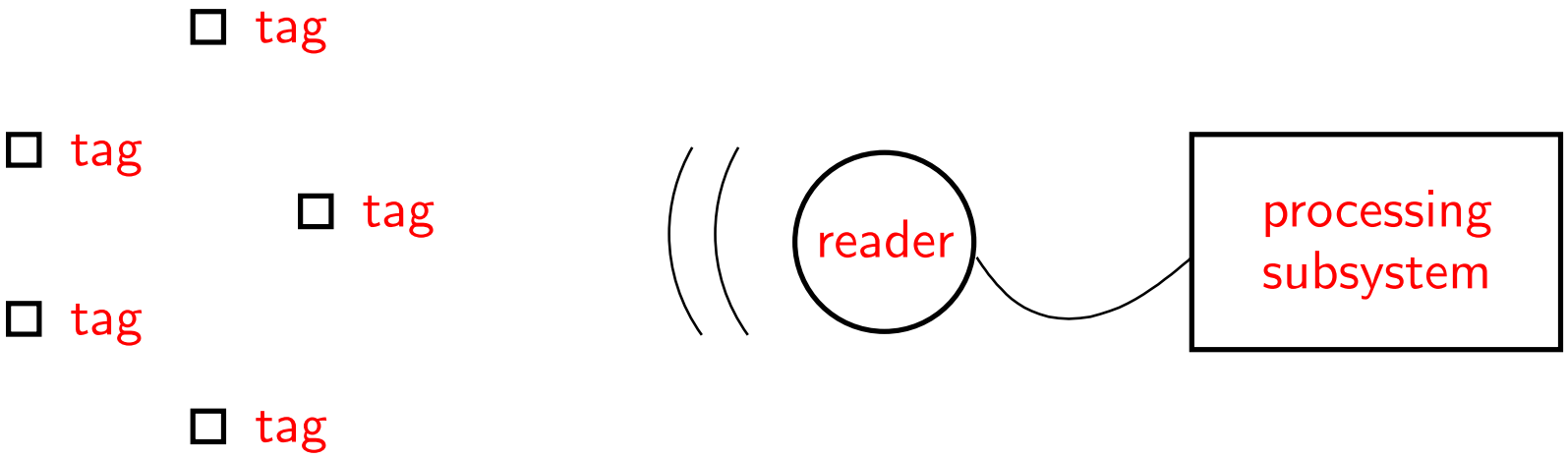
Malicious Traceability within RFID Systems

Gildas Avoine

EPFL, Lausanne, Switzerland

ITU-T Workshop "Networked RFID: Systems and Services"
Geneva, 14-15 February 2006

RFID Architecture



Threat Classification

- Denial of service
- Impersonation
  (tag authentication)
- Information leakage
  (reader authentication)
- Malicious traceability

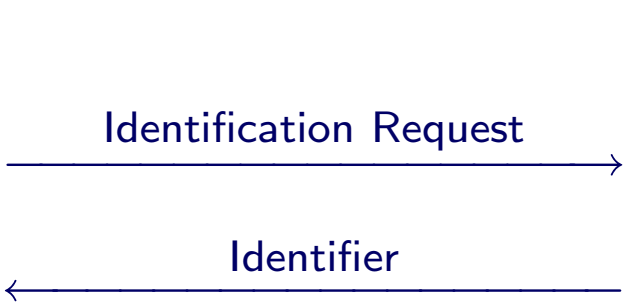
Malicious Traceability

Foreword

Malicious Traceability must be Considered Seriously

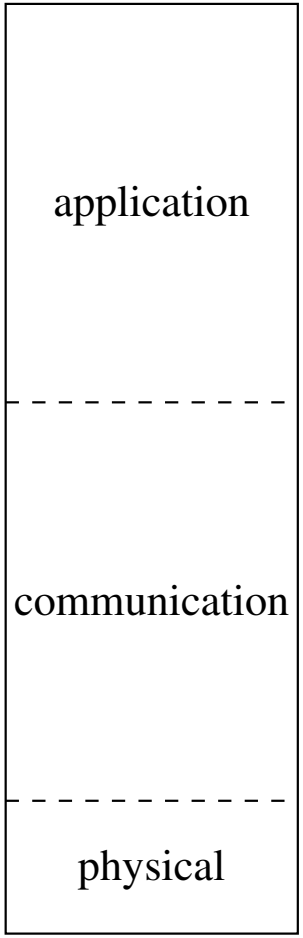
- Easier to track people using RFID than other technologies like Bluetooth, credit cards, video, etc.
  - Tags cannot be switched-off
  - Tags answer without the agreement of their bearers
  - Tags can be almost invisible
  - The trend is to increase the communication range
- Some applications are very sensitive like localization of children, pharmaceutical products, military applications, etc.
- Even if you do not think that privacy is important, some people think so and they are quite influential (CASPIAN, FoeBud)

Identification Protocol



- Use cryptographic primitives but
  - Not scalable
  - Expensive in terms of computation

Communication Model



Application layer
Identification protocol

Communication layer
Medium access protocol

Physical layer
Air interface (frequency, modulation, etc.)

Malicious Traceability Through the Layers

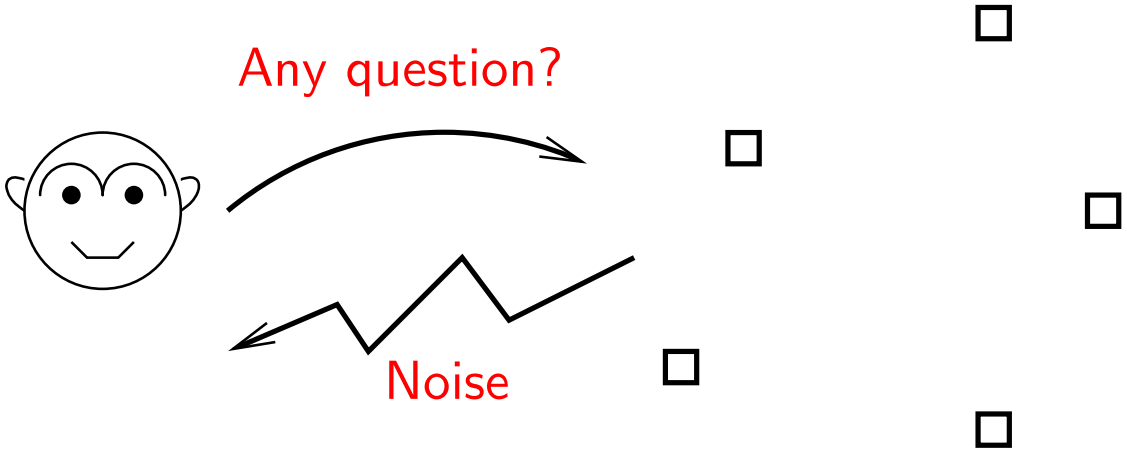
All efforts to prevent traceability in the application layer may be useless if no care is taken in the lower layers because information can leak from these layers.

Malicious traceability needs to be ensured at each layer

Malicious Traceability

The Communication Layer

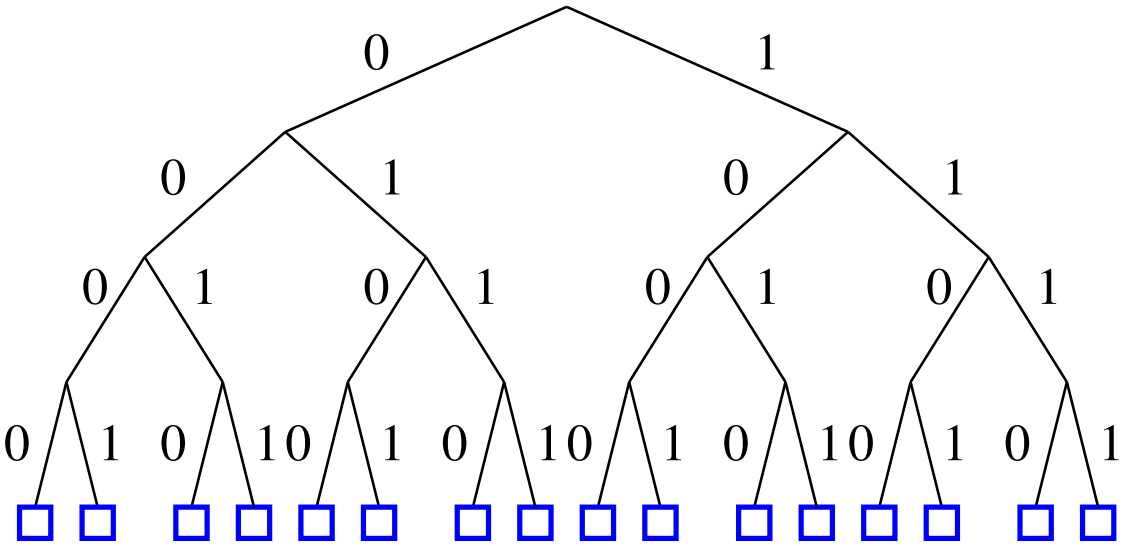
Collision Avoidance



- The reader must deal with the collision avoidance itself.
- Two families: deterministic and probabilistic protocols.

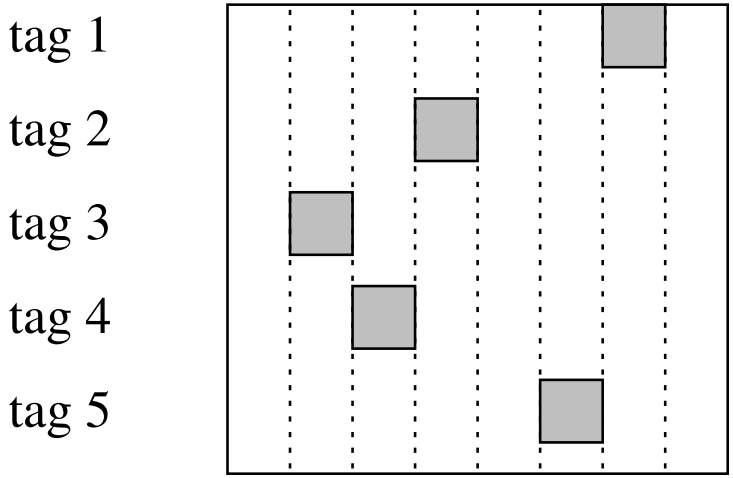
Deterministic Collision Avoidance

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



Probabilistic Protocols

Probabilistic protocols are based on a time division.



- The access to the communication channel is split into time slots (slotted Aloha).
- Each tag randomly chooses one slot and responds when its slot arrives.

Conclusion About the Communication Layer

- Tags can be traced easily thanks to the collision-avoidance protocol if no care is taken
- In practice, collision-avoidance protocols are not traceability-resistant
- Malicious traceability can be thwarted if a PRNG is used
- Lightweight solutions should be found

Malicious Traceability

The Physical Layer

Diversity of Standards

Signals from tags using different standards are easy to distinguish.

A problem arises when we consider sets of tags rather than a single tag.

If several standards are in use, each person in a few years may have a set of tags with a characteristic mix of standards which may allow a person to be traced.

Conclusion About the Physical Layer

Preventing traceability in the physical layer seems quite difficult because there is no benefit for the manufacturers in producing tags that use exactly the same technology.

Conclusion quite pessimistic in the physical layer but attacks within this layer require strong means.

CONCLUSION

Conclusion

- Not to afraid people about malicious traceability.
- Better understand this problem and to decide rationally, for a given application, whether or not this problem must be addressed.
- Using cryptographic tools in the application layer is not enough: malicious traceability must be addressed in the lower layers.
- Some solutions exist but research is still required to design lightweight solutions.
- RFID security becomes a very hot topic in the cryptography community.

More Information

http://lasecwww.epfl.ch/∼gavoine/rfid/

http://www.avoine.net