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

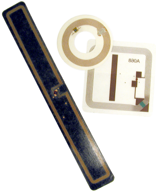

Figure: Verschiedene RFID Transponder [1]

---

[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 → eigene Spannungsquelle
  - Passiver Transponder → keine eigene Spannungsquelle

Grundlegendes Kommunikationsschema

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

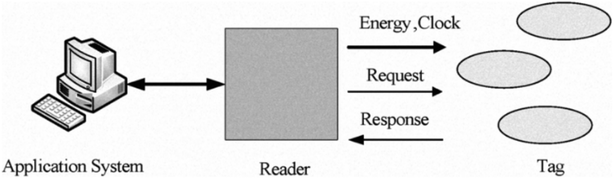

Figure: Kommunikationsschema [2]

---

[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
  - Speicherinhalt kann Schadcode enthalten
  - z.B.: SQL Injections
  - 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