RFID Sicherheit

Julian Hoever

24. Juni 2020

Einleitung

- RFID/NFC Technik kommt in vielen alltäglichen Anwendungen vor
  - Kontaktloses Bezahlen
  - Personalausweisen
  - Zeiterfassung mittels RFID Transponder
- Alte aber stetig weiterentwickelte Technik
- Durch die Funktionsweise und das Alter der Technik ergeben sich einige Sicherheitsprobleme

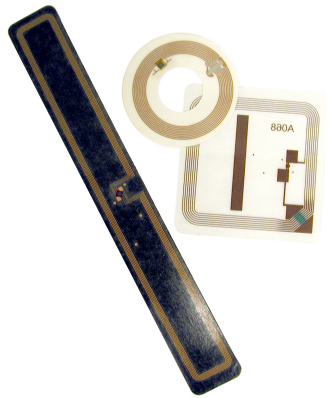


Figure: Verschiedene RFID Transponder [1]

[1] https://upload.wikimedia.org/wikipedia/commons/e/e3/RFID_Tags.jpg

Grundlagen

- Lesegerät liest Daten aus einem Transponder
- Transponder gibt es in vielen Größen und Formen
- Grundlegender Aufbau eines Transponders:
  - Spulenförmige Antenne
  - Schaltkreise zum Senden/Empfangen
  - Speicher
- Aktive/Passive Transponder
  - Aktiver Transponder $\rightarrow$ eigene Spannungsquelle
  - Passiver Transponder $\rightarrow$ keine eigene Spannungsquelle

Grundlegendes Kommunikationsschema

1. Lesegerät induziert Spannung und Taktfrequenz
2. Lesegerät sendet Anfrage an Transponder
3. Transponder übermittelt entsprechende Daten

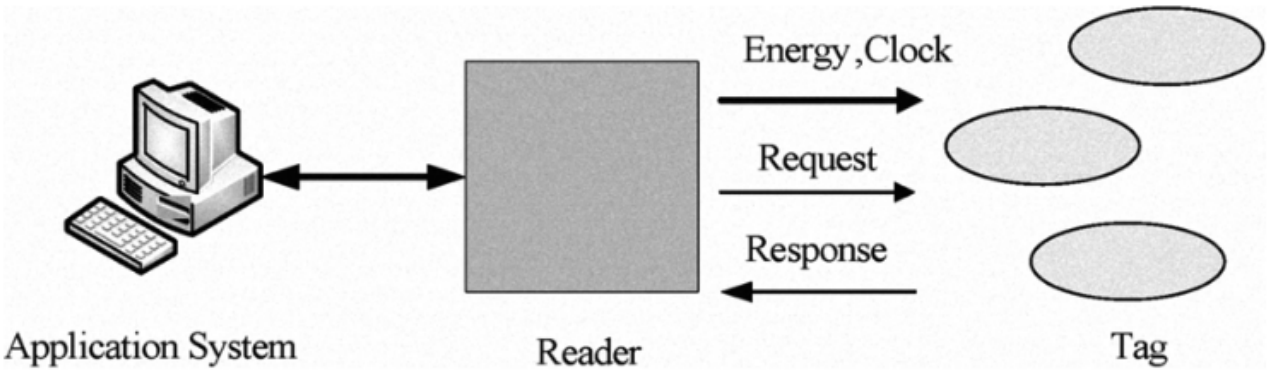


Figure: Kommunikationsschema [2]

[2] Chih-Yung Chen, Chien-Ping Kuo and Fang-Yuan Chien, "An exploration of RFID information security and privacy"

Schwachstellen

- Fehlende Authentifikation
  - Transponder übermittelt Speicherinhalt auf Anfrage
  - Jedes Lesegerät kann den Transponder lesen
- Übertragung im Klartext
  - Ursprünglich Übertragung im Klartext standardisiert
  - Übertragung kann abgehört werden
- Energieversorgung
  - Energieversorgung durch das Lesegerät mittels Induktion
  - Passiver Transponder ist darauf angewiesen

Schwachstellen

- Eindeutige Identifikation
  - Identifizierung durch Speicherinhalt und Identifikationsnummer
- Lesegerät kennt Daten nicht
  - Daten müssen gelesen und verarbeitet werden
  - Bedrohung für Softwareinfrastruktur
- Lesegerät muss Transponder lesen
  - Lesegerät kann nicht entscheiden wie relevant ein Transponder ist ohne ihn zu lesen
  - Lesevorgang belegt Rechenkapazität des Lesegerätes

Angriffe auf Sicherheit und Privatsphäre

- Folgende Schwachstellen werden genauer betrachtet:
  - Fehlende Authentifikation
  - Lesegerät kennt Daten nicht
  - Energieversorgung

Fehlende Authentifikation

- Unbefugte können Transponder lesen
- Kopieren von Transpondern
  - Jedes Lesegerät kann einen Transponder lesen
  - Gelesene Daten können auf neuen Transponder geschrieben werden
  - Daten der Kopie sind identisch mit dem Original
  - Flüchtigen Kontakt mit dem Originaltransponder
- Gefahr für beispielsweise Türsteuerungen

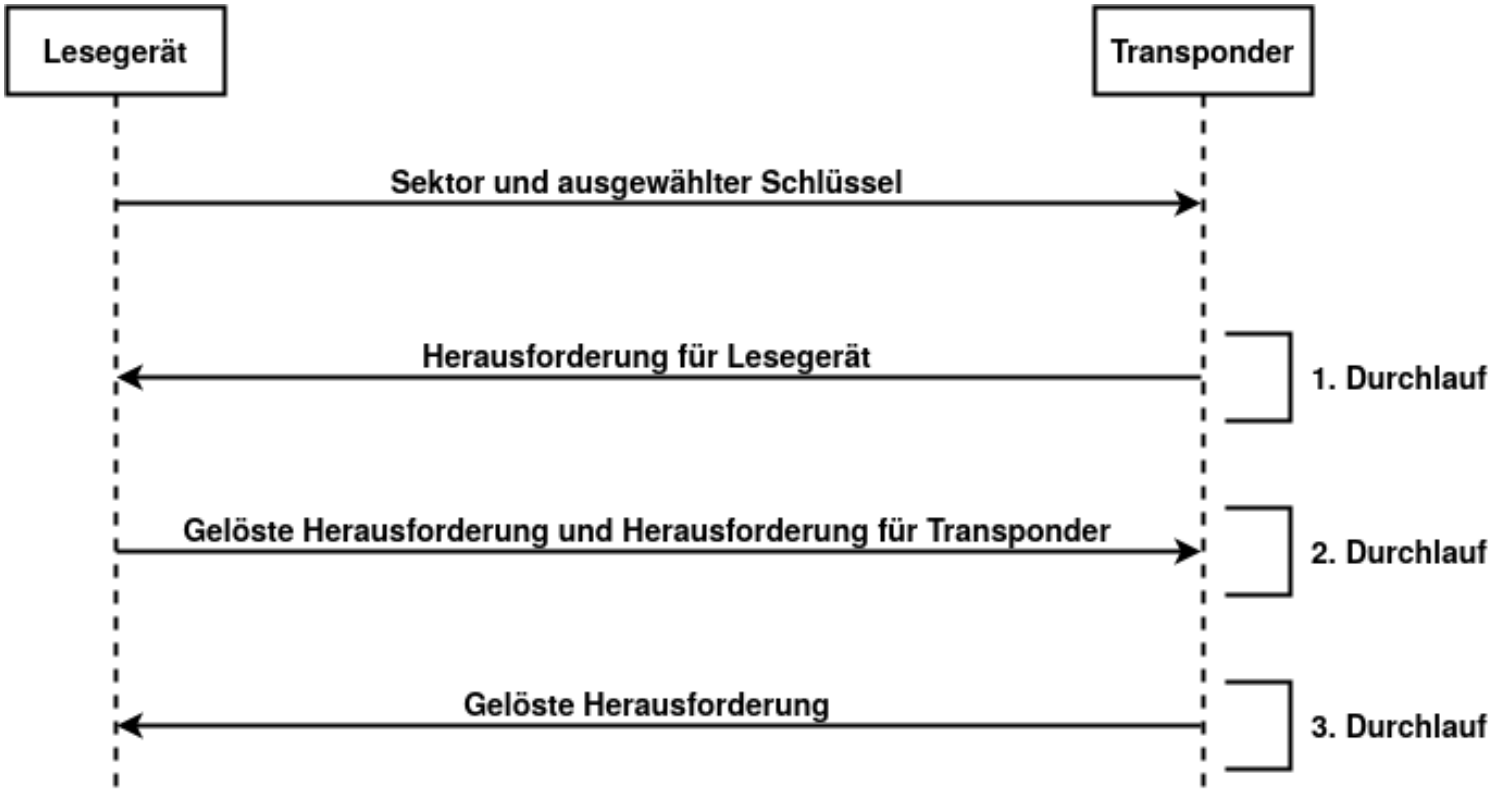
Sicherheitsmaßnahmen

- Verschiedene Ansätze eine Authentifikation zu implementieren
  - Unterscheidung in Sicherheit und Komplexität
- MIFARE Classic EV1 [3]
  - RFID Transponder mit 13.56 MHz Frequenz
  - Speicher in Sektoren aufgeteilt
  - Sektoren unterteilt in 16 Byte Blöcke
  - Jeder Sektor kann separat ausgelesen werden
    - Separate Authentisierung für jeden Sektor
  - Sector Trailer
    - Letzter Block eines Sektors
    - Schlüssel A, Zugriffsbedingungen, Schlüssel B (optional)

[3] https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

Sicherheitsmaßnahmen

- Drei-Phasen-Authentifikation der MIFARE Classic EV1 [4]



[4] https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

Sicherheitsmaßnahmen

- Rechteverwaltung durch Drei-Phasen-Authentifikation
  -

Kompromittieren des Lesegerätes

- Lesegerät liest Speicher des Transponders aus
- Ohne Authentifikation müssen alle Transponder gelesen werden
  - Nicht vertrauenswürdige Transponder
- Schadcode auf Transpondern
  - z.B. SQL Injections
- Daten können Softwareinfrastruktur schaden

Energieversorgung

- Denial of Service Angriff
  - Transponder wird vor elektrischem Feld des Lesegerätes abgeschirmt
  - Energieversorgung wird unterbunden
  - Lesegerät erkennt den Transponder nicht
  - Faradayscher Käfig
- Problem bei der Warensicherung mittels RFID

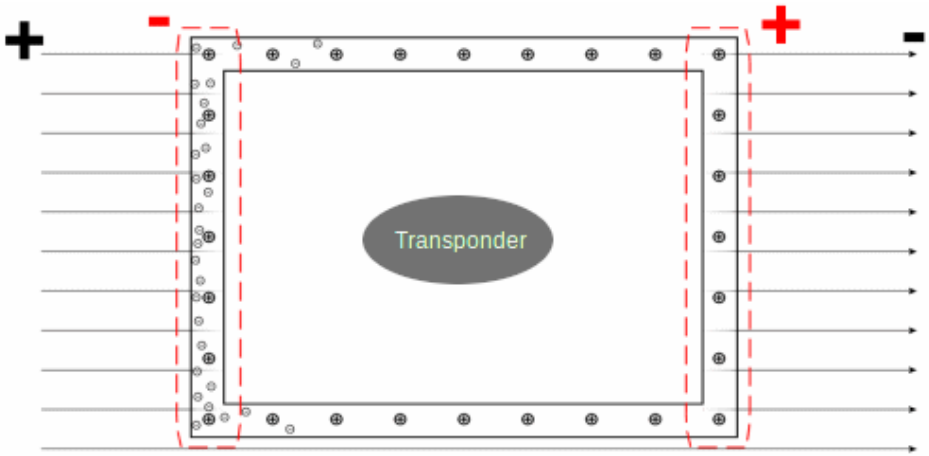


Figure: Transponder im Faradayschen Käfig [5]

[5] https://commons.wikimedia.org/wiki/File:Faraday_cage.gif#/media/Datei:Faraday_cage.gif

Sicherheitsmaßnahmen