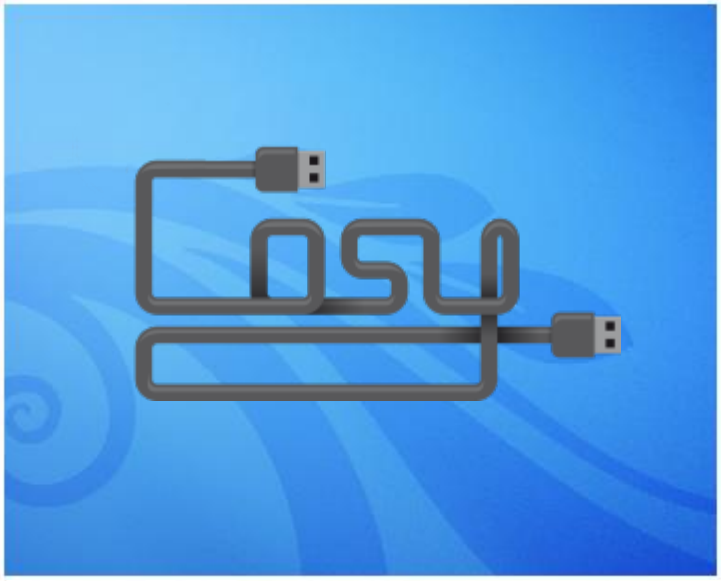


Wissenschaftliche Arbeitstechniken und Präsentation

18.1.2013
Wintersemester 2012

RFID-Sicherheitsrisiken, Angriffsmethoden und Abwehr

RFID-Security

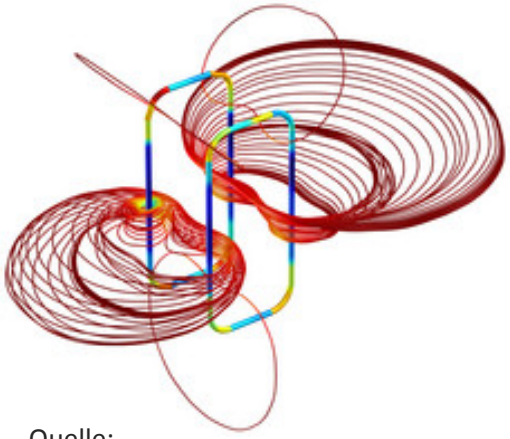
Fachbereich für Computerwissenschaften
Paris-Lodron-Universität Salzburg

Inhalt

- Einleitung
  - Begriffsdefinition und Systemübersicht
  - RFID-Kommunikationsarchitektur
- Physikalische Grundlagen
  - Energieversorgung des Tag
  - Datenübertragung Tag <-> Leser
- Sicherheitsrisiken in RFID-Systemen
  - Risiken im Unternehmensumfeld
  - Risiken in der privaten Nutzung
- Angriffe und Abwehrmechanismen bei RFID Systemen
- Zusammenfassung

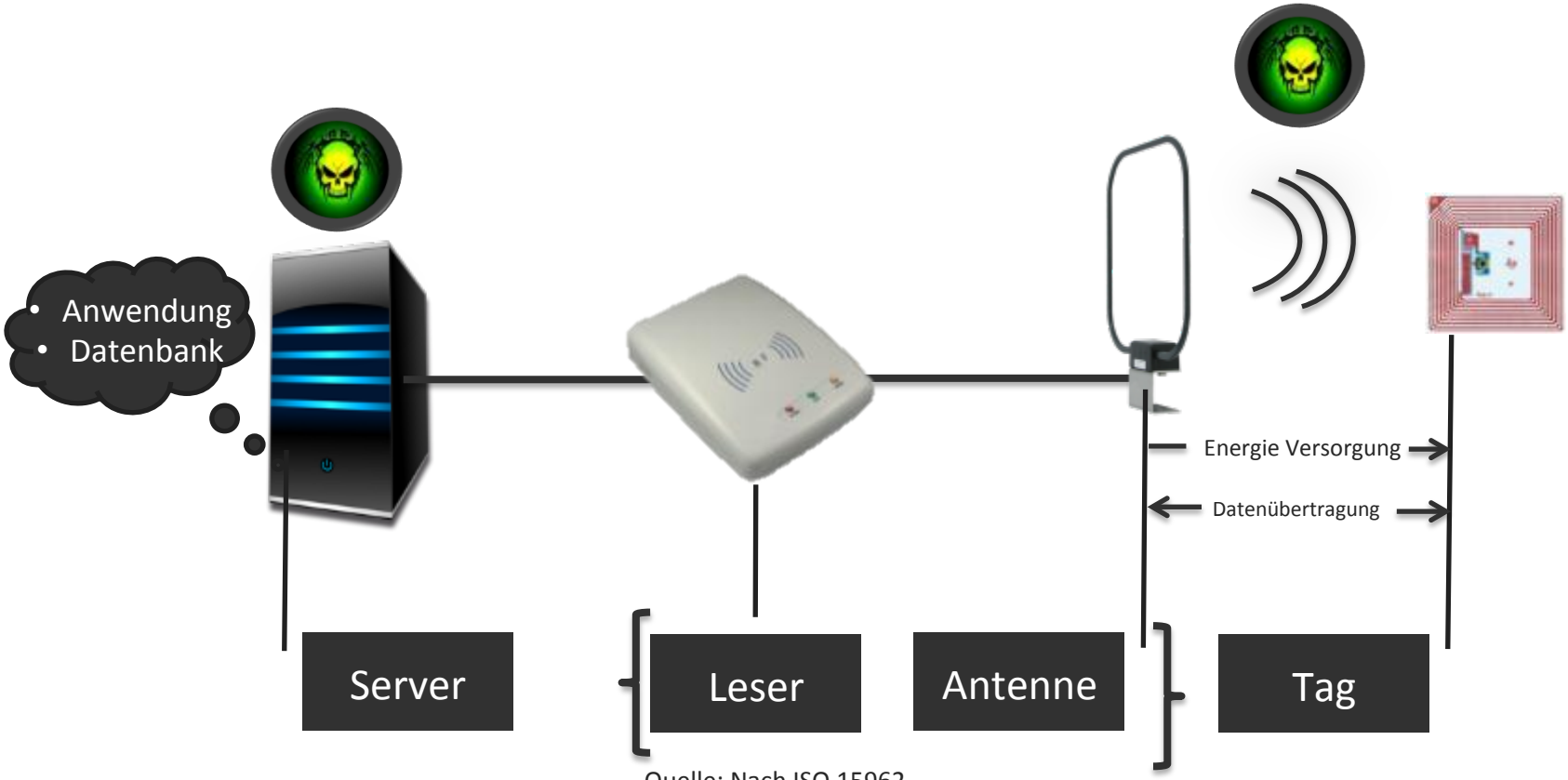
Begriffsdefinition

- RFID -> „radio-frequency identification“
  - Identifizierung / Lokalisierung von Objekten über Funk
  - Nutzt unterschiedliche Frequenzen
    - 123kHz
    - 13,56MHz
    - 433MHz
    - 900MHz
    - 2.4GHz
  - Problem Funk -> „gemeinsames Übertragungsmedium“



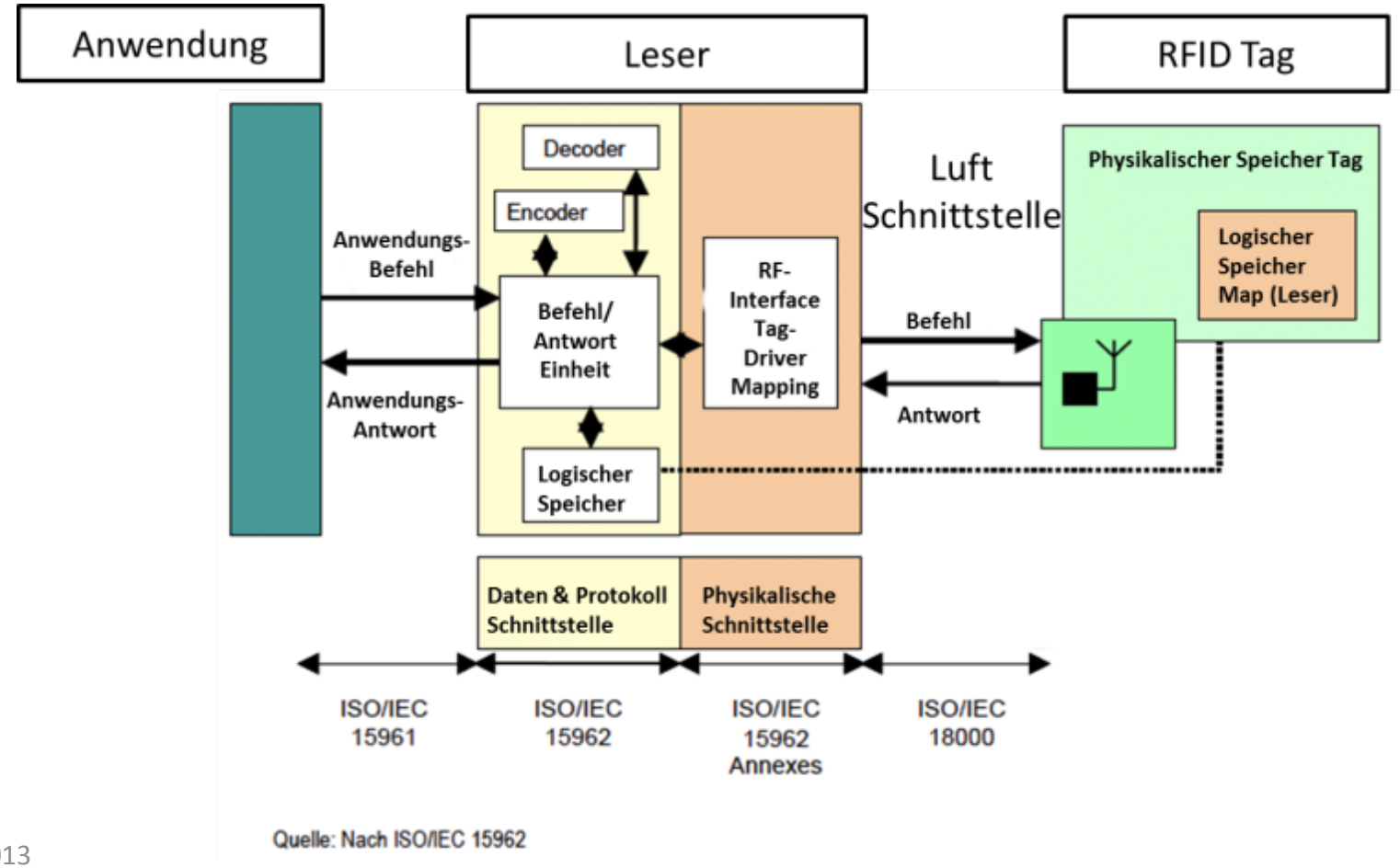
Quelle:
© COMSOL http://www.comsol.com/

Systemübersicht



Quelle: Nach ISO 15962

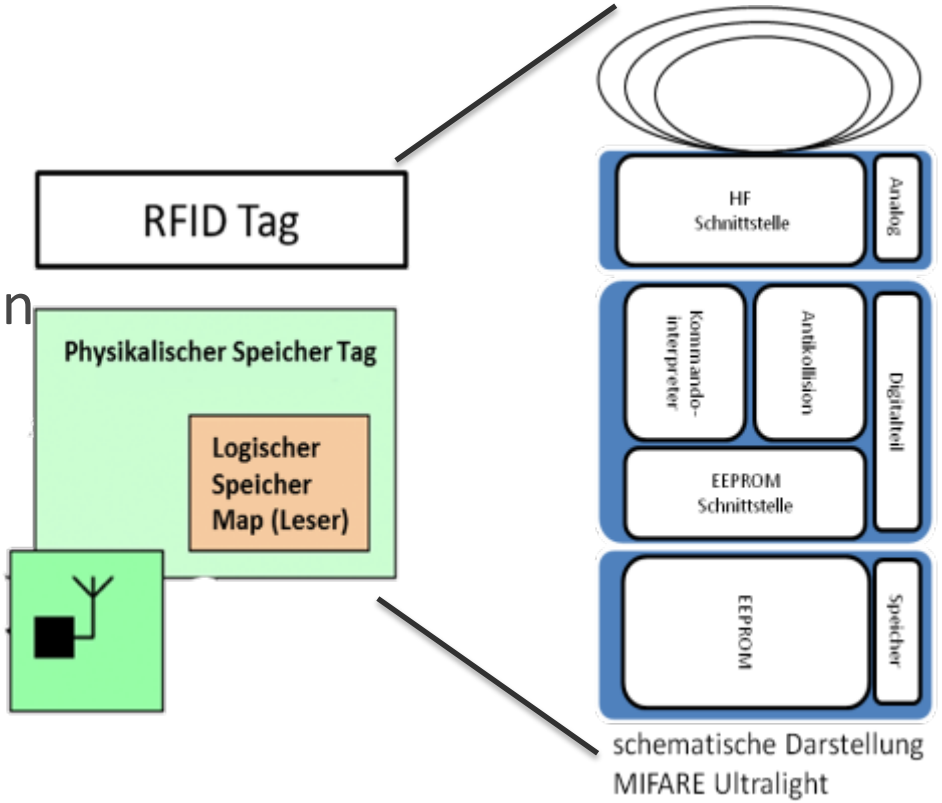
RFID Implementierung nach ISO



Quelle: Nach ISO/IEC 15962

RFID-Tag

- Aktiv oder passiv
- Datenträger mit verschiedenen Zugriffsmöglichkeiten
- Sicherheitsmechanismen
- Verschlüsselung
- Kommunikation über Luftschnittstelle



schematische Darstellung MIFARE Ultralight

RFID-Leser

- Physikalische Einheit
  - RF Interface
  - Endstufe
  - Bit Codierung
  - Tag Driver
  - Mapping Tag-Daten Anwendungs-Daten
- Digital Einheit
  - Protokoll Steuerung
  - Speichern laut Mapping Regeln
- Schnittstellen
  - Luftschnittstelle ISO 18000
  - Anwendungsschnittstelle ISO 15961

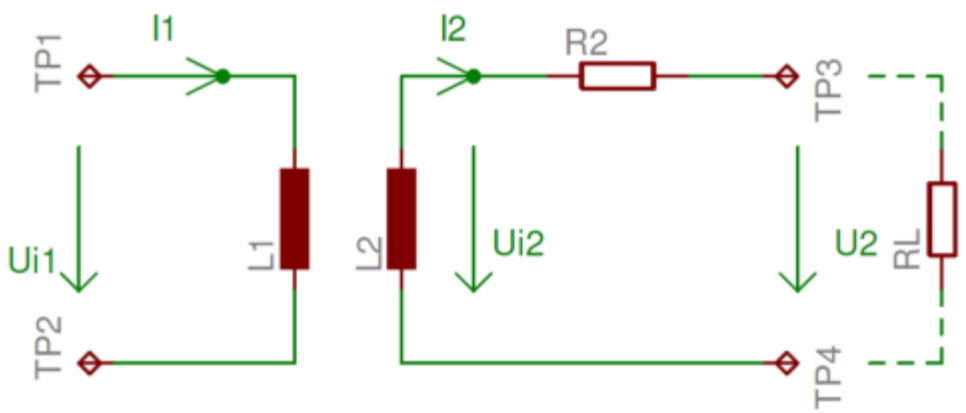
Quelle: Nach ISO 15962

Anwendung

- Verarbeitung der Tag-Daten
- Verschlüsselung
- Datenbank (Serial only)
- Keine Kenntnis über Schnittstelle zum Tag -> Abstraktion
- Möglicher Angriffspunkt

Prinzip

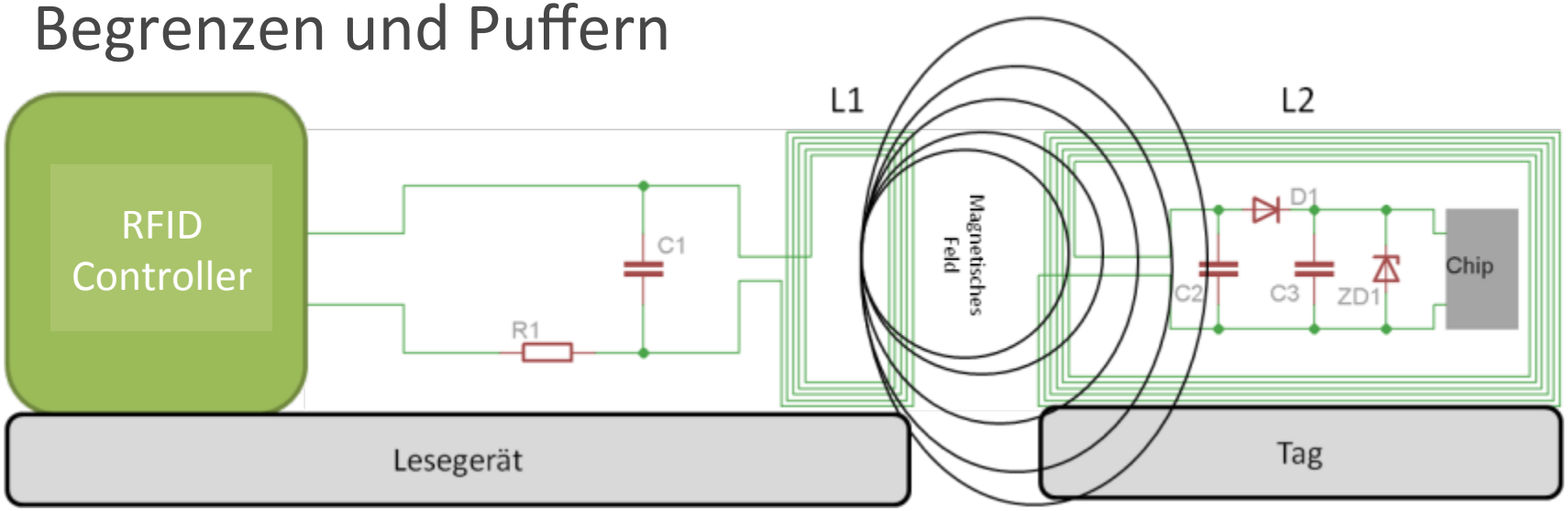
- Induktive Kopplung
- Nahfeld (d<<L)-> Magnetisches Wechselfeld (13,56MHz, 123kHz)
- Induktionsgesetz



Quelle: Nach Finkenzeller, Klaus, *RFID-Handbuch*

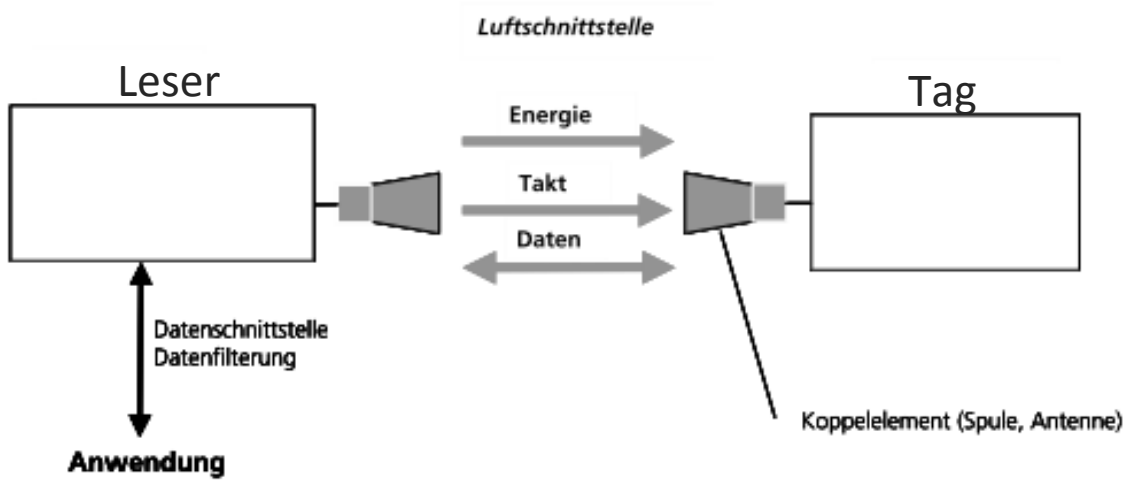
Energieversorgung des Tags

- Schwingkreis -> Resonanzüberhöhung (Spannung)
- Gleichrichten
- Begrenzen und Puffern



Quelle: Nach Finkenzeller, Klaus, *RFID-Handbuch*

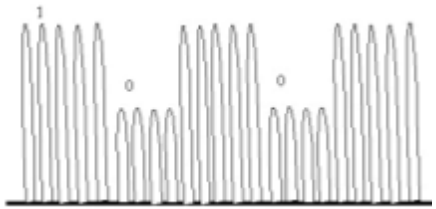
Übersicht: Datenübertragung

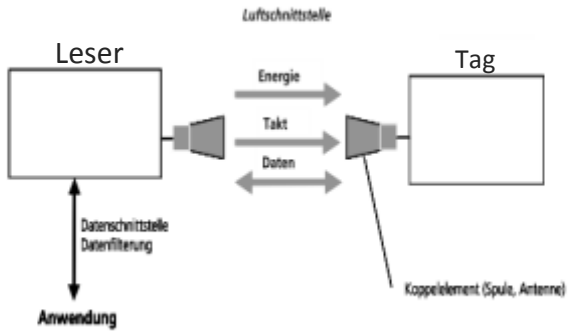


Quelle: Nach Finkenzeller, Klaus, *RFID-Handbuch*

Datenübertragung vom Leser zum Tag

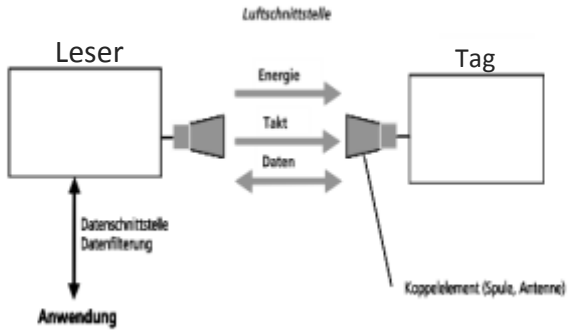
- Leser stellt Energieversorgung für Tag zur Verfügung
- Gibt den Takt vor -> Trägerfrequenz -> Resonanzfrequenz des Tags
- Kollisionserkennung
- Überträgt Befehle/Daten via AM des Trägersignals (<100%)





Datenübertragung vom Tag zum Leser

- Puffert Energie aus dem Feld des Lesers
- Optional Kollisionsvermeidung
- Überträgt Daten mittels passiver Lastmodulation
  - „Kurzschluss“ -> entnimmt dem Feld Energie
  - Rückwirkung auf Sendespule Impetanztransformation
  - AM
- U(Daten) << U(Träger) [~<10^4]

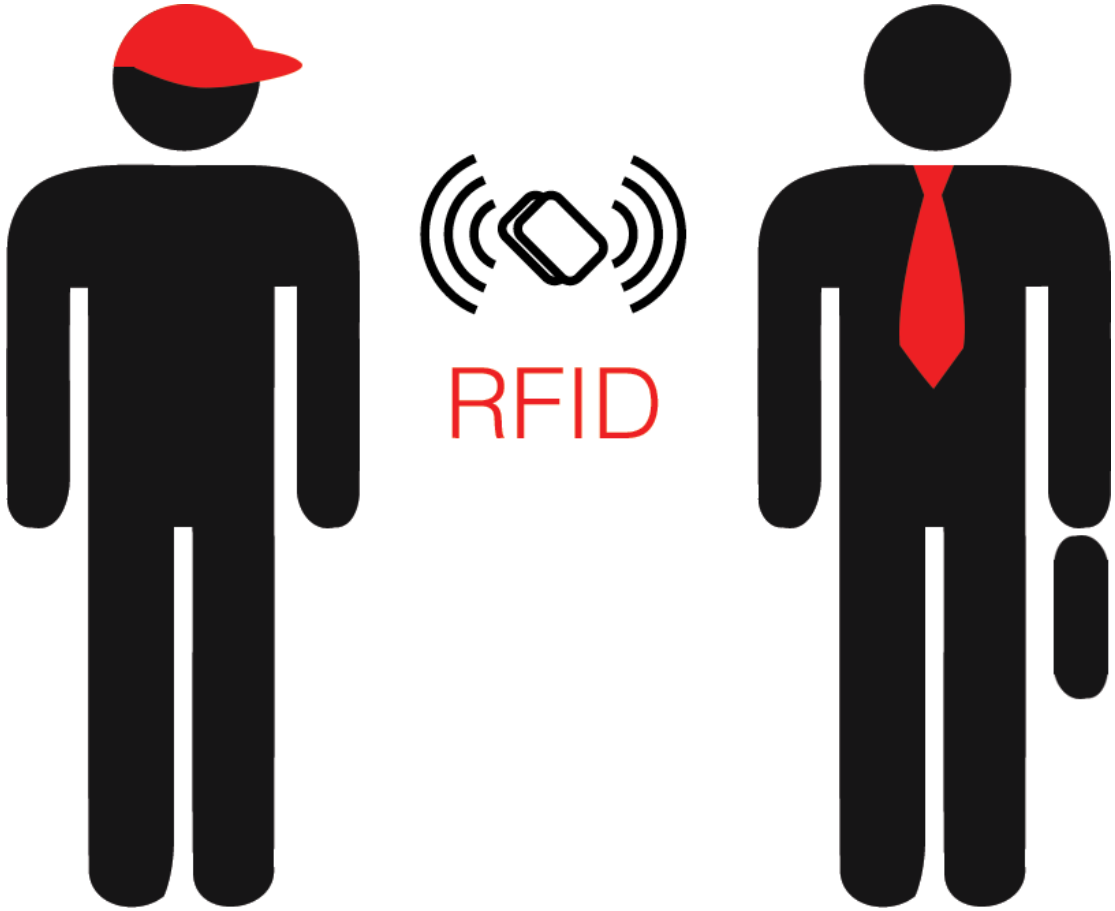


Quelle: Nach Finkenzeller, Klaus, *RFID-Handbuch*

Fazit

- P(Rückkanal) << als P(Trägersignals)
- Abhören des Sender viel einfacher als Abhören des Tags
- Energiedichte nimmt mit d^4 ab- > Sicherheitsfaktor Abstand

Sicherheitsrisiken



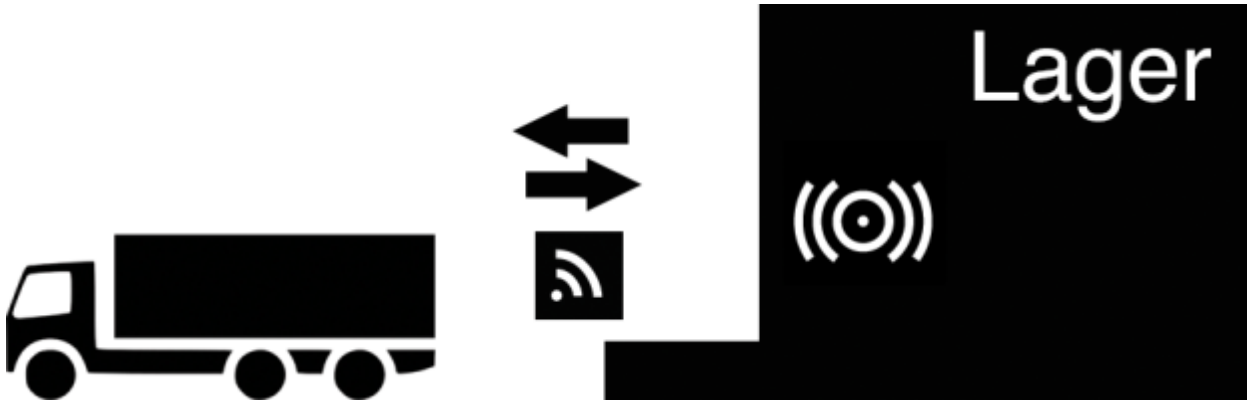
Risiken im Unternehmensumfeld

- Spionage Bedrohung
- Marketing Bedrohung
- Infrastruktur Bedrohung
- Umfang Bedrohung

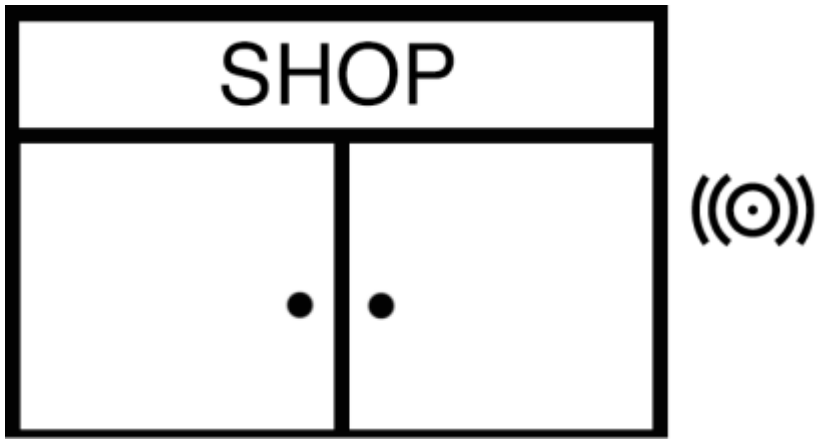
Risiken in der privaten Nutzung

- Aktion Bedrohung
- Assoziation Bedrohung
- Lage Bedrohung
- Vorliebe Bedrohung
- Konstellation Bedrohung
- Transaktion Bedrohung
- Brotkrümel Bedrohung

Geschäftliche Risiken: Spionage

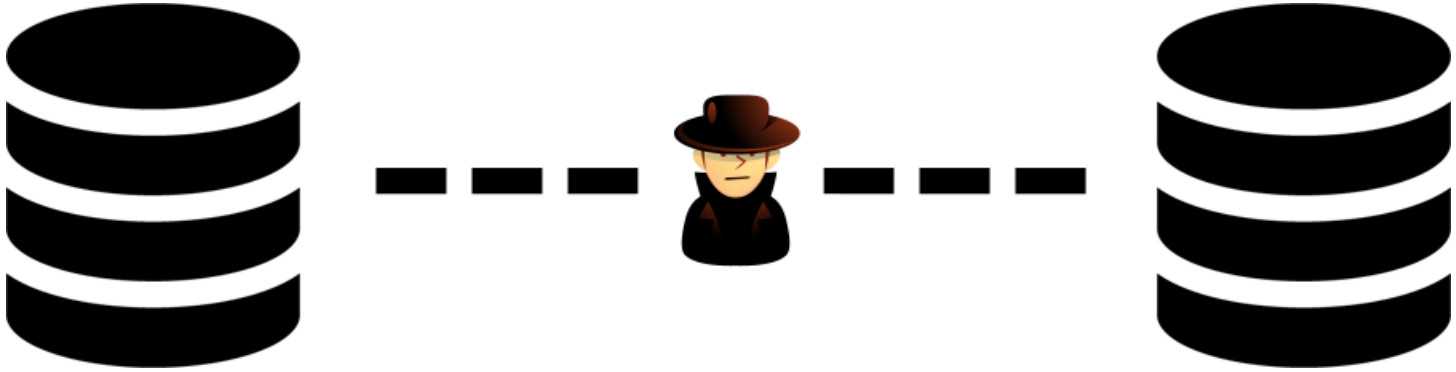


Competitive Marketing Bedrohung

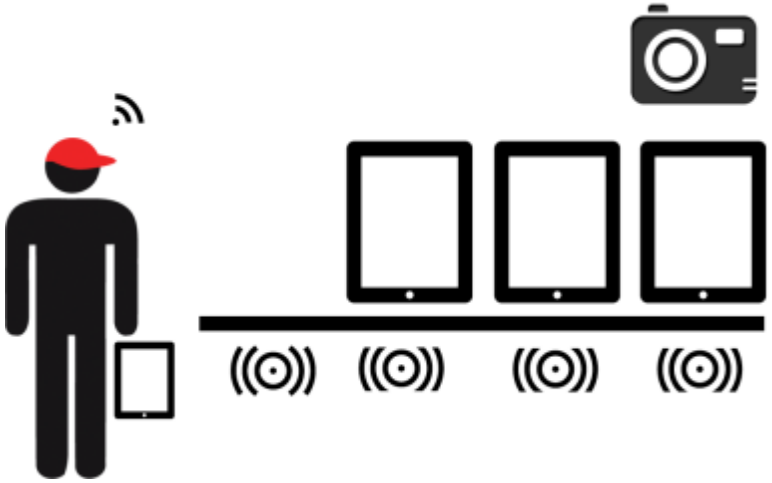


Geschäftliche Risiken: Infrastruktur

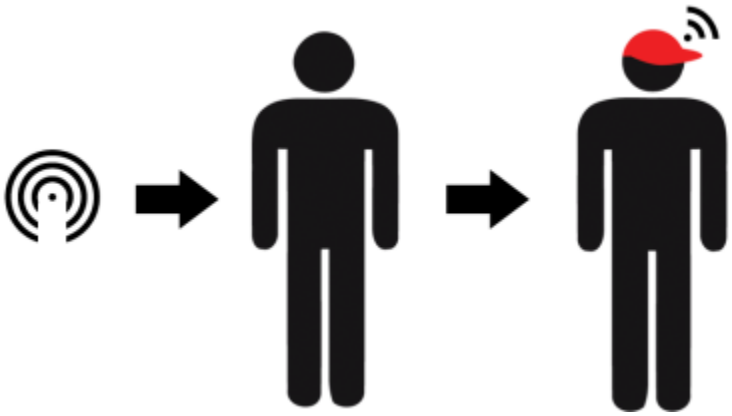
Umfang Bedrohung



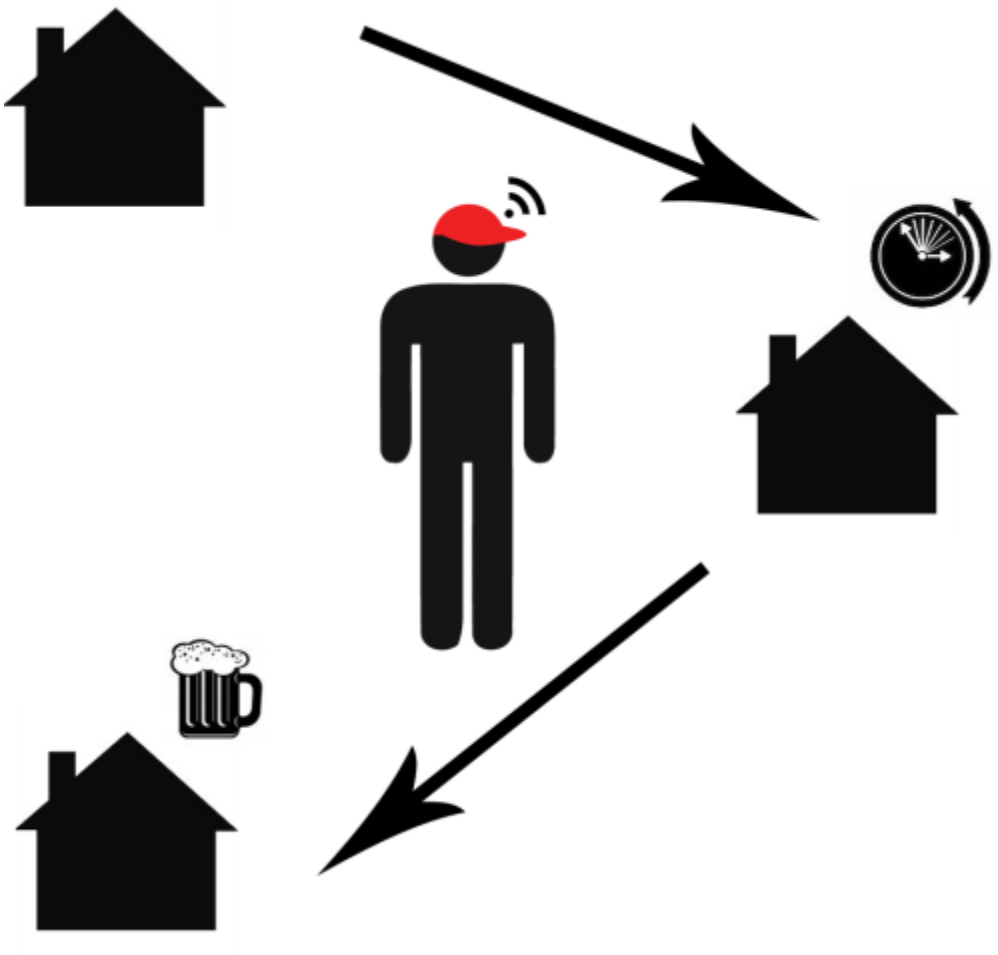
Aktion



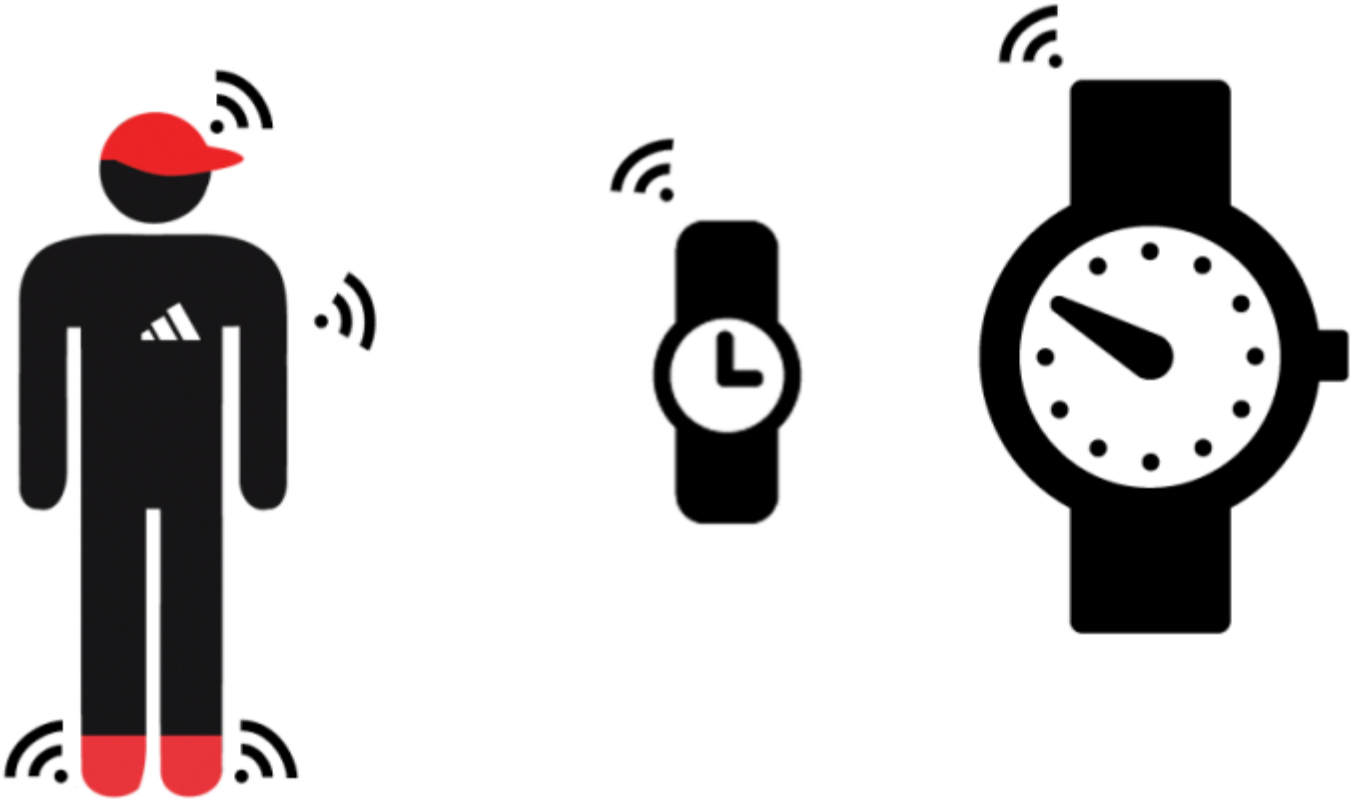
Assoziation



Lage

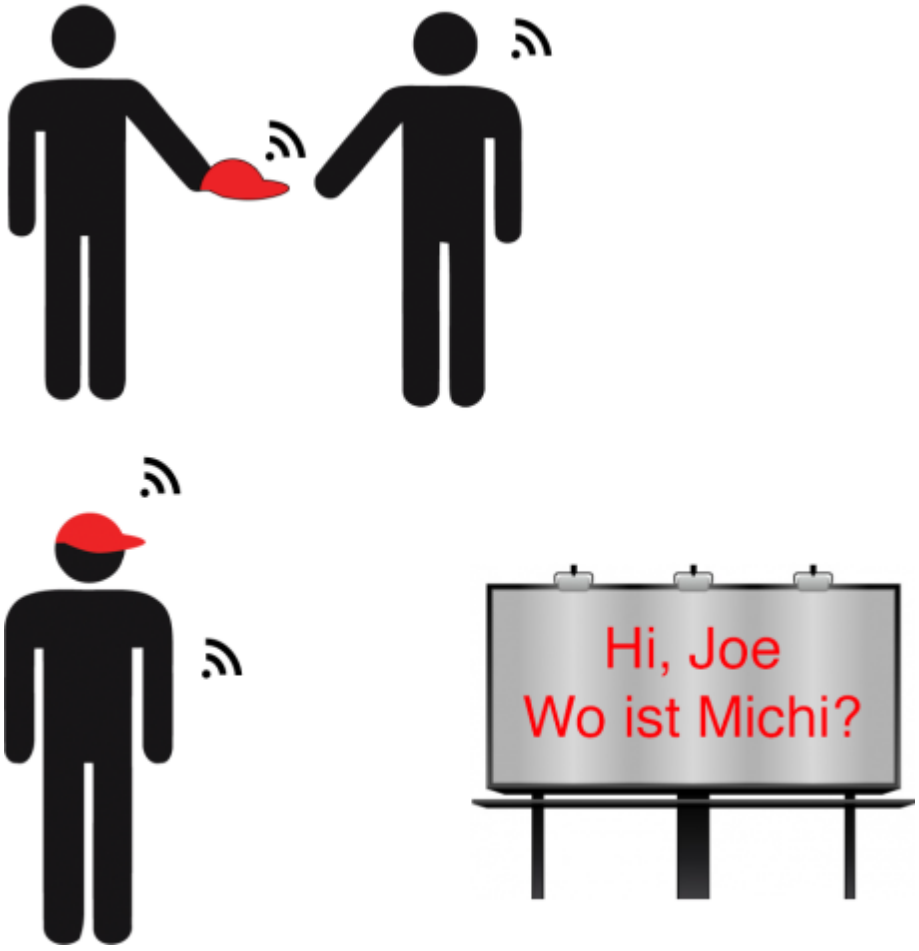


Vorliebe

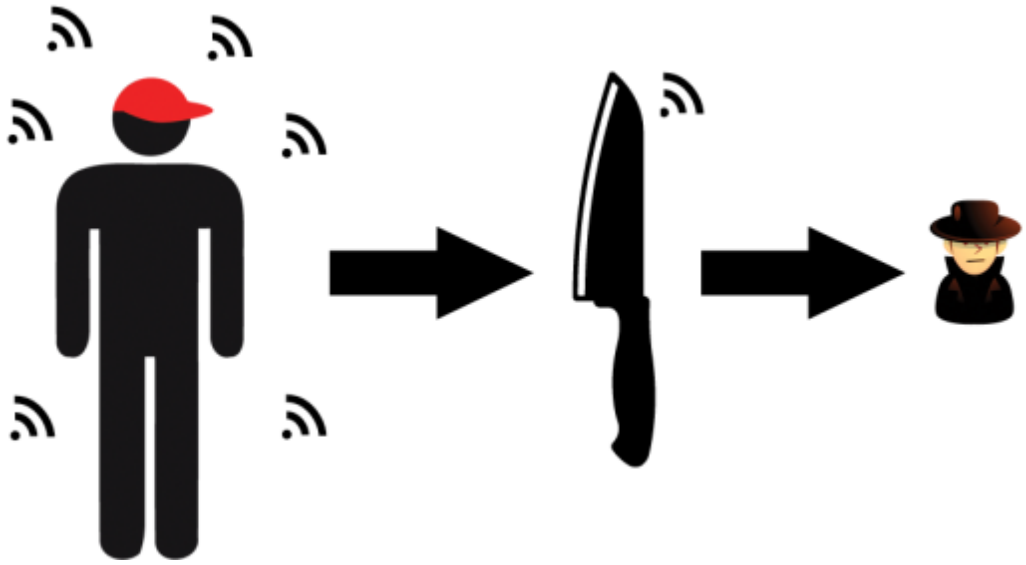


Konstellation

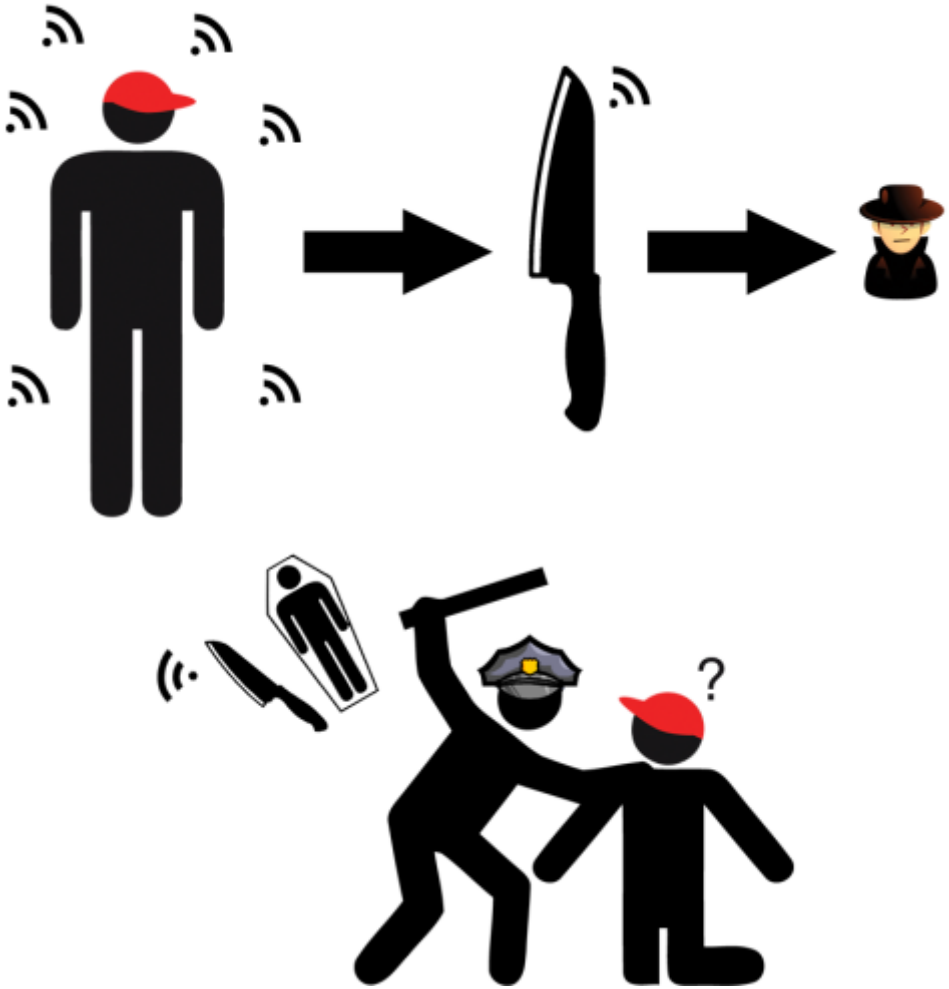
Transaktion



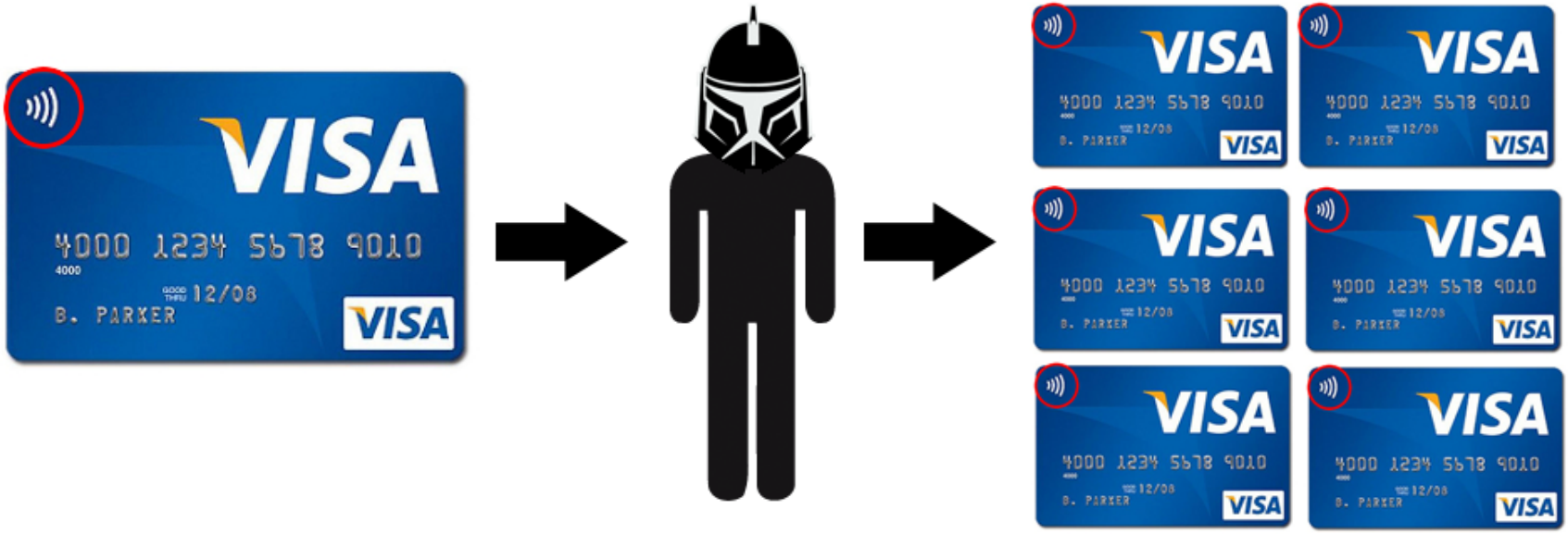
Brotkrümel



Brotkrümel



Klonen



Bonus


File system
EF.COM
Data Group Presence Map
EF.DG1
Machine-readable Zone Data
EF.DG2
Encoded Identification Feature: Face
EF.DG3
Encoded Identification Feature: Finger Prints
EF.DG11
Additional Personal Details
EF.DG12
Additional Document Details
EF.DG14
Security Options for Secondary Biometrics
EF.SOD
Document Security Object

Angriffsmethoden

- Sniffing
- Spoofing und Replay-Attacken
- Man-in-the-Middle-Attacken
- Cloning und Emulation
- Denial of Service

Angriffsmethoden Fortsetzung

- RFID-Malware
- Relay-Angriffe
- Tracking

Relay Angriff

Denial of Service Attacke

- Ziel: Stören oder unbrauchbar machen
- Einsatz eines Störsenders
- Mechanische Abschirmung
- Kill-Kommando

- RFID-Malware
  - Buffer-Overflow-Atacke
  - SQL-Injetion-Angriffe

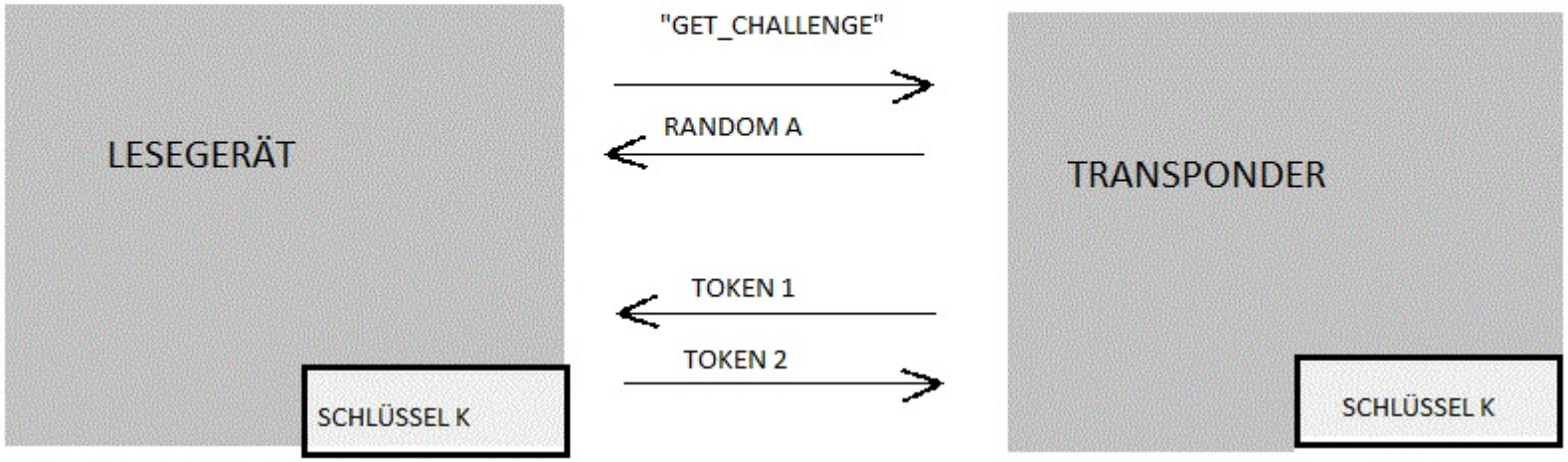
Abwehrmechanismen

- Kryptographische Maßnahmen
  - Gegenseitige symmetrische Authentifizierung
  - Authentifizierung mit Abgeleiteten Schlüssel
  - Streamcipher

- Lesereichweite begrenzen

Abwehrmechanismen Fortsetzung

- Gegenseitige symmetrische Authentifizierung



Fragen

Referenzen:

1. Finkenzeller, Klaus. *RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder, kontaktlosen Chipkarten und NFC*. 5 München: Hanser, 2008.
2. Garfinkel, Simson L., Juels, Ari and Pappu, Ravikanth. "RFID Privacy: An Overview of Problems and Proposed Solutions.." *IEEE Security & Privacy* 3 , no. 3 (2005): 34-43.
3. Waldmann, Ulrich, Hollstein, Thomas and Sohr, Karsten RFID-Studie 2007: Technologieintegrierte Datensicherheit bei RFID-Systemen. , Fraunhofer-Institut f{\"u}r Sichere Informations-Technologie (SIT), Darmstadt (2007).
4. Kim, Jung-Tae. "Comparison of Attacks and Security Analyses for Different RFID Protocols.." Paper presented at the meeting of the ICITCS, 2012.
5. Defend, Benessa, Fu, Kevin and Juels, Ari. "Cryptanalysis of Two Lightweight RFID Authentication Schemes.." Paper presented at the meeting of the PerCom Workshops, 2007.
6. Moessner, Markus B. and Khan, Gul N.. "Secure authentication scheme for passive C1G2 RFID tags.." *Computer Networks* 56 , no. 1 (2012): 273-286.

Vielen Danke für Ihre Aufmerksamkeit