RFID: Addressing, Event Management and Network Services

Security and Privacy Issues

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Overview

- Security issues
- Privacy issues
- Mitigation

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

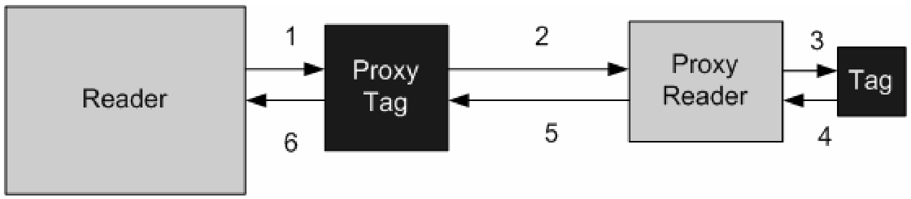
Brute force attack

- Mobile Speedpass key fob
- Uses 40-bit key with Texas Instruments Digital Signature Transponder
- Cracked in using COTS FPGA array (USD 3,500)
- Recovered 5 keys in under 2 hours
- John Hopkins and RSA Labs
- Details http://rfidanalysis.org/

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Relay attacks

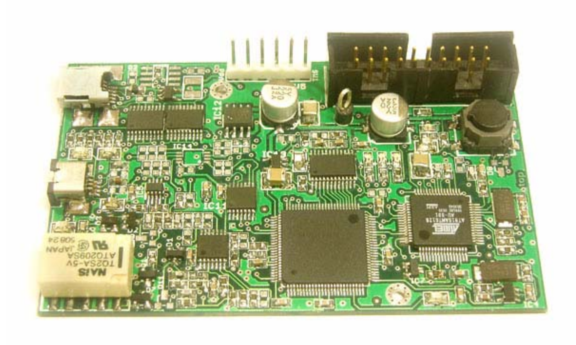
- Classic “man in the middle” attack
- Works because the actual range is far greater in practice
- Theorized in 2005, implemented in 2006
- Simple modifications to COTS equipment
- Distance 2 can be unlimited e.g. mobile communication
- Distance 3 can be up to 4 meters

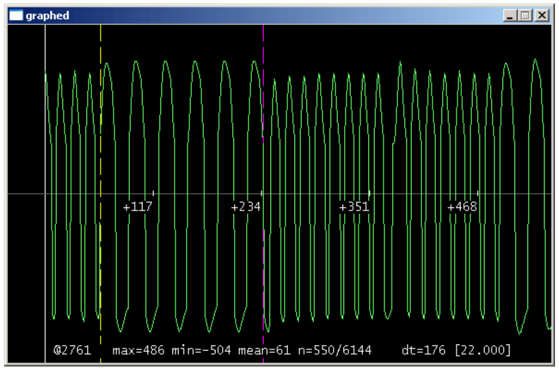


George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Cloning

- Implantable Verichip
- Custom hardware proxmark3
- Capture of transmission
- Analysis of signal (not simple replay) and ID extraction
- Transmission of recorded ID
- Details http://cq.cx/verichip.pl





Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Unauthorized data access

- Poor access control
- Open source software
- Easy availability of portable readers
- Metro Future Store price modifications
- More details at http://www.rfdump.org

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Data injection

- a.k.a. RFID virus http://rfidvirus.org
- Classic buffer overflow attack using EPC data
- Captured public imagination
  - your cat carries a computer virus…
- Limited scope in practice

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Power analysis

- Differential power analysis
- Uses the relationship of changes within the power consumption across the chip with operations within the cryptosystem
  - can recover the key
- "Side channel" cryptanalysis attack against the chip
- Possible but has not been fully developed
- cf. http://www.wisdom.weizmann.ac.il/~yossio/rfid/

ONS attacks

- ONS is running on top of DNS
- very well known vulnerabilities (RFC 3833)
  - packet interception, query prediction, cache poisoning, server betrayal, DoS
  - affect integrity and availability of ONS
- Some limitation of directory integrity concerns due to single domain operation under EPC
- Client access issues completely dependent on correctness of query responses
- Access control of ONS non-existent

EPC IS concerns

- Mostly an open question due to limited deployment
  - standardization ongoing, currently early stage
- Global repository of track and trace information
- Complex access control and trust federation issues
- Availability subject to complex WS application servers
- Edge of the enterprise network issues
- Major privacy concerns

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Privacy debate

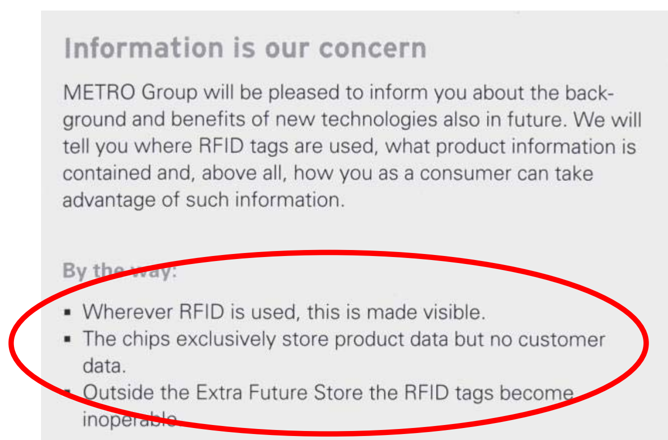
- RSA CEO “would be very worried of his privacy” (quoted by InfoWorld, April 2004)
- EPC Europe VP says “there are more myths in RFID than there are in Greek mythology” (quoted by BBC, April 2004)
- Sisley trial (Sisley is a Benetton brand)
  - Announced 11 Mar 2003,
  - CASPIAN calls for boycott 13 Mar 2003,
  - Sisley withdraws plans 15 Mar 2003

  (details at http://boycottbenetton.org)

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Real problems

- Metro Future Store
- http://www.future-store.org
- Violations of own privacy statements



Information is our concern

METRO Group will be pleased to inform you about the back-ground and benefits of new technologies also in future. We will tell you where RFID tags are used, what product information is contained and, above all, how you as a consumer can take advantage of such information.

By the way:

- Wherever RFID is used, this is made visible.
- The chips exclusively store product data but no customer data.
- Outside the Extra Future Store the RFID tags become inoperable.

Two Major Issues

- System operation is transparent
  - invisible, everywhere computing
  - guarantee the rights of consumers
- Trust is a non-cognitive process and thus is hard to compute with (trust is different to trustworthiness)
  - overall acceptance of RFID retail depends on whether it is perceived as "fair" by consumers
  - strategy cannot be based on expected public apathy because this can backfire cf. nuclear power

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Transparent Operation

- The product contains an RFID tag
- Option to remove or destroy tags when product is purchased
- No penalty for opting out of RFID use
  - Price discrimination
- Access to information and mechanisms for modification of erroneous information
- Notification of RFID monitored areas

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Three Decisions

1. Initial entitlement:
   - Allocation of property rights
   - Who should get the initial right to control the information generated by RFID?
2. Coercion and choice:
   - If you want discount you will get the chip.
3. Societal overrides:
   - When does society, regardless of your preference, get access to the data anyway?

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Mitigation

- Physical destruction of the tag
- Use strong crypto
- Use radio-opaque enclosures
- Disarm
- Clipped tag

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Crypto

- Weak encryption is not a unique RFID issue
- Low computational capability has led to weak choices e.g. symmetric and short keys
- Moore's law already allows for stronger crypto
  - AES implementation possible (TU Graz)
- Usual advice holds:
  - avoid proprietary/closed algorithms
  - unfortunately most tags use them (TI, Phillips)

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Enclosure

- Metal enclosures absorb the signal and prevent communication
- Solid enclosure
  - e.g. duct tape
- Wire frame creates Faraday cage which has same effect
  - US passport, shopping cart

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London

Disarmament

- EPC Gen2 Kill command
- Primarily a privacy and anti-counterfeiting mechanism
- Technical implementation left to device manufacturer
- Can be achieved via
  - Blowing an embedded fuse, following issue of correct “kill” string
  - Set a “killed” value in memory, disabling the protocol state machine
- Usually the second option is implemented which still leaves the tag vulnerable to power analysis attacks
- Clipped chip

Mobicom 2006 tutorial
George Roussos
g.roussos@bbk.ac.uk
Birkbeck College, University of London