18-452/18-750
Wireless Networks and Applications
Lecture 21: RFID and NFC

Peter Steenkiste
CS and ECE, Carnegie Mellon University

Spring Semester 2020
http://www.cs.cmu.edu/~prs/wirelessS20/
Working with Zoom

- You should be able to see my cursor move
  » This feature should be on by default

- I may use annotations for some slides
  » Again this should work automatically

- Please use the Raise Your Hand feature
  » But I will typically answer questions between slides
  » On my system:
    – Click on “Participants” at the bottom of the screen
    – You should then see a blue hand that you can click

- Mute your microphone, please

- Details depend on your set up
Plan, outline

- **RFIDs**
  - Concept and applications
  - EPC and backend processing
  - PHY and MAC
  - Security

- **Near Field Communication**

- **Schedule discussion**
What is RFID?

- Radio Frequency IDentification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags and RFID Readers.
- An enabling technology with many applications:
  - Data can be stored and retrieved from the tag automatically with a Reader.
  - Tags can be read in bulk.
  - Tags can be read without line of sight restrictions.
  - Tags can be write once read many (WORM) or rewritable.
  - Tags can require Reader authentication before exchanging data.
  - Other sensors can be combined with RFID.
- Technology has been around for a long time.
- Also has critics, e.g. privacy concerns.
What is RFID?

- A means of identifying a unique object or person using a radio frequency transmission
- Tags (or transponders) store information, that can be retrieved wirelessly in an automated fashion
- Readers (or interrogators), either stationary and handheld, can read/write information from/to the tags

How does it operate?

- **RFID tags** are affixed to objects and stored information may be written and rewritten to an embedded chip in the tag
- Tags can be read remotely when they receive a radio frequency signal from a reader and use the energy to respond
- Can operate over a range of distances
- Readers display tag information or send it over the network to back-end systems
Applications

- **Operational Efficiencies**
  - Shipping and Receiving
  - Warehouse management
  - Distribution
  - Asset management

- **Total Supply Chain Visibility**
  - Inventory visibility in warehouses
  - In-transit visibility, asset tracking
  - Pallet, case level
  - Item, instance level

- **Shrinkage, counterfeit**
  - Reduce internal theft
  - Reduce process errors
  - Avoid defensive merchandizing
  - Product verification
  - Origin, transit verification

- **Security, Regulations**
  - Total asset tracking
  - Defense supplies
  - Container tampering
  - Animal Tracking
Automated Identification Technology Suite

- Linear Bar Code
- CMB (Contact Memory Button)
- 2D Symbol (QR Code)
- Smart Card/CAC
- OMC (Optical Memory Card)
- RFID - Active
- RFID - Passive
- STS (Satellite-Tracking Systems)
RF ID Types

- **Passive Tags:** rely on an external energy source to transmit
  - In the form of a reader that transmits energy
  - Relative short range
  - Very cheap

- **Active Tags:** have a battery to transmit
  - Has longer transmission range
  - Can initiate transmissions and transmit more information
  - A bit more like a sensor

- **Battery Assisted Passive tags are a hybrid**
  - Have a battery transmit
  - But need to be woken up by an external source
A Bit of History

• Early technology was developed in the 40s
  » Originally used as eaves dropping devices
  » Used reflected power to transmit (transponder), e.g. the membrane of a microphone

• First RF IDs were developed in the 70s
  » Transmission based on reflected energy using information in memory – readers can now distinguish devices

• Dramatic growth since then driven by industry
  » Potential for significant gains in areas
  » Big organizations (DOD, Walmart) requiring the use of RFIDs from their vendors for easy inventory control

• Set of applications expanded rapidly
Standards

• Passive tags operate in the LF, HF, and UHF unlicensed spectrum
  • 30-300 KHz, 3-30 MHz, 300-3000 MHz
  • Distance drop with frequency

• Transmission consists of a bit stream and CRC

• Many standards exist, mostly incompatible
  » Early standards mostly defined by the ISO
  » Widely used standard: ISO/IEC14443

• In 2003 EPCGlobal was formed to promote RFID standards
  » Defined a standard for the Electronic Product Code (EPC)
  » Also defined standards for coding and modulation
Primary Application Types

Identification and Localization

• Readers monitoring entering and exiting a closed region
  » Security (RFID in identification cards)
  » Merchandise in stores
  » NFC in phones

• Readers tracking an RFID-tagged object
  » Business process monitoring (RFID tags on pallets)

• Tags marking a spatial location
  » An NFC enabled mobile phone passes tags in the infrastructure whose location is known
Example: Smart Card

Public transport system in Singapore

- FeliCa Smart Card
- 2001 – 2009
- Faster boarding times
- Other uses
  - small payments retail
  - identification
- Replaced by contactless card (RFID)
How Smart are RFIDs?

- Basic tags simply reply with a fixed bit string – “read” the tag
  - “I am Groot”
  - Already useful!

- Gradual move to richer functionality
  - Changing the state on the tag – “write”
    - E.g., keep track of a balance
  - Privacy and security: encryption, access control, ...
    - E.g., different parties and read and write the tag
  - Add computing capabilities (more general than crypto)

- Next step is processors that operate entirely based on harvested ambient energy
  - Vibrations, RF, solar, ...
Example “Oyster” Card

• Balance is maintained on the card
  » Cryptographically secured

• The “reader” updates the balance as you enter/leave the metro station
  » Enter: record when and where you boarded
  » Leave: update balance on the card
  » These operations are local

• Readers record all trips and periodically send information to servers
  » Auditing trail, lost cards, etc.
  » Riders can check their balance online
Plan, outline

• RFIDs
  » Concept and applications
  » EPC and backend processing
  » PHY and MAC
  » Security

• Near Field Communication
Electronic Product Code (EPC)

• "A Universal identifier for physical objects"
  » Designed to be unique across all physical objects in the world, over all time, and across all categories of objects.
  » Intended for use by business applications that need to track all diverse physical objects, whatever they may be.
  » urn:epc:id:sgtin:0614141.012345.6285210cc Syringe #62852 (trade item)

• Combined multiple components
  » EPC data located on the RFID tag
  » Reader’s middleware
  » Locate EPC Information Services (EPCIS), using Web Services like SOAP and WSDL

• Not exciting but standardization is critical to wide-spread adoption
EPC Network Concept (2001)

Object Name Service (ONS)

- external software application
  - EPC Information Service (EPCIS)
    - Savant Middleware
      - reader device
        - RFID transponder
          - reader interface protocol & PML Core
            - RFID protocols UHF Class 0/1 & HF Class 1

DNS

PML

PML

PML

Peter A. Steenkiste, CMU
What information does an RFID tag contain?

---

**Gen 2 tags have four memory banks**

<table>
<thead>
<tr>
<th>Bank 0</th>
<th>Bank 1</th>
<th>Bank 2</th>
<th>Bank 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reserved Memory</strong>&lt;br&gt;• 32-bit Kill Password&lt;br&gt;• 32-bit Access Password&lt;br&gt;(64 bits)</td>
<td><strong>EPC Memory</strong>&lt;br&gt;• 16-bit CRC&lt;br&gt;• 16-bit Protocol Control&lt;br&gt;• 96-bit EPC&lt;br&gt;(128 bits)</td>
<td><strong>Tag Identification Memory</strong>&lt;br&gt;• 8-bit Class Identifier&lt;br&gt;• 12-bit Tag Designer&lt;br&gt;• 12-bit Tag Model Number&lt;br&gt;• 32-bit Serial Number (optional)&lt;br&gt;(0, 32, or 64 bits)</td>
<td><strong>User Memory</strong>&lt;br&gt;• User-defined format&lt;br&gt;(0 or more bits)</td>
</tr>
</tbody>
</table>

---

The CBP “GDTI-96” bit unique number

A 64-bit TID memory bank contains a tag serial number that uniquely identifies a tag.

* TID and User Memory banks are not initialized on some Gen 2 tags

---

Example to illustrate concept
Passive RFID Tags

- **Power supply**
  - passive: no on-board power source, transmission power from signal of the interrogating reader
  - semi-passive: batteries power the circuitry during interrogation, once woken up by external signal
  - active: batteries power transmissions (can initiate communication, ranges of 100m and more, 20$ or more)

- **Frequencies**
  - low frequency (LF): 124kHz – 135 kHz, read range ~50cm
  - high frequency (HF): 13.56 MHz, read range ~1m
  - ultra high-frequency (UHF): 860 MHz – 960 MHz (some also in 2.45GHz), range > 10m
Standards

• ISO 18000: multipart standard for protocols in LF, HF, and UHF bands

• For example, HF:
  » ISO 14443 (A and B) for "proximity" RFID
  » ISO 15693 for "vicinity" RFID (basis for ISO 18000 part 3)

• Two classes:
  » Class 0: read only
  » Class 1: read/write, can for example be used for tracking

• Many more standards exist!
Transmission methods

• LF and HF: inductive coupling
  » Coil in the reader antenna and a coil in the tag antenna form an electromagnetic field
  » Tag changes the electric load on the antenna.

• UHF: propagation coupling: backscatter
  » Tag gathers energy from the reader antenna
  » Microchip uses the energy to change the load on the antenna and reflect back an altered signal
  » Different modulations used by reader and tag

From: http://www.highfrequencyelectronics.com/Archives/Aug05/HFE0805_RFIDTutorial.pdf
https://rfid4u.com/rfid-basics-resources/inductive-and-backscatter-coupling/
PHY Layer

- Depends on the frequency band used
- Different modulations used by reader and tag
  - Different constraints, e.g. power and complexity
  - E.g. cannot used amplitude modulation for HF tag (why?)
- Example of EPCGlobal symbols for UHF
What does an RFID tag look like inside a card?
MAC Layer

• Typically assumed that only one reader is present, i.e. no need for MAC on the reader

• MAC for tags is a challenge: very high concentrations of tags are present in many contexts
  » And tags are dumb, i.e. cannot have sophisticated protocols (carrier sense, RTS/CTS, ..)
  » Must also deal with multiple readers operating in the same environment

• Two types of schemes used (standard):
  » Binary tree resolution: reader explores a tree of relevant tag values
  » Aloha: tags transmit with a random backoff
Binary Tree Resolution

- Send requests to tags with ids that start with a certain string
- Narrow down search until one tag responds
General Security Concerns

• RFID tags raise a number of security concerns:
  » Privacy risks, e.g., eavesdropping
  » Cloning and forging of tags

• Specific disadvantages due to tag limitations
  » Some encryption algorithms may be too complex to be implemented on tags

• But also specific advantages:
  » Tags are slow to respond, maximum no. of read-out operations
  » Short transmission range means that an adversary has to be physically close
Privacy Concerns

• Tracking
  » Depends only on unique id (even if random)
  » Today:
    – automated toll-payment transponders
    – loyalty cards
  » Future: pervasive availability of readers

• Inventorying
  » Invisible items become visible
  » Libraries
  » Passports
  » Human implants: VeriChip
    – Medical record indexing
    – Physical access control
Privacy for Business Networks

- **Major concern for industry:**
  - Supply chain visibility
  - Supply chains and business networks are business assets

- **Example provenance checking:** competitors may be able to get a lot of information
  - Depending on how detailed the information associated is:
    - Where an object and its parts were manufactured
    - When it was manufactured
    - By which sub-contractors
  - Who are the suppliers of a company
  - Which companies are the customers of a company
Reading Ranges

- Controlling reading range can limit privacy risk
- Nominal read range (RFID standards and product specifications):
  > 10cm for contactless smartcards (ISO 14443)
- Rogue scanning range: sensitive reader with more powerful antenna or antenna array
  > 50cm
- Tag-to-reader eavesdropping range: need to power the tag limits range for passive RFIDs
  > Eavesdropping on communication while another reader is powering the smartcard: > 50cm
- Reader-to-tag eavesdropping: readers transmit at much higher power
Use for Authentication

- RFID tags uniquely identify objects
- Many proposals to use tags for authentication
  - Passport or driver's licence
  - Identification of stolen goods

- Counterfeiting attack
  - Scanning and replicating tags

- Possible options
  - EPC:
    - Simple bitstring
    - No access-control
  - VeriSign:
    - Digital signing
    - Against forging but not cloning
Plan, outline

• RFIDs
  » Concept and applications
  » EPC and backend processing
  » PHY and MAC
  » Security

• Near Field Communication
Near Field Communication (NFC)

• One device combines the functionality of
  » An RFID reader device
  » An RFID transponder (tag)
  » Bit rates ranging from 106 Kbs to 424 Kbs

• Integral part of mobile devices (e.g. mobile phones). NFC components can be accessed by software to

• Operates at 13.56 MHz (High frequency band) and is compatible to international standards:
  » ISO/IEC 18092 (also referred to as NFCIP-1),
  » ISO/IEC 14443 (smart card technology, “proximity coupling devices”),
  » ISO/IEC 15693 (“vicinity coupling devices”).

• Use of NFC is growing fast
  » Driven by NFC Forum (founded by Nokia, Philips, and Sony in 2004)
  » http://www.nfcworld.com/nfc-phones-list/#available
NFC Devices

Modes of operation

• **Smart Card emulation (ISO 14443):**
  » Phone can act as a contactless credit card
  » Information can be generated rather than pre-stored

• **Reader mode**
  » Allows NFC devices to access data from an object with an embedded RFID tag
  » Enables the user to initiate data services, i.e., retrieval of rich content, advertisements, ..

• **Peer-to-peer (ISO 18092)**
  » Allows two way communication between NFC devices
  » NFC can act as smart tag, i.e., generates information

Example: contactless payment applications
  Sony FeliCa, Asia
  MIFARE, Europe
  Google Wallet

(c) Google
Active and Passive Communication Modes

- Passive communication: one device acts as a reader and the other as a tag
  - Reader generates a field while the other responds
  - The second device can be a tag or another NFC device

- Active communication: both devices alternatively act as readers
  - Allows fairly general two way communication
  - Both devices must have a battery

- Since NFC devices can read and write, they must check for collisions
  - Compare received signal with transmitted signal
Comparison: Main Applications

RFID
• Retail
• Logistics
• Supply chain management
  » accurate inventories
  » product safety and quality

NFC
• Mobile payment
• Mobile ticketing
• Pairing of devices (esp. Bluetooth devices)
• Download of information from "smart posters"
## Remaining Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Mo</th>
<th>Tu</th>
<th>We</th>
<th>Th</th>
<th>Fr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 23</td>
<td>P2 CP1 L23</td>
<td>P2 meetings</td>
<td>L24</td>
<td>HW3</td>
<td></td>
</tr>
<tr>
<td>Mar 30</td>
<td>Draft</td>
<td>Draft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 6</td>
<td>P2 CP2</td>
<td>P2 meetings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 13</td>
<td>Surveys</td>
<td>Surveys</td>
<td>HW4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 27</td>
<td>Project Talks</td>
<td>Course Review</td>
<td></td>
<td>P2 Final Report</td>
<td></td>
</tr>
</tbody>
</table>
P2, Homework and Survey Discussion

• Identifying and ordering any hardware you need is a top priority
  » I can provide (limited) support, but you need to get approval before ordering

• There will be two more homeworks

• Past experience shows that starting late on your survey talk is a really bad idea
  » Make sure you send me a solid draft 2 weeks before the presentation

• Make sure you practice a few times
  » Time management, coordination with partner, tweak slides, ....
Some Thoughts about Surveys

• Many students use the google templates, which are generally poorly designed (24pt)
  » No slide numbers
  » Tiny font sizes (12pt) – I want to be bigger! (18pt)
  » 50%-80% of the slide is empty
  » Use the space wisely!

• Outline generally looks like:
  » Background: why useful, challenges, design options, etc.
  » Discussion on the three papers:
    – What is the key idea – this should be clear (figure!)
    – Some sample results illustrating benefits
    – You do not have to cover the full paper!!
  » Personal opinion on pros or cons (global or per paper)
Schedule Flexibility

• Flexibility in when we have lectures
• Some limited flexibility in the survey and project dates
• One possibility: Move final to last day of class and have projects due in finals week
  » Final would be two hours long
  » Plus: more time to work on projects
  » Less time to study for the final, but all course material would have been presented at least two weeks before the final
  » Short discussion now, poll if there seems to be strong enough interest