

RFID Security and Privacy

Gildas Avoine

Information Security Group
UCL Belgium

February 2011, Coruña, Spain



UCL
Université
catholique
de Louvain



INFORMATION
SECURITY
GROUP

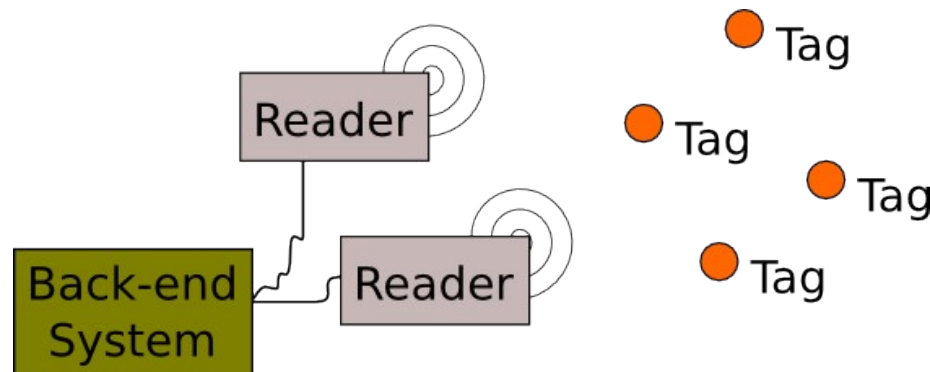
RFID Primer

RFID Primer

Definition

- “Radio frequency identification” (RFID) means the use of electromagnetic radiating **waves** or reactive field coupling in the radio frequency portion of the spectrum **to communicate to or from a tag** through a variety of modulation and encoding schemes **to uniquely read the identity** of a radio frequency tag **or other data stored on it.**”

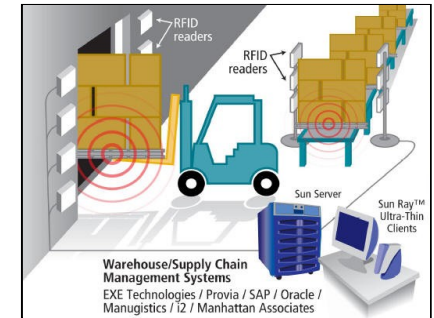
[European Commission Recommendation, 12.5.2009]



RFID Primer

Examples: Basic RFID Applications

- **Supply chain.**
 - Track boxes, palettes, etc.
 - Eg: EPC Global Inc.
- **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

RFID Primer

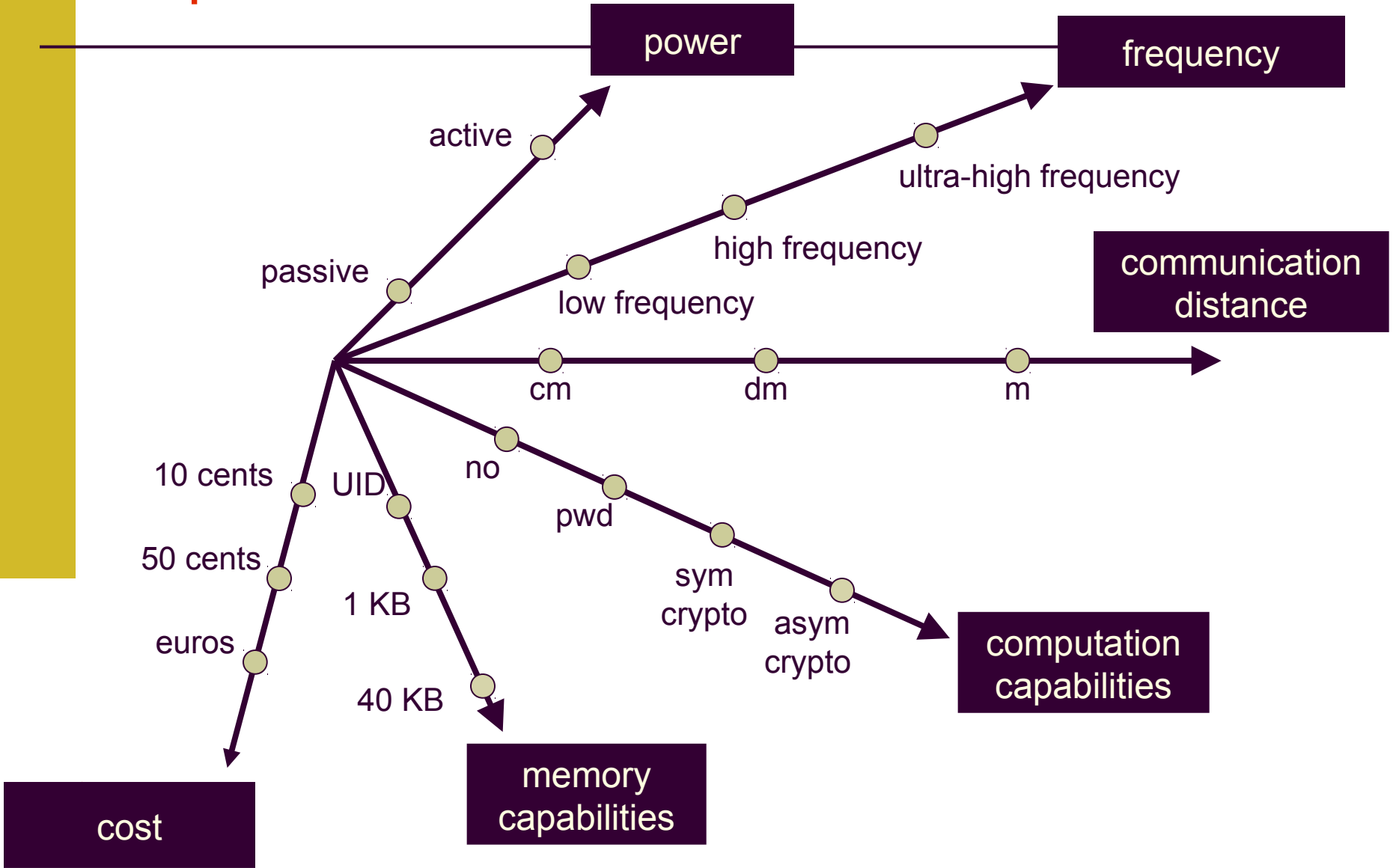
Examples: Evolved RFID Applications

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



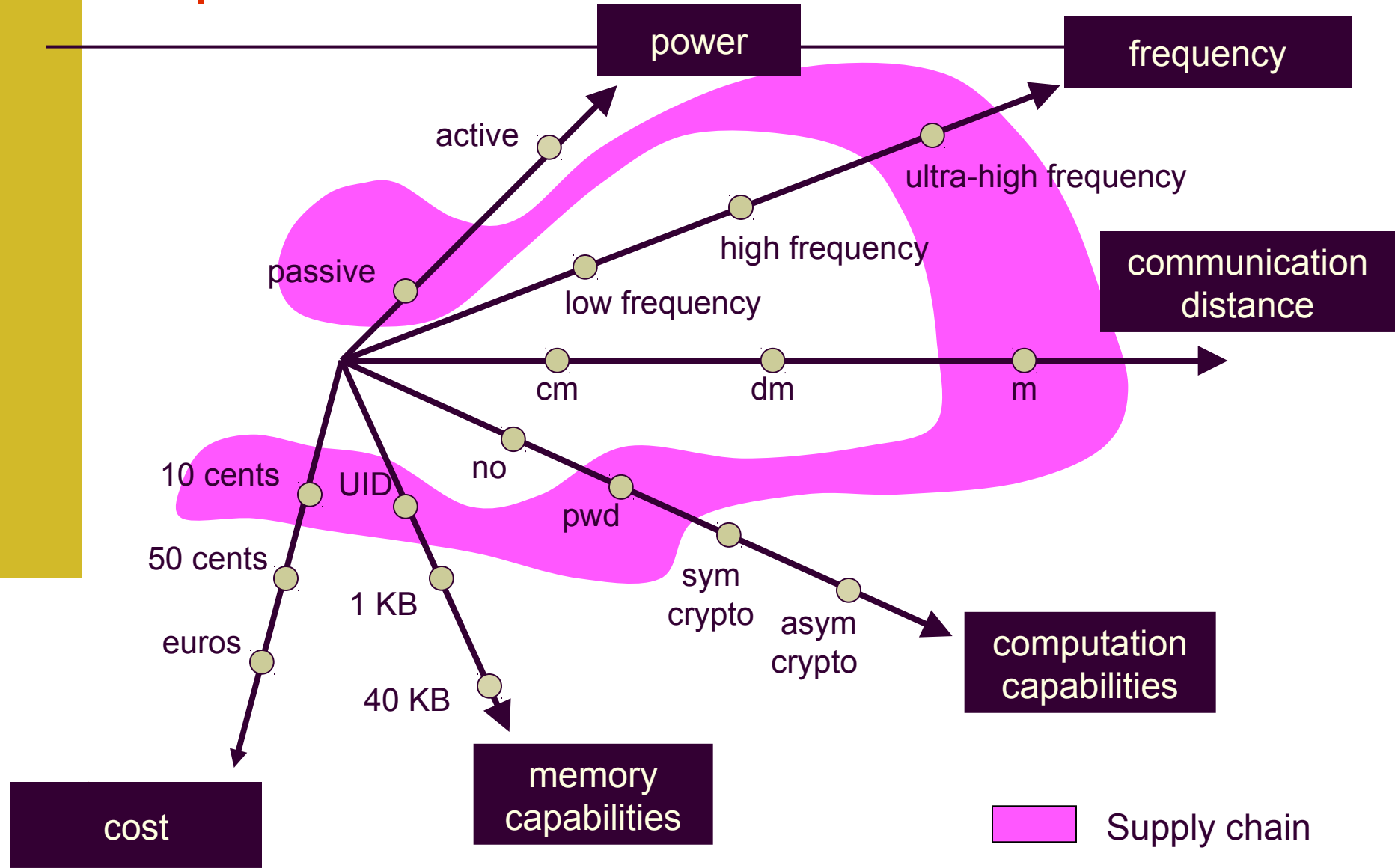
RFID Primer

Capabilities



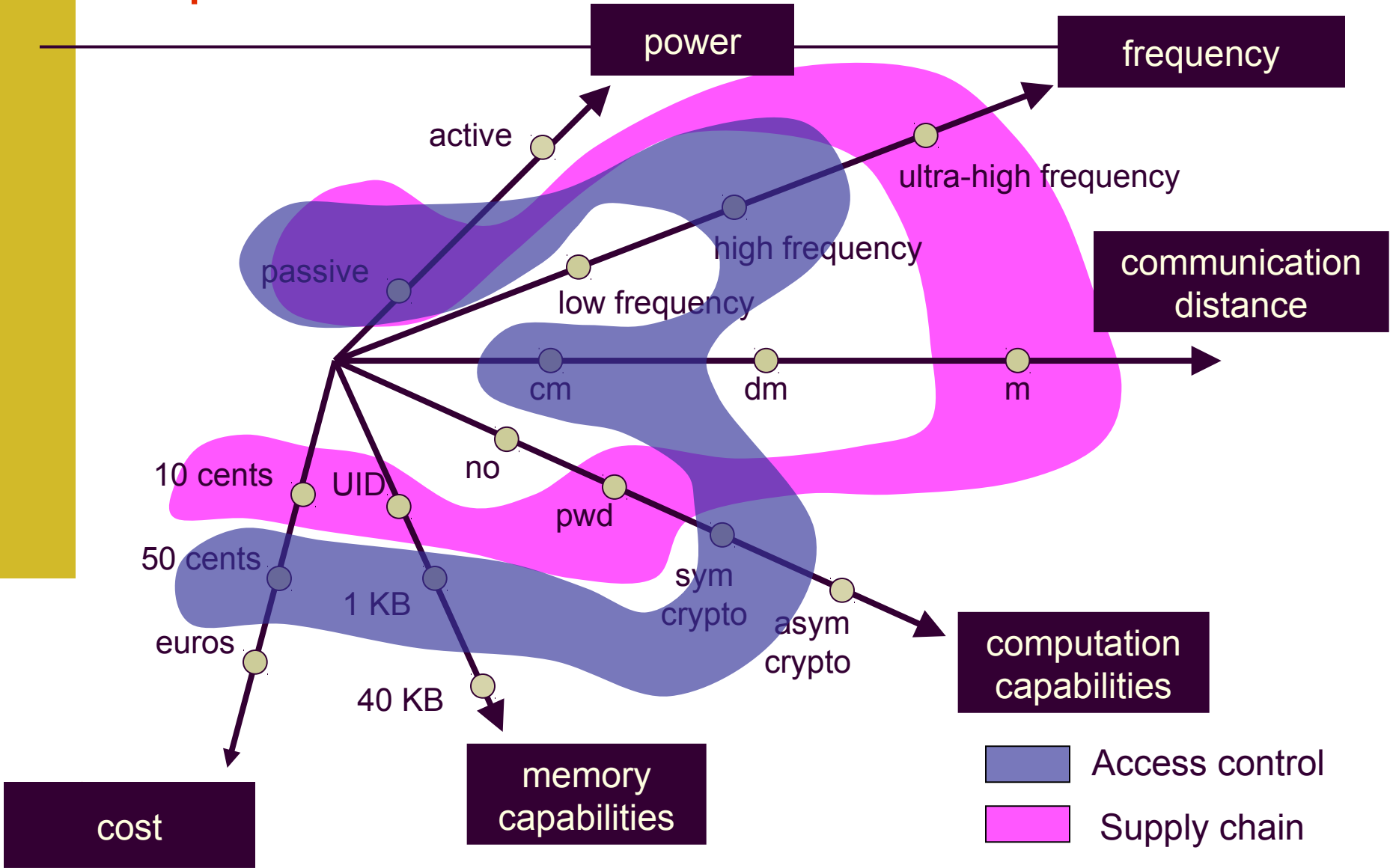
RFID Primer

Capabilities



RFID Primer

Capabilities



RFID Primer

Looking Inside



Source : jp.digikey.com

RFID Primer

Looking Inside



Source : jp.digikey.com

Who would be able to read this tag
(by the end of this talk)?

RFID Primer

Looking Inside



Source : jp.digikey.com



Source : www.sirlepaper.com

RFID Primer

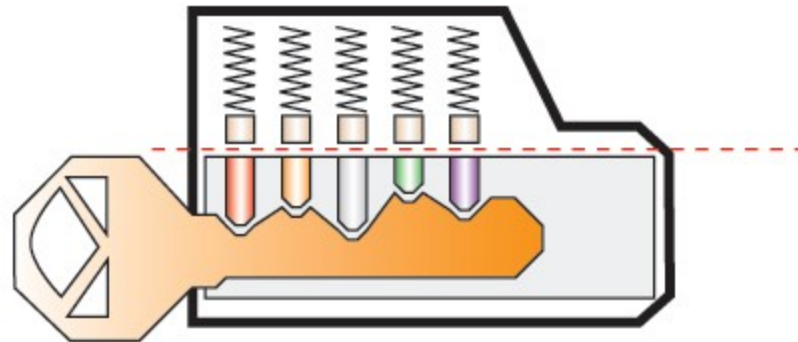
Looking Inside



Source : jp.digikey.com



Source : www.sirlepaper.com



Source : lirent.net

RFID Primer

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.



RFID Primer

Security Threat Classification

Impersonation

Information Leakage

Impersonation

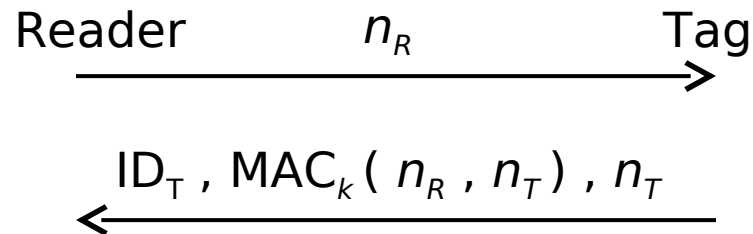
Impersonation

Several Approaches

- **Impersonation:** A fake tag is authenticated as a genuine one.
- Three **approaches** to impersonate a tag.
 - Clone a genuine tag.
 - Modified a genuine tag.
 - Create a fake tag from scratch.
- **Examples:**
 - Clone an access control card.
 - Modify your mass transportation pass.
 - Create a fake passport.

Impersonation Authentication Protocol

- **Authentication** can be done using:
 - A symmetric cipher, a keyed-hash function, a public-key cipher, a signature scheme, or a devoted authentication protocol.
- Example: Challenge-Response Protocol.
 - **ISO 9798-4** defines authentication protocols based on a MAC.



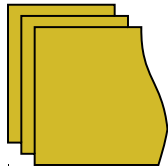
- We know how to design a **secure authentication** scheme.

Impersonation

Weaknesses

- **Cost** of the solution.
 - Require lightweight algorithms (wired logic).
- **Implementation** issues.
 - Both sides: readers and tags.
 - Miss-understanding of the standards.
- **Architecture** of the solution.
 - Building blocks are not enough: the whole solution must be secure.

Impersonation

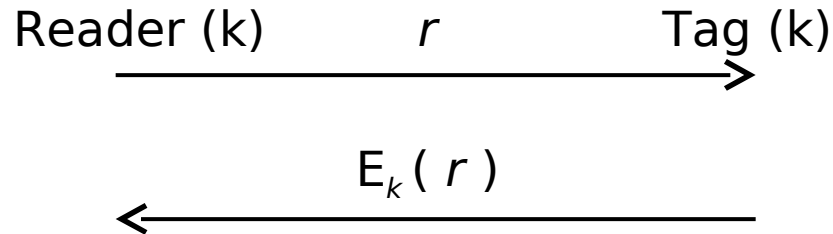


Attack on TI DST

- **TI**: Texas Instruments.
- **DST**: Digital Signature Transponder.
- More than **100 million** DST modules sold around the world.
- Car ignition key (eg. Ford) and payment cards.

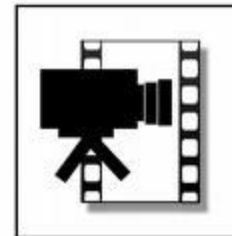
Impersonation

Video: Texas Instrument DST



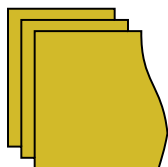
Adversary goal: retrieve the secret k in order to make a clone.

1. Query once the car's key (tag inside).
2. Try all the possible keys k until finding the one that correctly decipher $E_k(r)$. $|k| = 40$ bits. E revealed.
3. Steal the car simulating the car's key.



Impersonation

Attack on NXP Mifare Classic



Attack on Mifare Classic

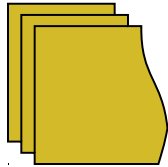
- Philips Semiconductors (NXP) introduced the **Mifare** commercial denomination (1994) that includes the **Mifare Classic** product.
- **Applications**: public transportation, access control, ticketing...
- **Memory read & write access are protected** by some keys.
- Several **100 million** Mifare Classic tags sold up to now.

Bad Example: NXP Mifare Classic

- Several attacks in 2008, Hoepman, Garcia, de Koning Gans, et al. reverse-engineered the cipher **Crypto1**: every **Mifare Classic tag broken** in a few minutes.

Impersonation

Relay Attacks



Relay Attacks

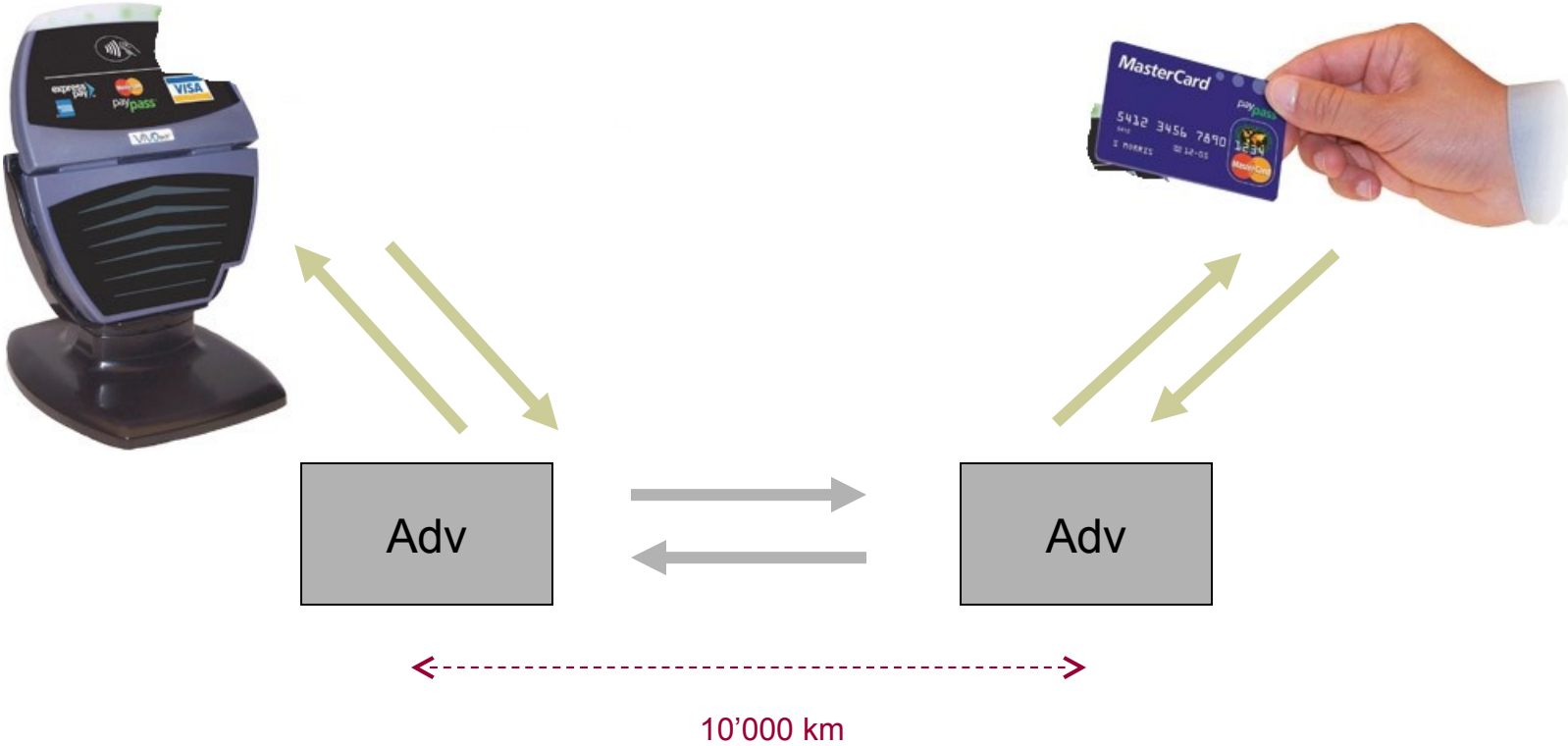
Impersonation Relay Attacks



Impersonation Relay Attacks



Impersonation Relay Attacks



Impersonation

Relay Attacks: Timing

- Reader **starts a timer** when sending a message.
 - To avoid half-opened connections.
- ISO **14443** “Proximity Cards”.
 - Used in most **secure** applications.
 - Default timer is around **4 ms**.
 - Tag can require more time, **up to...**

Impersonation

Relay Attacks: Feasibility

- Radio link over 50 meters (G. Hancke 05).
- With some locally-connected ACR122 (A. Laurie 09).
- With Nokia cell phones (A. Laurie 10).
- Over Internet (libNFC 10).



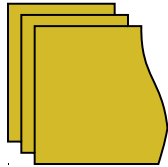
Information Leakage

Information Leakage

Classification

- **Information leakage**: some personal information is revealed without the person's agreement (belongs to **privacy**).
- Information **meaningful by itself**.
- Information meaningful when **associated with a database**.

Information Leakage



Information meaningful by itself

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

Information Leakage

Information Meaningful by Itself

Top-priced Wig



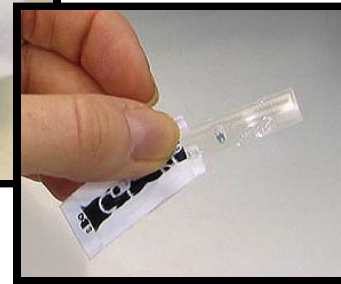
Viagra

Credit : Ari Juels (modified image to fit this presentation)

Information Leakage

Information Meaningful by Itself

Top-priced Wig

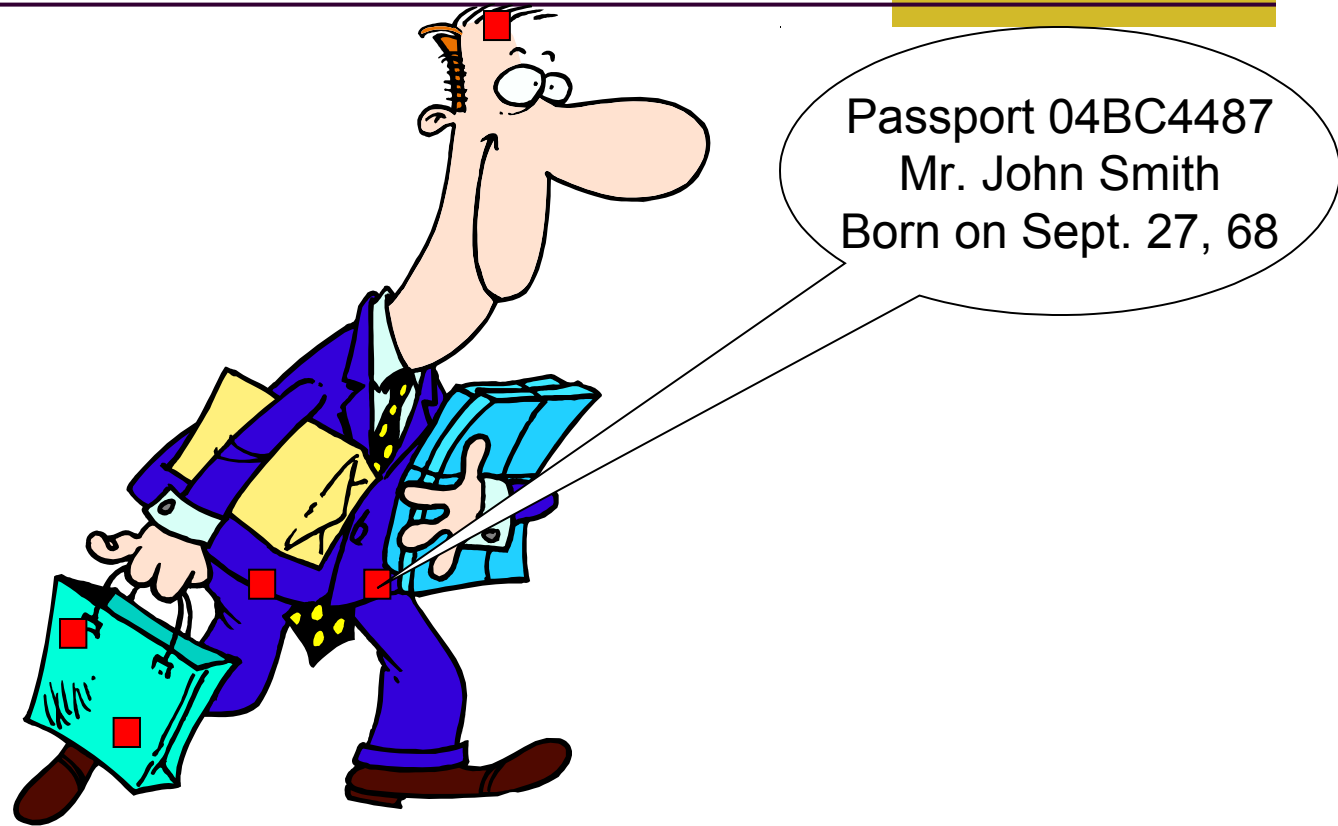


Viagra

Credit : Ari Juels (modified image to fit this presentation)

Information Leakage

Information Meaningful by Itself



Credit : Ari Juels (modified image to fit this presentation)

Information Leakage

Information Meaningful by Itself



Subway
22/09/10, 9:04am
Line 4
Stop Coruña
Train Station

Credit : Ari Juels (modified image to fit this presentation)

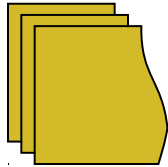
Information Leakage

Information Meaningless by Itself



Credit : Ari Juels (modified image to fit this presentation)

Information Leakage



Information meaningful when associated to a database

Information Leakage

Information meaningful when associated to a database



Credit : Ari Juels (modified image to fit this presentation)

Information Leakage

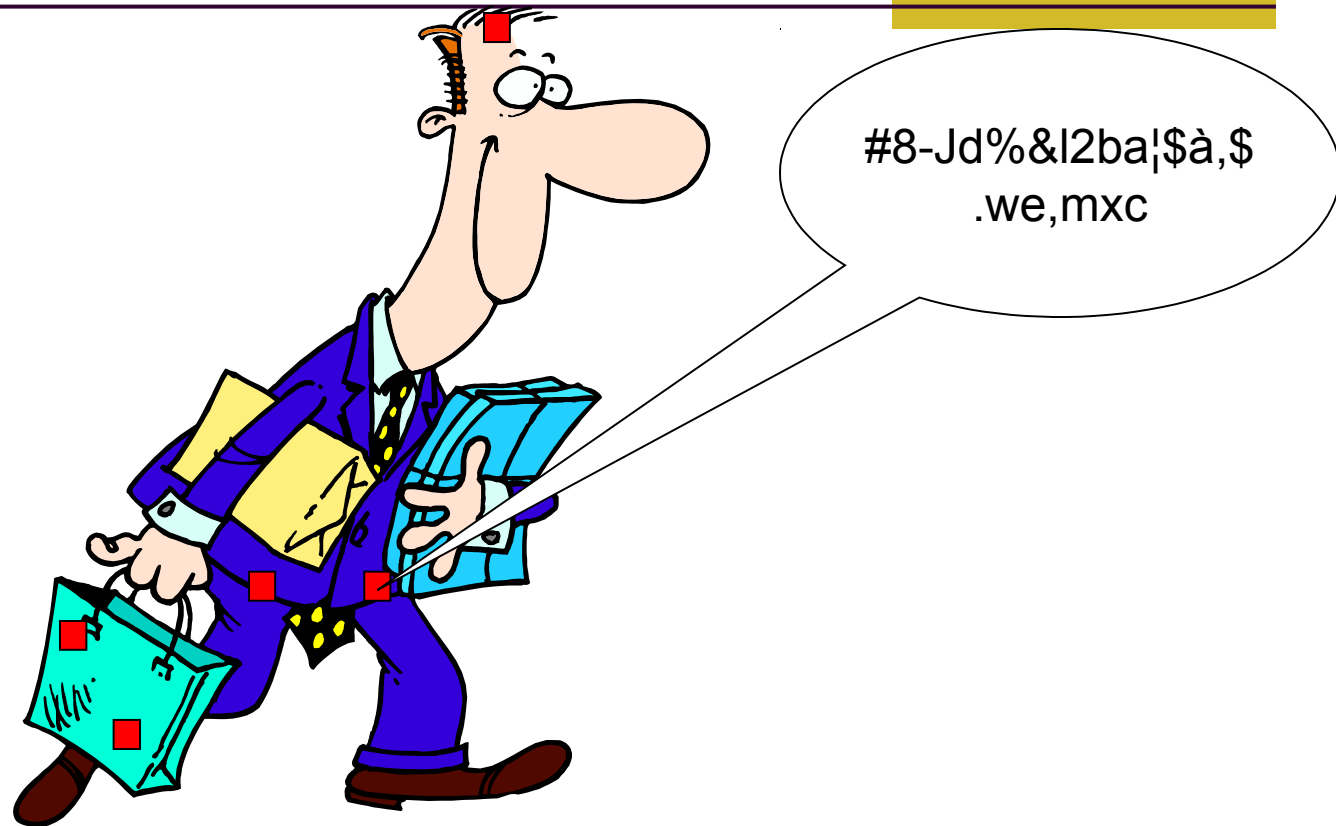
Why should Manufacturers Deal with this Issue?

- **Economical.**
 - Required by the customers and activists.
 - Liability due to personal data theft.
 - Incentive not to kill the tag.

- **Legal.**
 - EU and national regulations.
 - Privacy-related laws.

Information Leakage

Encryption of the data



Credit : Ari Juels (modified image to fit this presentation)

Information Leakage

Require authentication before delivering data



Credit : Ari Juels (modified image to fit this presentation)

Conclusion

Conclusion

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.
- Blocker tags, RFID Guardian.

Conclusion

Privacy and Security from the Outset

- 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]

Conclusion

Reasons of Information Leakage

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

Conclusion

What about the Future?

- **Building blocks** available in the tags are more secure in recent products (lightweight implementation of standardized algorithms)
- Secure building blocks do not make themselves secure applications.
 - The security of the **whole** application must be considered.
 - Many **SMEs** involved in RFID.

Conclusion

RFID Security: A Large Body of Literature



The screenshot shows a Mozilla Firefox browser window displaying the website <http://www.avoine.net/rfid/>. The page is titled "Information Security Group" and is part of the "RFID Lounge Security & Privacy" section. The website header includes the GSI logo and navigation links: Home, People, Research, Publications, Press, Industry, Our Labs, and RFID Lounge. The main content area features a "RFID MENU" with links to Articles, Books, and Mailing list. A text block describes the lounge's purpose and provides contact information for Gildas Avoine. A list of articles is visible, including one from 2009 by Denis Trček and Pekka Jäppinen. The footer contains the address: Place Saint Barbe, 2, Building Réaumur, B-1348 Louvain-la-Neuve, Belgium.

[http://sites.uclouvain.be/security/
gildas.avoine@uclouvain.be](http://sites.uclouvain.be/security/gildas.avoine@uclouvain.be)