GOsafeonline
A monthly infocomm security newsletter

Monthly Newsletter – Issue No. 2013-04

# The Security Issues in Mobile Near Field Communication

**Near Field Communication (NFC)** is a short range low power wireless Radio Frequency Identification (RFID) technology that allows the exchange of data between two devices within 10 cm distance. NFC chips are embedded into several mobile phones to provide services such as:

1. **Tickets or boarding passes:** Replace paper tickets or boarding passes on public transport systems or airlines.

2. **Payments:** Replace cash and credit cards to make payments for shopping and parking meter.

3. **Access control:** Replace traditional keys to gain physical access into your house, care, office and even university.

4. **Coupon:** Replace paper vouchers and coupons for redemption.

5. **Download information:** NFC chips embedded in posters and other promotional materials allow customers to unlock additional information such as maps, video, URLs.

## How Mobile NFC Works

A NFC device either creates its own Radio Frequency (RF) or retrieves power from the RF generated by another NFC device. NFC device that has power supply to generate its own RF is known as an active device, otherwise, it is known as a passive device, such as a contactless smart card.

An NFC-enabled mobile phone is an active device. To transfer data with another NFC device, all you need to do is place your NFC-enabled mobile phone together with the device, or bring them into close proximity. Such data transfer method is usually used in smart phones and other electronic devices for identification purpose to gain access to systems and receive or transmit information. Unlike the RFID chip in contactless smart card which is a one way communication channel that only sends information when requested, a NFC chip is a two way communication device based on a message and reply concept. It has the ability to power up a passive chip to receive information.

Although NFC is not limited to two devices, device A has to select a receiving device B prior to sending the message, which will be ignored by the non-selected devices and only device B is able to reply. As such, message broadcasting for promotional purposes is not possible since a device cannot send or receive data from more than one device at a time.

# Security Issues In Mobile NFC

Despite all the advantages of using mobile NFC, as with all the wireless technologies, there are various security issues. Let’s learn about the possible types of mobile NFC attacks.

| | |
|---|---|
| **Eavesdropping** | An attacker is able to use an antenna to receive the RF signal for the wireless data transfer. The distance from which an attacker needs to be in order to eavesdrop, depends on several parameters such as the quality of the antenna and location (e.g. barriers like walls) of the attacker. The attacker has to be fairly close in proximity, usually less than 10m for the attack to happen. However, a passive device is harder to eavesdrop as compared to an active device. |
| **Data Corruption** | It is a form of Denial of Service (DoS) attack where an attacker blocks the reception of the transmitted data, or disturbs the communication such that the receiver is not able to decipher the data. The attacker does not need to decipher the data transferred since the aim is to destroy the data transferred by deliberately transmitting radio signals to reduce the signals to random noises.<br>NFC device checks for RF signal when sending data. As the power to corrupt data is bigger than sending the data, the sending device is able to detect the attack and stop the data transmission automatically. |
| **Data Manipulation** | An attacker intercepts and manipulates the data by modifying the binary value before sending the data back to the intended receiver.<br>NFC device is able to detect the increased in power that is required for the usual communication and stop the data transmission automatically. |
| **Data Insertion** | An attacker inserts data into the communication channel before the answering device makes a reply. This happens only if the answering device requires a longer time to reply. If the inserted data and the data from the answering device overlap, the data will be corrupted. |
| **Man-In-The-Middle** | An attacker acts as a middleman between two NFC devices to intercept the data without the knowledge of the two NFC devices. The attacker either reads and records or manipulates the data before relaying it to the receiving device.<br>Due to the short range proximity and the detection capabilities of NFC devices, it is difficult for this attack to happen especially when RF signals has to be aligned in an active-active communication mode. |

# Tips To Secure Your Mobile NFC

Even though the short range communication of NFC has reduced the possibility of attacks, let's look at some tips to better secure the mobile NFC.

| | |
|---|---|
| **Disable Mobile NFC** | Disable your mobile NFC whenever it is not required, this helps to prevent any attacker from hitching your NFC signal. |
| **Use SSL Application** | The best way to ensure NFC security is to choose applications that use secure channels such as Secure Sockets Layer (SSL) which the transmitted data are encrypted. This helps to protect against eavesdropping and data manipulation attacks. |
| **Enable Password Lock** | Losing your NFC enabled mobile device allows any finder to wave the phone over a card reader to make purchase or transfer any sensitive information. By enabling password lock on your mobile device, it prevents the access to NFC if the device is stolen. |

## Interesting Reads

- What is NFC:

  http://en.wikipedia.org/wiki/Near_field_communication

- Uses of NFC:

  http://www.gsma.com/mobilenfc/

- Benefits of using NFC:

  http://online.wsj.com/article/SB10001424127887324103504578372450500759438.html

- Types of attacks:
  http://www.nearfieldcommunication.org/nfc-security.html

www.gosafeonline.sg

www.facebook.com/gosafeonline

Published by: A member of:

iDA SINGAPORE

gosafeonline.sg Cyber Security Awareness Alliance

## In the next issue...

Learn about the security usage of external devices such as hard disk or thumb drive.

Let us know what you like about this newsletter and what we can do to better serve your infocomm security awareness needs.

If you have any enquiries or feedback for our newsletter, do write to us at contact_us@gosafeonline.sg.

BE AWARE, RESPONSIBLE AND SECURE!