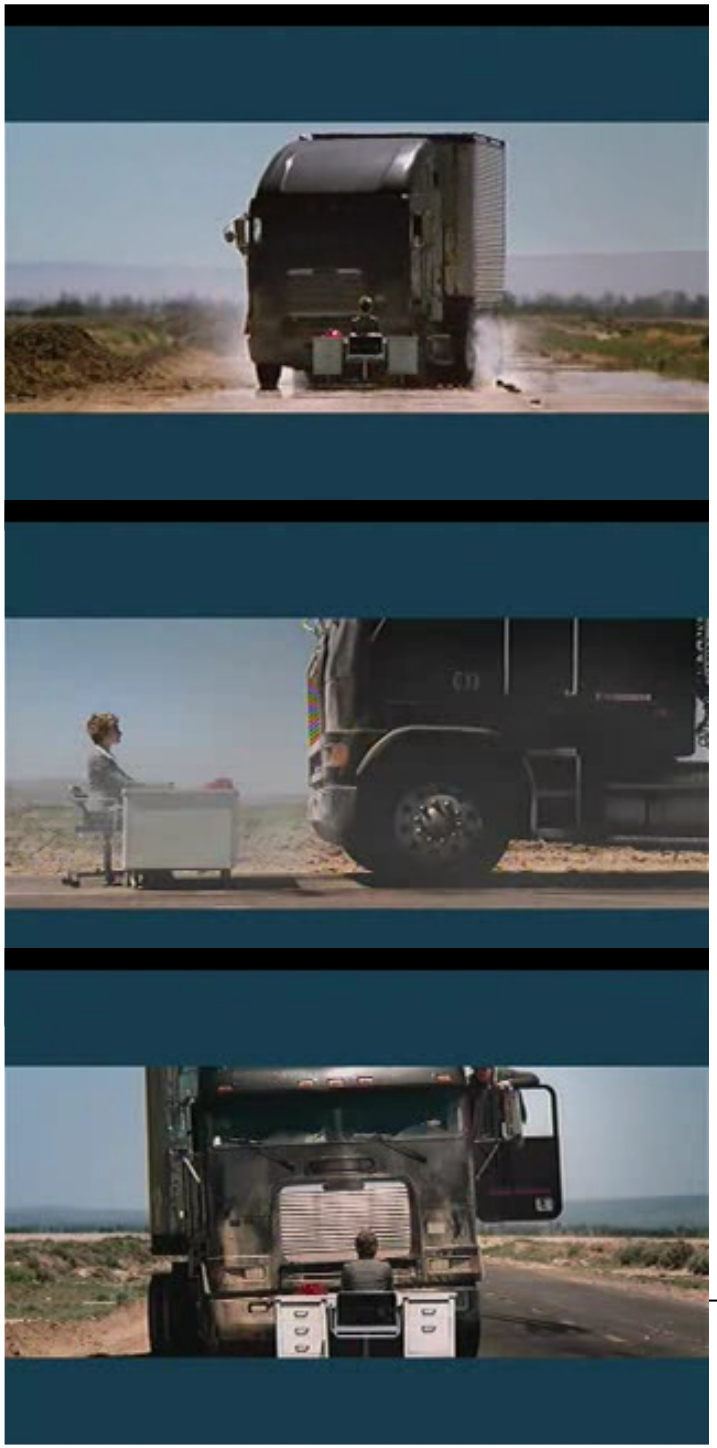
Wireless Location Privacy: Angriffspotential durch RFID und Gegenmaßnahmen

Markus Korte

Betreuer: Thorben Burghardt

Aktuelle Herausforderungen von Datenschutz und Datensicherheit in modernen Informationssystemen

Seminar im Sommersemester 2007
Universität Karlsruhe (TH)



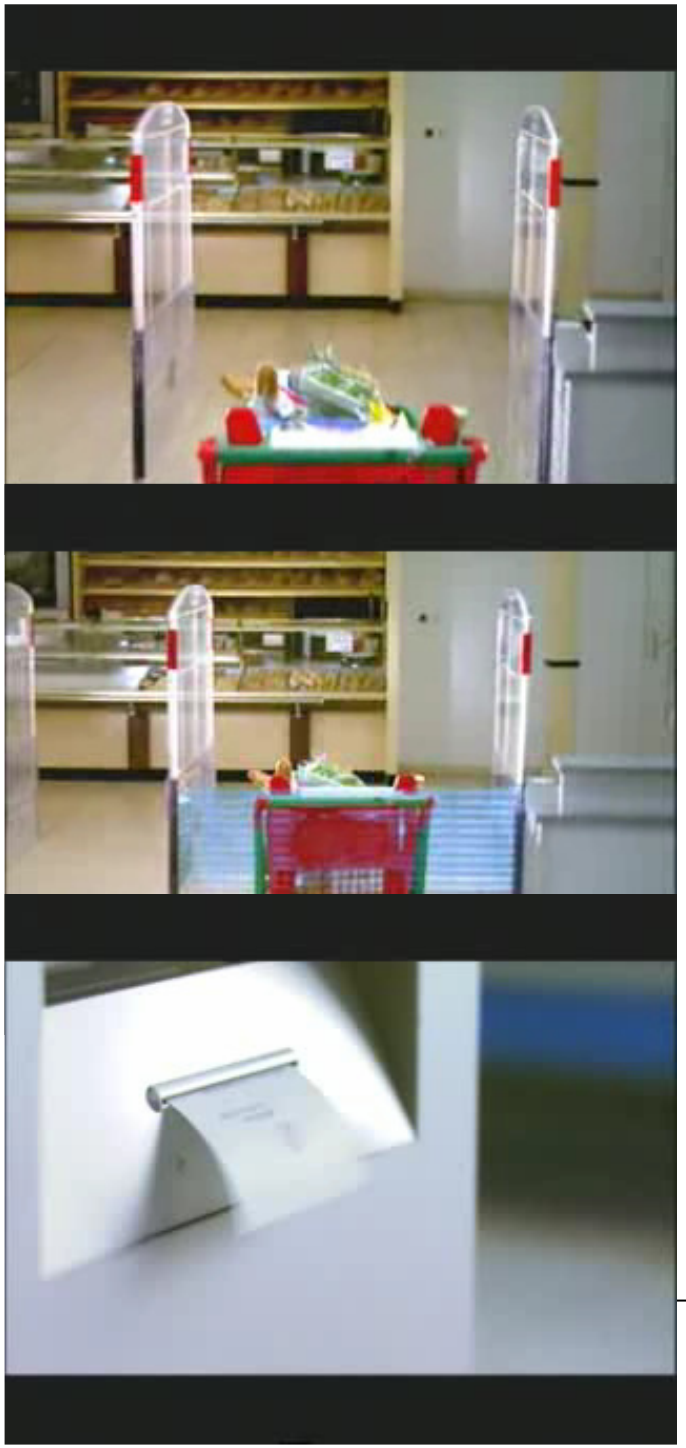
Motivation durch die Werbung

- Werbung, die den Unternehmer ansprechen soll
- Für den Logistiker wichtig: Tracking & Tracing
- RFID ist der „Heilige Gral“ für einen Logistiker

<u>Aussagen der Werbung</u>

„RFID Radio Tags on the Cargo
[...] Helps Track Shipment“

„Inventory off Track? IBM can help“



Motivation durch die Werbung

- Werbung, die den Verbraucher ansprechen soll

<u>Aussage der Werbung</u>

Schlange stehen an der Kasse gehört der Vergangenheit an

Motivation auch für ältere Menschen, denen langes Stehen besonders schwer fällt

IBM

MetroGroup Future Store Initiative

Gliederung

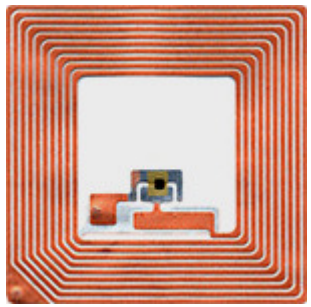
1. Grundlagen
   a) Funktionsweise von RFID
   b) Unterscheidung der RFID Transponder
   c) Genauere Betrachtung von RFID Tags
2. Aktuelle/Zukünftige Anwendungen von RFID
3. Angriffe auf die Privatsphäre durch RFID
   a) Identifizierbar durch RFID Tags
   b) Verfolgbar durch RFID Tags
   c) Einordnung in ein soziales Netz
   d) Bevormundung
4. Schutz vor Angriffen auf die Privatsphäre
   a) Manuelle Schutzmaßnahmen: Clipped Tag; Faraday Käfig
   b) Automatisierte Schutzmaßnahmen: Blocker Tag, RFID Guardian
5. Zusammenfassung

Funktionsweise von RFID

- RFID = Radio Frequency Identification
- RFID System bestehend aus
  - RFID Transponder: Chip mit Antenne
    - Antenne dient zum Senden und Empfangen von Daten
    - Antenne aber auch Spule, die einen Kondensator auflädt
  - Lese/Schreibgerät (Reader)
    - Daten anfragen und senden mittels Radiowellen
    - Aber auch Energieversorger; Radiowelle als Energieträger
  - Middleware: Schnittstelle zur Datenbank

- Aktive Transponder: eigene Batterie; groß und teuer
- Passive Transponder: keine Batterie; klein und billig

Unterscheidung der RFID Transponder



- Personenbezogene (Smartcards) → teuer
  - geschützte Datenübertragung hat hohe Priorität
  - Unterstützung von Kryptografie
  - geringe Auslesereichweite (bis 15 cm)
- Objektbezogene (RFID Tags) → billig
  - niedriger Preis hat hohe Priorität
  - Daher weniger Funktionalität (keine Kryptografie)
  - große Auslesereichweite (bis zu 10 m)

RFID Tags kommen wegen des geringen Preises (1 Cent) für eine große Verbreitung in Frage, daher hier Gegenstand der Betrachtung

Genauere Betrachtung von RFID Tags

- Verfügen über einen kleinen Speicher (< 1024 bits)
- Speichern die EPC-Nummer (Electronic Product Code)
- Das getagte Objekt selbst wird in einer Datenbank repräsentiert
- EPC ist der Schlüssel für das Objekt
- Soll in Zukunft den Strichcode ersetzen
- Jeder Artikel kann eindeutig identifiziert werden

	Header	**General Manager Number**	**Object Class**	**Serial Number**
GID-96	8	28	24	36
	0011 0101 (Binary value)	268,435,456 (Decimal capacity)	16,777,216 (Decimal capacity)	68,719,476,736 (Decimal capacity)

Struktur der 96-bit EPC Nummer [1]

Aktuelle Anwendungen von RFID

Anwendungsbeispiele von RFID [2]

- E-Zpass: Erfassung von Mautgebühren
  (bis 100 Meilen/h)
- Wegfahrsperre für Autos
- SmarTrip
  (Bezahlsystem für öffentliche Verkehrsmittel)

- Elektronischer Pass
- Fußball WM Tickets 2006 in Deutschland
- Bibliothek
- Kreditkarte (American Express‘ expressway)
- Tierkennzeichnung

Zukünftige Anwendungen von RFID

- RFID Tags ersetzen den Strichcode
  - Automatische Bestandsverwaltung macht Inventur überflüssig
  - Haushaltsgeräte bieten unterstützende Funktionen an
  - Kleiderempfehlung im Kaufhaus

- Echtheitsprüfung (auch von Geldscheinen)
  - Hitachi hat die Herstellung von 0,15x0,15 mm Chips angekündigt

- Patientendaten im Krankenhaus (Armband mit RFID Transponder)
- Implantation für Menschen (heute bereits von VeriChip Corp.)

Gliederung

1. Grundlagen
   a) Funktionsweise von RFID
   b) Unterscheidung der RFID Transponder
   c) Genauere Betrachtung von RFID Tags
2. Aktuelle/Zukünftige Anwendungen von RFID
3. Angriffe auf die Privatsphäre durch RFID
   a) Identifizierbar durch RFID Tags
   b) Verfolgbar durch RFID Tags
   c) Einordnung in ein soziales Netz
   d) Bevormundung
4. Schutz vor Angriffen auf die Privatsphäre
   a) Manuelle Schutzmaßnahmen: Clipped Tag; Faraday Käfig
   b) Automatisierte Schutzmaßnahmen: Blocker Tag, RFID Guardian
5. Zusammenfassung

Identifizierbar durch RFID Tags

- Das Auslesen von RFID Tags ist berührungslos und ohne Sichtkontakt möglich
- Jede Person mit einem Lesegerät kann den eindeutigen EPC des RFID Tags auslesen

- daraus ergeben sich folgende Gefahren [3]:
  - der Angreifer kann feststellen welche Objekte in meinem Besitz sind
    - er kann ein Profil von mir erstellen, um gezielte Werbung anzuwenden
    - ein Dieb kann mich so unbemerkt auf lohnende Beute durchsuchen
    - der Mensch wird durch seine Tags identifizierbar

      → **Voraussetzung für die nächsten beiden Folien**

  - Angreifer benötigt Zugriff auf die „Objekt-Datenbank“
    Object Name Service (Auto-ID Center), EPC Discovery Service (Verisign)

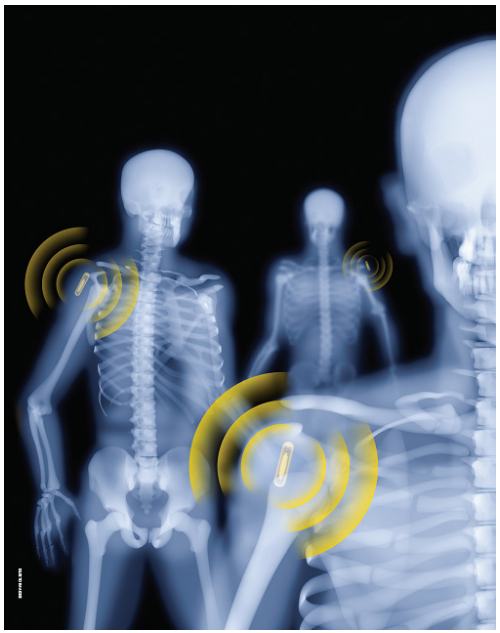
Verfolgbar durch RFID Tags

- Kann der Mensch über RFID Tags identifiziert werden, dann ist er technisch gesehen ein getagtes Objekt.
- Die Eingangsfolie hat gezeigt, das Objekte verfolgbar sind. Gleiches gilt dann also auch für den Mensch.

→ Somit geht Location Privacy verloren

- RFID Tags legen eine Spur aus „Brotkrümmeln“ zu ihrem Besitzer. Auch wenn er die Objekte gar nicht mehr hat [4].
  - er kann so fälschlicherweise für Objekte haftbar gemacht werden, die er gar nicht mehr besitzt
  - diese Gefahr besteht insbesondere bei zusätzlicher Verwendung von Treuepunkte-Karten

Soziale Netze



- es geht um das Finden von Personengruppen, die auf eine soziale Weise miteinander verbunden sind (z.B. Arbeitskollegen, Familie)
- unter der Annahme, dass innerhalb eines sozialen Netzes gleiche Interessen bestehen, kann gezielte Werbung angewendet werden
- die Polizei hat ein Interesse kriminelle Gruppen aufzudecken (z.B. Krawallmacher)

Durch eine feingranulare Analyse der gesammelten Daten von vielen Lesegeräten können soziale Netze gefunden werden [3].

Die besondere Gefahr besteht darin, einer falschen Gruppe zugeordnet zu werden.

Bevormundung

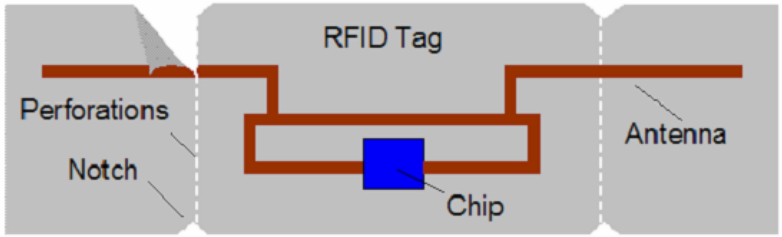
- RFID Tags können eingesetzt werden, um den Benutzer auf ein falsches Verhalten zu überprüfen [3]
- Beispiel ist unsere 24h-Bibliothek, die Alarm schlägt, wenn ein Benutzer das Gebäude verlassen möchte, ohne die Bücher auszuleihen
- Gerade im Haushaltsbereich können Anwendungen dieser Art folgen (Waschmaschine, Kühlschrank)

→ was anfänglich eine Erleichterung für den Benutzer zu sein scheint, könnte bald ein Gefühl der Bevormundung hervorrufen

Gliederung

1. Grundlagen
   a) Funktionsweise von RFID
   b) Unterscheidung der RFID Transponder
   c) Genauere Betrachtung von RFID Tags
2. Aktuelle/Zukünftige Anwendungen von RFID
3. Angriffe auf die Privatsphäre durch RFID
   a) Identifizierbar durch RFID Tags
   b) Verfolgbar durch RFID Tags
   c) Einordnung in ein soziales Netz
   d) Bevormundung
4. Schutz vor Angriffen auf die Privatsphäre
   a) Manuelle Schutzmaßnahmen: Clipped Tag; Faraday Käfig
   b) Automatisierte Schutzmaßnahmen: Blocker Tag, RFID Guardian
5. Zusammenfassung

Manuelle Schutzmaßnahmen



- Clipped Tag von IBM [5]
  - Verkürzen der Antenne
  - Reduktion der Auslesereichweite

- Faradayscher Käfig [6]
  - Physikalisches Prinzip
  - Aluminium als Schutzschild gegen Radiowellen

Automatisierte Schutzmaßnahmen – Blocker Tag

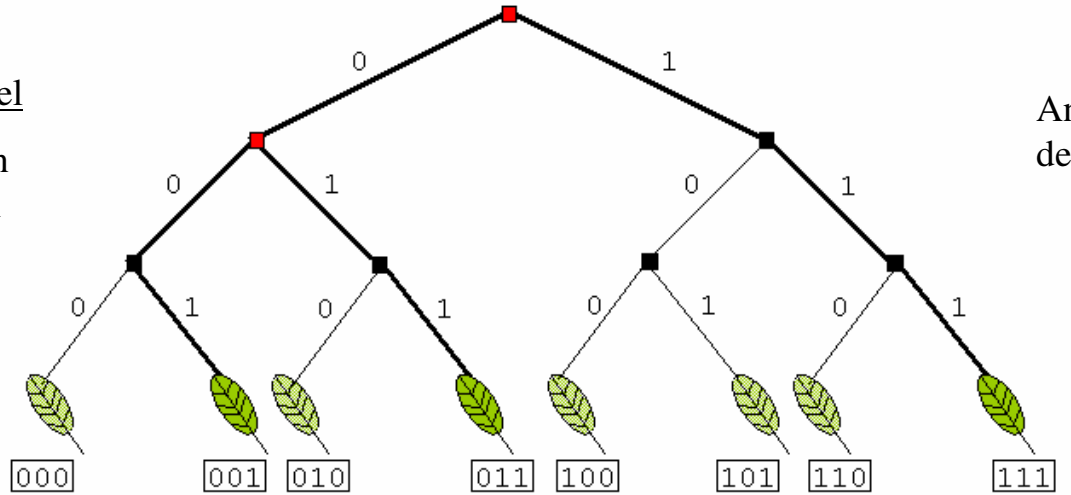
Hintergrund: Auslesen der EPC Nummer

- Lesegeräte können zu einem Zeitpunkt nur mit einem Tag kommunizieren
  - Daher Einsatz von Singulation Protokollen zur Kollisionsauflösung
  - Das **Tree-walking** Protokoll ist ein solches

<u>Erläuterung am Beispiel</u>

3 Tags befinden sich in der Umwelt und sollen ausgelesen werden:

- 001
- 011
- 111



Anzahl möglicher Tags in der Umwelt: $2^3 = 8$

Blocker Tag - Full Blocker

- Das Full Blocker Tag [7] meldet sich bei jeder Anfrage als 0 und 1
  - D.h. in jedem Knoten des Baumes wird ein Konflikt vermerkt
  - Der Konflikt taucht unabhängig von tatsächlichen Tags in der Umwelt auf

- Das Full Blocker Tag simuliert also alle möglichen RFID-Tags
- Bei Verwendung von EPC mit 96 bit sind das 2^{96} Tags

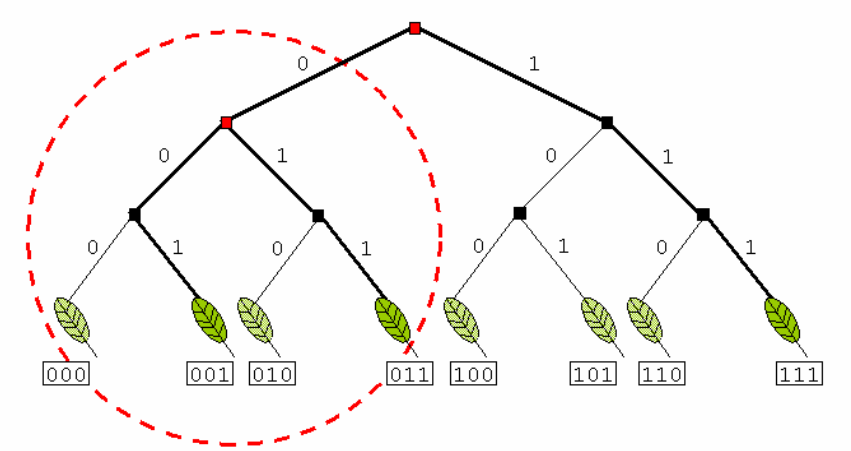
- In der Folge muss das Lesegerät 2^{96} Tags anfragen
  - Es kommt zum timeout

- **Vorteil:** unbemerktes Auslesen wird ohne eine Aktion des Benutzers verhindert
- **Nachteil:** Missbrauch (Denial of Service Attacke);
  Ungewollte Blockierung: Einkauf im Supermarkt muss an der Kasse auslesbar bleiben

Blocker Tag – Selective Blocker

- Wünschenswert, dass nur bestimmte Zonen im Baum geblockt werden
- Im Bespiel simuliert der Selective Blocker [7] alle Tags mit Anfangsbit 0
  - Problem: Das Lesegerät muss 2^{96-1} simulierte Tags abfragen → timeout

- Daher darf das Lesegerät nicht versuchen geblockte Zonen auszulesen
  - Lösung: Ein Bit des EPC wird als Privacy Bit deklariert
  - Alle Tags mit Privacy Bit gleich 1 werden geblockt
  - Privacy Bit gleich 1, dann versucht das Lesegerät nicht den Tag auszulesen



Zone, die nicht ausgelesen werden kann, weil sie durch das Selective Blocker Tag simuliert wird

Automatisierte Schutzmaßnahmen – RFID Guardian

Idee eines portablen Gerätes, das z.B. im Handy integriert ist und folgende Funktionen bietet [8]:

- *Auditing:* in der Umgebung nach neuen Tags suchen, sie aufzeichnen und anzeigen, sowie illegale Leseversuche melden
- *Key management:* verwalten von Passwörtern, die für Tags mit erweiterter Funktionalität (z.B. sleep/wake Befehle) benötigt werden
- *Authentication:* das Lesegerät muss sich zu erkennen geben
- *Access Control List:* auf der folgenden Folie erläutert

Automatisierte Schutzmaßnahmen – RFID Guardian

- Anhand der Access Control List (ACL) prüft der RFID Guardian welche Befehle ein Lesegerät auf welchen Tags ausführen darf
- Versucht ein Lesegerät verbotenerweise einen Befehl auszuführen, sendet der Guardian ein Störsignal (Selective Jamming)
- Das Störsignal wird zufällig moduliert, um ein Ausfiltern durch das Lesegerät zu verhindern

Vorteil: unbemerktes Auslesen kann durch eine gezielte Strategie verhindert werden

Nachteil: Guardian selbst wird zu einem lohnenden Angriffsziel, weil er sensitive Daten speichert; Einsatz von Störsignalen könnte illegal sein.

Action	Source	Target	Command	Comment
block	*	MYTAGS	*	Suppress all queries targeting user‘s tags
allow	Home	MYTAGS	*	Home system can query user‘s tags
allow	Wal-Mart	MYTAGS	Read data block	Wal-Mart can read (not write) data from user‘s tags
allow	*	*	*	All queries to other RFID tags are OK

Beispiel für eine Access Control List (ACL) [9]

Zusammenfassung

- Die vorgestellten Anwendungsbeispiele lassen erahnen welches Potential in der RFID Technik steckt.
- Auf der anderen Seite wurde gezeigt, dass mit der Einführung von RFID Technik auch potentielle Probleme verbunden sind.
  - Hauptaugenmerk lag hier auf der Privatsphäre, deren Schutz durch einen Missbrauch von RFID gefährdet ist.
- Es wurden zwei „off-tag Verfahren“ vorgestellt, die ihrerseits durch den Einsatz von RFID Technik einen Angriff abwehren sollen (Blocker Tag, RFID Guardian)

ENDE

Bist Du sicher, dass Du bei deinem letzten Arztbesuch nur eine Impfung bekommen hast?

Literatur

[1] EPCglobal: EPCTM Tag Data Standards Version 1.1 Rev.1.24

[2] Ron Weinstein: RFID - A Technical Overview and Its Application to the Enterprise; (IT Professional 3/2007)

[3] Spiekermann, S., Ziekow, H.: RFID: A Systematik Analysis of Privacy Threats and a 7-Point Plan to Adress Them (Journal of Information System Security, Vol. 1, No. 3, 2006)

[4] Garfinkel, Juels, Pappu: RFID Privacy - An Overview of Problems and Proposed Solutions; (IEEE Security and Privacy 3/2005)

[5] IBM White Paper: Privacy-Enhancing Radio Frequency Identification Tag - Implementation of the Clipped Tag

[6] http://foebud.org

[7] Juels, Rivest, Szydlo: The blocker tag - selective blocking of RFID tags for consumer privacy (CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, Seiten 103-111)

[8] Rieback, Crispo, Tanenbaum: RFID Guardian - A Battery-Powered Mobile Device for RFID Privacy Management (ACISP 2005 Seiten 184-194)

[9] Rieback, Crispo, Tanenbaum: Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags (4/2005)

[ ] Bilder auf Folie 13 und 23 entnommen aus IEEE Spectrum 3/2007

Gegenmaßnahmen

- In dieser Arbeit nur off-Tag Verfahren betrachtet
- Es gibt aber auch Schutzmechanismen, die im Chip integriert sind.
- On-Tag Lösungen:
  - Tag Killing (wird vom aktuellen EPC Standard unterstützt)
  - Sleep/Wake Befehle
  - Pseudonyms
  - Hash Locks
  - Cryptography/Authentication