.3.5 Theft of a NFC-device

If an attacker steals a complete NFC-device it becomes really hard to protect it against data intrusion. The protection against these types of attacks lies no longer in the hands of the NFC communication but instead in the security of the device itself by for example a strong password. Because of this we have decided to only mention this type of attack and will not go in to any further details on it.

2.3.6 Virus on NFC-device

A passive NFC-device could potentially be infected by a virus that spread to active devices that scan these. Studies from 2006 shows that RFID tags, that are very similar in a technical aspect to NFC tags, are vulnerable to those attacks. By 2010 came the first virus to smartphones [18] which tells us that these types of attacks can be performed today.

2.4 Real attacks on NFC-devices

Here we will present how NFC is threatened in the reality.

2.4.1 Attack on Samsung Galaxy S3 [20] [21]

In a study were researchers in 2012, from the company MWR labs, able to completely take over another device using NFC. The attack was performed by having two Samsung galaxy S3 right next to each other and letting one of the devices trying to gaining control over the other. The attacked device never noticed anything because the attacking software runs like a background program. The android version that was used here was 4.0.4 and this attack has been prevented in Android version 4.1.

The attack was performed by letting the attacking device having a malicious file that it uploads to the other device. The malicious file itself has nothing to do with NFC but was here just used to prove a point. To attack the security flaw in android 4.0.4 the malicious program then trigger this security flaw 185 times to breach the system. After this was performed the malicious program then used a second security flaw to gain complete access of the device.

The reason why this attack becomes possible was because ASLR (address space layout randomization) was not completely developed until android 4.1 and this attack have now been prevented.

2.4.2 Cloning of LIU-card

By using an Identive SCL3711 smart card reader/writer, a MIFARE card with writeable uid and a computer with Ubuntu 14.04 we were able to clone our own student card. We were able to use it in the same way as the original which is a serious threat. It is as powerful as stealing the victim's card but with a lower risk that they notice it.

The software used for the cloning was obtained by installing the packages “nfc-lib” and “nfc-bin” from Ubuntu’s package management system apt-get.

3. Solutions and Analysis

The security of the communication is important to both devices communicating. This is why the different threats have to be countered. In this section we will discuss solutions for the threats mentioned in the threats section.

3.1 Countermeasures

Here we will present how to protect NFC against the threats we found.

3.1.1 Eavesdropping [16]

There are several solutions to these attacks. A first solution could be building a faraday cage around the devices that communicate that make it impossible for other devices to intercept messages in the conversion. A second, more realistic solution is to create a secure channel for the devices to communicate over.

3.1.2 Denial-of-service attack [16]

While an active device are sending data it simultaneously checks the radio frequency signal to detect if someone is trying to interfere the data transmission using a lot more energy than just an active device would do. Then it can temporarily stop the sending and continue when the interfering signals has stopped. This however does not help against a simultaneous noise signal which you cannot protect against.

An active NFC device, that people shall be able to scan with NFC tags, shall have some mechanism to turn on and off to make it harder to perform denial of service attacks on them by keeping a tag close to it at all time [24]. By remembering who has scanned it before and not serve the same user again for a certain amount of time could also prevent to this types of attacks.

3.1.3 Man-in-the-middle attack [16]

A solution could be if you use distance bounding protocols that enables the reader to check if the sender really are in the electromagnetic field or if it is under attack by a man in the middle. Another prevention to these attacks could be building a faraday cage as explained under eavesdropping attacks.

RFID technology has also a frame waiting time (FWT) that is a time limit of how long time there could be between a request and a response. This makes it harder for the man in the middle to be able to deliver data in time so the sender and receiver do not understand that they are under attack.

3.1.4 Virus on NFC devices [8]

As mentioned earlier a passive NFC-tag could have a read-only memory that in an easy way prevents the infection of these devices. Installing anti-virus software on NFC devices and use a secure channel for communication could protect active devices from these attacks.

4. Conclusions

With this report we have concluded that the security in NFC is pretty good because of its short operating range and the technology itself. Without concerning availability, we only see Eavesdropping as a threat in reality that can really harm the users because it is hard to prevent.

This is a pretty new technology and there has not been research much. Because of that we were not able to find that much information about physical attacks on it and have been focusing more on theoretical attacks instead.

5. References

[1] -

[2] Haselsteiner, Ernst, and Klemens Breitfuß. "Security in near field communication (NFC)." *Workshop on RFID security*. 2006.

[3] History of near field communication, Available at: http://www.nearfieldcommunication.org/history-nfc.html (Accessed: 1 May 2014).

[4] The difference between RFID and NFC, Available at: http://rapidnfc.com/blog/72/the_difference_between_nfc_and_rfid_explained (Accessed: 1 May 2014).

[5] About the technology, Available at: http://nfc-forum.org/what-is-nfc/about-the-technology/ (Accessed: 1 May 2014).

[6] Technical specifications, Available at: http://members.nfc-forum.org/specs/spec_list/ (Accessed: 1 May 2014).

[7] Bluetooth vs NFC, Available at: http://www.dailywireless.org/2011/07/22/bluetooth-4-0-vs-nfc/ (Accessed: 1 May 2014).

[8] How NFC works, Available at: http://www.nearfieldcommunication.org/how-it-works.html (Accessed: 1 May 2014).

[9] Inside NFC - how it works, Available at: http://apcmag.com/inside-nfc-how-near-field-communication-works.htm (Accessed: 1 May 2014).

[10] Tag types, Available at: http://www.nearfieldcommunication.org/tag-types.html (Accessed: 1 May 2014).

[11] NFC in action, Available at: http://nfc-forum.org/what-is-nfc/nfc-in-action/ 1/5 (Accessed: 1 May 2014).

[12] Ways to use NFC, Available at: http://www.nearfieldcommunication.org/using-nfc.html (Accessed: 1 May 2014).

[13] KORTVEDT, Henning Siitonen. Securing Near Field Communication. 2009.

[14] NFC security, Available at: http://www.nearfieldcommunication.org/nfc-security.html (Accessed: 1 May 2014).

[15] Hancke, Gerhard. "Eavesdropping attacks on high-frequency RFID tokens." *4th Workshop on RFID Security (RFIDSec)*. 2008.

[16] Vulnerabilities and principals attack schema, Available at: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/ (Accessed: 1 May 2014).

[17] Hancke, Gerhard P. "A practical relay attack on ISO 14443 proximity cards." *Technical report, University of Cambridge Computer Laboratory* (2005): 1-13.

[18] RFID tags vulnerable to viruses, study says, Available at: http://www.computerworld.com/s/article/109560/RFID_tags_vulnerable_to_viruses_study_says (Accessed: 1 May 2014).

[19] Security risks, Available at: http://www.nearfieldcommunication.org/nfc-security-risks.html (Accessed: 1 May 2014).

[20] Security researchers hack Android via NFC to gain full control, steal data from a Samsung Galaxy S3, Available at: http://thenextweb.com/google/2012/09/19/security-researchers-hack-android-via-nfc-samsung-galaxy-s-iii/ (Accessed: 1 May 2014).

[21] Galaxy S3 hacked via NFC at Mobile Pwn2Own competition, Available at: http://forums.cnet.com/7726-6132_102-5363152.html (Accessed: 1 May 2014).

[22] NFC Phones Raise Opportunities, Privacy And Security Issues, Available at: https://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues (Accessed: 1 May 2014).

[23] Verdult, Roel, and François Kooman. "Practical attacks on NFC enabled cell phones." *Near Field Communication (NFC), 2011 3rd International Workshop on*. IEEE, 2011.

[24] Gerald et. al., “NFC Devices: Security and Privacy”, The Third International Conference on Availability, Reliability and Security, IEEE, 2008.