

RFID: A New Challenge for Cryptographers?

Gildas Avoine

EPFL, Lausanne, Switzerland



RFID Primer

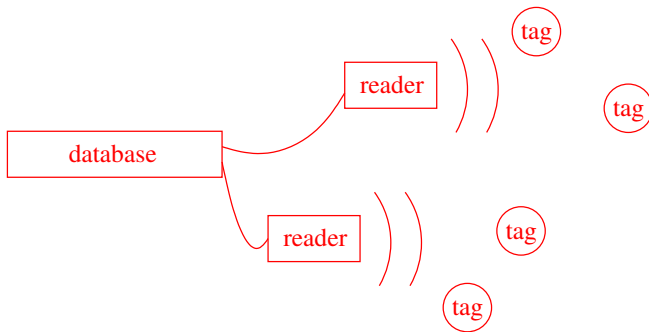
Cryptographic RFID Protocols

Adversarial Model

RFID Primer

Radio Frequency Identification

Identify objects remotely by embedding tiny devices capable of transmitting data into these objects.



The **RFID technology is not new**, e.g., contactless smartcards were already RFID devices (public transport, tollways).

The **Auto-ID center** has been created in 1999 at the MIT in order to promote and establish standards on **small** and **cheap** RFID technology.



Hitachi's μ -tag
(0.4mm \times 0.4mm \times 60 microns)

- Extremely limited storage and computation capabilities
- Not tamper-resistant
- No battery
- Reader-to-Tag channel: up to 100 meters
- Tag-to-Reader channel: up to a few meters

RFID tags could replace the bar-codes in the near future. RFID tags and bar-codes differ from several points:

- A tag can be remotely read **without optical access**.
- Tags can be read **en masse**.
- While a bar-code represents a lot of items, an RFID tag has its own **unique identifier**.

These properties open the door to **new applications**:

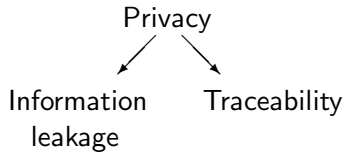
- Management of stocks and stocktakings
- Speed up the checkouts in the shops
- Libraries
- Recycling
- Pets identification
- Anti-counterfeiting
- Sensor networks

- **Wal-Mart** announced that it wants their suppliers to embed RFID tags in products at the pallet/carton level.
- **Michelin** has decided to implant RFID tags inside the rubber sidewall of its tires. These tags aim at pinpointing tires belonging to a defective batch.
- **Gillette** razors are one of the most shoplifted items in the world.
- **Benetton** planned to fit clothing with RFID tags.
- **Libraries** Santa Clara Library, University of Nevada, etc.

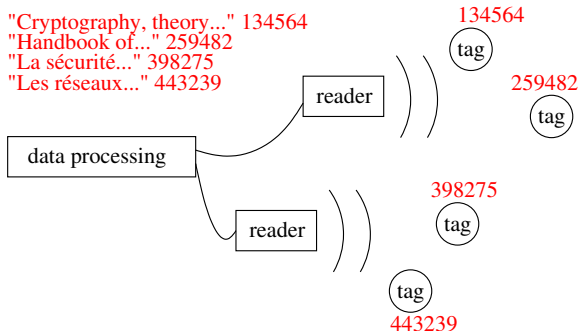
Threats on the system

Denial of service attacks, tag forgery, ...

Threats on the tag's bearers



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



Using **identifiers chosen randomly** such that only the data processing manager can match the identifiers with the corresponding items.

Traceability: Thanks to the tag's identifier, an adversary is able to track the tag, and therefore its bearer.

- Rather easy to track
- Also true in Bluetooth, GSM
- Boycott campaigns

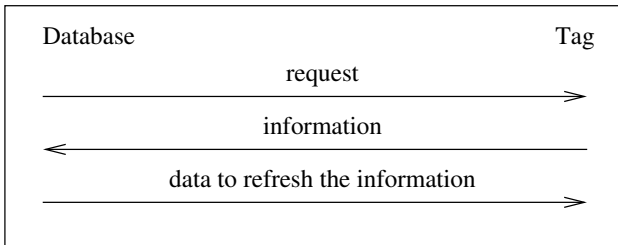
- Killing the Tags
- Interfering the request/answer
- Using a cryptographic protocol

The **goal** is to design an RFID protocol such that an authorized party only is able to **identify** a tag while an adversary is not able to **track** it.

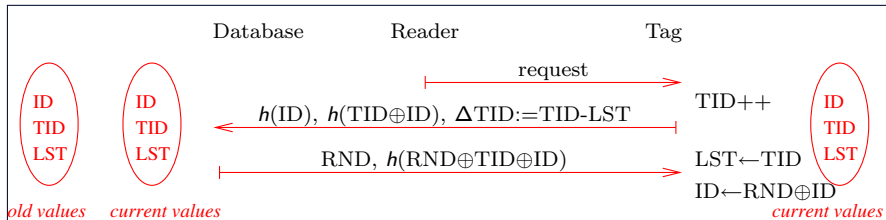
The idea of most of the existing protocols is to refresh the information sent by the tag each time it is queried by a reader s.t. these datas are not linkable by **unauthorized parties**.

Cryptographic RFID Protocols

- Identification or Authentication?
- Tamper-resistant?
- Cryptographic functions?
 - Prot. without cryptographic functions in the tag
 - Prot. with symmetric cryptographic functions in the tag
 - Prot. with asymmetric cryptographic functions in the tag

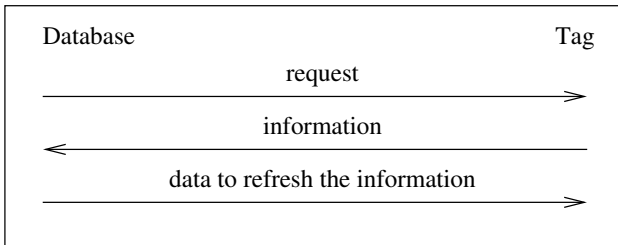


- Traceability is always possible between two “correct” identifications.
- The third message is usually vulnerable.
- Cryptographic functions are nevertheless needed to avoid traceability in the physical and communication layers.

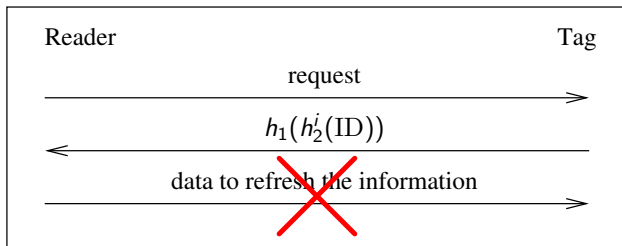


ID: Current identity, **TID**: Current session number, **LST**: Last successful session number Other protocols suffering from some flaws:

- Juels and Pappu,
- Golle, Jakobsson, Juels, and Syverson,
- Saito, Ryou, and Sakurai,
- Saito, Ryou, and Sakurai, reloaded.



- Traceability is always possible between two “correct” identifications.
- The third message is usually vulnerable.
- Cryptographic functions are nevertheless needed to avoid traceability in the physical and communication layers.

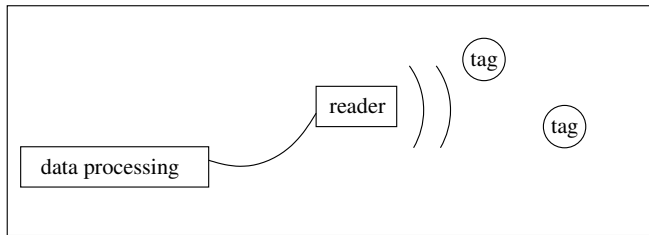


This protocol requires n operations to identify **one** tag (in the worst case), where n is the number of tags managed by the database, and requires n^2 operations to identify n tags.

This protocol requires n operations to identify **one** tag (in the worst case), where n is the number of tags managed by the database, and requires nk operations to identify n tags, where k is a parameter corresponding to the fixed length of the hash chains.

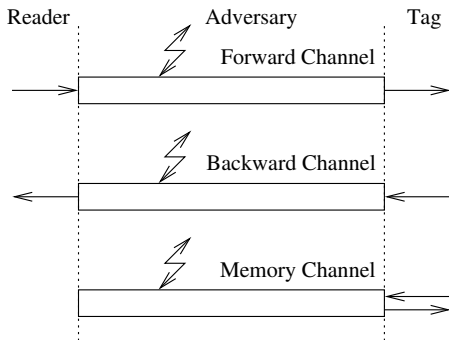
- Not possible due to the low capabilities of the tags.
- If asymmetric cryptography on the tags was possible, it may reduce the complexity: every tag has the public key of the system and encrypts its identifier with this public key.
- We could take benefit of the capacities of the reader: the encryption would require light computations while decryption would need heavier computations.

Adversarial Model

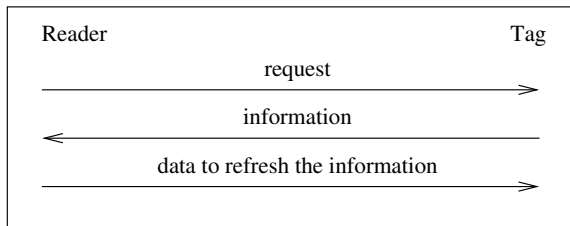


Studying the communication channel between the database and the readers is not relevant. Readers and database **are considered as a single and unique entity** in the analysis of security.

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(π_T^i, m): \mathcal{A} requests T through the forward channel and sending him the message m after having received its answer.
- Send(π_R^j, m): \mathcal{A} sends the message m to R through the backward channel and receiving its answer.
- Execute(π_T^i, π_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(π_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 $\Omega_{I_2}(T_2)$.

\mathcal{A}

T

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 $\mathcal{O} \subset \{Q, S, E, R\}$.

What differentiates **existential**, **universal**, and **forward** is the manner in which I_1 and I_2 are fixed.

- If there exist I_1 and I_2 such that the adversary is able to overcome the challenge then we talk of **existential traceability**.
- If he is able to win for all I_1 and I_2 , then we talk of **universal traceability**.
- If he is able to win for all I_1 and I_2 when $I > I_1, I_2$ meaning that $(\forall i, j, i \in I, j \in I_1 \cup I_2) \Rightarrow (i > j)$, then we speak of **forward traceability**.

Existential Untraceability (Parameters: l_{ref} , l_{chal} , \mathcal{O})

- 1 \mathcal{A} requests the *Challenger* thus receiving his target T .
- 2 \mathcal{A} chooses I and calls $\text{Oracle}(T, I, \mathcal{O})$ where $|I| \leq l_{\text{ref}}$ then receives $\hat{\Omega}_I(T)$.
- 3 \mathcal{A} requests the *Challenger* thus receiving his challenge T_1 and T_2 .
- 4 \mathcal{A} chooses I_1 and I_2 such that $|I_1| \leq l_{\text{chal}}$, $|I_2| \leq l_{\text{chal}}$, and $(I_1 \cup I_2) \cap I = \emptyset$.
- 5 \mathcal{A} calls $\text{Oracle}(T_1, I_1, \mathcal{O})$ and $\text{Oracle}(T_2, I_2, \mathcal{O})$, then receives $\hat{\Omega}_{I_1}(T_1)$ and $\hat{\Omega}_{I_2}(T_2)$.
- 6 \mathcal{A} decides which of T_1 or T_2 is T , then outputs his guess T' .

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

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

$$\text{Existential-UNT} \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \text{Forward-UNT} \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \text{Universal-UNT}$$

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

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

- Boom enjoyed by the RFID technology
- Most of the RFID protocols do not ensure privacy
- Secure protocols imply huge complexity
- Lack of formalism

`http://lasecwww.epfl.ch/~gavoine/rfid/`