

Kontaktlose Smartcards Angriffe und Gegenmaßnahmen

Lehrstuhl für Kommunikationssicherheit

Seminar von Hendrik Dettmer
Betreuer: Timo Kasper

Übersicht

- 1) Einführung und Geschichte
- 2) Das RFID-System
- 3) Angriffe und Gegenmaßnahmen

Einführung und Geschichte

- ▶ Kontaktlose Smartcards Untergruppe von RFID
- ▶ RFID (Radio Frequency Identification)
- ▶ Die ersten Entwicklungen gab es im 2ten Weltkrieg
- ▶ Die Apparaturen waren riesig und klobig



- ▶ Ab den 80ern Jahren wurden RFID Systeme kleiner
- ▶ Auch in elektronischen Warensysteme gegen Diebstahl
- ▶ Neuer Standard mit EPCglobal
- ▶ Die aktuellen Smartcards sind mit RFID ausgerüstet
- ▶ von-Neumann-Architektur



Beispiel:

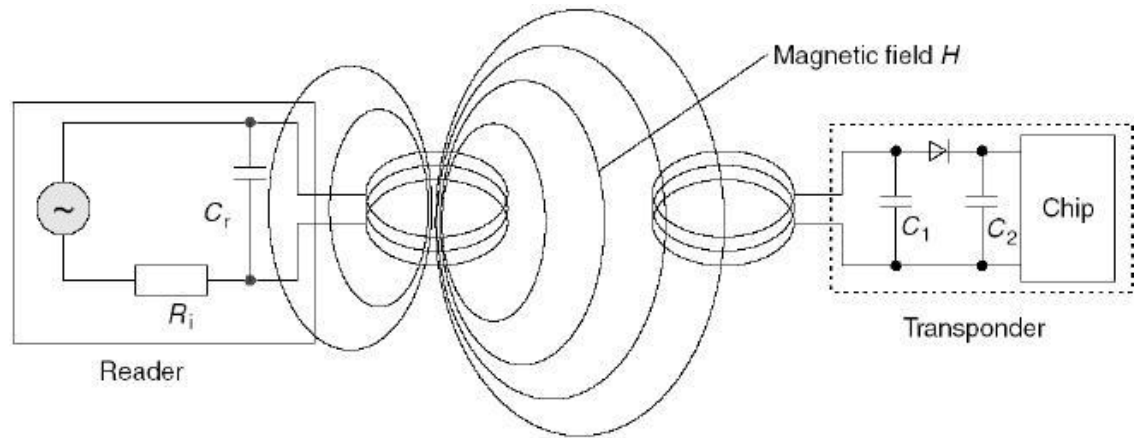
Der Elektronische Reisepass



Ein RFID System

- ▶ Smartcards oder „nur“ RFID

- ▶ aktive oder passive Tags



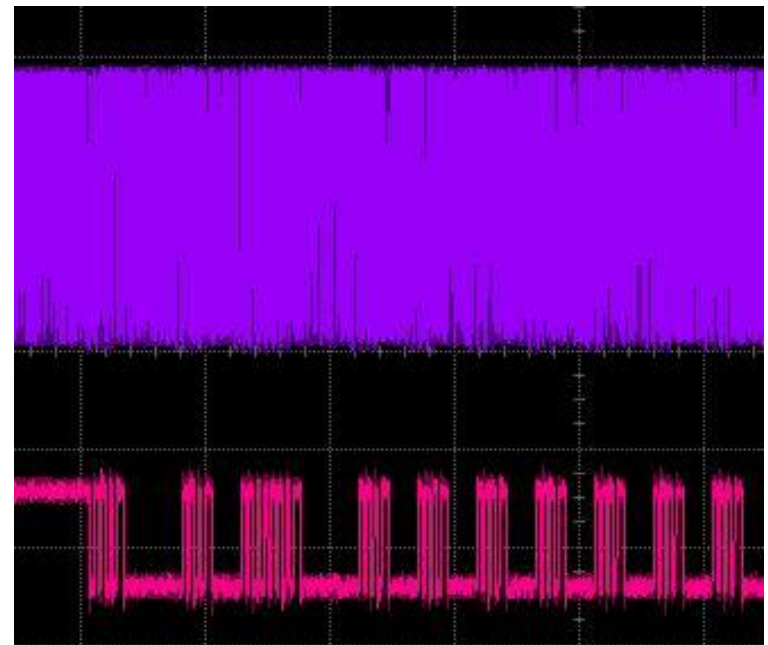
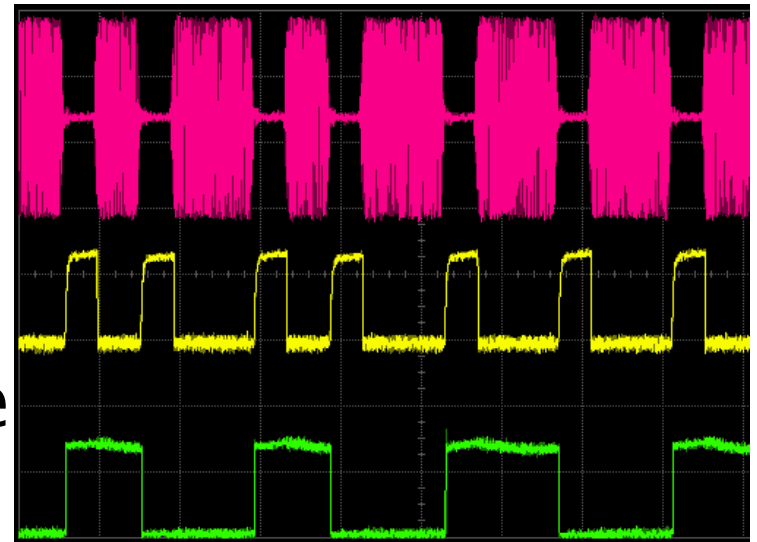
- ▶ unterschiedliche Reichweiten

- ▶ ISO 14443 (Philips Mifare)

- ▶ Energie und Informationen über das elektromagnetische Feld



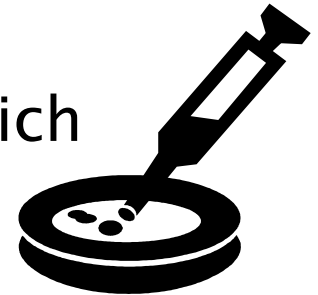
- ▶ Lesegerät sendet den modifizierte Miller Code
- ▶ Kondensator speichert die Energie
- ▶ Tag sendet seine Antwort mit einer Lastmodulation
- ▶ Manchester-Codierung (Transformator)



Angriffe und Gegenmaßnahmen

1. Inhalt eines Tags fälschen

- Gefälschte Daten werden injiziert
- Ohne Sicherheitsmaßnahmen leicht möglich
- Mit Passwort schützen, verschlüsseln



2. Tag klonen

- Mit Schlüsseln ein Tag klonen
- Bei alten ePässen möglich
- Signaturen und Hashfunktionen verhindern das Ändern von Daten



3. Deaktivieren

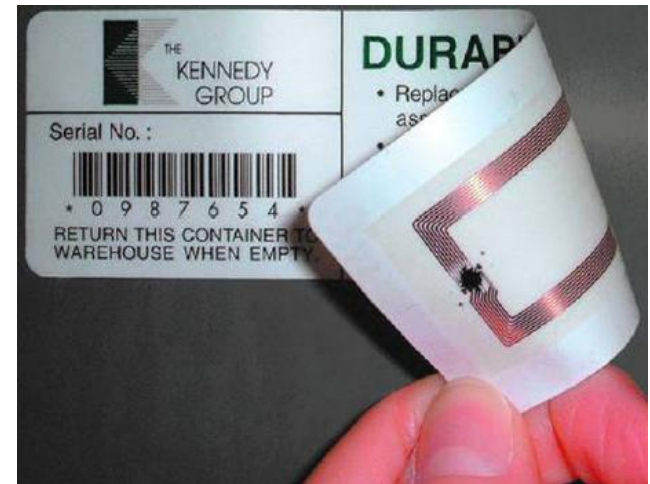
- Kill- oder Löschbefehle entfernen alle Daten
- Sind Passwort geschützt (32 Bit)
- Einfache physische Mittel

4. Ablösen

- „Umkleben“ von Preisschildern
- Nur durch physische Mittel zu lösen

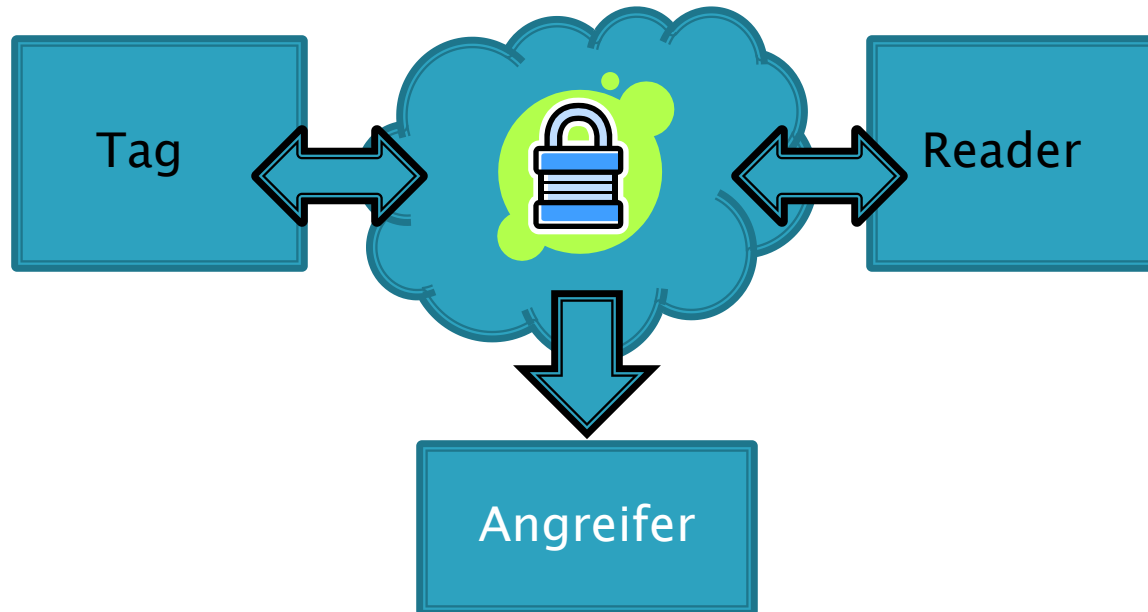
5. Stören

- Mit einfachen Mitteln möglich
- Keine Robustheit



6. Abhören (Eavesdropping)

- Mit einem selbstgebautem „Sniffer“
- Der Luftkanal kann schlecht abgeschirmt werden
- „Sniffer“ können klein und günstig sein
- Verschlüsselung bietet Sicherheit



7. Blocken

- Blocker-Tags kann man kaufen
- Gebaut für ein einziges Antikollisionsprotokoll

8. Identität des Readers fälschen

- Nicht immer ohne Back-End möglich
- Challenge und Response Protokoll



9. Verfolgen eines Tags

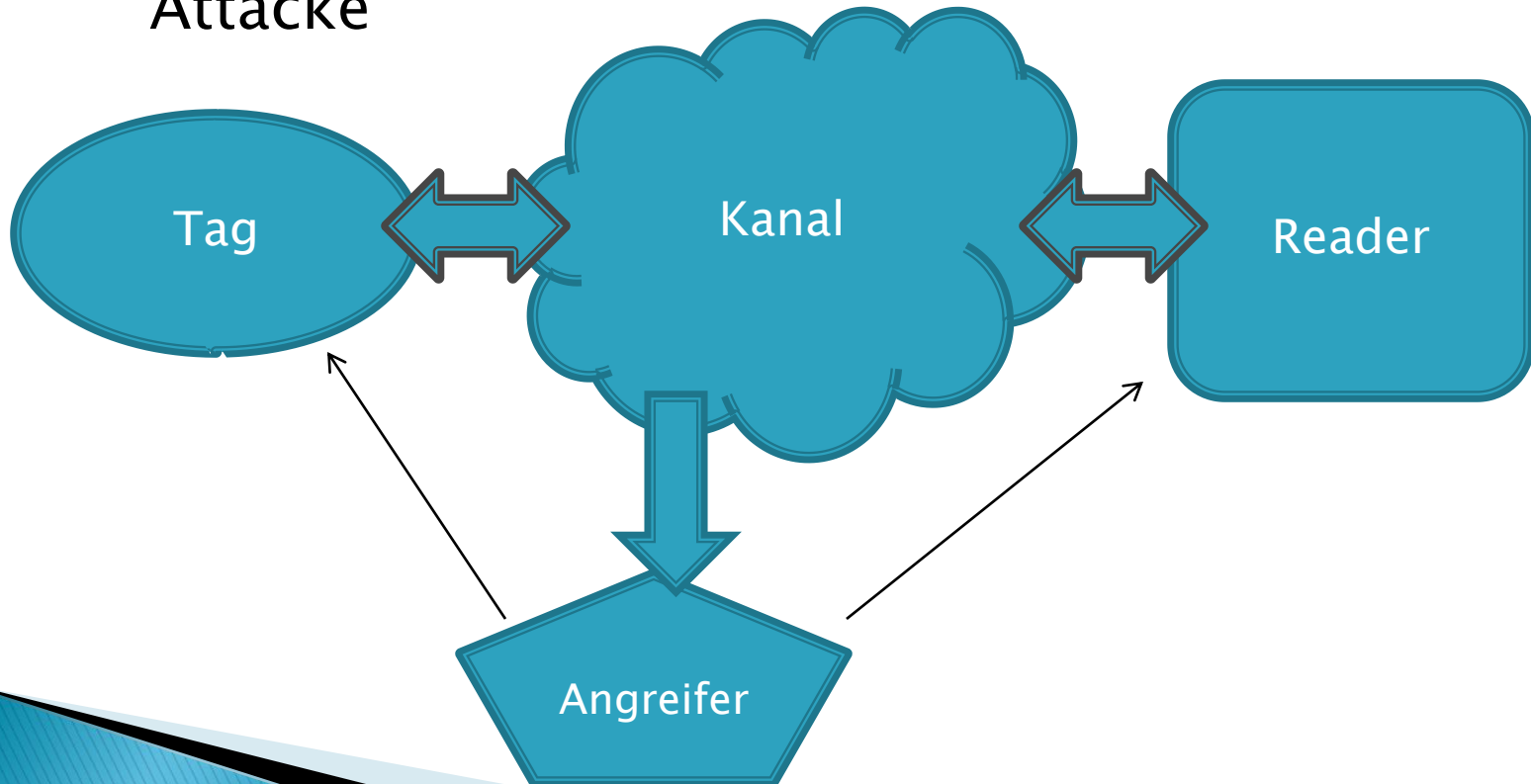
- Eindeutige Tags können verfolgt werden
- Große Massen können überprüft werden
- Die meisten „Angreifer“ sind Firmen



w
w
w
.
b
r
-
o
n
l
i
n
e
.
d
e

10. Replay

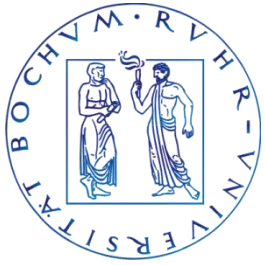
- Erst die Kommunikation mitschreiben
- Die gleiche Kommunikation wird wieder gesendet
- Einfache Attacke
- Challenge und Response Protokolle verhindern die Attacke



11. Relay

- Der Luftkanal wird über den Angreifer geschleift
- Der Reader und das Tag können weit von einander entfernt sein (50 m)
- Man-in-the-Middle Attacke
- Versuche diese Attacke zu verhindern (UWB Ultra Wide Band)
- Tags abschirmen





Fragen???

