Cataloging RFID Privacy and Security

Marcel Queisser, Florian Dautermann, Pablo Guerrero,
Dr. Mariano Cilia, Prof. Alejandro Buchmann

Databases and Distributed Systems Group

Technische Universität Darmstadt, Germany

RFID Workshop 2006, July 4th, Fraunhofer IIS, Erlangen

TECHNISCHE
UNIVERSITÄT
DARMSTADT

DVS

Motivation

- Security and Privacy concern both the private and commercial sector
- Commercial sector:
  - Access control
  - Eavesdropping
- Private sector:
  - Information gathering
  - Traceability

Critical Security Problems in RFID Systems

- Denial of Service Attacks
  - there is no solution to this problem
- Information leakage
  - an unauthorized person or reader is able to obtain information about the tagged item

- Secure RFID System:
  - a system in which information leakage is impossible

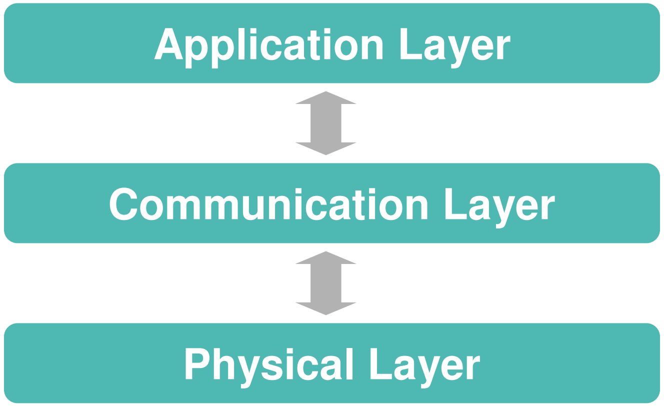
Critical Privacy Threats in RFID Systems

- Traceability
  - an unauthorized person or reader is able to link two sightings of the same tag

- Privacy Protecting RFID System:
  - a system which grants Non-Traceability

Layered Catalog of P&S Issues

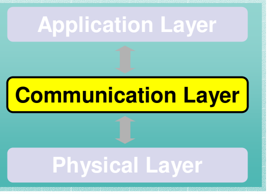
- Physical Layer
  - tracing a tag by its radio fingerprint or a person by the characteristic mix of tags
- Communication Layer
  - tracing a tag in an open Singulation Session
- Application Layer
  - eavesdropping
  - spoofing
  - tracing a tag by its unique identifier



Protection addressing the Physical Layer

- Erasing the tag ID
  - the ID of the tag can be shortened, removed (“killing”) or recoded
    - shortening does not solve all problems
    - removing prohibits benefits
    - recoding allows tracing
- Privacy-Protecting Tag
  - the size of the antenna can be reduced
    - tracking is only possible from a range of a few centimeters
    - overpowered / directed readers can enhance reading range

Attacks on the Communication Layer


Application Layer

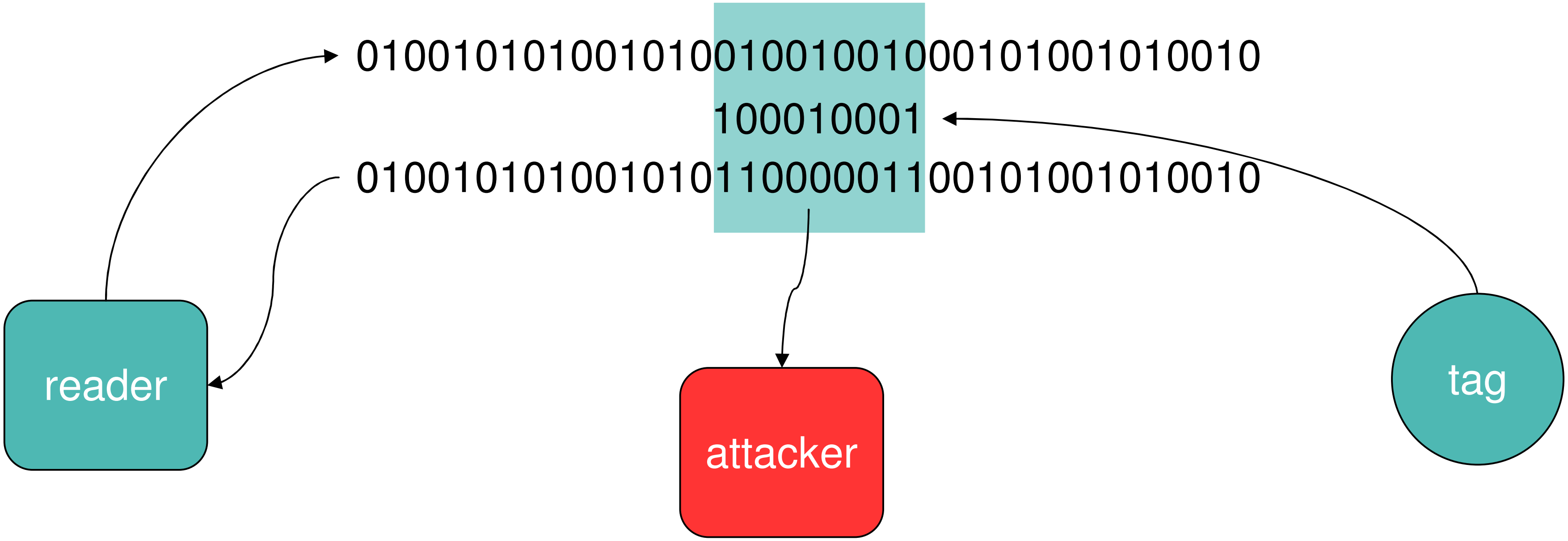
Communication Layer

Physical Layer

- Singulation is needed to guarantee undisturbed communication between a reader and several tags
  - there are deterministic and probabilistic approaches
- No change of ID during Singulation Sessions
  - tracing is possible
  - solution: timeouts

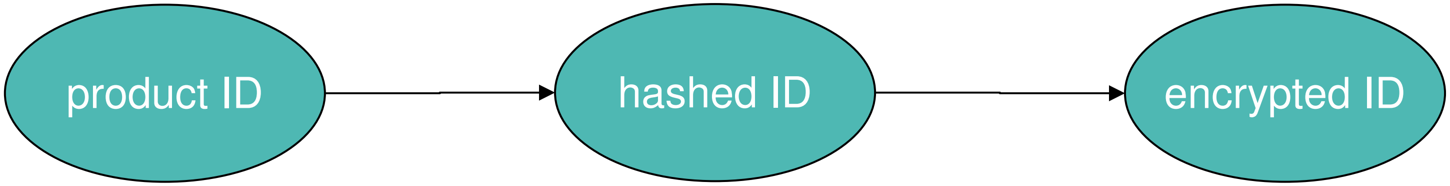
Cloaking

- Noisy Tags (Code-Based)
  - reader generates random bits
  - tag sends session key over the same channel
  - only reader can reconstruct session key



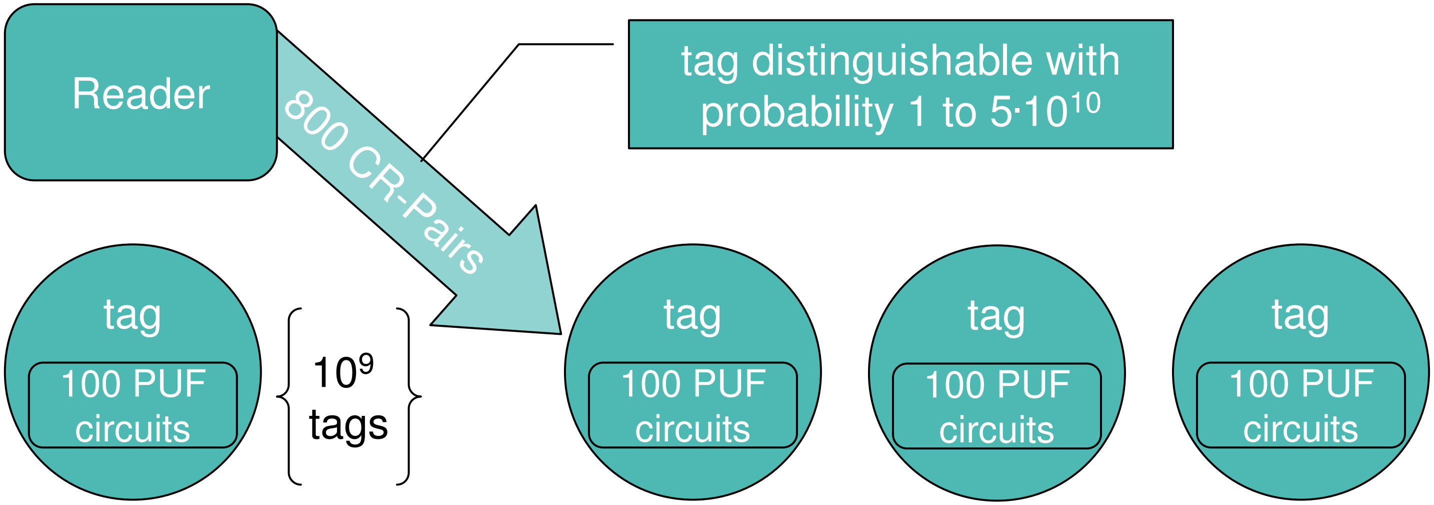
Encryption

- MACs - Message Authentication Codes
  - 128 bit ID is stored
    - constructed of the original ID using a hash function and encryption
- fabrication of fake tags is harder
- no information leakage
- Tracing is still possible



Tag authentication

- PUF Circuits
  - Challenge-Response-Protocol for tag authentication
    - challenges stored in database
    - responses created using individual chip characteristics
  - creation of fake tags is virtually impossible
  - vulnerable to replay attacks
  - huge amount of data in the backend

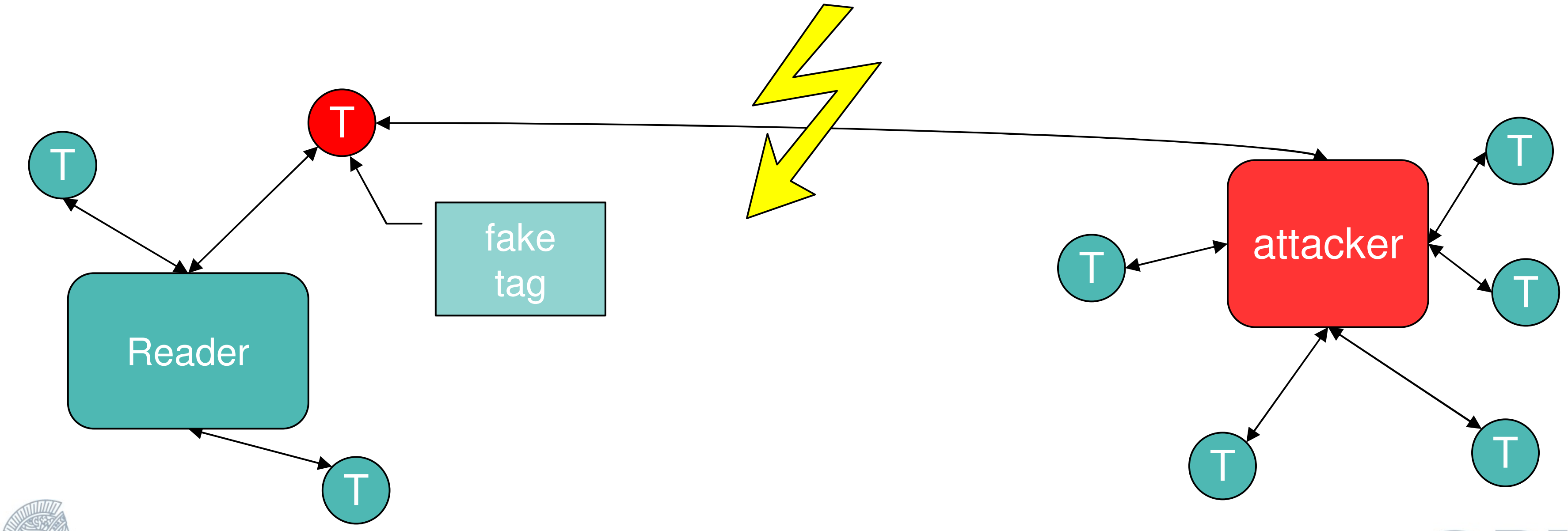


Protection for Low-Cost-Chips

- Many Shared Secrets
  - challenge response pairs stored on the tag
  - reader obtains next pair from database and challenges
  - mutual authentication
  - access limited by tag memory
  - must be online

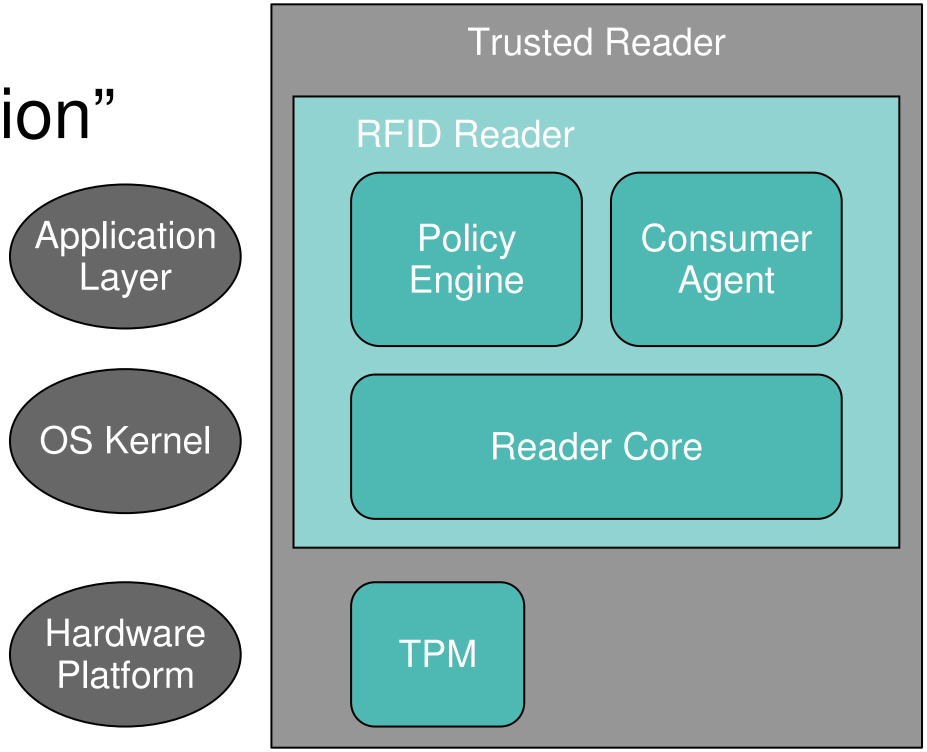
Distance Bounding

- Provides possibility to prevent relay attacks
- Guarantees the proximity of tag to reader
  - triangulation is used to calculate the distance
  - uses Challenge-Response-Protocol
  - correct response only accepted in a fixed time window

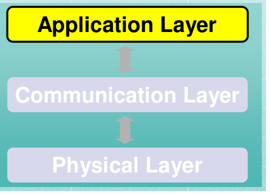


Trusted Computing

- Reader design divided into three parts:
  - Reader Core
  - Policy Engine
  - Consumer Agent
- Uses “Remote Attestation”
  - ensures S&P of communication if reader compromised
- Only suitable for online readers



Pseudonym Protocol



- Generation of pseudonym ID codes on questioning
  - inscrutable to a reader
  - application layer questions trusted center to get desired information
    - must authenticate itself
  - tracing is virtually impossible
  - must be online
    - trusted center can give next pseudonym IDs to read the tag more than once
  - ownership transfer is made easy

Conclusions

- RFID technologies have promised multiple benefits
  - can only be achieved if quality attributes are addressed properly
- Trust in RFID has to be established
  - only possible with secure, privacy-protecting interaction between tags and readers
- Tradeoff: Security/Privacy vs. Price per Tag
- Layered catalog helps to understand and to apply techniques
  - Keep extending the catalog with further techniques and eventually more layers

References

- G. Avoine and P. Oechslin. RFID Traceability: A Multilayer Problem. In Procs. Financial Cryptography and Data Security FC'05, Roseau, The Commonwealth of Dominica, Feb 2005
- M. Bhuptani and S. Moradpour. RFID Field Guide. Prentice Hall, 2005.
- C. Bornhovd, T. Lin, S. Haller, and J. Schaper. Integrating Smart Items with Business Processes: An Experience Report. Procs. 38th Hawaii International Conference on System Sciences, 08:227c, 2005.
- C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In Procs. International Conference on SmartCard Research and Advanced Applications CARDIS'06, Tarragona, Spain, Apr 2006.
- G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In Procs. 1st. IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, Sep 2005.
- F. Kahn. Can Zero-Knowledge Tags Protect Privacy? Cryptology ePrint Archive, Report 2005/049, Nov 2005.
- G. Karoth and P. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. Procs. ACM Workshop on Privacy in Electronic Society, Nov 2005.
- D. Molnar, A. Soppera, and D. Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In Procs. Workshop on RFID and Lightweight Crypto, Graz, Austria, Jul 2005.
- D. Molnar, A. Soppera, and D. Wagner. Privacy For RFID Through Trusted Computing. In Procs.Workshop on Privacy in the Electronic Society WPES'05, Alexandria, VA, USA, Nov 2005.
- D. Ranasinghe, D. Engels, and P. Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In Procs. Auto-ID Labs Research Workshop, Zürich, Switzerland, Sep 2004.