RFID
UPC

- Wallace Flint first suggested an automated checkout in 1932
- UPC bar code formats developed in the 40's, 50's, 60's
- Grocery Industry adopted the UPC (based on an IBM proposal) April 3, 1973
- With computerized scanning, inventory. With computerized scanning, inventory, UPCs are ubiquitous on every product!

http://educ.queensu.ca/~compsci/units/encoding/barcodes/history.html
UPC are insufficient to many applications

- Cattle stock monitoring
- Person identification
- Tracking children and patients
- Toll collection on highway
- Remote keyless entry
- Vehicle Parking Monitoring
- Toxic Waste Monitoring
- Asset Management
- Local Positioning Systems
  - GPS useless indoors or underground, problematic in cities with high buildings
  - RFID tags transmit signals, receivers estimate the tag location by measuring the signal's time of flight
RFID

- Radio Frequency IDentification
- Not a specific technology, but an entire class of “tagging” items by radio accomplished through a variety of means
- RFID has been much hyped recently as the replacement for the UPC... and more
- Privacy and security concerns have cropped
RFID History

- WWII roots as the British put IFF transponders in planes (Identification: Friend or Foe) to identify returning aircraft
- In the 70’s, Los Alamos developed RFID tagging of nuclear equipment and personnel for safety
- Amtech and Identronix spun off released research
- Cattle stock monitoring, tracking (after trying and failing to use Bar Code Technology) through railroads
RFID History (Cont.)

- Some obvious spin-offs:
  - Fleet vehicle identification (tractors/trailers/cargo)
  - Toll collection on highways
    - FastLane (automated toll collection on Mass Pike, etc.) uses an active transponder operating in the 900MHz band
  - Remote keyless entry
- By 1984, several manufacturers, several flavors
RFID System

- Three components
- **RFID tag or transponder**
  - Antenna, wireless transducer, encapsulating material
  - Passive tags: operating power induced by the magnetic field of RFID reader, which is feasible up to distances of 3 m, low price (a few US cents)
  - Active tags: on-chip battery powered, distances up to 100 m
- **RFID reader or transceiver**
  - Antenna, transceiver, decoder
- **Data processing subsystem**
RFID Overview

- **Data rate**
  - Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
  - 9.6 – 115 kbit/s

- **Transmission range**
  - Passive: up to 3 m
  - Active: up to 30-100 m
  - Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

- **Frequency**
  - 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

- **Security**
  - Application dependent, typ. no crypt. on RFID device

- **Cost**
  - Very cheap tags, down to < $1 (passive)

- **Availability**
  - Many products, many vendors

- **Connection set-up time**
  - Depends on product/medium access scheme (typ. 2 ms per device)

- **Quality of Service**
  - none

- **Manageability**
  - Very simple, same as serial interface

- **Special Advantages/Disadvantages**
  - Advantage: extremely low cost, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
  - Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/transmission of ID)
RFID Overview (Cont.)

- **Function**
  - Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
  - Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)

- **Features**
  - No line-of sight required (compared to, e.g., laser scanners)
  - RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
  - Products available with read/write memory, smart-card capabilities

- **Programmability**
  - WORM (write once, read many times) usually at manufacture or installation
  - Direct Contact or RF (reprogrammable 10,000-15,000 times)
  - Full Read/Write (Identronix had some 64 prototypes by 1984)
Example Products

- **Example Product: Intermec RFID UHF OEM Reader**
  - Read range up to 7m
  - Anticollision algorithm allows for scanning of 40 tags per second regardless of the number of tags within the reading zone
  - US: unlicensed 915 MHz, Frequency Hopping
  - Read: 8 byte < 32 ms
  - Write: 1 byte < 100ms

- **Example Product: Wireless Mountain Spider**
  - Proprietary sparse code anti-collision algorithm
  - Detection range 15 m indoor, 100 m line-of-sight
  - > 1 billion distinct codes
  - Read rate > 75 tags/s
  - Operates at 308 MHz
Relevant Standards

Air interface protocol, data content, conformance, applications

- **American National Standards Institute**

- **Automatic Identification and Data Capture Techniques**

- **European Radiocommunications Office**

- **European Telecommunications Standards Institute**

- **Identification Cards and related devices**

- **Identification and communication**

- **Road Transport and Traffic Telematics**

- **Transport Information and Control Systems**
ISO Standards

- **ISO 15418**
  - MH10.8.2 Data Identifiers
  - EAN.UCC Application Identifiers
- **ISO 15434 - Syntax for High Capacity ADC Media**
- **ISO 15962 - Transfer Syntax**
- **ISO 18000**
  - Part 2, 125-135 kHz
  - Part 3, 13.56 MHz
  - Part 4, 2.45 GHz
  - Part 5, 5.8 GHz
  - Part 6, UHF (860-930 MHz, 433 MHz)
- **ISO 18047 - RFID Device Conformance Test Methods**
- **ISO 18046 - RF Tag and Interrogator Performance Test Methods**
Performance Metrics

- **Access rate**
  - # tags reliably read per unit time

- **Accuracy**
  - % tags read reliably in a given duration
  - Tradeoff between accuracy and access rate

- **Energy usage**
  - Energy usage on RFID tags or sensors
  - Energy usage on readers
Exploiting Tag multiplicity

- Multiple tags on an object to enhance reliability
  - Should all tags on the same objective have the same ID?
  - How to read?
    - Reader can treat simultaneous transmissions from multiple tags as a single transmission in a multipath environment
  - How to write?
    - Explicit association:
      - Different RFIDs on the same object contain different IDs
      - External database maps the IDs to the object
    - Implicit association
      - A few bits in the ID reserved to distinguish tags on the same object
      - Or use timestamp to implicitly differentiate between the tags
Exploiting Tag multiplicity

- Use multiple tags to improve localization
  - Existing localization techniques work if an object is associated with a single tag
  - With multiple tags, we can extract constraints for each individual tag and the constraints that bound the distance between these tags
Exploiting reader multiplicity

- **Motivation**
  - Readers are getting cheaper
  - Multiple readers are required to cover an area
  - Support concurrent reads

- **Interference from multiple readers ➔ collisions**
  - Potential solutions
    - Assign different channels
    - Use direction antennas
    - Control transmission power
    - Develop effective MAC protocol to minimize collisions

- **Improve tag access rates**
  - Non-cooperative approach
    - Implicit communication: write to tags and then read from the tags
  - Cooperative approach
    - Readers communicate with each other to decide which readers read which tags
Information Access

- RFID network can generate lots of data
- Desirable to aggregate data before transmission
  - Example
    - Reporting max, min, mean, median does not require sending all tag data
    - Remove redundant data collected by nearby readers
  - Difference from aggregation in sensor networks
    - All sensors are low-end vs. powerful reader and low-end tags
      ➜ what intelligence to put in the tags vs. readers
Hacking Cryptographically-Enabled RFID Device

- Team at Johns Hopkins University reverse engineer Texas Instrument’s Digital Signature Transponder
  - Paid for gas with cloned RFID tag
  - Started car with cloned RFID tag

- Lessons
  - Security by obscurity does not work
  - Use standard cryptographic algorithms with sufficient key lengths
RFID-enabled passport

- Metallic anti-skimming material added in cover and spine to reduce read distance to 1 inch

- PIN number printed on cover must be entered in reader to read tag and it encrypts communication

- New industry for wallet makers creating Faraday cages for passports
Security Threats

- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege
Security Threats to RFID

- A competitor or thief performs an unauthorized inventory of a store by scanning tags with an unauthorized reader to determine the types and quantities of items.
  - Spoofing
  - Information disclosure

- An attacker modifies the EPC number on tags or kills tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue.
  - Tampering with data
  - Denial of service

- An attacker modifies a high-priced item’s EPC number to be the EPC number of a lower cost item.
  - Tampering with data
Security

- Denial-of-Service attacks are always possible
  - Interference of the wireless transmission, shielding of transceivers
- IDs via manufacturing or one time programming
- Key exchange via, e.g., RSA possible, encryption via, e.g., AES
Privacy Threats by RFID

- **Bypass personal privacy**
  - Placing RFID tags hidden from eyes, and using it for stealth tracking
  - Using the unique identifiers provided by RFID for profiling and identifying consumer pattern and behavior
  - Using hidden readers for stealth tracking and getting personal information.

- **Examples**
  - A bomb explodes when there are 5+ Americans with RFID-enabled passports detected.
  - A mugger marks a potential victim by querying the tags in possession of an individual.
  - A fixed reader at any retail counter could identify the tags of a person and show the similar products on the nearby screen.
  - A reader reads tags in your house or car.

- The ISO 14443 standard proposed for passports specifies about 4 inches (10 cm) as the typical range. However, NIST with a special purpose antenna read it at 30 feet (10 meters)!

- **RFID enables tracking, profiling, and surveillance of individuals on a large scale.**
Top Privacy Threats by RFID

- Tracking - Determine where individuals are and where they have been

- Hotlisting - Single out certain individuals because of the items they possess

- Profiling - Identifying the items an individual has in their possession
5 Principles of Privacy

- **Notice.** There must be no personal-data, record-keeping systems whose very existence is a secret.
- **Access.** There must be a way for a person to find out what information about the person is in a record and how it is used.
- **Choice.** There must be a way to prevent personal information that was obtained for one purpose from being used or made available for other purposes without the person’s consent.
- **Recourse.** There must be a way for a person to correct or amend a record of identifiable information about the person.
- **Security.** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
Alan F. Westin’s Privacy Classifications

- **Privacy Fundamentalist (11%)**
  - Very concerned
  - Unwilling to provide data

- **Privacy Unconcerned (13%)**
  - Mild concern
  - Willing to provide data

- **Privacy Pragmatists (75%)**
  - Somewhat concerned
  - Willing to provide data if they are notified and get a benefit
Methods to protect privacy
Methods to protect privacy

- RSA Blocker Tags: spam any reader that attempts to scan tags without authorization to trick the reader to believe many tags in proximity.

- Kill switches: New RFID tags are shipped with kill switch to disable tags.
Fast and Reliable Estimation Schemes in RFID Systems
Estimation Schemes

- **Deterministic identification algorithms**
  - The reader polls a set of tags in a given slot using slotted ALOHA
  - Tree-based identification algorithms

- **Probabilistic identification algorithms**
  - Reader sends a framed ALOHA
  - Tags pick a particular slot to respond
  - Repeat the process until all tags have transmitted at least once successfully in a slot without collisions
Cardinality Estimation

- The previous approaches are not effective for cardinality estimation
  - They take long time to estimate cardinality
  - Deterministic identification algorithms query tags based on their IDs, which violates privacy constraints

- Contributions
  - Estimate cardinality based on # idle slots and # collision slots
  - Unified simple estimator provides a high level of accuracy within a single frame
  - Unified probabilistic estimator has a running time independent of the size of estimated tag set for a given accuracy requirement
Unified simple estimator

- The reader probes the tag with frame size f
- Tags pick a slot j in the frame uniformly at random and transmit in that slot

\[
E[N_0] = (1 - \frac{1}{f})^t \approx fe^{-\rho}
\]

\[
E[N_1] = t \cdot \frac{1}{f} \cdot (1 - \frac{1}{f})^{t-1} \approx f\rho e^{-\rho}
\]

\[
E[N_c] = f - E[N_0] - E[N_1] \approx f \left(1 - (1 + \rho)e^{-\rho}\right)
\]

where \( \rho = \frac{t}{f} \)

- Since \( E[N_0] \) and \( E[N_c] \) are monotonic, we use them to estimate cardinality
Advantages?
Advantages

- Fast counting
- Anonymization
Limitations?
Limitation

- The algorithms rely on the ability of accurately estimating # idle slots and # collision slots
- Hard to achieve in practice due to packet losses
  - Slots with traffic (either one tag response or multiple tag responses) can be perceived as idle slots due to packet losses
  - Slots with high interference and background noise can be perceived as collision slots
Limitation

- The algorithms rely on the ability of accurately estimating \# idle slots and \# collision slots
- Hard to achieve in practice due to packet losses
  - Slots with traffic (either one tag response or multiple tag responses) can be perceived as idle slots due to packet losses
  - Slots with high interference and background noise can be perceived as collision slots
Unified simple estimator (Cont.)

- **Operating range for the estimators**
  - When $t \gg f$, both zero estimator and collision estimator will not have finite estimates
  - $\Pr[N_0=0] = e^{-\lambda} < 0.01 \Rightarrow \lambda = fe^{-\rho} \leq 5$
  - $\Pr[N_0=0,N_1=0] = e^{-\lambda_0-\lambda_1} < 0.01 \Rightarrow \lambda_0 + \lambda_1 = fe^{-\rho} \leq 5$
  - Derive initial frame size based on upper bound on tag size and upper bound of probability of having infinite estimates
  - Collision estimator works well for a greater range of load factors

- **How to improving the accuracy of estimators?**
Unified simple estimator (Cont.)

- **Operating range for the estimators**
  - When $t \gg f$, both zero estimator and collision estimator will not have finite estimates
  - $\Pr[N_0=0] = e^{-\lambda} < 0.01 \Rightarrow \lambda = fe^{-\rho} \leq 5$
  - $\Pr[N_0=0, N_1=0] = e^{-\lambda_0 - \lambda_1} < 0.01 \Rightarrow \lambda_0 + \lambda_1 = fe^{-\rho} \leq 5$
  - Derive initial frame size based on upper bound on tag size and upper bound of probability of having infinite estimates
  - Collision estimator works well for a greater range of load factors

- **Improving the accuracy of estimators**
  - Reduce variance by repeating the experiments multiple times
    - $m$ independent experiments each with variance of $\sigma^2$ has variance of $\sigma^2/m$
  - Zero estimator and collision estimator are complementary
    - $ZE$ achieves higher accuracy under low load
    - $CE$ achieves higher accuracy under high load
  - Apply both zero estimator and collision estimator, and choose the result from the estimator that gives the smaller variance
Limitation of Unified simple estimator

- Simple estimator allows all tags to contend in every frame
- Assume an upper bound on the tag size and a fixed frame size that stretches up to the upper bound
- The optimal frame sizes for computing a low variance estimate are lower bounded by the tag size
- But how to work for an arbitrarily large tag size?
Unified Probabilistic Estimator

Tags each pick randomly among $f$ slots and transmit in that slot if they choose to contend with probability $p$

\[
N_0 \sim N[\mu_0, \sigma_0^2] \quad \mu_0 = fe^{-p\rho} \quad \sigma_0^2 = fe^{-p\rho}(1-(1+p^2\rho)e^{-p\rho})
\]

\[
N_c \sim N[\mu_c, \sigma_c^2] \quad \mu_c = f(1-e^{-p\rho}(1+p\rho))
\]

\[
\sigma_c^2 = fe^{-p\rho}((1+p\rho)-(1+2p\rho+p^2\rho^2+p^4\rho^3)e^{-p\rho})
\]