Module 3 – RFID Privacy, Safety and Security

Main Objectives:

1. What are the potential privacy issues that may arise in a RFID implementation?
2. Why is it important to protect data that can identify a person?
3. What are the potential safety issues that can arise from the use of RFID equipment?
4. Could data exchanged between a reader and a tag be intercepted?
5. What are the potential problems of intercepted data?

1. What are the potential privacy issues that may arise in a RFID implementation?

RFID is the exchange of data between an item and a reader which then hands off that data to another system for processing. That data may be used to identify an individual person directly (e.g. an employee badge) or to indirectly derive a person's identity (e.g. a credit card number which leads to the person). Such data needs to be carefully managed in order to comply with any regulatory requirements and also to respect the individual's right to privacy.

2. Why is it important to protect data that can identify a person?

- Privacy laws
- Possibility of identity theft
- Possibility of data theft and misuse (stolen credit card number and unauthorized use of funds, unauthorized access to buildings, unauthorized access to information, and liability derived from these acts, etc.)

3. What are the potential safety issues that can arise from the use of RFID equipment?

RFID equipment uses electric current to operate and radiates energy when seeking tags of exchanging data, so it is important that all RFID equipment is operated safely, in line with health and safety regulations and without any adverse impact on the surrounding environment.

To ensure that your installed system is safe, make sure that:

- All hardware is installed and operated in accordance with manufacturer's specifications.
- Hardware using electrical current is grounded.
- You follow safety requirements of the location.

There are many regulations and standards related to operation of electric and wireless technologies, below are the main ones:

- **FCC** – **Part 15.247-i** Limits of exposure to radio frequency energy levels
- **ICNIRP** - The International Commission on Non-Ionizing Radiation Protection (allied to WHO)
  - Frequencies under 10 MHz can have effects on **central nervous system** due to electric current flow in the human body. The exposure to low frequencies cannot be time-averaged.
  - Frequencies above 100 kHz can have a **warming effect** on the human body. Can be time averaged.
- **Military specs** (complying with ANSI/IEEE)
  - Safe dosimetric parameter for exposure to RF fields is **0.4 W/kg** for controlled exposure and **0.08 W/kg** for uncontrolled exposure. This ensures at least the safety factor of 10 below the body specific absorption rate, which is 4 watts per kilogram (W/kg).
  - Example: 200 pound (90 kg) person – 7.2 W safe exposure
    110 pound (50 kg) person – 4 W safe exposure
- Safe distance from UHF antenna – 9 inches

- **ATEX -** The ATEX Directive consists of two EU directives describing what equipment and work environment is allowed in an environment with an explosive atmosphere.
  - ATEX derives its name from the French title of the 94/9/EC directive: *Appareils destinés à être utilisés en ATmosphères Explosibles*

- US equivalent of ATEX are **Explosion Proof (Class 1 Div 1) and Intrinsically Safe** ratings for devices operating in defined areas:
  - C1D1 – **Class 1, Division 1** - An area where ignitable concentrations of flammable gases, vapors or liquids can exist all of the time or some of the time under normal operating conditions.
  - C1D2 – **Class 1, Division 2** - An area where ignitable concentrations of flammable gases, vapors or liquids are not likely to exist under normal operating conditions.

- **IEC-EX** – International Electrotechnical Commission sets standards for equipment operating in Explosive Environment

- **HERO** - Hazards of Electromagnetic Radiation to Ordnance (HERO)

- **TEMPEST** - **A** National Security Agency specification and a NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations

- **IP – INGRESS PROTECTION** (protection of equipment) - The IP number is composed of two numbers, the first referring to the protection against solid objects and the second against liquids. The higher the number, the better the protection. For instance: IP67 (6 = Total protection against dust, 7 = Protected against the effect of immersion between 15cm and 1m).

4. Could data exchanged between a reader and a tag be intercepted?

The exchange of RFID data by radio transmission could be subject to unauthorized interception of the transmission and capture of the data being exchanged. While this would require sophisticated equipment and techniques, it must still be guarded against. Even encrypted data can be intercepted. Whether this encrypted data can be decrypted and misused, would depend on the encryption difficulty and hacker's sophistication.

5. What are the potential problems of intercepted data?

- Data replication – used for counterfeiting of products
- Data theft and identity theft – used for financial theft, personal gain or to damage person's private life or business
- Data change – re-pricing products, changing identification of products, changing expiration dates on drugs, changing audit data (if housed on the tag).

Study List

For comprehensive explanation, please review:

NFC Security
NFC Device Architecture and Secure Element