NFC on mobile devices

Seminar IT-Security Workshop
Winter term 2013

Daniel Bendyk **Manuel Rüger**
Robert Sprunk **Paul Wilhelm**

Institut für Informatik

27. September 2013

Outline

1. Introduction
2. NFC - Use cases
3. NFC - Available Hardware
4. NFC - Available Software
5. Vulnerabilities in NFC
6. Linux on Android devices
7. Conclusion

NFC - Basics

Near **F**ield **C**ommunication is based on **R**adio-**F**requency **ID**entification technology with focus on

- short ranges
- secure data transmission

Specs:

- Frequency: 13.56 MHz
- Bit rate: 424 $\frac{kbit}{s}$
- Range: below 0.2m

Initial goals

- Getting used to available NFC tools, exploits and vulnerabilities
- Executing common Mifare exploit tools (mfoc, mfcuk) on mobile devices
- Playing around with replayed or proxied NFC communication

NFC - Use cases

- Authentication (passport)
- Monetary transactions (wallet)
- Data transmission

NFC - Available hardware (I)

Mobile devices with NFC support

- Samsung Galaxy Nexus (NXP PN65N)
- Google Nexus 7 (2013) (Broadcom BCM20793M)
- Samsung Galaxy S4 Mini (Broadcom BCM20794)

Recent (Broadcom) NFC controllers are unable to read/write Mifare Classic tags (NXP protocol extensions are proprietary)

Type 1 (Innovision Topaz), NFC Forum Type 2 (Mifare Ultralight), Type 4 (Mifare DESFire) are supported.

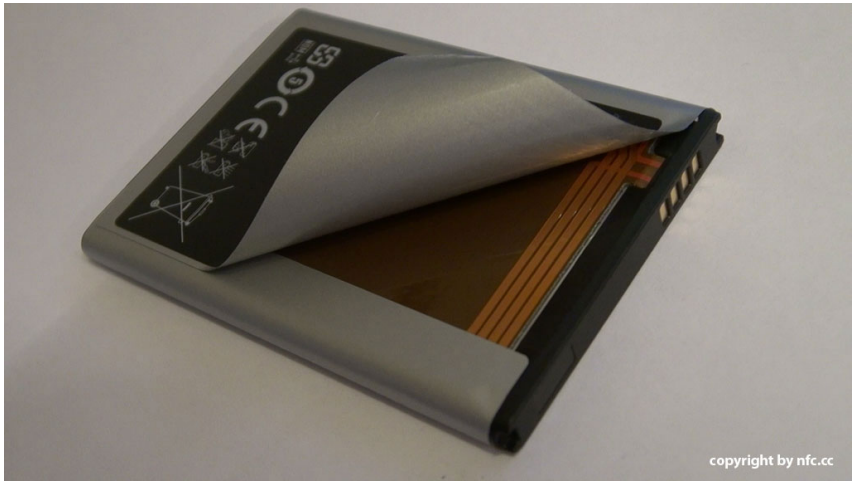
NFC - Available hardware (II)

NFC Tags

- Mensacard (Mifare Classic 1K)
- Access card for Johann-von-Neumann-Haus (Mifare Classic 4K)
- nPA (ISO 14443A)
- Biometric passport (ISO 14443A)

Our choice: Samsung Galaxy Nexus

- Wide range of supported NFC tags
- Decent ROM support, not too recent



NFC - Available Software (I)

Software stacks

- libnfc-nxp
  - Android's original NFC-stack
  - Supported only in SDK (Java)
  - No support in NDK (only with Java Native Interface)
  - No lowlevel API, only highlevel commands available
- opennfc
  - NFC Simulator (Win32 only ☹)
  - Android support (can replace the Android stack)
  - No widespread support

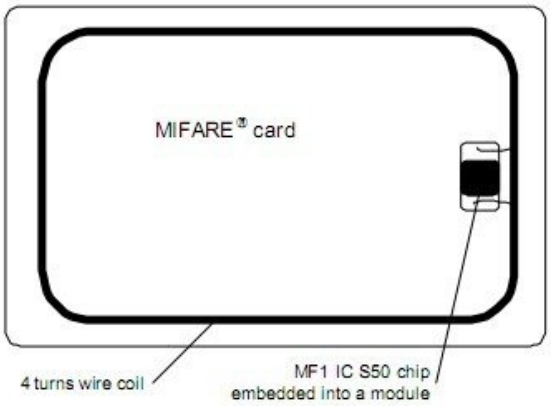
NFC - Available Software (II)

Software stacks

- libnfc
  - Support for multiple exploiting tools
  - Uses libusb as backend
  - No native support for Android available
  - Drivers available for Acr122, PN53x
  - Galaxy Nexus uses unsupported controller
- Linux kernel NFC-stack
  - Available since kernel 3.1
  - Userspace daemon: Neard
  - Support for PN54x chipsets
  - Galaxy Nexus' PN65N includes PN544

NFC - Mifare Classic

- Two types: 1K or 4K
- 16 sectors (1K) or 32+8 sectors (4K)
- Blocks per sector 4 (1K) or up to 16 (4K)
- 2 Keys per sector (called key A and B)
- Implements a weak proprietary stream cipher Crypto-1
- Unencrypted sectors use one of a small set of default keys



Vulnerabilities in Mifare Classic

Attacks:

- Darkside Attack (Nicolas T. Curtois, 2009)
  - Works for every card, takes a longer time
- Offline Nested-attack (Nijmegen/Oakland Group, 2009)
  - If one sector is encrypted with a known key, other sectors are crackable in a short amount of time

Tools:

- mfoc (Mifare Offline Cracker), implements Offline Nested-attack
- mfcuk (Mifare Classic universal toolkit), implements Darkside Attack

Both tools depend on the libnfc stack.

Linux on Android devices

- Emulation / Running in a container
  - "Virtual terminal solution"
  - No direct access to hardware
- Replacing Android userland
  - Uses libhybris to translate glibc to bionic syscalls
  - Android kernel, Linux userland
- Expanding Android userland
  - Same as above, plus access to Android tools

The last two options have only pre-alpha implementations

Existing problems

- NFC is dead(?), maybe not.
- Older vulnerable tags are widespread
- Secure tags are more expensive
- Many different software stacks on devices
- No unified ultimate stack

Discussion

- *I'm walking down the street and I need pants [trousers]. My phone has an NFC chip. It knows where I am. It tells me about two stores, one to the left with a 20% discount and one to the right with a 30% [discount].*

  Eric Schmidt, 2010

- NFC stands for Nobody Fucking Cares.