RFID
Building an Internet of Things

Debasish Sahoo
Regd no-0821209032
Contents

- Introduction RFID
- RFID Network Architecture
- RFID Applications
- RFID Security & Privacy
Contents

Introduction RFID
What is RFID

- Radio Frequency Identification
  - Describes any system of identification wherein an electronic device that uses radio frequency or magnetic field variations to communicate is attached to an item.
What’s wrong with Bar-code

- Barcode is prevalent in commercial world.
- However, there are shortcomings of bar codes
  - Line-of-sight
  - One-at-a-time
  - Manual handling
  - Limited range
  - Limited data
Radio Frequency Identification offer the potential to eliminate these shortcomings

- Non-line-of-sight
- 100(s) at a time
- Automatic handling
- Several meter
- 50 bits - Kbits
Example: Supply Chain
RFID Network Architecture
The RFID Network Architecture is composed of four fundamental elements:

- Electronic Product Code (EPC)
- Hardware System (RFID tags and readers)
- RFID middleware
- Object Name Service (ONS)
Electronic Product Code

- Numerous identification coding standards exist:
  - Universal Product Code (UPC)
  - International Standard Book Number (ISBN)
  - IP Address
  - MAC Address

- **EPC aims to uniquely identify physical objects over the world**
Electronic Product Code

- Standard EPC is 96 bit
- EPC is comprised of four distinct numbers
  - Version
  - Domain Manager Number (P&G, Pepsi)
  - Object Class Number (Pepsi Cola)
  - Serial Number

```
01.203D2A.916E8B.8719BAE03C
```

```
<Version>.<Domain Manager>.<Object>.<Serial>
```
Hardware--Reader and Tag
RFID Tag

1. Coil
2. Microchip
3. Surface acoustic wave baffles (not a microchip)
Chip of RFID Tag
RFID Tag

104 Pantene Cases

SAW RFID Tags
RFID Reader

- Passive tags must have radio transmitters somewhere to power them.
- It's the reader's role to know how to talk to tags, how to create low-level data from reads, and how to send these data to middleware.
Normally a very weak reply is obtained
Two collision-related issues:

- **Reader Collision** – Interference caused by an overlap in reader signals
- **Tag Collision** – Interference caused when more than one tag responds to a signal at the same time
In order to reduce network traffic, modular components of RFID Middleware will be used to process, filter, and digest events.
✓ Since only the EPC is stored on an item’s tag, computer systems need a way of matching the EPC to information about the item

✓ ONS is an automated networking service similar to Domain Name Service (DNS) and built over top of the DNS framework
Networking the Physical World
RFID Network: Trace and Track

1. **Manufacture Database A**
   - **Register**: 1.2.3.4 is in Database A

2. **Middleware**
   - **Verify Receiving Information**

3. **ONS**
   - **ONS Finding**: Where can I find information of 1.2.3.4
   - **ONS Return**: Database B

4. **Retailer Database B**
   - **Receive 1.2.3.4**
   - **Send 1.2.3.4**
The right of the consumer

- to know what items possess RFID tags
- to remove or deactivate the RFID tag once a product is purchased
- to know where, when, and why an RFID tag is being read
- to know what information is being stored inside an RFID tag
Vulnerability

- **Tag**
  - Data on the tag is stored unencrypted
  - Without physical supervision, anyone on the premises with physical access to tags can remove a tag or switch one tag with another

- **Reader**
  - The data traffic from tag to reader is not encrypted
  - Readers do not authenticate the tags
Possible Countermeasures

- **Tag**
  - Using re writable tags only where appropriate
  - With proper access control (physical or encryption)

- **Reader**
  - Communication between readers and tags can be encrypted.
  - Readers should require proper authentication and authorization to allow access to their services
Why is the RFID information vulnerable to attacks?

**Reason**
The RFID system is designed to be fully open, the RFID IC itself and the communication process between reader and tag are easily attacked.

**Example**
RFDump: Anyone who installs a reader in his laptop can get the data in passive tags within 3 feet area by using RFDump SW.

**Present**
No overall security mechanism has been proposed.
Resource

- [RFID and RFID privacy, http://www.rsasecurity.com](http://www.rsasecurity.com)
- [Technical characteristics of RFID http://www.rsasecurity.com](http://www.rsasecurity.com)
Thank You!