

What is RFID?

Does it make sense to have a specific domain devoted to security and cryptography in RFID?

Gildas Avoine

Université Catholique de Louvain
Belgium

RFID

- Radio Frequency Identification.
- “RFID is a **generic term** that is used to describe a system that **transmits the identity** (...) of an object or person wirelessly, using **radio waves**.”

Information Security Group

Université catholique de Louvain, B-1348 Louvain-le-Neuve, Belgium

<http://site.uclouvain.be/security/>

Identification

- Is it **only** identification?
- Is it **at least** identification?

The screenshot shows the RFIDSec18 Program website. The top part displays a schedule for the event, organized by time slots and activities. The bottom part lists the accepted papers, including their titles and authors.

Paper No.	Paper Title	Authors
Paper 1	Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model	Saxena, Nitesh, Voris, Jonathan
Paper 2	Cryptanalysis of the David-Prasad RFID Ultralightweight Authentication Protocol	Hernandez-Castro, Julio Cesar, Tapiador, Juan, C.W. Phan, Raphael, Pires-Lopes, Pedro
Paper 3	Practical NFC Peer-to-Peer Relay Attack using Mobile Phones	Francis Lishoy, Markantonakis, Konstantinos, Mayes, Keith, Handke, Gerhard
Paper 4	Strong Authentication and Strong Integrity (SAS) is not that Strong	Caipred, Xavier, Avouine, Gildas, Martin, Benjamin
Paper 5	On the claimed privacy of EC-RAC II	Fan, Junfeng, Vercauteren, Frederik, Hermans, Jens
Paper 6	EC-RAC: Enriching a Capacitance RFID Attack Collection	Radomirovic, Sasa, Van Deursen, Ton
Paper 7	Anonymous RFID Authentication using Trusted Computing Technologies	Dietrich, Kurt
Paper 8	Tree-Based RFID Authentication Protocols Are Definitely Not Privacy-Friendly	Martin, Tania, Martin, Benjamin, Avouine, Gildas
Paper 9	Privacy-Preserving Pattern Matching for Anomaly Detection in RFID	Kerschbaum, Florian, Oerter, Nina



Communication Model

- There are reader-tag communications only (no tag-tag).



- EPC Global considers peer-to-peer communications (class IV)

Communication Initiator

- Only the reader can initiate the communication
 - This partially discards the active RFID.

Operator Intervention

- The tag always answers **automatically without intervention** of the user.
- Not so bad, but **not perfect**:
 - What does “without intervention” mean? No button, but presence required.
 - Some technologies discarded.



Information Security Group

Université catholique de Louvain, B-1348 Louvain-le-Neuve, Belgium
<http://site.uclouvain.be/security/>

Computation Capabilities

- RFID tag = **low-capability** device.
- Where is the limit between a low-capability device and a powerful device?



RFID vs Contactless Smartcards

- People from the **smartcard** world usually consider that smartcards are not **RFID**.
 - RFID means **unsecure**.
- W/o **microprocessor**?

So... what?

- Contactless using radio waves?
- At least identification?
- Low-capabilities?
- Reader-Tag communication model?
- No intervention of the user in the communication process?

So... what?

- Next year's brainstorming: **When did the RFID appear?**