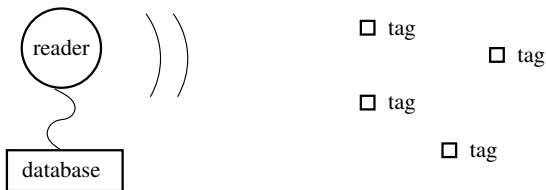


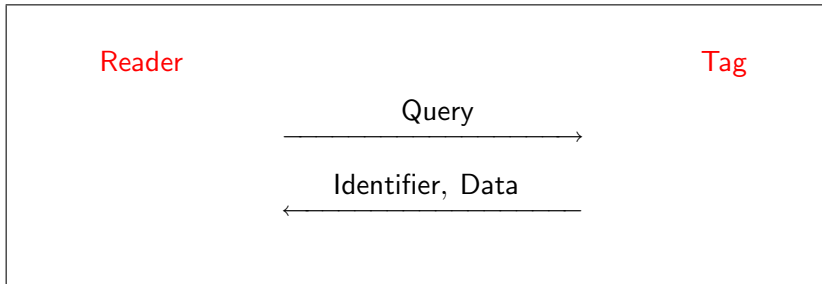
**RFID Primer  
&  
Foretaste of Security and Privacy**

**Gildas Avoine**

Radio Frequency Identification (**RFID**) is a technique to remotely identify some objects or subjects by querying transponders (**tags**) using a reader.



# Identification Protocol



# Tags



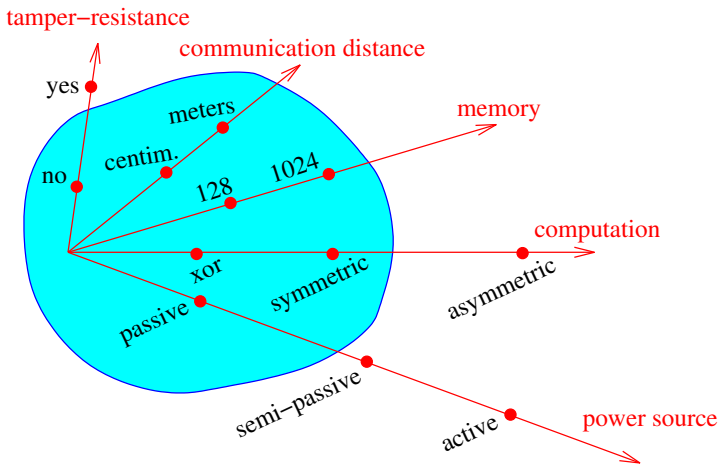
# Some Applications



# Some Applications (cont')



# Tags Properties



Why do I want to use RFID?

# Classification of the Applications



# Classification of the Applications



**Authentication**



**Identification**



# Identification vs Authentication

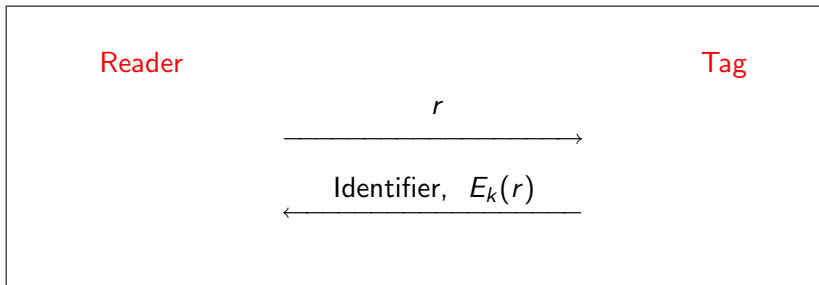
**Identification:** Get **Identity** of remote party.

- ▷ Denial of service
- ▷ Information leakage
- ▷ Malicious traceability

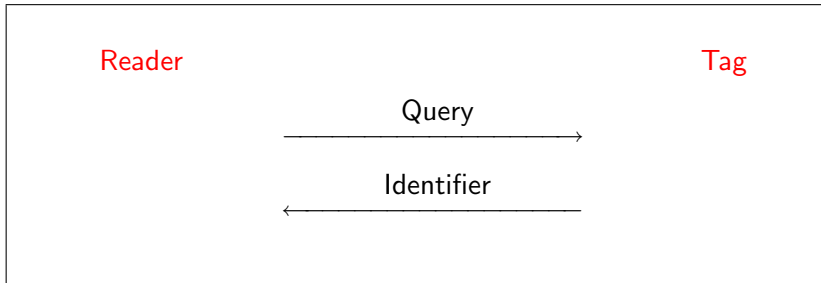
**Authentication:** Get **Identity + Proof** of remote party

- ▷ Denial of service
- ▷ Information leakage
- ▷ Malicious traceability
- ▷ Impersonation

# Impersonation

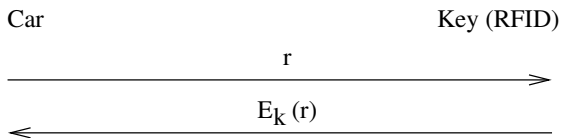


- ▶ **Use of cryptography** (authentication of the tag): lightweight protocols and algorithms (symmetric crypto only), problem of key management, tags are not fully tamper-resistant, etc.
- ▶ Do not cut the price by using weak algorithms or weak keys.



Priya Agrawal said: "If you are counting cattle, the cattle are not going to impersonate each other; there is no need for strong encryption. Members of the MIT population are not cattle; we need strong encryption."

- ▶ Bono *et al.*'s attacked the TI's Digital Signature Transponder.



- ▶ The cipher is not public.
- ▶ Length of the cryptographic key is **40 bits**.
- ▶ Attack succeeds in less than **one minute** (TMTO).

Recovering the cryptographic key / Impersonating the ignition key / Impersonating the SpeedPass card

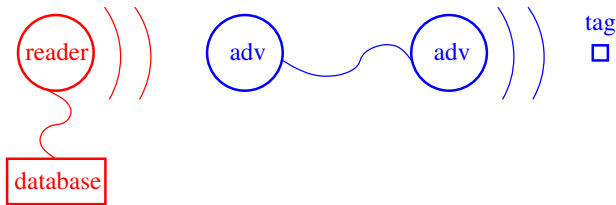
# E-Passport Case

- ▶ To solve the key-management problem, the key that allows to read the electronic data is printed on the e-passport.
- ▶ The key is generated from **date of birth**, **date of expiration**, and **passport number**: lack of entropy.

(This topic will be the core of a further presentation)

# Relay Attack

- ▶ The reader believes that the tag is in its electromagnetic field while it is not the case. The adversary acts as an extension cord.



- ▶ The countermeasure consists in measuring the round trip time between the reader and the tag (do-able in practice?).

# Information Leakage

- ▷ Information revealed by the **back-end system**.
  - ▶ Problem already exists but **amplified** (everything logged).
  
- ▷ Information revealed by the **tag**.
  - ▶ Easy to **get** information, e.g. e-passport, truck on a parking lot.

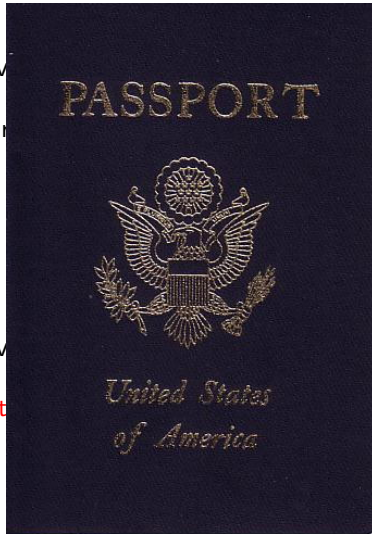
# Information Leakage

▷ Information revealed

▶ Problem already solved (no logging needed, no logging logged).

▷ Information revealed

▶ Easy to get (e.g., lost passport on a parking lot).



# Information Leakage

- ▶ Information revealed (e.g., name, date of birth, sex, etc. being logged).
- ▶ Problem already solved (e.g., name, date of birth, sex, etc. being logged).



- ▶ Information revealed (e.g., name, date of birth, sex, etc. being logged).
- ▶ Easy to get (e.g., name, date of birth, sex, etc. being logged) on a parking lot.

# Information Leakage

▷ Information

▶ Proble

▷ Information

▶ Easy to



d).

arking lot.

# Information Leakage

▷ Information

▶ Proble

▷ Information

▶ Easy to



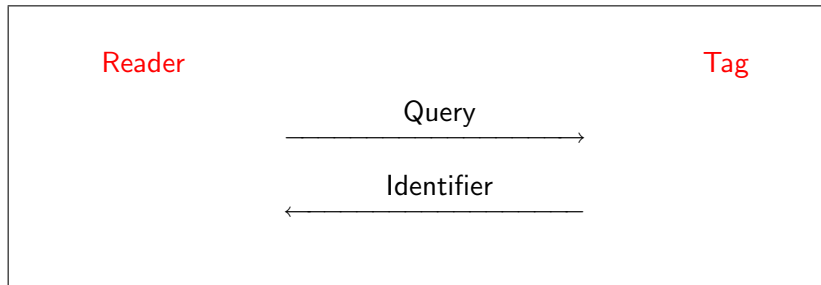
d).

arking lot.

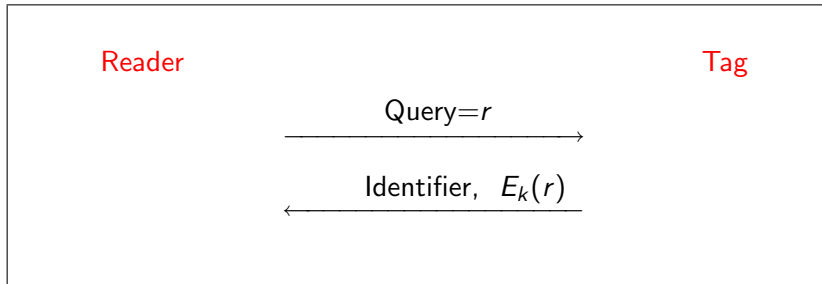
- ▷ **Palliative techniques:** Faraday cage, kill-command, removable antenna, blocker tag, etc.
- ▷ **Use of cryptography** (encryption of the tag's content or auth of the reader): lightweight protocols and algorithms (symmetric crypto only), problem of key management, tags are not fully tamper-resistant, etc.

- ▶ Given a set of interactions between readers and tags, an adversary should not be able to find relations between these communications.

# Malicious Traceability (Identification Protocol)



# Malicious Traceability (Identification Protocol)



# Malicious Traceability (Use of Cryptography)

- ▶ New **concept** in cryptography.
- ▶ Protocol such that the information sent by the tag is **indistinguishable** (by an adversary) from a random value.
- ▶ The reader must check **every key**.
- ▶ Attacks using **side channels**, e.g. within the communication lower layers.

# Malicious Traceability (Reality or Science Fiction?)

- ▶ Some organizations defending the civil liberties fight the RFID technology: **Caspian**, **Foebud**.

# Malicious Traceability (Reality or Science Fiction?)

- ▶ Some organizations are concerned about the technology:



the RFID

# Malicious Traceability (Reality or Science Fiction?)

- ▶ Some organizations defending the civil liberties fight the RFID technology: **Caspian**, **Foebud**.

# CONCLUSION

- ▷ Denial of service
- ▷ Information leakage
- ▷ Malicious traceability
- ▷ Impersonation