RFID Sicherheit

Julian Hoever

24. Juni 2020

Julian Hoever RFID Sicherheit 24. Juni 2020 1/16

Einleitung

- 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

Julian Hoever RFID Sicherheit 24. Juni 2020 2 / 16

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
 - $\bullet \ \, \mathsf{Aktiver} \ \, \mathsf{Transponder} \to \mathsf{eigene} \ \, \mathsf{Spannungsquelle}$
 - $\bullet \ \, \mathsf{Passiver} \ \, \mathsf{Transponder} \to \mathsf{keine} \ \, \mathsf{eigene} \ \, \mathsf{Spannungsquelle}$

3 / 16

Julian Hoever RFID Sicherheit 24. Juni 2020

Grundlegendes Kommunikationsschema

- Lesegerät induziert Spannung und Taktfrequenz
- 2 Lesegerät sendet Anfrage an Transponder
- Transponder übermittelt entsprechende Daten

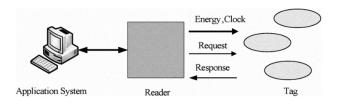


Figure: Kommunikationsschema ²

Julian Hoever RFID Sicherheit 24. Juni 2020 4 / 16

²Chih-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
 - 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

Julian Hoever RFID Sicherheit 24. Juni 2020 6 / 16

Angriffe auf Sicherheit und Privatsphäre

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

Julian Hoever RFID Sicherheit 24. Juni 2020 7/16

Fehlende Authentifikation

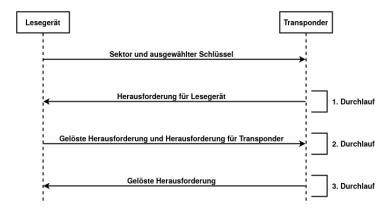
- Unbefugte können Transponder lesen
- Kopieren von Transpondern
 - Jedes Lesegerät kann einen Transponder lesen
 - Gelesene Daten können auf neuen Transponder geschrieben werden
 - Daten der Kopie sind identisch mit dem Original
 - Flüchtigen Kontakt mit dem Originaltransponder
- Gefahr für beispielsweise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

Julian Hoever RFID Sicherheit 24. Juni 2020 8 / 16

- Verschiedene Ansätze eine Authentifikation zu implementieren
 - Unterscheidung in Sicherheit und Komplexität
- MIFARE Classic EV1³
 - 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)

Julian Hoever RFID Sicherheit 24. Juni 2020 9/16

Drei-Phasen-Authentifikation der MIFARE Classic EV1



Julian HoeverRFID Sicherheit24. Juni 202010 / 16

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

11 / 16

Durchführbarkeit

- 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

Julian Hoever RFID Sicherheit 24, Juni 2020 12 / 16

Energieversorgung

- 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

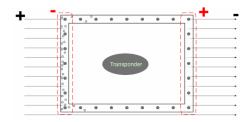


Figure: Transponder im Faradayschen Käfig ⁵

Julian Hoever RFID Sicherheit 24. Juni 2020 13 / 16

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

Durchführbarkeit

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

Julian Hoever RFID Sicherheit 24. Juni 2020 15 / 16

Fazit

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

Julian Hoever RFID Sicherheit 24. Juni 2020 16 / 16