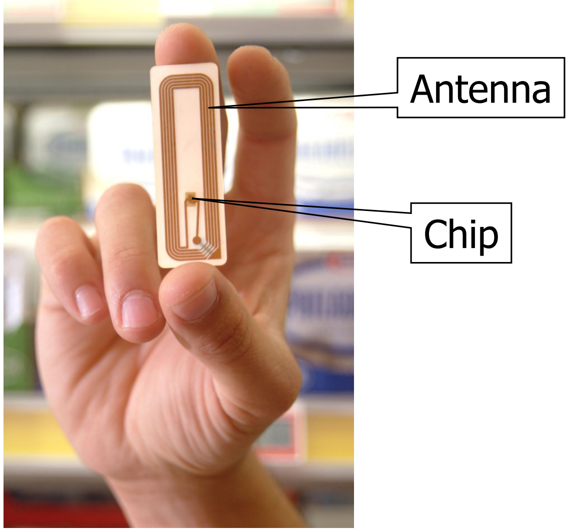
RF ID Security and Privacy

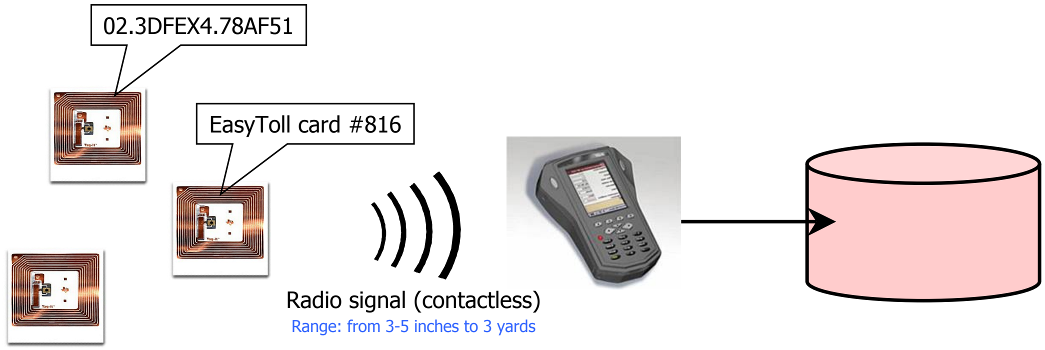
EJ Jung
11/15/10

What is RFID?

- Radio-Frequency Identification Tag



How Does RFID Work?



02.3DFEX4.78AF51

EasyToll card #816

Radio signal (contactless)

Range: from 3-5 inches to 3 yards

Tags (transponders)

Attached to objects, "call out" identifying data on a special radio frequency

Reader (transceiver)

Reads data off the tags without direct contact

Database

Matches tag IDs to physical objects

RFID is the Barcode of the Future

Barcode

Line-of-sight reading

- Reader must be looking at the barcode

Specifies object type

- E.g., "I am a pack of Juicy Fruit"

RFID

Fast, automated scanning (object doesn't have to leave pocket, shelf or container)

Reading by radio contact

- Reader can be anywhere within range

Specifies <u>unique</u> object id

- E.g., "I am a pack of Juicy Fruit #86715-A"

Can look up this object in the database

RFID Tag Power Sources

- Passive (this is what mostly used now)
  - Tags are inactive until the reader's interrogation signal "wakes" them up
  - Cheap, but short range only
- Semi-passive
  - On-board battery, but cannot initiate communication
    - Can serve as sensors, collect information from environment: for example, "smart dust" for military applications
  - More expensive, longer range
- Active
  - On-board battery, can initiate communication

RFID Capabilities

- No or very limited power
- Little memory
  - Static 64- or 128-bit identifier in current 5-cent tags
- Little computational power
  - A few thousand gates at most
  - Static keys for read/write access control
- Not enough resources to support public- or symmetric-key cryptography
  - Cannot support modular arithmetic (RSA, DSS), elliptic curves, DES, AES; hash functions are barely feasible
    - Recent progress on putting AES on RFID tags

Where Are RFID Used?

- Physical-access cards
- Inventory control
  - Gillette Mach3 razor blades, ear tags on cows, kid bracelets in waterparks, pet tracking
  - http://www.youtube.com/watch?v=4Zj7txoDxbE

- Logistics and supply-chain management
  - Track a product from manufacturing through shipping to the retail shelf
- Gas station and highway toll payment
  - Mobil SpeedPass

Commercial Applications of RFID

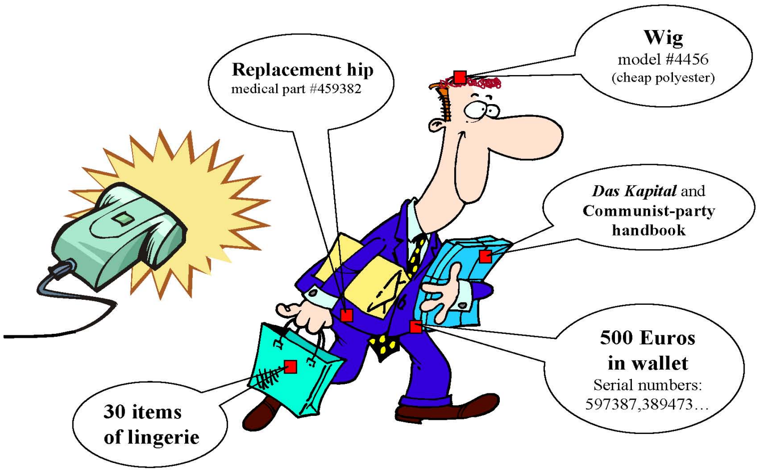
- RFID cost is dropping dramatically, making it possible to tag even low-value objects
  - Around 5c per tag, $100 for a reader
- Logistics and supply-chain management is the killer application for RFID
  - Shipping, inventory tracking, shelf stocking, anti-counterfeiting, anti-shoplifting
- Massive deployment of RFID is in the works
  - Wal-Mart pushing suppliers to use RFID at pallet level, Gillette has ordered 500,000,000 RFID tags
  - Backlash by privacy advocates

Futuristic Applications

- Prada store in New York City already uses RFID to display matching accessories on in-store screens
- Refrigerator shelves that tell when milk expires
- Airline tickets with RFIDs on them that help direct travelers through the airport
- Microwave ovens that read cooking directions from RFID tags on food packages
- RFID tags on postage stamps
- Businesses may attach RFID tags to invoices, coupons, and return envelopes

Privacy Issues (due to Ari Juels)

RFID tags will be *everywhere*…



Risks

- Personal privacy
  - FDA recommended tagging drugs with RFID “pedigrees”; ECB planned to add RFID tags to euro banknotes…
    - I’ll furtively scan your briefcase and learn how much cash you are carrying and which prescription medications you are taking
- Skimming: read your tag and make my own
  - In February 2005, JHU-RSA Labs team skimmed and cloned Texas Instruments’ RFID device used in car anti-theft protection and SpeedPass gas station tokens
- Corporate espionage
  - Track your competitor’s inventory

Cloning RFID

- Human implant with health information
  - VeriMed by VeriChip Corp.

- Cloned in August 2006
  - record the signals from RFID
  - replay to the interrogator
  - http://www.rfidjournal.com/article/articleview/2607/1/1/

- Credit card
  - 1st generation of credit card could be recorded and replayed
  - http://www.nytimes.com/2006/10/23/business/23card.html
  - http://youtube.com/watch?v=xPkzFETzueQ
  - http://prisms.cs.umass.edu/~kevinfu/video/RFID-CC-clips.mov

Reading private information

- ➢ Passport reading from RFID
  - half inch opened passport is readable
    - – http://youtube.com/watch?v=-XXaqraF7pI
- ➢ Collective information from database
  - EZ pass information tracks whereabouts
    - – http://www.msnbc.msn.com/id/20216302/

Blocking Unwanted Scanning

- ➢ Kill tag after purchase
  - Special command permanently de-activates tag after the product is purchased
  - Disables many futuristic applications
  - IBM Clipped tags
- ➢ Faraday cage
  - Container made of foil or metal mesh, impenetrable by radio signals of certain frequencies
    - – Shoplifters are already known to use foil-lined bags
  - Maybe works for a wallet, but huge hassle in general
- ➢ Active jamming
  - Disables all RFID, including legitimate applications

Location privacy in phones

- Location-based services arising
  - foursquare, geofencing, etc
  - “check-in”
  - how foursquare works:
    - http://www.youtube.com/watch?v=DUA7BokQn_E
- Danger of location updates
  - http://www.youtube.com/watch?v=NcTDa7POkXk
  - http://news.cnet.com/8301-1009_3-10260183-83.html

k-Anonymous location privacy

- Collect k people’s locations and present an aggregated value
  - e.g. weighted average of coordinates
  - useful in metro areas
  - not so much in less inhabited areas
- Research in progress
  - e.g. Policy-aware sender anonymity in location based services by Deutsch et al., ICDE 2010

Temporal delay

- Give a location in the past or projected future
- Usually combined with aggregation
- Application-dependent utility
  - e.g. traffic information from the past is not useful

Through intermediaries

- Your cell phone company knows where you are
  - ask cell phone companies to forward information
  - useful in diaster situations