# Attacks on Near Field Communications on Mobile Phones

Håkon Nymo Matland
hakonnym@stud.ntnu.no
TTM4137 Wireless Security Technical Essay

November 17, 2013

## 1 Introduction

The Near Field Communication (NFC) technology is being deployed in mobile phones all over the world. The technology's applications is wide [1]. Several companies focus on one of it's most promising applications: payment solutions using NFC [2]. An analysis by Berg Insight claim that one in three mobile phones will come with NFC by 2017 [3], making the technology a huge future marked.

NFC is a set of standards for devices to establish radio communication with each other by bringing them in close proximity, usually not more then a few centimeters. The standards are based on RFID, and mixed with other standards cover data exchange formats and communication protocols. Communication is possible between two NFC enabled devices, or a NFC enabled device and unpowered NFC chip.

The need of security and robustness is very important, as an insecure and attackable device would give criminals new ways to steal funds, or simply take control over the device. Different attacks have been proven successful and malicious, and the threat should be taken seriously by both individuals and corporations. Simple RFID-stickers and vulnerabilities in software is all an attacker need to do harm. This essay will present and discuss some of the successful or potential attacks previously demonstrated by experts in the field of NFC and security.

## 2 Potential threats on NFC enables devices

### 2.1 Smart poster URI spoofing

With the deployment of NFC capable mobile phone, the concept of smart posters came. The poster is used to advertise or give the customer a service. The user only has to tap their NFC enabled mobile phone in close proximity to the advertisement, and something happens on the phone [4] [5]. Through social engineering or software vulnerabilities this can be exploited. Changing the RFID chip in the poster makes it possible for customers to believe they are accessing a legitimate service, while they are not.

#### 2.1.1 Web browser exploits and malicious software download

A possible scenario is an user tapping their phone on a smart poster to gain the URL of a service. If an attacker has changed the RFID chip to one of his own, he can trick the users to enter a spoofed URL, with the goal of phishing sensitive information through a login or sign up form.

In 2012 security researcher Charlie Miller proved how he with a simple RFID sticker could gain full root shell access on an Android phone [6] [7]. With full root shell acces, several exploits are possible. Charlie miller was able to download every file on the Although the attack primarily used exploitable bugs in the browser, the attack was triggered by the mobile phones NFC.

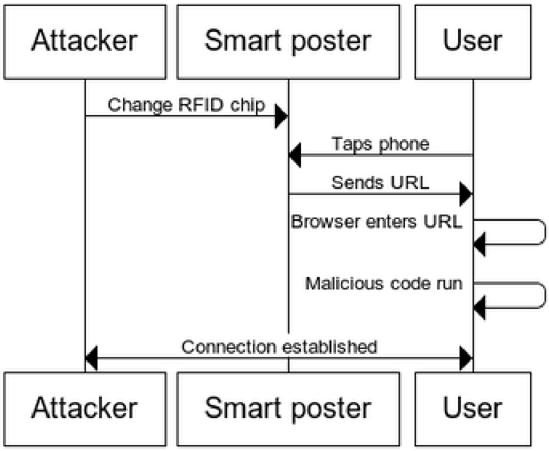

Figure 1: Possible smart poster attack

The concept described in the previous above can also be used more explicitly to run malicious code on the device. The attacker has the possibility to trick the user into downloading an application to install directly. On Android devices you could simply use the smart poster to direct the user to a .apk file on the internet. If the poster is trying to advertise an app, a user not thinking critically might install the application, and make the device send all kind of data to the attacker. The application may appear like the one the user wanted to download, with a similar name and icon.

#### 2.1.2 Premium rated telephone services

Similar to have a RFID chip send a web URL, it can also be used to invoke telephone connections or sending sms [8]. The user might be asked if he wants to call or send, but some users will likely not pay attention to what is says on the screen if it is received from what looks to be a legitimate source. This opens a whole new range of premium service rate scams. A poster claiming to let you call a free service might suddenly make an user call an expensive premium rate number. A user trying to purchase something from a vending machine might end up with a high phone bill, and no snack.

### 2.2 Dirty use of USSD codes

) Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. Some device manufacturers have also implemteded their own set of USSD codes to make the device change or view settings. Several devices also have USSD codes to reboot the device, or even factory reset the device.

In 2012 security expert Ravi Borgaonkar showed how USSD codes could be used in NFC attacks [9].

### 2.3 Eavesdropping

As with every other wireless communication interface eavesdropping is an obvious threat. If the communication is not properly encrypted and secured, parties not participating in the transmission of data may capture the radio frequencies and store them for analysis. An experiment as part of the master thesis by Henning Siitonen Kortvedt at the Norwegian University of Science and Technology concluded that it is practical possible to capture and demodulate data sent in both directions between two NFC devices [10] [11]. If the data communicated is not correctly secured, the threat of eavesdropping is quite clear. No services benefit from giving illegitimate third parties the opportunity to eavesdrop on the communication of the service.

### 2.4 Denial-of-Service attacks

A Denial-of-service attack(DoS attack) is an attempt to make a service unavailable to its intended users. The motivation for an attacker to perform a DoS attack may vary, but the result is nonetheless destructive. DoS attacks may be used to destroy the trust relationship between the customer and the service provider.

## 3 Conclusion

(a) Scale=0.20

(b) Scale=0.15

(c) Scale=0.10

Figure 2: The Linksys WRT54G line of routers include both 802.3 Ethernet and 802.11b/g wireless LAN.

## References

[1] Diogo Remedios, Luís Sousa, Manuel Barata, and Luís Osório. Nfc technologies in mobile phones and emerging applications. In *Information Technology For Balanced Manufacturing Systems*, pages 425–434. Springer, 2006. Available online at: http://link.springer.com/chapter/10.1007/978-0-387-36594-7$_4$5.

[2] Garry Wei-Han Tan, Keng-Boon Ooi, Siong-Choy Chong, and Teck-Soon Hew. {NFC} mobile credit card: The next frontier of mobile payment? *Telematics and Informatics*, 2013.

[3] Sarah Clark. One in three mobile phones to come with nfc by 2017. `http://www.nfcworld.com/2013/06/05/324448/one-in-three-mobile-phones-to-come-with-nfc-by-2017/`. [Online; accessed 5-November-2013].

[4] Irene Luque Ruiz and Miguel Ángel Gómez-Nieto. University smart poster: Study of nfc technology applications for university ambient. In *3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008*, pages 112–116. Springer, 2009. Available online at: http://link.springer.com/chapter/10.1007/978-3-540-85867-6$_1$3.

[5] NFC Forum. Smart posters, how to use nfc tags and readers to create interactive experiences that benefit both consumers and businesses. `http://www.nfc-forum.org/resources/white_papers/NFC_Smart_Posters_White_Paper.pdf`, 2011. [Online; accessed 13-November-2013].

[6] Charlie Miller. Exploring the nfc attack surface. `http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf`. [Online; accessed 6-November-2013].

[7] Sebastian Anthony. Black hat hacker lays waste to android and meego using nfc exploits. `http://www.extremetech.com/computing/133501-black-hat-hacker-lays-waste-to-android-and-meego-using-nfc-exploits`. [Online; accessed 6-November-2013].

[8] Collin Mulliner. Vulnerability analysis and attacks on nfc-enabled mobile phones. In *Availability, Reliability and Security, 2009. ARES'09. International Conference on*, pages 695–700. IEEE, 2009. Available online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5066549.

[9] Ravi Borgaonkar. Dirty use of ussd codes in cellular network. `http://www.youtube.com/watch?v=Q2-0B04HPhs`, note = [Online; accessed 16-November-2013.

[10] Henning Siitonen Kortvedt and Stig F Mjølsnes. Eavesdropping near field communication. In *The Norwegian Information Security Conference (NISK)*, 2009.

[11] Henning Siitonen Kortvedt. *Securing Near Field Communication.* PhD thesis, Norwegian University of Science and Technology, 2009.