

Introduction to RFID

Gildas Avoine

UCL, Louvain-la-Neuve, Belgium

Department of Computing Science and Engineering



RFID Primer

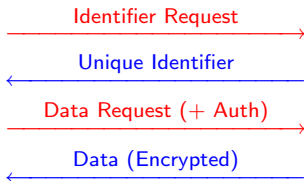
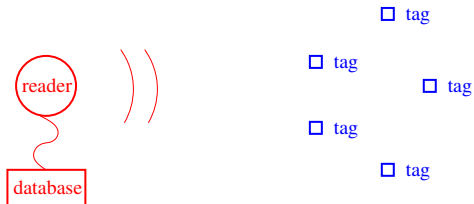
Radio Frequency Identification (**RFID**) is a method of storing and remotely retrieving data (typically an identifier) using devices called RFID **tags** or transponders.

An RFID tag is a **small object** that can be **attached to or incorporated** into a product, animal, or person.

RFID tags contain **antennas** to enable them to receive and respond to radio-frequency queries from an RFID **transceiver**.



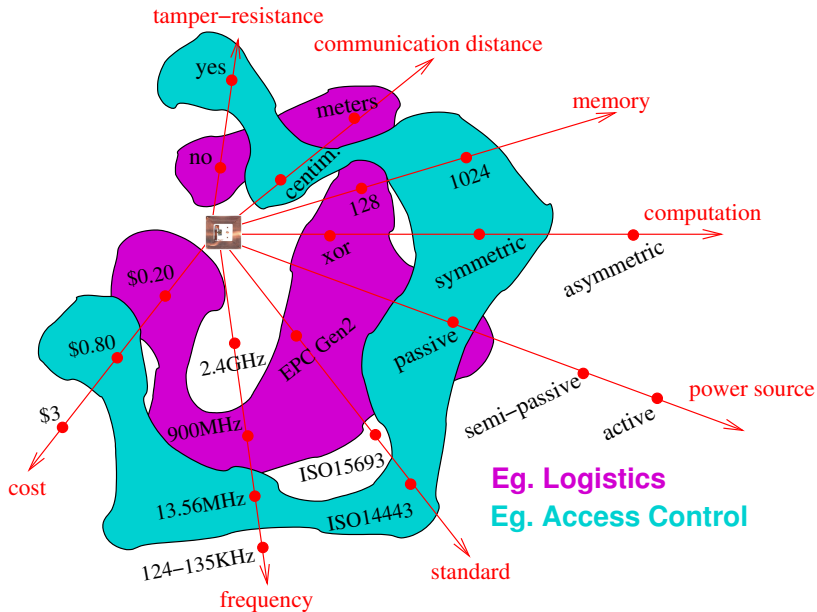
- RFID exists since the **forties** (IFF, Russian spy).
- Commercial RFID applications appeared in the **early eighties**.
- Boom which RFID technology is enjoying today relies on the willingness to develop **small** and **cheap** RFID tags.
- Auto-ID Center created in **1999** at the MIT. (EPC code)



- Management of stocks (Wal-Mart, US DoD, etc.)
- Libraries (Santa Clara Library, etc.)
- Pets identification
- Anti-counterfeiting (luxury articles, etc.)
- Access control (Building, Famous Baja Beach Club, etc.)
- Automobile ignition keys (TI DST Module, etc.)
- Localization of people (Amusement parks, hospital, etc.)
- Electronic documents (IDs, Passports, etc.)
- Public transportation (Paris, Boston, etc.)



Tag Characteristics



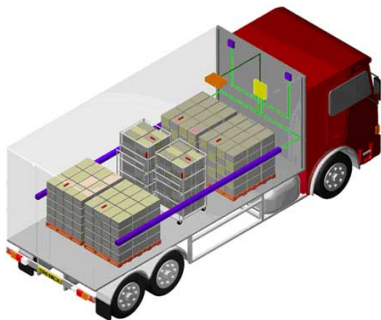
Collateral Damage

- Information Leakage
- Malicious Traceability
- Denial of Service
- Reputation

Data sent by the tag **could reveal information** intrinsic to the marked object.

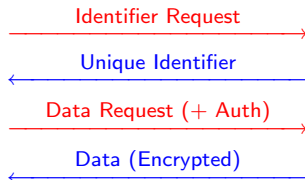
- Tagged books in **libraries**.
- Tagged **pharmaceutical** products.
- E-documents (eg. **passports**, ID cards, etc.).
- **Directory** of identifiers (eg. EPC code).

- Tag holder is threatened.
- RFID system is threatened.



- More and more **data collected** = valuable target (eg. during the manufacturing).
- **Unaware** information leakage (backup, HD thrown out, housekeeping).
- Do not figure out that **some privacy is disclosed** (cf. RTBF April 23th, 2008).
- **Abusive use** (eg. French police's confidential files, Charlie Card in Boston).

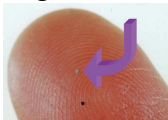
An adversary should **not be able to track** a tag holder, ie, he should not be able to **link** two interactions tag-reader.



Example: tracking military troops.

Differences between RFID and the other technologies e.g. video, credit cards, GSM, Bluetooth.

- RFID is a **wireless** technology
- Tags cannot be **switched-off**
- Tags answer **without the agreement** of their bearers
- Easy to **analyze the logs** of the readers
- Increasing **communication range**
Eg. US-Canadian crossing-border facilities
- Tags can be almost **invisible**



A DoS attack aims at preventing the target from fulfilling its normal service.

Threatened by DoS attacks if:

- There is an interface inside/outside.
- Wireless technology (if reader/devices close to public zone).

Techniques:

- Electronic noise
- kill or hide tags
- Exploit on reader middleware
- Viruses
- Kill-command
- Blocker tag

Goal in RFID:

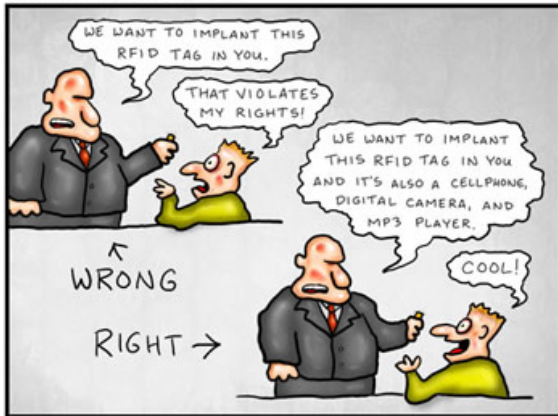
- For fun
- For disturbing a competitor
- For proving that RFID is not secure

RFID may tarnish a company's reputation when something becomes out of control.

- Secure RFID **solution broken** (eg. NXP Mifare).
- Database containing personal **data leaks**.
- **Boycott** campaign (eg. Benetton, Gillette).
- Poor **communication** (eg. Navigo).

DOCTOR FUN

16 Jan 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

Conclusion

- Privacy-compliant protocol
- kill-command
- Faraday cages
- Blocker tags
- Removable antenna
- Tag must be pressed
- Bill of Rights

Who is the victim?

Where is the weakest link?

Who is the attacker?

“The ‘authorized parties’ pose a greater threat to privacy than the criminals” (K. Albrecht, 2007)