50 ways to break RFID privacy

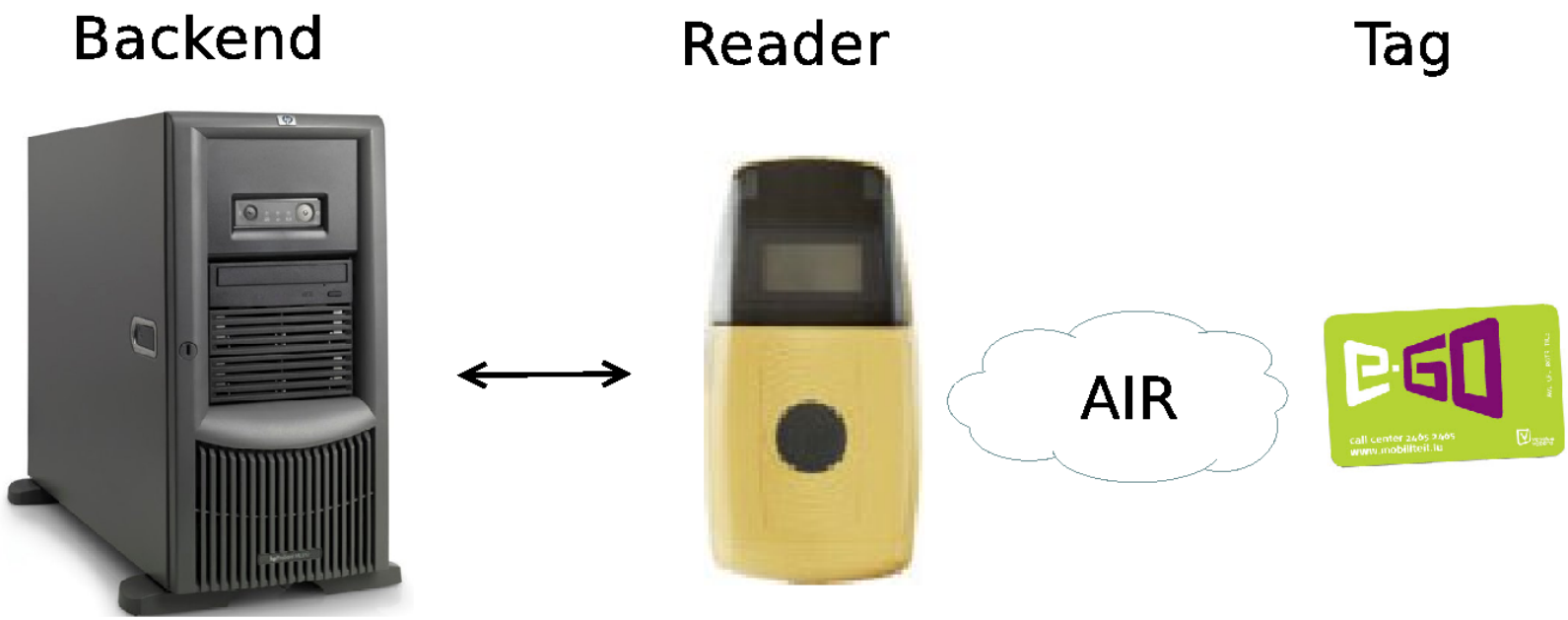
Ton van Deursen[1]
University of Luxembourg
ton.vandeursen@uni.lu

[1]Financial support received from the Fonds National de la Recherche (Luxembourg).

Outline

- Radio frequency identification (RFID)
- Privacy considerations in RFID
- RFID layered communication model
  - Physical layer
  - Communication layer
  - Application layer
- Privacy attacks
- Correlation attack

Radio frequency identification



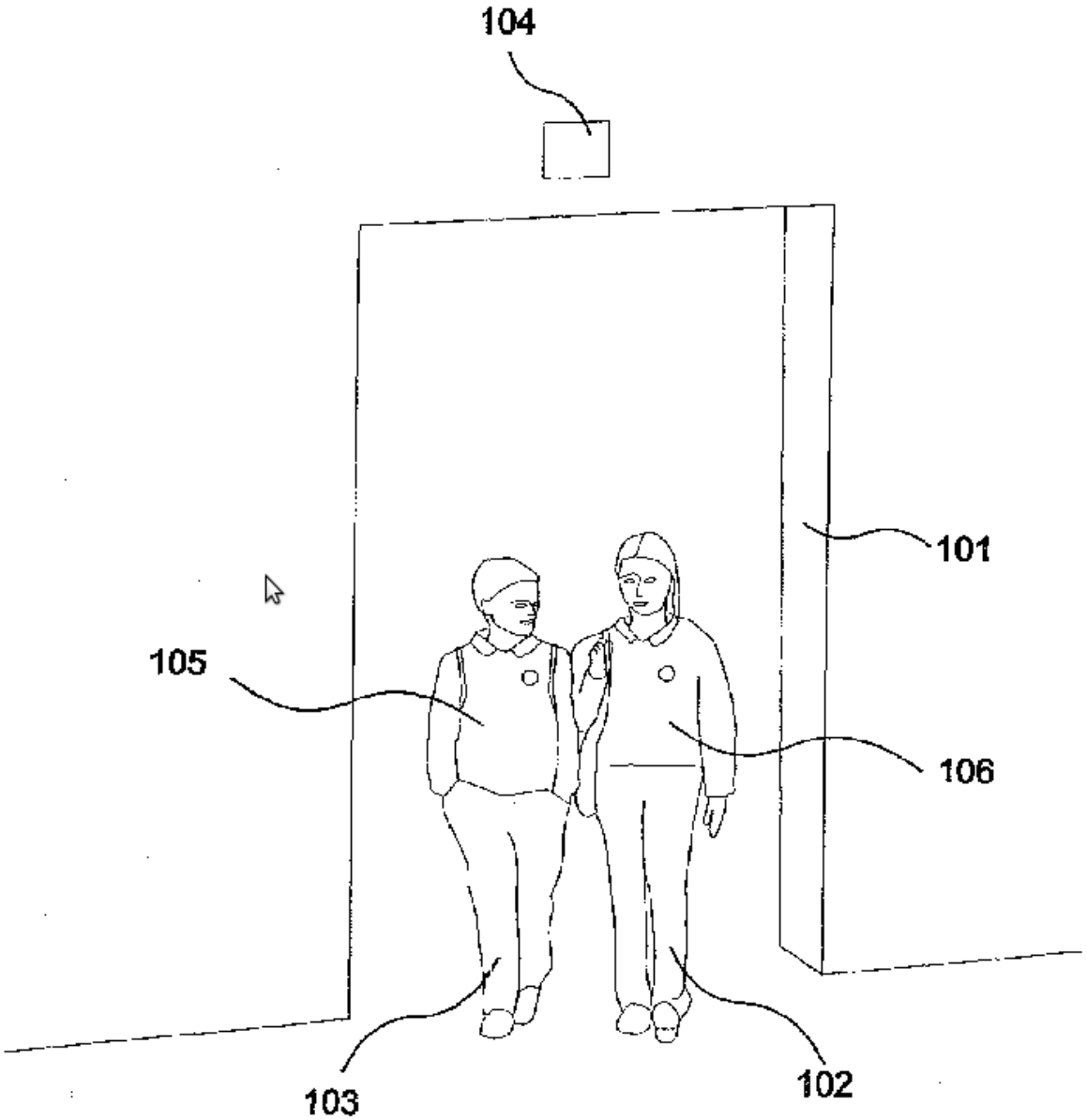
Radio frequency identification

Key properties of RFID:

- Wireless technology
- Cheap technology
- Unique identifiers
- No power source needed

RFID in your pocket

RFID in your underwear


104
101
105
106
103
102

RFID research

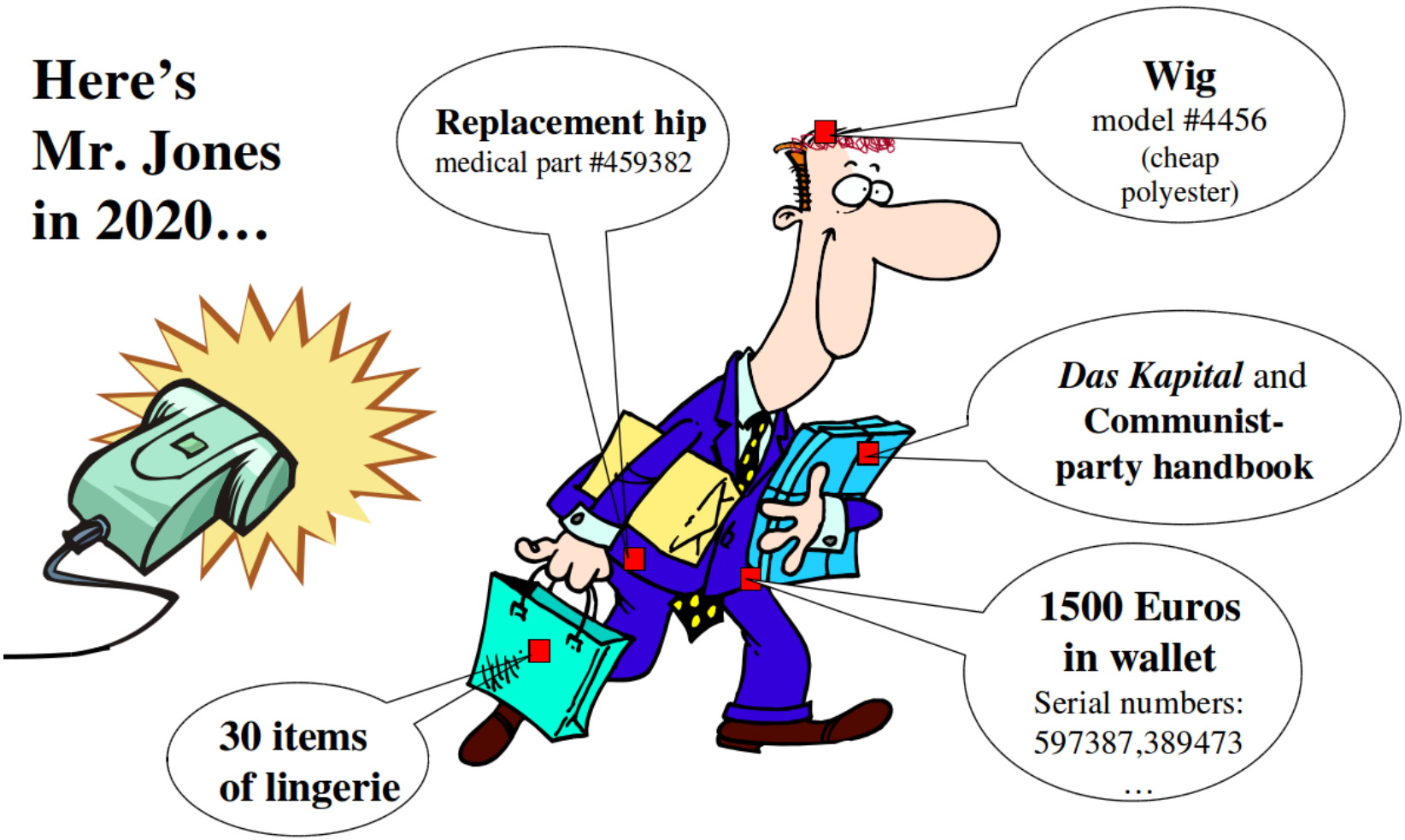
RFID security research mainly focuses on:

- Authenticity: is the tag who he claims to be?
- Proximity: is the tag in my vicinity?
- Privacy

The adversary can

- Impersonate a reader
- Impersonate a tag
- Eavesdrop on messages
- Block messages
- Modify messages

Privacy problems



Taken from Ari Juels: RFID Security and Privacy: A research Survey, IEEE Journal on Selected Areas in Communications 24 (2): 381-394 (2006)

Plain identities

Item	**ID**	**Message sent**
Wig	W125	W125
Replacement hip	H123	H123
Das Kapital	DK234	DK234
500 euro note	FH128	FH128
500 euro note	FH129	FH129
500 euro note	FH130	FH130
Lingerie	L180	L180

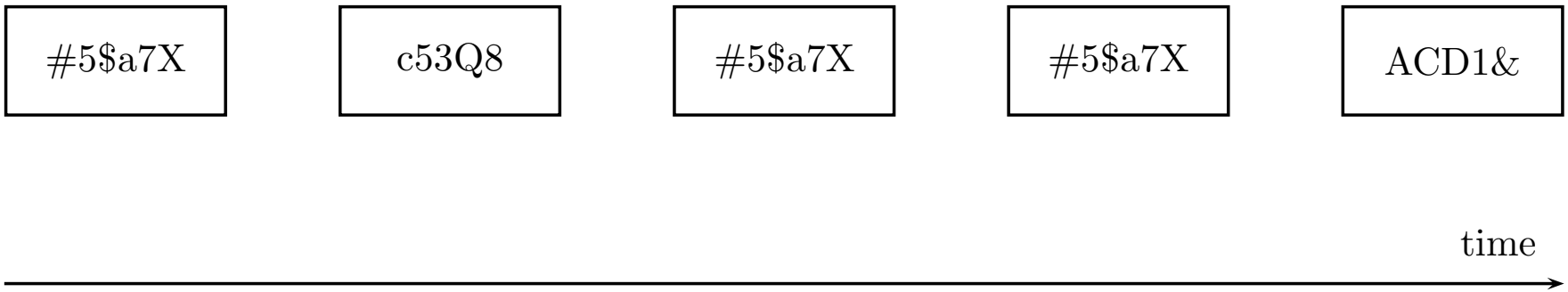
Solution: encrypt the identity of the tag

Encrypted identities

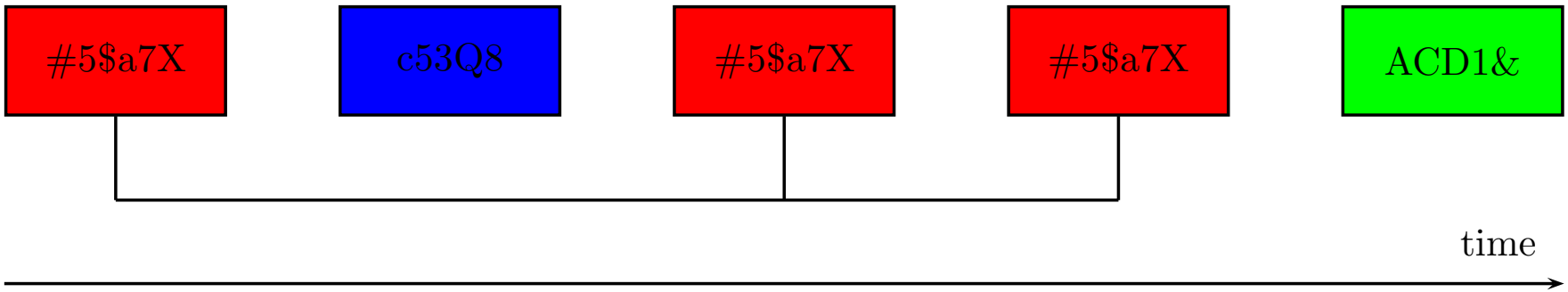
Item	**ID**	**Message sent**
Wig	W125	#5$a7X
Replacement hip	H123	rB91Ur7x
Das Kapital	DK234	T3tUM
500 euro note	FH128	DX0mbvs
500 euro note	FH129	pIFV2y
500 euro note	FH130	rny5Lr
Lingerie	L180	PxXmhJ8uJ

Solution: encrypt the identity of the tag

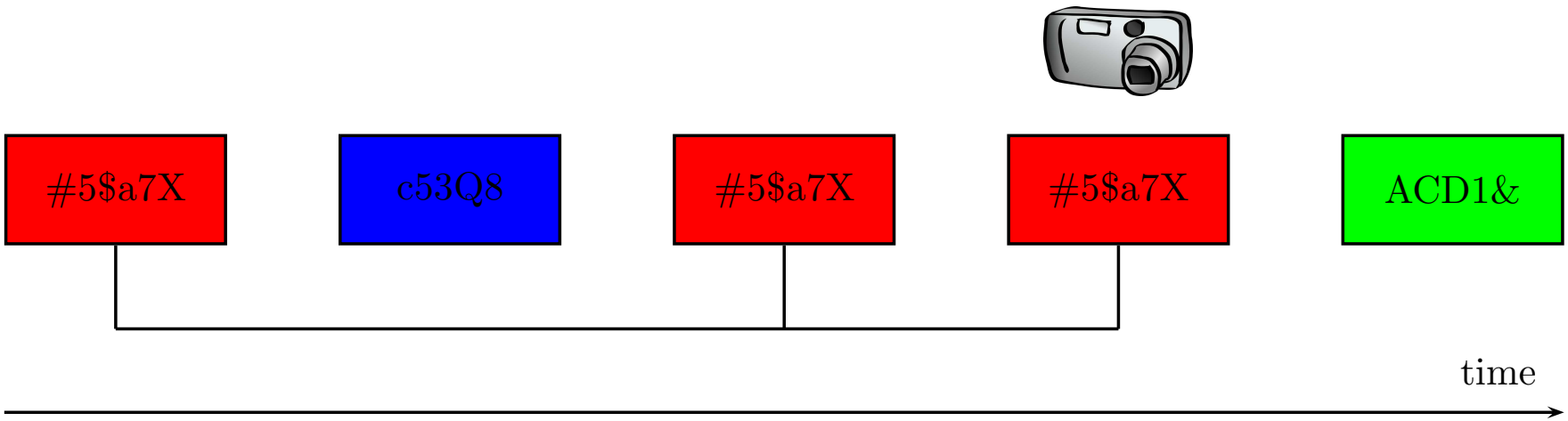
Untraceability



Untraceability



Untraceability



Untraceability

#5$a7X | c53Q8 | #5$a7X | #5$a7X | ACD1&

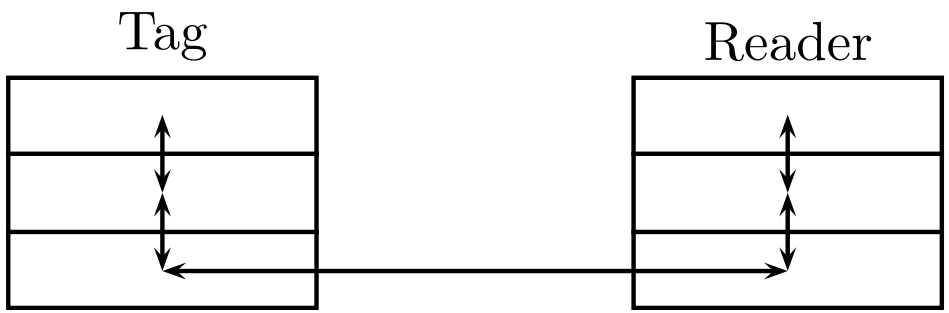
time

Untraceability

We call an RFID system untraceable if an adversary cannot recognize a tag he has seen before

Untraceability is sometimes called (strong) privacy, indistinguishability, or unlinkability.

RFID stack



3. Application
2. Communication
1. Physical

RFID communication layers

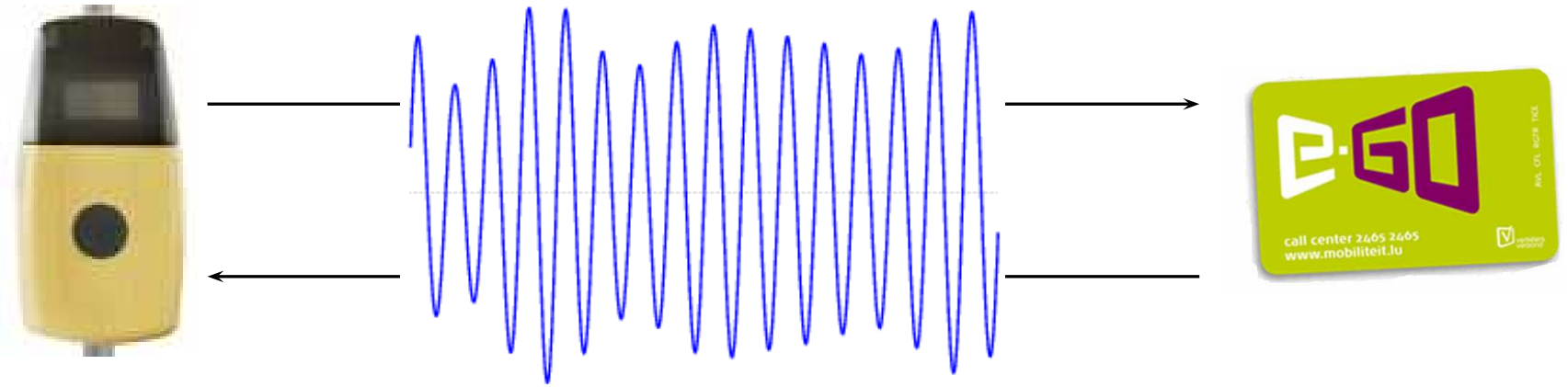
- Physical layer: Transmission of bits
  - Modulation/demodulation protocols
  - Anti-collision protocols
- Communication layer: Cryptographic services
  - Identification/authentication protocols
  - Key update protocols
  - Distance-bounding protocols
- Application layer: RFID application
  - Data access/interpretation protocols.
    - Photo on e-passport
    - Building access privileges

Physical layer: Fingerprinting RFIDs

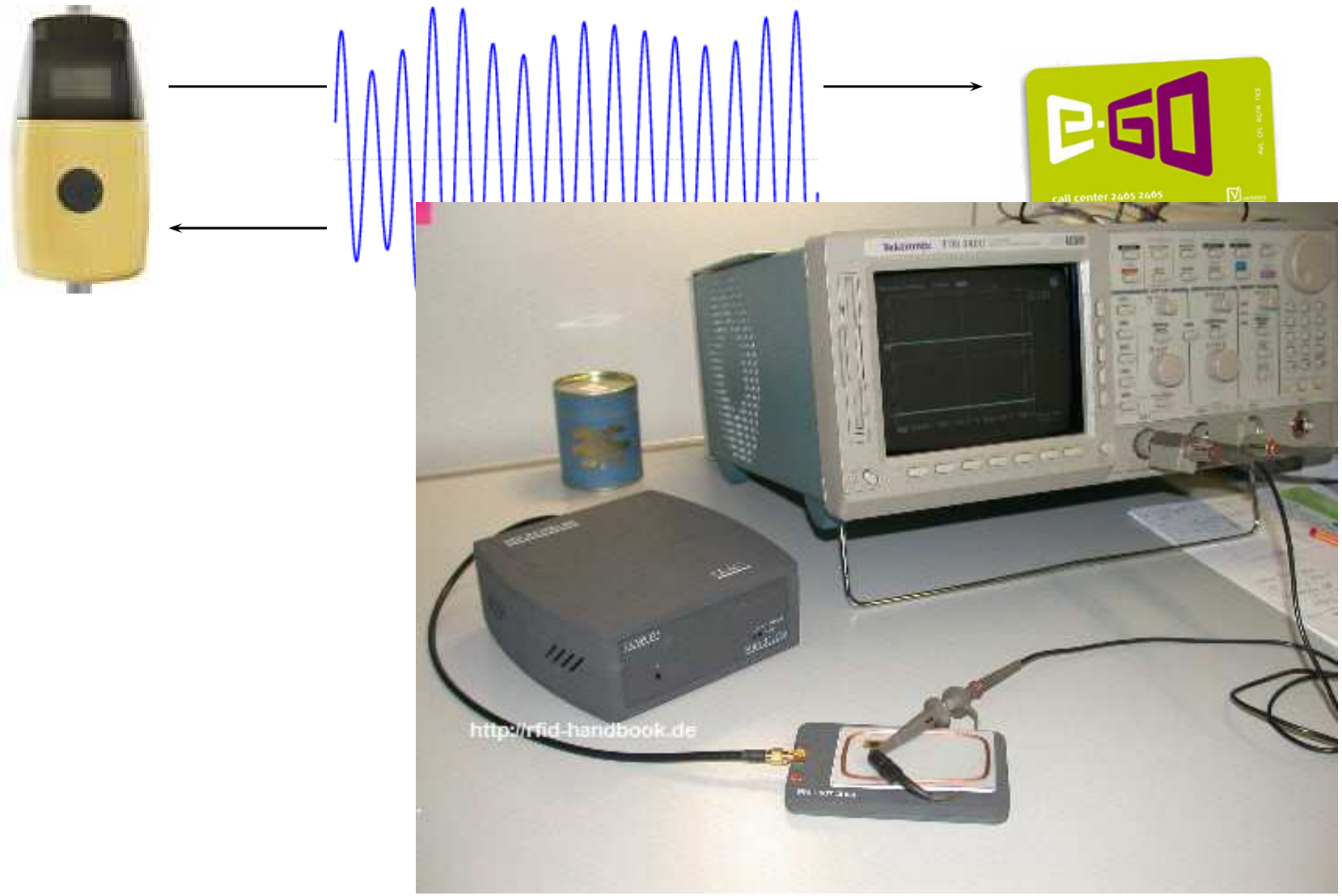
"wake up"

"I'm ready"

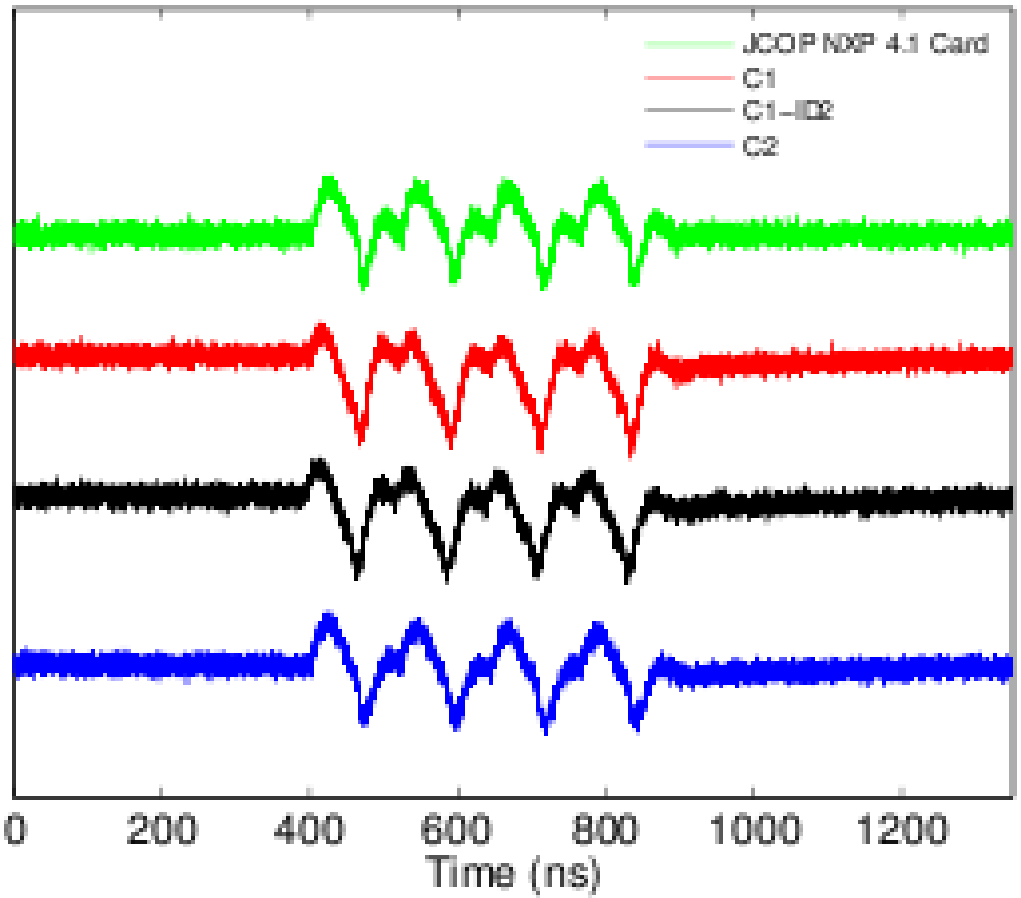
Physical layer: Fingerprinting RFIDs



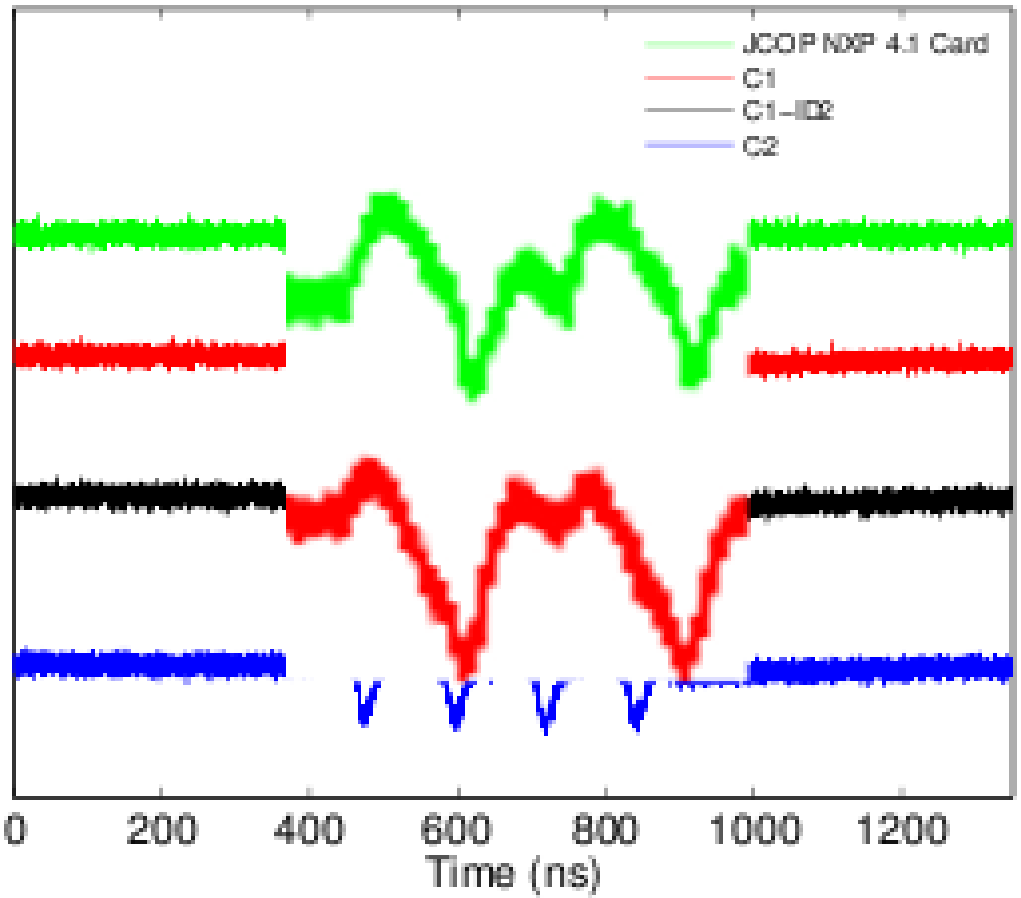
Physical layer: Fingerprinting RFIDs



Physical layer: Fingerprinting RFIDs



Physical layer: Fingerprinting RFIDs



Physical layer: Fingerprinting RFIDs

Fingerprinting RFIDs:

- Only possible in a controlled environment
- Expensive equipment needed

Performance results (Danev et al. 2009):

- Sample size of 50 "identical" JCOP tags: correct identification in 95% of the cases.
- Sample size of 8 e-passports: correct identification in 100% of the cases.

Physical layer: UIDs

Anti-collision:

- Before running communication-layer protocols, the reader and tags performs an anti-collision protocol
- Anti-collision singles out one tag for communication
- Tags assume anti-collision identifiers: UIDs (unique identifiers)

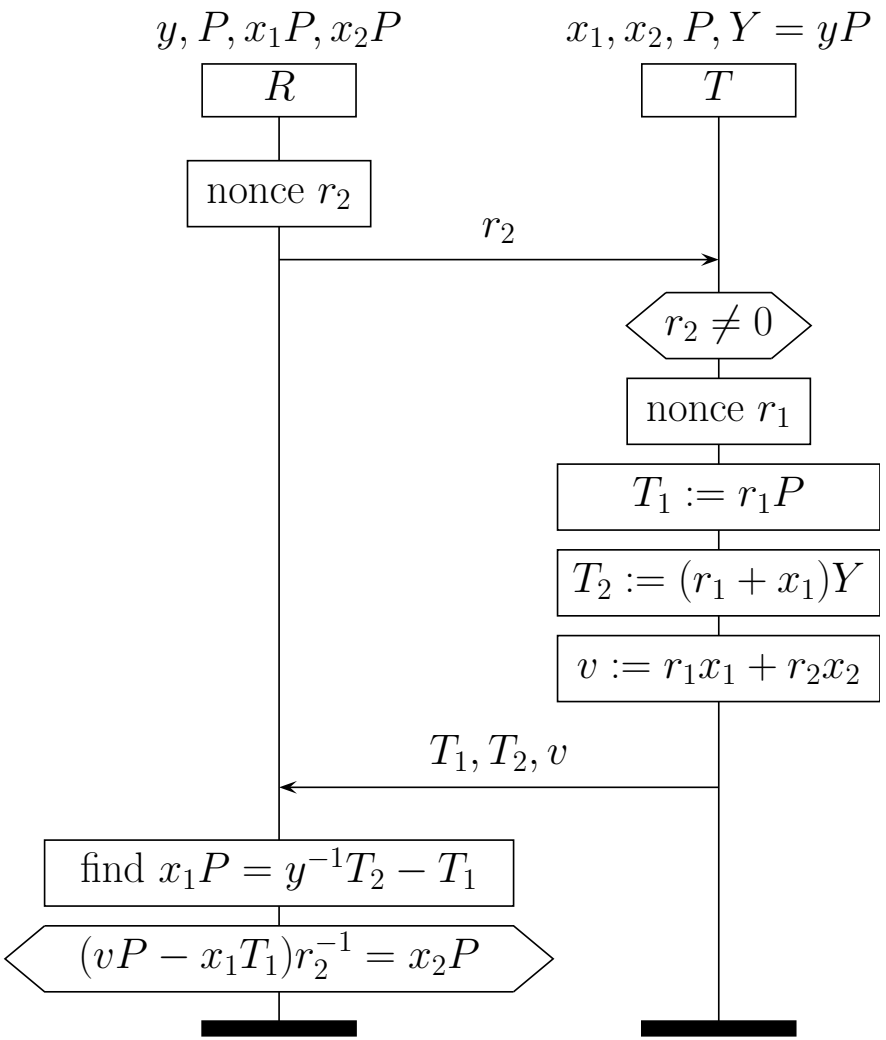
Unique identifiers are almost always static.

And can be read out by anybody with an RFID reader.

RFID reader

Available at www.touchatag.com for EUR 30/$40.

Communication layer: Unique attribute attacks



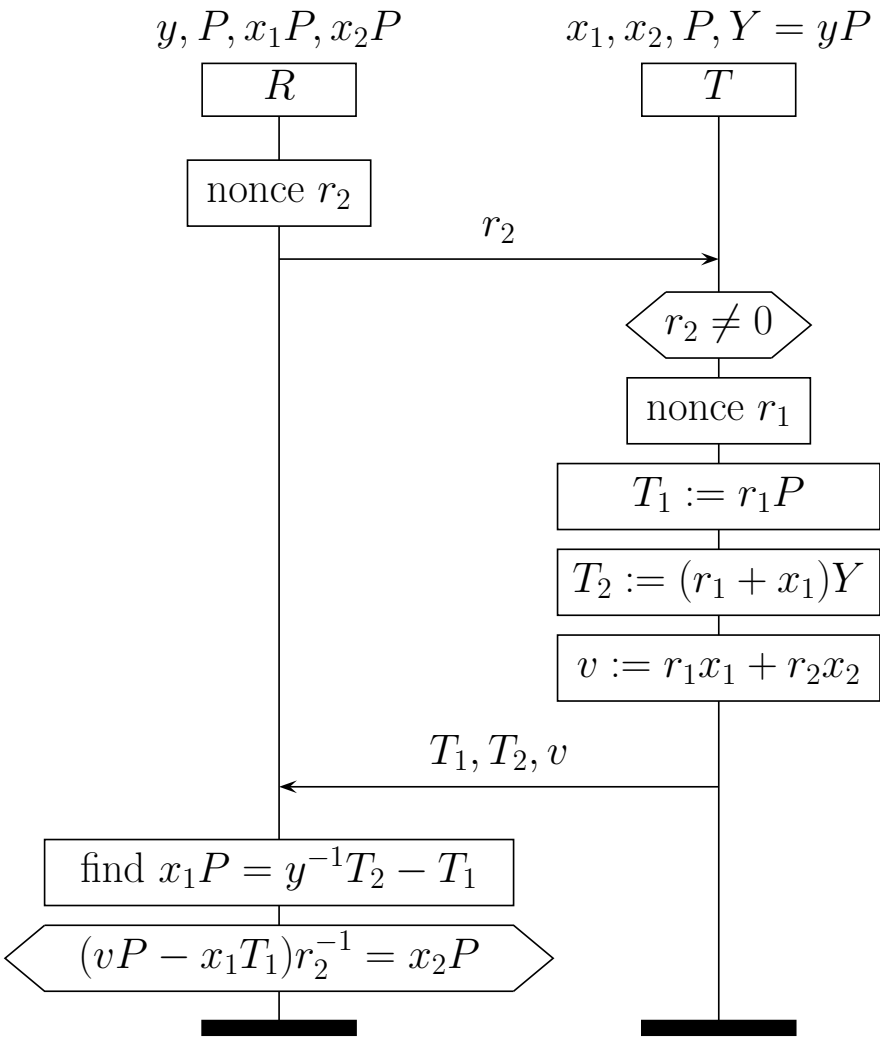
Authentication protocol (Lee et al. 2008)

- Challenge response structure
- Public-key based
- Randomized tag responses

Design goals:

- Authentication
- Untraceability

Communication layer: Unique attribute attacks



Reader computes:

$$y^{-1}T_2 - T_1$$

$$= (r_1 + x_1)P - r_1P = x_1P$$

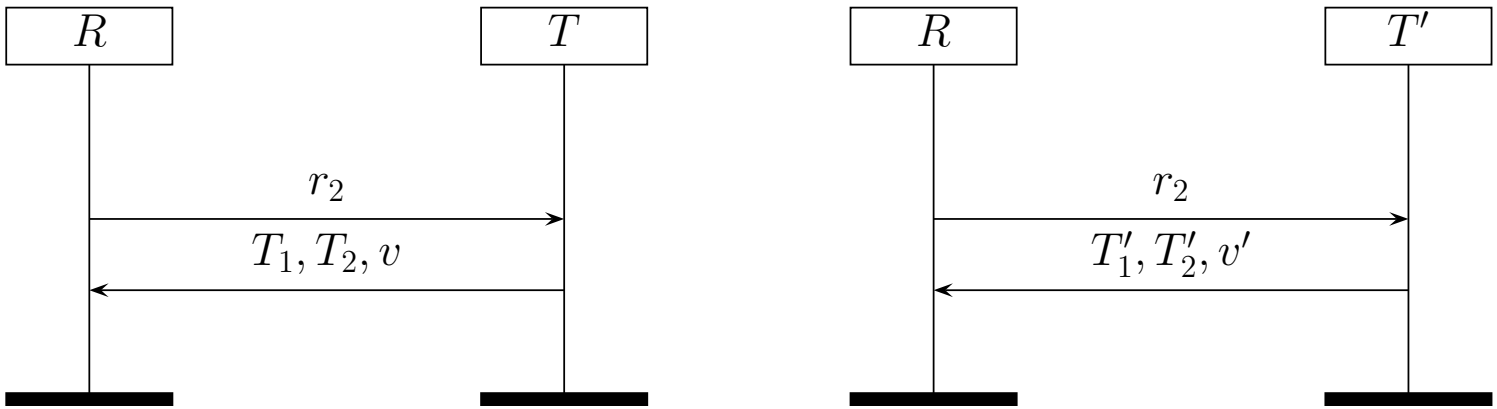
And verifies:

$$(vP - x_1T_1)r_2^{-1}$$

$$= r_1x_1P - r_1x_1P + r_2r_2^{-1}x_2P$$

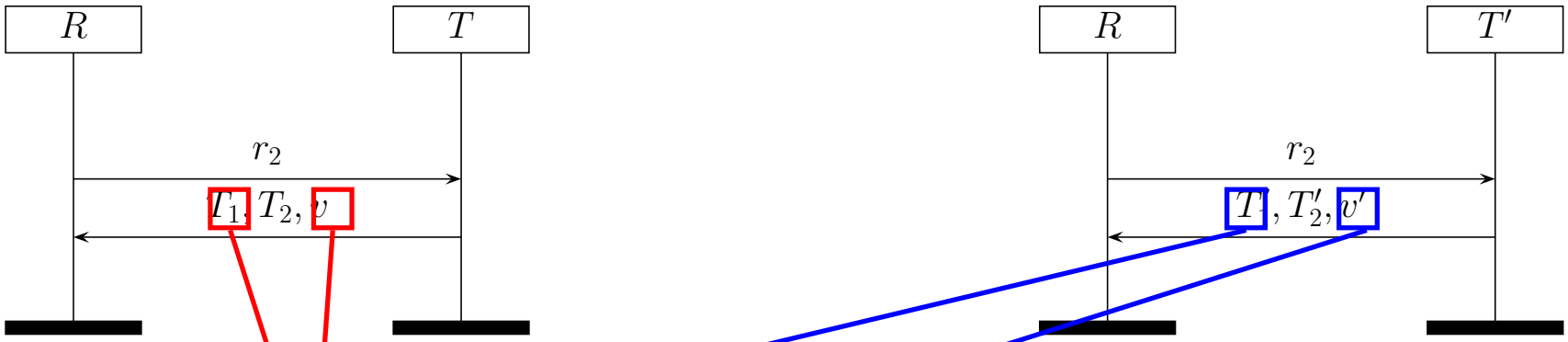
$$= x_2P$$

Communication layer: Unique attribute attacks



Question: $T \stackrel{?}{=} T'$

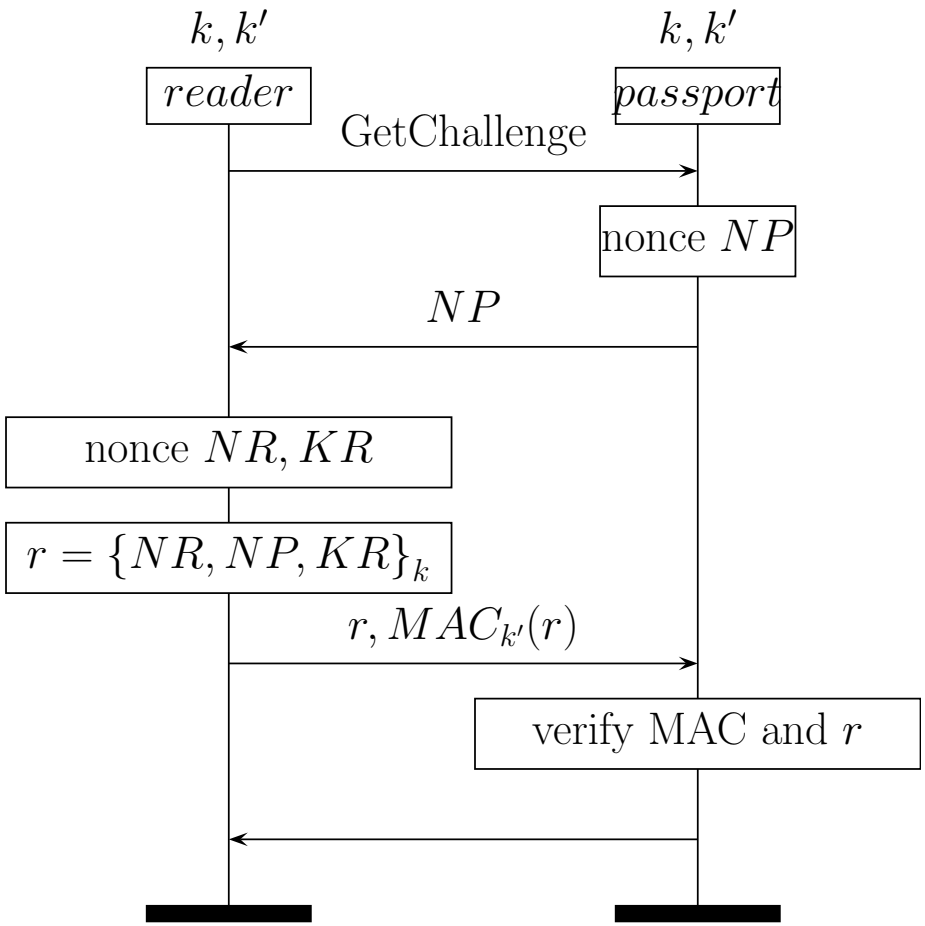
Communication layer: Unique attribute attacks



$$\frac{T_1 - T_1'}{v - v'} = \frac{(r_1 - r_1')P}{(r_1 - r_1')x_1} = x_1^{-1}P$$

Communication layer: e-passports

Basic access control protocol



Communication layer: e-passports

- The passport first verifies the MAC
- Then it verifies the encryption

Verification of the MAC and the encryption takes time.

Communication layer: e-passport

The attacker can (Chothia/Smirnov, 2010):

- Record a message of a person with passport P he wants to trace
- Replay that message later to any passport P' in his vicinity

- For a passport $P \neq P'$ the MAC and encryption will not verify correctly
- For passport P the MAC will verify correctly, but the encryption will not

Therefore, the passport P will take longer to respond with an error message than any other passport $P' \neq P$.


The Register®
Hardware Software Music & Media Networks Security Public Sector Busin
Crime Malware Enterprise Security Spam ID
Print Retweet Facebook
Defects in e-passports allow real-time tracking
This threat brought to you by RFID
By Dan Goodin in San Francisco • Get more from this author
Posted in Security, 26th January 2010 22:07 GMT
Computer scientists in Britain have uncovered weaknesses in electronic pas
the US, UK, and some 50 other countries that allow attackers to trace the mo

Even if all layers maintain privacy...

- Assume all layers are properly protected.
- And a single tag is not traceable.

- An attacker can still find out which protocols a tag runs.
- And figure out the type and brand of a tag

Even if all layers maintain privacy...

Scenario:

- A store wants to trace their customers
- Installs an RFID reader at the store entrance
- Then the store owner can see the amount and types of all tags one carries

The following two customers can be easily distinguished:

- Customer 1's set of tags: $\{A, BB, CCCCC, DDD\}$.
- Customer 2's set of tags: $\{AA, C\}$.

Even if all layers maintain privacy...

Effectiveness:

- Increases if the number of tags people carry on them increases
- Increases if the number of different tags increases
- Very effective against people with 'rare' tags
- Very hard to counter

Question: How does one analyze the privacy loss in this situation?

Conclusion

Summary:

- RFID layered communication model
- Taxonomy of traceability attacks
  - Physical layer:
    - Fingerprinting RFIDs
    - Unique identities: UIDs
  - Communication layer:
    - Unique attribute attacks
    - Passport tracing
  - Application layer
- Correlation attack

Future work

Future work:

- Analyze privacy loss under correlation attack
- Find minimal conditions to maintain privacy

Thank you!

http://satoss.uni.lu/ton