

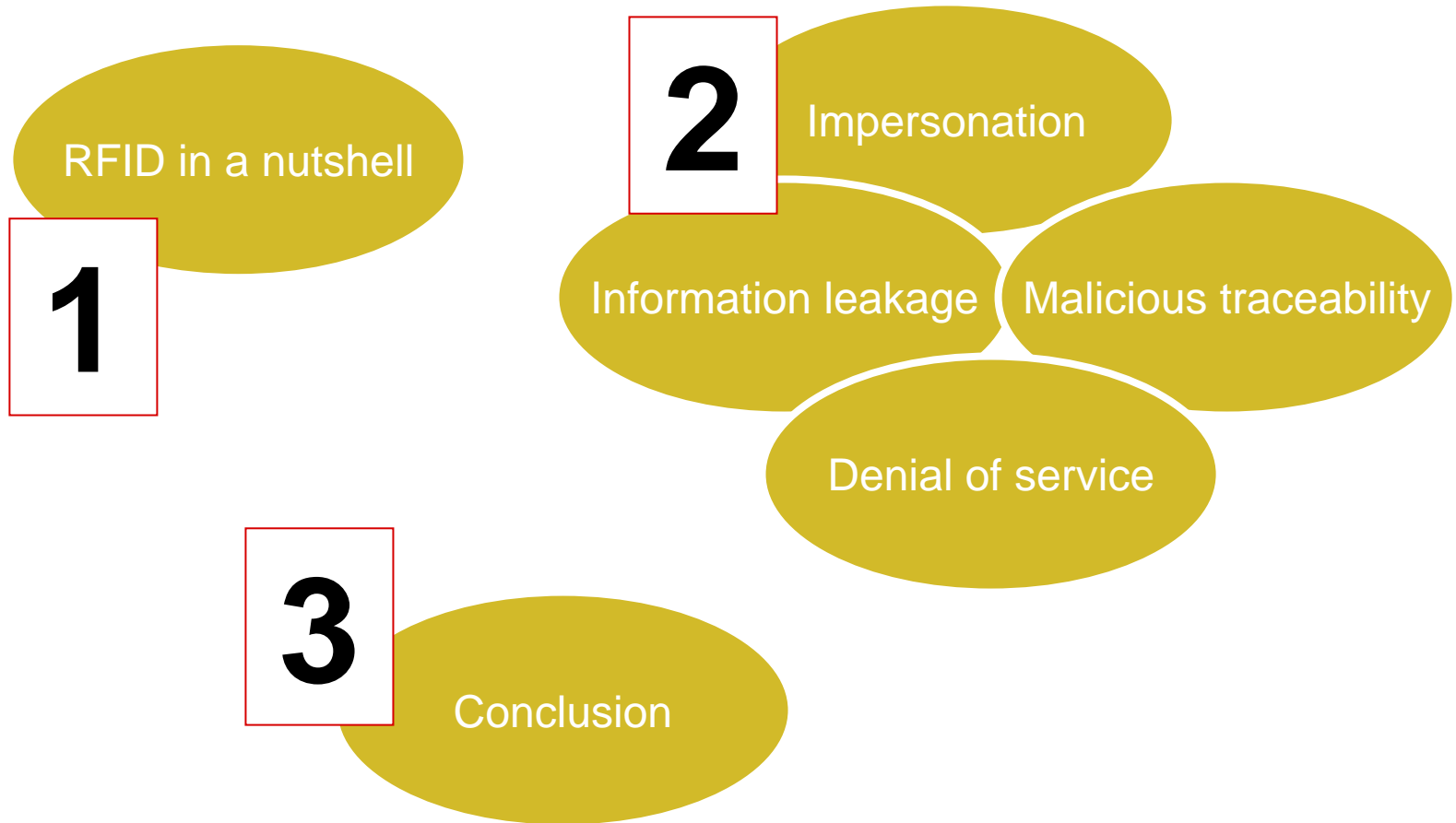
RFID: Classification of the Security Issues

Gildas Avoine, UCL Belgium

SACOSE Meeting

April 23rd 2010, Toulon, France

Outline



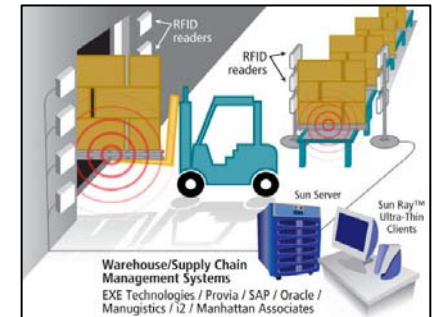
RFID in a Nutshell

Definition

- Radio Frequency Identification.
- An **RFID tag** can be a **low-capability** integrated circuit with an antenna e.g. for pet identification, but also a **powerful** contactless **smartcard** e.g. for biometric passports.

Basic RFID

- **Supply chain.**
 - Track boxes, palettes, etc.
- **Libraries.**
 - Improve book borrowing procedure and inventory.
- **Pet identification.**
 - Replace common identification tattoo by electronic one.
 - Will become mandatory in the EU.



Source: www.dcllogistics.com



Source: www.rfid-library.com



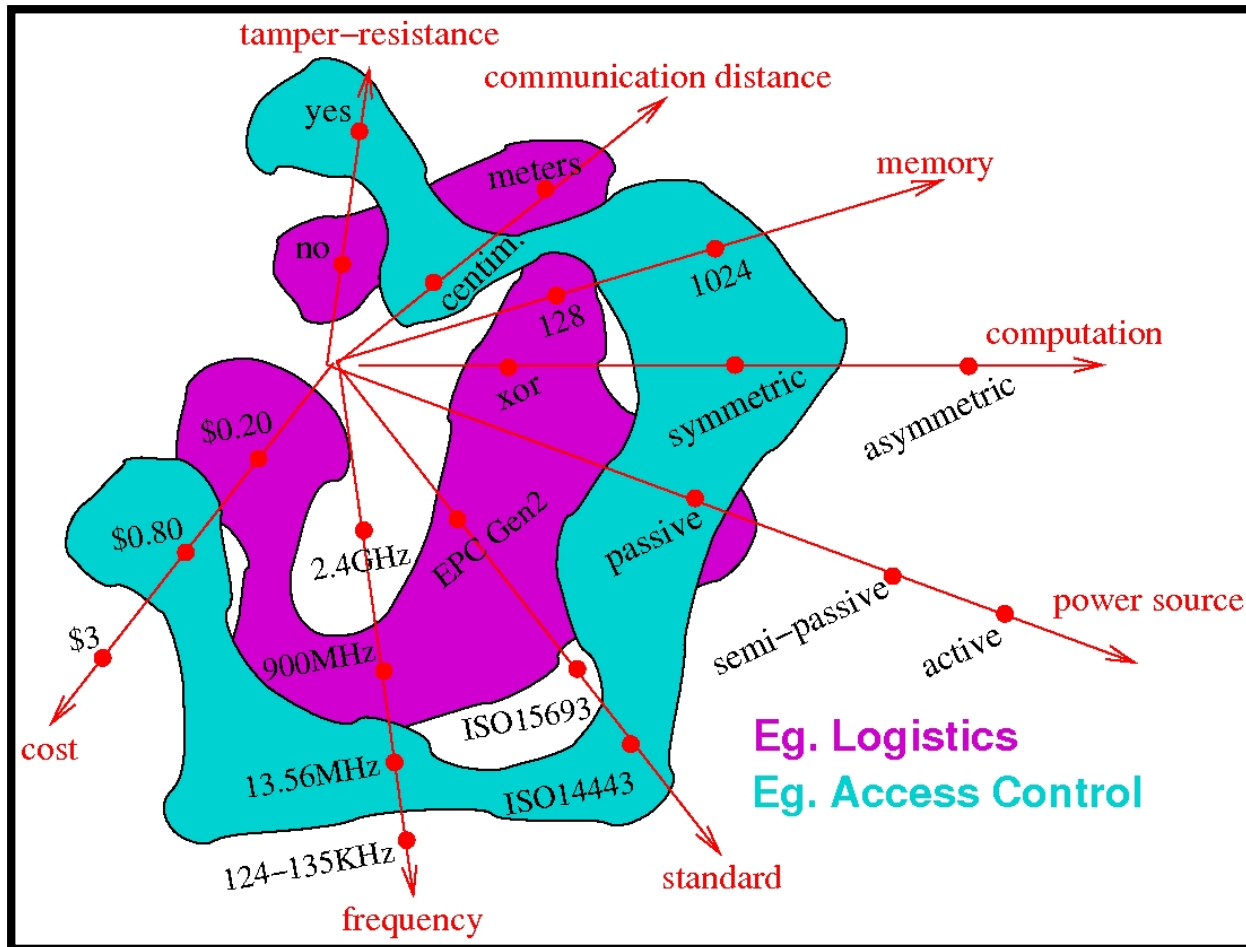
Source: www.flickr.com

Evolved RFID

- Building access control.
- Automobile ignition keys.
- Passports.
 - Electronic passports since 2004.
- Public transportation.
 - Eg. Brussels, Boston, Paris, London.



Typical Configurations



Summary: RFID in a Nutshell

- **Wireless.**
 - Easier to skim and eavesdrop.
- **Low-capabilities.**
 - Calculation, Memory, Bandwidth.
- **Answer without holder's agreement / awareness.**
 - Easier to skim, Attack not detected.

Impersonation

Detection, Identification, and Authentication

Detection

Get the proof that something/one is present.

Identification

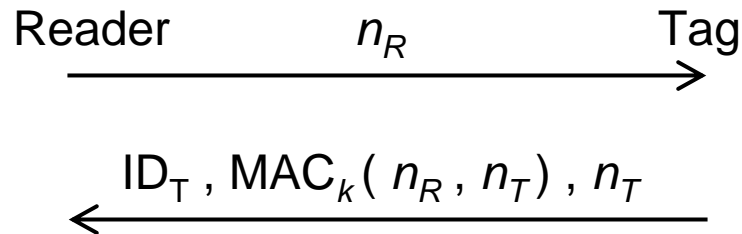
Get identity of remote party.

Authentication

Get identity + proof of remote party

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.



- We know how to design a **secure authentication** scheme.

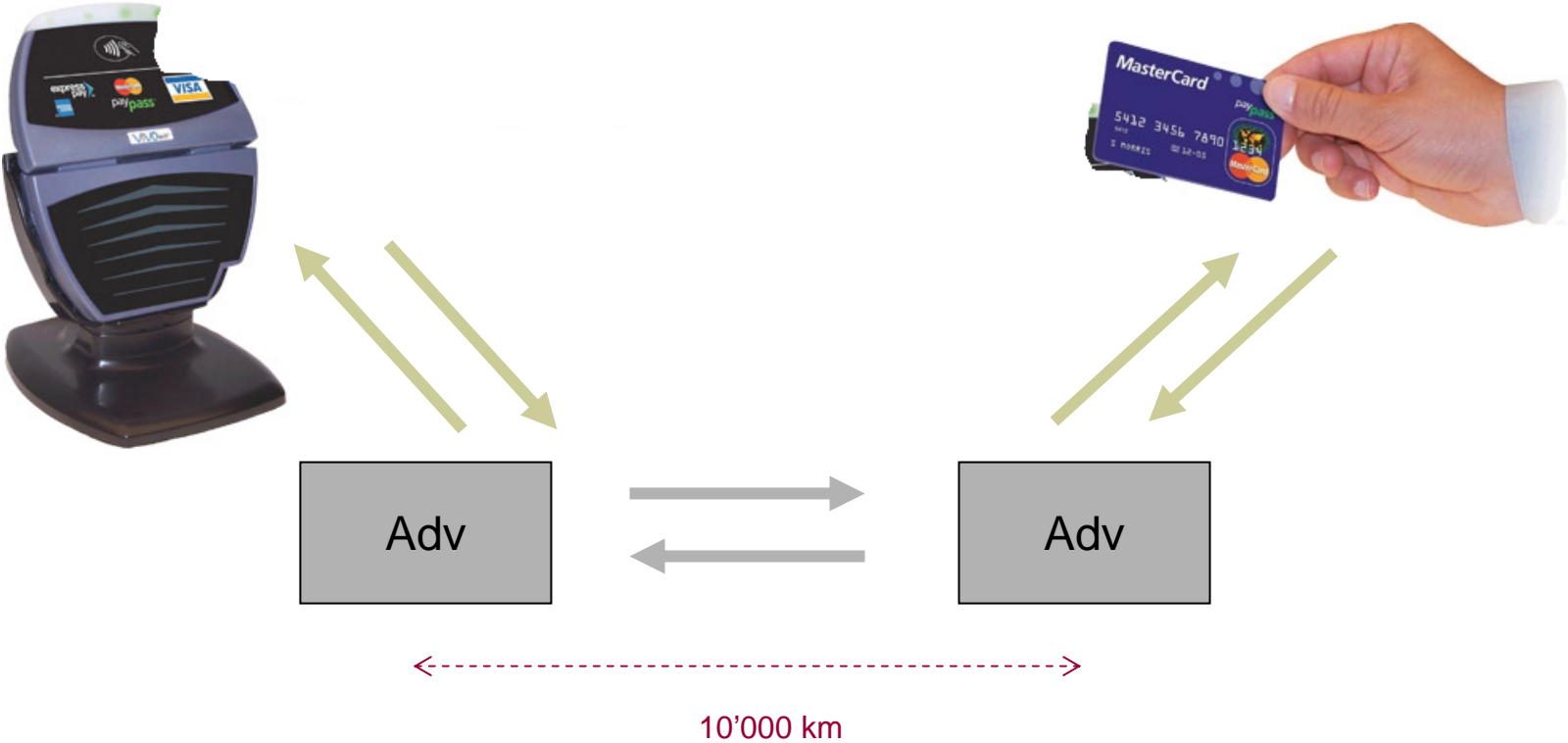
Practical Challenges in the Real Life

- Authentication is done using an identification protocol.
 - Eg. **MIT** access card.
- Proprietary algorithms.
 - Keys too short eg. **TI DST**.
 - Weaknesses in the algorithms eg. **Mifare Classic**.
 - ...

Example of Poor Design: 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** and **2009**: Crypto1 revealed and any **Mifare Classic** tag can be **broken** today in a few seconds.

Relay Attacks



Relay Attacks

- Feasibility of the **attacks**.
 - Labs or real life?
 - Maximum distance?
- Feasibility of the **solutions**.
 - Compute the round-trip-time of a message.
 - Practicability.

Summary: Impersonation

- We know how to deal with this problem, in **theory**.
- **Cost** of the solution.
 - Require lightweight algorithms (wired logic).
- **Implementation** issues.
 - Both readers and tags, pseudo-random generators.
- **Architecture** of the solution.
 - Building blocks are not enough: the whole solution must be secure.
- **Relay** attacks and distance bounding.
- New **challenges**.
 - Group authentication, path authentication.

Information Leakage

Impact

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

Hidden Tag in the Real-life



Liberty Rights Organization

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



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.”

The screenshot shows the CNIL website interface. At the top, there's a navigation bar with the CNIL logo, flags for France, UK, and Spain, contact information (allo CNIL, tél : 01 53 73 22 22), a newsletter sign-up button (lettre info CNIL je m'inscris), and an RSS feed icon. Below this is a red banner with the slogan: "L'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés". The breadcrumb trail reads: Accueil > Dossiers > Déplacements-Transports > Fiches pratiques > L'invasion des puces !. The main content area is titled "Fiches pratiques" and includes options for text size, sending, and printing. The article title is "L'invasion des puces !". The text discusses RFID technology, its applications, and privacy concerns. A sidebar on the left contains a menu with categories like "La CNIL", "Vos libertés", "Vos responsabilités", "Dossiers" (with sub-items like Banque-Crédit, Collectivités locales, Conso-Pub-Spam, Déplacements-Transports, Identité numérique, Internet-télécoms, Police-Justice, Santé, Scolarité-Mineurs, Travail, Vie citoyenne), and "En savoir plus". A search bar and a "Voir aussi" section with a link to "La radio-identification" are also visible.

CNIL

allo CNIL
tél : 01 53 73 22 22

lettre info CNIL
je m'inscris

RSS

L'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés

Accueil > Dossiers > Déplacements-Transports > Fiches pratiques > L'invasion des puces !

Fiches pratiques

taille du texte

envoyer

imprimer

L'invasion des puces !

Les RFID (Radio Frequency Identification)

Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micro-puce (également dénommée étiquette ou tag) et d'une antenne qui dialogue par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros.

D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi-invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm2, possèdent une capacité de stockage de 512 Ko (kilo octets) et échangent des données à 10Mbps.(méga bits par seconde).

NFC est un standard de communication développé depuis 2002, qui permet à différents types de puces de communiquer et inter-opérer. Les distances de communication pour un débit maximal de 424kbps sont de 10cm.

Comment sont-elles utilisées ?

Les puces sans contact envahissent peu à peu notre quotidien. Elles utilisent plusieurs technologies comme RFID (Radio Frequency Identification) ou NFC (Near Field Communications).

Aujourd'hui, elles sont déjà présentes dans les titres de transports (ex : passe Navigo ou carte Velib), les passeports électroniques, les badges d'accès aux immeubles (ex : Vigik), des porte monnaies électroniques, les clés de contact des voitures, la logistique pour la gestion des bagages dans les aéroports ou des stocks dans les magasins.

La technologie de radio-identification (RFID) devient ainsi un enjeu économique majeur notamment dans les applications de la distribution et du transport.

Mais, l'avenir nous promet des applications encore plus diversifiées. Les puces permettront sans doute de connaître instantanément le contenu d'un caddie au supermarché. Elles pourront analyser les objets achetés ; les produits de luxe seront « tagués » pour éviter les contrefaçons ; les paiements seront sans contact quand des lecteurs NFC équiperont les téléphones. Les médicaments et poches de sang seront « tagués » pour assurer ainsi une meilleure traçabilité.

Des expérimentations sont par ailleurs en cours pour équiper les nouveau-nés, dans certaines maternités, de bracelets RFID, afin d'éviter qu'ils soient kidnappés. A quand la puce implantée sous la peau ? Déjà en Espagne des puces RFID sont injectées sous la peau pour servir de moyen de paiement dans certaines discothèques, ce qui apparaît comme tout à fait disproportionné.

Quels enjeux informatique et libertés ?

European commission

- **Commission Recommendation** of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification (notified under document number C(2009) 3200) (2009/387/EC)
- “Member States should ensure that operators (...) conduct an assessment of the implications of the application implementation for the **protection of personal data and privacy**, including whether the application could be used to **monitor an individual**.”
- “(...) the potential exists for [the RFID] to be used to **monitor individuals** through their possession of one or more items that contain an **RFID** item number.”

Classification

- Information **meaningful by itself**.
- Information meaningful when **associated to a database**.
- Information meaningless **without the appropriate key**.
 - (related to malicious traceability).

Information Meaningful by Itself

Meaningful by Itself

- Information leakage appears when the data sent by the tag **reveals information intrinsic** to the marked object or the holder of the object.
- Tagged books in **libraries**.
- Tagged **pharmaceutical** products, as advocated by the US Food and Drug Administration.
- **E-documents** (passports, ID cards, etc.).
- Loyalty cards, **Public transportation passes**.

Ari Juels' Famous Picture

Wig model #4456
(cheap polyester)

Replacement hip
medical part
#459382

Das Kapital and
Communist-party
handbook

30 items
of lingerie

500 Euros
in wallet
Serial numbers:
597387,389473...

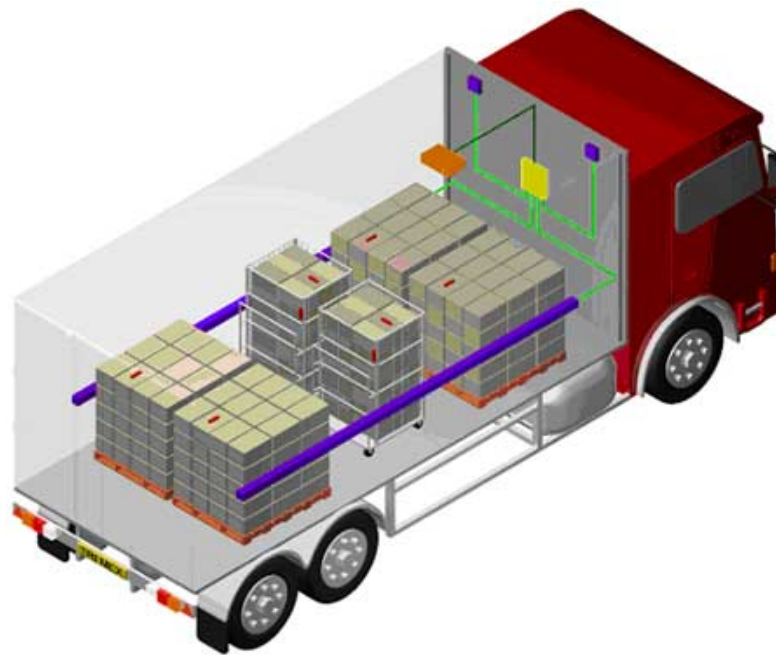


What does Anonymous Mean?

- An information that is anonymous (from an electronic point of view) may be in some way linked to a given person.

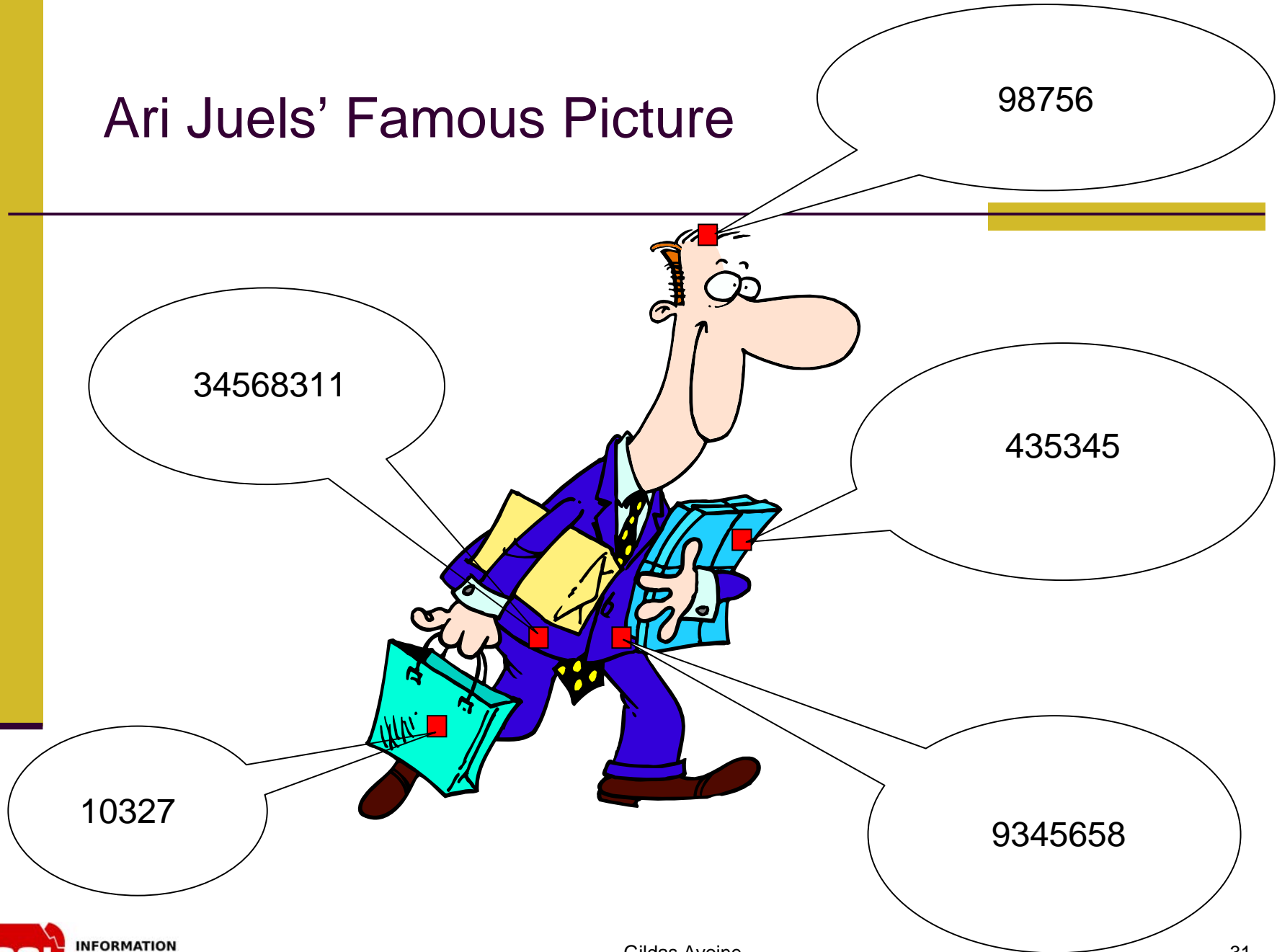
Who is the Victim?

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

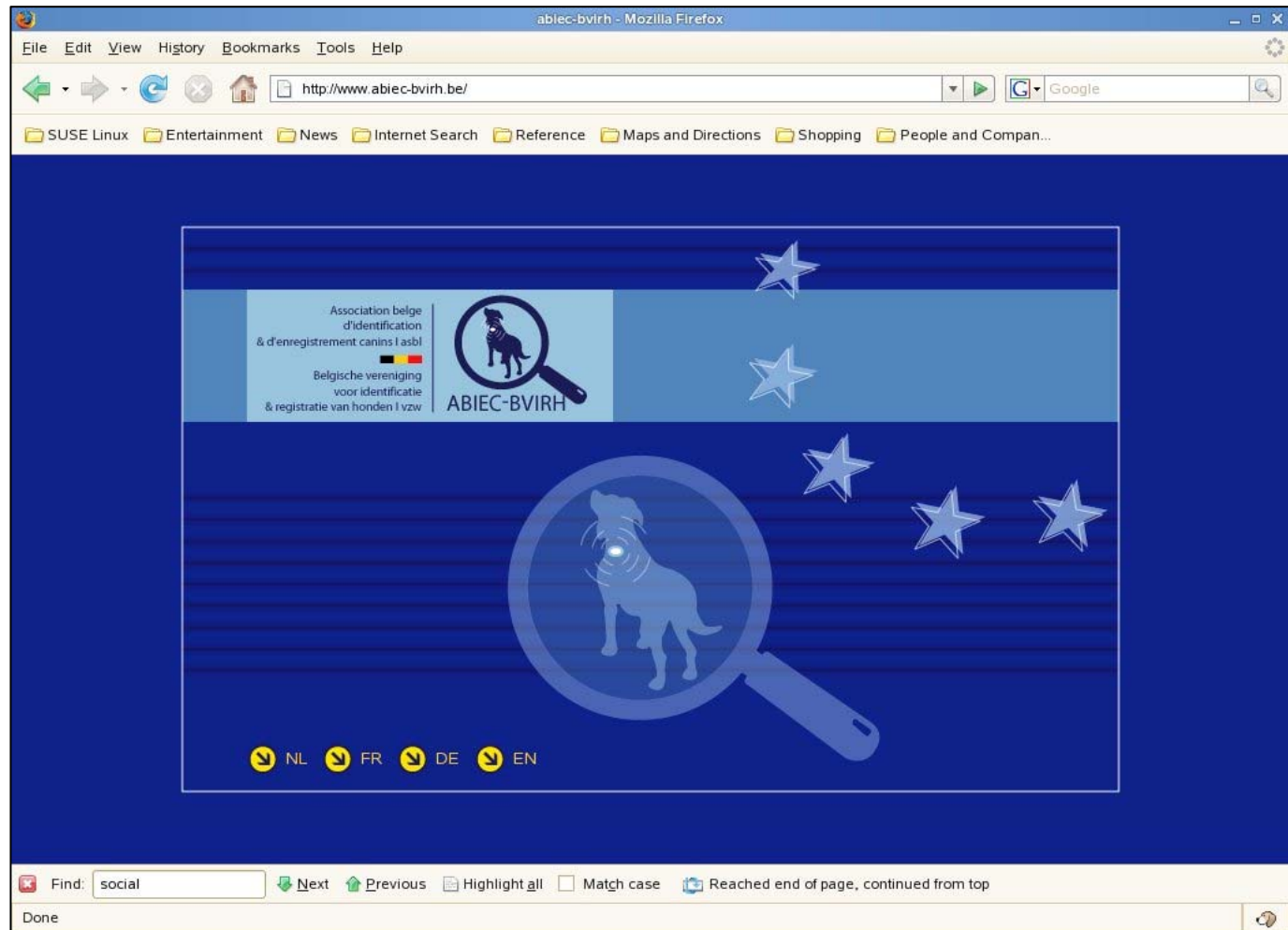


Information Meaningful When Associated to a Database

Ari Juels' Famous Picture



Example: Leakage from the Backend



Summary: Information Leakage

- More and more data collected: “logphilia”.
- Conservative assumption: Information may eventually leak.
- Do we really need to store all these data?
- Encrypt the sensitive data.

Malicious Traceability

Importance of Avoiding Traceability

- 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 customers in a shopping mall, employees by the boss, children in an amusement park, military troops, etc.
- Also considered by authorities e.g. malicious traceability taken into account in the **ePassport**.

Palliative Solutions

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



Secure passport sleeve from www.idstronghold.com

Privacy and Security from the Outset

- **Anne Cavioukan**, Information and Privacy Commissioner of Ontario (Canada):

“Privacy and Security must be built in from the Outset, at the design Stage”

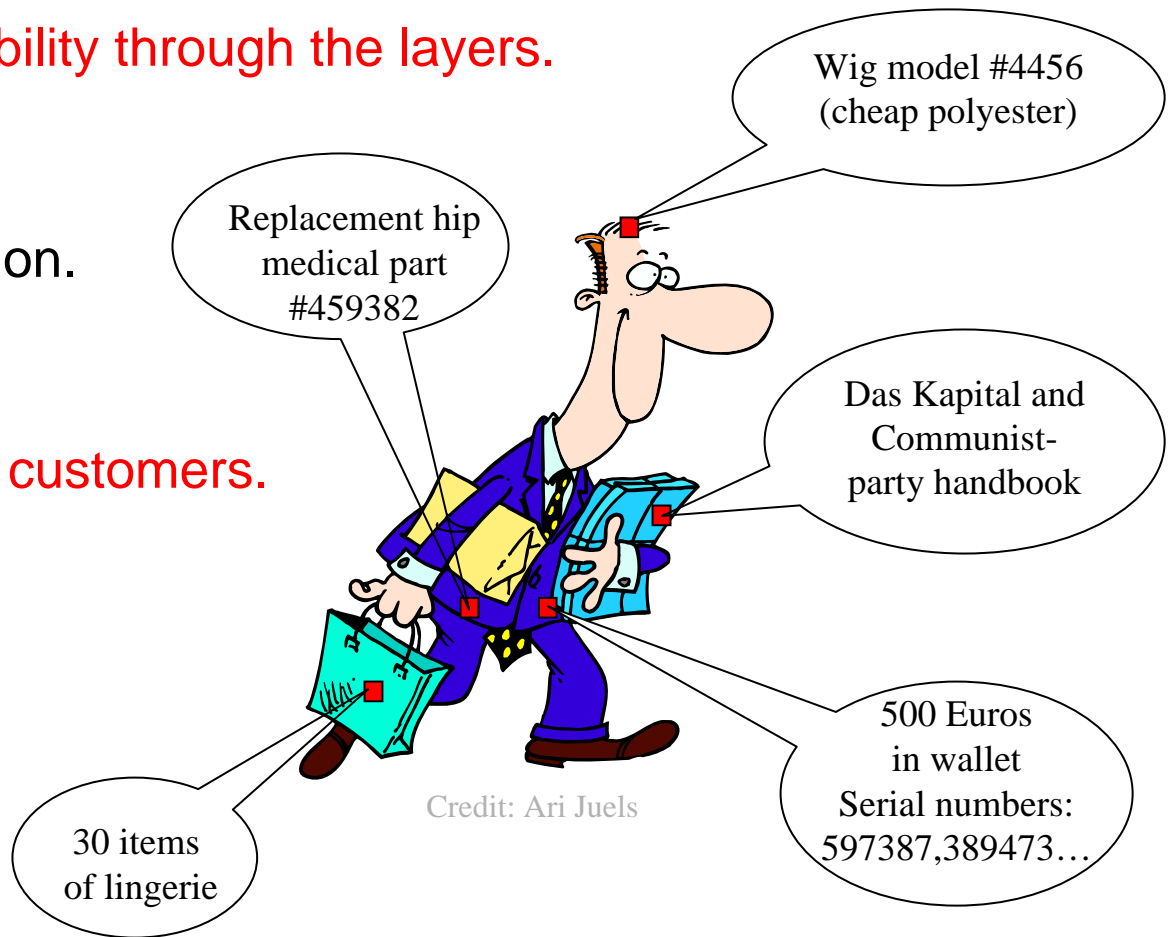
In Privacy Guidelines for RFID Information Systems available on the web site <http://www.ipc.on.ca>.

Impossibility of Avoiding Traceability

- Malicious traceability through the layers.

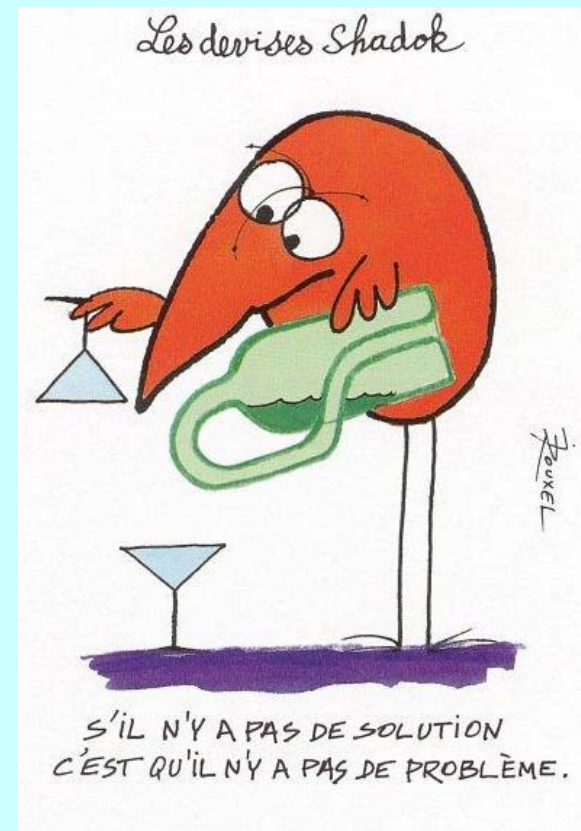
- Application.
- Communication.
- Physical.

- Fingerprinting of customers.



Summary: Malicious Traceability

- No solution.
- **Mitigate** the problem.
 - Eg. No proof of traceability.



Denial of Service

Definition

- **Reasons.**

- For fun.
- For disturbing a competitor.
- For proving that RFID is not secure.

- **Techniques.**

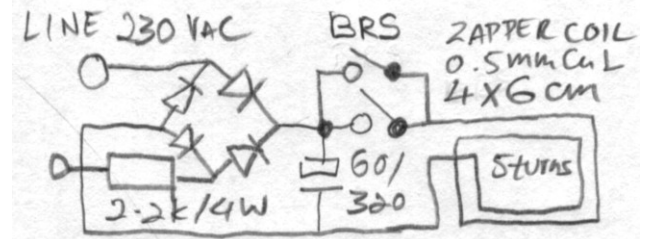
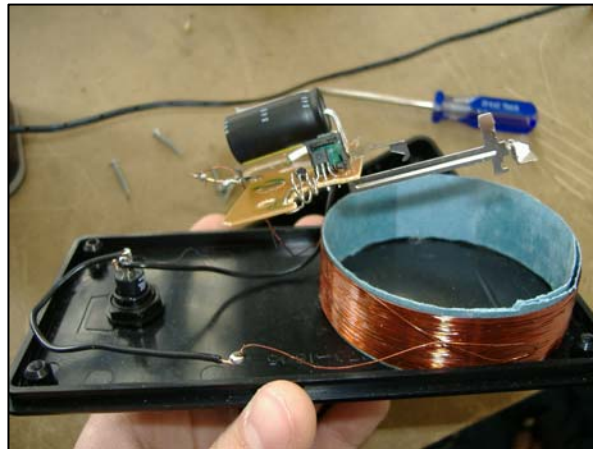
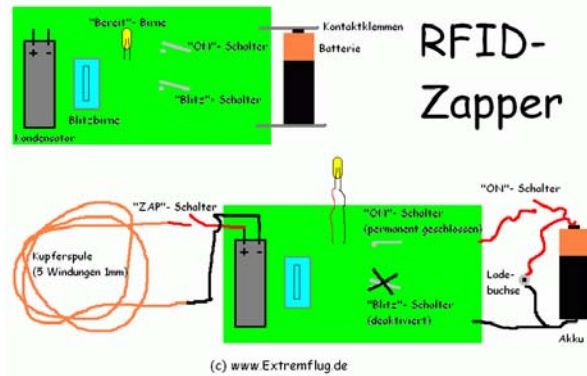
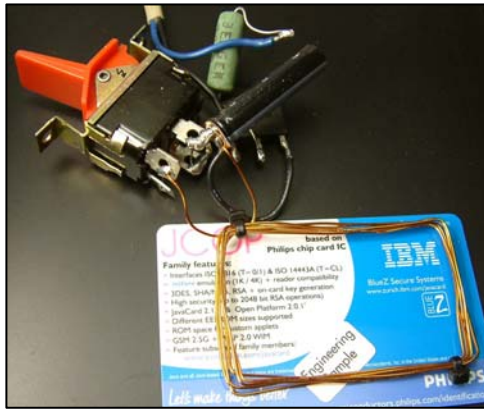
- Electronic noise.
- Disturbing the collision-avoidance protocol.
- Exploiting the kill-command.
- Hide tags.
- Destroy tags.
- Exploiting a bug in the reader.

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



Summary: Denial of Service

- Not so many technical solutions, but care must be taken anyway ...

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.
 - Practical attacks (TI, Mifare, Keyloq,...)

Conclusion

- **From 2011?** The mature age.
 - Formalization, formalization, and formalization.
 - Consideration of the practical constraints.
 - Pseudo-random generators.
 - Public-key cryptography without microprocessor.
 - Side channel attacks.
 - Distance bounding.
 - Path checking, group authentication.

RFID Security: A Large Body of Literature



<http://sites.uclouvain.be/security/>