A Hacker’s Guide to RFID Spoofing and Jamming

Melanie Rieback
DefCon 14
4 August, 2006
What is RFID?

RFID = Radio Frequency Identification
History of RFID Tag Technology

1959 – Radio tags invented for tagging wildlife

1970’s – Radio tags become commonplace for anti-theft technology

1973 – Passive radio tags (RFID) patented

1990’s – Passive radio tags increasingly used as anti-theft technology
History of RFID Tag Technology

1997 – First all-polymer RFID tag

2000 – RFID standards documents emerge

2003 – Euro. Central Bank initiates discussions about embedding RFID tags in Euro bills

Now – RFID trials begin at: Wal-Mart, Gillette, Benetton, Marks & Spencer, Tesco, etc..
Current RFID Tag Technology

- Used as “radio barcodes”
- Low-cost tags (1 kbit, < $0.25)
- Contactless smartcards (72 kbits, > $1.00)
- Acquiring sensor functionality (temperature, pressure, humidity, acceleration, biological agents, tampering)

KSW Microtec TempSens
Modern RFID Applications
VeriChips – Subdermal RFID
VeriChips – Subdermal RFID
VeriChips – Subdermal RFID
VeriChips – Subdermal RFID
VeriChips – Subdermal RFID
VeriChips – Subdermal RFID

What about security?
VeriChips – Subdermal RFID

What about security?

Applied Digital's implantable chips do not employ cryptography as of yet. The system is nevertheless safe because its chips can only be read by the company's proprietary scanners.

- Scott Silverman, CEO of Applied Digital

http://www.siliconvalley.com/mld/siliconvalley/9154114.htm
RFID Security Problems

Some Security Problems:

- Unauthorized tag reading
- Eavesdropping
- Tracking
- Tag cloning
- Denial of Service
- Malware
RFID Security Solutions

The RFID Guardian

• Handheld mobile device for personal RFID privacy management

• Main device characteristics:
  1. Portable
  2. Battery-powered
  3. 2-way RFID communications
RFID Guardian HW

RFID Guardian prototype

RFID tag

RX/Tx Receiver

XScale \(\mu\)-controller (PXA270)

Melexis RX/Tx

1010011...

Host interface

Transmitter

Receiver

RFID reader
RFID Guardian, V1
RFID Guardian, V2
RFID Guardian Demo

The RFID Guardian

Vrije Universiteit, Amsterdam
RFID Guardian SW

**SW Architecture:**

<table>
<thead>
<tr>
<th>Application-level logic</th>
<th>Data Structures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag task</td>
<td>Reader task</td>
</tr>
<tr>
<td>UI task</td>
<td>Timer task</td>
</tr>
<tr>
<td>Device drivers</td>
<td>RFID (ISO) stacks</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tag Spoofing

Real vs. Spoofed RFID Tag Response:
Selective RFID Jamming

- Tag 1
- Tag 2
- Tag 3
- Tag 4
- Guardian

Shared Medium

Timeslot: 2 4 6 8 10 12 14 16

Collisions
RFID Guardian

Main Functionality:

• Protects either people or fixed locations

• Main functions:
  1. Auditing
  2. Key Management
  3. Access Control
  4. Authentication
For More Information

http://www.rfidguardian.org
Questions?

DOCTOR FUN

TAG! NOW WE CAN TRACK YOUR MOVEMENTS FOREVER!

The new fun game of RFID tag

Copyright © 2003
http://bibli.org/Dave/dfun-html
This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.