

RFID Security and Privacy

Gildas Avoine, UCL Belgium

Lecturer Presentation

Lecturer Presentation: University

- Prof. **Gildas Avoine**.
- Hired at the **UCL Belgium** in Sept 2007, **CS Department**.
- University created in 1425, about 20'000 students.



Lecturer Presentation: IS Group

- **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.
 - Practical attacks.
- **Algorithms related to security (time-memory trade-off)**.
 - Cracking systems (eg passwords).
 - Using TMT0 in a constructive way.

Aim of the Presentation

- **Introduce 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 contains a microcircuit and an antenna to enable it to receive and respond to radio-frequency queries from an RFID reader/writer.



Architecture



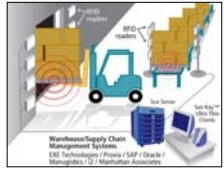
History

- RFID exists since the forties (IFF, Russian spy).
 - Commercial RFID applications appeared in the early eighties.
 - 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

Management of Stocks

- The goal is to improve the supply chain.
- Examples: Wal-Mart, US Department of Defense.



Libraries

- Replacing the bar-codes by RFID tags.
- Improve the book borrowing procedure and the inventory.
- Examples: Santa Clara, Vienna, Leuven, Rennes.



Pet Identification

- Replace common identification tattoo by electronic one.
- ISO 11784, ISO 11785.



Source: www.flickr.com

Sensors

- Pressure or temperature sensors.



Source: www.prodescom.biz



Building Access Control

- Building access control.



- Access to the VIP Zone: Baja Beach Club.



Source: www.prodescom.biz

Automobile keys

- Door locks: KeeLoq.



Source: www.pisa.info

- Ignition key: Texas Instrument DST Module.



Source: www.carthiefstoppers.com

Real Time Location

- In amusement parks: Track children using the **SafeTZone** technology.



Source: www.safetzone.com

Electronic Documents

- Example: **Passports**, standardized by ICAO. Issued since 2004 in Belgium ; today, more than 50 countries.



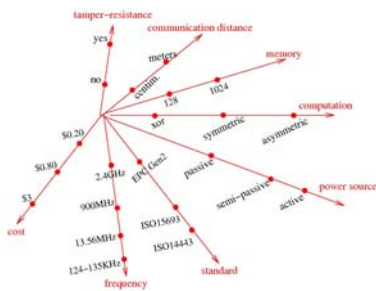
Public Transportation

- **Examples:** Paris, Boston, Brussels, NYC, Singapore, London,



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.
- **Asymmetric** cryptography (ie public-key).
 - RSA, ECC.
 - Microprocessor required.

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).

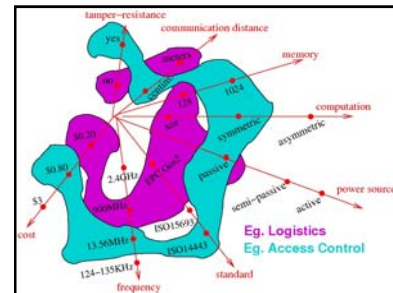
Class-3: Semi-passive tags

- 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 1.4: Identification vs Authentication

Identification vs Authentication

- A major issue when designing a protocol is defining its purpose.
- Applications can be classified into two categories:
 - Those whose initial goal is to provide **security** to the system.
 - Those whose initial goal is to provide **functionality**.

Examples

- Management of stocks.
- Electronic documents.
- Public transportation.
- Counting cattle.
- Pets identification.
- Access control.
- Localization of people.
- Libraries.

Definitions

- **Definition (Identification Protocol)**
 - An **identification** protocol allows a reader to obtain the identity claimed by a queried tag.
- **Definition (Authentication Protocol)**
 - An **authentication** protocol allows a reader (resp. tag) to obtain the true identity of a queried tag (resp. querying reader).
 - A **mutual authentication** protocol allows a reader to obtain the true identity of a queried tag, and this latter to obtain the true identity of the querying reader.

In Brief...

- **Identification:** Get Identity of remote party.
- **Authentication:** Get Identity + Proof of remote party

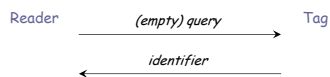
Part 2: Security and Privacy Threats

Part 2.1: Impersonation

Definition

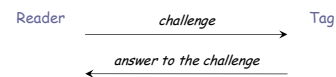
- **Definition (resistance to impersonation)**
 - The probability is negligible that any adversary distinct from the tag, carrying out the protocol playing the role of the tag, can cause the reader to complete and accept the tag's identity.
- Speaking about **impersonation** when dealing with **identification** does not make sense: Impersonation is related to **authentication**.

Identification Protocol



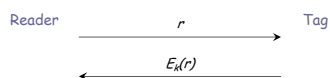
- The identifier is not necessarily the UID (eg: pet identification).
- **Replay attack** is possible.

Auth. Protocol: Challenge/Response



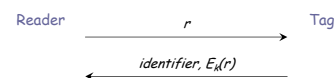
- **Challenge** is never used twice.
- **Answering** to the challenge requires to know a secret shared between the reader and the tag only.
- A **replay attack** is no longer possible.

Auth. Protocol: Challenge/Response



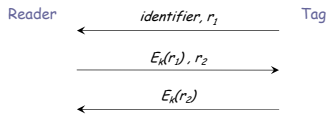
- r is the challenge (nonce).
- k is the secret key shared by the reader and the tag.
- E is a cryptographic operation, eg an encryption function or a keyed hash function.

Auth. Protocol: Challenge/Response



- In practice, the **identifier** is required in the answer to know which key should be used by the reader.

Mutual Authentication Protocol



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

- An **identification** protocol is used for the **MIT's access control**.
- This is not unusual!
- Eavesdropping the communication reader-tag once, or skimming the tag once allows to create a cloned access card.



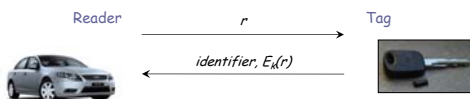
Bad Example: KeeLoq

- **KeeLoq**: Car locks and alarms, sold by Microchip, used by Chrysler, Daewoo, Honda, BMW, Jaguar, Fiat, GM, Volvo, Toyota.
- $2^{44.5}$ cryptographic operations to crack any card.
 - Secure requires 2^{80} , recommended is 2^{128} .
 - The poor design allows to recover the master key.
- **Two days** on 50 Dual Core machines.



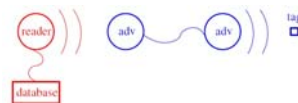
Bad Example: Texas Instrument DST

- 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**: active attack in less than 1 minute (**time-memory trade-offs**).



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**.



Solutions to Relay Attacks

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

Moral of the Story

- Do not cut the price by using weak primitives.
- Use well-known primitives.
- Know what you use (client, manufacturer).
- Be up-to-date.

Part 2.2: Information Leakage

Definition

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

Californian Senate Bill 682

- In **California**, the **Senate Bill 682** planned to limit use of RFID in ID cards. In its initial version (Feb 22, 2005) the pending act was very restrictive:

*"The act would **prohibit identity documents** created, mandated, or issued by various **public entities** from **containing a contactless integrated circuit** or other device that can broadcast personal information or enable personal information to be scanned remotely."*

Who is the Victim?



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).

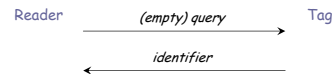
ABIEC Information Leakage



Part 2.3: Malicious Traceability

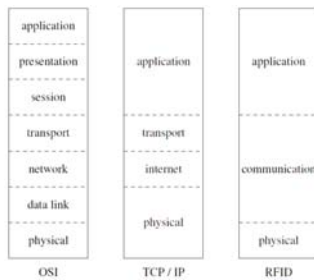
Definition

- 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.



- **Do-able** from a technical point of view.

Traceability in Lower Layers

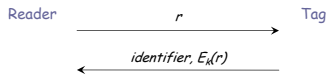


Traceability in Lower Layers: Concept

- 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.

Application Layer

- Most of the proposals focus on this layer only.



- Challenge-response protocols avoiding malicious traceability **do not scale well**.

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.

Palliative Solutions

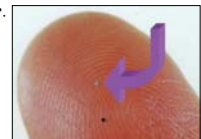
- kill-command.
 - Eg: EPC Gen 2 standard requires a 32-bit kill command.
- Faraday cages.
- Blocker tags.
- Bill of Rights.
- Removable antenna.
 - US Patent 7283035 - RF data communications device with selectively removable antenna portion and method.
- Tag must be pressed (SmartCode Corp.).



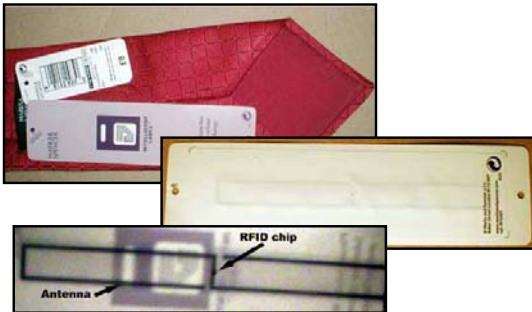
Secure passport sleeve from www.usstronghold.com

Importance of Avoiding Traceability

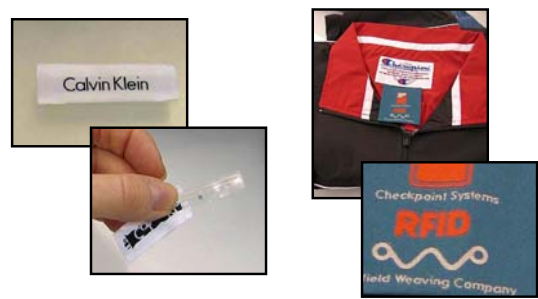
- Differences between RFID and the other technologies e.g. video, credit cards, GSM, Bluetooth.
 - Tags cannot be switched-off.
 - Tags answer without the agreement of their bearers.
 - Easy to analyze the logs of the readers.
 - Increasing of the communication range
 - Eg. Crossing the US-Canadian border.
 - Tags can be almost invisible.



Hidden Tag in a Tie



Hidden Tags in Calvin Klein Clothes

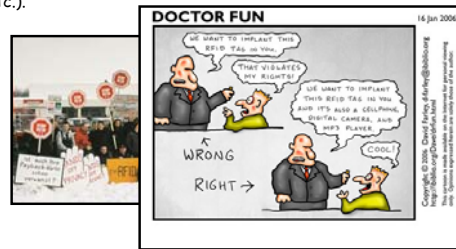


Hidden Tags in Diapers



Liberty Rights Organizations

- Even if you do not think that privacy is important, some people think so and they are rather influential (CASPIAN, FoeBud, etc.).



Part 2.4: Denial of Service

Definition

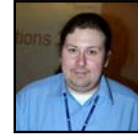
- A DoS attack aims at preventing the target from fulfilling its normal service.
- Threatened by DoS attacks if:
 - Wireless technology (if reader/devices close to public zone).
 - There is an interface inside / outside.
- Hard to thwart such attacks.
- Reasons:
 - For fun.
 - For disturbing a competitor.
 - For proving that RFID is not secure.

Techniques

- Kill-command
- Blocker tag
- Electronic noise
- kill or hide tags (electronics, etc.)
- Bug in the Reader/Back-end System
- Viruses

Example in 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**.



Part 3: The Passport Case

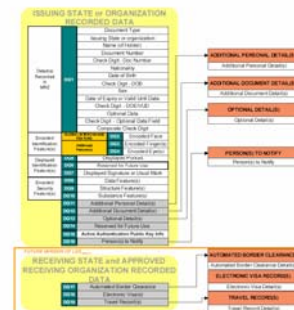
Basics on the Passport

- 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

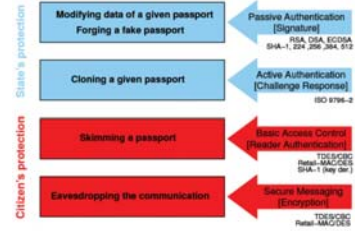


Content of the Belgian Passports

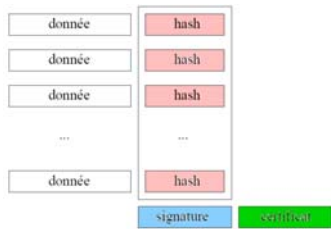
```

BELGIAN PASSPORT CRACKING - UCL CRYPTO GROUP - LOUVAIN LA NEUVÉ, BELGIUM
python passport.py
BELGIAN PASSPORT CRACKING - UCL CRYPTO GROUP - NOV 2007
Detection... (speed 115200 bauds)
Passport detected with UID #063648284
This is a first generation passport
Information available on the chip...
Mandatory: Data Recorded in Machine Readable Zone
Mandatory: Digitized Photo
Optional: Digitized Manuscript Signature
Optional: Place and Date of Birth
Optional: Place and Date of Issue
Optional: Active Authentication Public Key
Attack completed in 0.4217 seconds
    
```

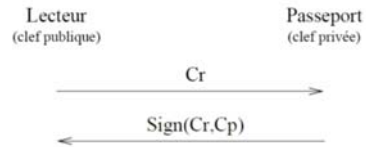
Protection Mechanisms



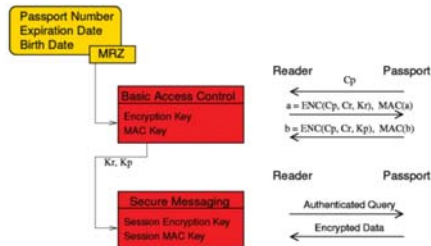
Passive Authentication



Active Authentication



Basic Access Control & Secure Messaging



Low Entropy of the Keys

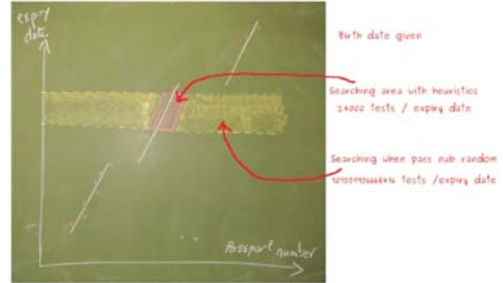
- BAC keys are derived from the MRZ, especially **date of birth**, **date of expiry**, **passport number**.

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



Attack in Practice



Conclusion

Up-to-Date Security View

- Security issues in RFID are usually due to:
 - Poorly designed algorithms and protocols, **not audited** by experts.
 - Secure systems simplified to fit the practical requirement (eg. use the same key in all the tags because the reader do not support multiple keys).
- Heavy cryptography still requires a **microprocessor** (expensive) but some more lightweight algorithms or implementations appear, and can use only **wired logic**:
 - AES with 4000 logic gates.
 - XTEA: block cipher requiring few logic gates.
 - GPS: public-key authentication.
- Solving the **malicious traceability** issue with cryptographic means is still an **open problem**.

Up-to-Date Security View

- The **relay attacks** may become more dangerous than expected. Solutions exist in the laboratory. Are these solutions **implementable**?
- The victim is not only the **tag's holder**, it may also be the **system** itself.

Going Further



- MISC**: security-devoted magazine (in French).
- Dossier about RFID in Oct 07
 - Special issue on smartcards (incl. contactless) in Oct 08.

Going Further

- **RFID Security and Privacy Lounge.**
 - www.avoine.net/rfid/
 - About 700 people registered to the mailing list.
 - List of academic research papers.
 - Should be extended in 2009 with some RFID tools.
- **RFID Training days at the UCL in 2009**
 - Topic: Security and Privacy in RFID System.
 - A comprehensive course devoted to industrials.
 - Just an idea up to know.
 - Will depend if some people interested.

RFID
Security & Privacy