What is RFID?

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

Gildas Avoine

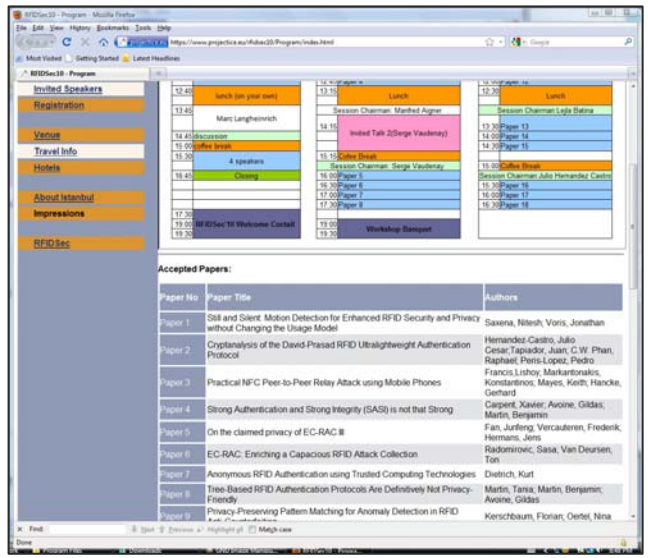
Université Catholique de Louvain
Belgium

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.”

Identification

- Is it only identification?



- Is it at least identification?

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.

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?