Brandi Crawford

Donald Raikes

CS9223: Mobile Security

Spring 2014

Team Project

Security Concerns for NFC

**Near Field Communication (NFC)** is contactless communication between mobile devices using radio frequency identification (RFID). The devices can either be a passive tag or an active reader. There are 3 modes of operation:

* **Reader/Writer Mode** – Device is Proximity Coupling Device, or an active card reader. It generates its own RF fields while trying to discover passive devices to read.
* **Card Emulation Mode** – Device acts as a Proximity Inductive Coupling Device,or a passive tag.
* **Peer-to-Peer Mode** – There’s bidirectional communication between devices. They both can shift between active and passive mode.

**NFC Data Exchange Format (NDEF)** defines the format to store NFC data in RFID tags. Standardized by the NFC Forum, NDEF defines a number of NFC specific data types that RFID tags can store and transport. The NC Forum also defines **Simple NFC Exchange Protocol** for the specification of the communication between two NFC devices.

As with all types of technology, there are several security concerns. The most basic issue is the lack of link level security. NFC requires no validation and wireless communication is not encrypted. Basic usage is when the mobile device comes close enough to read a tag, it simply reads the tag and performs an action. The web browser component is controllable by NFC, so if the tag read contains a URL, the browser will just open up and redirect to the URL.

NFC’s short range is a great defense against **sniffing** attacks. Also, **eavesdropping** on passive devices is nearly impossible because passive devices send data using inductive coupling on the field generated by the active devices. General rule of thumb is 1 m (~3.2 feet) for passive devices and 10 m for active devices.

The only thing a NFC device can do against **Denial of Service attacks** is to detect them. However, **data modification** is more complicated on the part of the attacker. It is possible for bits rates higher than 106 kbit/s because of the signal encoding, bit highly improbable at 106 kbit/s rate.

In **Man-in-the-middle (MITM) attacks**, an attacker sits between two parties and tricks them into believing they’re communicating with one another when they’re really communicating with the attacker. First, the attacker sets up communication with Device#1, pretending to be Device#2, and catches the messages from Device#1. Then the attacker sets up communication with Device#2, and communicates with Device#2 with messages it receives from Device#1. With NFC, devices are able to receive and transmit data at the same time. They can verify the radio frequency field and detect a collision if the received signal does not match with the transmitted signal to twat MITM.

In conclusion, NFC as a technology has its proximity and card reader mode as a great asset to its implementation. However, as Van Damme and Wouters claim, “perfect security can only be obtained when dedicated cryptography is used to establish a secure channel between communicating devices.”

References

* Mulliner, Collin. “Hacking NFC and NDEF: why I go and look at it again.” NinjaCon 2011. June 18 2011. Web. 25 Mar 2014. <http://www.mulliner.org/nfc/feed/nfc\_ndef\_security\_ninjacon\_2011.pdf>
* Van Damme, Gauthier, and Karel Wouters. “Practical Experiences with NFC Security on Mobile Phones.” Katholieke Universiteit Leuven. Web. 1 Apr 2014. <http://www.cosic.esat.kuleuven.be/publications/article-1288.pdf>