Tuesday

1

Sources

- "RFID Security and Privacy: A Research Survey" by Ari Juels, and references therein.
- "Strong Authentication for RFID Systems Using the AES Algorithm" by M. Feldhofer, S. Dominikus, and J. Wolkerstorfer
- "A Case Against Currently Used Hash Functions in RFID Protocols" by M. Feldhofer and C. Rechberger
- "An Elliptic Curve Processor Suitable For RFID-Tags" by L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede
- "Authenticating pervasive devices with human protocols." by A. Juels and S. Weis.
- "Security and Privacy Issues in E-passports" by A. Juels, D. Molnar, and D. Wagner
- "Crossing Borders: Security and Privacy Issues of the European e-Passport" by Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur

2

Solutions

- Passive RFID tags
- Symmetric-key RFID tags
- Public-key RFID tags

3

Passive RFID tags

- Practically storage devices
- Simply return what is in memory
- Could be re-writable
- Do not perform any type of computation

4

- Killing the tag
- Relabeling (once or several times from a pool of pseudonyms)
- "Re-encryption"

5

- Proxy devices
- Distance metric
- Blocking via privacy bit

6

Symmetric-key RFIDs

- Limited computational power (typically hash functions or "custom-made" MACs, AES, 3DES, etc.)
- Few thousand gates
- Very cheap ==> no tamper resistance
- Affected by timing attacks, power analysis, etc.

7

- Shared-key challenge-response authentication protocols
- Man-in-the-middle attacks

8

- Privacy and key discovery
  - Tag emits encrypted nonce, (P, E_k(P))
  - Reader searches for the key
  - Alternatively, tag could emit E_k(c_i)

9

- HB and HB+
  - HB for passive attackers
  - HB+ for active attackers

10

Reader Tag

$a \in_R \{0,1\}^k$

a →

$v \in \{0,1\}$,
$P[v = 1] = \gamma$

← $z = a \cdot x \oplus v$

Accept if $z = a \cdot x$

11

- Guessing will fail r/2 times and reader expects fewer than (r gamma) incorrect answers
- Binary inner product is very efficient
- The noise bit v can be generated from physical properties

12

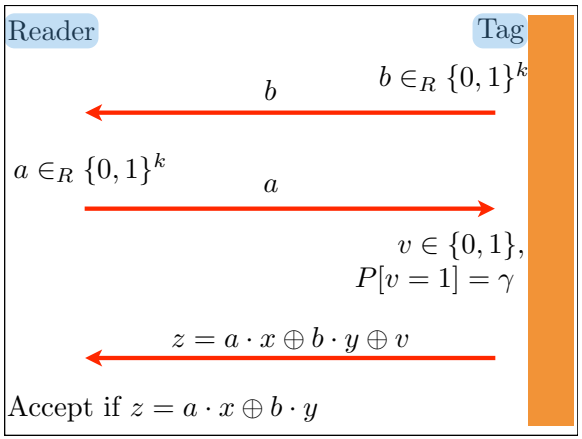
Security based on LPN (Learning Parity in the Presence of Noise):

Let A be a random $q \times k$ binary matrix, let x be a random k-bit vector, let $\gamma \in (0, 1/2)$, and let v be a random q-bit vector such that $|v| \leq q\gamma$.
Given A, $z = (A \cdot x) \oplus v$, find a k-bit vector x' such that $|(A \cdot x') \oplus z| \leq q\gamma$.

13

- Active attack against HB
- New solution in the detection model

14



15

Public-key RFIDs

- Capable of performing costly operations
- Typically modular add./mult. and exponentiations
- RFID tags in future passport (ICAO specs)?
- Current proposals are based on Elliptic-Curve Cryptography (ECC)

16

- Feldhofer et al. show that AES requires less than 5K gates
- Feldhofer and Rechberger argue that standard hash functions cost more than AES on RFID tags
- Batina et al. show that an EC processor is feasible on RFID tags. It requires about 8.5K~14K gates

17

A case study: US Passports

- International Civil Aviation Organization (ICAO) guidelines
- The chip must contain name, DOB, passport #, and digitized picture, optionally fingerprint and iris data
- In the future also digital visas or information on recent travels
- RF blocking material in the cover (Faraday cages)

18

Issues

- Security Issues
- Privacy Issues
- RFID vs. Contact tag. Hoepman et al. suggest:
  - Higher data rates
  - No wear
  - No change of standard format

19

Cryptography

- Passive authentication: Data on the tag must be signed (RSA, DSA, ECDSA)
- Basic access control: Optical scanning of the key to enforce access control
- Secure Messaging: Messages are encrypted and authenticated
- Active authentication: Challenge-response protocol

20

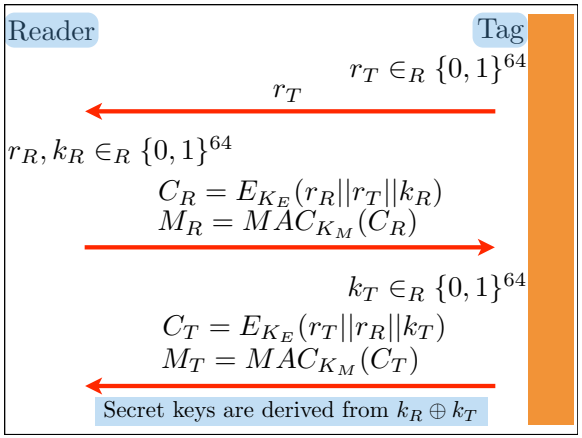
Basic Access Control

Reader Tag

Key Seed is generated from passport #, DOB, expiration date

$$K_{Seed} \longrightarrow K_E, K_M$$

21



22

- Problems:
  - Low entropy
  - Fixed Keys K_E, K_M (no access revocation)

23

Secure Messaging

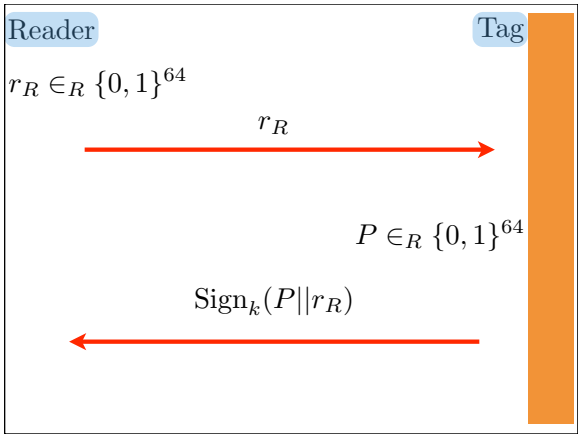
- Messages are encrypted and authenticated
- Secret keys are derived from the seed generated after BAC
- A counter is used to prevent replay attacks

24

Active Authentication

- Anti-cloning measure
- The tag must be able to sign (RSA-based signature)
- A public key must be tied to the passport via optical scanning
- If not after BAC, tracking could be an issue (unique modulus, etc.)

25



26

Current deployments

- See http://rfidiot.org/
  - Australian passport
  - Italian passport
  - US passport

27