Privacy Challenges in RFID

Gildas Avoine

Information Security Group
Université catholique de Louvain
Belgium

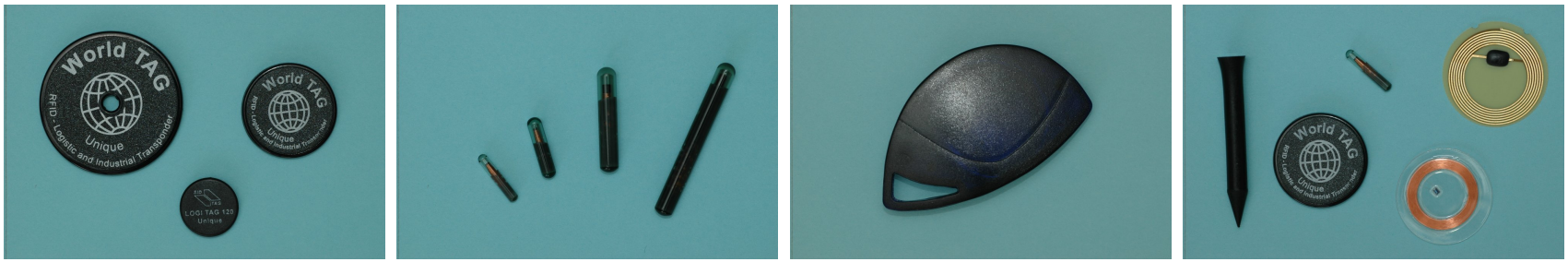
SUMMARY

- Background about RFID
- Privacy: Information Leakage
- Privacy: Malicious Traceability
- Is Privacy a Research Challenge?

BACKGROUND ABOUT RFID

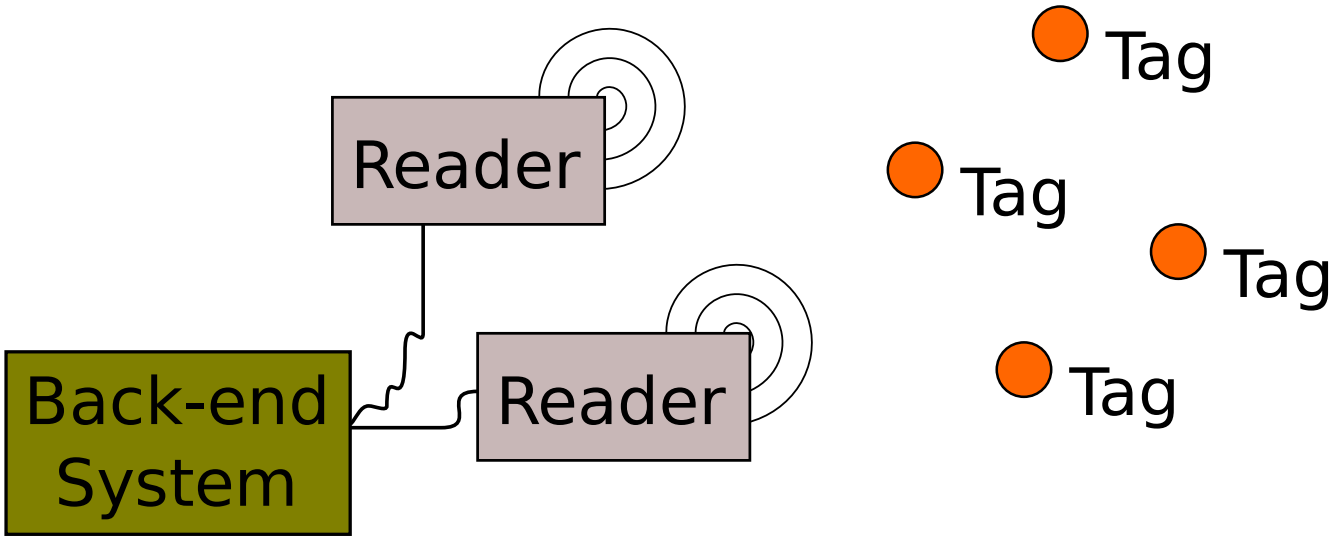
- Background about RFID
- Privacy: Information Leakage
- Privacy: Malicious Traceability
- Is Privacy a Research Challenge?

- Radio Frequency IDentification (RFID) consists in remotely retrieving datas (identifier and potentially additional datas) using devices called RFID tags.
- An RFID tag contain a microcircuit (chip) and an antenna to enable it to receive and respond to radio-frequency queries from an RFID reader/writer.
- An RFID tag can be a low-capability device e.g. for pet identification, but also a powerful contactless smartcard e.g. for biometric passports.

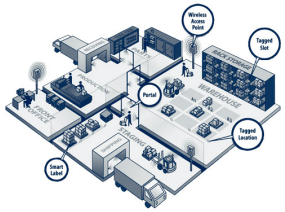


Credit: Gildas Avoine

Architecture



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



www.aeroid.co.uk

- Libraries.
  - Improve book borrowing and inventories.

www.rfid-library.com

- Pet identification.
  - Replace tattoos by electronic ones.
  - ISO11784, ISO11785.

www.flickr.com

- Localisation.
  - Children in amusement parks, Elderly people.
  - Counting cattle.

www.safetzone.com

- Building access control.
  - Eg. UCL, MIT.
- Automobile ignition key.
  - Eg. TI DST, Keeloq.
- Public transportation.
  - Eg. Brussels, Boston, Paris, ..., Thalys.
- Payment.
  - Eg. Visa, Baja Beach Club.
- Electronic documents.
  - Eg. ePassports.
- Loyalty cards.

Credit: G. Avoine

Credit: G. Avoine

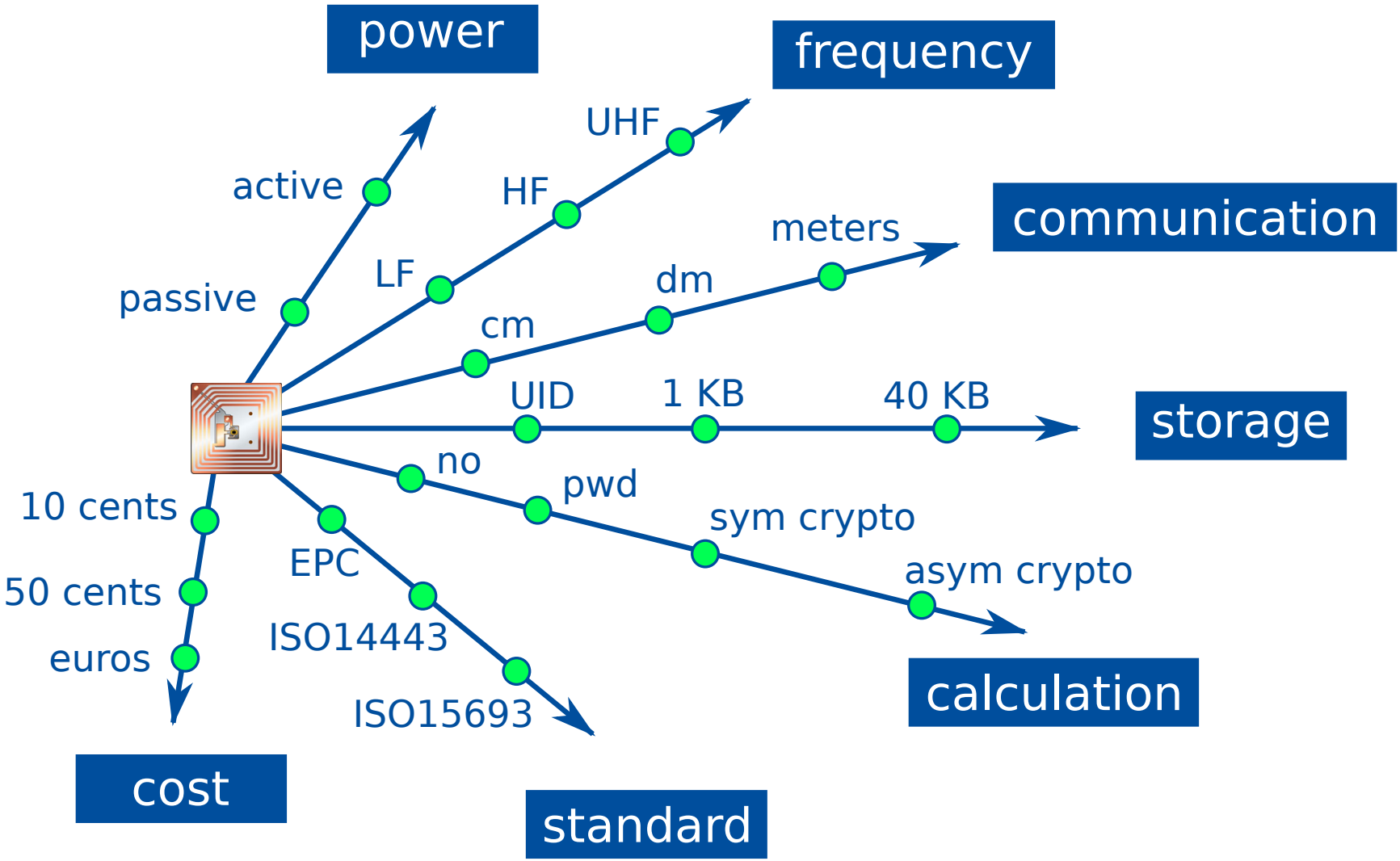
www.carthiefstoppers.com

www.brusselnieuws.be

blogs.e-rockford.com

www.bajabeach.es

Tag Characteristics



Security Specificities

- Low capabilities.
- Wireless.
- Ubiquity.
- Fast authentication.

Security Threats Classification

- Security.
  - Impersonation.
  - Denial of service.
- Privacy.
  - Information leakage.
  - Malicious traceability.

Research fields about RFID Privacy

http://www.avoine.net/rfid/

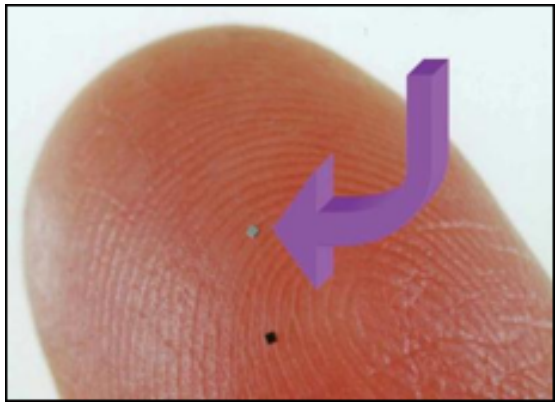
- Privacy models.
- Untraceable (lightweight) protocols.
- Untraceable (scalable) protocols.
- Counterfeiting.
- Grouping Proof.
- Ownership transfer.
- Applications: ePassport, pacemakers, etc.

PRIVACY: INFORMATION LEAKAGE

- Background about RFID
- Privacy: Information Leakage
- Privacy: Malicious Traceability
- Is Privacy a Research Challenge?

Importance of Avoiding Traceability
Other Technologies

- 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.



Importance of Avoiding Traceability
Liberty Rights Organizations

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

European Commission

- 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.

- Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of security and privacy by design).

  [Viviane Reding, EC Recommendation, 12.5.2009]

Importance of Avoiding Traceability
Anne Cavioukan

- "Privacy and Security must be built in from the outset, at the design Stage".

  [Privacy Guidelines for RFID Information Systems, 2006, Anne Cavioukan, Information and Privacy Commissioner of Ontario]

- Kill-command (Eg.: EPC Gen 2 requires a 32-bit kill command.)
- Faraday cages.
- Blocker tags.
- Bill of Rights.

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.).

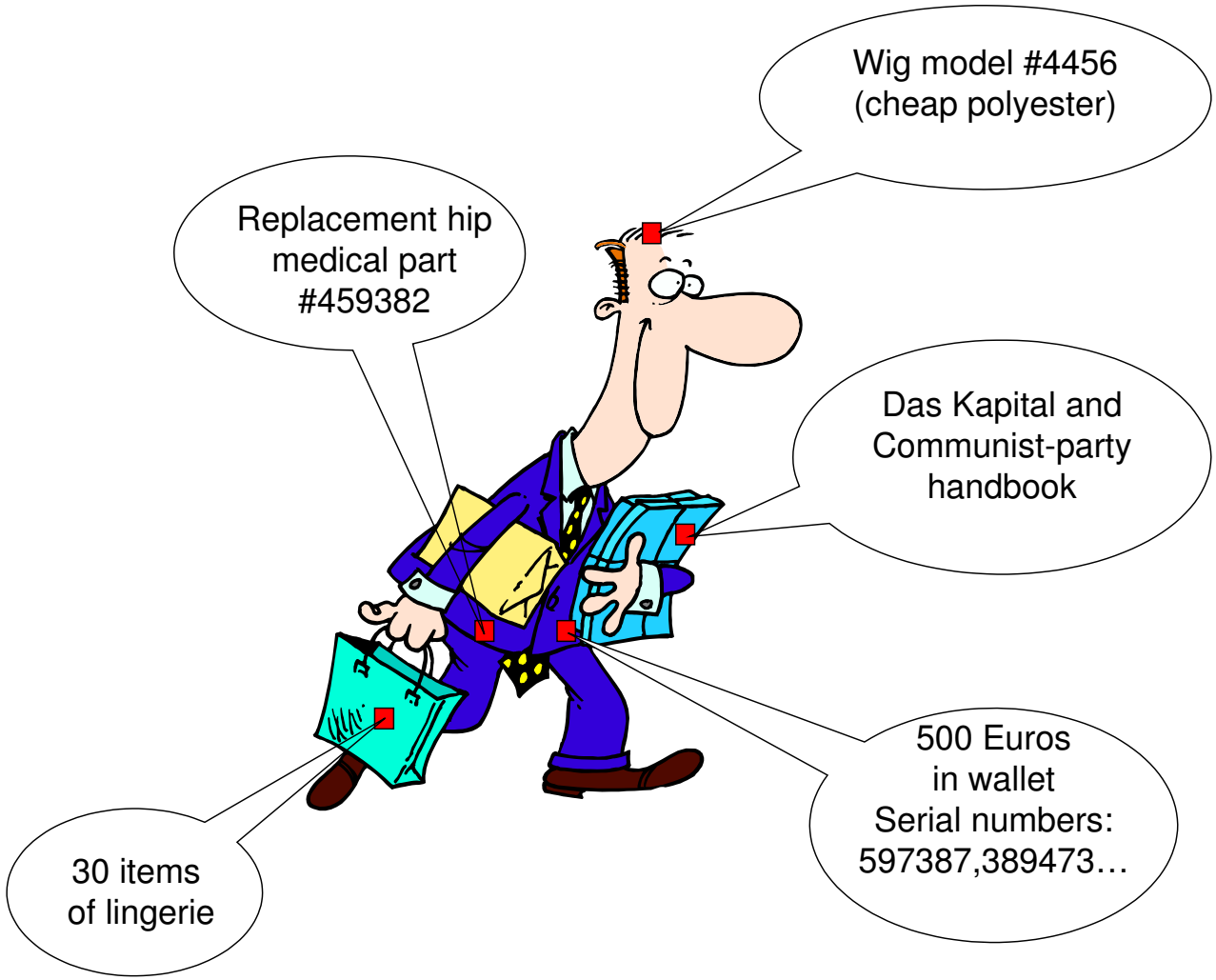
Classification

- Information meaningful by itself.
- Information meaningful with the database.

Information Meaningful by Itself
Typical Examples

- 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 be the US. Food and Drug Administration.
  - E-documents (passports, ID cards, etc.).
  - Loyalty cards, Public transportation passes.

Information Meaningful by Itself
Ari Juels's Famous Picture



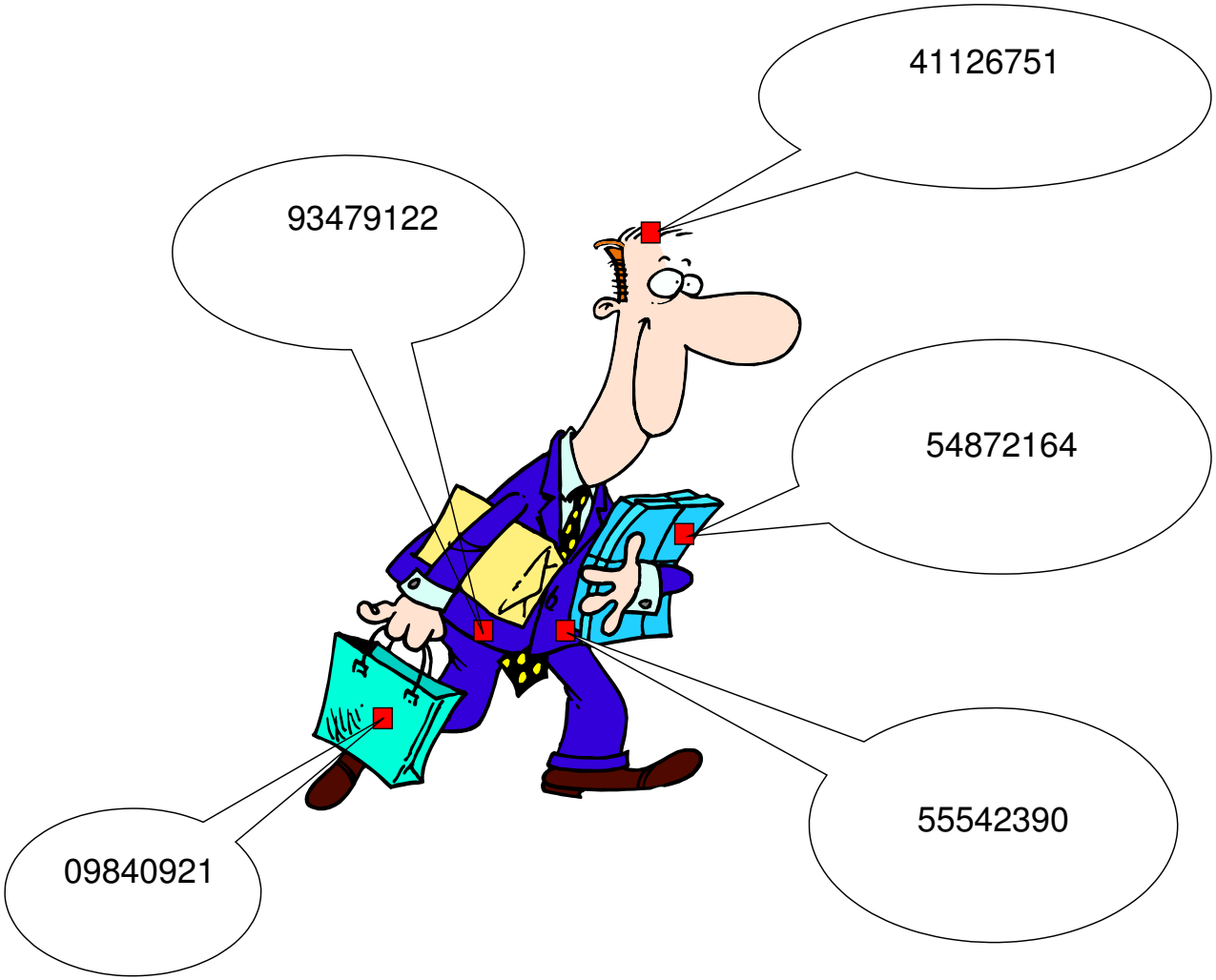
Credit: Ari Juels

Information Meaningful by Itself
Public Transportation: MOBIB Card in Brussels

- MOBIB card (RFID) launched in Brussels in 2008.
- Before getting in a subway, bus or tram, customers are required to show up their MOBIB card in front of a validator.
- MOBIB is 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: name, birthdate, zipcode.
- Information about 3 last validations: date, time, bus line, bus stop, subway station, ...

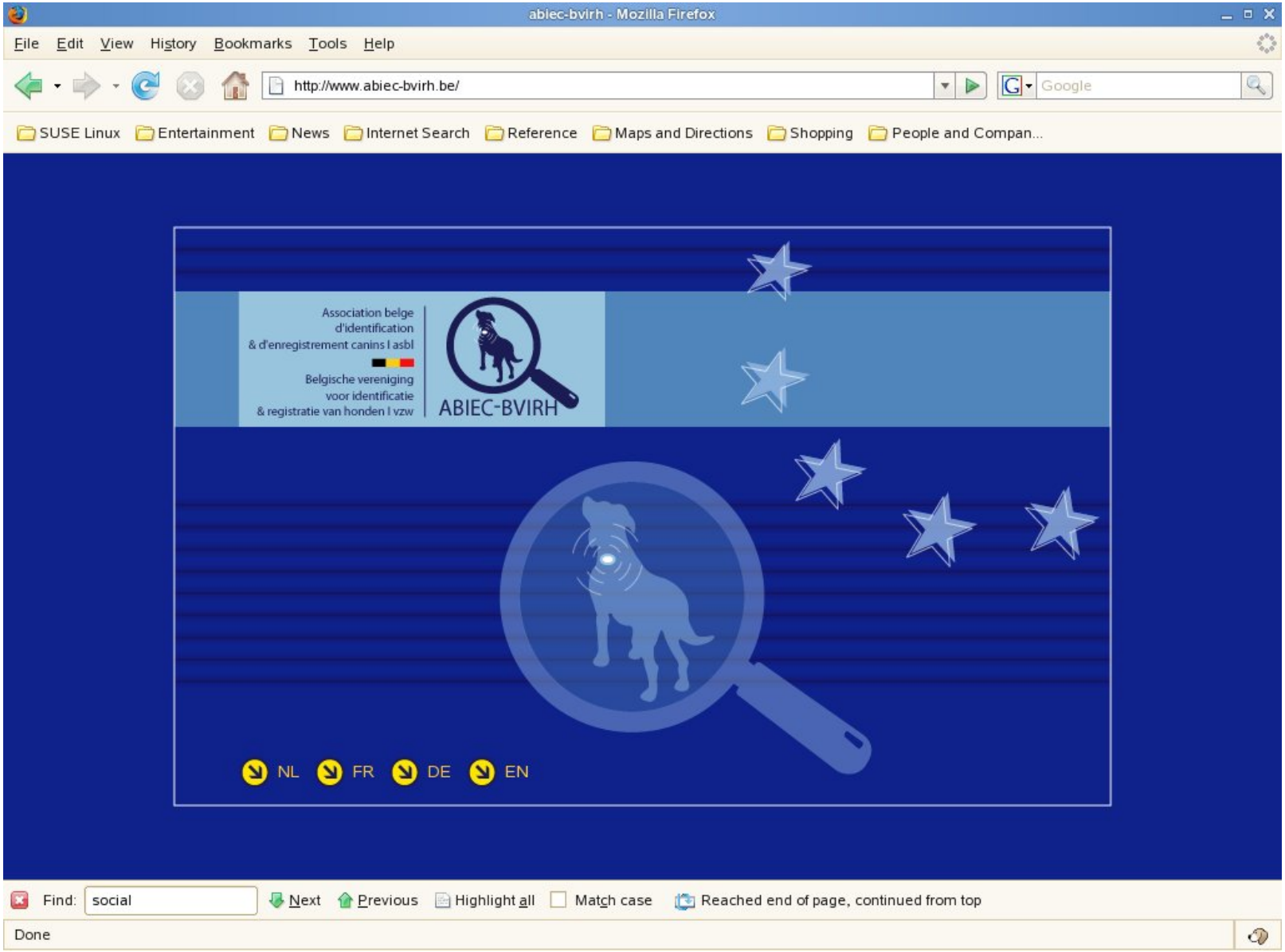
Information Meaningful with a Database

Ari Juels's Famous Picture



Credit: Inspired by Ari Juels

Information Meaningful with a Database
ABIEC Information Leakage



PRIVACY: MALICIOUS TRACEABILITY

- Background about RFID
- Privacy: Information Leakage
- Privacy: Malicious Traceability
- Is Privacy a Research Challenge?

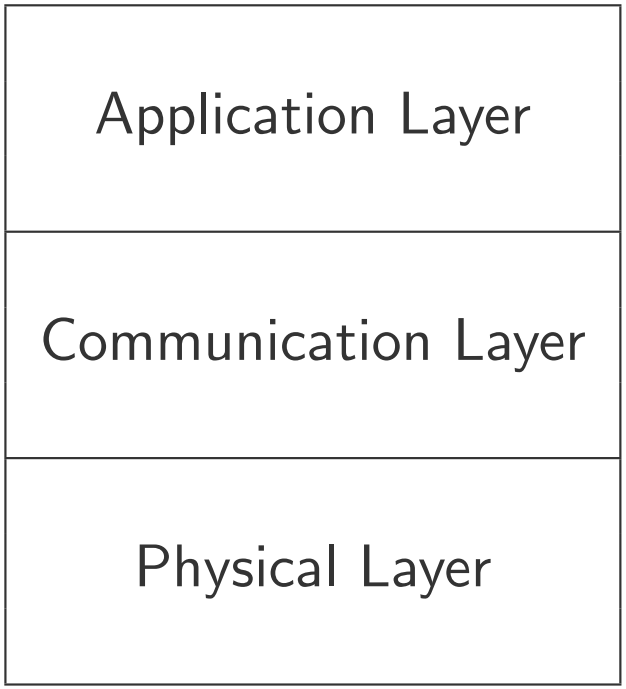
Privacy: Malicious Traceability
Informal Definition

- An adversary should not be able to track a tag holder, ie. he should not be able to link two interactions tag/reader.
- Eg. tracking of employees by the boss, tracking of children in an amusement park, tracking of military troops, etc.

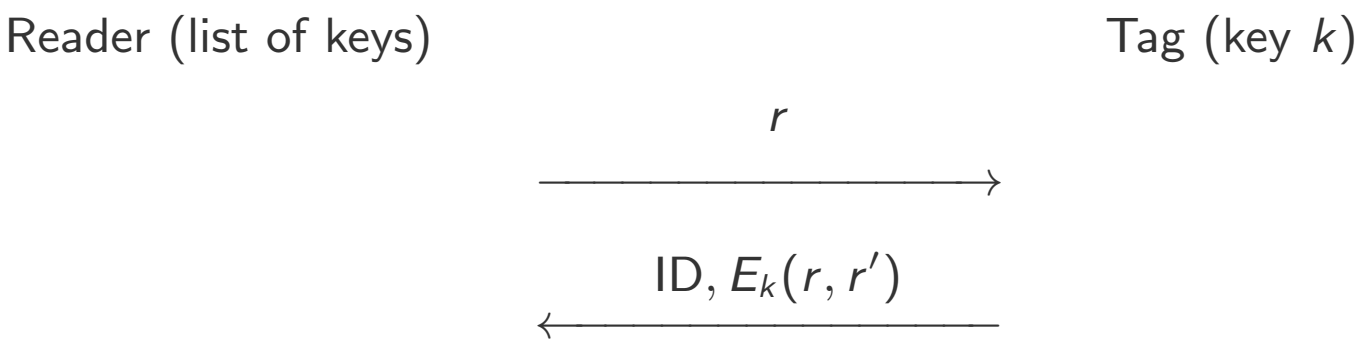
Privacy: Malicious Traceability
Tracking through the Layers

- 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.

Privacy: Malicious Traceability
Traceability Through the Layers



- Authentication / Identification.
- Collision-avoidance.
- Radio fingerprints.
- Diversity of standards.



- This protocol is not privacy-friendly because the ID is revealed.
- CR protocols avoiding malicious traceability do not scale well.
  - Authenticating one tag requires $O(n)$ operations.

Privacy: Malicious Traceability
Summary

- 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.

IS PRIVACY A RESEARCH CHALLENGE?

- Background about RFID
- Privacy: Information Leakage
- Privacy: Malicious Traceability
- Is Privacy a Research Challenge?

Research Challenge

- There are clearly privacy issues in RFID systems
- Is privacy still a meaningful concept nowadays?
- We already lost the control of our privacy.
- People no longer care about privacy (vote...)
- There is no business model behind privacy.
- We could have privacy if it was free.
- Privacy never comes for free.
- All existing works on RFID privacy are practically useless.
- Consider privacy with a larger view.
- Do not try to get the best.
- Find some metrics to privacy.
- Enforce privacy using certifications.

http://sites.uclouvain.be/security/
gildas.avoine@uclouvain.be