

Funktion und Einsatz von RFID

Aus den Augen aus dem Sinn

Tobias Mueller

Uni Hamburg

CampusGrün Datenschutzkongress - 2011-04-02



1 RFID Basics

- History
- Funktion
- Gefahren
- Wo gibt es RFID
- Daten auf RFID

2 RFID Schutz

- Crypto auf RFID
- Ausleseschutz
- Politisch

3 Q&A



About me

Kontakt

Jabber muelli@jabber.ccc.de
ACF0 F5EC E9DC 1BDC F09D
B992 4147 7261 7CB6 4CEF

Mail muelli@cryptobitch.de
CF3E D935 AE6B DE0A D508
AF86 3EE0 57FF AA20 8D9E

- 🐾 Talk ~ 45 mins
- 🐾 Sehr high level
- 🐾 **Sofort fragen**
- 🐾 Danach hacken :-)

Motivation

Why the heck?

- 🐾 Funktionsweise von RFID
- 🐾 Verbreitung von RFID
- 🐾 Maßnahmen gegen RFID
- 🐾 Aufklärung



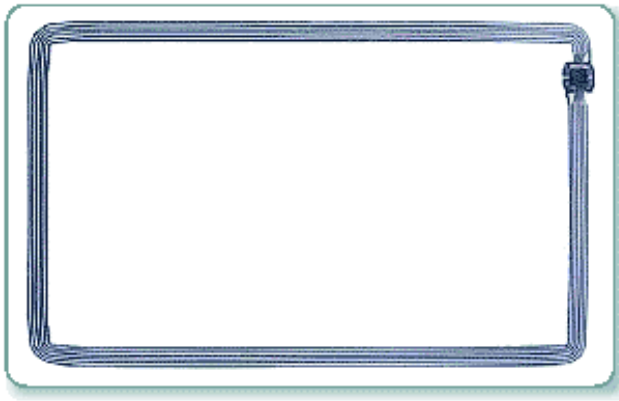
History - Magnetkarte



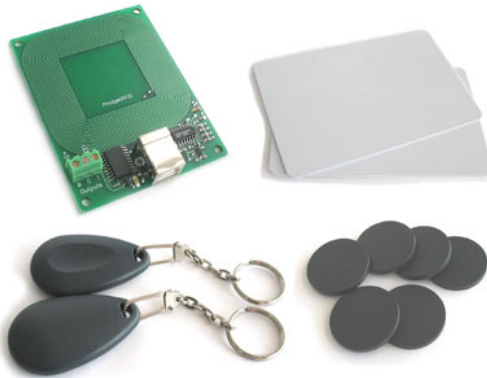
History - Barcode



History - RFID Tag



History - RFID Tag - Buttons



A photograph showing a roll of white 'MATRICS' tape with green circular patterns and red diagonal stripes. The tape is being applied to a dark suitcase. A label on the suitcase reads 'FRA 100' and '100'.

History - RFID Tag - Oystercard



History - RFID Tag - Legic Prime



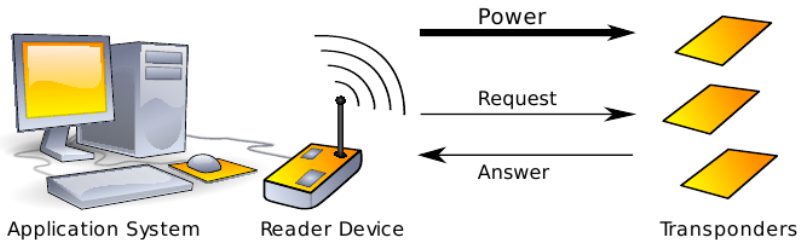
History

- 🐾 Vom Barcode zum Funkchip
- 🐾 Aber auch crypto und smart cards
- 🐾 ISO 14443 (und weitere)
- 🐾 135 kHz, *13.56 MHz*



Funktion

Kontaktlose Datenübertragung:



Gefahren

Barcode Ersatz?

Barcode	RFID
Gleich pro Produkt auf Sicht physisch groß one-at-a-time manuelles Lesen ~ 100 Bit	Eindeutig via Funk wenige Millimeter 100te gleichzeitig automatisches Lesen ~ 1000 Bit



Gefahren (cont.)



Gefahren (cont.)

Szenarios

- 👣 Einkaufsverhalten ausspionieren
- 👣 Lesegeraete koennten ueberall sein (Tuerschwellen, Tanksaeulen, ...)
- 👣 Funk = Elektrosmog (?)
- 👣 Umweltbelastung?



Gefahren - Diskussion

Leseentfernung zu groß

- 👣 Verschiedene Entfernungen
- 👣 aktive vs. passive Tags
- 👣 wenig Entfernung uU gewollt

Zu wenig Lesegeräte um tracken

- 👣 Statt alle paar Meter: Keypunkte



Gefahren - Diskussion (cont.)

Zu wenig Informationen auf Tags

- 🐾 Seriennummer ist Referenz (Schuhe)
- 🐾 Profil meist eh interessanter (Produkte, Aufenthaltsorte, ...)

Herstellung von RFID und Verarbeitung von Daten teuer

- 🐾 Google
- 🐾 Hardware / Computing Preise werden fallen



Wo gibt es RFID

-  Metro Future Store
-  ePass
-  ePerso
-  Bahncard 100
-  Tiere (ISO/IEC 11784 und ISO/IEC 11785)
-  Buecher
-  Geld?



Daten auf RFID

- ☞ Mensakarten
 - ☞ Schattenkonto
 - ☞ Transaktionen auf der Karte?
- ☞ Dublin Bus / LUAS
 - ☞ Format noch nicht verstanden
- ☞ Taiwan Payment + Public Transport
 - ☞ Eingestiegen
 - ☞ Ausgestiegen
 - ☞ Kaffee gekauft



Crypto auf RFID

Generell

- Mehr Transistoren
- größeren IC
- teurere Produktion

Mifare Ultralight

- Billige Lösung für wegschmeißbare Karten
- Kein Crypto
- alle Sektoren lesen
- beschränkt schreiben
- relativ einfach zu emulieren
- billiges Zugangssystem

<http://www.youtube.com/watch?v=Srzf2MSC06Y>



Crypto auf RFID (cont.)

Mifare Classic

- teurere Karten für, i.e. Mensakarten
- Crypto1 gebrochen
- lesen von allen Sektoren
- schreiben von allen Sektoren
- EasyCard <http://www.youtube.com/watch?v=Dws9gpaMV40>

Mifare DESFire

- bspw im Reisepass
- offene, gute Crypto



Crypto auf RFID (cont.)

Legic Prime

- high-end Lösung fuer Zugangskontrolle zu Militär- oder Flughafenanlagen
- Crypto broken
- <http://www.youtube.com/watch?v=r5q-5zoNyCo>



Schutz vor RFID - technisch

- 🐾 Metallhüllen (wie Ziercke und seinem Reisepass. . .)
- 🐾 Antenne durchtrennen
- 🐾 Mikrowelle (Vorsicht!)
- 🐾 Blockertag (Stalled)



Gesetzlicher vor RFID

- 🐾 Forderung des FoeBud
- 🐾 Drang oder Zwang zu RFID Nutzung verbieten
- 🐾 Zweckbestimmtheit von RFID Nutzung und deren Daten
- 🐾 Hackerlaubnis
- 🐾 RFID nicht in “anonymitäts verhindernder” Weise einsetzen



Q&A

Who dares to have a question?!

Questions?!



Referenzen

<http://chaosradio.ccc.de/cre098.html>

<http://kif.fsinf.de/wiki/KIF345:Chipkarten>

<http://www.jurawiki.de/UniChipKarte>

<http://www.ccchb.de/wiki/PM:MensaCard>

https://wiki.chaosradio.ccc.de/Chaosradio_135

<https://events.ccc.de/congress/2010/Fahrplan/events/4114.de.html>

<http://events.ccc.de/congress/2009/Fahrplan/events/3510.en.html>



Lizenz

CC-BY-NC-SA 3.0 DE

This work is licensed to the public under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Germany License.

