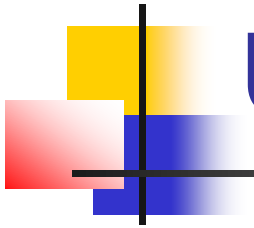
Untersuchung NFC Interface auf Android Telefonen

- Teilnehmer : Frank Lange, Johannes Rother
- Betreuer : Dominik Oepen
- Datum : 28.09.2012



Überblick

1. Vorwissen
2. Die Guthaben- App
3. NFC Kartenemulation
4. Ausblick

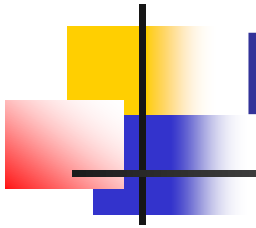
Vorwissen

- NFC
- Mensakarte

NFC

- Near Field Communication
- 13.56 MHz
  - Smart cards
  - Personalausweis
- Reichweite : 1-4 cm
- In einigen neuen Handys verbaut

(ca. 85; HTC, Samsung, etc...)



Mensakarte

- Mifare Classic 1K
- 1 KByte Speicher
  - 16 Sektoren mit jeweils 4 Blöcken
  - 1 Block hat 16 Byte
- Erste Blöcke unverschlüsselt
  - Rest hat einheitlichen Key

Die Guthaben- App

- Arbeitsmaterialien
- Karte knacken und auslesen
- Portierung auf Android
- Fazit

Arbeitsmaterialien

- Reader mit NFC
- Mensakarte
- Libraries und Tools
  - libnfc
  - NFC-Tools

Karte knacken und auslesen

- mit mfoc (Mifare Classic Offline Cracker) auslesen → Inhalt abspeichern (Dump)
- Dump
  - Entschlüsselt und liefert Key
  - 1 KByte großer Inhalt in Hex
- Auswertung
  - mehrere Dumps mit versch. Guthaben
  - Vergleich zeigt veränderte Bytes

Beispiel

Block : 12

- 3,13 €

00 00 01 39 38 00 00 00 21 21 00 53 53 00 00 01

- 3,63 €

00 00 01 6b 6a 00 00 00 21 21 00 54 54 00 00 01

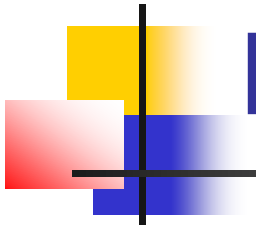
Guthaben | Prüfsumme Aufladungen

- 16,30 €

00 00 06 5e 58 00 00 00 21 21 00 23 23 00 00 01

Portierung auf Android

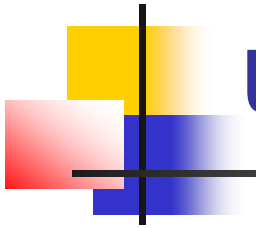
- Voraussetzungen
  - Android SDK (für API und libraries)
  - Eclipse mit Plugins
- API bietet Funktionen für Zugriff auf einzelne Sektoren und Blöcke
  - Keys für Sektoren angeben
- interessante Bytes auslesen und Guthaben berechnen



Fazit

- Geringer Aufwand beim Auslesen
  - alle Mensakarten haben gleichen Key
  - Guthaben nicht stark verschlüsselt
- Guthaben erhöhen ...
  - API zum Schreiben da
  - Backend vorhanden und tägliche Kontrolle

NFC Card Emulation unter Android



Zielsetzung

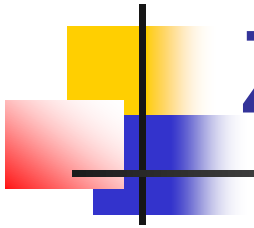
Schritte / Vorgehen

NFC Proxy (App)

Simply Tapp (App)

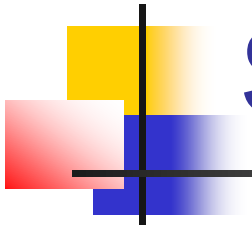
Fazit

Ausblick



Zielstellung

Untersuchen ob/wie NFC Kartenemulation mit einem (NFC fähigen) Android Gerät möglich ist



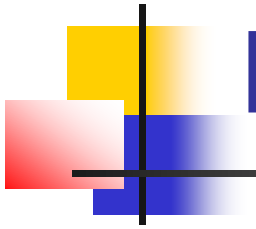
Schritte

Device rooten

CyanogenMod 9 installieren

App: NFC Proxy (Eddie Lee) testen

App: SimplyTapp (Doug Yeager) testen



NFC Proxy (Eddie Lee)

Ausgangspunkt: Vortrag auf der Defcon20 (Juli 2012)

http://www.blackwinghq.com/assets/labs/presentations/EddieLeeDefcon20.pdf

Bietet NFC Proxy und Kartenemulation

Demo:

http://www.youtube.com/watch?v=w_vYuLyfw3E

Probleme – NFC Proxy

funktioniert out of the box nur mit Kreditkarten

Benötigt ISO-14443 Patch von Doug Yeager

- Mifare Classic nicht 100% ISO 14443 konform

Selbst mit APDUs vom nPA keine korrekte Emulation möglich

Vermutung: kein Einfluss auf NFC Stack

Simply Tapp (Doug Yeager)

Yeager verantwortlich für
Kartenemulationspatches für CyanogenMod

Stellt mit seiner App ein Google Wallet
Äquivalent für CM Nutzer

App *emuliert erfolgreich* ISO 14443 Karten

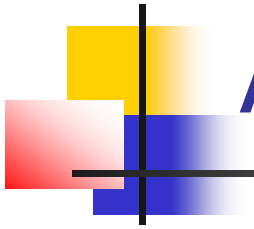
Leider nicht Open Source

Fazit - Kartenemulation

Kartenemulation unter Android technisch realisierbar (auch MifareClassic)

SimplyTapp liefert starkes Indiz für Emulation des neuen Personalausweises, da mit der App ISO-14443 Karten emuliert werden können

Für MifareClassic aber z.Z. Noch keine Werkzeuge zur Verfügung



Ausblick – weitere Schritte

Genaue Untersuchung von SimplyTapp und den dazu gehörigen Android Patches

Dazu evtl. Kontaktaufnahme mit Doug Yeager

Noch genauere Analyse der NFC Proxy App, vlt. reichen „kleinere“ Tweaks