

# Traceability in RFID Systems

Gildas Avoine

EPFL, Lausanne, Switzerland



Introduction and Motivation

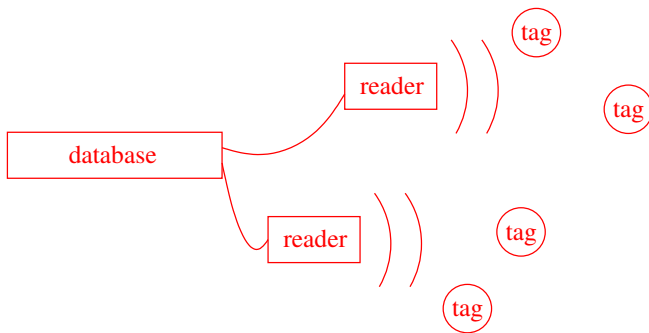
RFID Protocols

Adversarial Model

# Introduction and Motivation

## 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).

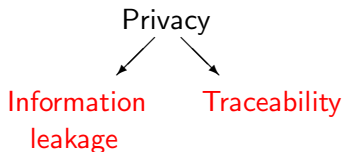
The current trend is to design and establish standards on **small** and **cheap** RFID tags.

- 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.

- Tags can be remotely read **without optical access**.
- Tags can be read **en masse**.
- Tags can be **re-writable**.
- Tags have **unique identifiers**.

- Management of stocks (Wal-Mart, Gillette, Benetton, etc.)
- Speed up the checkouts in the shops
- Libraries (Santa Clara Library, University of Nevada, etc.)
- Recycling
- Pets identification
- Anti-counterfeiting
- Sensor networks (Michelin, etc.)
- Localization

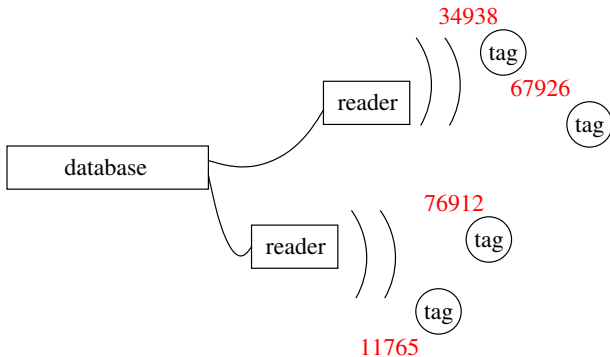


**Information leakage:** The tag reveals some information related to the object holder.

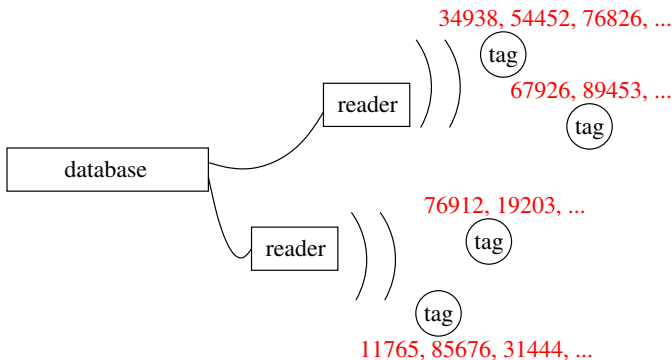
**Traceability:** An adversary could track the tag, and therefore its bearer.

- Companies suffer from boycott campaigns
- Easier to track with RFID than other technologies e.g. video, credit cards, GSM.
- Tags cannot be switched-off
- Tags can be almost invisible

The idea is to send an information which is **indistinguishable** by an adversary from a random value s.t. only the database is able to **link** the object with this information.

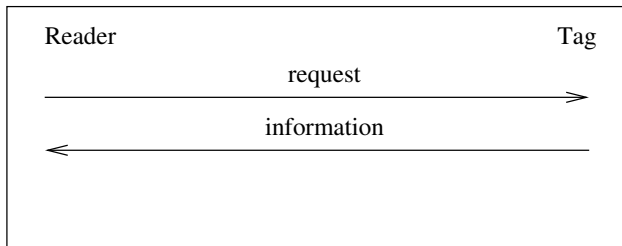


The idea is to **refresh** the information sent by the tag each time it is queried by a reader s.t. only the database is able to **link** the object with these different answers.

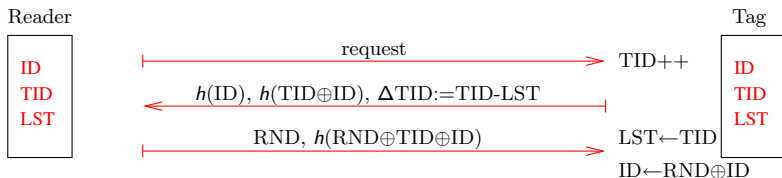


## RFID Protocols

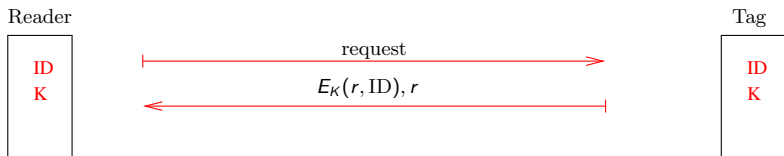
The **goal** is to design an RFID protocol such that an authorized party only is able to **identify** a tag while an adversary is not able to **track** it.



2-rounds protocol



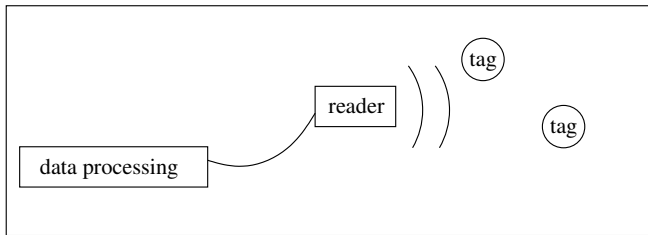
**ID:** Current identity, **TID:** Current session number, **LST:** Last successful session number



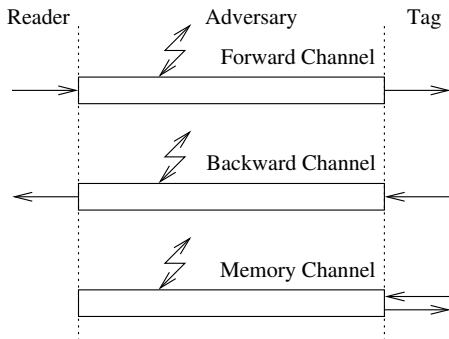
**ID**: Static identity, **K**: Key shared by the tag and the database,  
**E**: Symmetric encryption function

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

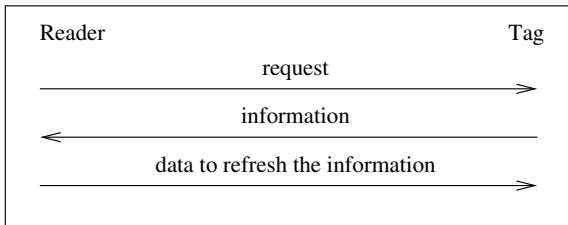
## Adversarial Model



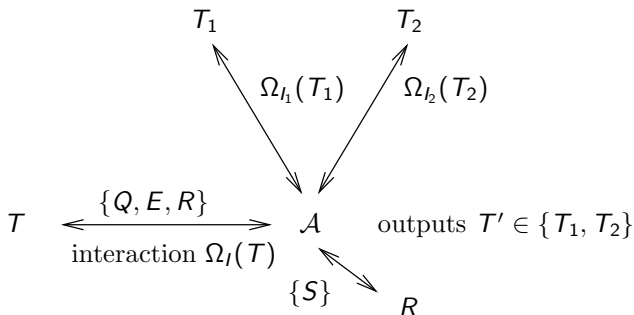
Studying the communication channel between the database and the readers is not relevant. Readers and database **are considered as a single and unique entity** in the analysis of security.



- $\text{Query}(\pi_T^i, m)$ :  $\mathcal{A}$  requests  $T$  through the forward channel and sending him the message  $m$  after having received its answer.
- $\text{Send}(\pi_R^j, m)$ :  $\mathcal{A}$  sends the message  $m$  to  $R$  through the backward channel and receiving its answer.
- $\text{Execute}(\pi_T^i, \pi_R^j)$ :  $\mathcal{A}$  executes an instance of  $P$  between  $T$  and  $R$ , obtaining so the messages exchanged on both the forward and the backward channels.
- $\text{Reveal}(\pi_T^i)$ :  $\mathcal{A}$  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**  $\mathcal{O} \subset \{Q, S, E, R\}$ .

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

$$\text{Existential-UNT} \begin{matrix} \Rightarrow \\ \neq \end{matrix} \text{Forward-UNT} \begin{matrix} \Rightarrow \\ \neq \end{matrix} \text{Universal-UNT}$$

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

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

- Boom enjoyed by the RFID technology
- Most of the RFID protocols do not ensure privacy
- Secure protocols imply huge complexity
- Very low cost asymmetric cryptography, time-memory trade-off
- Formalization