Additional Topics: RFID

Dr Robert Harle

CST Part II

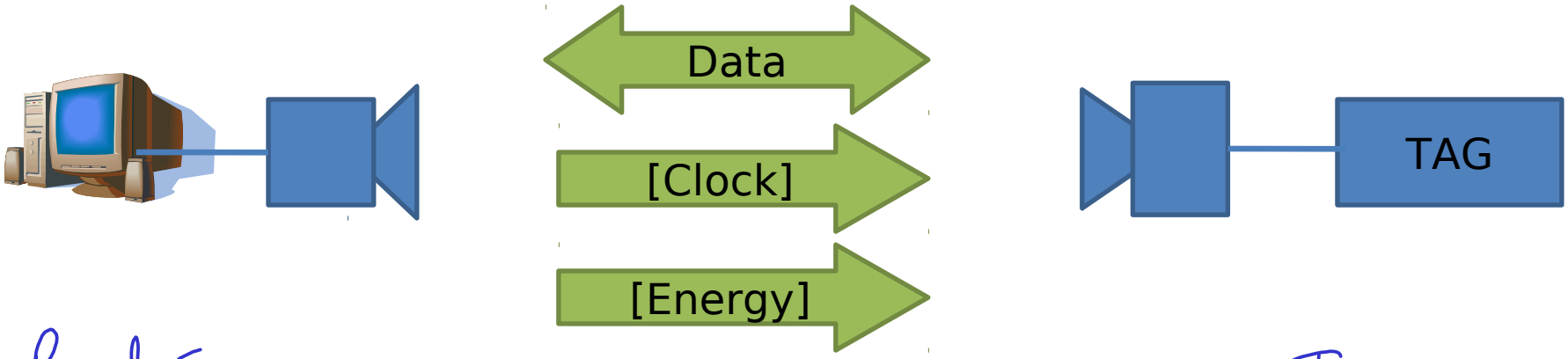
Easter 2009/10

What is RFID?

- Radio Frequency Identification
- An RFID tag is a device that can be identified without physical contact using electromagnetic phenomena
- Note how general this definition is

- Depending which newspapers/websites you read you could be forgiven for thinking RFID tags are the spawn of satan.
  - Unfortunately, the writers in the press are often rather ignorant and more than a little sensational!

Principles



Reader

Coupling medium

Tag

- ID
- Contain data

Active Tags

Disadvantages

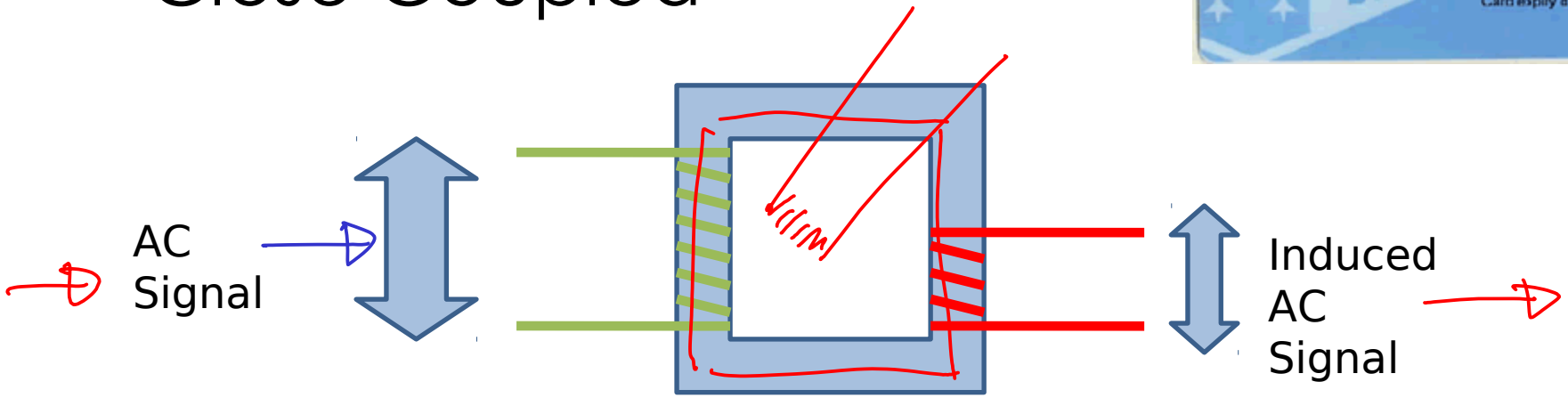
- Not 'cool'
- Battery adds size
- Battery will run out eventually...
- Battery adds cost (harder to manufacture, more components)
- Battery adds weight

Advantages

- Reliable communications
- Better range (powered antenna)
- Better capabilities (powered processor)
- Stateful (can power memory)

Types of Passive Tag

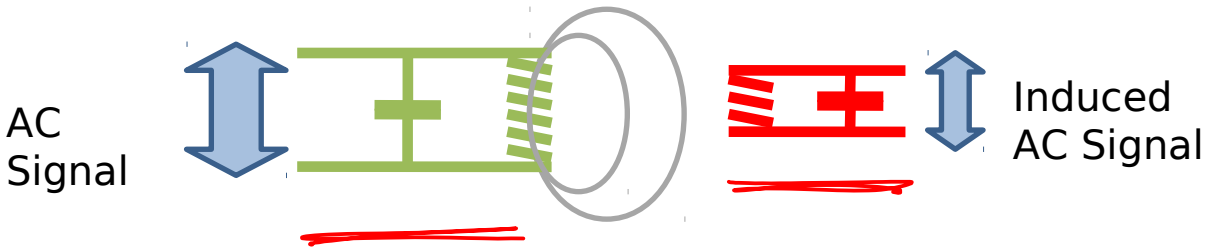
- Close Coupled



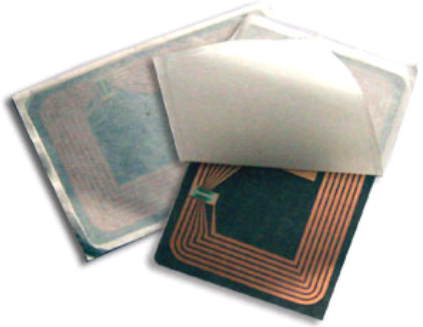
- Ferrite core gives good power transfer
- Typical range **< 1cm**
- ~30MHz freqencies
- Communication possible through mutual inductance. The tag connects/disconnects a coil to alter the induced current in the reader and transmit data

Types of Passive Tag

- Remote-Coupled (Inductive)



  - Typical range < 1m
  - <135kHz, 13.56MHz
  - Power not as reliable as before so we can't do as much
    - Can usually support local memory

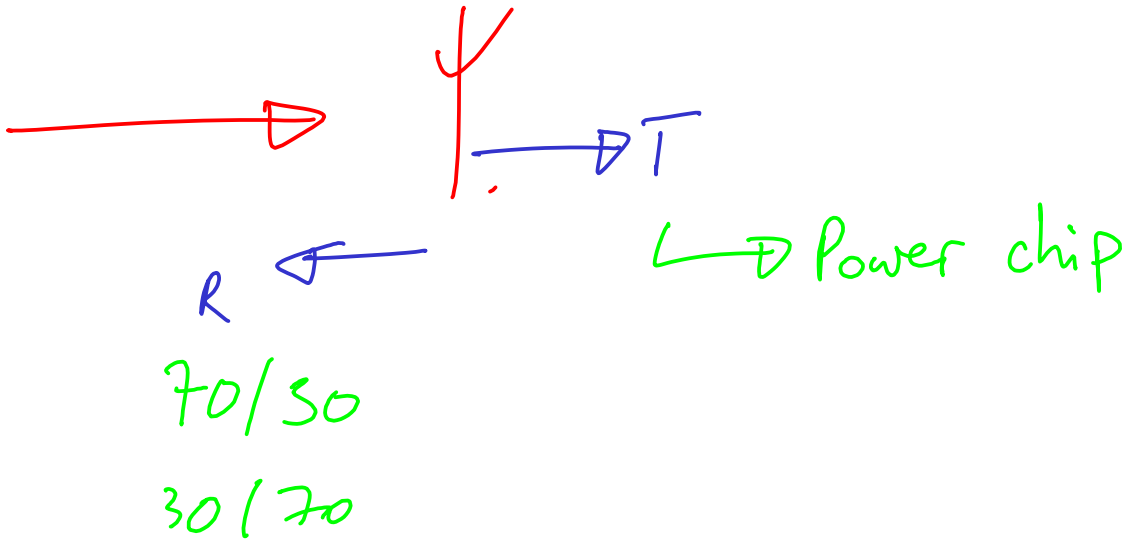


Types of Passive Tag

- Long Range "RFID
  - Need to use far-field EM waves
  - UHF (100s of MHz)
  - Microwave (GHz)

- But radio transmitters kill batteries fast
  - And we don't even have a battery!
  - Use backscattering...

Backscattering



Switch electronics ⇒ change impedance

⇒ alters R/T balance

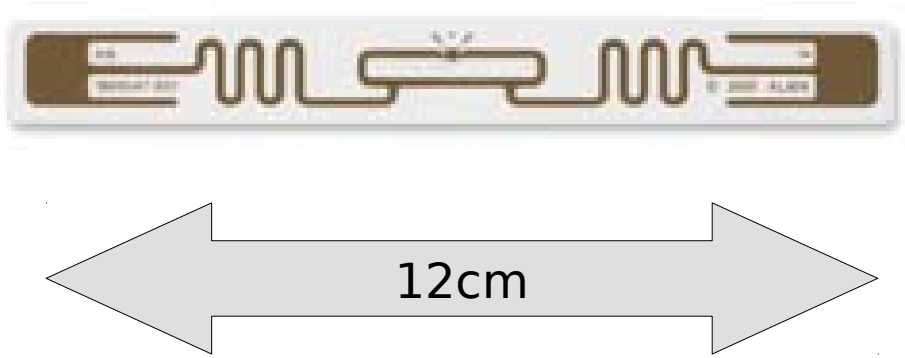
Backscattering

- So each tag has a unique identifier
- When instructed by the reader, it spits out the serial number by encoding it on the reflected signal by switching its impedance ("load modulation").
- More advanced tags may support a small number of other commands such as "shut up" or "get data" (if the tag is advanced enough to carry extra data)

Properties

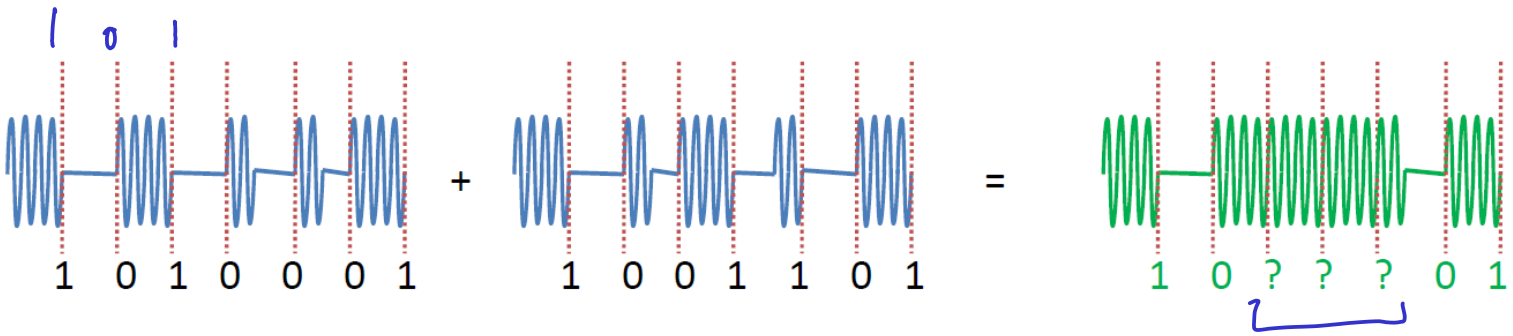
- Tags up to 3GHz exist (most use 900MHz)

- Read ranges are usually around **3m** (10m for high powered directional antennas)
- Depends on environment and reader power



Tag Enumeration ("Singulation")

- Most common task is to find all the tags that are within range.
- Since the tags use the same incident signal to 'talk', they all end up talking at the same time
- First trick is to use manchester encoding to spot the collisions



- This tells us the bit positions where collisions occur

Binary Tree Walking

- To actually enumerate, we usually use binary tree walking

  1. Request that all tags identify themselves
  2. Detect collisions in the response
  3. Now walk over a binary tree to figure out the collision bits

- All we need is a special reader command: **[REQ | bbbb]** : all tags with an ID less than bbbb (i.e. binary integer) should reply

Example

Tags: 1000 1100 1101

① [REQ | 1111]

1000
1100
1101

1X0X

② [REQ | 1011] → 1000

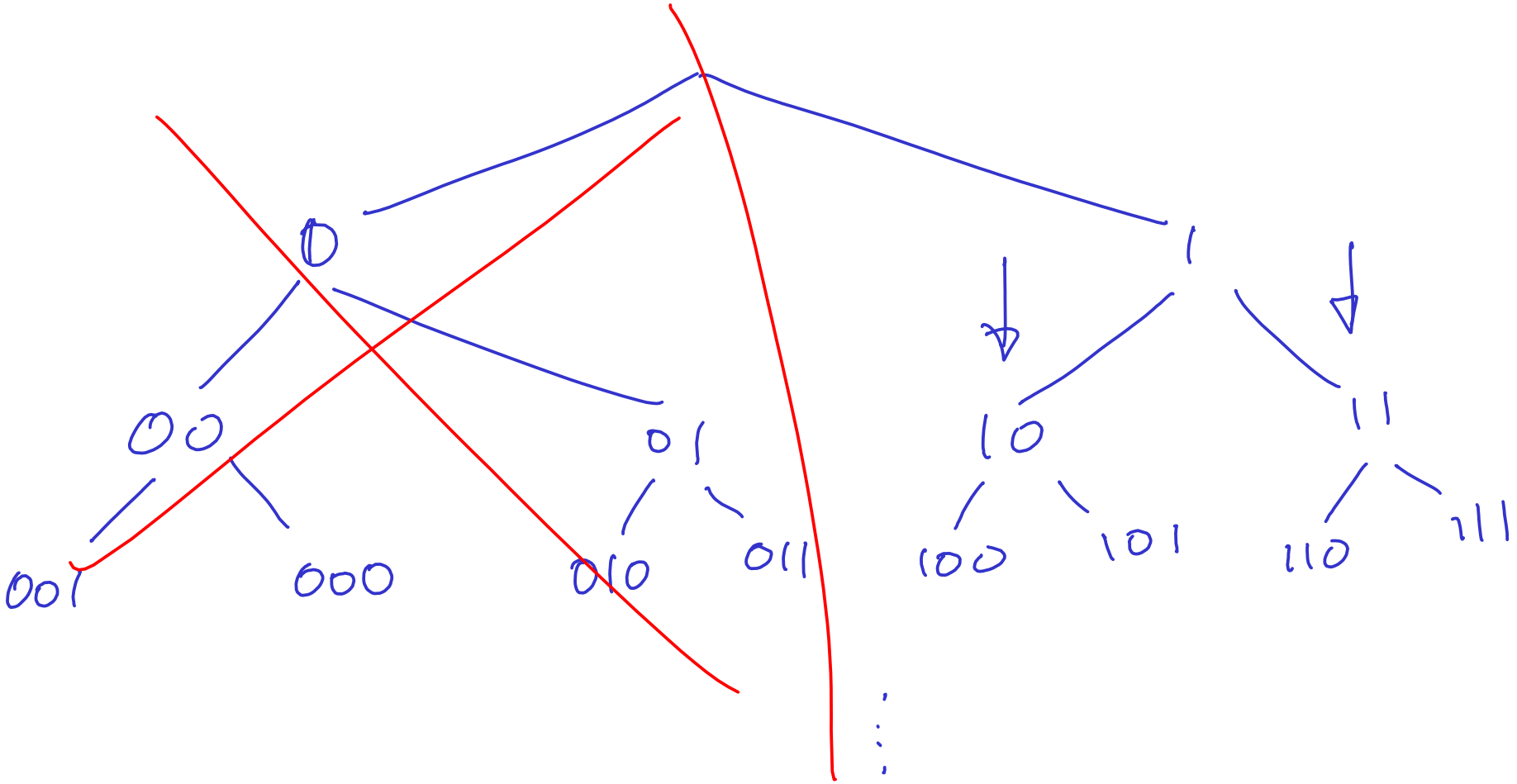
③ [REQ | 1101] → 110X

1100

1101

Example

Tags: 1000 1100 1101



Issues: Radio Power

- A radio signal has to travel to the tag, and then back (having also lost power in the reflection) so we have to start with something quite powerful at the reader
- In fact, today's readers pump out as much as 4W of radio power
  - Wifi base stations are restricted to 100mW
  - A GSM 1800MHz phone handset is restricted to 1W
  - A DECT handset is restricted to 250mW
  - And these are peak powers (on average DECT produces 10mW); RFID readers have a constant power output...
  - *This might all be perfectly safe but it's not 100% clear - any volunteers to test?*

Issues: Orientation

- It turns out that the orientation of the inexpensive passive tags strongly affects the strength of the reflected beam to the reader

"Tag orientation also impacts read range. Whenever possible, try to vertically orient dipole tag antennas. Horizontal orientations are prone to miss-reads..."

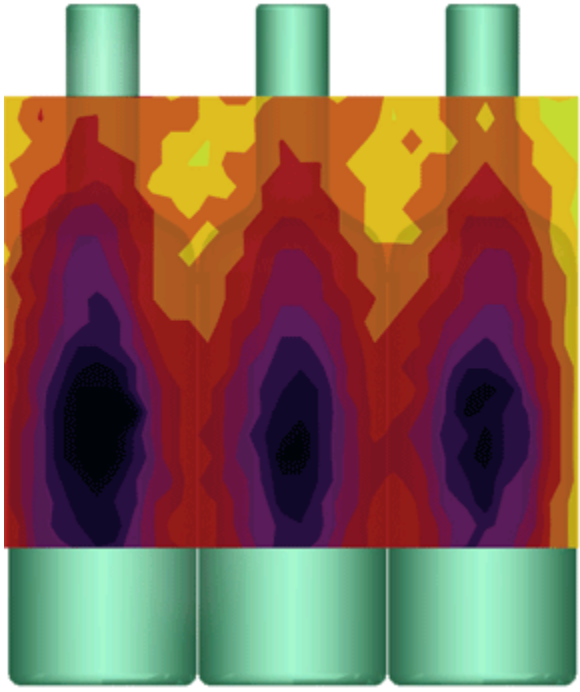
Alien whitepaper.

- This means a random assortment of tagged items (as per a shopping trolley) is very unlikely to be read 100% and this can be serious
  - Who is responsible if you walk out with a 50" plasma and the system misses the tag..?
  - For some apps you can control the orientation (e.g. baggage in airports or on palettes of goods).
    - Reports suggest 99% accuracy possible with lots of fine tuning
    - What about that other 1%..!

RFID in Use…

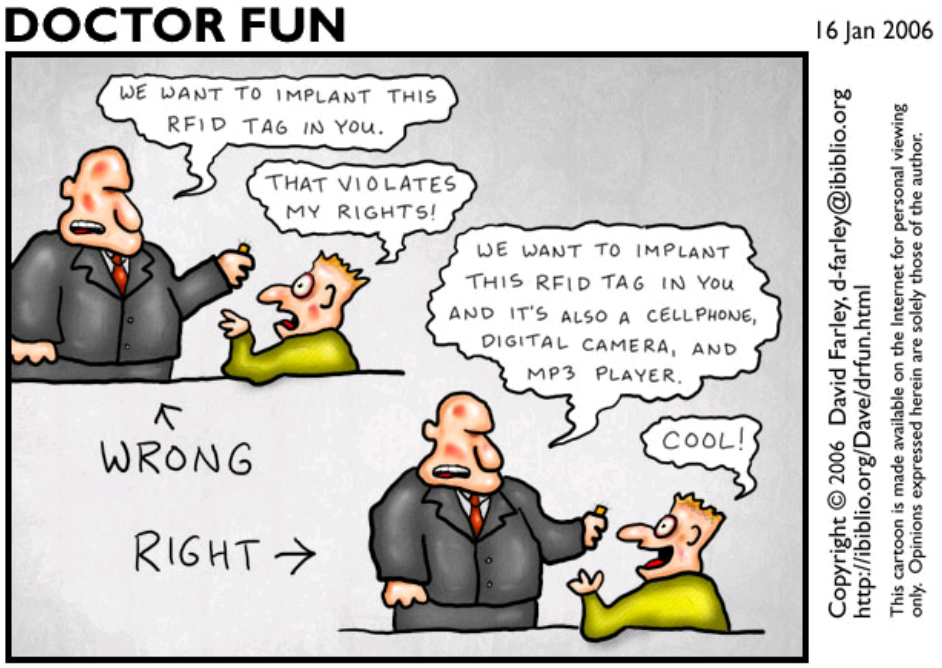
Issues: Interference

- An attached object can affect the quality of the tag response. The image below shows responses measured at the Auto-ID research labs in Cambridge
- Passive tags were attached to cases of wine at various points (three bottles illustrated)
  - Yellow – good response
  - Black – little or no response
- Factor of four in the read distance depending on position of tag!
- A difference in tag position of just 1cm can halve



Issues: Privacy

- The press always concentrate on the privacy implications (perhaps rightly)
- RFID tags are not like wifi-enabled laptops: they're limited in capabilities, maening many standard crypto solutions are out.
- There have been some suggestions for how to address the issue...



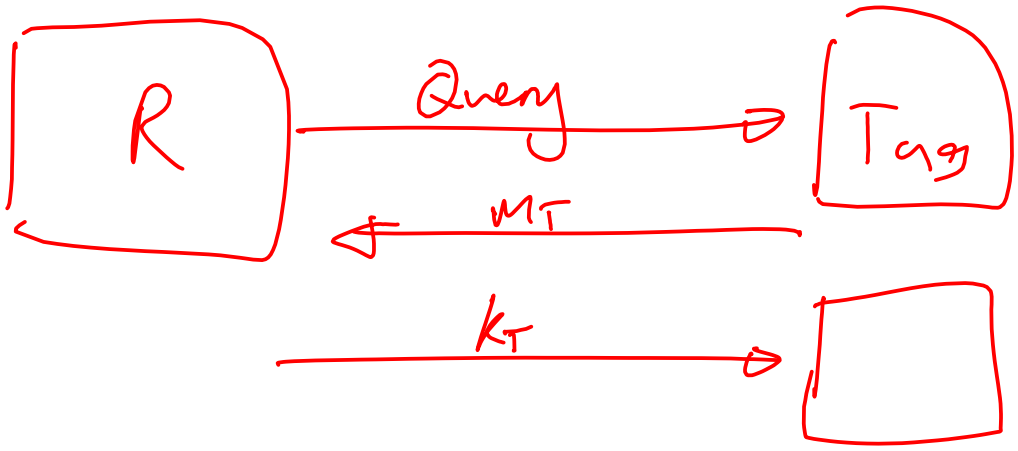
Kill Command!

- Classic solution: implement a tag command that results in self-destruction (burn out the radio circuit or similar)
- AutoID Center [sic] did this – you supplied a hardcoded password to fry your tag.
- Dramatically reduces the user benefits of the technology!

Hash-based Authentication

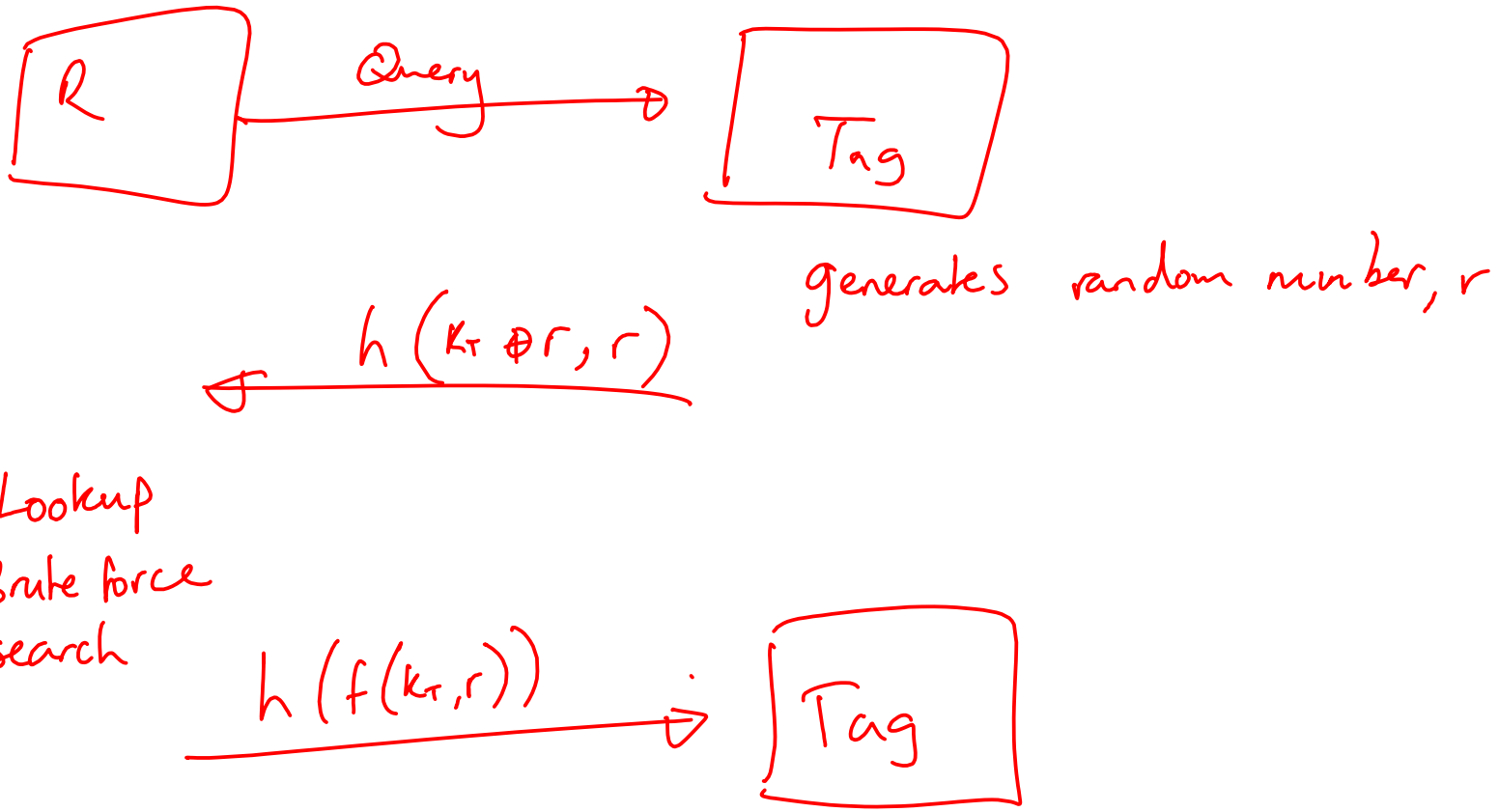
k_T = key for tag

$M_T = h(k_T)$



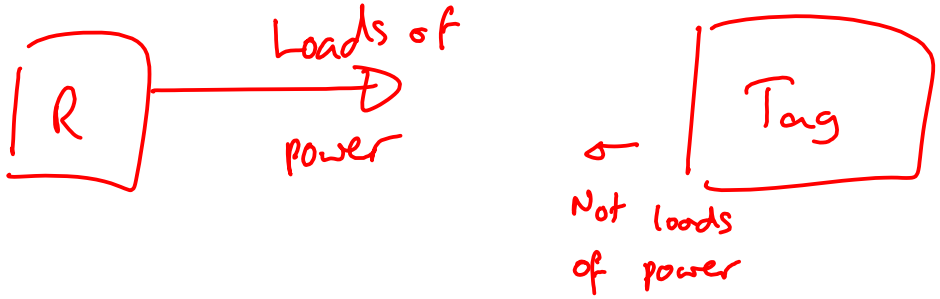
Eavesdropper

Randomized Authentication



Silent Tree Walking

Asymmetry reader and tag.



① On send, tag generates one time pad, P

② Reader responds Msg ⊕ P

① n^{th} bit ⇒ collision $x=1$
no collision $x=0$

② $(n+1) \oplus x$ ⇒ can only get ID if you know x

The Blocker Tag

- We create a tag that always responds when the reader starts to explore a specific subtree of tag IDs
- The idea would be that you move the IDs of the tags into that tree at the checkout (to indicate they are now personal)
  - And you carry the blocker tag in your bag.

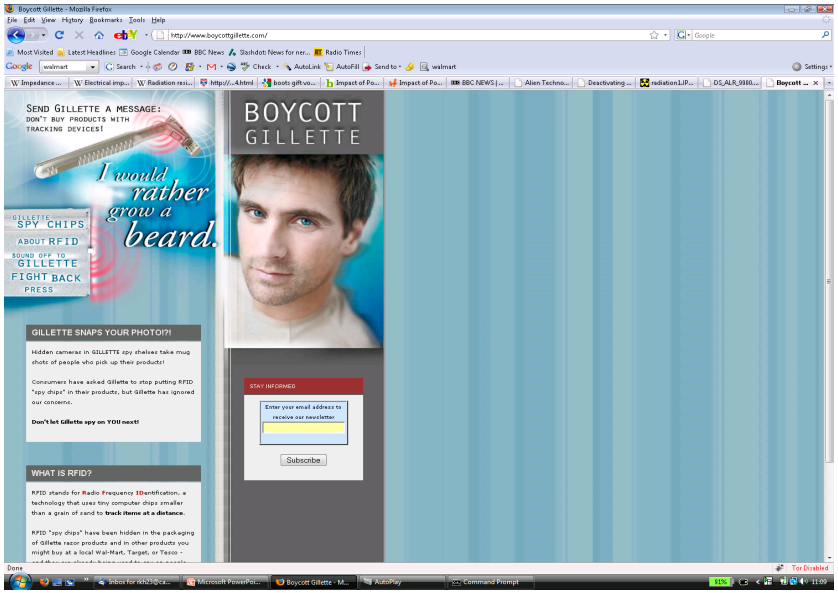
Real world Deployments

- Walmart
  - **2003** – Walmart announces 100 top suppliers will use RFID tags to tag pallets by Jan 2005. All at own cost – not popular.
  - **2007** – Wall street journal suggests that the pilot isn't going too smoothly. Walmart denies.
  - **2007** – Walmart announces change of focus. Now only tracking specific items for specific parts of distribution.
  - **2009** – Proctor & Gamble pull out, implying that Wal-mart is not doing what it should with the RFID info
  - Overall, not that clear how successful, although one study suggests that RFID reduces the number of out-of-stock items on the shelves by 16%.

Walmart
Save money. Live better.

Deployments

- Gillette
  - Gillette order 500 million tags from Alien for Mach 3 blades. Aim: Keep the shelves stacked with their latest product. Initial target Walmart.
  - Tested in Tesco in Cambridge, UK. Guardian headline: "Tesco Tests Spy Chip Technology". Turns out they hid a small camera and used the RFID to detect when someone picked up a razor (apparently Gillette razors are top of the thieving list).
  - Abandoned after protests. www.boycottgillette.com still exists



Deployments

- Gillette
  - Gillette order 500 million tags from Alien for Mach 3 blades. Aim: Keep the shelves stacked with their latest product. Initial target Walmart.
  - Tested in Tesco in Cambridge, UK. Guardian headline: "Tesco Tests Spy Chip Technology". Turns out they hid a small camera and used the RFID to detect when someone picked up a razor (apparently Gillette razors are top of the thieving list).
  - Abandoned after protests. www.boycottgillette.com still exists