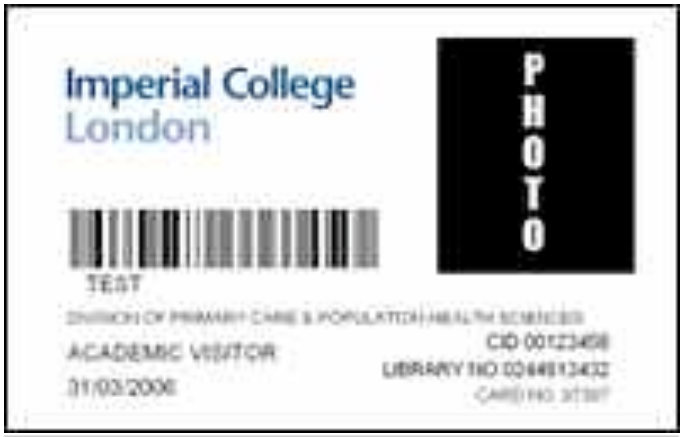
What's In Your Wallet?
RFID: Operation and Security

Rob Shakir (rjs205@ic.ac.uk)

You're already carrying RFID tags.



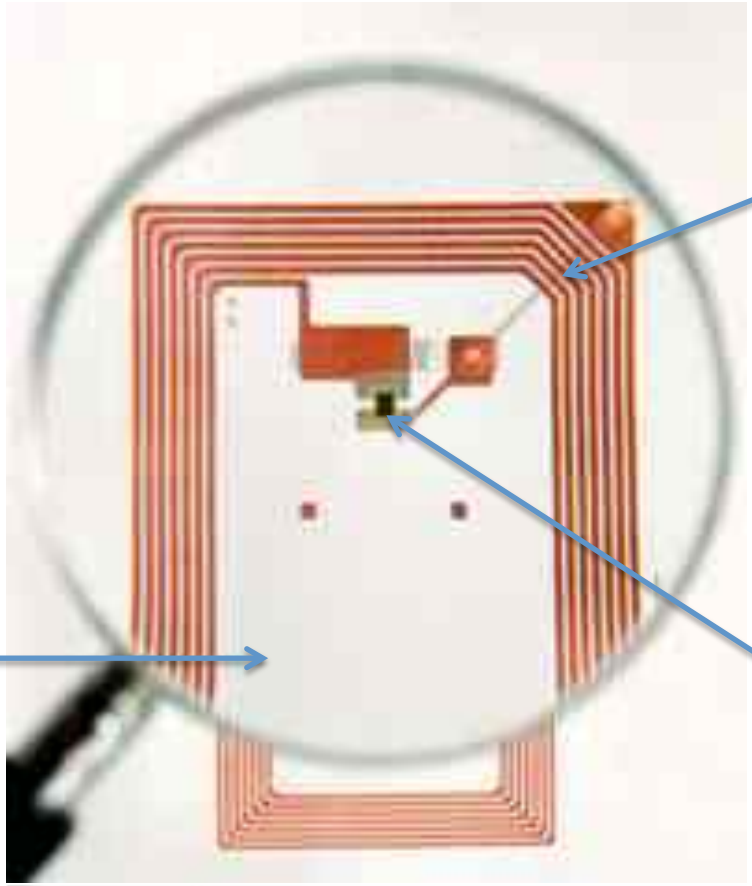
http://www.segway.com/blog/wp-content/uploads/2007/06/oyster-card.jpg http://www.ips.gov.uk/passport/images/biometrics4.jpg http://www3.imperial.ac.uk/pls/portallive/docs/1/7274500.JPG

RFID: The Basics

- Radio Frequency IDentification
  - Passive/Semi-Passive/Active tags
  - Reader

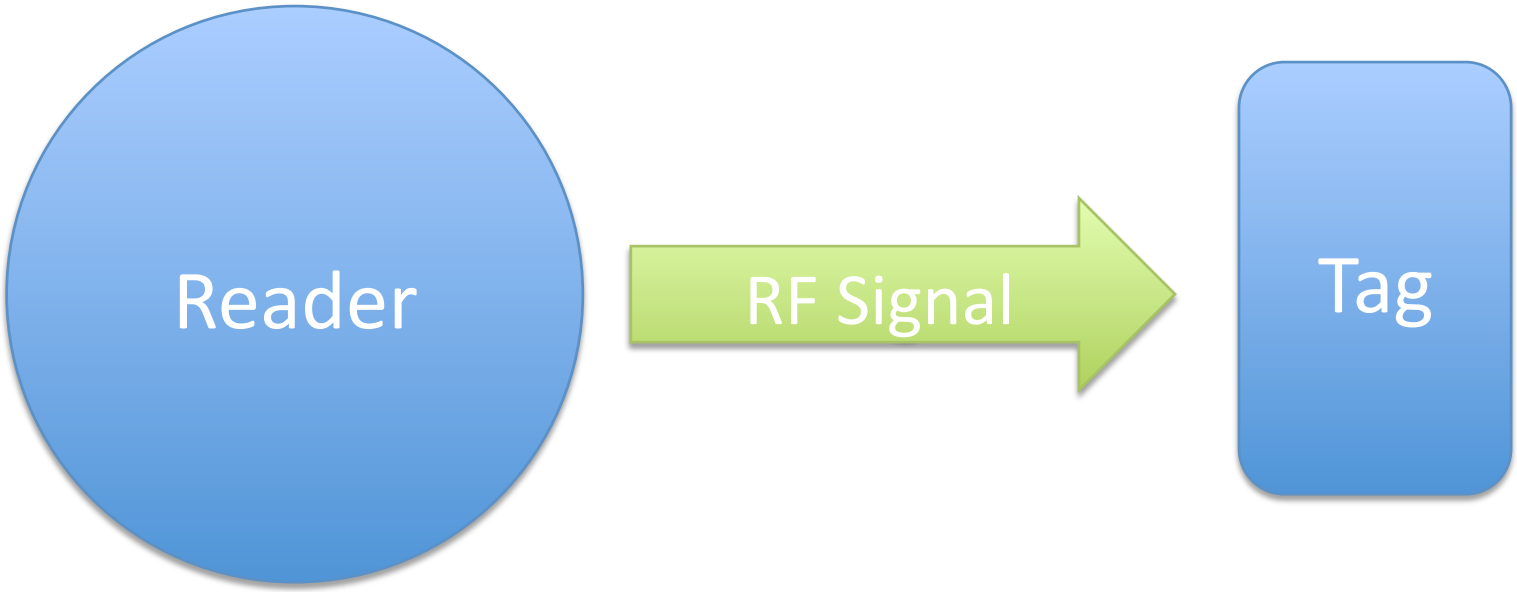
- Key concepts
  - Faraday's law – induction.
  - Near-field/Far-field for RF waves.
  - Digital Signal Processing.

Passive Tags – How do they work?

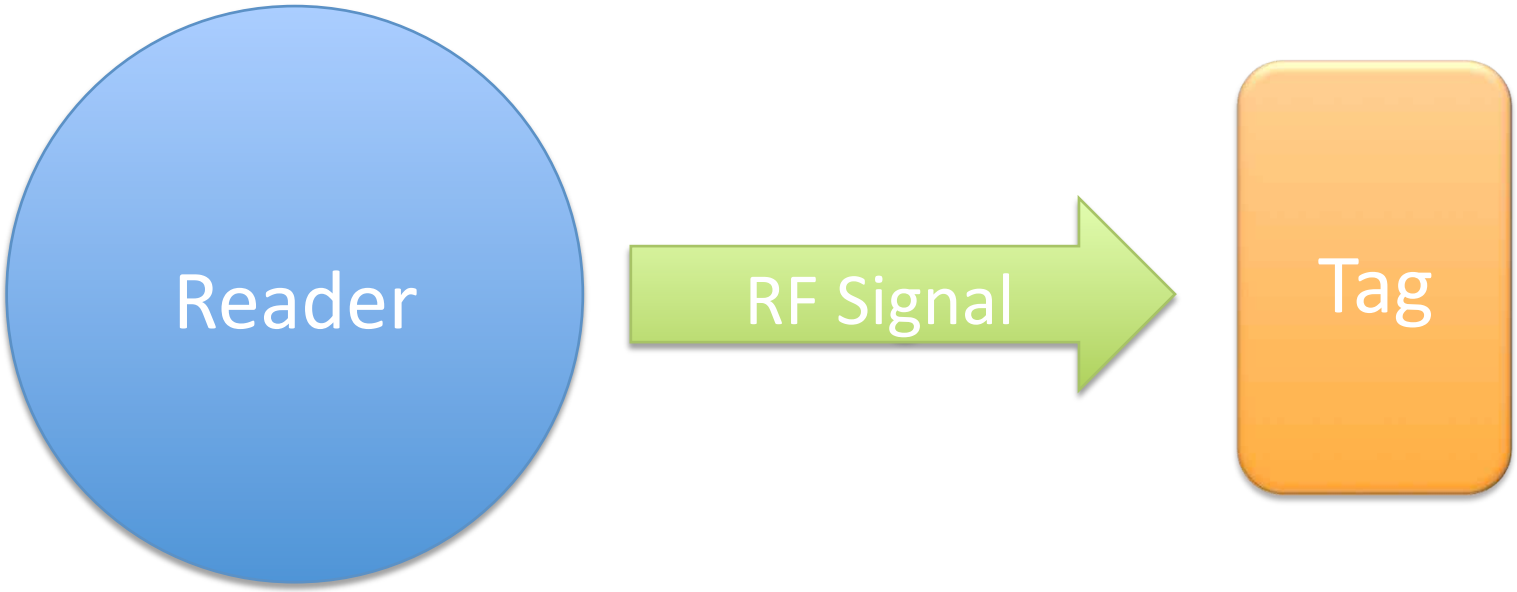


http://static.howstuffworks.com/gif/rfid-2.jpg

Passive Tags – Reading (High f)

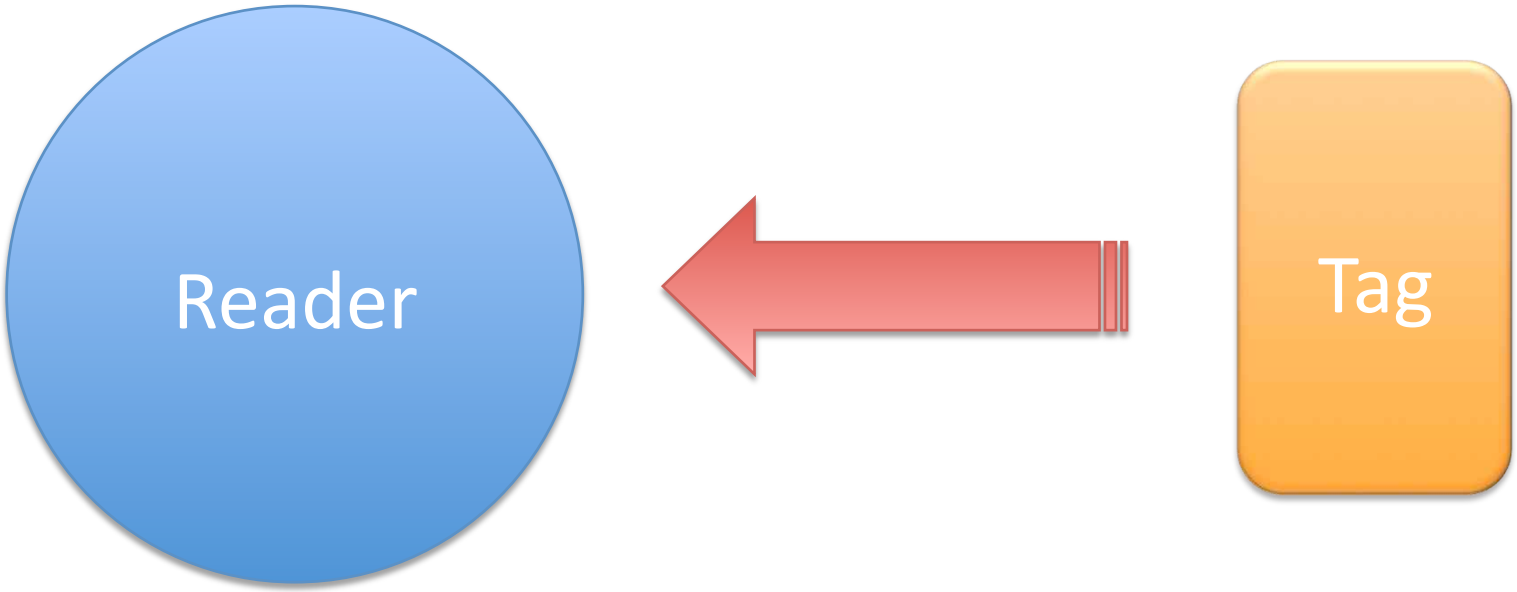


Passive Tags – Reading (High f)



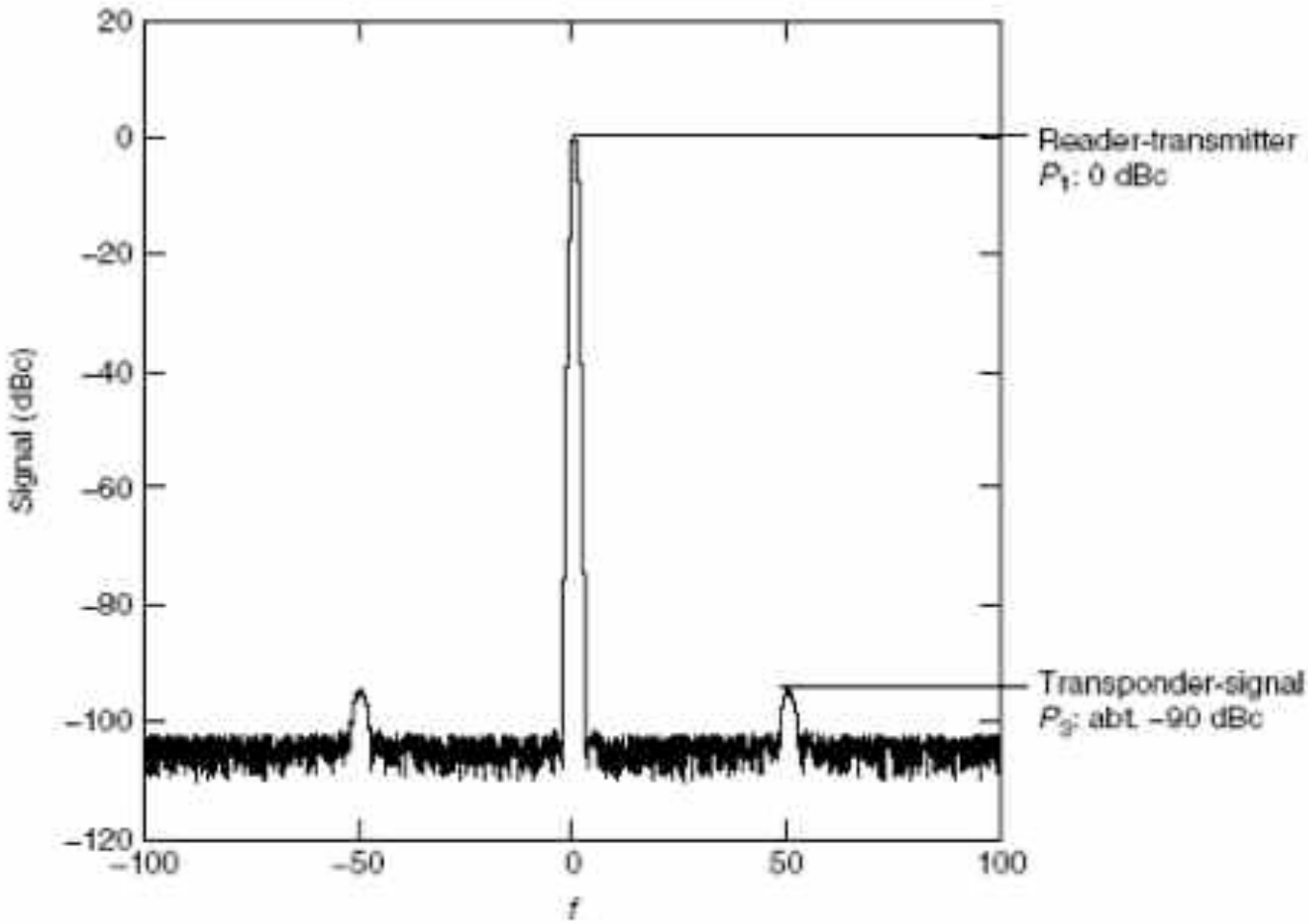
Tag Powered On

Passive Tags – Reading (High f)



Modulated Signal Reflected

Passive Tags – Reading (High f)

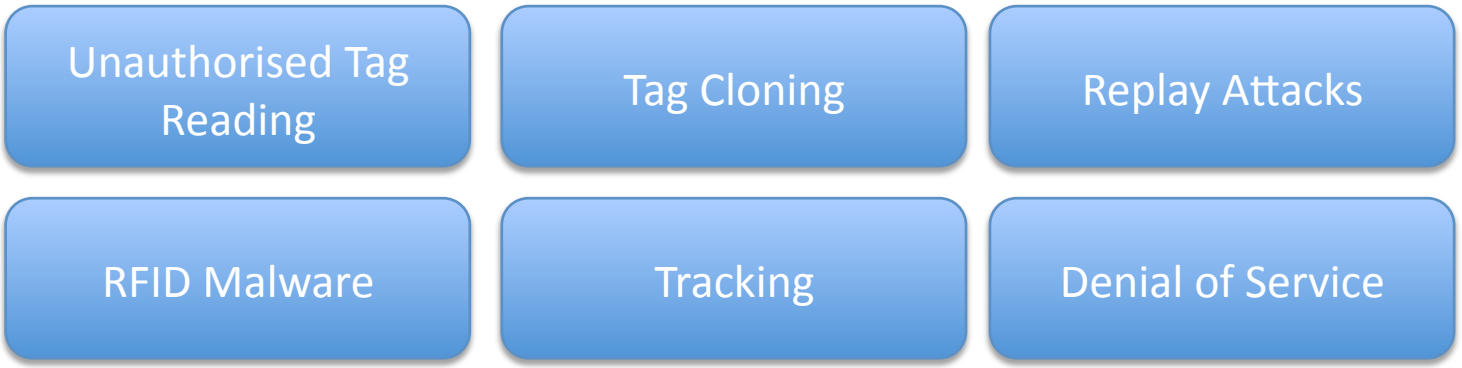


More Advanced Passive Tags

- Tags discussed just give an ID.
  - Vulnerable to many attacks.
- Handshake protocols
  - e.g. Oyster
- Writeable Tags
  - Store data on the tag (not just an ID)

Hacking RFID

- So, you have a VeriChip (RFID chip) implanted in your arm…
  - "Applied Digital's implantable chips do not employ cryptography as of yet." (http://www.siliconvalley.com/mld/siliconvalley/9154114.htm)



Crypto isn't safe either…

- Oyster (Mifare, 13.56MHz)
  - Reverse engineered crypto circuits.
- British Passport
  - Cracked (~40 minutes!)
- Standard cryptographic problems, or RFID specific?

A Radio-Frequency Firewall?

- Metals (e.g. tin foil)
  - Skin depth

- Much more sophisticated methods
  - RFIDGuardian

In Summary

- RFID has many uses.
  - Stock control, ticketing systems, safety, access…
- Technically, very simple.
  - Some challenges, e.g. auto-collision.
- Big problems with security?
  - Need to be aware of the problems.

Questions? Comments?

RFID: The Key to Automating Everything – Roy Want, Scientific American, January 2004

The RFID Handbook - Klaus Finkenzeller. John Wiley & Sons, 2003.

Practical RFID Attacks –Milosch Meriac, Henryk Plötz – CCC '07 (2007-08-10)

MIFARE – Little Security, Despite Obscurity – Karsten Nohl, Henryk Plötz, 24C3, 2007-12-28

M.R. Rieback, B. Crispo, A.S. Tanenbaum. *"Is Your Cat Infected with a Computer Virus?"* Proc. 4th IEEE Intl. Conf. on Pervasive Computing and Communications. (PerCom 2006), Pisa, Italy, March 2006.

M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. *"A Platform for RFID Security and Privacy Administration"* 20th USENIX/ SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006

Additional Slides

Q&A

Q: Why don't we encrypt tags (better)?

A: Building crypto electronics is hard at this size.

- We have 3DES cards (MIFARE DESFire)
  - Good standard of encryption.
  - Cost per card increases.
- 3DES still not perfect.
- Limited memory means limited key length.
  - Limits the best security we can get (AES not practical)

Q: So, is RFID useless?

A: Definitely not.

- Oyster not yet cracked (easily)
- Replay attacks can be impractical
- Many attacks require timing control of the reader
  - Generally not available when attacking.
- But brute-force attacks need to be dealt with.

Q: So, how does Oyster work?

A: We don't know exactly (not published).

- 1KB storage on card (MIFARE Standard)
- 48 bit cipher, encrypted with a key agreed during challenge-response conversation.
- Card stores journey details.
- Consolidation of card details with central database daily.

Q: Imperial IDs and Oyster interfere, why?

- Both are MIFARE 13.56MHz tags (I think!)
- Collision between the reflected signals.
- Design error (probably by Imperial College)
- Can be stopped by putting tinfoil between the two cards (as discussed earlier).

Q: I want to play with RFID, where should I look?

- Chaos Computer Club's (ccc.de) conferences are really good for RFID discussion
  - http://events.ccc.de/
- Popular science magazines give a good overview.
- OpenPCD.org – an open source 13.56MHz reader/writer.
- OpenPICC – sniffer/replay device.