THE KNOWLEDGE PLACE

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

Seminar: RFID

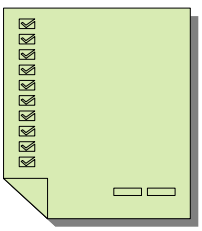
B3: Security- und Privacy-Aspekte bei RFID

ROMAN – Consulting & Engineering AG
Dr. I. ROMAN, CISSP
info@roman.ch, www.roman.ch

Gottlieb Duttweiler Institut, Rüschlikon, 26. Januar 2005

Inhalt

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



- RFID Security News
- RFID Gefährdungen
- Angriffe an RFID Systeme
- Angriffsmöglichkeiten
- Gefährdung der Vertraulichkeit persönlicher Daten
- Abwehrlösungen
- Forderungen

RFID Security News (I)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

RFID: Auch Hacker kommen auf den Geschmack

Von Richard Shim und Joachim Kaufmann
CNET News.com
29. Juli 2004

Die unter Datenschützern umstrittene RFID-Technologie gerät Experten zufolge zunehmend ins Visier von Hackern. Damit ergeben sich für Unternehmen völlig neue Bedrohungsszenarien. Ein Beispiel: Künftig könnten Ladenpreise einfach im Vorbeigehen manipuliert werden.

"Es ist ein großes Risiko für Unternehmen", so Lukas Grunwald, Berater bei der DN-Systems Enterprise Solutions GmbH. "Es eröffnet eine neue Ära für Ladendiebstahl und Chaos-Attacken. Die sinkenden Preise von RFID-Equipment sorgen für eine immer weitere Verbreitung. Im Zusammenspiel mit einem Handheld könnte so ein teueres Produkt quasi im Vorbeigehen günstiger gemacht werden.

Anzeige

http://www.zdnet.de/itmanager/tech/0,39023442,39124515,00.htm

RFID Security News (II)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

Preismanipulation durch RFID-Technologie

Neues Software-Tool gefährdet Warenkennzeichnung

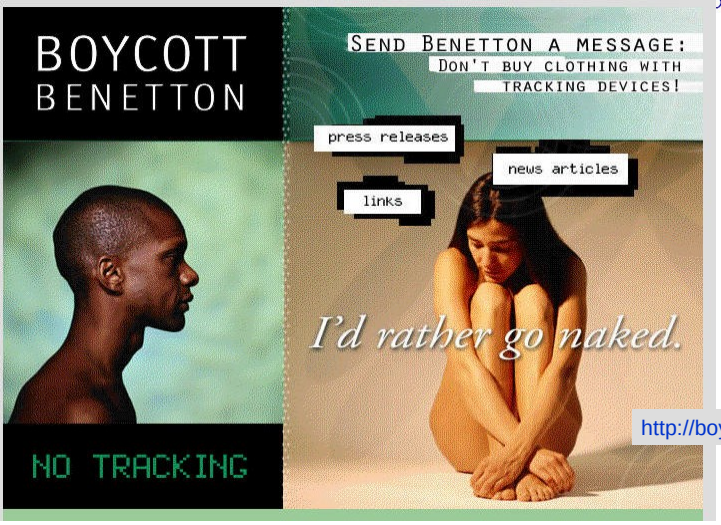
Hildesheim (pte, 29. Jul 2004 14:17) - Neue Technologien ermöglichen es Hackern die auf Radio-Frequency- Identification-Chips (RFID) gespeicherten Daten zu manipulieren. Bedrohte die RFID-Technologie bisweilen die Privatsicherheit der Konsumenten, so könnten nun auch Geschäfte darunter leiden, meint Lukas Grunwald, Berater des deutschen Security-Anbieters DN-Systems http://www.dn-systems.de. Kostengünstige RFID-Etiketten werden von vielen Verkäufern zur Kennzeichnung ihrer Waren eingesetzt. Produktinformationen und Preise könnten durch das neue Software-Tool RFDump sehr leicht verändert werden, berichtete, heute Donnerstag der Branchendienst Cnet http://www.news.com .

Das Lesen und Überschreiben von RFID-Codes wird durch RFDump entscheidend erleichtert.
Das System kann auch auf kleinen tragbaren Geräten eingesetzt werden. Hacker können damit ohne weiteres hohe Preise löschen und stattdessen den Code einer billigeren Waren speichern. Durch ein willkürliches Vertauschen von Produktdaten könnte außerdem ein regelrechtes Chaos ausgelöst werden. Hinzu kommt das RFDump Minderjährigen helfen kann Altersbeschränkungen zu umgehen.

http://www.pressetext.ch/pte.mc?pte=040729030

RFID Security News (III)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



http://boycottbenetton.org/

RFID Security News (IV)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

www.boycottgillette.com/spychips.html

RFID Gefährdungen

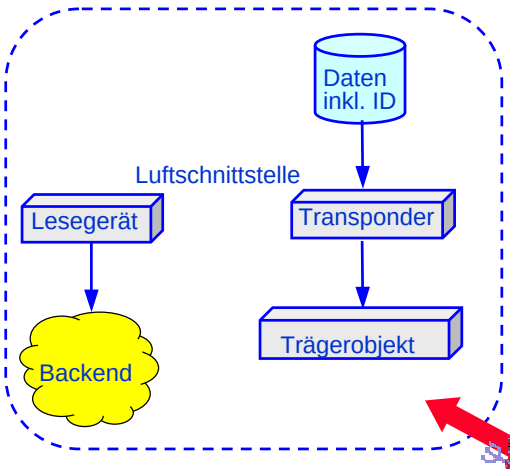
ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- Angriffe an RFID Systeme

- Gefährdung der Vertraulichkeit persönlicher Daten

Angriffe an RFID Systeme

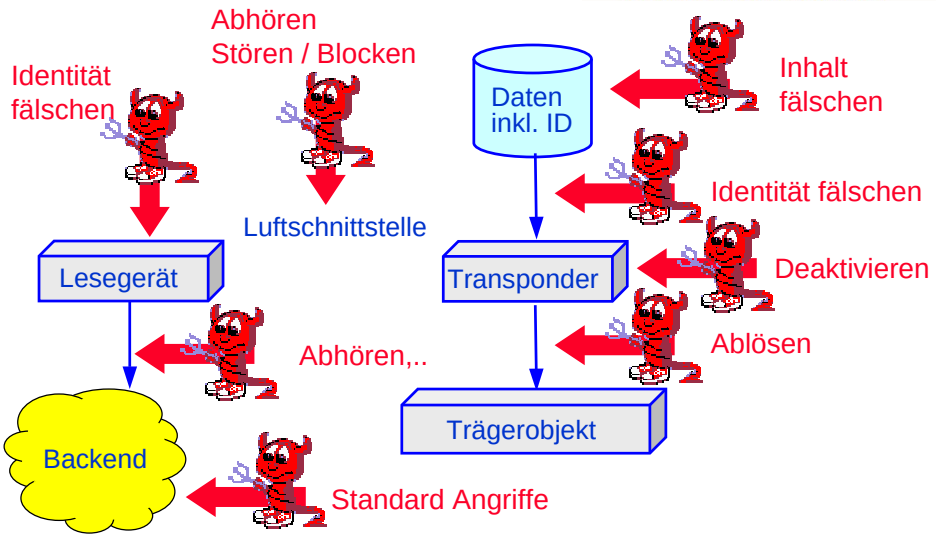
ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



- Der Angreifer verschaft sich unberechtigten Zugang zu Informationen.
  ➔ Ausspähen
- Der Angrifer speist unzutreffende Information ein.
  ➔ Täuschung
- Der Angreifer beeinträchtigt die Verfügbarkeit des RFID Systems.
  ➔ DOS (Denial of Service)

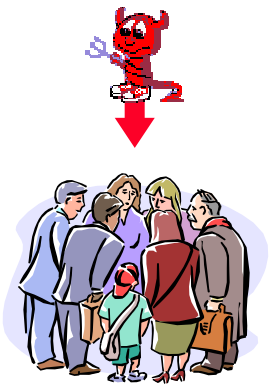
Angriffsmöglichkeiten

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



Gefährdung der Vertraulichkeit persönlicher Daten

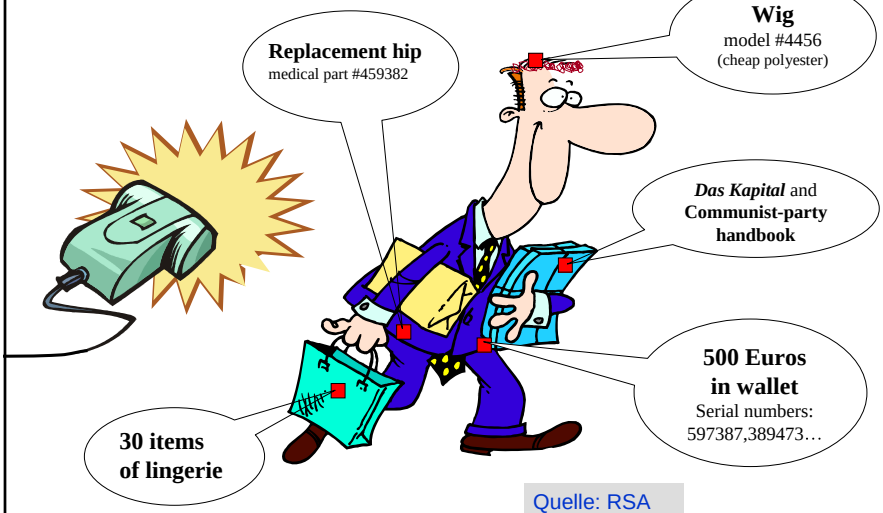
ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



- Erstellung von Bewegungs-, Konsum- und Kontaktprofilen
- Möglichkeit, dass unberechtigte Personen Informationen lesen, weiterverarbeiten oder manipulieren.
- Unberechtigte Verknüpfung von Daten und Personen.
- .....

Unsere Zukunft ?

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES



Quelle: RSA

Datenschutz Schweiz (I)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

Gesetze und Kommentare: Schweiz

Rechtssammlungen:
- Systematische Sammlung des Bundesrechts
- Bundesgericht

- Bundesverfassung Art. 13 Schutz der Privatsphäre
- Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992
- Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG)
- Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988 (pdf)
- Revision des Bundesgesetzes über den Datenschutz
- Verordnung über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung vom 14. Juni 1993 (VOBG)
- Kommentar zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG)
- Verordnung vom 3. Juli 2001 über den Schutz von Personaldaten in der Bundesverwaltung

http://www.edsb.ch/ /d/gesetz/schweiz/index.htm

Datenschutz Schweiz (II)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

CONFOEDERATIO HELVETICA
Die Bundesbehörden der Schweizerischen Eidgenossenschaft

Homepage
Mail
Suche

Systematische Sammlung des Bundesrechts
Inhaltsverzeichnis des Landesrechts
Deckblatt | SR 101 Bundesverfassung der Schweizerischen Eidgenossenschaft
2. Titel: Grundrechte, Bürgerrechte und Sozialziele
1. Kapitel: Grundrechte
◀ **Art. 12** Recht auf Hilfe in Notlagen
▶ **Art. 14** Recht auf Ehe und Familie

français
italiano

Art. 13 Schutz der Privatsphäre

1 Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief—, Post- und Fernmeldeverkehrs.

2 Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Stand am 11. Mai 2004

http://www.admin.ch/ch/d/sr/101/a13.html

Datenschutz Schweiz (III)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

Eidg. Datenschutzbeauftragter : 11. Tätigkeitsbericht 2003/2004

.....

Wenn der Verknüpfung elektronischer Überwachungsnetze das Wort geredet wird, ist darauf hinzuweisen, dass heute aufgrund der technischen Möglichkeiten Kontrollen Orwell'schen Ausmasses realisierbar sind. Mit der Chip-Markierung (über RFID-Etiketten) sind Güter, Personen oder ihre Dienste auf dem ganzen Territorium lokalisierbar. Die daraus gewonnen Informationen könnten problemlos mit andern Datenbanken (Telefonverbindungsdaten, Kreditkarteneinkäufe, Bankkonti, Kundenkarten usw.) verknüpft werden, was die Erstellung von sehr detaillierten Persönlichkeitsprofilen ermöglichen würde. Der gläserne Mensch ist längst keine literarische Metapher mehr, sondern eine mögliche Perspektive für die sehr nahe Zukunft.

.....

http://www.edsb.ch/d/doku/jahresberichte/tb11/index.htm

RFID Gefährdungen
➔ Abwehrlösungen sind da !

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- Angriffe an RFID Systeme
- Gefährdung der Vertraulichkeit persönlicher Daten

Abwehrlösungen (I)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- Starke gegenseitige Authentifizierung zwischen Lesegerät und Transponder (z.B. ISO 9798, „Three-pass mutual authentication protocol“)
- Verschlüsselung
- Verlagerung aller Daten bis auf die ID ins Backend
- Einsatz von Read-only Tags
- Abhörsichere Antikollisionsprotokolle
- Pseudonymisierung („Verschleierung der Tag-Identität“)

Abwehrlösungen (II)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- Einsatz von Detektoren, welche das Versorgungsfeld eines Lesegeräts erkennen
- Starke mechanische Verbindung des Tags mit Trägerobjekt
- Temporäres Verhindern des Auslesens durch Blocker (Bsp. RSA Lösung)*)
- Dauerhafte Deaktivierung durch Kill Befehl *)
- .....

*) *Beim Missbrauch kann diese Funktion auch zum Angriff eingesetzt werden ➔ Autorisierung notwendig*

Forderungen (I)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- RFID Systeme sichtbar anbringen.
- Vollständige Transparenz bezüglich der Eigenschaften der eingesetzter RFID Systeme.
- Vollständige Transparenz bezüglich der Verwendung der ausgelesenen RFID-Daten
- Nur geringe (notwendige) Datenmengen auf den Transponder anbringen.

Forderungen (II)

ROMAN - Consulting & Engineering AG
NETWORK TECHNOLOGY SERVICES

- Offene und nicht hersteller-spezifische Standards einsetzen.
- Recht auf Zerstörung des RFID-Tags nach Kauf, ohne Nachteile für den Käufer.
- Technologie-Kontrolle durch den Gesetzgeber