

RFID Sicherheit

Julian Hoever

24. Juni 2020

- RFID 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

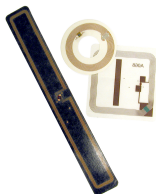


Figure: Verschiedene RFID Transponder ¹

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

- 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

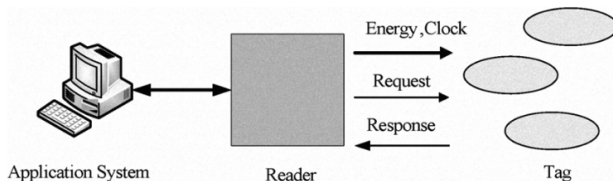


Figure: Kommunikationsschema ²

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

- 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

- Eindeutige Identifikation
 - Identifizierung durch Speicherinhalt und Identifikationsnummer
 - Ermöglicht Tracking
- 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

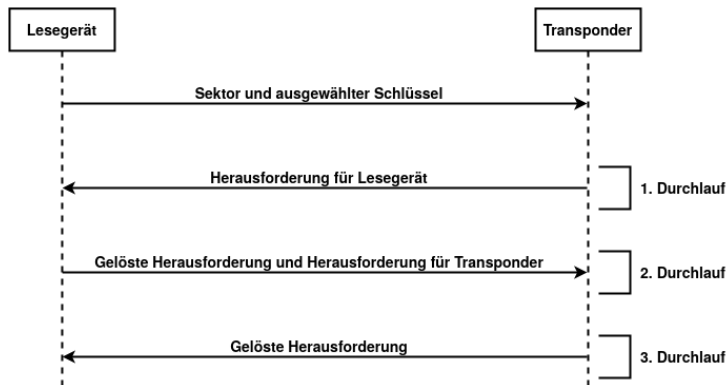
- Folgende Schwachstellen werden genauer betrachtet:
 - Fehlende Authentifikation
 - Energieversorgung

- Unbefugte können Transponder lesen
- Kopieren von Transpondern
 - Gelesene Daten können auf neuen Transponder geschrieben werden
 - Flüchtigen Kontakt mit dem Originaltransponder
 - Daten der Kopie sind identisch mit dem Original
- Gefahr für beispielsweise Türsteuerungen
- Persönliche Daten könnten aus dem Transponder gelesen werden

- 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)

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

- Drei-Phasen-Authentifikation der MIFARE Classic EV1 ⁴



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

- Rechteverwaltung durch Drei-Phasen-Authentifikation
 - Separate Schlüssel für jeden Sektor
 - Lesegerät kann nur Sektoren lesen für das es den Schlüssel besitzt
- Schutz vor Vervielfältigung und unberechtigtem Zugriff
- Leistungsfähiger Transponder benötigt
- Alternatives Authentifikationsverfahren
 - Einfaches Passwort
 - Kommunikationspartner tauschen Passwort zu Beginn aus
 - Problem: Übertragung im Klartext

- Kopieren und Auslesen sehr leicht durchführbar
 - Kurzer Kontakt
 - Unbeaufsichtigte Brieftasche, Schlüsselbund, etc.
- Heutzutage wirkungsvolle Authentifizierungsmaßnahmen
- Transponder ohne Authentifizierung sind ein erhebliches Sicherheitsrisiko
- Sicherheitsanforderungen hängen von Anwendung ab

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

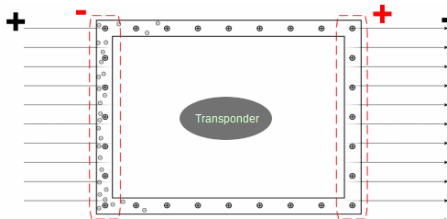


Figure: Transponder im Faradayschen Käfig ⁵

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

- Transponder sind abhängig von elektrischem Feld
- Transponder für das Lesegerät nicht existent
- Schwachstelle kann nicht ohne weiteres behoben werden
- Zusätzliche Maßnahmen je nach Anwendung:
 - Videoüberwachung
 - Ladendetektiv
 - ...

- Denial of Service Angriffe auf Transponder sind sehr leicht durchführbar
- RFID blockierende Beutel (\Rightarrow Faradayscher Käfig)
- Hohes Schadenspotenzial
 - z.B. Diebstahlsicherungen im Einzelhandel

- RFID bietet viele Möglichkeiten
 - Kontaktloses Bezahlen, Diebstahlsicherung, Kontaktlose Zugangskontrollen, etc...
- Schwachstellen beachten
- Sicherheit an die jeweiligen Anforderungen anpassen
- Privatsphäre der Nutzer beachten