Advanced Cryptographic Protocols for RFID Tags

Giuseppe Ateniese

Syllabus

- Introduction, RFID tags, case study
- Proposed solutions for passive, symmetric-key, and public-key tags
- Proxy re-signature and re-encryption (proof of path, access control, etc.)
- Untraceable tags via insubvertible encryption

Monday

Sources

- "RFID Security and Privacy: A Research Survey" by Ari Juels (RSA Laboratories). A must-read survey.
- "Analysis of a Cryptographically-Enabled RFID Device" by S. Bono, M. Green, A. Stubblefield, A. Rubin, A. Juels, M. Szydlo. Usenix Security 2005 (http://rfidanalysis.org)

4

RFID Tags

- Radio-Frequency Identification (passively or actively powered)
- Chip+antenna
- RF wireless network
- Successor of the barcode

5

Fuzzy Definition

- Passively or actively powered RFIDs
- Smartcards
- Sensors
- My view

6

Current Main Applications

- Supply chains and Inventory
- Pet ID tags (human too...)
- Shoplifting prevention
- Vehicle identification (toll booths, plates)
- Anti-theft systems (Immobilizer)
- Payment systems (Speedpass, credit cards)
- Passports
- Detection of counterfeit pharmaceuticals
- Identification for access control

7

Future Applications

- Automated homes
- Shopping
- Post-sale services
- Etc.

8

Issues

- Tracking (no on/off switch, limited access control)
- Cloning
- Swapping

9

A Real Case

- Attack on TI DST
- Performed by JHU PhD students
- Details on http://rfidanalysis.org

Thanks to Matt Green for providing the next few slides + video