

# La technologie RFID : un don de Dieu ou un défi du Diable ?

**Gildas Avoine**

EPFL, Lausanne, Switzerland



RFID Primer

Security Threats in RFID Systems

Enforcing Security and Privacy in RFID Systems

# RFID Primer

- What does RFID mean?
- What are the tags' characteristics?
- What's the purpose of the RFID?

Radio Frequency IDentification (**RFID**) is a method of remotely **identifying** objects or subjects using transponders (tags) queried through a **radio frequency** channel.

Google outputs more than **40 million** links related to “RFID”.

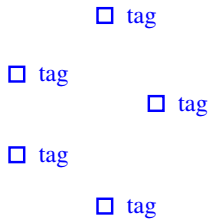
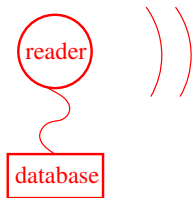
It was used during the **Second World War** by the RAF to distinguish allied aircrafts from enemy aircrafts.

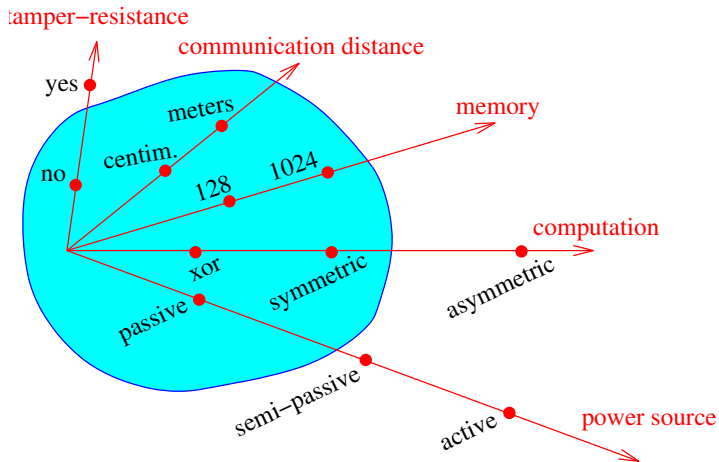
It has also been used **for many years** in: motorway tolls, ski lifts, identification of livestock and pets, automobile ignition keys, etc.

Today, we focus on **small** and **cheap** RFID tags.

- Management of stocks
- Libraries
- Anti-counterfeiting
- Access control
- Localization of people
- Electronic documents
- Counting cattle

Videos and heavy pictures have been removed from this version.





- Primal goal of RFID is to provide **security**
- Primal goal of RFID is to provide **functionality**

- Management of stocks
- Libraries
- Anti-counterfeiting
- Access control
- Localization of people
- Electronic documents
- Counting cattle

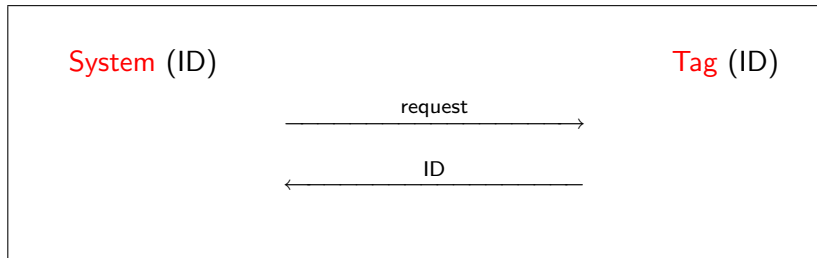
**Definition****Tag Authentication**

The authentication of a tag consists for the reader in obtaining the identity of the tag and a **proof** that the claimed identity is correct.

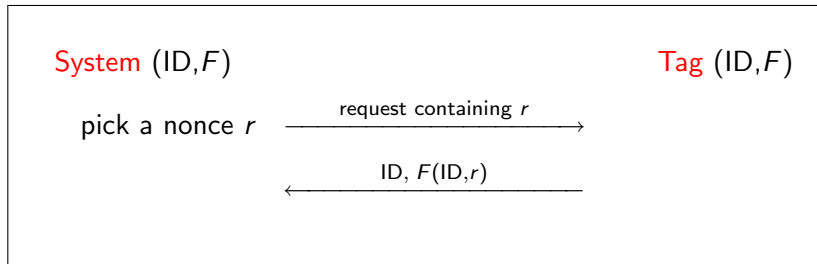
**Definition****Tag Identification**

The identification of a tag consists for the reader in obtaining the identity of the tag, but **no proof is required**.

**Example:** Systematic access controls force two people accessing the restricted area at the same time, both to pass the check.



Basic identification scheme

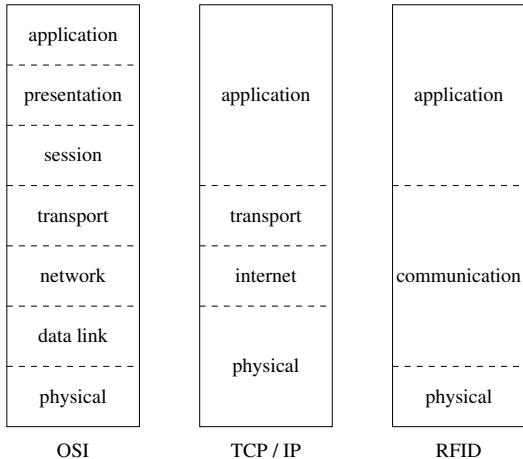


Basic challenge-response authentication scheme

# Security Threats in RFID Systems

- Denial of Service
- Impersonation
- Leakage of information
- Malicious traceability

Leakage of information + Malicious traceability = Privacy



## Definition

## Resistance to Impersonation

The probability is negligible that any adversary distinct from the tag, carrying out the protocol playing the role of the tag, can cause the reader to complete and accept the tag's identity.

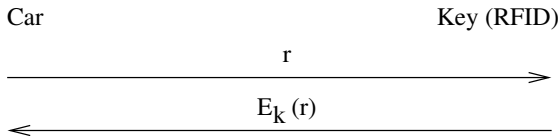
- An **authentication** protocol must be used
- The protocol must be **well designed**
- **Relay attacks** must be thwarted

Be careful! Sometimes identification solutions are sold as ensuring authentication!

**Example:** The RFID-based MIT ID Card.

**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.”

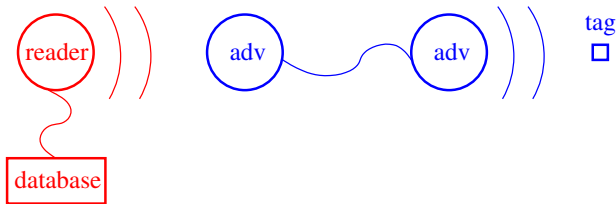
Attack of Bono *et al.* against the Digital Signature Transponder manufactured by Texas Instrument, used in automobile ignition key (more than **130 millions** DST devices exist).



Cipher (not public) uses **40 bit keys**: active attack in **less than 1 minute** (time-memory trade-offs)

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

**Relay Attack:** The reader believes that the tag is within its electromagnetic field while it is not the case. The attacker behaves as an extension cord.



The **information leakage** problem emerges when the data sent by the tag reveals information intrinsic to the marked object.

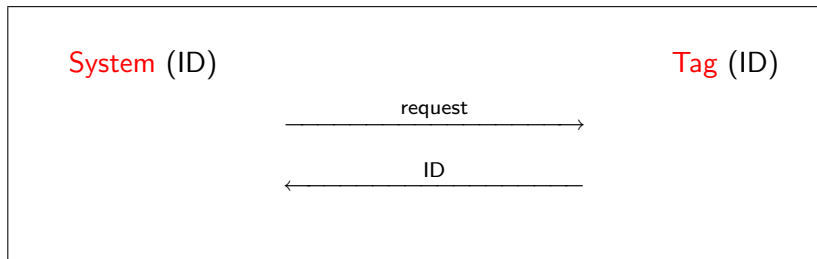
- Tagged books in **libraries**
- Tagged **pharmaceutical** products
- Electronic documents: **passports**, ID cards, etc.

**Definition****untraceability**

Given a set of readings between tags and readers, an adversary must not be able to find any relation between any readings of a same tag or set of tags.

**Example:** tracking of employees by the boss, tracking of children in an amusement park, tracking of military troops, etc.

Extension to **forward** untraceability.



Basic identification scheme

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

- Tags cannot be **switched-off**
- Tags answer **without the agreement** of their bearers
- Easy to **analyze the logs** of the readers
- Increasing of the **communication range**
- Tags can be almost **invisible**

Videos and heavy pictures have been removed from this version.

Even if you do not think that **privacy is important**, some people think so and they are rather influential (CASPIAN, FoeBud, etc.)

Videos and heavy pictures have been removed from this version.

## Enforcing Security and Privacy in RFID Systems

- Kill-command
- Faraday cages
- Blocker tags
- Combining both RFID and optical data
- Policies

How can we design an RFID protocol such that only an authorized party is able to **identify** a tag while an adversary is neither able to **identify** it nor to **trace** it?

The adversary should not be able to **distinguish** the information sent by the tag from a **random value**.

Protocols where the **reader is involved** in the refreshment of the information sent by the tag.

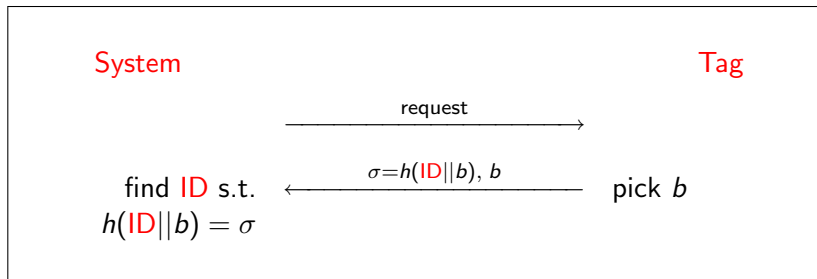
These protocols are only secure within a **weak adversary model**.

Protocol	Weaknesses pointed out by
[GolleJJS04]	[SaitoRS04], [Avoine05]
[SaitoRS04]	[Avoine05]
[HenriciM04]	[AvoineO05]
[Juels04]	[Juels04]
[JuelsP03]	[Avoine04], [ZhangK05]
[VadjaB03]	[VadjaB03]



Protocols where the reader is not involved, which are based on a **challenge-response**.

Protocol	Weaknesses pointed out by
[JuelsW05]	[GilbertRS05]
[WeisSRE02]	
[MolnarW04]	
[FeldhoferDW04]	
[RheeKKW05]	
[OhkuboSK03]	



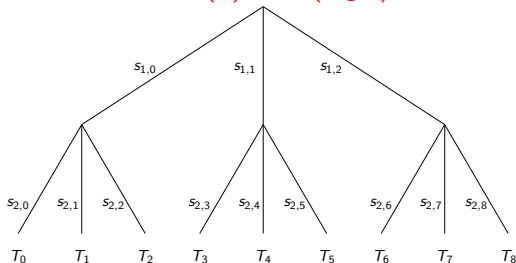
Protocol of Weis, Sarma, Rivest, and Engels  
(CHES 2002)

Challenge-response protocols are **secure** (in term of untraceability) if we deal with a pseudo-random function but suffer from a high **complexity**.

Contrary to the approach we usually take in cryptography, here the verifier **does not know the identity** of the prover before the protocol starts.

Is it possible to design an RFID protocol with a complexity **better than linear**?

[MW04] reduces the complexity of the identification of one tag from  $O(n)$  to  $O(\log n)$ .



$n$ : number of tags,  $\delta$ : branching factor  $\ell$  :, depth =  $\log_{\delta}(n)$

Identifying one tag requires  $\delta \log_{\delta}(n)$  operations instead of  $n$ .

**Trade-off** between complexity and traceability.

[AO04] reduces the complexity of the identification of one tag using a **time-memory trade-off**.

This technique requires a **precomputation phase** that consists in carrying out an exhaustive search once.

As efficient as [MW04], but **does not degrade** the privacy.

## Conclusion



*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.*  
By Klaus Finkenzeller.



*RFID: Applications, Security, and Privacy.*  
By Simson Garfinkel and Beth Rosenberg (Eds)



*Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID.*  
By Katherine Albrecht and Liz McIntyre

- <http://www.rfidjournal.com>
- <http://www.epcglobalinc.org>
- <http://www.rfidanalysis.org>
- <http://www.spsychips.com>
- <http://lasecwww.epfl.ch/~gavoine/rfid>