TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik, Institut für Technische Informatik, Professur VLSI-Entwurfssysteme, Diagnostik und Architektur

RFID – Sicherheit

Dresden, 30.06.2010

Stephan Richter

s3300266@mail.zih.tu-dresden.de

Gliederung

Grundlagen

- 01 Einführung
- 02 Unterscheidungsmerkmale
- 03 Akteuere
- 04 Einsatzgebiete

Angriffsmethoden, Sicherheit, Datenschutz...

- 05 Angriffsmethoden
- 06 Sicherheitsanforderungen und Maßnahmen
- 07 Bedrohungen
- 08 Beispiel Risiken
- 09 Zusammenfassung

Grundlagen

- 01 Einführung
- 02 Unterscheidungsmerkmale
- 03 Akteuere
- 04 Einsatzgebiete

01 Einführung (1)

RFID:

- **R**adio **F**requency **ID**entification
- Technologie zur Identifizierung mit Hilfe von elektromagnetischen Wellen.
- System besteht aus Transponder und Lesegerät

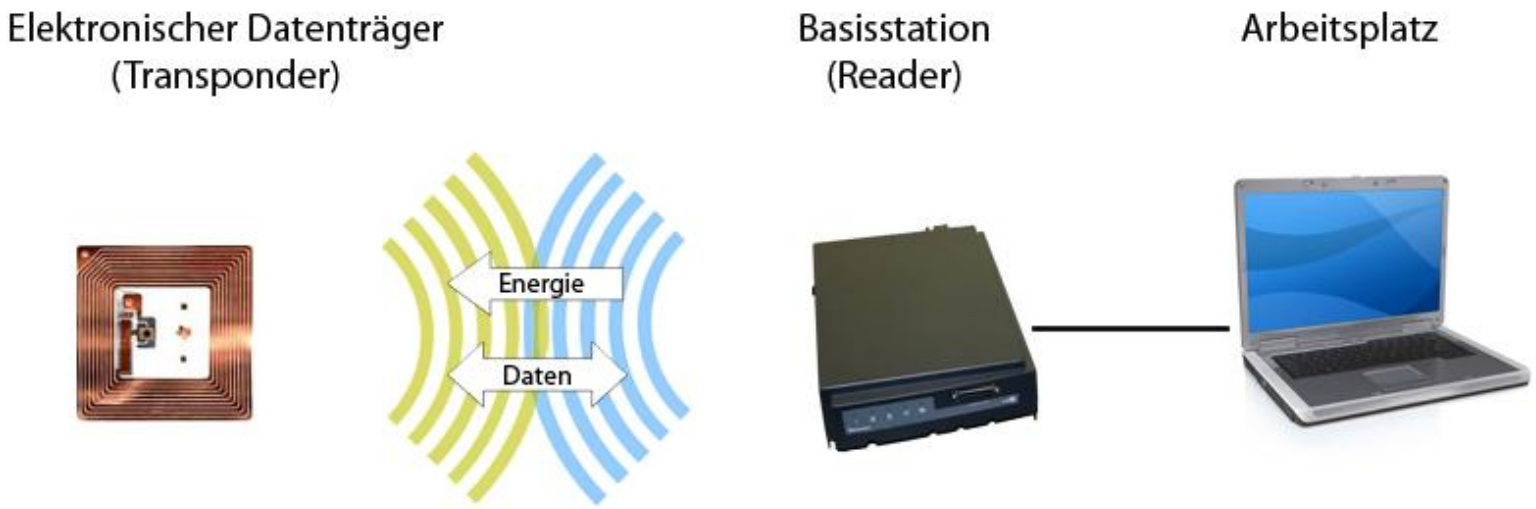
Lesegerät:

- Erzeugt durch eine Induktionsspule ein elektromagnetischem Feld, um mit einem Transponder zu kommunizieren

Transponder:

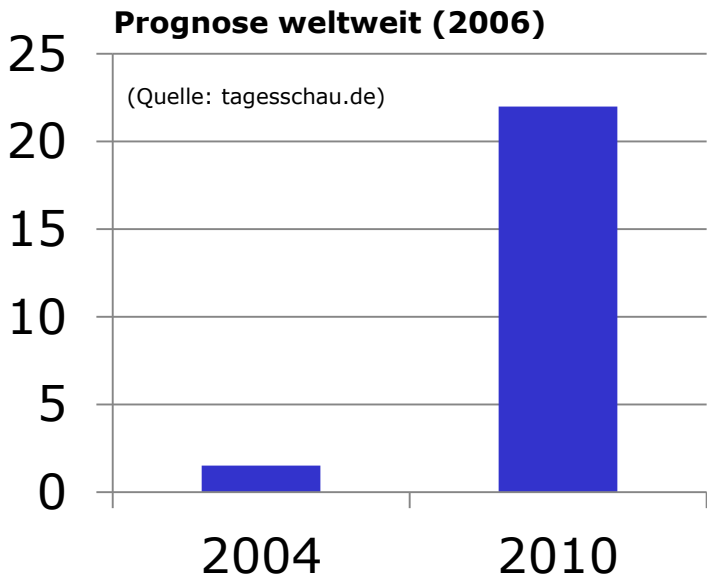
- Chip mit Datenspeicher, der mit Basisstation kommuniziert
- Passiv oder aktiv
- Oft Bezeichnet als RFID-Tag oder RFID-Chip

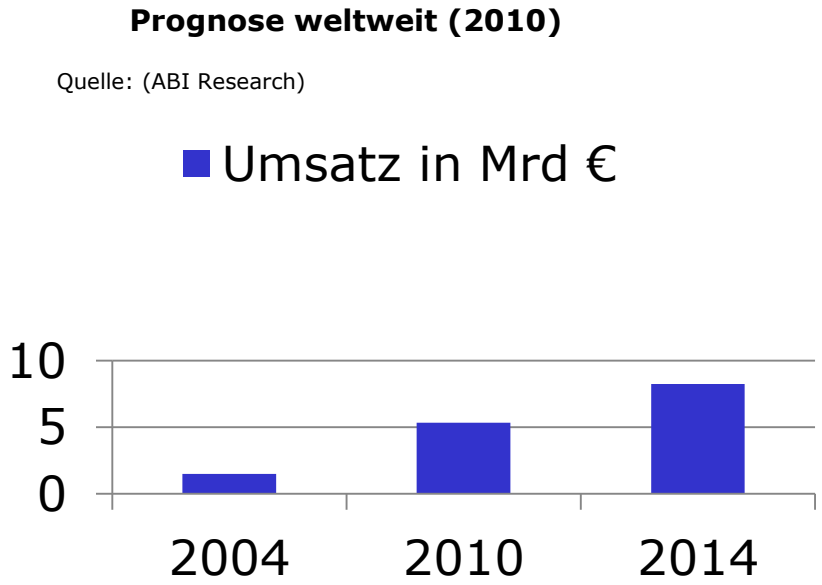
01 Einführung (2)



Aufbau eines RFID Systems

01 Einführung (3)





02 Unterscheidungsmerkmale von RFID-Systemen(1)

- **Reichweite**
  - Close Coupling (bis 1cm)
  - Remote Coupling (bis 1m)
  - Long Range (1m – 10m)
- **Frequenz**
  - 1Hz bis 2,5GHz
- **Energieversorgung (des Transponders)**
  - (Semi-) Passiv (Induktiv)
  - (Semi-) Aktiv (Batterien)

02 Unterscheidungsmerkmale von RFID-Systemen(2)

- **Speicherkapazität**
  - 1 Bit Transponder (Eignen sich als Warenetikett)
  - Automaten und Mikroprozessoren (bis 8MB)
- **Beschreibbarkeit**
  - Meist nicht-flüchtig (zb. EEPROM, FRAM)
  - Selten flüchtig: (SRAM)
  - Oft „Read-Only“
- **Standards (ISO Normen, EPC)**
- **Kosten**
- **Bauformen**
  - …

02 Unterscheidungsmerkmal : Bauformen

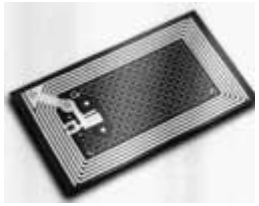
Metalltransponder

Direkttransponder

Karte

Schlüssel

Glastransponder



Smart Labels

Plastiktransponder

02 Unterscheidungsmerkmal : Kosten

Pauschale Aussagen nicht möglich, aber folgende Kosten entstehen bei nahezu jedem System

Komponente	Kosten pro Stk. bzw. Meter
Transponder	0,30 - 35 €
Lesegeräte	50 - 5.000 €
Antennen & Multiplexer	15 - 300 €
Kontroller	500 - 2.000 €
Kabel	7 €

03 Akteure

Aktive Partei = Betreiber des RFID-Systems, bedroht durch

- Angriffe durch Passive Partei
- Angriffe durch eine Drittpartei(Konkurrenten, Wirtschaftsspione, Cyberterroristen…)

Passive Partei = Träger von Transpondern, bedroht durch

- Nutzung oder Weitergabe der Daten durch die Aktive Partei
- Angriffe von Außen

04 Einsatzgebiete (1)

Quelle: Bundesministerium des Innern

- **Logistik**
  - Flughäfen, Packstationen…
  - Logistische Probleme gibt es in allen Branchen, in denen man rationalisieren kann
- **Warensicherung**
  - In Kaufhäusern, eigentlich ein sehr unsicheres Verfahren mit „RF-Etiketten“ und „Hard-Tags“
  - Ersatz für Barcode
- **Reisepass**

04 Einsatzgebiete (2)

- **Fahrzeugen**
  - Toll collection
  - Fahrzeugidentifikation (e-Plate Nummernschilder)

- **Kontaktlose Chipkarten**
  - Fahrkarten im ÖPNV
  - Studentenausweis / Emeal
  - Zutrittskontrolle, Zeiterfassung
  - Fußball WM Eintrittskarten (2006) um Ticketschwarzhandel zu unterbinden

- **Tracking von Personen und Tieren**
- **. . .**

Sicherheit und Datenschutz

- **05 Angriffsmethoden**
- **06 Sicherheitsanforderungen und Maßnahmen**
- **07 Bedrohungen**
- **08 Beispiel Risiken**
- **09 Zusammenfassung**

05 Angriffsmethoden (1)

- **Sniffing**
  - Passiv laufende Datenkommunikation mitlesen
  - Aktives Auslesen mittels eigenem Lesegerät
- **Spoofing**
  - Auslesen wie Sniffing
  - Zusätzlich Manipulieren der Daten
- **Replay Attacke**
  - Abhören einer Datenkommunikation
  - Erneutes Einspielen, dadurch Vortäuschen eines autorisierten Lesegerätes, obwohl Passwort unbekannt

05 Angriffsmethoden (2)

- **Man-in-the-Middle-Attacken**
  - Angreifer schaltet sich zwischen Lesegerät und Transponder
  - Abgesendete Daten werden abgefangen und manipuliert weitergereicht
- **Cloning und Emulation**
  - Nachbauen eines Transponders
- **RFID-Malware**
  - Hacking Attacken (Viren, Würmer)
  - Ausnutzen von Softwarefehlern im RFID Lesegerät sowie Schwachstellen im Transponder zur Einbringung von schädlichem Code

*"**Is Your Cat Infected with a Computer Virus?**"[1]*

05 Angriffsmethoden (3)

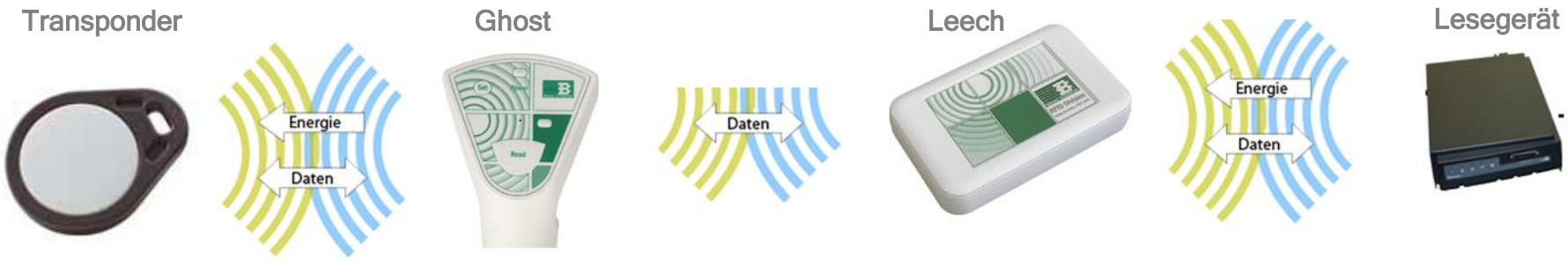
- **Denial of Service (Destruktion des Transponders)**
  - Mechanische Zerstörung des Chips
  - Absenden von Kill Kommandos (erfordert Autorisierung von Schreibzugriffen)
  - Abschirmung des Tags
  - Aktiver Störsender
  - Blocker Tags täuschen RFID-Tags vor
- **Tracking**
  - Erstellen von Bewegprofilen durch Zuordnung von RFID-Nummern zu Ort und Zeit

05 Angriffsmethoden (4)

- **Relay-Angriffe**
  - „Ghost" dient der Kommunikation mit RFID-Transponder
  - „Leech" dient der Kommunikation mit RFID-Lesegerät

    → höhere Reichweite

    → vortäuschen der physikalischen Existenz des RFID-Tags, die dann weitere Aktionen auslösen



06 Sicherheitsanforderungen und Maßnahmen

Anforderung (Auszug)	Maßnahmen
Senden von Daten **nur** durch Aktivierung eines autorisierten Lesegeräts	• An-/Ausschalter (Mechanisch) • Authentisierung (Passwort-basiert, kryptografisch) • Read-Only Tags • Sperrung nicht benötigter Speicherbereiche
Abhörsicherer Datenverkehr, vor allem bei größeren Distanzen	• Verschlüsselung beim Speichern/Auslesen • Verschlüsselte Datenübertragung
Informationelle Selbstbestimmung	• Keine Technischen Maßnahmen, RFID Chips können überall versteckt sein
Schutz vor Korruption und Fälschungen	• Kryptografische Prüfsumme • Erkennung von Duplikaten

07 Bedrohungslage

Für die aktive Partei (RFID Systeme)

- Im Vergleich zu technischen Schwierigkeiten des Betriebs eher gering
- Kosten für Sicherheitsmaßnahmen sinken, sind aber beachtlich

Für die passive Partei (Träger von Tags)

- Privatsphäre gefährdet
  - Weniger durch Angriffe auf RFID-Systeme, sondern vielmehr durch den Normalgebrauch
  - Aufbau von Datenbeständen
  - Frage der Relevanz im Vergleich zu akzeptierten Systemen

08 Beispiel Risiken (1)

Künstliche Einschränkung der Kompatibilität und Lebensdauer

- Geräte akzeptieren nur noch Austauschteile von Herstellern
  - Zb Tintenpatronen:
    - Haben ein Verfallsdatum, danach wird die Patrone nicht mehr akzeptiert

RFID Reisepass speichert Daten

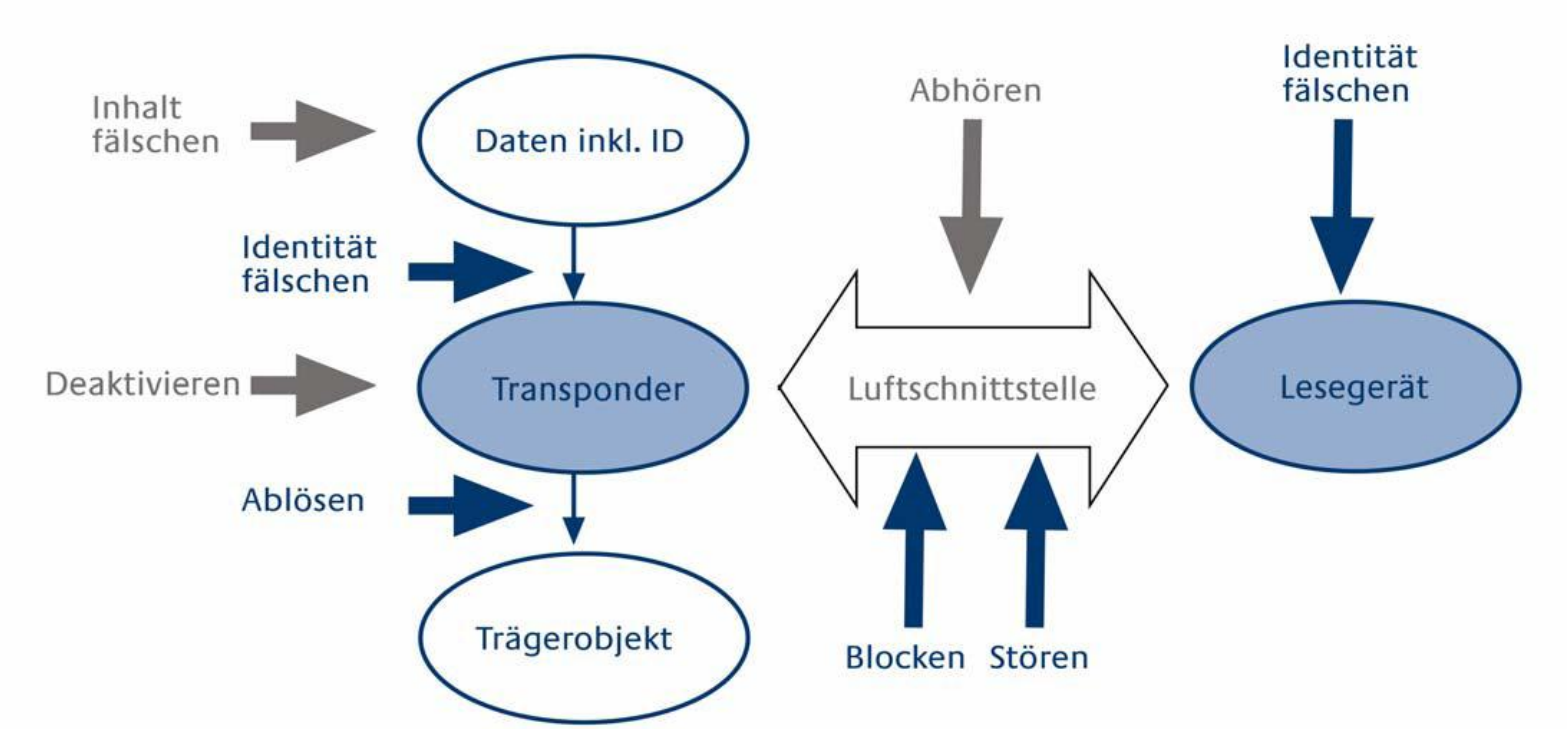
- Name, Geb.-Datum, Geschlecht, Staatsangehörigkeit
- Seriennummer, ausstellender Staat, Dokumententyp, Gültigkeitsdatum
- Biometrische Informationen
  - Passfoto
  - 2 Fingerabdrücke

08 Beispiel Risiken (2)

RFID Reisepass Sicherheitsmerkmale

- Passive Authentication Signatur verhindert Fälschungen
- 28-/ 56-Bit Authentisierungsschlüssel
- Unbemerktes Auslesen
  - Durch Sniffing
  - Entschlüsseln der aufgezeichneten Kommunikation möglich, wenn Informationen über Person bekannt (zb. Name)
  - Hacken des Schlüssels mittels Brute-Force

09 Zusammenfassung



Danke für Ihre Aufmerksamkeit.

Quellen

- *http://www.lsb-plattform.de/rfid-labor/ (Bilder)*
- *http://www.rfid-ready.de (Bilder)*
- *http://www.tagesschau.de/wirtschaft/meldung98372.html (Statistik)*
- *http://www.rfid-basis.de/ (Angriffsmethoden und Bilder)*
- *www.drheinecke.de/fh_ge/files/isyb_ss09/praes07.pdf (Reisepass)*
- *Deutsche Wikipedia : Stichwort „RFID"(Def., Einsatzgebiete und Bilder)*
- *Bundesamt für Sicherheit https://www.bsi.bund.de/cae/servlet/contentblob/477116/publicationFile/30573/RIKCHA_pdf.pdf S.41 (Skizze der Zusammenfassung)*

- *[1] M.R. Rieback, B. Crispo, and A.S. Tanenbaum (Zitat)*

»Wissen schafft Brücken.«