

# RFID Security Issues

Gildas Avoine

Lecture Selected Topics on Security and Cryptography

EPFL, Lausanne, Switzerland

April 2005

*(Pictures and videos have been removed from this downloadable version)*



- Google outputs **10'800'000** links related to “RFID”.
- More than **40** research papers related to security in RFID systems published between 2002 and 2005.
- In 2004, Kevin Ashton, Co-founder of the Auto-ID Center, predicted that more than **half trillion** tags would be consumed annually by 2010.
- Every magazine or daily newspaper publishes articles on RFID technology.

*(Pictures and videos have been removed from this downloadable version)*

Who knows precisely what is the RFID technology?

What is the goal of the RFID technology?

Is it a new technology?

What are the capabilities of this technology?

What is the link between RFID and security?

What about privacy?

Chapter 1: RFID Primer

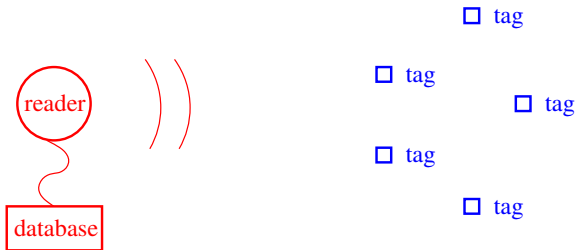
Chapter 2: Classical Security Issues

Chapter 3: Privacy Issues

Chapter 4: Adversarial Model

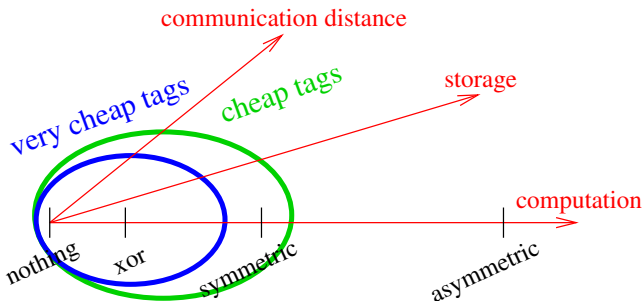
# Chapter 1: RFID Primer

**R**adio **F**requency **I**dentification: Identification of objects remotely by embedding in these objects tiny devices (**tags**) capable of transmitting data.



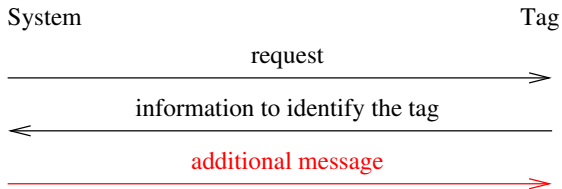
Security analysis consider **database** and **reader** as a unique entity.

The RFID technology is not new e.g. **military applications** (from several decades), **commercial applications** (from several years).



The boom which RFID technology is enjoying today relies essentially on the willingness to develop **small** and **cheap** RFID tags.

Most of the RFID protocols rely on a 3-round protocol.



- Frequency
- Extremely limited storage and computation capabilities
- No battery
- Not tamper-resistant
- Low cost

*(Pictures and videos have been removed from this downloadable version)*

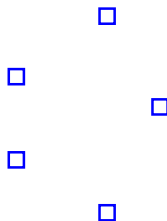
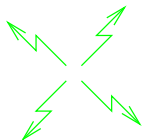
- Management of stocks (Wal-Mart, Gillette, etc.)
- Libraries (Santa Clara Library, University of Nevada, etc.)
- Anti-counterfeiting
- Pets identification
- Recycling
- Sensor networks (Michelin's tyres, etc.)
- Automobile ignition keys (Texas Instruments, etc.)
- Localization of people (Amusement parks, etc.)

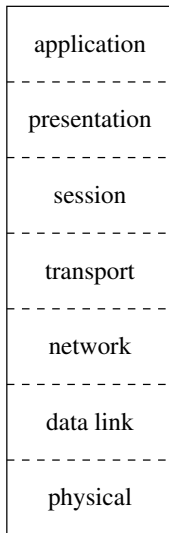
**Authentication:** we want to be sure that we speak with the correct party (proof required)

**Identification:** we want to know with who we speak (no proof required)

## Chapter 2: Classical Security Issues

**Physical denial of service:** the attacker interferes on the frequency band.



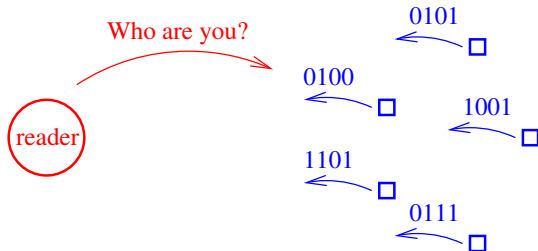


OSI



RFID

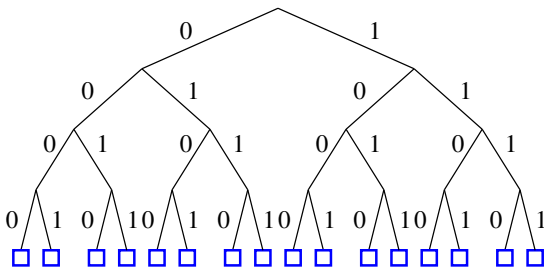
Denial of service in the communication layer:



The computational power of the tags is very limited and they are unable to communicate with each other:  
the reader must deal with the collision avoidance itself.

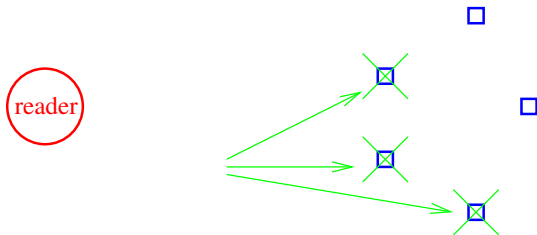
- The access to the communication channel is split into time slots (slotted Aloha).
- The number of slots is chosen by the reader which informs the tags they will have  $n$  slots to answer.
- Each tag randomly chooses one slot among the  $n$  and responds when its slot arrives.
- Collisions can occur.
- In order to recover the missing information, the reader interrogates the tags one more time, possibly with a larger  $n$ .

Deterministic protocols are based on a binary tree search which represents the identifiers of the tags.



An attacker can simulate the whole tree. Blocker tags [JRS03] use this technique to enforce privacy.

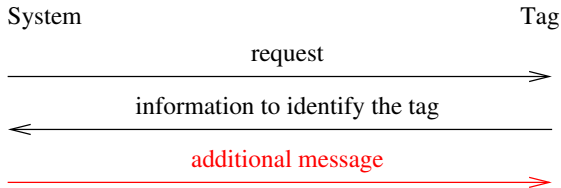
Destruction of tags: physical destruction, kill key, etc.



Hiding the tags: Faraday cage, sleep key, etc.

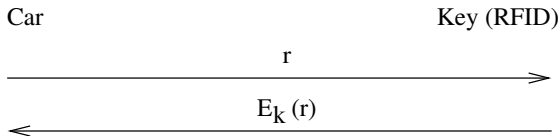


## Impersonation of tags:



Easy if the information sent by the tag is **static**. Require to **tamper with** the tag otherwise.

Attack of Bono *et al.* [BGSJRS05] against the Digital Signature Transponder manufactured by Texas Instrument, used in automobile ignition key (there exist more than 130 millions such keys).



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

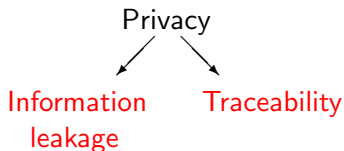
*(Pictures and videos have been removed from this downloadable version)*

Cheap RFID tags (which are not tamper-resistant) are not suited to authentication! Strong security has a cost!

“Marketing pressure” implies trade-off between security and cost.

Ratio cost / benefit e.g. we can not use a unique key in all the tags because the cost is negligible compared with the benefit.

## Chapter 3: Privacy Issues



**Information leakage:** The tag reveals some information related to the object holder.

**Traceability:** An adversary could track the tag, and therefore its bearer.

- Easier to track with RFID than other technologies e.g. video, credit cards, GSM.
  - Tags cannot be **switched-off**
  - Tags can be almost **invisible**
  - Easy to **analyze the logs** of the readers (e.g. data mining)
  - Increasing of the **communication range**
- Companies suffer from boycott campaigns

- **Physical solutions** e.g. Faraday cages, blocker tags, kill the tag
- **Software solutions** based on Cryptographic protocols

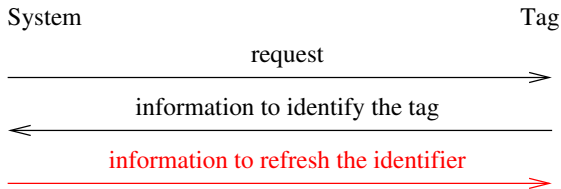
How designing an RFID protocol such that only an authorized party is able to **identify** a tag while an adversary is not able to **track** it?

## Protocols for **very cheap** tags

**no** cryptographic function in the tags (only xor)

## Protocols for **cheap** tags

**symmetric** cryptographic functions in the tags



The information must be indistinguishable from a random value

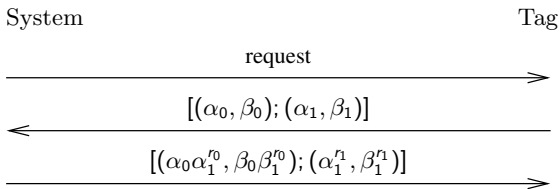
The information need to be refreshed each time the tag is requested

All these (analyzed) protocols suffer from weaknesses

[GJJS04] based on a **universal re-encryption** scheme i.e. a scheme where re-encryptions of a message  $m$  are performed neither requiring nor yielding knowledge of the public key.

Let  $E$  be the ElGamal encryption scheme, and  $U$  be the corresponding re-encryption scheme, we have  $U(m) := [E(m); E(1_G)]$ . Let  $q$  be the order of  $\mathcal{G}$ , and  $g$  a generator.

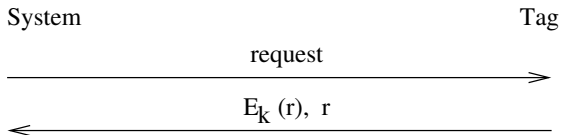
- **Key generation:** private key  $x \in \mathbb{Z}$  and public key  $y = g^x$ .
- **Encryption:** let  $(r_0, r_1)$  be a random element picked in  $\mathbb{Z}_q^2$ .  
 $U(m) = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(my^{r_0}, g^{r_0}); (y^{r_1}, g^{r_1})]$ .
- **Decryption:** given the ciphertext  $[(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ , if  $\alpha_0, \beta_0, \alpha_1, \beta_1 \in \mathcal{G}$  and  $\alpha_1/\beta_1^x = 1$ , then the plaintext is  $\alpha_0/\beta_0^x$ .
- **Re-encryption:** let  $(r'_0, r'_1)$  be a random element picked in  $\mathbb{Z}_q^2$ .  
The re-encrypted value of a ciphertext  $[(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$  is  $[(\alpha_0\alpha_1^{r'_0}, \beta_0\beta_1^{r'_0}); (\alpha_1^{r'_1}, \beta_1^{r'_1})]$ .



If an attacker sends a fake re-encrypted identifier to the tag, the database will not be able to identify the tag in the future.

[GJS04] claims that this attack does not allow the tag to be traced, at the most it will harm the normal functioning of the system.

Attacks in [SRS04] and [Avo05].



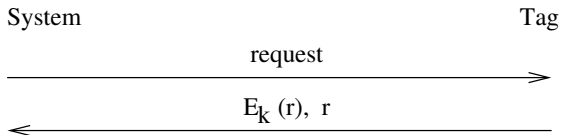
The key  $k$  is the identifier of the tag. The second message must be indistinguishable (by an attacker) from a random value. Thus the protocol can be proven to be secure.

The main difference with well-known authentication protocols is that the system does not know with which party it speaks with and therefore does not know which key  $k$  it should use.

The system carries out an exhaustive search over all the symmetric keys it stores.

**Problem:** If an attacker is able to tamper with the tag, she can track its past events.

**Exercise:** Propose a protocol which thwarts this problem. Instead of using an encryption function, use hash chains.



We assume that the system manages  $n$  tags.

- $k$  is the same for all tag:

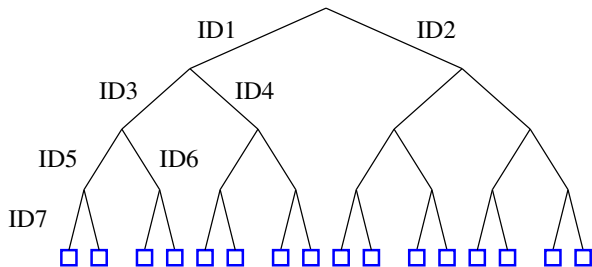
To identify one tag:  $O(1)$

- $k$  is different for each tag:

To identify one tag:  $O(n)$

To identify the whole system i.e.  $n$  tags:  $O(n^2)$

- [OSK04] degrades the privacy compared with [OSK03]: if an attacker can tamper with the tag, she can track (a given number of) its past events.
- [AO05] improved [OSK03]: it does not degrade privacy but requires memory and pre-computations.
- [MW04] reduces the complexity of the identification of one tag from  $O(n)$  to  $O(\log n)$  but...

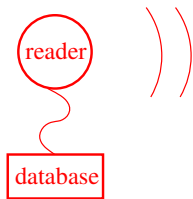


Identification of one tag:  $O(\log n)$  requests,  $O(\log n)$  identifiers stored in the tag,  $O(\log n)$  decryptions.

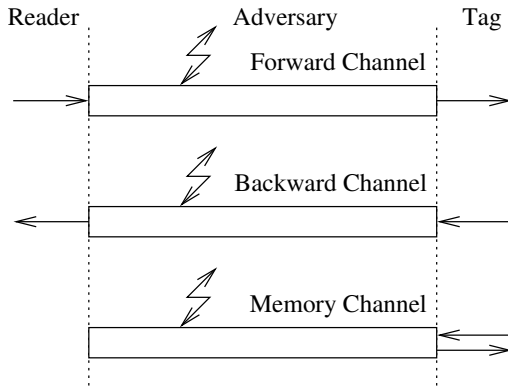
## Exercise:

- 1 Why can we say that this technique degrades the privacy?
- 2 How can an attacker track tags probabilistically?

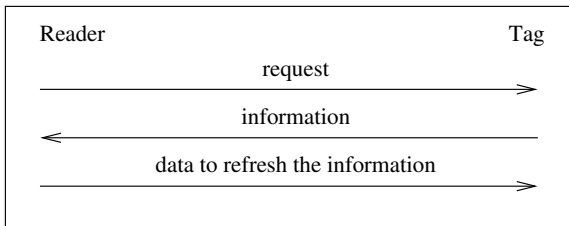
## Chapter 4: Adversarial Model



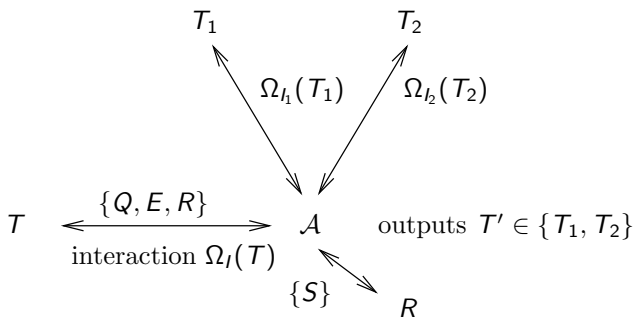
The sources of information which can benefit an adversary are limited to the channels between the reader and the tag i.e., **forward channel** and **backward channel**, as well as the contents of the **memory** of the tag.



- **Query**( $\pi_T^i, m$ ):  $\mathcal{A}$  requests  $T$  through the forward channel and sending him the message  $m$  after having received its answer.
- **Send**( $\pi_R^j, m$ ):  $\mathcal{A}$  sends the message  $m$  to  $R$  through the backward channel and receiving its answer.
- **Execute**( $\pi_T^i, \pi_R^j$ ):  $\mathcal{A}$  executes an instance of  $P$  between  $T$  and  $R$ , obtaining so the messages exchanged on both the forward and the backward channels.
- **Reveal**( $\pi_T^i$ ):  $\mathcal{A}$  obtains the content of  $T$ 's memory channel.



After having interacted with a target tag  $T$  and possibly some readers and thus obtaining an **interaction**  $\Omega_I(T)$ , an adversary  $\mathcal{A}$  needs to find his target among two tags  $T_1$  and  $T_2$  which are presented to him. In order to do this, he can query both  $T_1$  and  $T_2$ , thus obtaining two interactions  $\Omega_{I_1}(T_1)$  and  $\Omega_{I_2}(T_2)$ .



The **advantage** of the adversary for a given protocol  $P$  is:

$$\text{Adv}_P^{\text{UNT}}(\mathcal{A}) = 2 \Pr(T' = T) - 1$$

If  $\mathcal{A}$ 's advantage is negligible,  $P$  is said to be **UNT- $\mathcal{O}$**  secure, where  $\mathcal{O} \subset \{Q, S, E, R\}$ .

One can mix and match the **goals** {Existential-UNT, Forward-UNT, Universal-UNT} of the adversary and his **means**  $\mathcal{O} \subset \{Q, S, E, R\}$ .

$$(\forall \mathcal{O}, \mathcal{O}' \subset \{Q, S, E, R\}, \mathcal{O}' \subset \mathcal{O}) \implies (\text{UNT-}\mathcal{O} \implies \text{UNT-}\mathcal{O}')$$

$$\text{Existential-UNT} \begin{array}{l} \implies \\ \not\Leftarrow \end{array} \text{Forward-UNT} \begin{array}{l} \implies \\ \not\Leftarrow \end{array} \text{Universal-UNT}$$

$$\text{UNT-QSER} \implies \text{UNT-QSE} \implies \begin{array}{|l} \text{UNT-E} \\ \text{UNT-Q} \end{array}$$

Protocol	is	is not
Golle <i>et al.</i>	–	Existential-UNT-Q Existential-UNT-E
Saito <i>et al.</i>	–	Existential-UNT-Q
Saito <i>et al.</i> , reloaded	–	Universal-UNT-QS
Henrici and Müller	–	Existential-UNT-Q Universal-UNT-QE
Weis <i>et al.</i>	Existential-UNT-QSE	Forward-UNT-QSER
Ohkubo <i>et al.</i>	Existential-UNT-QSE Forward-UNT-QSER	

## Conclusion

- Design of “not too bad” RFID protocols suited to **very cheap** tags.
- Reduction of the complexity of the RFID protocols suited to **cheap tags**.
- Formalization of the notion of **privacy**.

- *Sanjay Sarma, Stephen Weis, and Daniel Engels.* RFID systems and security and privacy implications.
- *David Molnar and David Wagner.* Privacy and Security in Library RFID: Issues, Practices, and Architectures.
- *Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita.* Cryptographic Approach to “Privacy-Friendly” Tags.
- *Gildas Avoine.* Adversarial Model for Radio Frequency Identification.

<http://lasecwww.epfl.ch/~gavoine/rfid/>