Mobile and Ubiquitous Computing
Privacy, Security and Trust

George Roussos
g.roussos@dcs.bbk.ac.uk
Overview

• Security of RFID
• Privacy and UUIDs in RFID
• Location data and analytics
• Can we trust mobile and ubiquitous systems?
Unauthorized data access

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

- Implantable Verichip
- Custom hardware proxmark3
- Capture of transmission
- Analysis of signal (not simple replay) and ID extraction
- Transmission of recorded ID
- Similar device for HF tags is the HF Demotag
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
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
Resolution service attacks

- Object Naming Service (EPCglobal) and OID Resolution Service (ISO)
  - developed on top of DNS
- Inherit well known vulnerabilities (RFC 3833)
  - packet interception, query prediction, cache poisoning, server betrayal, DoS
  - affect integrity and
- 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
Tracking

• Mostly an open question due to limited practical experience
  – Lessons to be learnt from location privacy
• EPC Standards describe global repository of track and trace information
• Complex access control and trust federation issues
• Major privacy concerns
RFID Constellations

The consumer privacy problem

Mr. Jones in 2020...

- Replacement hip medical part #459362
- Wig model #4456 (cheap polyester)
- Das Kapital and Communist-party handbook
- 1500 Euros in wallet Serial numbers: 597387, 389473...

Juels, 2005
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
Real-world problems

• Metro Future Store
• http://www.future-store.org
• Violations of own privacy statements
Strong sentiments
True concerns
Participatory Applications

Participatory Air Quality Sensing

Sense Networks
www.sensenetworks.co
Gaming and healthcare

Uncle Roy All Around You

Equator

Medical Body Wireless Sensor Networks
Significant locations

- Identify significant places
- Use mobile phone location records
- Identify hot-spots of activity
- Time specific
- Commercially available through Sense Networks
- Track real-world consumer behaviour

sensenetworks.com
RFID Analytics

- RFID-tagged products and locations
- Scan traffic at specific chock points
- Analyse traffic and identify hot-spots or problem areas
- Visual tools
- Different spatial resolution

Illic et al, Auto-ID Lab Zurich
Social networks

- Observe social networks in the real world
- Tag and rank location of individual
- Identify meetings through collocation or device-to-device interaction
- Create social network graph
- Conduct analysis
- Reality mining data set

Shen et al, UC Davies
Patterns of behaviour

• Identify typical behaviours
• Possibly context and task specific
• Applications in navigational assistance, personalisation, recommendations
• Best-trails i.e. most popular pathways followed
  – GPS data from London Zoo
• Daily activity patterns
  – Reality Mining data

Experience Recorder

Shen et al, UC Davies
Prediction

• Predict driver destination
• Use dense grid to identify locations
• Metric representations of space extremely costly
• Machine learning to identify common behaviours
• Used for navigational assistance

Krumm et al
Microsoft Research
Navigational assistance

- Find best route between two places
- Use data from an expert data set
- Taxi drivers are considered experts in this task
- Navigate like a cabbie
- Similarities of geographic navigation and web navigation
Summarization

- Reduce a complex data set to typical behaviours
- GSM tracks over metropolitan area
- Cluster typical behaviours in profiles
- Use road graph to identify sequences
- Topological descriptions of space are more efficient

Adrienko et al
Fraunhofer IAIS
Points of Interest analysis
Using all trails in the data set.  
Using best trails only.

Using wifi traces from the Dartmouth and RM datasets.
Identify individual without ID

Reality-mining data set
Identify user 39 using 2 months for training and test on next month
Privacy in the US

The right to be Let Alone:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fourth amendment of the Bill of Rights
Privacy in Europe

• Honour and dignity in the public sphere
Everyone has the right to respect for his private and family life, his home, and his correspondence

European Convention of Human Rights
Two Major Issues

• System operation is transparent
  – invisible, everywhere computing
  – guarantee the rights of consumers

• Trust is an emotional process (trust is different to trustworthiness)
  – overall acceptance of MUC depends on whether it is perceived as used fairly
  – strategy cannot be based on expected public apathy because this can backfire cf. nuclear power
Trusting RFID: Assessment

• Privacy Impact Assessment Framework
• A principled method for assessing threats to privacy for the general public
• Initial stage of EU mandate on RFID
• Very limited uptake
  – often accused as too onerous or costly
• Includes provisions for RFID emblem
  – similar to CCTV notification
Regulation

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?