

A Few Words About RFID Security

Gildas Avoine

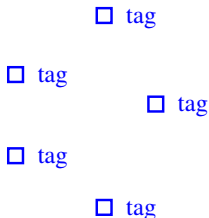
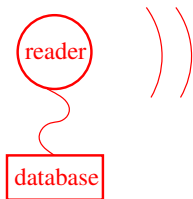
MIT, USA

<http://www.avoine.net>



RFID Primer

RFID is a technology to identify an object or a person, remotely, using a small transponder (**tag**) that is attached or incorporated to the object or person to identify.

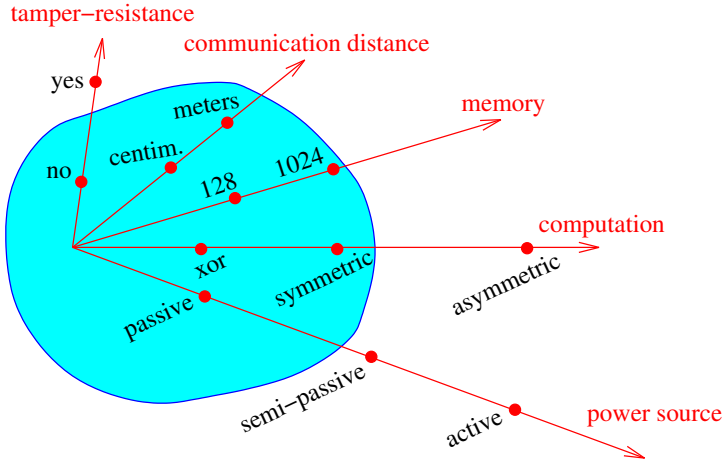


RFID in Daily Lives



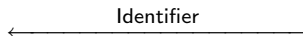
- **Identification** (e.g. Cattle identification)
- **Authentication** (e.g. Access control)
- **Data** (e.g. Passport, Sensors in Tyres)

Characteristics of Low-Cost Tags



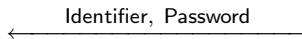
Reader

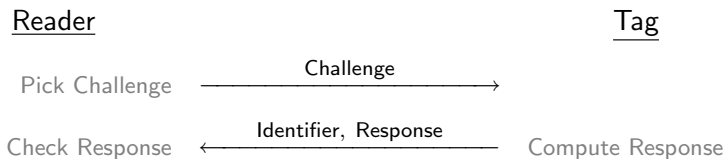
Tag



Reader

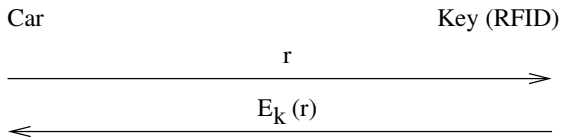
Tag





Some Interesting Security Problems in RFID

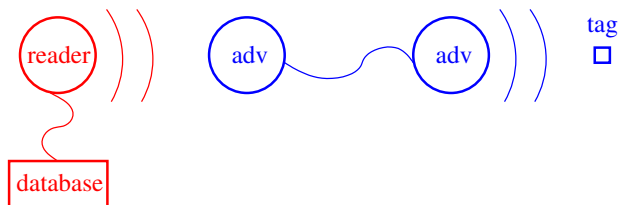
Digital Signature Transponder manufactured by Texas Instrument, used in automobile ignition keys (about **130 millions** DST modules).



Cipher uses **40-bit keys** allowing attack in less than **1 minute**

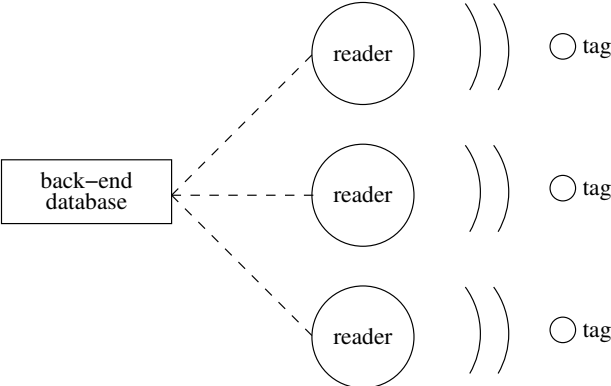
- 1 Recovering the cryptographic key
- 2 Impersonating the car ignition key
- 3 Impersonating the SpeedPass payment card

The reader believes that the tag is **within its field** while it is not the case (the attacker behaves as an **extension cord**).



Countermeasures consist in computing the **round trip time**.

Relieving the Back-End System



- Authentication **without revealing the identifier**.

- Authentication **without being tracked**.

(Given a set of interactions between provers and a verifier, an adversary must not be able to find any correlation in this set)

