



**UCL**

Université  
catholique  
de Louvain



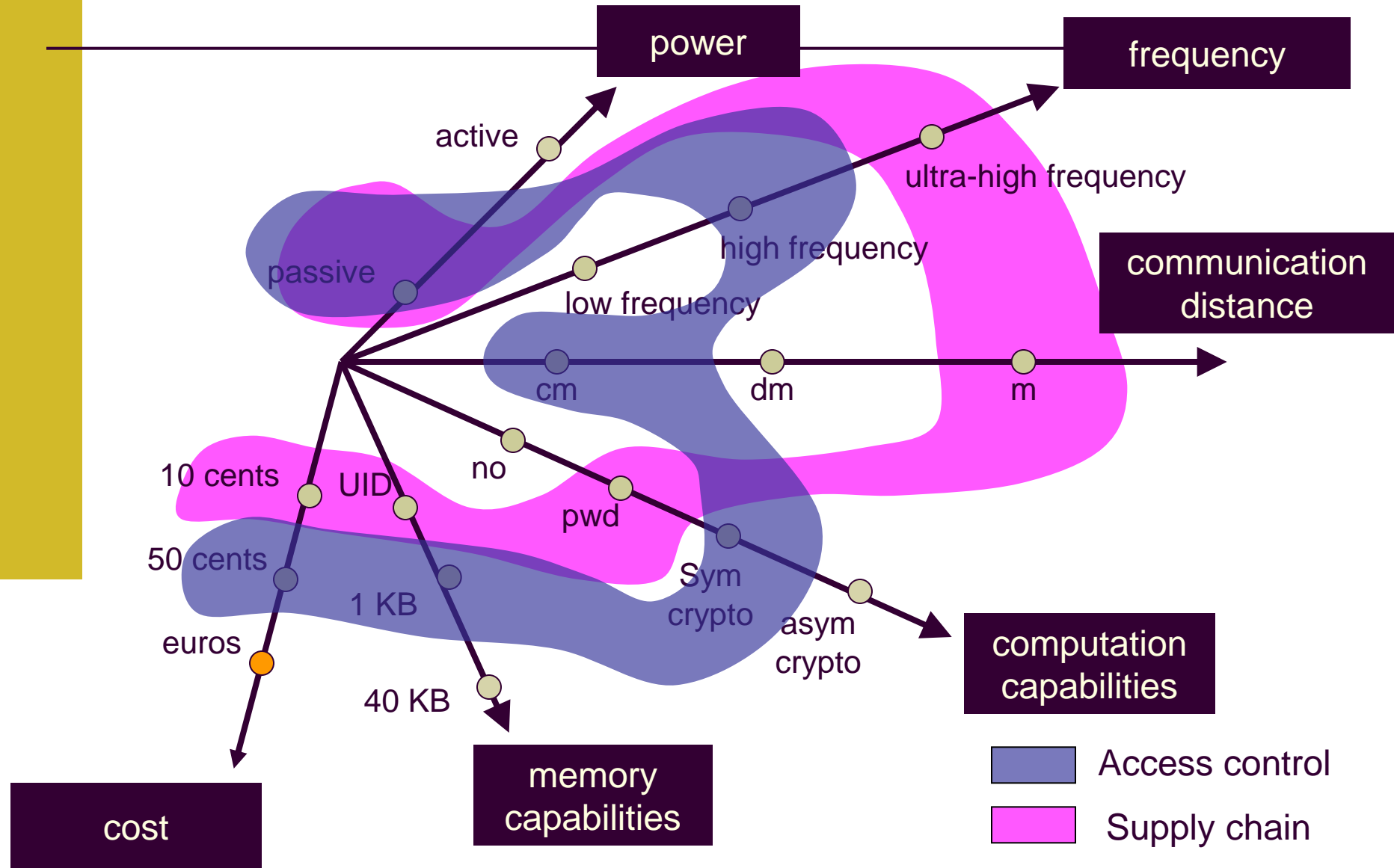
# RFID: Classification of the Security Threats

Gildas Avoine, UCL Belgium



September 27<sup>th</sup> 2010, London, UK

# RFID Capabilities

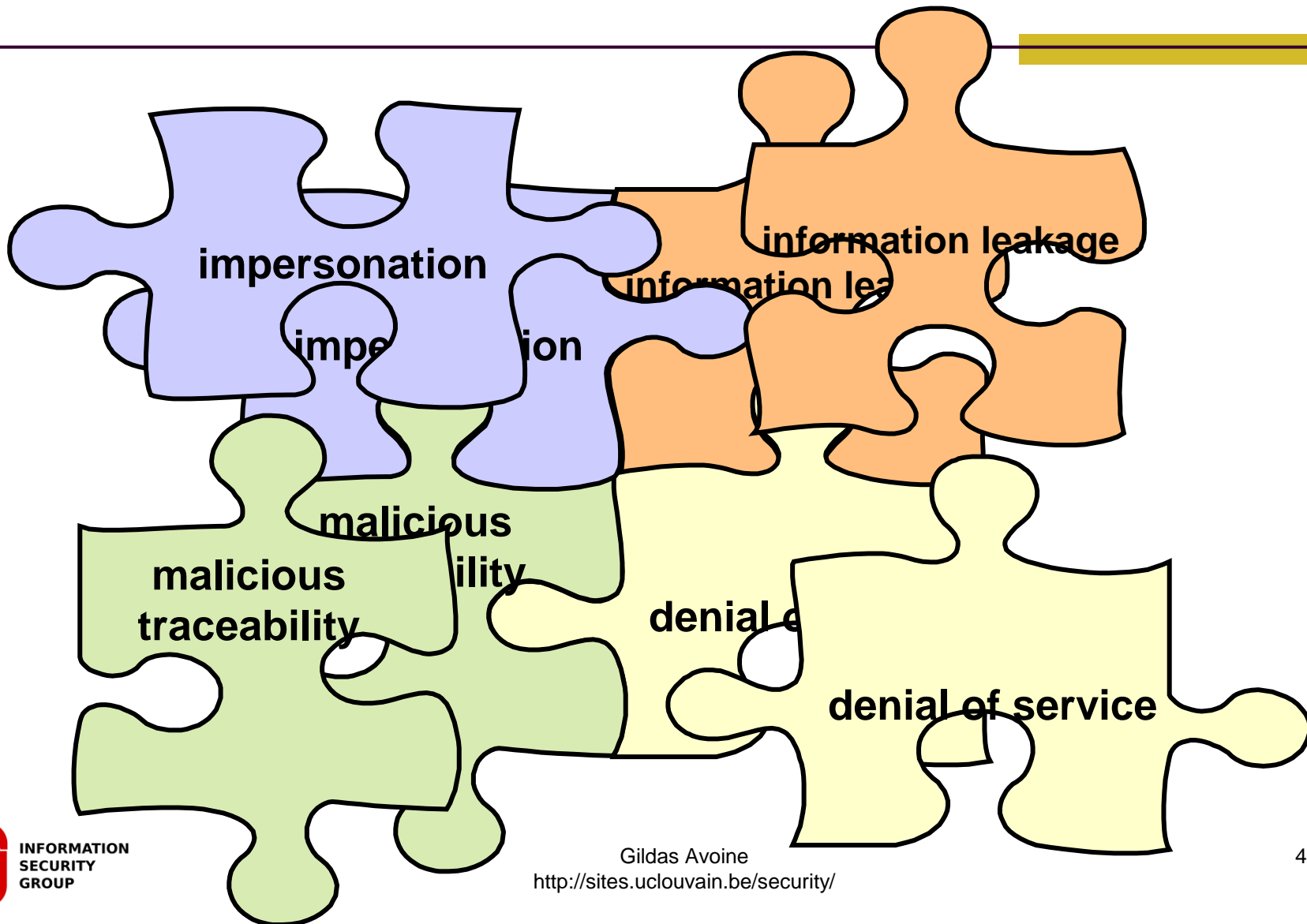


# RFID Security Specificities

---

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

# Security Threat Classification



# Denial of Service

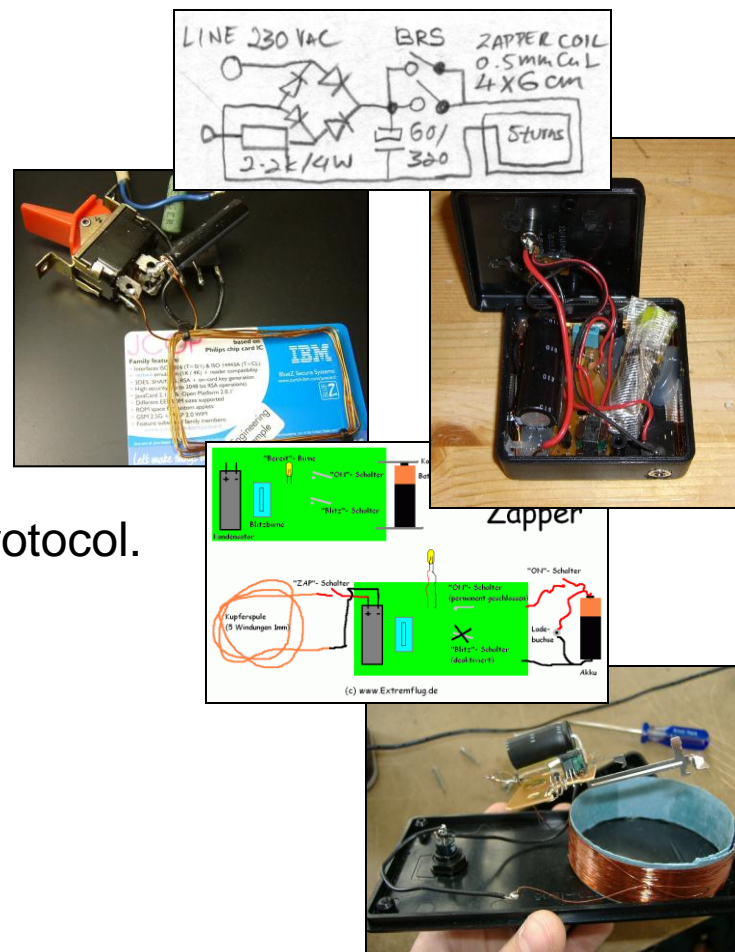
# Denial of Service: Definition

## ■ 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.



# Denial of Service: Interests

- Attacker interest: **low**.
- Customer interest: **low**.
- Academia interest: **low**
  - Not really a research problem.
  - No theoretical solution.
- Industry interest: **low**.
  - Industry should be careful, though, to **youthful errors**:
  - Avoid to deliver the tag freely writable (default keys,...)
  - Sanitary check of the readers' programs.

# 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

# Impersonation

- We know in theory how to design a **secure authentication**.
  - Challenge/Response protocols (eg. ISO9798).
  - Symmetric cipher, a keyed-hash function, a public-key cipher.
- **Cost** of the solution.
  - Require lightweight algorithms (wired logic).
  - Use of weak tags: Mifare Classic, TI DST, Indala,...
- **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.

# Impersonation: Interests

- Attacker interest: **high**.
- Customer interest: **low**.
- Academia interest: **high**.
  - New challenges: Group authentication, Path authentication, Lightweight crypto (no processor), Compromised readers, relay attacks, ...
- Industry interest: **medium**.
  - Cost.
  - Problem can be mitigated, though.

# Information Leakage

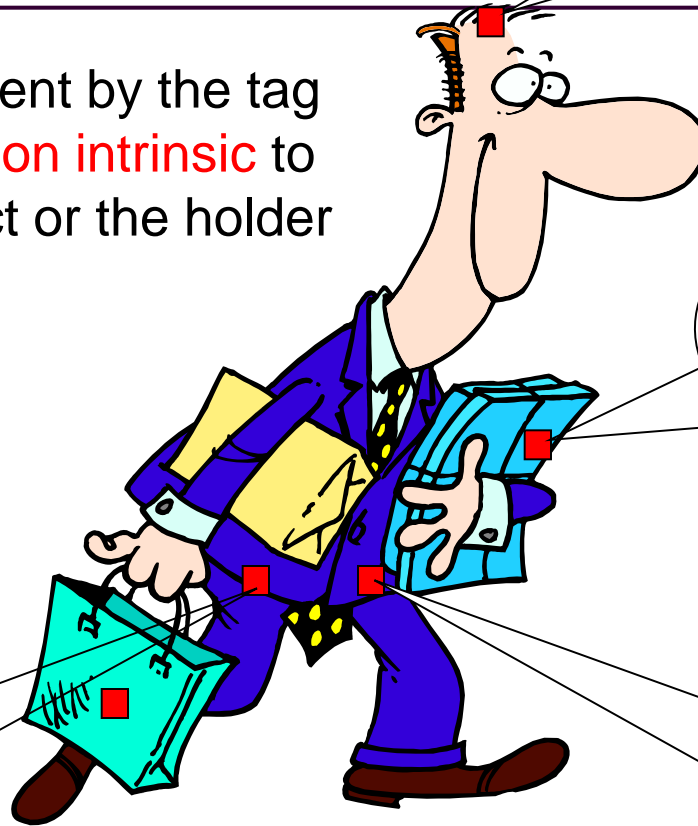
# Classification

---

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

# Meaningful by Itself

When the data sent by the tag **reveals information intrinsic** to the tagged object or the holder of the object.



Wig model #4456  
(cheap polyester)

Das Kapital and  
Communist-party  
handbook

Transportation  
valid. 22/09/10, 9:04am  
Line 4 Station  
Churchill

Passport 04BC44487  
Mr. John Smith  
Born on 27 Sept. 68

Famous picture by Ari Juels, RSA Labs.  
Text modified to fit this presentation.

# Meaningful when Associated to a Database



# Why Dealing with this Issue?

---

- **Economical.**
  - Required by the customers and activists.
  - Liability due to personal data theft.
  - Incentive to not kill the tag.
  
- **Legal.**
  - EU and national regulations.
  - Privacy-related laws.

# 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.”

# 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.

# Information Leakage: Interests

- Attacker Interest: **medium**.
- Customer Interest: **high**.
- Academia Interest: **low**.
  - More an engineering problem than a research problem.
- Industry interest: **medium**.
  - Ex: public transportation.

# Malicious Traceability

# Definition and Palliative Solutions

---

- An adversary should not be able to track a tag holder, ie, he should not be able to **link two interactions tag/reader**.
- 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.
- Blocker tags, RFID Guardian.

# 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”

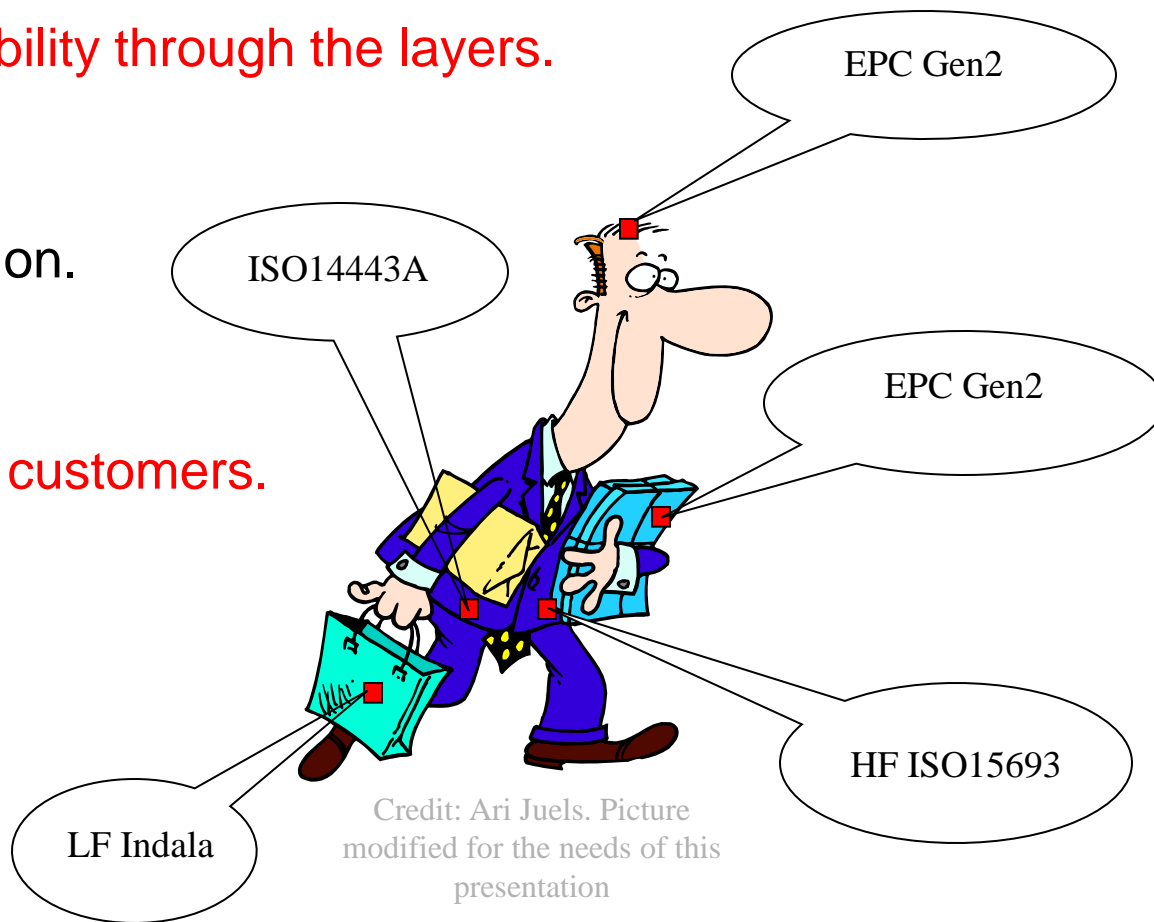
In Privacy Guidelines for RFID Information Systems available on the web site <http://www.ipc.on.ca>.

# Impossibility of Avoiding Traceability

- Malicious traceability through the layers.

- Application.
- Communication.
- Physical.

- Fingerprinting of customers.



Credit: Ari Juels. Picture modified for the needs of this presentation

# Malicious Traceability: Interests

- Attacker Interest: **low**.
- Customer Interest: **medium**.
- Academia Interest: **high**.
  - Some funny challenges. Open problem.
  - Mitigate the problem.
- Industry interest: **low**.

# Conclusion

# Conclusion (1/2)

- **2002-2004:** Discovery age of RFID Security.
  - About 35 papers.
  - Privacy.
- **2005-2010:** Pedestrian approach of RFID Security.
  - About 450 papers. (how many valuable?)
  - **Privacy**, Reader complexity, **Lightweight building blocks** (mostly symmetric), Distance bounding, Models.
  - Focus on Tag-Reader communication.
  - Practical attacks (TI, Mifare, Keyloq,...)

# Conclusion (2/2)

- **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.
  - Compromised readers (restore security a posteriori)
  - Privacy certification.
    - Considering the whole system.
    - Not looking for the “perfect” security.

# RFID Security: A Large Body of Literature



<http://sites.uclouvain.be/security/>  
[Gildas.avoine@uclouvain.be](mailto:Gildas.avoine@uclouvain.be)