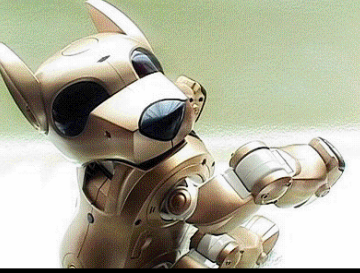


A Hacker's Guide to RFID Spoofing and Jamming

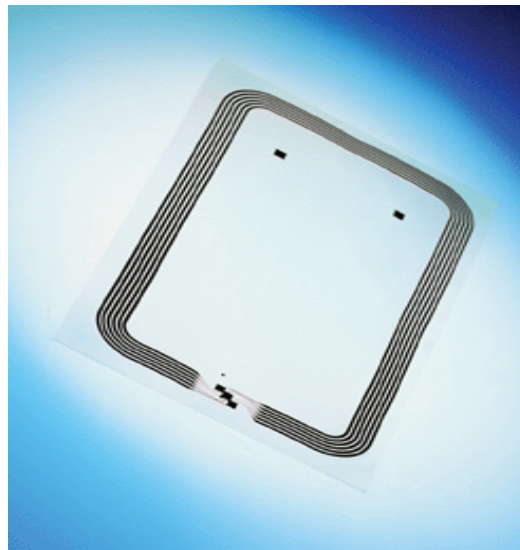


Melanie Rieback
DefCon 14
4 August, 2006



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**





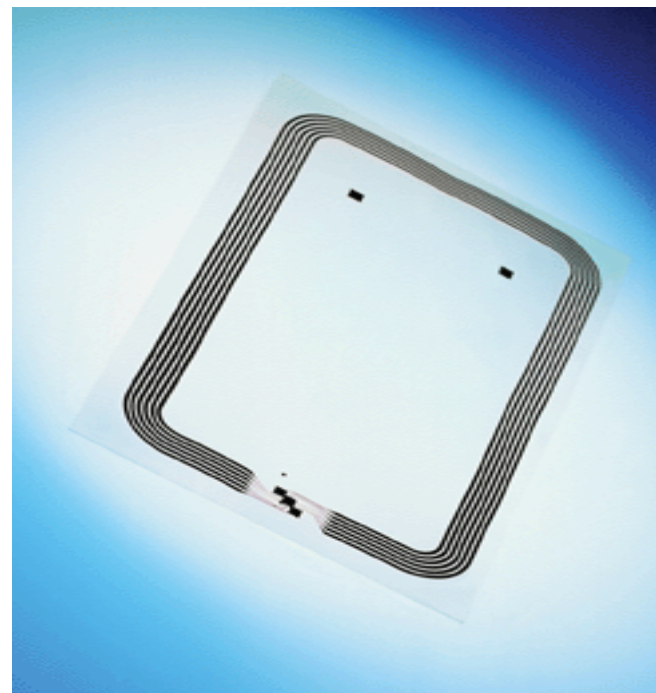
History of RFID Tag Technology

1997 – First all-polymer RFID tag

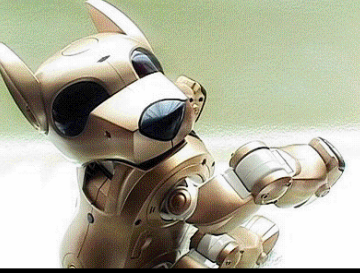
2000 – RFID standards documents emerge

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..**

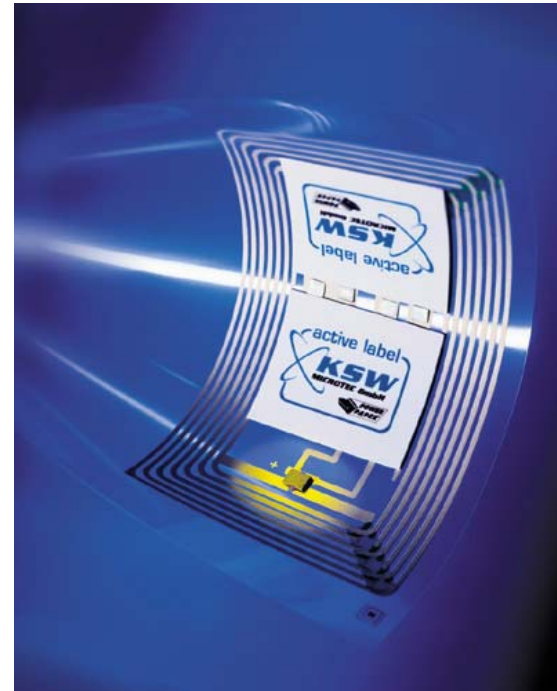


Philips I.Code RFID Tag



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

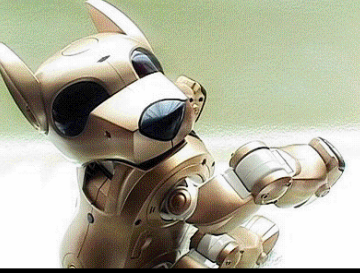


vrije Universiteit amsterdam

Security in Ubiquitous Computing

Modern RFID Applications



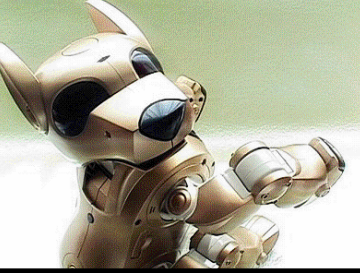


vrije Universiteit amsterdam

Security in Ubiquitous Computing

VeriChips – Subdermal RFID



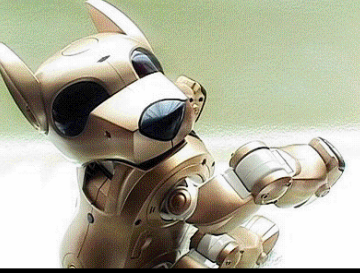


vrije Universiteit amsterdam

Security in Ubiquitous Computing

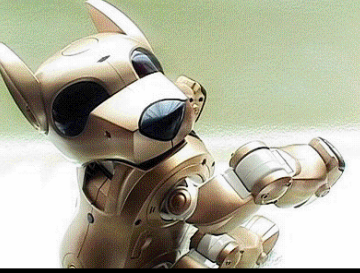
VeriChips – Subdermal RFID





VeriChips – Subdermal RFID



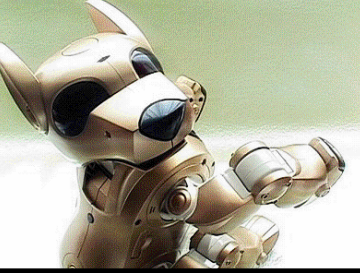


vrije Universiteit amsterdam

Security in Ubiquitous Computing

VeriChips – Subdermal RFID



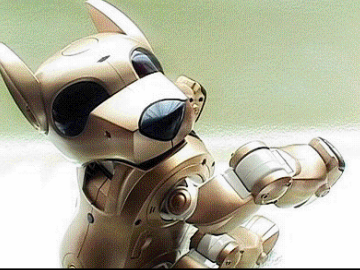


vrije Universiteit amsterdam

Security in Ubiquitous Computing

VeriChips – Subdermal RFID





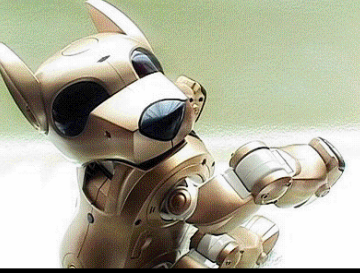
vrije Universiteit amsterdam

Security in Ubiquitous Computing

VeriChips – Subdermal RFID

What about security?





vrije Universiteit

amsterdam

Security in Ubiquitous Computing

VeriChips – Subdermal RFID

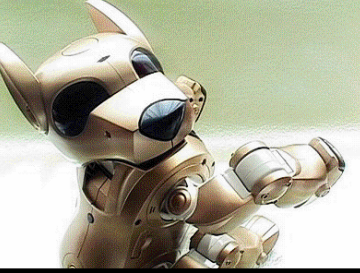
What about security?

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



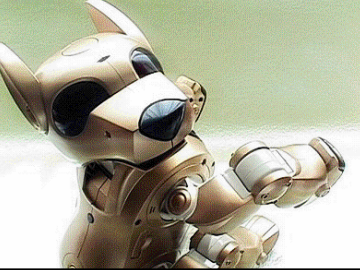
<http://www.siliconvalley.com/mld/siliconvalley/9154114.htm>



RFID Security Problems

Some Security Problems:

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

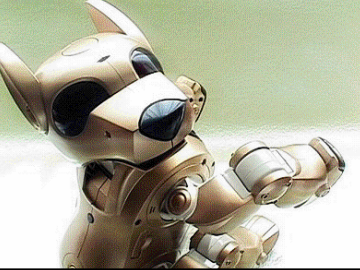


RFID Security Solutions

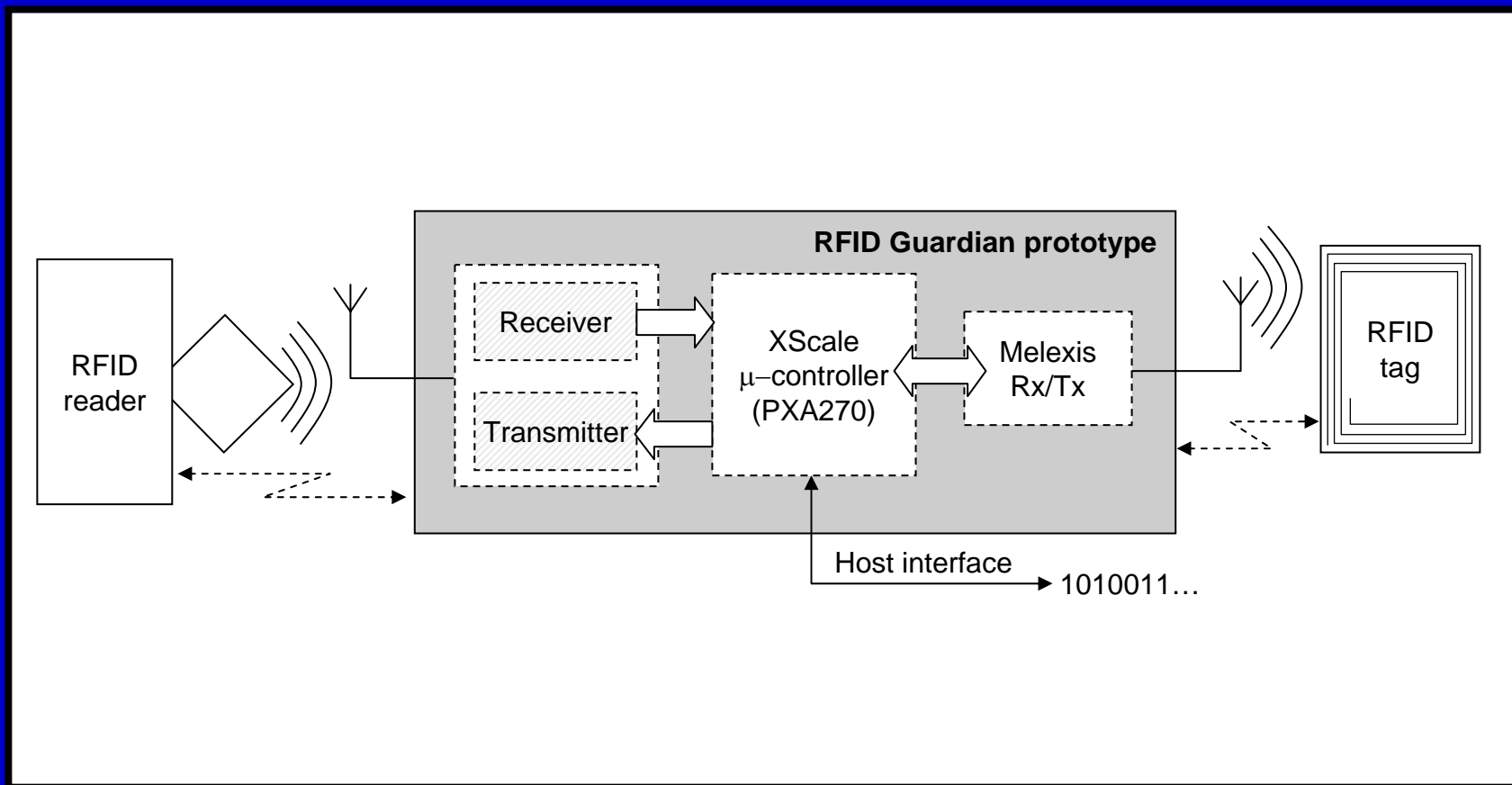
The RFID Guardian

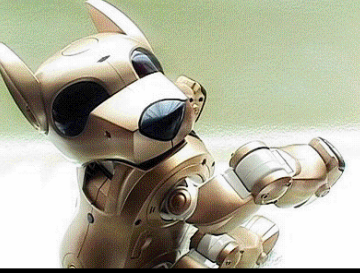
- **Handheld mobile device for personal RFID privacy management**
- **Main device characteristics:**
 1. **Portable**
 2. **Battery-powered**
 3. **2-way RFID communications**



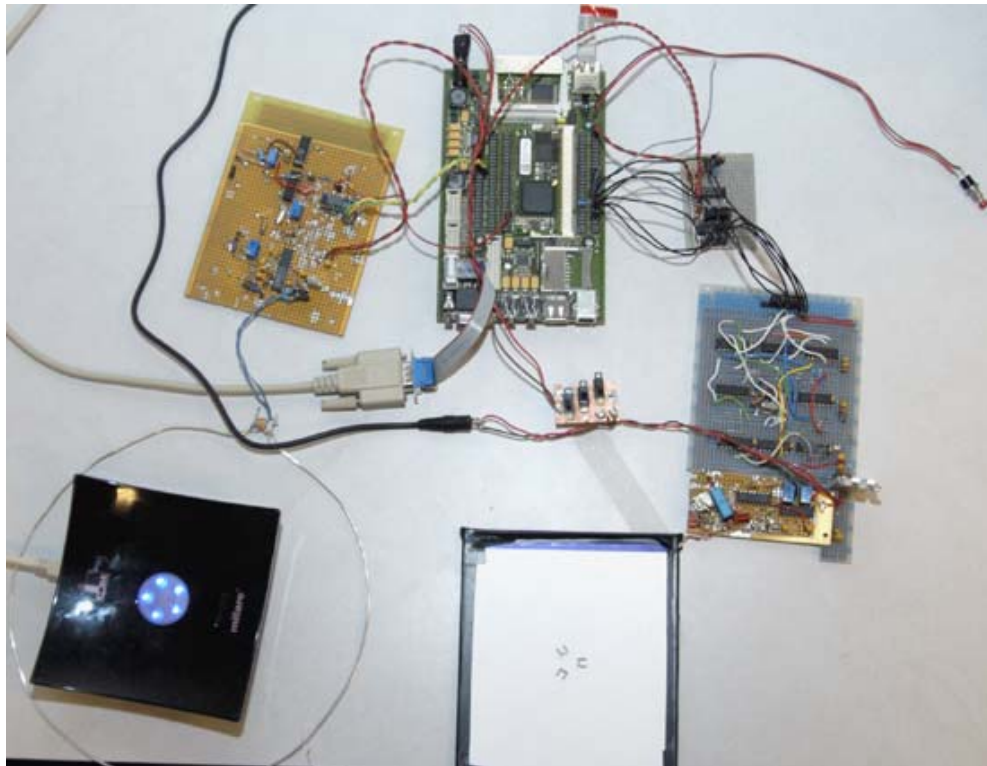


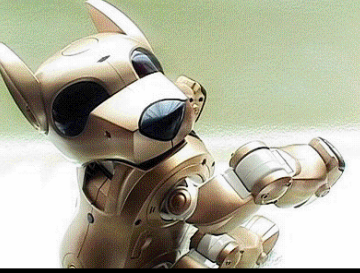
RFID Guardian HW



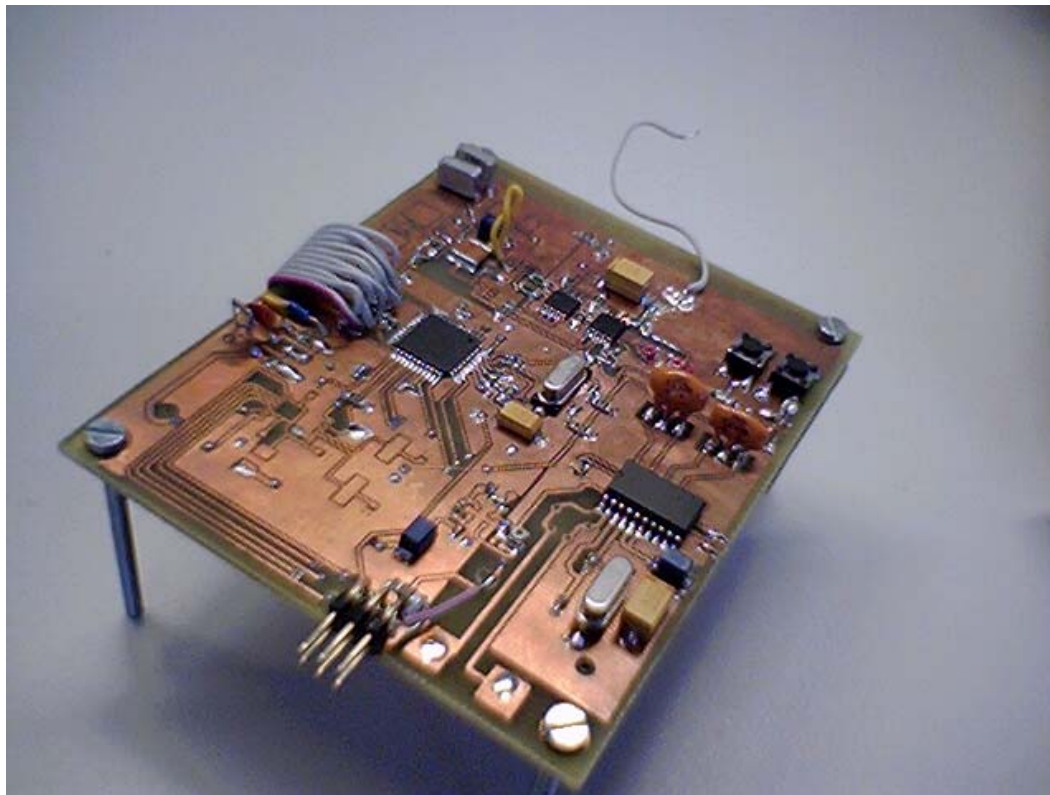


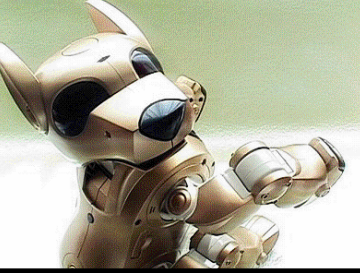
RFID Guardian, V1





RFID Guardian, V2





vrije Universiteit amsterdam

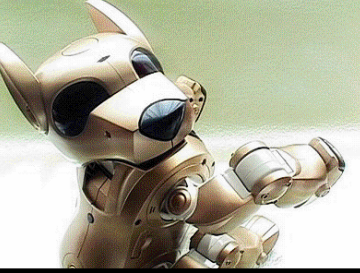
Security in Ubiquitous Computing

RFID Guardian Demo

The RFID Guardian

Vrije Universiteit, Amsterdam





RFID Guardian SW

SW Architecture:

Application-level logic

Data Structures

Tag task

Reader task

UI task

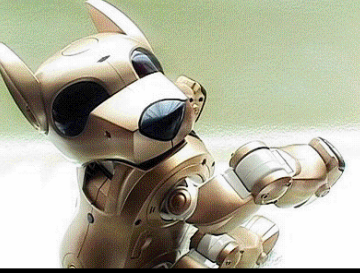
Timer task

Device drivers

RFID (ISO) stacks

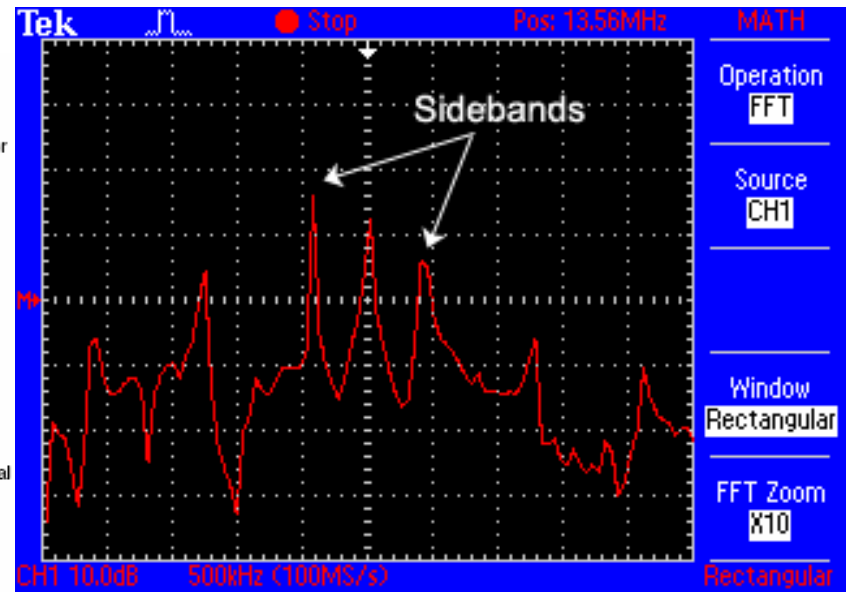
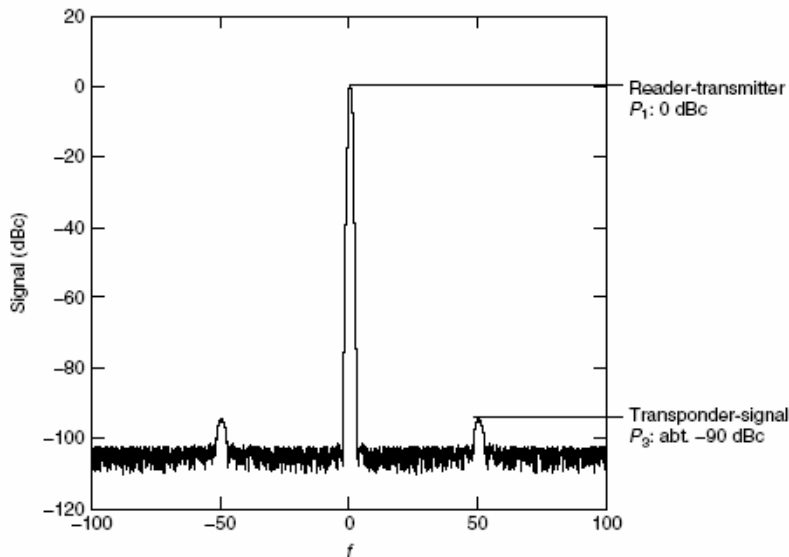
Storage libraries

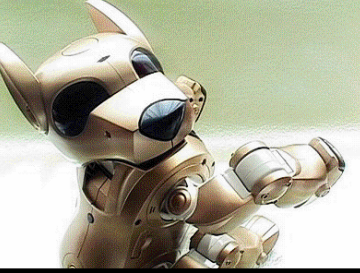
eCOS Real-Time Operating System



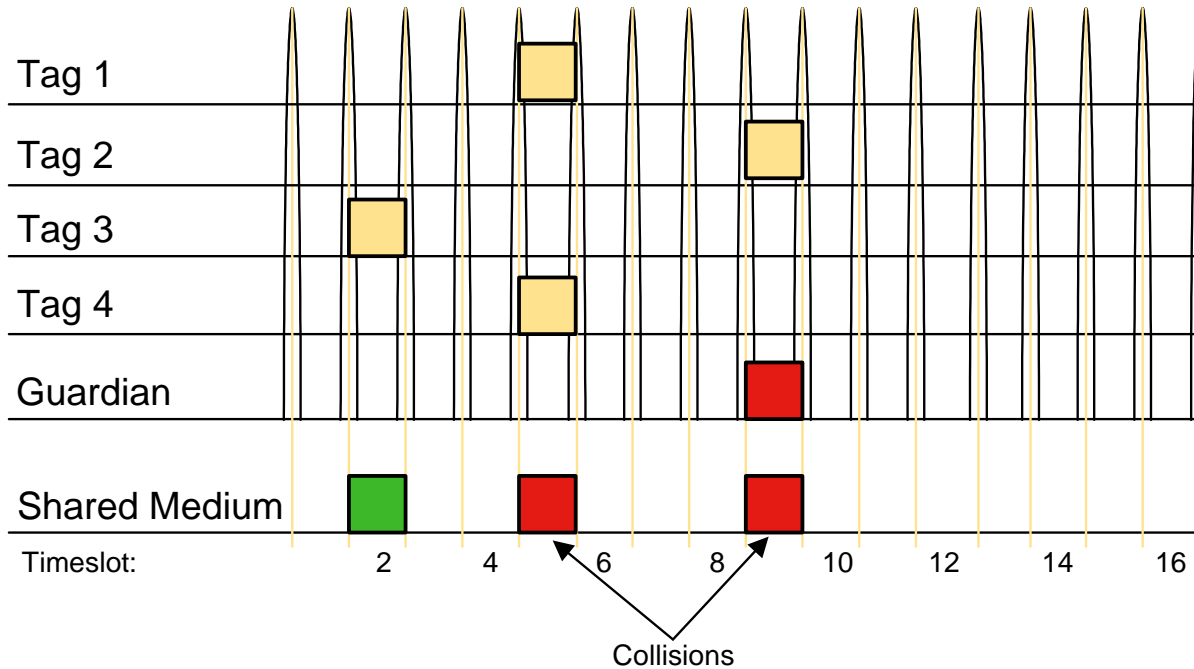
Tag Spoofing

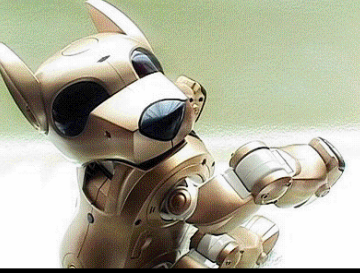
Real vs. Spoofed RFID Tag Response:





Selective RFID Jamming



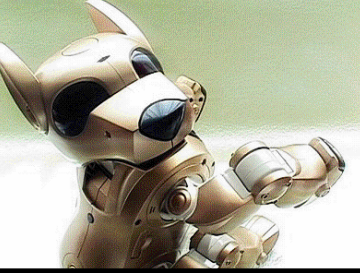


RFID Guardian

Main Functionality:

- Protects either people or fixed locations
- Main functions:
 1. Auditing
 2. Key Management
 3. Access Control
 4. Authentication





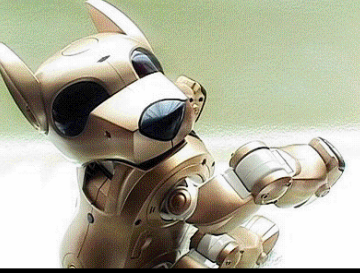
vrije Universiteit amsterdam

Security in Ubiquitous Computing

For More Information



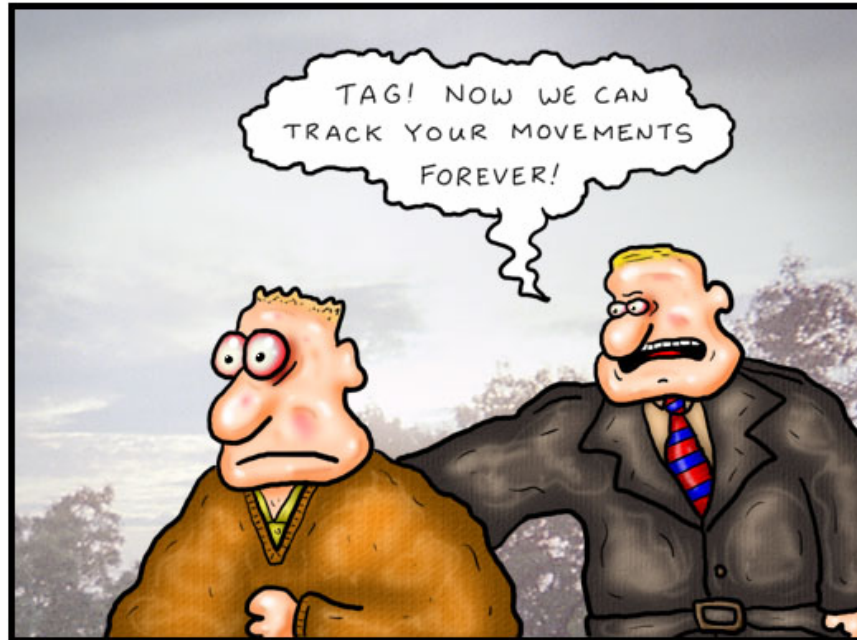
<http://www.rfidguardian.org>



Questions?

DOCTOR FUN

8 Dec 2003



Copyright © 2003 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The new fun game of RFID tag