RFID Security and Privacy

Gildas Avoine, UCL Belgium

INFORMATION SECURITY GROUP

These slides will be soon available at
http://sites.uclouvain.be/security/publications.html

Lecturer Presentation

Lecturer Presentation: University

- Prof. Gildas Avoine.
- Université catholique de Louvain.
  - University created in 1425, about 20'000 students.
- Computer Science Departement
- I

Lecturer Presentation: GSI

- Applied Cryptography.
  - Cryptographic protocols.
  - Building blocks.
  - Put the theory into practice.
- RFID Security and Privacy.
  - Design of application-layer cryptographic protocols.
  - Design of practical solutions.
  - Audit of real-life solutions and practical attacks.
- Algorithmics related to security (time-memory trade-off).
  - Cracking systems (eg passwords).
  - Using TMTO in a constructive way.

Aim of the Presentation

- Better understand the RFID technology.
  - Applications, technologies.
- Present the security and privacy threats.
  - Classification, description and feasibility of the threats.
- Describe Solutions.
  - Current and future approaches.

Summary

- Part 1: RFID Primer
  - Definitions and Past Facts
  - Daily Life Examples
  - Tag characteristics
  - Identification vs authentication
- Part 2: Security and Privacy Threats
  - Impersonation
  - Information Leakage
  - Malicious Traceability
  - Denial of Service
- Part 3: The Passport Case (if remaining time)

Part 1: RFID Primer

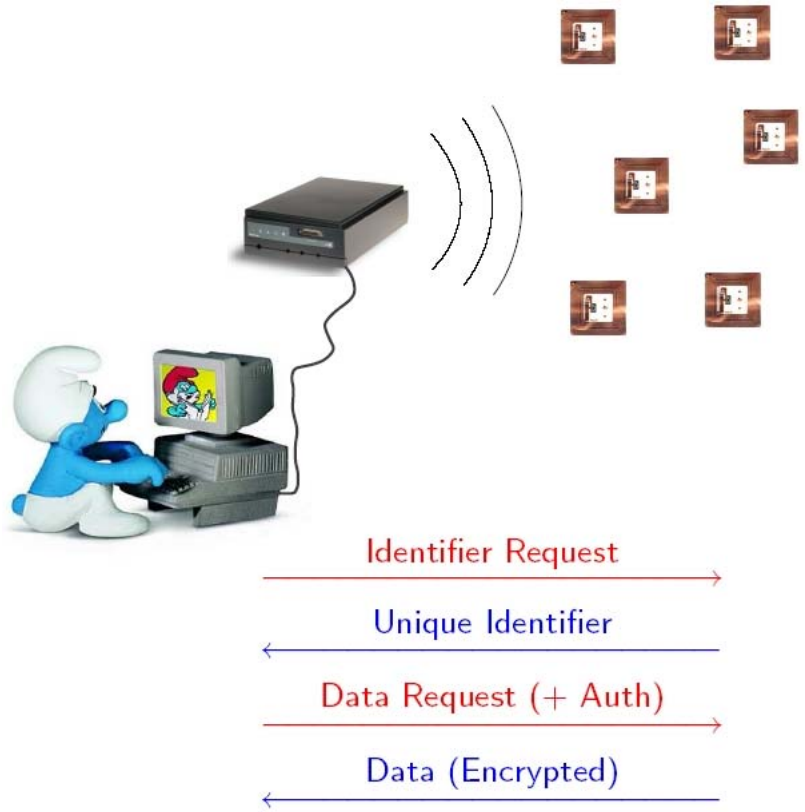
Part 1.1: Definitions and Past Facts

Definitions

- Radio Frequency IDentification (RFID) is a method of storing and remotely retrieving data using devices called RFID tags.
- An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person.
- An RFID tag contain a microcircuit and an antenna to enable it to receive and respond

- An RFID tag can be a low-capability device e.g. for pet identification, but also a powerful

Architecture



History

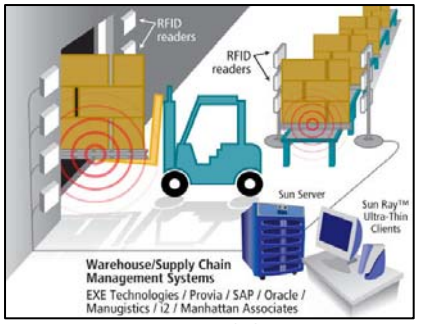
- RFID exists since the forties (IFF, Russian spy).
- Commercial RFID applications appeared in the early eigthies.
- Boom which RFID technology is enjoying today relies on the willingness to develop small and cheap RFID tags.
- Auto-ID Center created in 1999 at the MIT. (EPC code)

- Several hundred million tags sold every year (eg. Mifare Classic).

Part 1.2: Daily Life Examples

Basic RFID

- Supply chain.
  - Track boxes, palettes, etc.



Source: www.dclogistics.com

- Libraries.
  - Improve book borrowing procedure and inventory.

Source: www.rfid-library.com

- Pet identification.
  - Replace tattoos by electronic ones.
  - Will become mandatory in the EU.
  - ISO 11784, ISO 11785.


Source: www. flickr.com

- People tracking.
  - Amusement parks.
  - Elderly people.


Source: www.safetzone.com

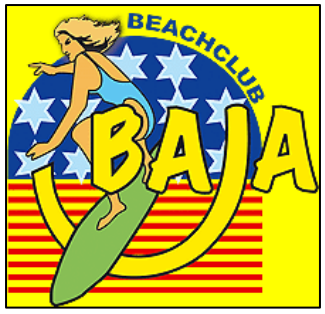
Evolved RFID

- Building access control.

- Automobile ignition keys.

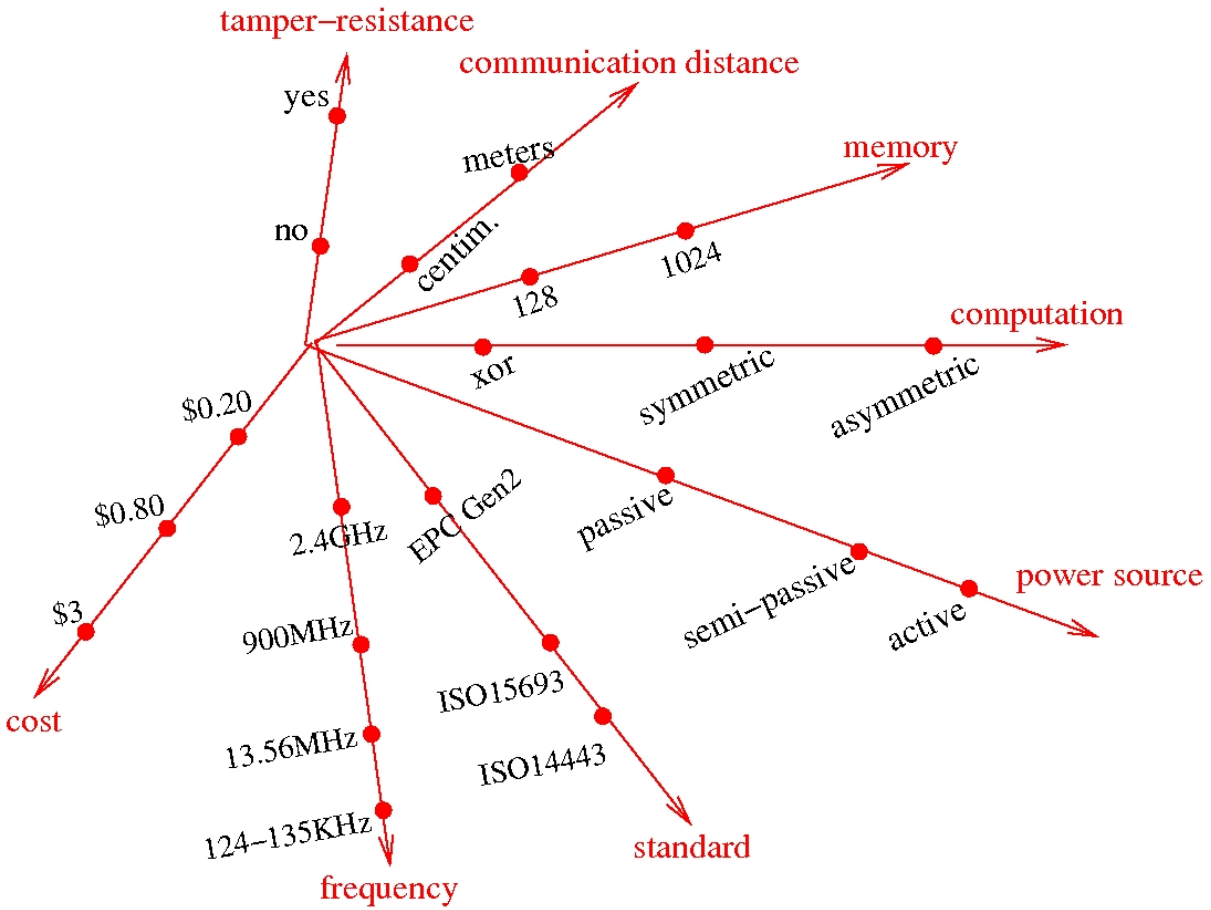
- Passports.
  - Electronic passports since 2004.
  - Standardized by ICAO. More than 50 countries.
- Public transportation.
  - Eg. Brussels, Boston, Paris, London.

- Anti-counterfeiting.
  - Eg. luxurious items.



Part 1.3: Tag Characteristics

Tag Characteristics



Power Source

- Passive
  - Tags do not possess any internal energy source. They obtain energy from the reader's electromagnetic field.
- Active
  - Tags have a battery that is used both for internal calculations and transmission.
- Semi-Passive
  - Tags have a battery for internal calculations. However, the energy required for transmission still comes from the reader's electromagnetic field.

Frequency Band

- 125–134 kHz (LF): Pet identification, livestock tracking.
- 13.553–13.567 MHz (HF): Smartcards, libraries, clothing identif.
- 860–960 MHz (UHF): Supply chain tracking.
- 2.4000–2.4835 GHz (UHF): Highway toll, vehicle fleet identif.

Communication Range

The communication range depends on:

- Transmission Power.
  - See ETSI EN 300-330, EN 300-220, EN 300-440, EN 300-328.
- Frequency (LF, HF, UHF).
  - LF: centimeters.
  - HF: centimeters to decimeters.
  - UHF: meters.
- Electronic considerations (antennas, etc.).

Communication Range

- With a stronger power and better antennas, a tag can be read at a distance greater than the claimed one (eg. 1m in 13.56 MHz).
- The reader-to-tag channel (forward channel) can be read at a distance greater than tag-to-reader channel (backward channel)

Memory

- Tags have at least a few bits to store a unique identifier UID.
  - UID size 32 to 128 bits.
  - Usually, the UID is chosen by the manufacturer and cannot be changed by the user.
- Tags can have additional memory (EEPROM).
  - 1KB is a common value among EEPROM-enabled tags.
  - About 70KB is a the memory size of a passport.
- EAS tags (Electronic Article Surveillance) have only 1 bit (enabled EAS / disabled EAS): no identification! no RFID!

Computation Capabilities

- No computation capabilities (memory).
- Simple logic operations.
  - Eg. to check a password.
- Symmetric cryptography.
  - DES, AES, proprietary algorithm.
  - Microprocessor not necessarily required.
    - E.g. Implementation of AES by TU Graz.
- Asymmetric cryptography (ie public-key).
  - RSA, ECC.
  - Microprocessor required.
    - Current works to perform PKC without microprocessor, e.g. GPS, WIPR.

Tamper Resistance

Tamper resistance is a controversial issue.

- Some people consider that tags are tamper-resistant: be careful, e.g., if the same key shared by all tags!
- Some (more reasonable people) consider that tags are not tamper-resistant but cost of an attack can be expensive compared to the gain: we put a different key in every tag.
- Sometimes not being tamper-resistance is counter balanced by the fact that it is hard to have access to the tag, e.g. subdermal tag.

Standards

- ISO: International Organization for Standardization.
  - www.iso.org
  - 14443, 15693, 11785, 17364, 15459, 24721, 17367, 19762, etc.
- EPC: Electronic Product Code
  - http://www.epcglobalinc.org/
  - "The EPCglobal Network was developed by the Auto-ID Centre, a global research team directed through the Massachusetts Institute of Technology with labs around the world."
  - "EPCglobal is a neutral, consensus-based, not-for-profit standards organisation."
  - Class 1 Gen 2 Standard.

Class-1: Identity passive tags

- Tags with the following minimum features:
  - An electronic product code (EPC) identifier.
  - A tag identifier (TID).
  - A 'kill' function that permanently disables the tag.
  - Optional password-protected access control.
  - Optional user memory.

Class-2: Higher-functionality passive tags

- Tags with the following anticipated features above and beyond those of class-1 tags:
  - An extended TID.
  - Extended user memory.
  - Authenticated access control.
  - Additional features (TBD).

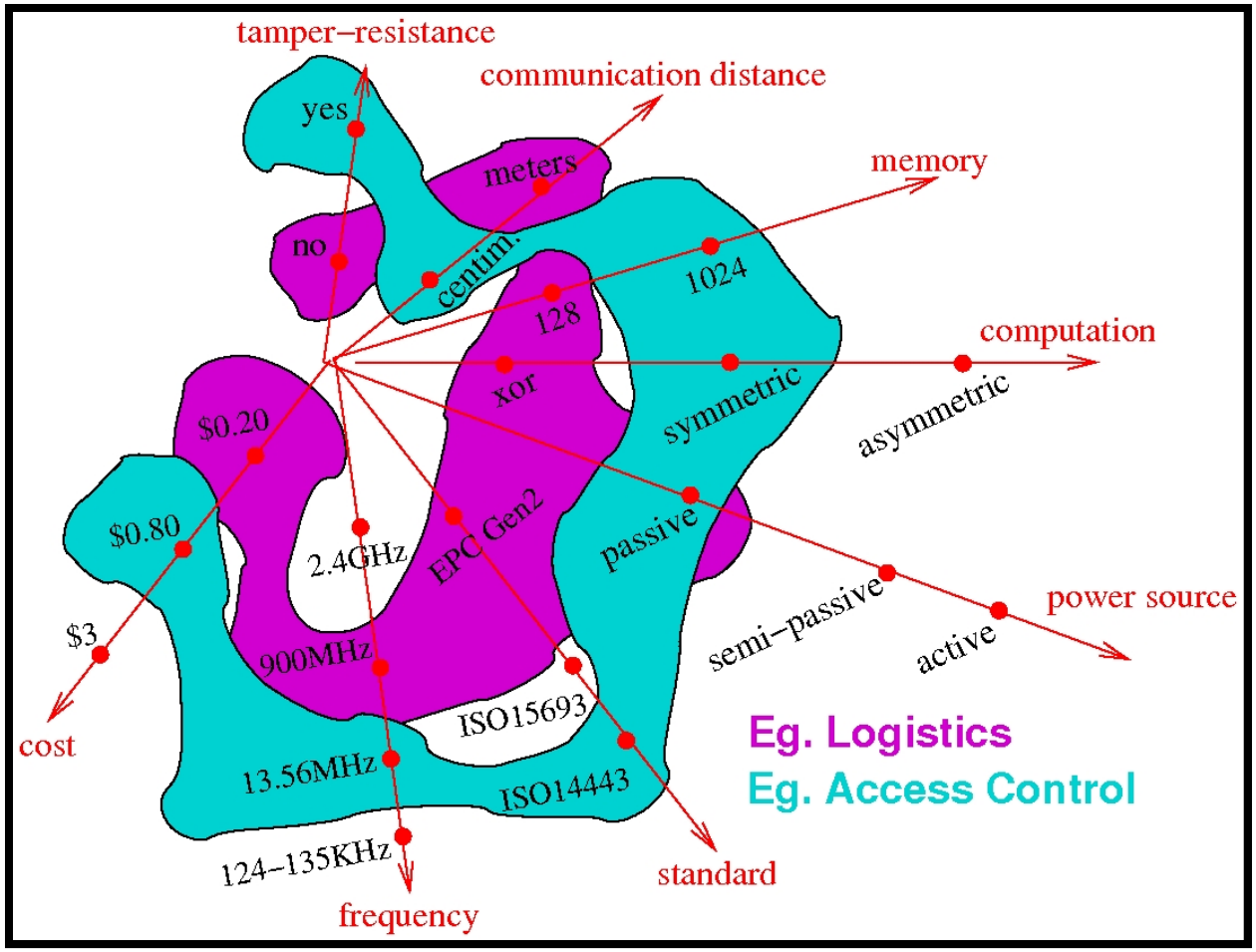
Class-3: Semi-passive tags

- Tags with the following anticipated features above and beyond those of class-2 tags:
  - An integral power source
  - Integrated sensing circuitry

Class-4: Active tags

- Tags with the following anticipated features above and beyond those of class-3 tags:
  - Tag-to-Tag communications
  - Active communications
  - Ad-hoc networking capabilities

Typical Configurations

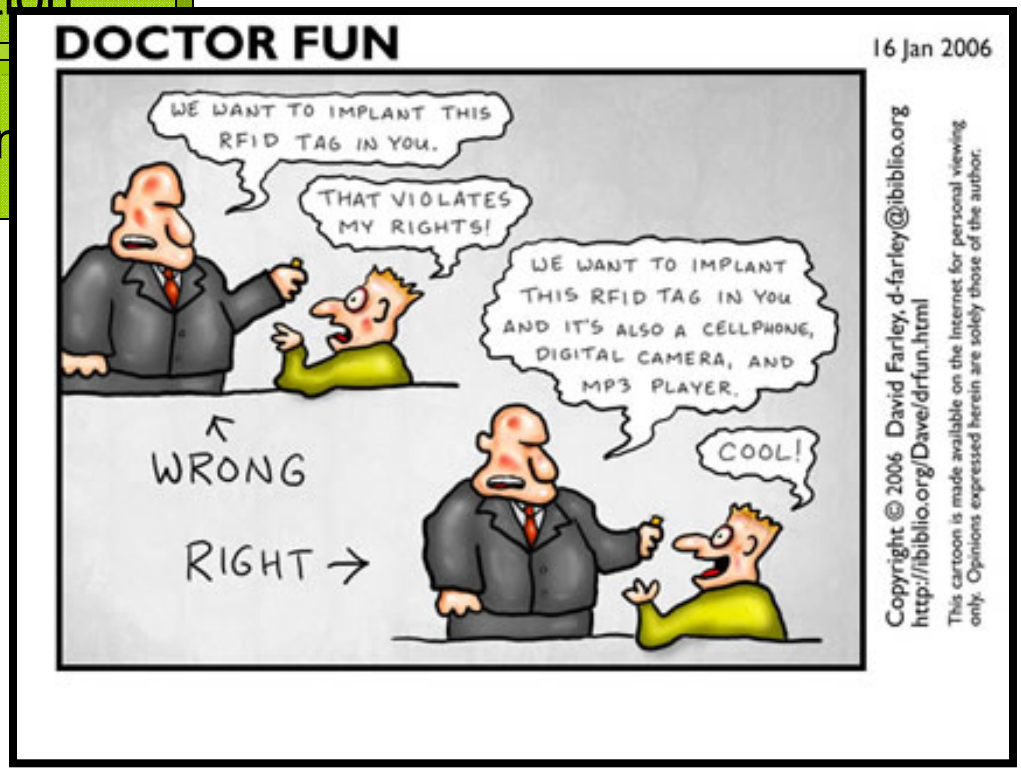


Part 2: Security and Privacy Threats

Classification of the Security Issues

Impersonation

Inform



Part 2.1: Impersonation

Detection, Identification, and Authentication

- A major issue when designing a protocol is defining its purpose.
  - Detection.
  - Identification.
  - Authentication.

- Examples:
  - Access control.
  - Management of stocks.
  - Electronic documents.
  - Counting cattle.
  - Pets identification.
  - Anti-cloning system.

Detection

Get the proof that someone is present.

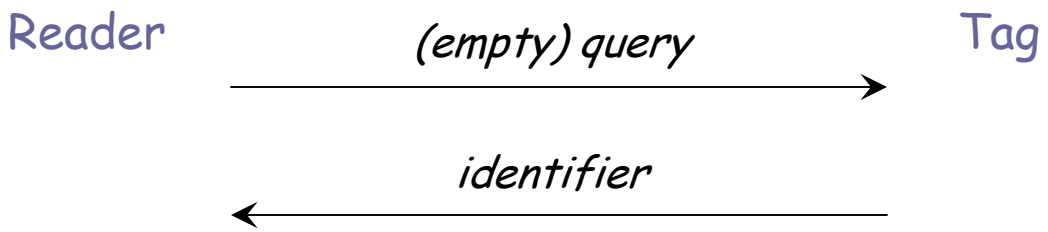
Identification

Get identity of remote party.

Authentication

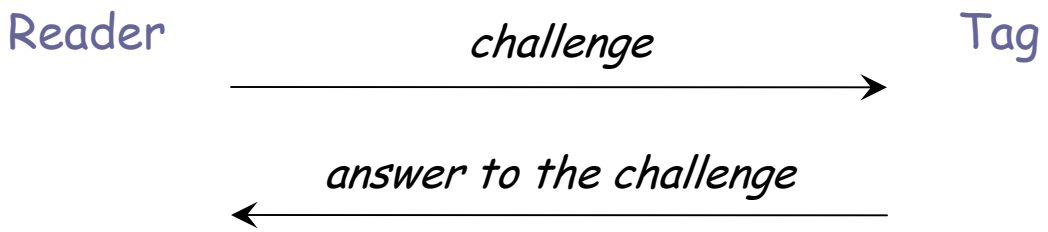
Get identity + proof of remote party

Identification Protocol



- The identifier is not necessarily the UID (eg: pet identification).
- Replay attack is possible.

Auth. Protocol: Challenge/Response



- Challenge is never used twice.
- Answering to the challenge requires to know a secret shared between the reader and the tag only.
- A replay attack is no longer possible.

Authentication

- Authentication can be done using:
  - A symmetric cipher, a keyed-hash function, a public-key cipher, a signature scheme, or a devoted authentication protocol (eg. ZK).

- Example: Challenge-Response Protocol.
  - ISO 9798-4 defines authentication protocols based on a MAC
  - SKID 2 is a variant of ISO 9798-4 Protocol 3.

SKID2
$$\begin{cases} T \leftarrow R & n_R \\ T \rightarrow R & H_{k_{TR}}(n_R, n_T, R), n_T \end{cases}$$

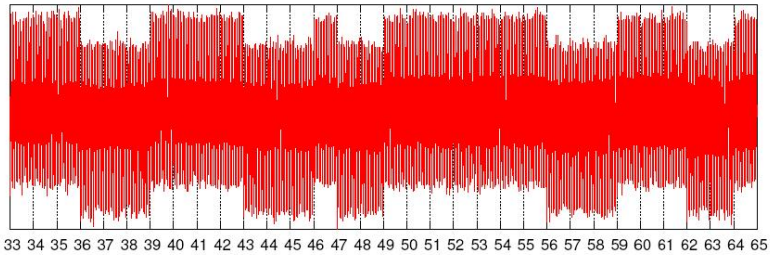
Main Issues

- We know how to design a secure authentication protocol.
- Issues in the real life:
  - Authentication is sometimes done using an identification protocol.
  - Keys are too short.
  - Algorithm is proprietary, poorly designed, and not audited.

Bad Example: MIT

- The MIT access control card includes an RFID tag.
- Frequency of the tag is 125 KHz.
- No cryptographic features available on the tag.

- Eavesdropping twice the communication gives the same broadcast.
  - The broadcast contains 224 bits.
  - Only 32 bits of them vary from card to card.

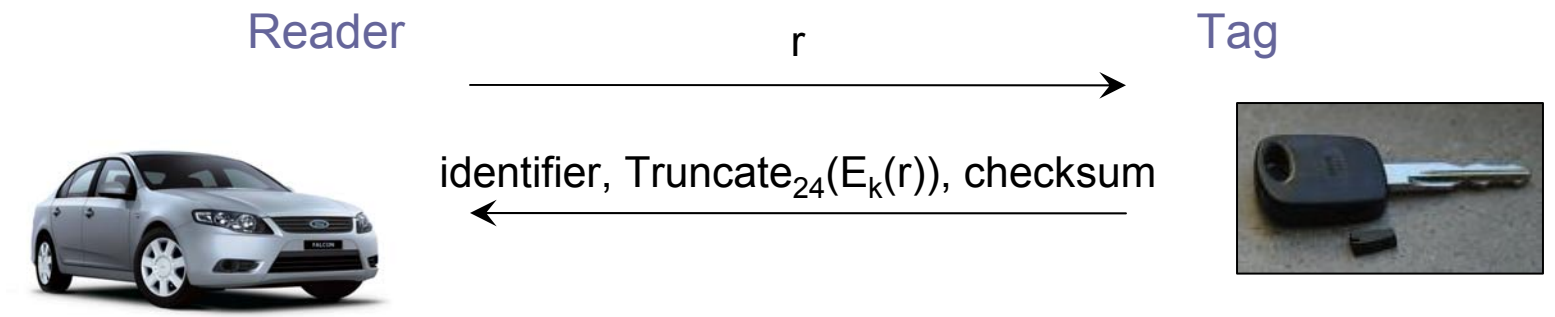


Source:
http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall04-papers/mit_id/mit_id.html

Bad Example: Texas Instrument DST

- Attack of Bono et al. against the Digital Signature Transponder manufactured by Texas Instrument, used in automobile ignition key (there exist more than 130 million such keys).

- Cipher (not public) uses 40-bit keys.
- They reverse-engineered the cipher.
- Active attack in less than 1 minute (time-memory trade-offs).



Source: http://www.usenix.org/events/sec05/tech/bono/bono.pdf

video1

video2

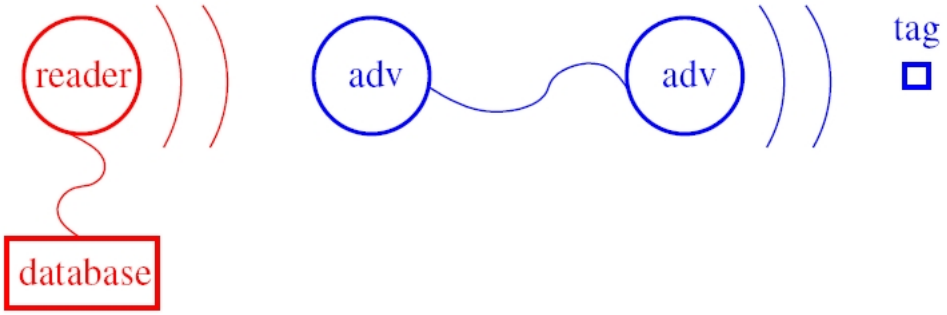
video3

Bad Example: NXP Mifare Classic

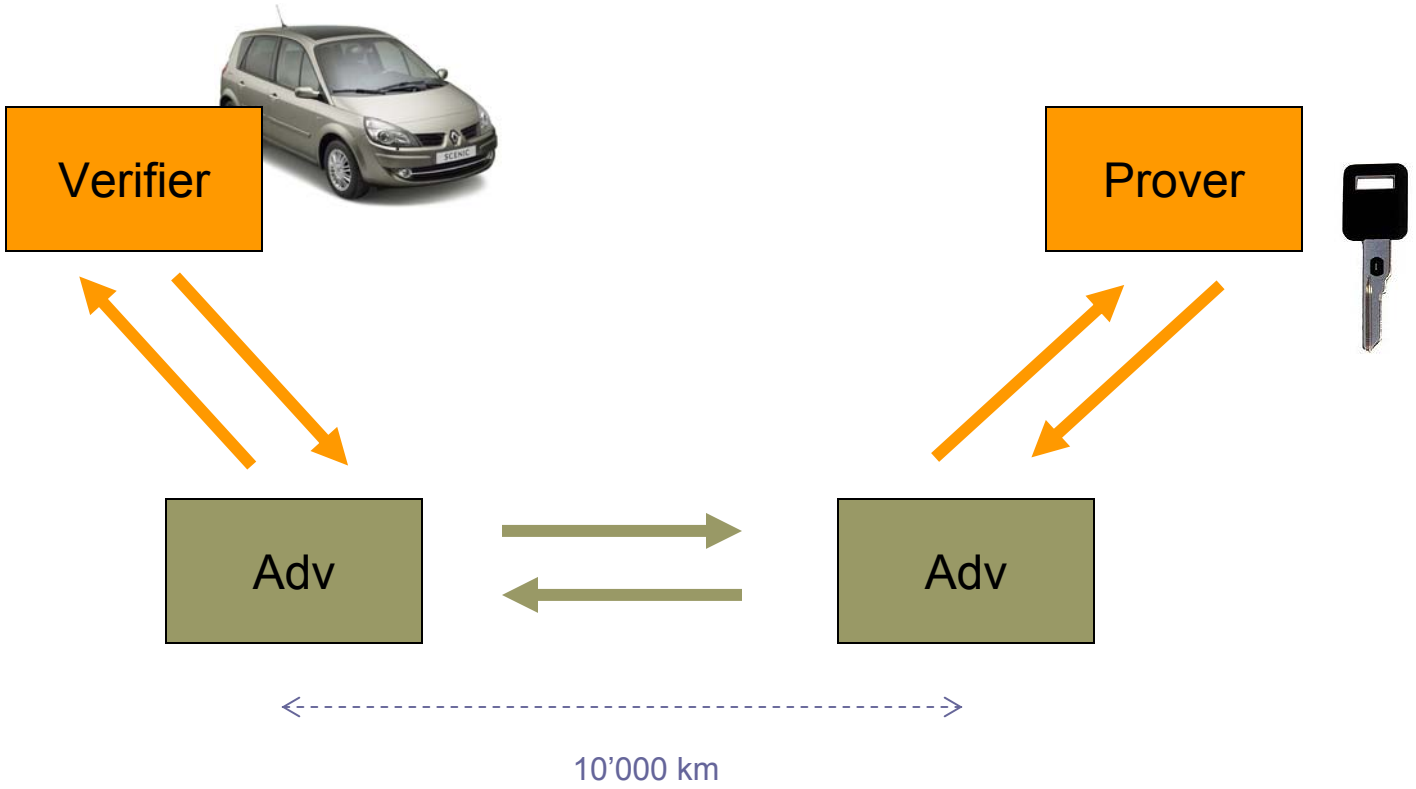
- Philips Semiconductors (NXP) introduced the Mifare commercial denomination (1994) that includes the Mifare Classic product.
- Mifare Classic's applications: public transportation, access control, event ticketing.
- Memory read & write access are protected by some keys.
- Several attacks in 2008, Hoepman, Garcia, de Koning Gans, et al. reverse-engineered the cipher Crypto1: every Mifare Classic tag broken in a few seconds.
- Move to a more evolved tag, eg. Mifare Plus.

Relay Attacks

- Even if the protocol is well-designed and secure from a cryptographic point of view, a relay attack is still possible.
- A relay attack is based on a passive man-in-the-middle attack.
- The reader believes that the tag is within its electromagnetic field while it is not the case. The attacker behaves as an extension cord.



Relay Attacks



Relay Attacks

Solutions to Relay Attacks

- No solution yet on the market today.
  - NXP Mifare Plus.
- The countermeasure consists in measuring the round trip time between the reader and the tag (do-able in practice?)

Current and Future Challenges

- Today.
  - We know pretty well how to design a secure authentication protocol, but…

- Challenges.
  - Designing good pseudo-random number generators.
  - Designing light cryptographic building blocks, ie without processor.
  - Tamper-resistance and side channel attacks.
  - Compromised readers.
  - Group authentication.
  - Security in very low-cost tag.
  - Relay attacks and distance bounding.
  - Authenticating the path.

Part 2.2: Information Leakage

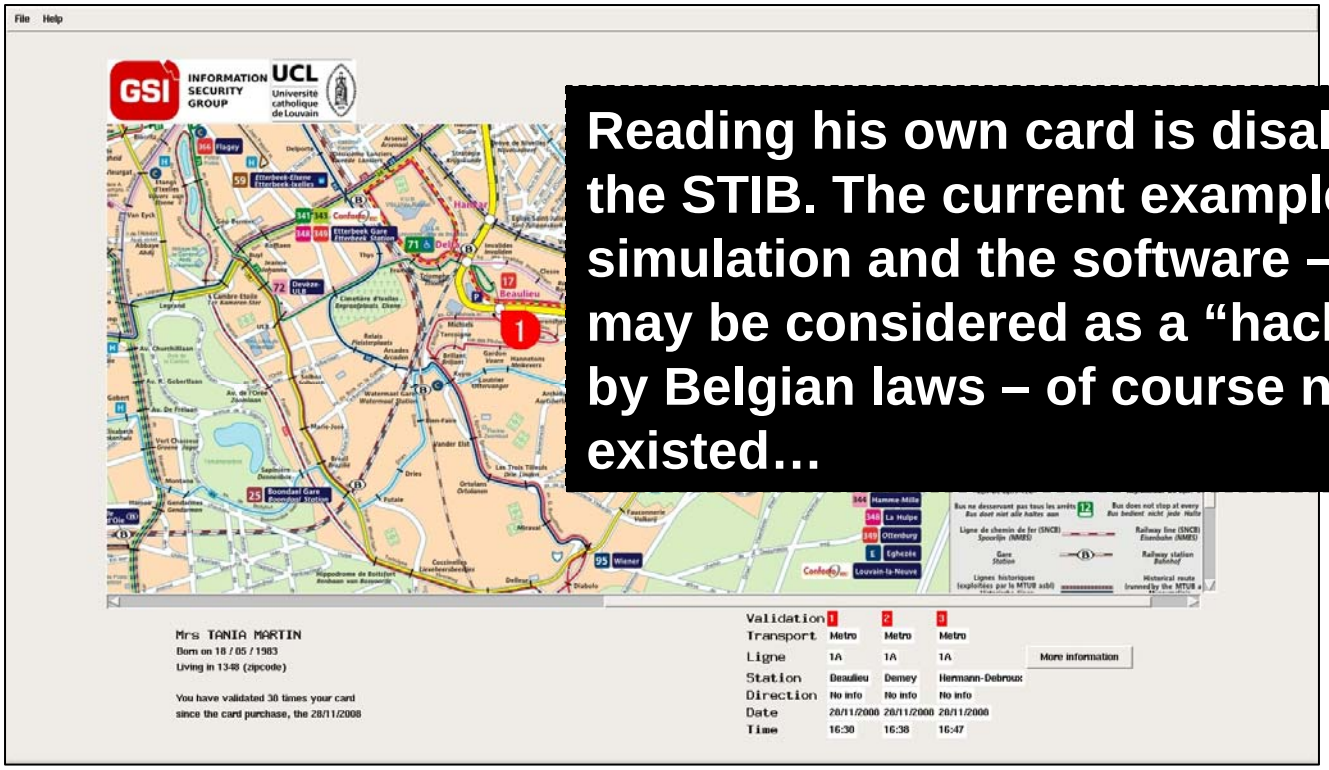
Definition

- The information leakage problem emerges when the data sent by the tag or the back-end reveals information intrinsic to the marked object.
  - Tagged books in libraries.
  - Tagged pharmaceutical products, as advocated be the US. Food and Drug Administration.
  - E-documents (passports, ID cards, etc.).
  - Directories of identifiers (eg. EPC Code).

Example: Leakage from the MOBIB Card

- MOBIB card (RFID) launched in Brussels in 2008.
- MOBIB is a Calypso technology.
- MOBIB cards are rather powerful RFID tags that embed cryptographic mechanisms to avoid impersonation or cloning.
- Personal data are stored in the clear in the card.
  - Data stored in the card during its personalization: name of the holder, birthdate, zipcode, language, etc.
  - Data recorded by the card when used for validations: last three validations (date, time, bus line, bus stop, subway station, etc.), and some additional technical data.

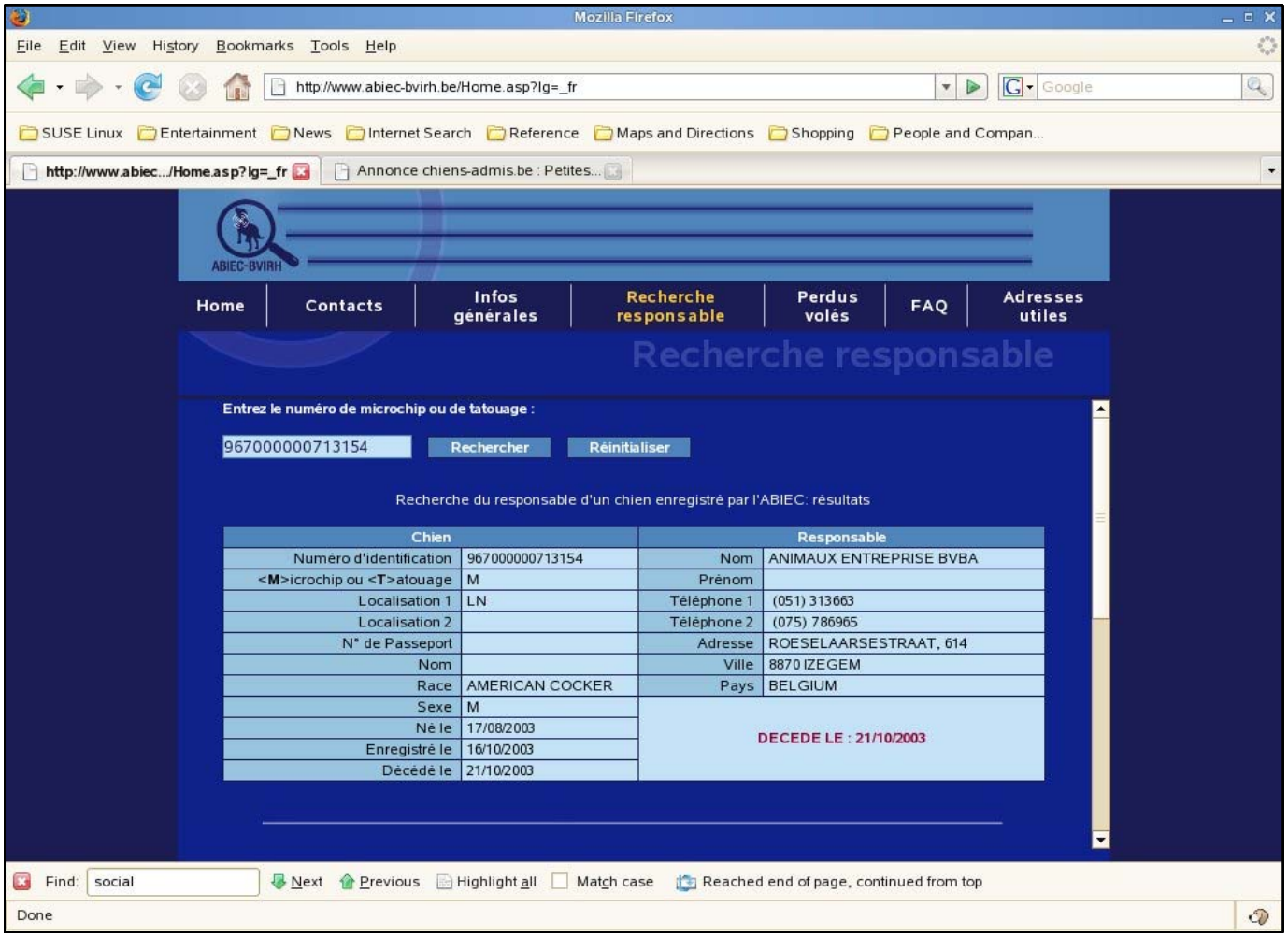
Example: Leakage from the MOBIB Card



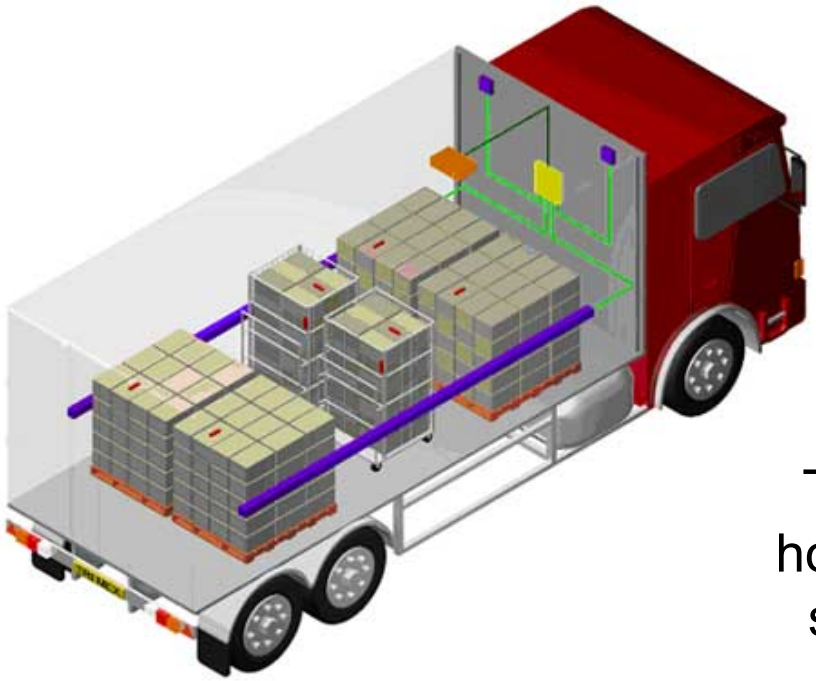
Reading his own card is disallowed by the STIB. The current example is just a simulation and the software – which may be considered as a "hacker tool" by Belgian laws – of course never existed…

MOBIB Extractor by G. Avoine, T. Martin, and J.-P. Szikora, 2009

Example: Leakage from the Backend



Who is the Victim?



The victim is not only the tag's holder, but can also be the RFID system's managing company: competitive intelligence.

Spying Activities

- The victim is not only the tag holder but also the RFID system.
- More and more data collected = valuable target (eg. during the manufacturing).
- Unaware information leakage (backup, HD thrown out, housekeeping).
- Abusive use (eg. French police's confidential files, Charlie Card in Boston).
- Do not figure out that some privacy is disclosed (eg. ABIEC).

Challenges

- More and more data collected: the "logphilia".
  - "philia" is a prefix "used to specify some kind of attraction or affinity to something, in particular the love or obsession with something" (wikipedia).
- Information may eventually leak (conservative assumption).
  - Backup, HD thrown out, abusive use by the staff, etc.
- More engineering challenges than research challenges.
- Ownership transfer.

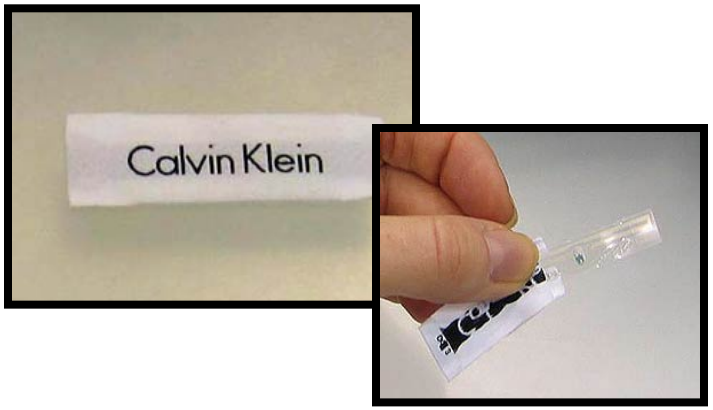
Part 2.3: Malicious Traceability

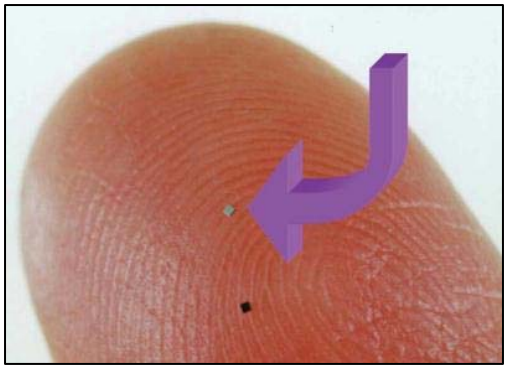
Informal Definition

- An adversary should not be able to track a tag holder, ie, he should not be able to link two interactions tag/reader.
- E.g., tracking of employees by the boss, tracking of children in an amusement park, tracking of military troops, etc.
- Some organizations are quite powerful: CASPIAN, FoeBud, etc.
- Also considered by authorities e.g. malicious traceability taken into account in the ePassport.

Importance of Avoiding Traceability

- Differences between RFID and the other technologies e.g. video, credit cards, GSM, Bluetooth.
  - Passive tags answer without the agreement of their bearers : tags cannot be switched-off.
  - Ubiquity.
  - Tags can be almost invisible.
  - Easy to analyze the logs of the readers.





Palliative Solutions

- Kill-command (Eg: EPC Gen 2 requires a 32-bit kill command.)
- Faraday cages.

Secure passport sleeve from www.idstronghold.com

- Removable antenna.
  - US Patent 7283035 - RF data communications device with selectively removable antenna portion and method.
- Tag must be pressed (SmartCode Corp.).
- Blocker tags.
- None of these solutions are convenient.

Application Layer

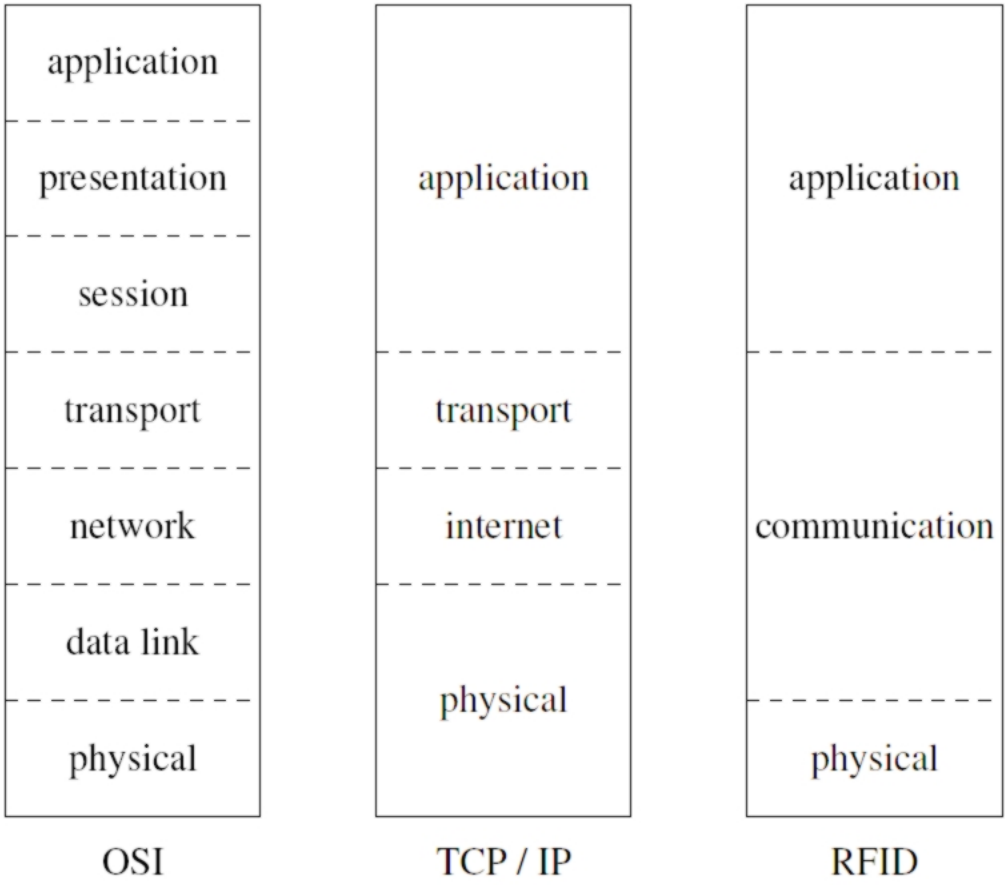
SKID2

$T \leftarrow R \quad r_R$

$T \rightarrow R \quad H_{k_{TR}}(r_R, r_T, R), r_T$, *I am T*

- This protocol is not privacy-friendly because the ID must be revealed.
  - How can one make the protocol privacy-friendly?
- Challenge-Response avoiding malicious traceability do not scale well.
  - Authenticating one tag requires $O(n)$ operations.
  - Authenticating the whole system requires $O(n^2)$ operations.

Traceability in Lower Layers



Traceability in Lower Layers: Concept

- The main concepts of cryptography, i.e, confidentiality, integrity, and authentication, are treated without any practical considerations.
- If one of these properties is theoretically ensured, it remains ensured in practice whatever the layer we choose to implement the protocol.
- Privacy needs to be ensured at each layer: All efforts to prevent traceability in the application layer may be useless if no care is taken at the lower layers.

Communication Layer

- Collision-avoidance protocol.
- The computational power of the tags is very limited and they are unable to communicate with each other.
- The reader must deal with the collision avoidance itself.
- Collision avoidance protocols are often (non-open source) proprietary algorithms. Some standards appear: ISO and EPC.
- Two large families: deterministic protocols and probabilistic protocols.
  - With probabilistic protocols, the attacker can track the tag if it always answers during the same time slot.
  - With deterministic protocols, the attacker can track the tag because the identifier is static. The straightforward solution is to renew the identifier (of the communication layer) each time the tag is identified by a reader.

Physical Layer

- Air interface (frequency, modulation, etc.)
- The physical signals exchanged between a tag and a reader can allow an adversary to recognize a tag or a set of tags.
- Threats due to the diversity of standards.
  - Signals from tags using different standards are easy to distinguish.
  - A problem arises when we consider sets of tags rather than a single tag.
  - If several standards are in use, each person in a few years may have a set of tags with a characteristic mix of standards which may allow a person to be traced.

Physical Layer

- Threats due to radio fingerprints.
  - Even if the tags follow the same standard, there will be several manufacturers in the market and their tags will have different radio fingerprints.
  - It will thus be possible to trace a person by a characteristic mix of tags from different manufacturers.
  - Preventing traceability through radio fingerprints seems quite difficult because there is no benefit for the manufacturers in producing tags that use exactly the same technology, producing the same radio fingerprint.
- Conclusion quite pessimistic in the physical layer but attacks within this layer require strong means.

Today

- In the physical layer.
  - Hard to avoid malicious traceability, but tracking one tag is far from being easy in practice.
- In the communication layer.
  - Malicious traceability is usually do-able in practice.
  - Can be avoided if a cryptographically-secure PRNG is used.
- In the application layer.
  - Malicious traceability can be avoided but challenge-response protocols do not scale well.

Challenges

- Can we design a better protocol ie privacy and low complexity?
  - All proposals have been broken.
  - Manage the keys differently (eg. ePassports).
- Can we implement a PK cipher on a tag in wired logic only?
  - Some current works e.g. GPS, WIPR.
- Can we design secure PRNGs?
  - Still an open work.
- Definition of a formal model.

Part 2.4: Denial of Service

Definition

- A DoS attack aims at preventing the target from fulfilling its normal service.
  - For fun.
  - For disturbing a competitor.
  - For proving that RFID is not secure.

- Techniques.
  - Electronic noise.
  - Disturbing the collision-avoidance protocol.
  - Exploiting the kill-command.
  - Exploiting a bug in the reader.
  - Destroy tags.

Example: the Electronic Passport

- Lucas Grunwald, German security expert, found a buffer-overflow attack against two ePassport readers made by different manufacturers.

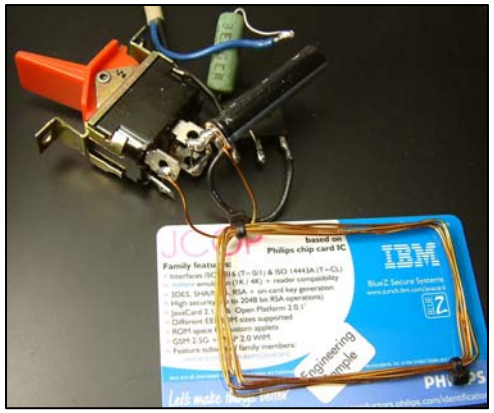
- He copied the content of a passport, modified the JPEG2000 face picture, and wrote the modified data in a writable chip. The reader crashed.

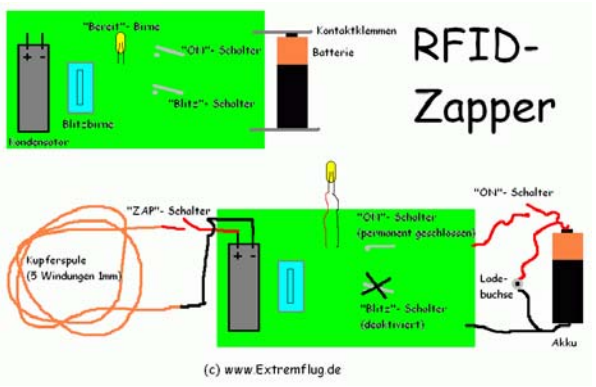
Example: The Original RFID-Zapper

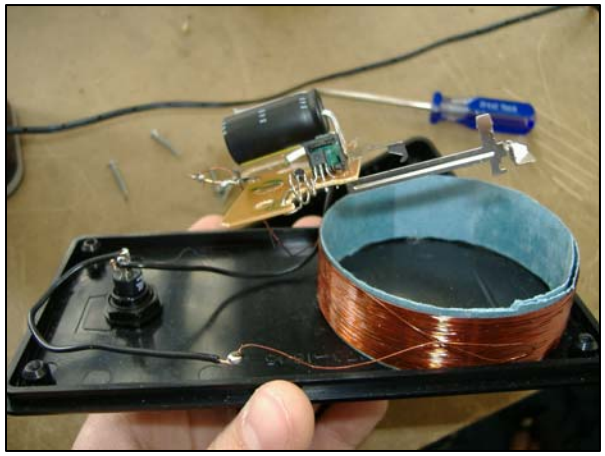
- Presented at Chaos Communication Congress 2005.

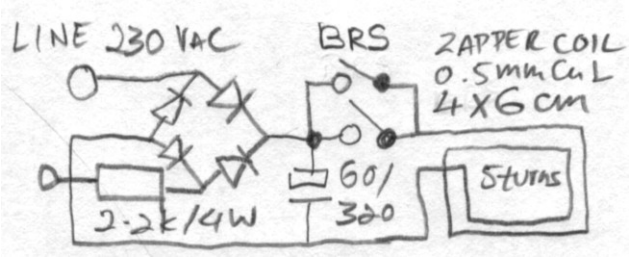
- Disposable camera with flash.
  - Flash is removed.
  - Flash capacitor connected to a coil.
  - When capacitor is loaded, switching the circuit produces a strong electromagnetic pulse.
  - The field induces a current inside the chip that is definitively killed.

Some RFID-Zappers Found on the Web









GSI INFORMATION SECURITY GROUP

Summary

- Today.
  - Hard to thwart such attacks, especially the electronic ones.
- Challenges.
  - Design protocols resistant to DoS attacks.
  - Engineering problem.
  - Be ready to react and communicate.

Part 3: The Passport Case

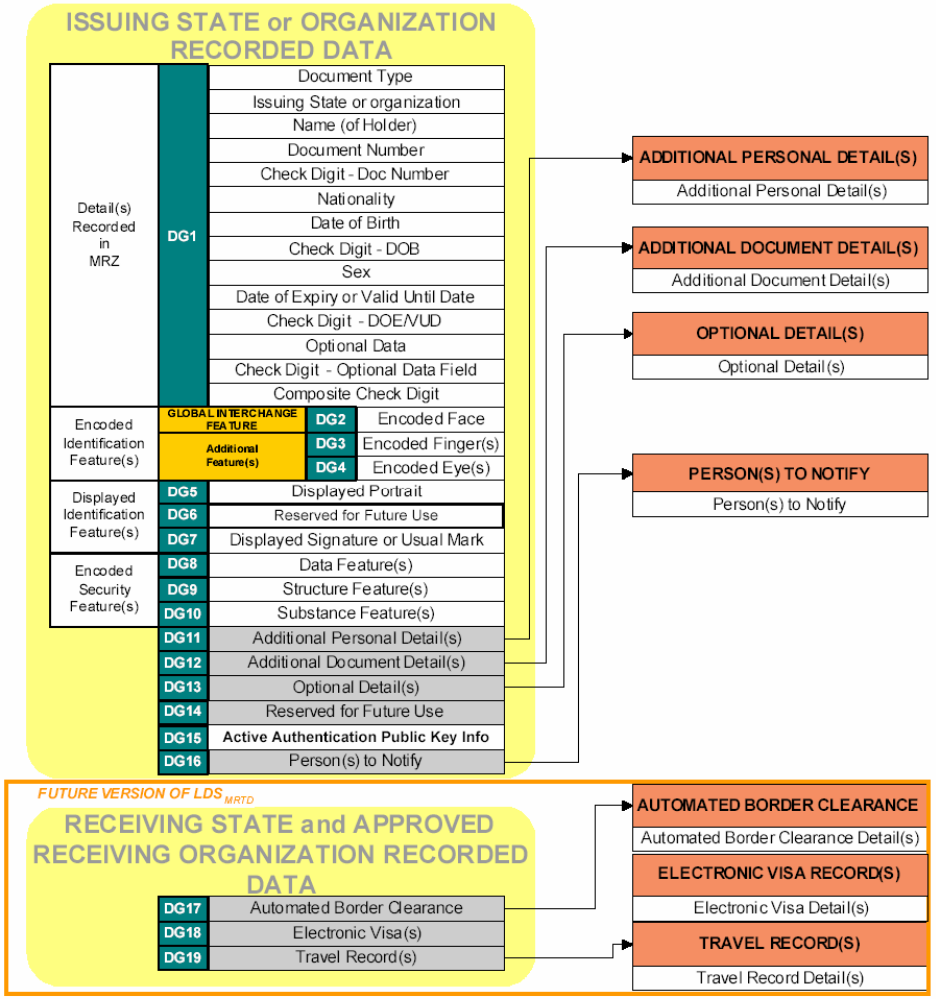
Basics on the Passport

- International Civil Aviation Organization (ICAO)
- ICAO works on electronic passport (ePassport) since late 90s
- ICAO Standard (Doc 9303) released in 2004
- First ICAO-compliant electronic passport issued end 2004
- More than 50 countries today
- Securing passports with chip: Davida & Desmedt Eurocrypt'88
- First electronic passports: Malaysia (1998)

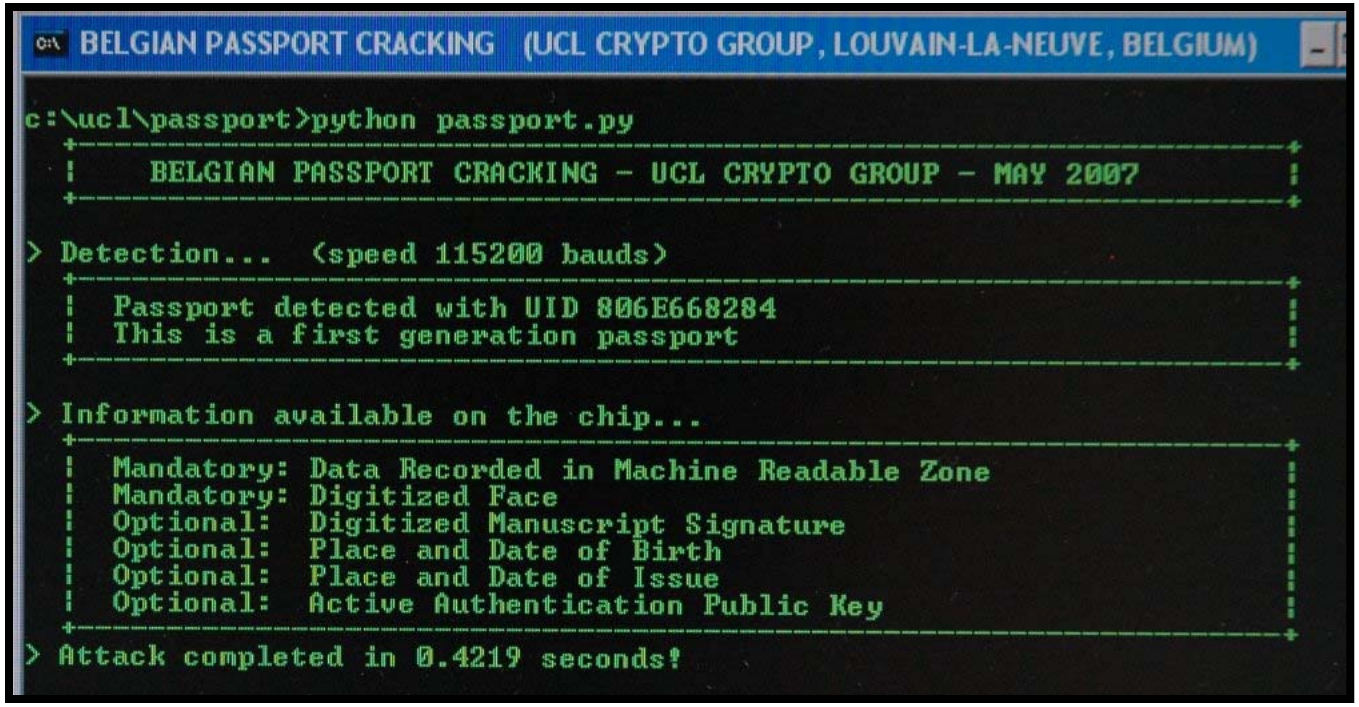
Technical Facts on the Passport

- Tag is passive ie no internal battery.
- Tag has a microprocessor (public-key crypto).
- Compliant ICAO Doc 9303 and ISO 14443.
- Distance 10 cm, 1m (in labs).

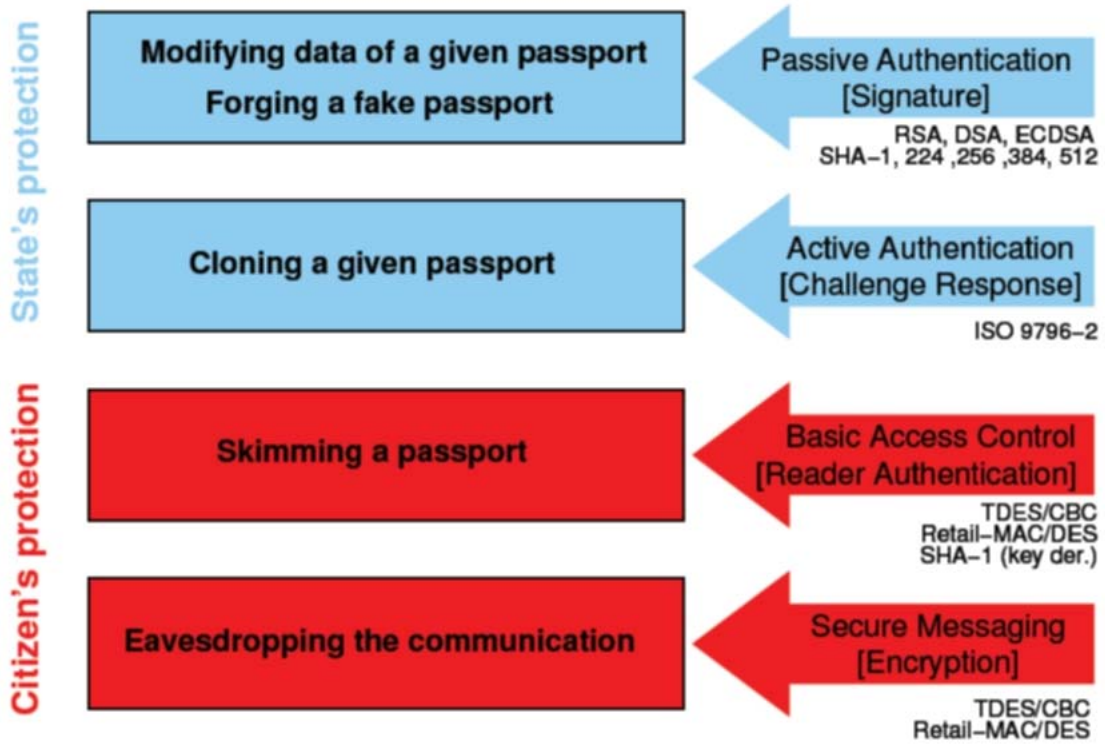
Content of the Passports



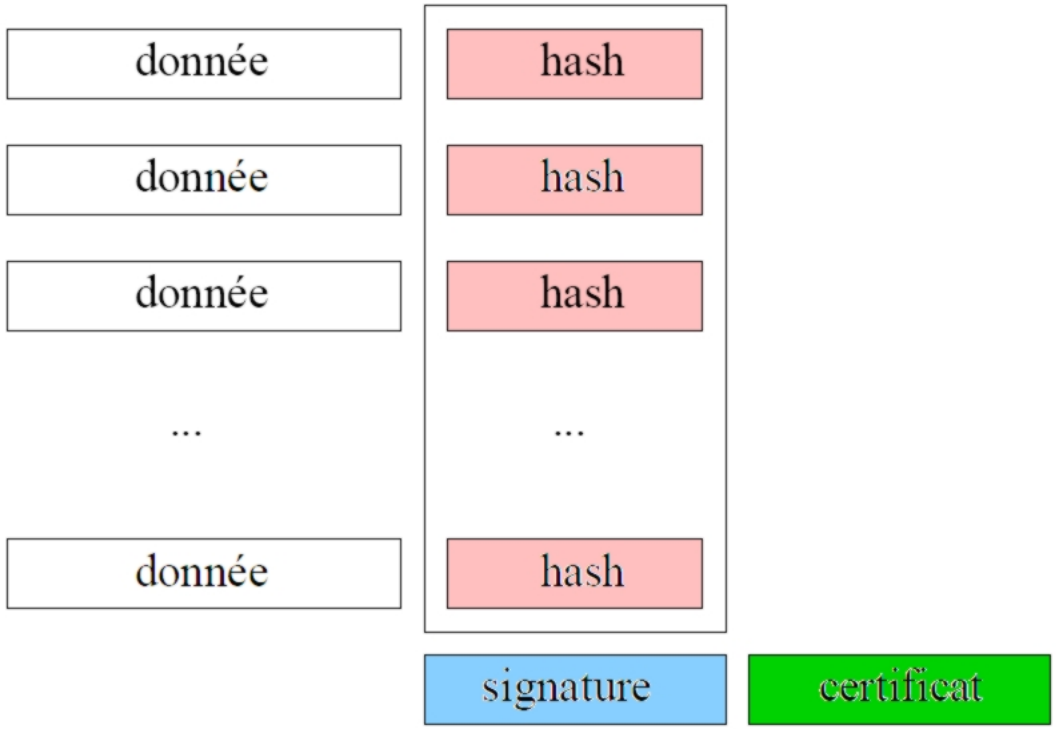
Content of the Belgian Passports



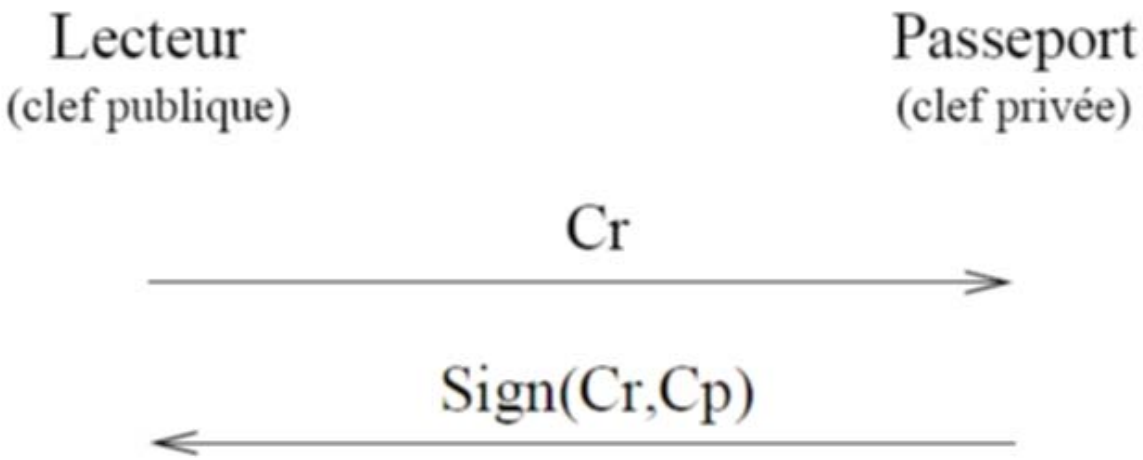
Protection Mechanisms



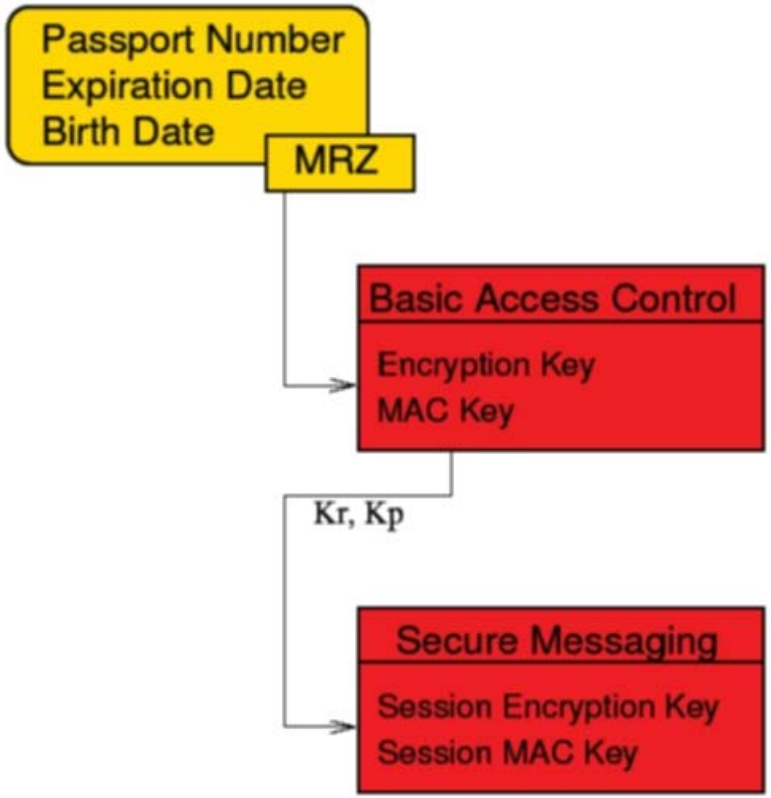
Passive Authentication

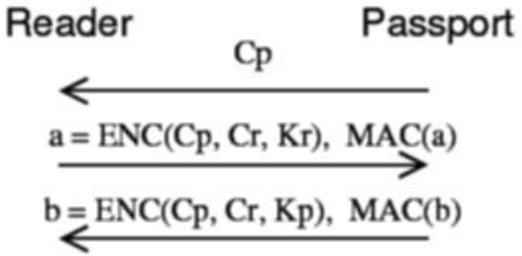


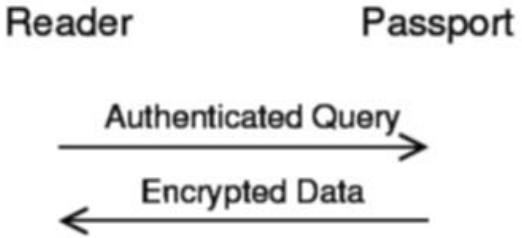
Active Authentication



Basic Access Control & Secure Messaging





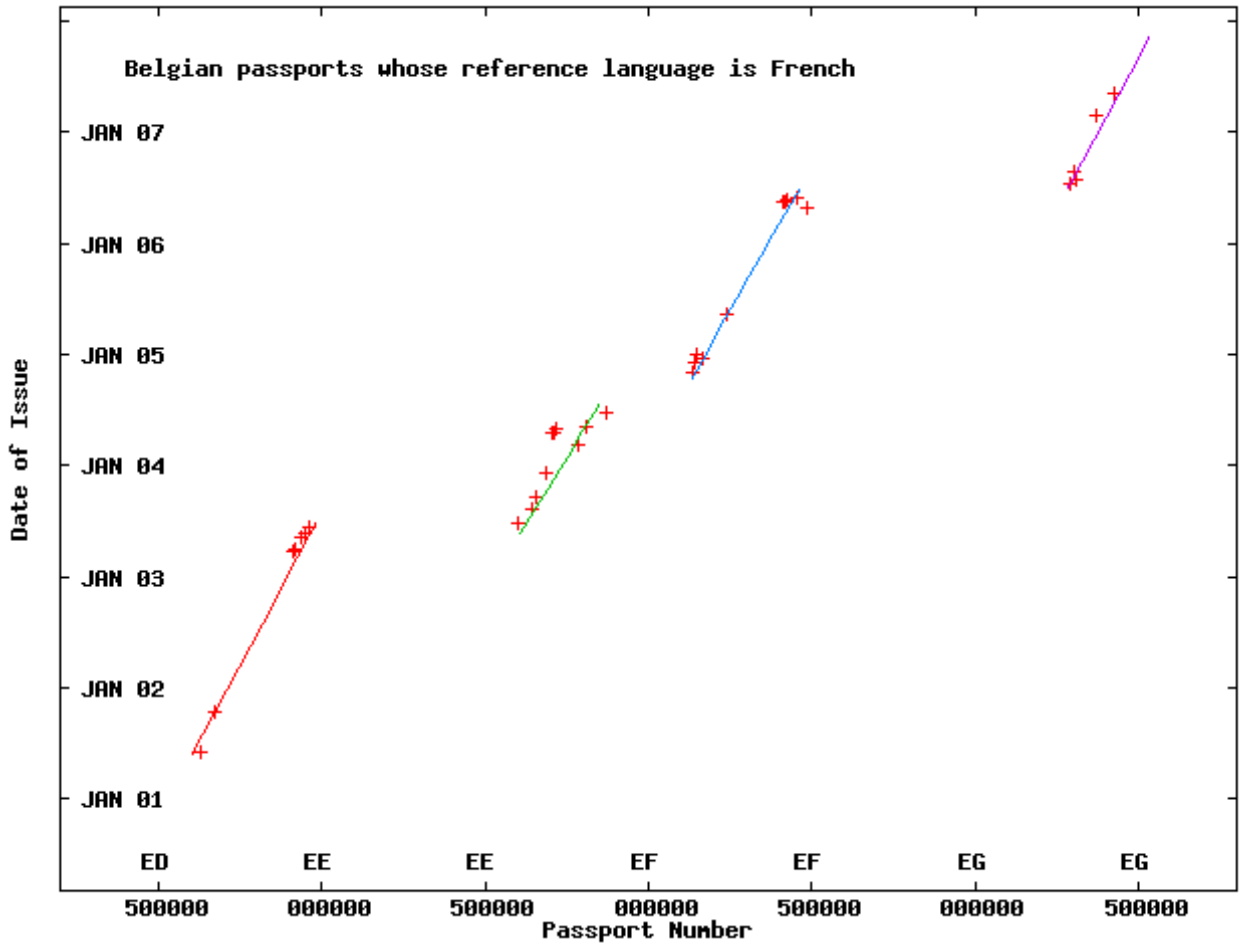


Low Entropy of the Keys

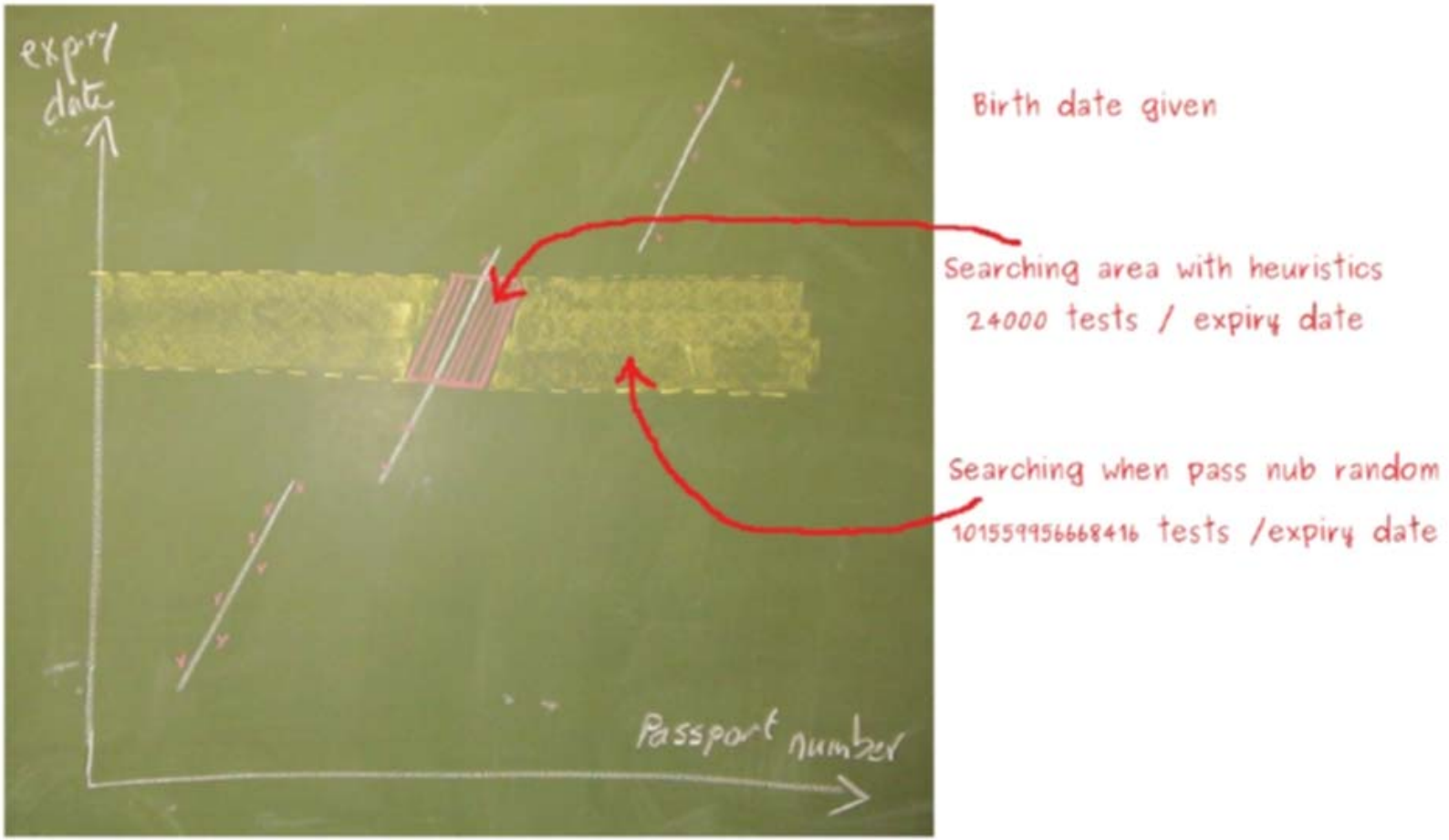
- BAC keys are derived from the MRZ, especially date of birth, date of expiry, passport number.

Country	Effective	Birth date known
Germany	55	40
USA	54	39
Netherlands	50	35
Belgium	38	23

Belgian Passport Numbers: Issuance



Belgian Passport Numbers: Search Space



The Experiment

- Off-line vs on-line attack
- First vs second generation

ePassport viewer

- http://sites.uclouvain.be/security/epassport.html

Conclusion

Conclusion

- 2002-2004: Discovery age of RFID Security.
  - About 35 papers.
  - Privacy.
- 2005-2010: Pedestrian approach of RFID Security.
  - About 350 papers. (how many valuable?)
  - Ad-hoc privacy, Reader complexity, Lightweight building blocks (mostly symmetric), Distance bounding, Models.
  - Focus on Tag-Reader communication.

Conclusion

- From 2011? The mature age.
  - Formalization, formalization, and formalization.
  - Split between low and high layers (applications).
  - Consideration of the practical constraints.
  - Pseudo-random generators.
  - Public-key cryptography without microprocessor.
  - Side channel attacks.
  - Distance bounding.
  - Path checking, group authentication.

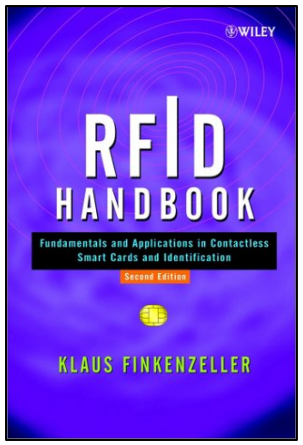
Going Further

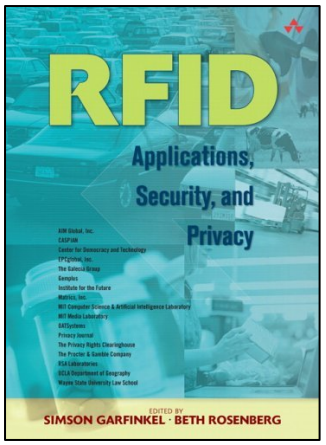
RFID Security & Privacy

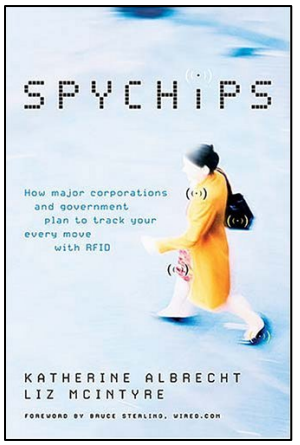
- RFID Security and Privacy Lounge.
  - www.avoine.net/rfid/
  - www.sites.uclouvain.be/security/
  - About 750 people on the mailing list.
  - About 400 academic research papers.

- RFID Training days at the UCL in 2010
  - Topic: Security and Privacy in RFID System.
  - A comprehensive course devoted to industrials.
  - A whole week on the topic with theory and practice.

Going Further







MISC: security-devoted magazine (in French).

- Dossier about RFID in Oct 07
- Special issue on smartcards (incl. contactless) in Oct 08.