

RFID

Computer-Sicherheit für Paranoiker
(SS 2006)

Jonathan Wigglesworth
email: jonathan.wigglesworth@gmail.com

Übersicht

- Was heisst RFID?
- Was macht man damit?
- Wer macht was damit?
- Angriffe
- Konklusion

Radio Frequency ID

- keine Feststellung
- Passiv, Semi-aktiv, oder Aktiv
- vergleichbar mit Barcodes:
verschiedene spezifikationen für verschiedene
Anwendungen

Passiv RFID



- backscatter (Rückstreuung)
- für kurze Distanzen
- $0.15\text{mm}^2 \times 7.5\mu\text{m}$
- können gedruckt werden
- 13.56 Mhz, 860-960 Mhz
- \$0.10 pro Tag

Semi-aktiv RFID



- backscatter
- kleine Akku
- schneller
- unpopulär

Aktiv RFID



- Ausstrahlung
- großer Akku
- längere Distanzen
- 433 Mhz
- \$20 pro Tag

Allgemeinheiten

- widersprüchlich Meinungen zu Angaben, bzw. Distanzen
- meistens nicht verschlüsselt
- meistens überschreibbar
- erlaubt Frequenzen sind von Länder abhängig
- Kollisionserkennung: zufällige Aussendung

Was macht man damit?

- Autobewachung
- Benzin kaufen
- Lieferkette/Einordnen
- Personalausweiserkennung
- Diebstahlschutz

Autobewachung

- Autos kann nicht ohne den Schlüssel gestartet werden
- Autos genau identifizieren, auch wenn gefarbt oder anders verdeckt
- Autos finden wenn geklaut oder verloren
- Fahrerflucht Unfälle verhindern

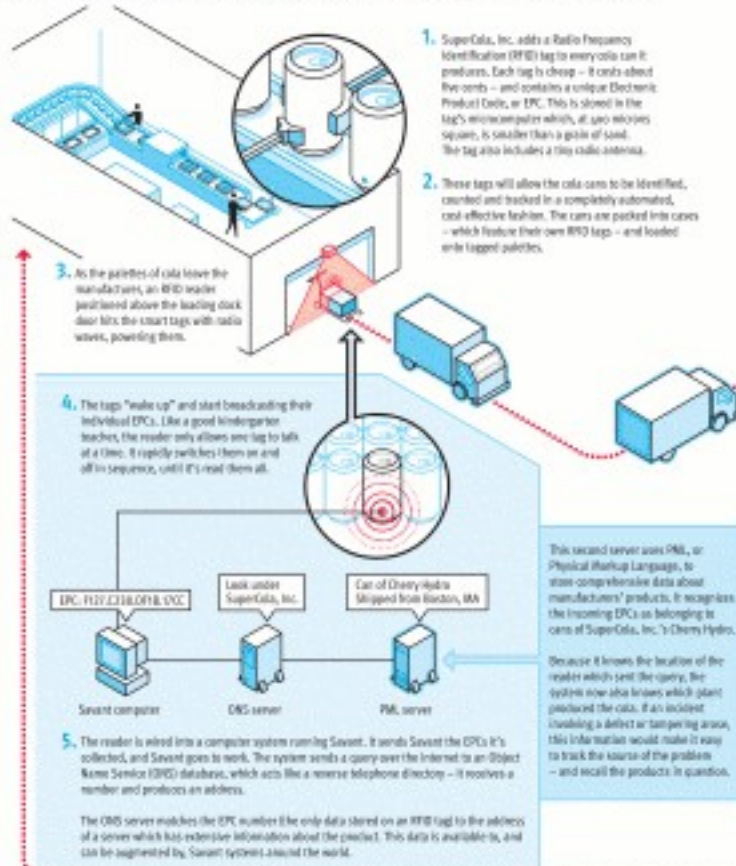
Automatisch aus dem Girokonto:

- Benzin kaufen
- Zoll bezahlen
- Parkplatz bezahlen
- usw. ...

Lieferkette

HOW THE AUTO-ID SYSTEM WILL AUTOMATE THE SUPPLY CHAIN

With Auto-ID technology, physical objects will have embedded intelligence that will allow them to communicate with each other and with businesses and consumers. Auto-ID technology offers an automated, numeric system of smart objects that revolutionizes the way we manufacture, sell, and buy products. Here's how it works:



XPLANATIONS™ by XPLANE™

Wer macht was?

- 1939: England: Flugzeuge identifizieren während des Zweiten Welt Krieg
- 1945: Léon Theremin entwickelt RFID-ähnlich Abhörwanze
- 1997: ExxonMobil: Benzin/Zoll Bezahlung (SpeedPass/EZ-Pass)
- 2001: Department of Veterans Affairs: Einordnen (Talking Prescriptions)
- 2004: Toyota: Autobewachung (Smart Start)
- 2005: Wal*Mart: Lieferkette, diebstahlschutz (EPC)

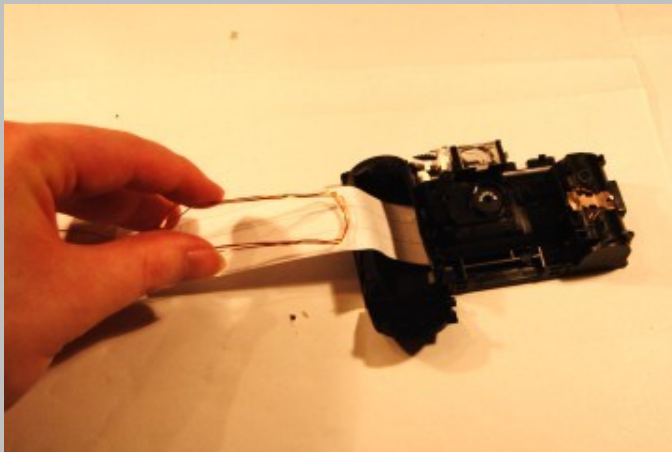
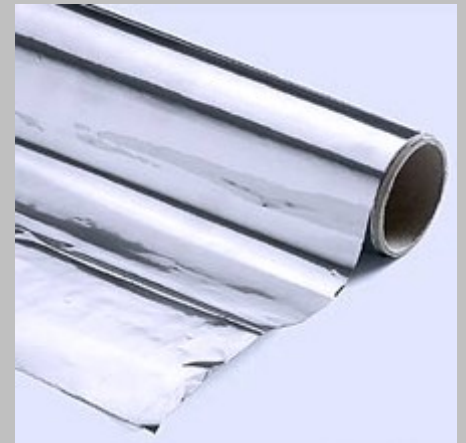
Angriffe gegen RFID

- Zerstören/Abdecken
- Wechseln/Bearbeiten
- Cloning (klonen)
- Entfernen
- Zufügen

Angriffe gegen RFID

- Cloning (klonen)
 - Personal impersonifizieren, DDoS, klauen
- Entfernen
 - klauen, entführen/kidnappen
- Zufügen
 - DDoS, belauern/spionieren

Zerstören/Abdecken



Bearbeiten

- RFDump
- Löschen
- Preise wechseln
- Personaldatei ändern
- Konterbande verdecken

zum Schluss

- RFID ist alt, aber trotzdem sehr unreif
- viele verschiedene sorten
- offer unverschlüsselt oder leicht entschlüsselt
- mit ein Faraday Cage abdeckbar
- überladbar (RFID-Zapper)

Quellen

- <http://de.wikipedia.org/wiki/Rfid>
- <http://rfidanalysis.org/>
- <http://www.aimglobal.org/technologies/rfid/>
- <https://events.ccc.de/congress/2005/wiki/RFID-Zapper>
- <http://www.rf-dump.org> (?)
<http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-grunwald/bh-us-04-grunwald.pdf>
<http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-grunwald/bh-us-04-grunwald-tool.zip>
- <http://www.egomexico.com/images/Noticias/Laboratorio/AutoID%20supply%20chain.jpg>
- <http://www.technovelgy.com/>