Cybersecurity in IoT devices

Antoni Martínez Ballesté
Universitat Rovira i Virgili

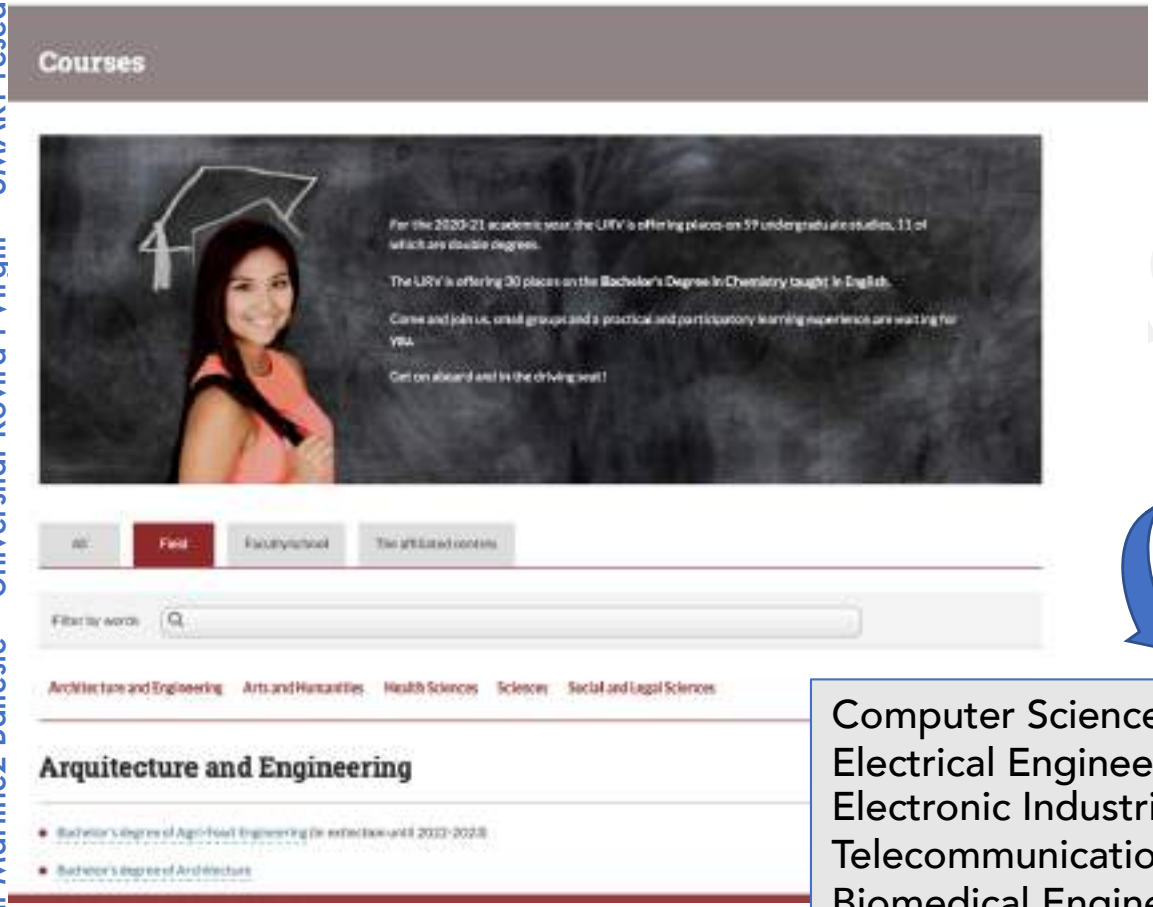
smart technologies
research group

UNIVERSITAT ROVIRA i VIRGILI

LA URV A CATALUNYA

UNIVERSITAT ROVIRA i VIRGILI
C/ de l'Escorxador, s/n
43003 Tarragona
Tel. +34 977 55 80 00
info@urv.cat
www.urv.cat
twitter.com/universitatURV
facebook.com/universitatroviravirgili
linkedin.com/company/universitat-rovira-i-virgili
youtube.com/canalURV

UNIVERSITAT ROVIRA i VIRGILI



- Arts and Humanities
- Health Sciences
- Sciences
- Social and Legal Sciences
- Architecture and Engineering

Computer Science and Engineering
Electrical Engineering
Electronic Industrial and Automatic Engineering
Telecommunications Systems and Services Engineering
Biomedical Engineering

smart technologies research group

UNIVERSITAT ROVIRA i VIRGILI

LA URV EN XIFRES

14.041	ESTUDIANTS DE GRAU, MÀSTER I DOCTORAT 2018-19	**1.174**	PERSONAL DOCENT I INVESTIGADOR (EJC) 2018	**1.399**	PUBLICACIONS WOS/SCOPUS 2018
34%	ESTUDIANTS INTERNACIONALS DE MÀSTER I DOCTORAT 2018-19	**486**	PERSONAL DOCENT I INVESTIGADOR PERMANENT 2018	**51%**	PUBLICACIONS EN REVISTES DEL PRIMER QUARTIL 2018
4.168	ESTUDIANTS DE FORMACIÓ PERMANENT 2018	**717**	PERSONAL D'ADMINISTRACIÓ I SERVEIS 2018	**110,7**	PRESSUPOST (M€) (2019)

(EJC): Equivalents a jornada completa.

smart technologies research group

- IoT, technology and computer science applied to health and quality of life.
- Analysis of information systems in health services and critical infrastructures.
- Security and privacy of health related technologies.

http://www.smarttechresearch.com

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

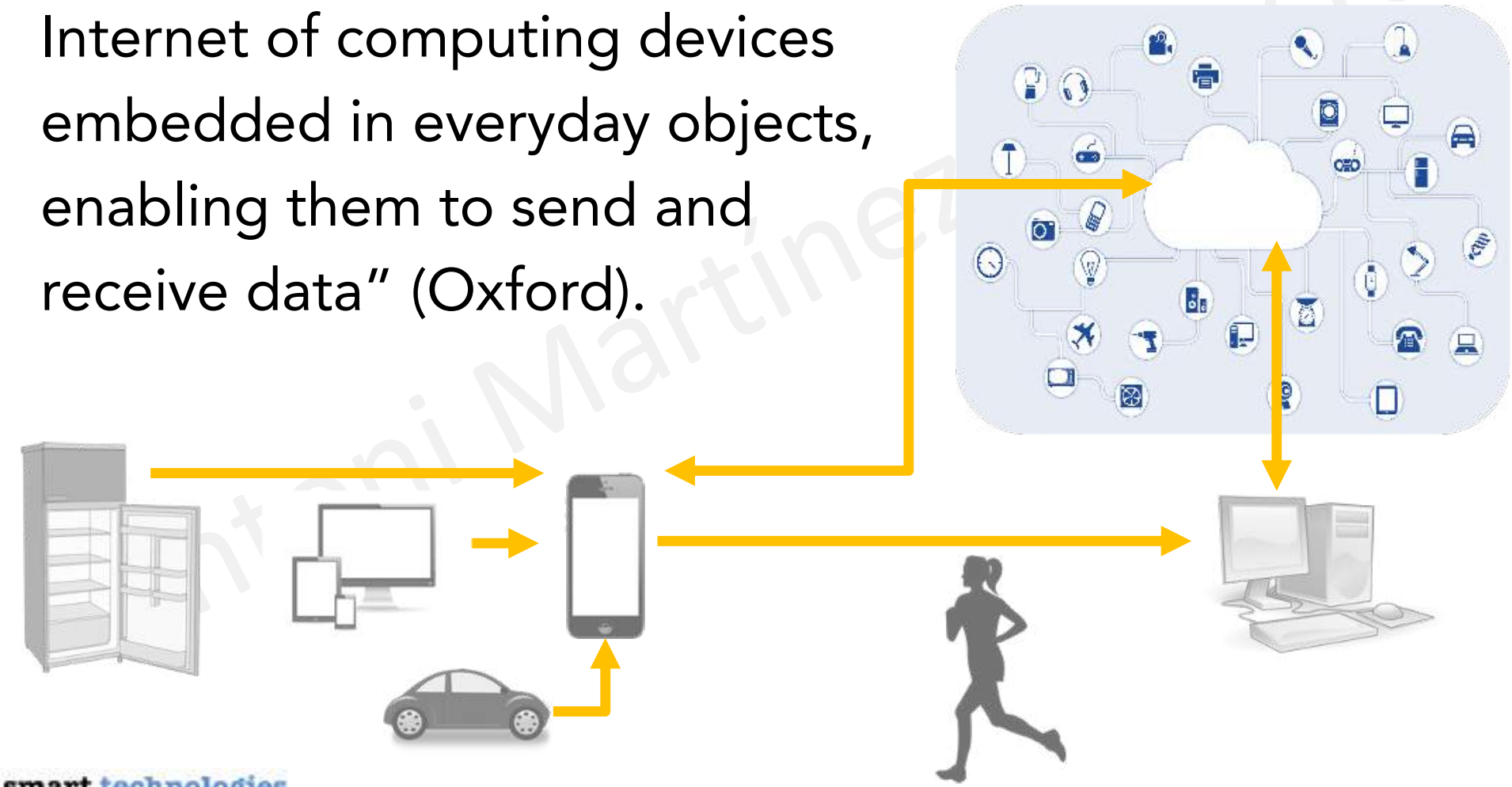
Content

- The Internet of Things
- Some real threats
- How to address cybersecurity
- IoT under attack
- People and society
- Guidelines

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

- "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data" (Oxford).



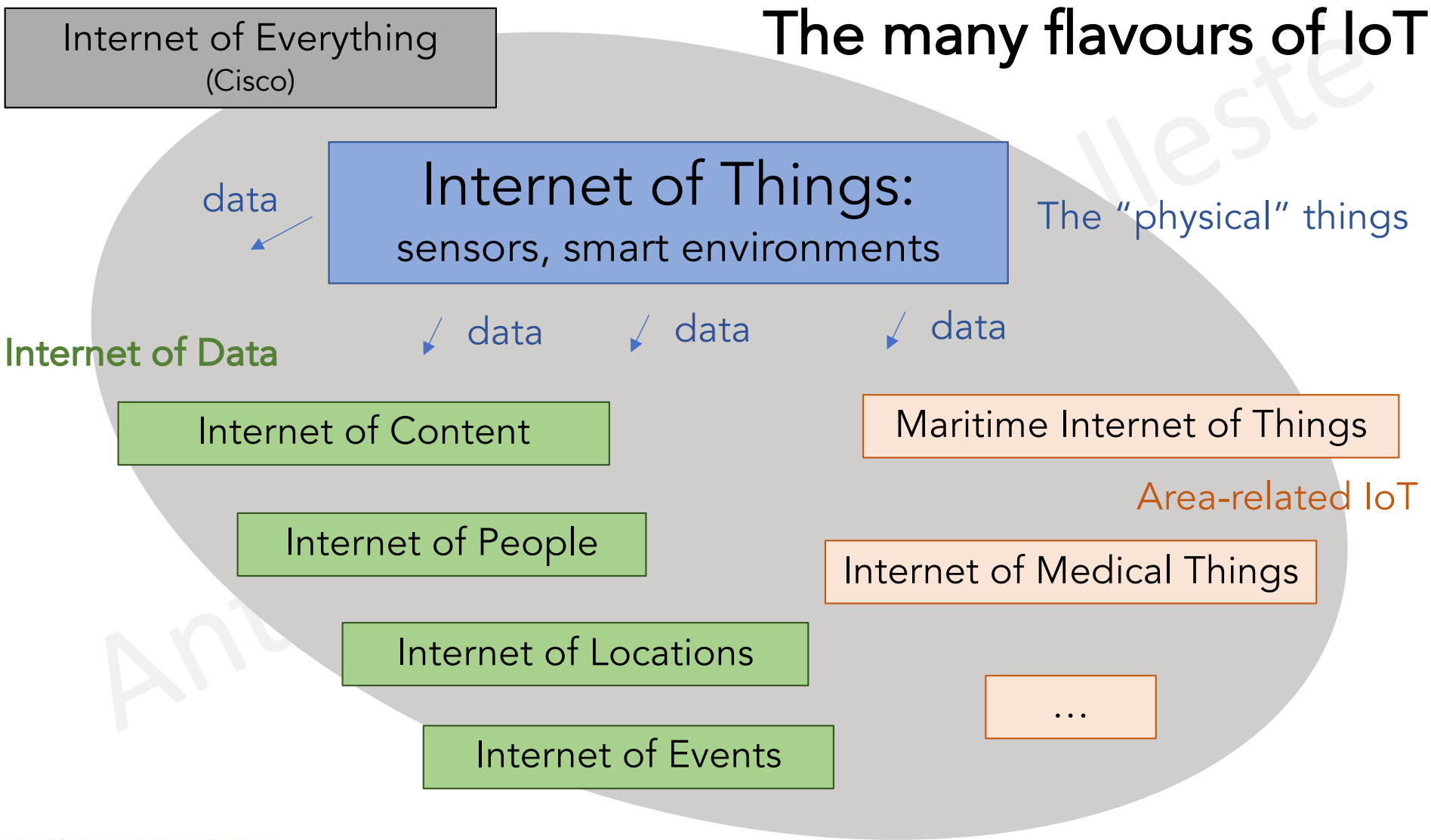
Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

The term "Internet of Things" was coined in 1999 by Kevin Ashton (RFID pioneer).

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

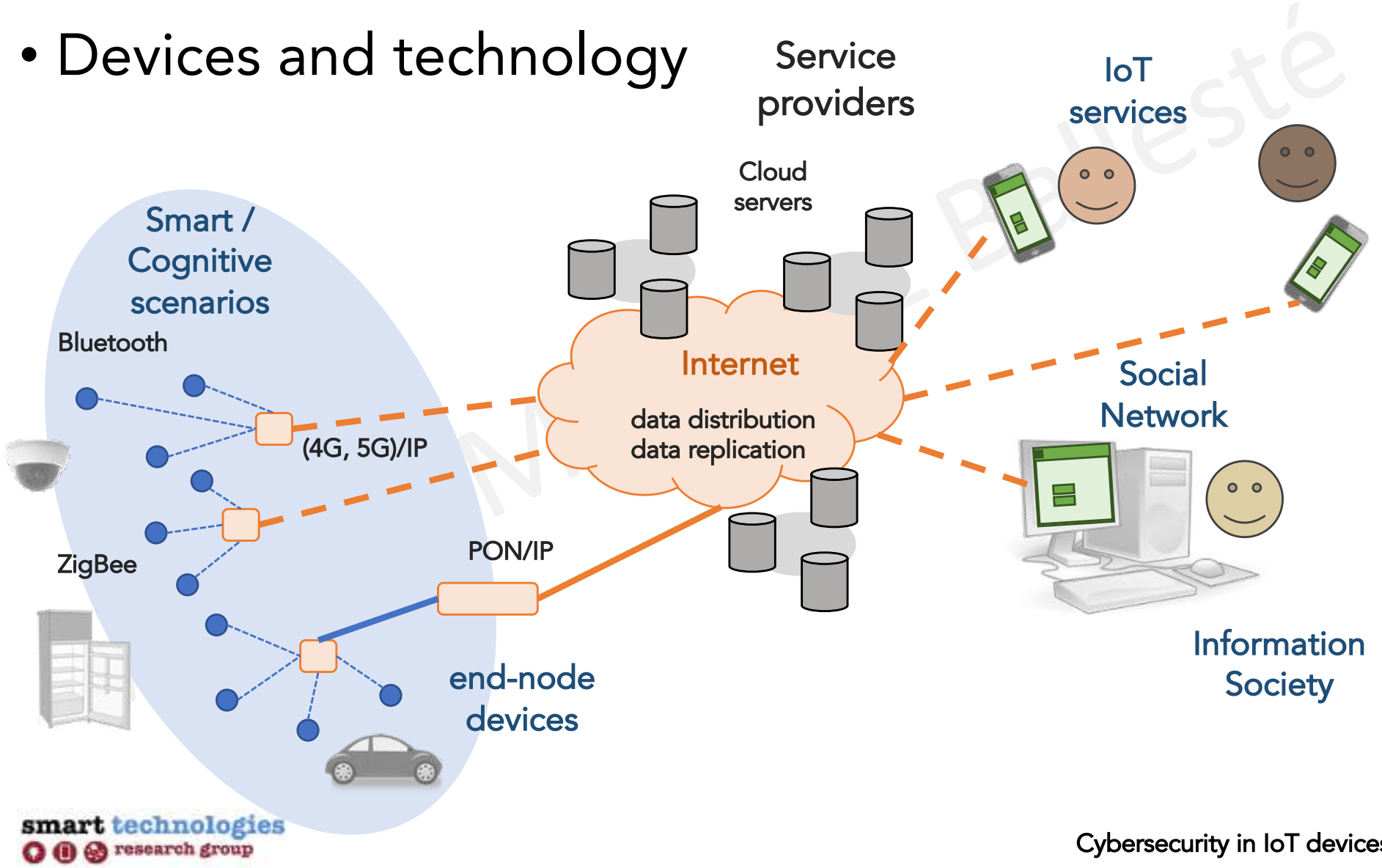
The Internet of Things



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

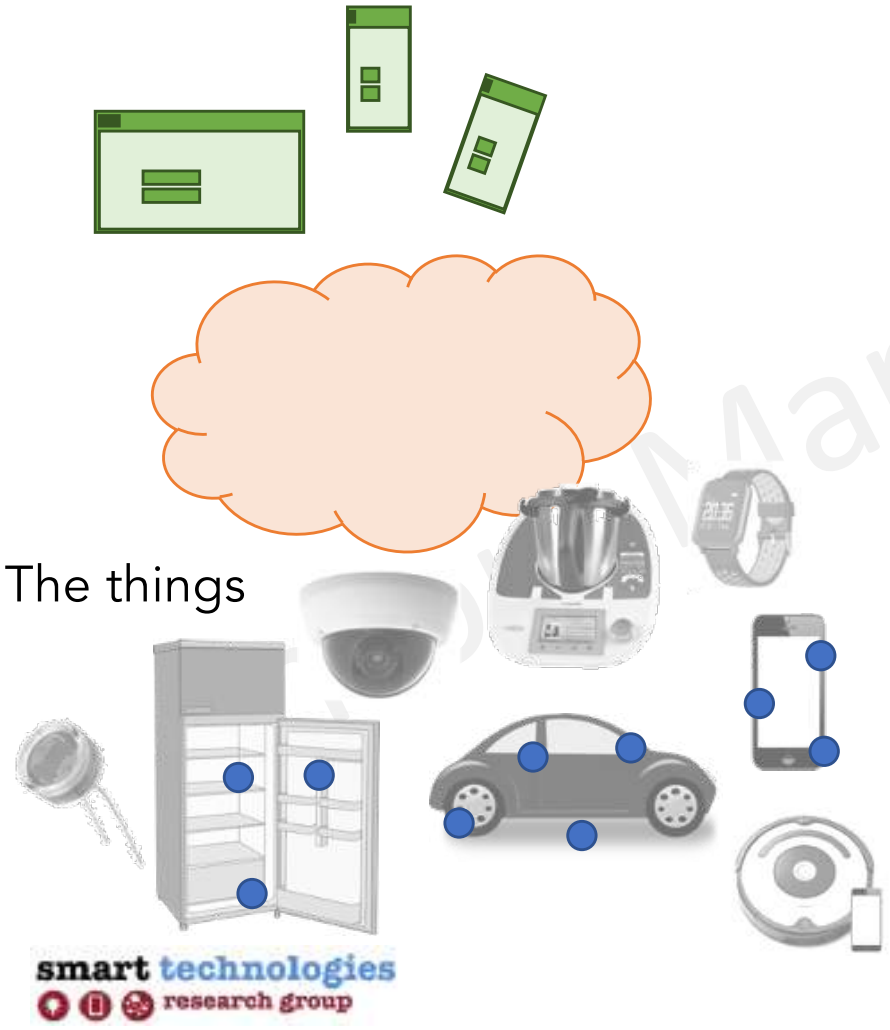
- Devices and technology



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

- The IoT architecture



5-layer approach	3-layer approach
Application	Service
Middleware	Transportation
Internet	
Access Gateway	
Field data acquisition layer	Perception

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

- "The things"
  - **Level 1. Very simple things:** analogical/digital sensors/actuators that must be connected to a controller (Arduino, Raspberry) so as to send/receive data over the Internet.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

- "The things"
  - **Level 2. Small things:** multipurpose devices typically connected using Bluetooth and the like. Must be connected to a controller.

Ruuvi Tag

micro:bit

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

- "The things"
  - **Level 3. Full stack things:** wifi/IP/HTTP access, web services implementation, etc. Can interact with remote servers and cloud services.
    - Open platforms / vs private products.
    - Open APIs (e.g. to communicate with digital assistants).

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

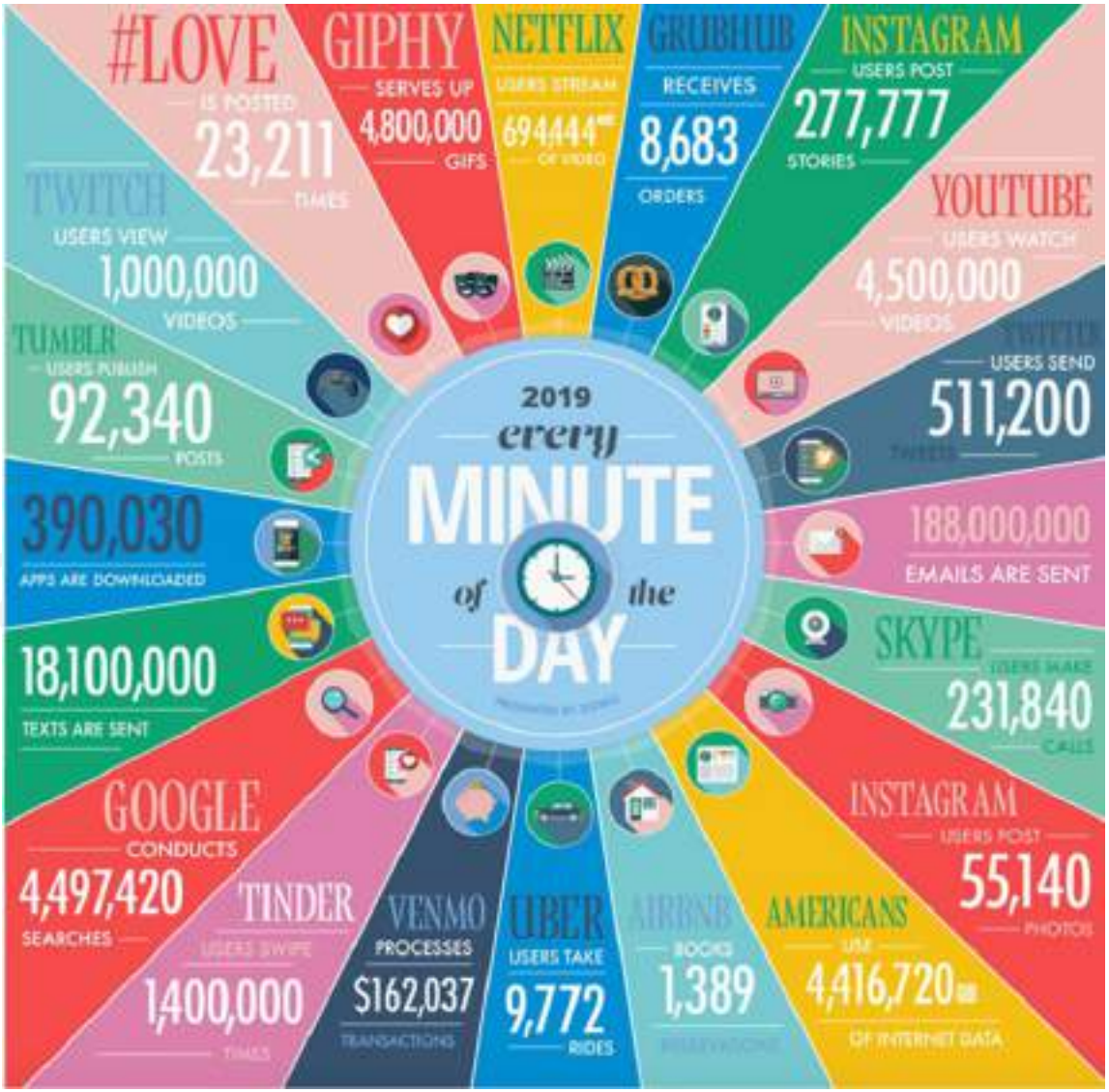
smart technologies research group

The Internet of Things

The upper the level… the more security problems and attacks exist!

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

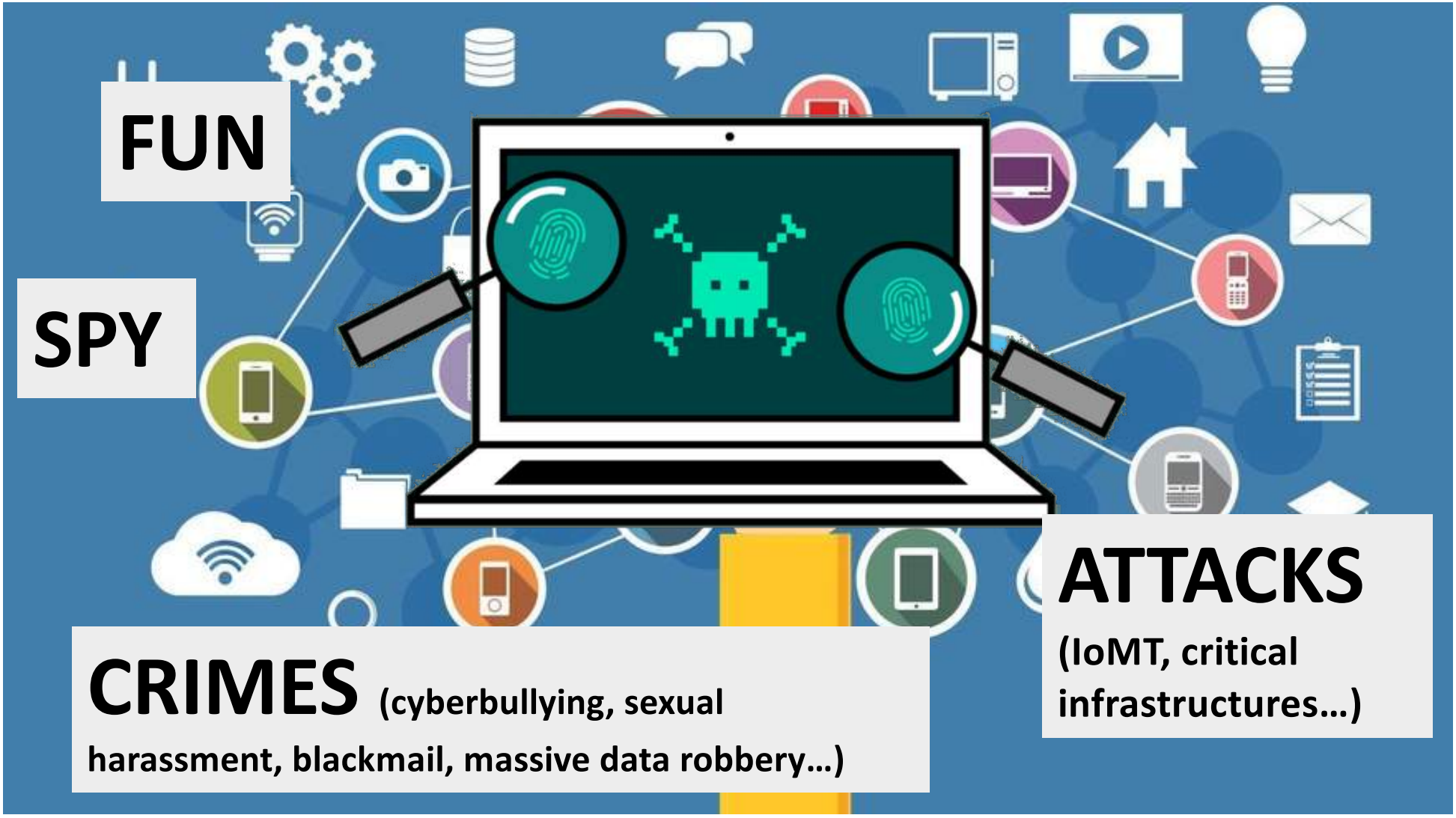
The Internet of Things



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

smart technologies research group

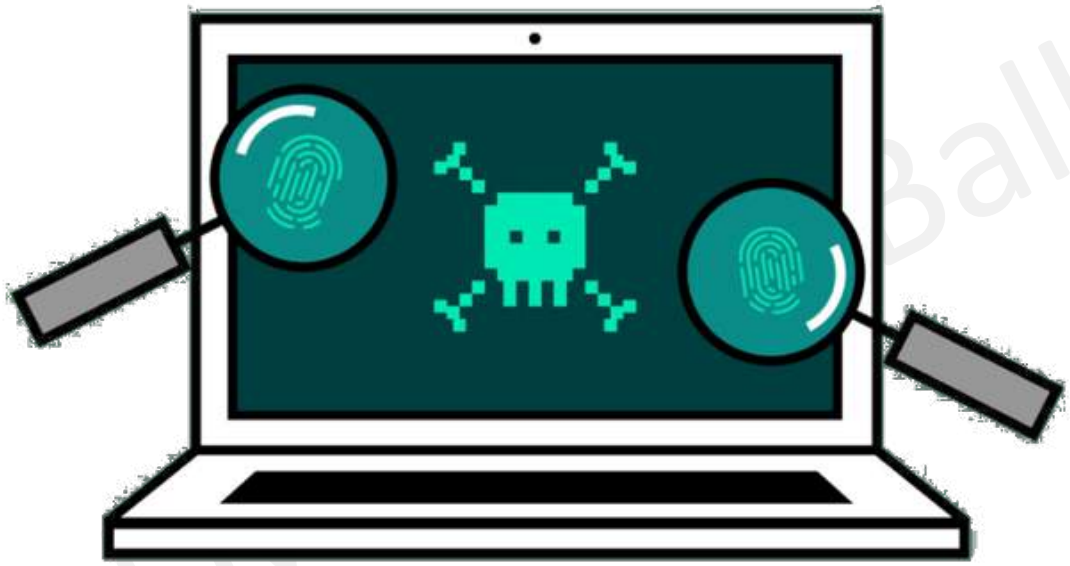
The Internet of Things



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The Internet of Things

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group



"Without security, the Internet of Things will cease to exist." GSMA (Association for Global System for Mobile Communications)

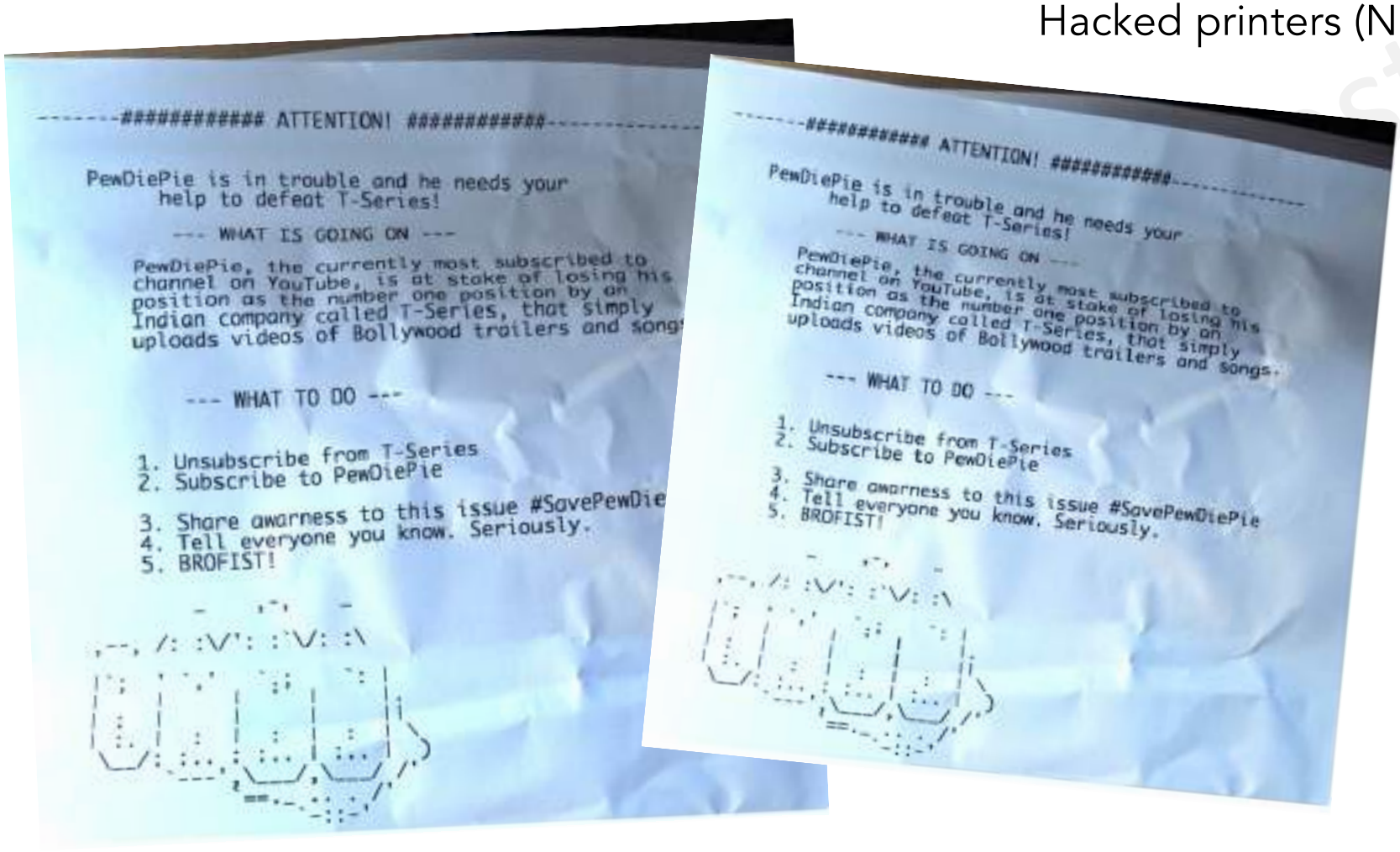
Content

- The Internet of Things
- **Some real threats**
- How to address cybersecurity
- IoT under attack
- People and society
- Guidelines

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Some real threats

Hacked printers (Nov. 2018)



Some real threats

Your kitchen robot may spy on you

The kitchen robot with a hidden microphone and a vulnerable Android version

Internet of Humans | Tell Us About You | ioh-general

alberto 1 Jun 17

The francophone media are all the rage with the story of Monsieur Cuisine Connect, a kitchen robot sold by low-cost supermarket chain Lidl. MCC contains a tablet-like device as a touch-screen control interface; it runs Android, and it turned out to be quite simple to hack [1]. As hackers took the kitchen robot apart in search of new cools hacks, they discovered a microphone, of which no mention was made in the marketing literature, nor in the product documentation.

The microphone was not simply forgotten in the tablet around which the MCC is built [1]. It is mounted outside of the table, secured to the chassis for a clearer, unmuffled sound. The chassis itself has a small hole in correspondence of the microphone, for even better results. In engineering terms, this is a smoking gun: the manufacturer wanted Monsieur Cuisine Connect to be able to listen in.

Even worse, MCC runs Android 6, which has important unfixed vulnerabilities. At the time of hitting the market (2019), those vulnerabilities were already well known (the final Android 6 security patch was released in 2017).

Antoni Martínez Balleste – Universitat Rovira i Virgili – SMART research group

Some real threats

Lovely toys easily hacked because of a flaw in their information systems

A CloudPet is simple to use. The parent or child speaks into a microphone inside the toy, which uses a Bluetooth interface to upload the recording to cloud storage via an Android or iOS smartphone app tied to an account. Recipients download and listen to the message on a second CloudPets toy.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Some real threats

The Romantik Seehotel Jagerwirt (Austria)

Hackers controlled both key card system and room locks…

They demanded a €1500 ransom, in Bitcoin.

With a full house of 180 guests, management felt as though they didn't have time to find an alternative solution. They paid the ransom.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Some real threats

Bees, our beloved pollinators about being extinct…

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

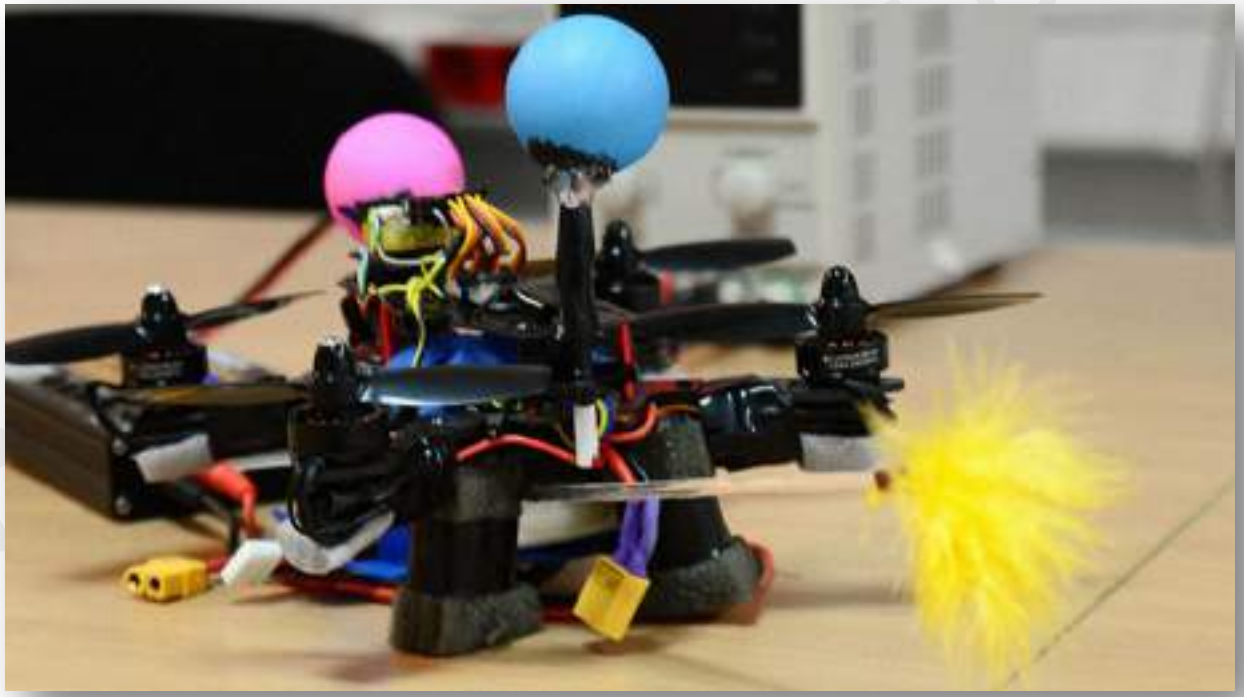
Some real threats

These are IoT bees: small robots able to act as pollinators. However, they are used by the government to spy people, and they can even be hacked so a swarm of b-drones are able to sting this man to death.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Some real threats

Warsaw University of Technology



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Content

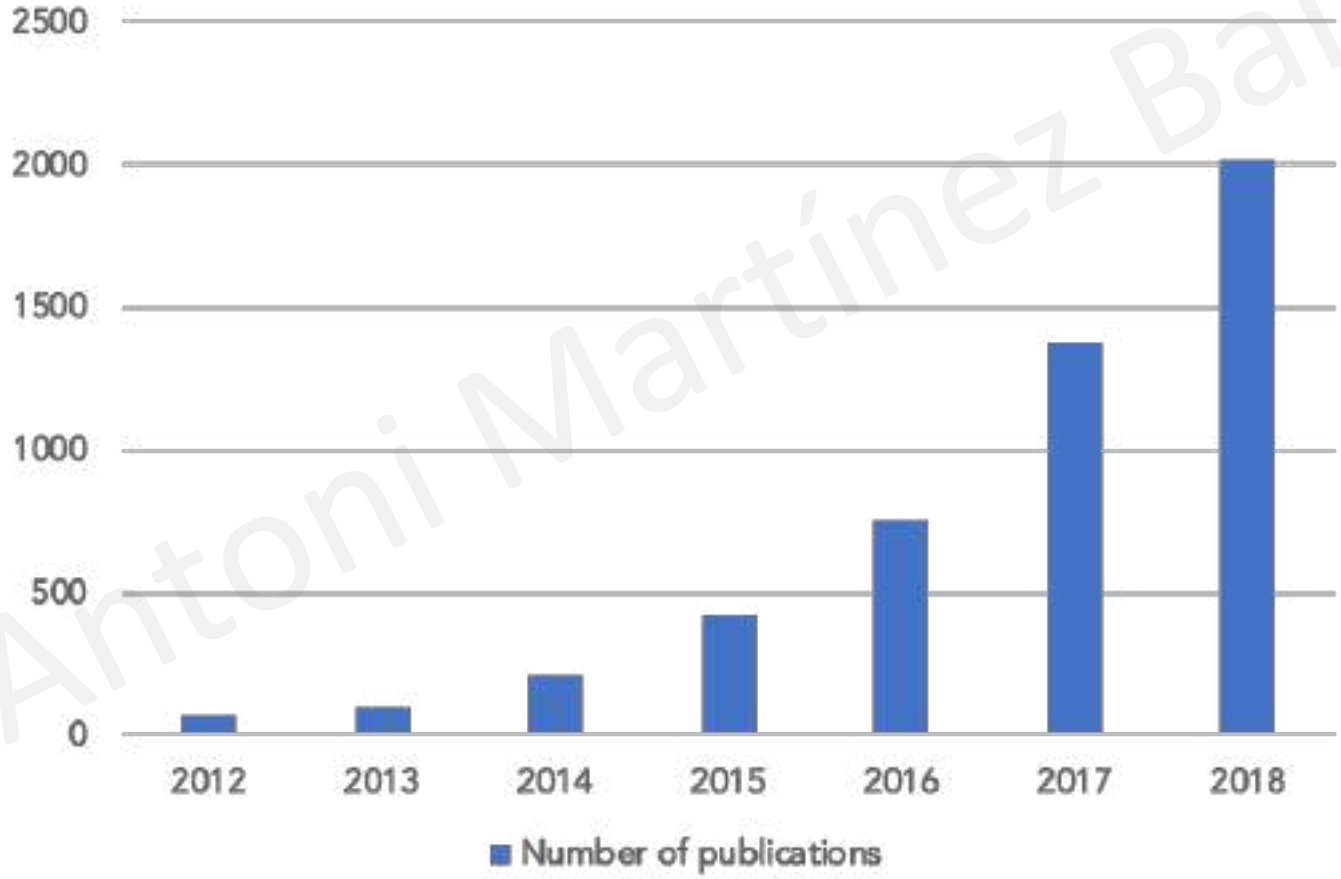
- The Internet of Things
- Some real threats
- **How to address cybersecurity**
- IoT under attack
- People and society
- Guidelines

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity

- IEEExplore

Conference papers and articles
IoT AND (Security OR Cybersecurity)



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity

Rodrigo Roman et al. / Computer Networks 57 (2013) 2266-2279

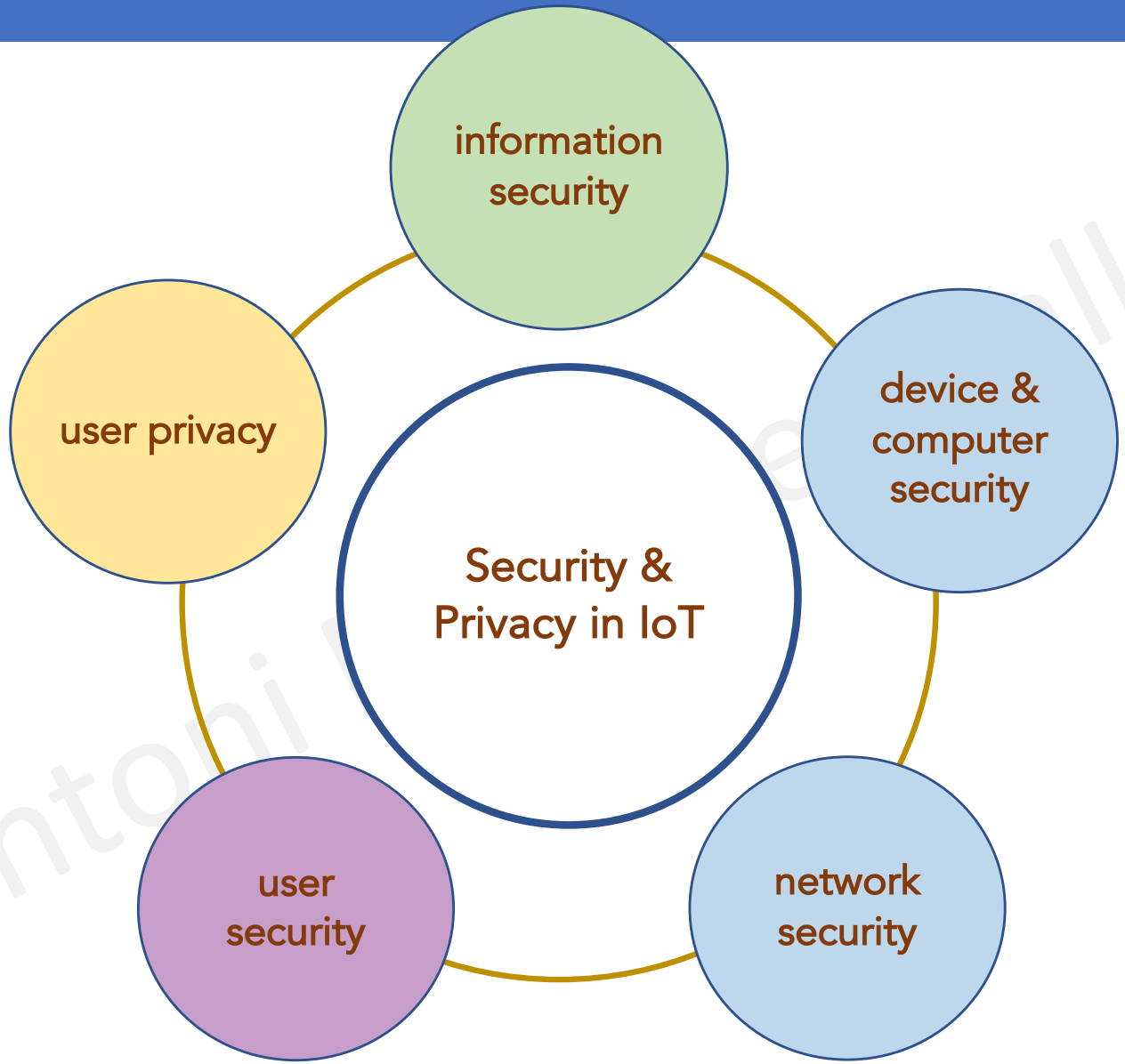
How to protect the communications?

How to manage authentication and access control in a world of billions of things?

What about the privacy of the users, and the security of the data generated by the things?

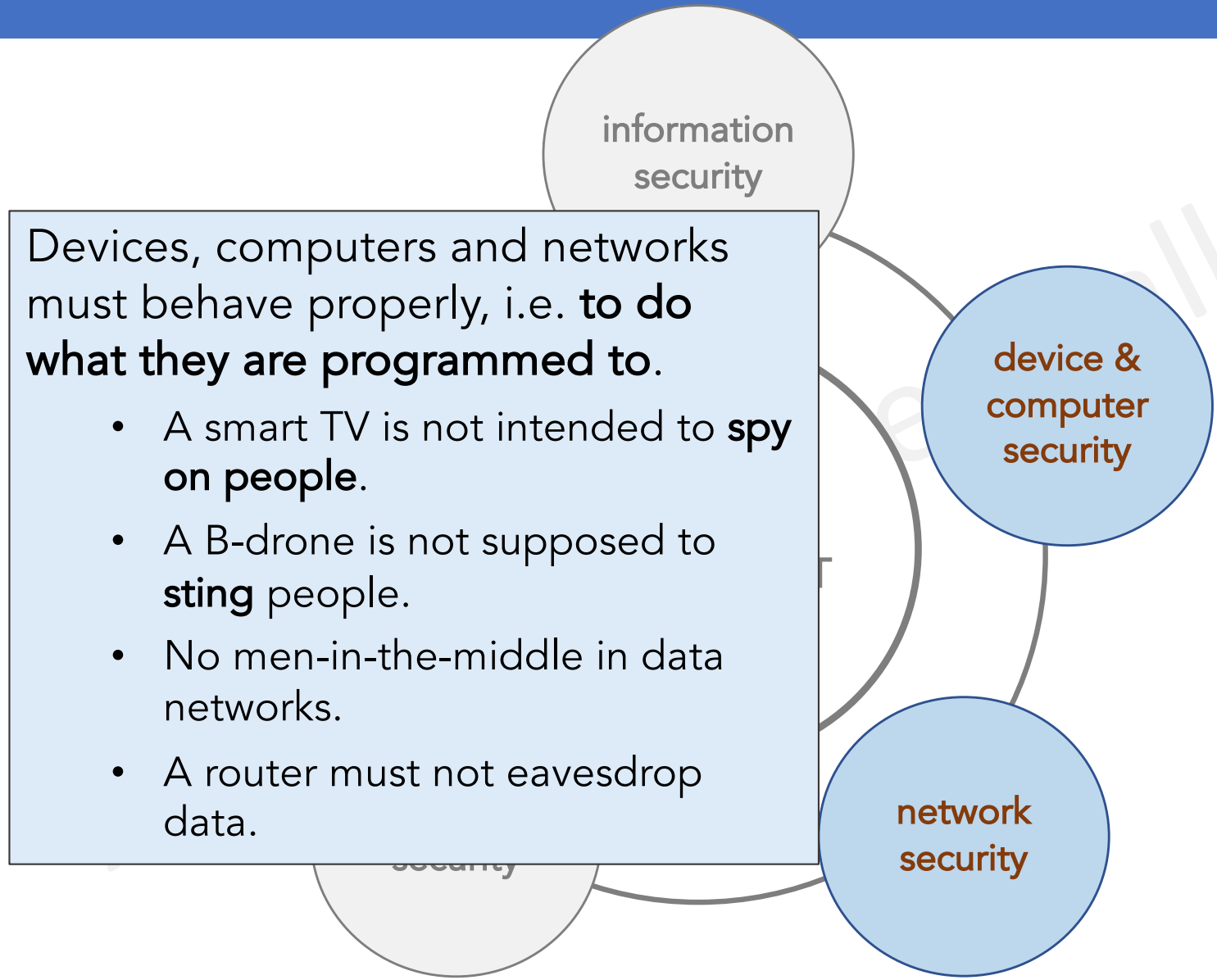
Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity

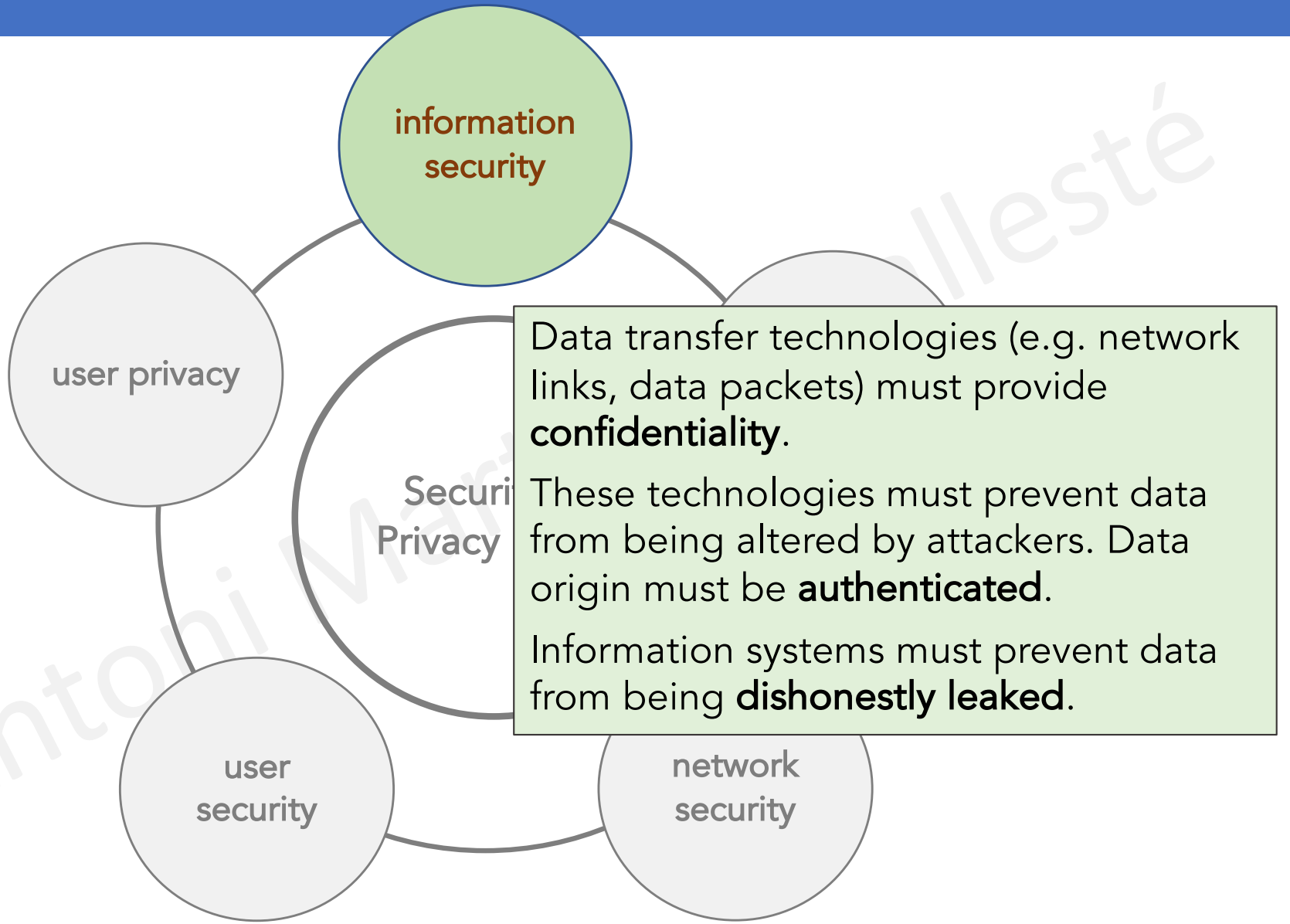


Devices, computers and networks must behave properly, i.e. **to do what they are programmed to**.

- A smart TV is not intended to **spy on people**.
- A B-drone is not supposed to **sting** people.
- No men-in-the-middle in data networks.
- A router must not eavesdrop data.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity



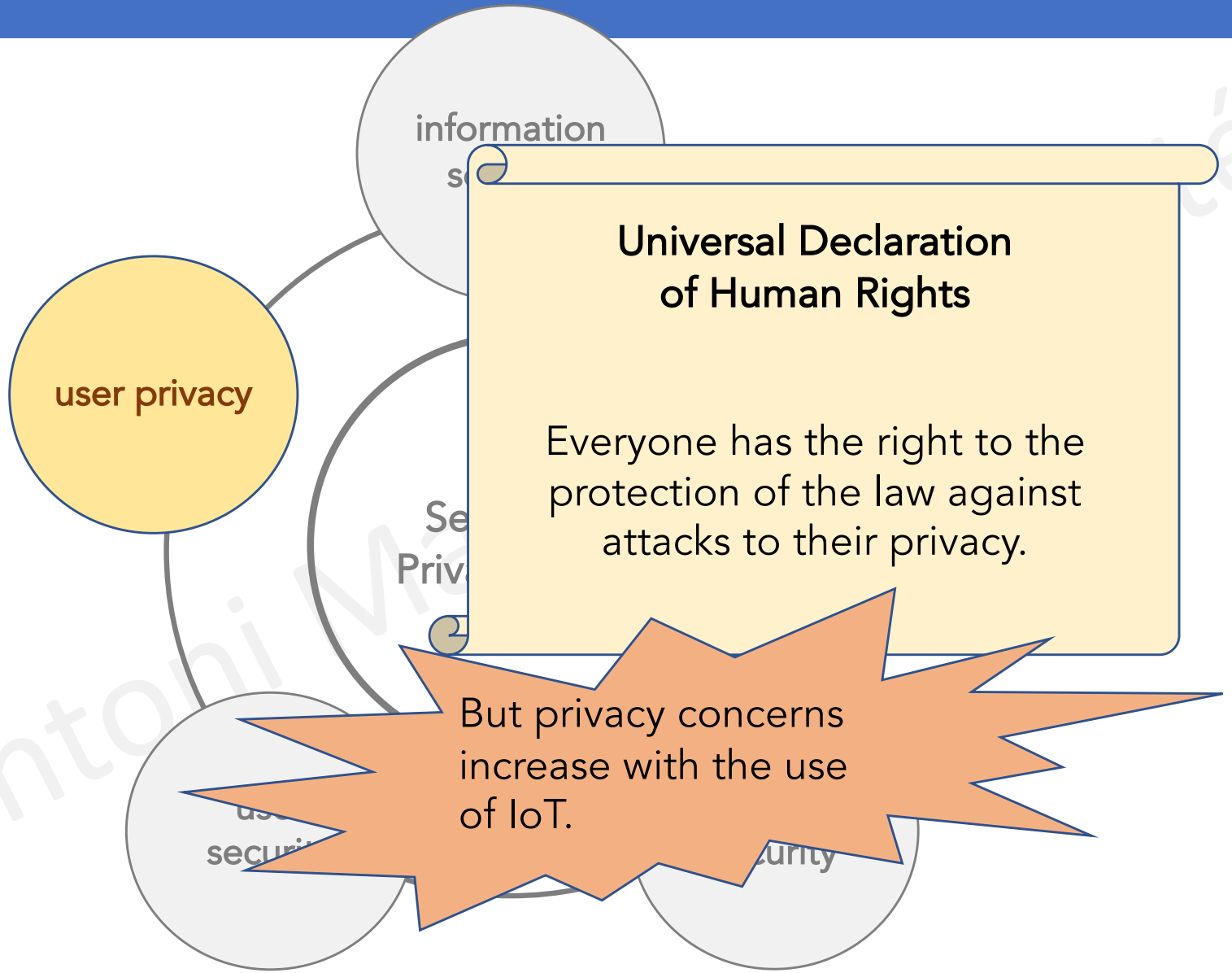
Data transfer technologies (e.g. network links, data packets) must provide **confidentiality**.

These technologies must prevent data from being altered by attackers. Data origin must be **authenticated**.

Information systems must prevent data from being **dishonestly leaked**.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity

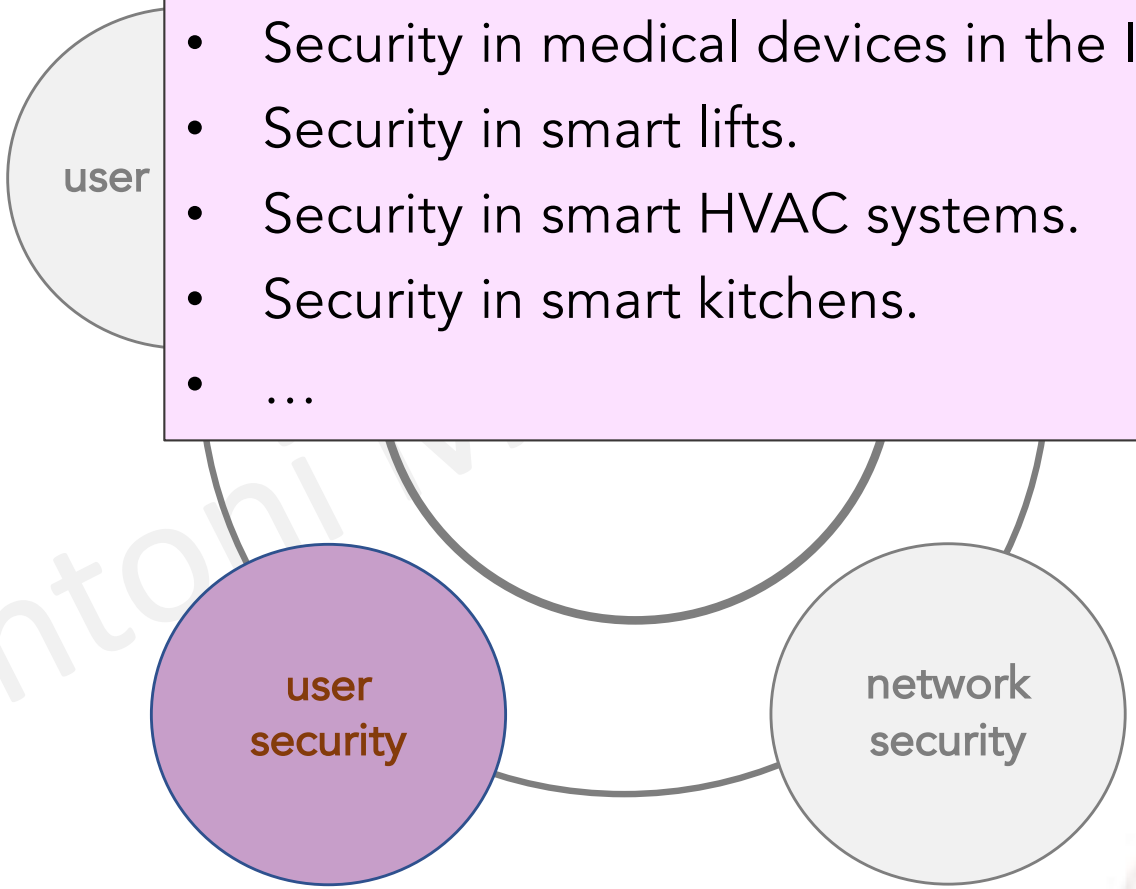


Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

How to address cybersecurity

Cybersecurity attacks in the IoT jeopardize the **physical security** of users:

- Security in connected vehicles: hacked driving assistants.
- Security in medical devices in the IoMT.
- Security in smart lifts.
- Security in smart HVAC systems.
- Security in smart kitchens.
- …



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

smart technologies research group

Content

- The Internet of Things
- Some real threats
- How to address cybersecurity
- **IoT under attack**
- People and society
- Guidelines

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

1990

Viruses

10^7 personal computers

2000

Internet attacks
phishing, worms, DoS…

10^8 Internet computers

2010

$3 \cdot 10^9$ Smartphones

10^9 Computers

2020

$2 \cdot 10^{10}$ IoT devices

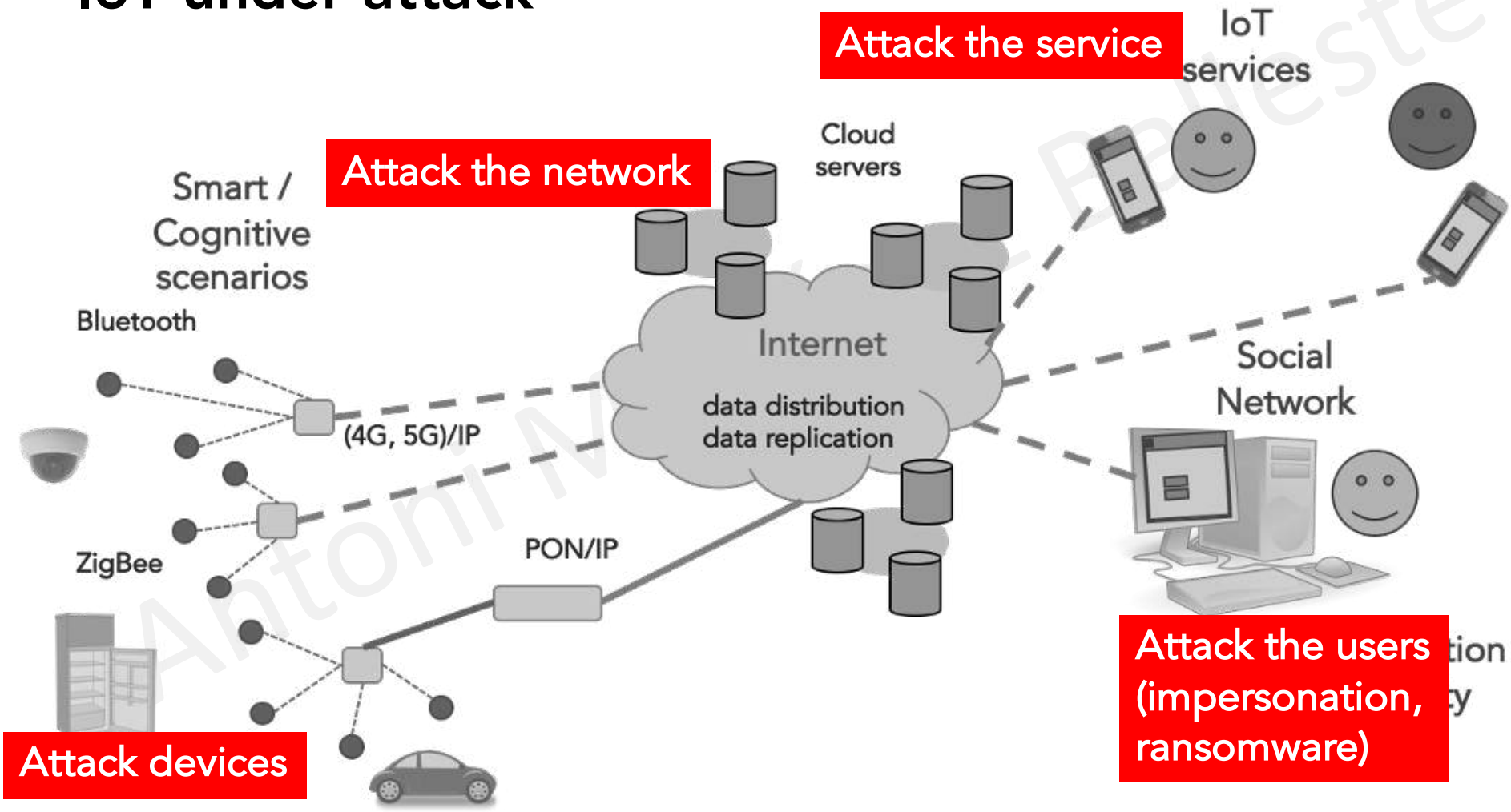
$3 \cdot 10^9$ Smartphones

10^9 Computers

smart technologies research group

The IoT under attack

- IoT under attack



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

- **Physical damage**
  - Physically attacking devices and communication networks…
  - Such events must be monitored and reported
    - From video surveillance to heartbeat communication between devices.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

- **Denial of Service (DoS)** at different levels
  - Jamming channels
    - Random frequency hopping
  - Controlling the infrastructure (entirely / a part of)
    - Insecure devices (think about low-cost routers that connect millions of homes to the Internet and provide UPnP easy connectivity from the outside world…)
  - Service provider DoS
    - Typically deployed on renowned cloud platforms that count with DoS countermeasures ($$$).

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

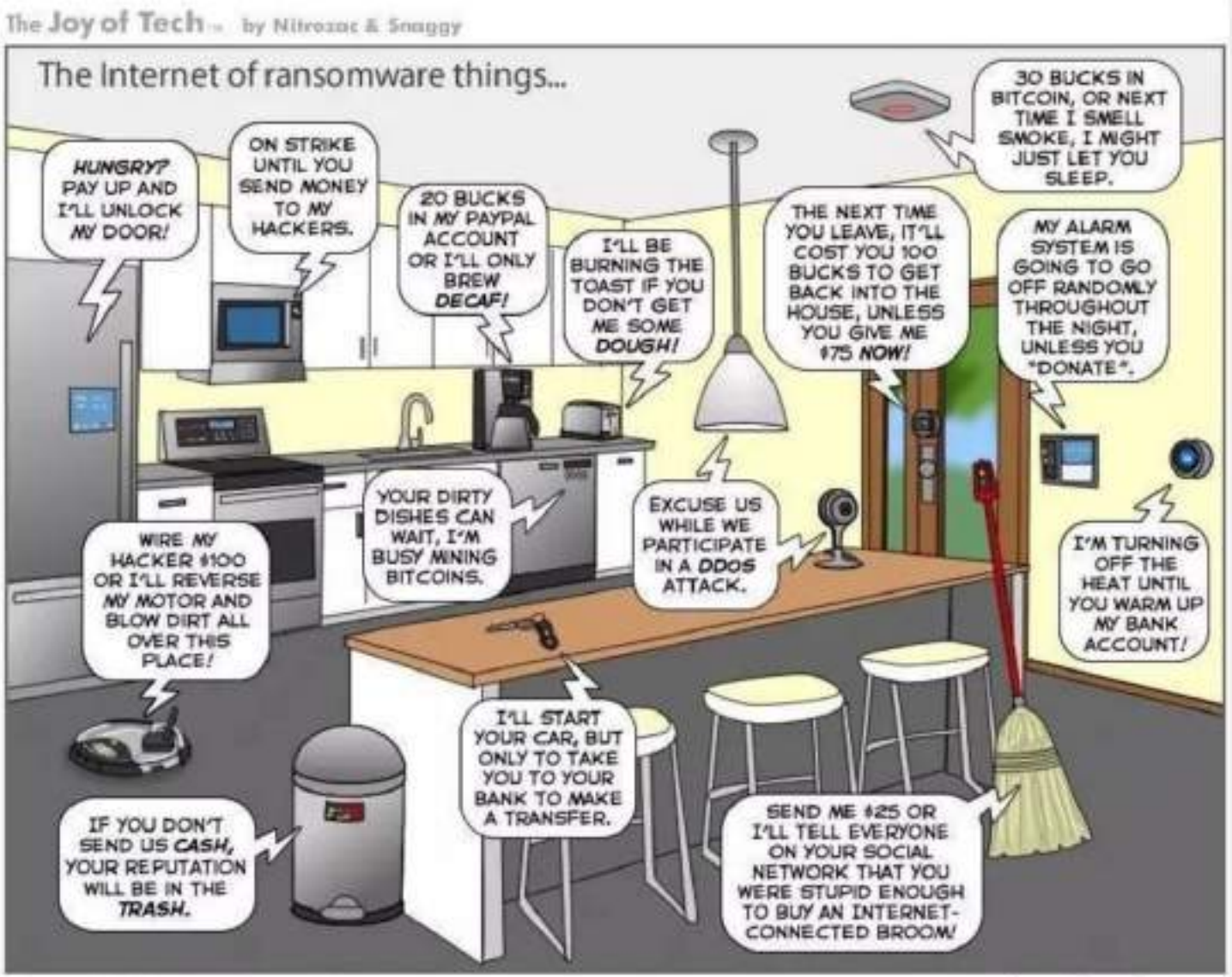
The IoT under attack

- **Node capturing /eavesdropping**
  - Extract the information by hacking the thing / from communication channels.
  - Hacking from the Internet, hacking the gateway, hacking as a faux device in the perception layer.

- **Ransomware**
  - Attackers threaten the unless a ransom is paid.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

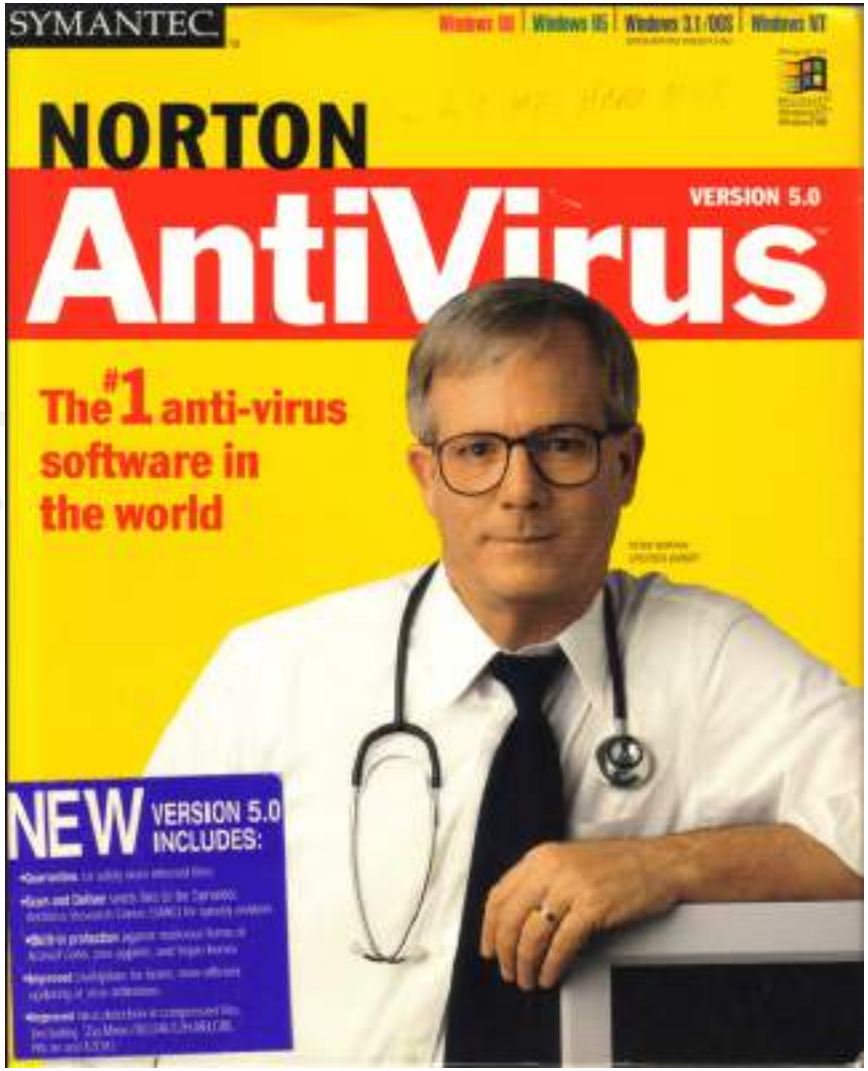
The IoT under attack



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

Can we apply classical security technology to secure IoT devices?



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

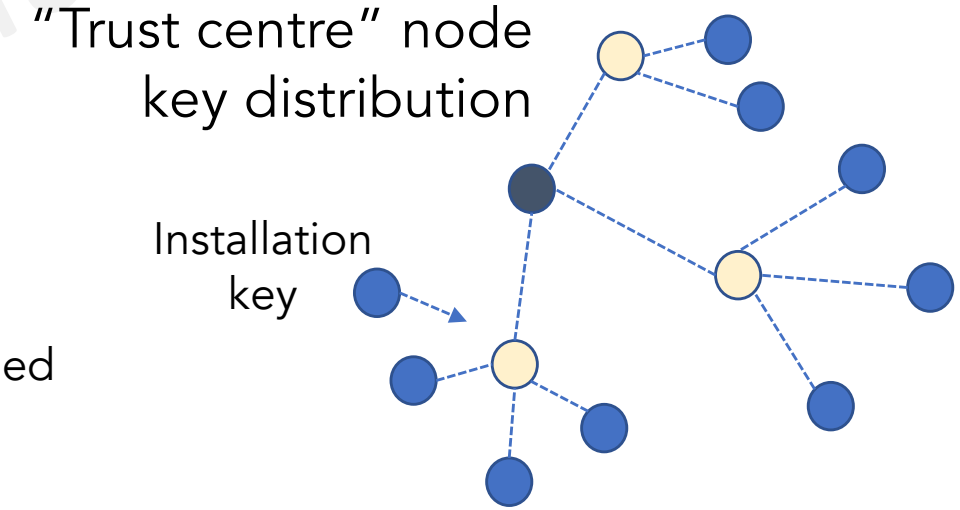
The IoT under attack

- **Challenge #1**
  - **Constrained resources**
    - For the sake of **power consumption**, many IoT devices have constrained processing capabilities and so that **lightweight cryptographic protocols** are to be used.

ZigBee

128-bit AES

Network key
Link key
Periodically changed



The IoT under attack

- **Challenge #2**
  - **Heterogeneity**
    - IoT involves interaction with **heterogeneous devices and systems**. **Interoperability standards.**

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

- **Challenge #3**
  - **Identity and Access Management (IAM)**
    - **Classical computer security relies on public-key cryptography… IoT poses a real scalability problem.**
      - **Identity management.** Billions of things!
      - **Universal authentication of users and things.** Ensuring the origin of the data.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

The IoT under attack

- **Challenge #4**
  - **Fault tolerance**
    - Intrusion detection and prevention mechanisms: in a Bluetooth piconet? In a smart city?
    - Recovery services: Locate attacked devices/services. Restoration or redirection to other working devices/services.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

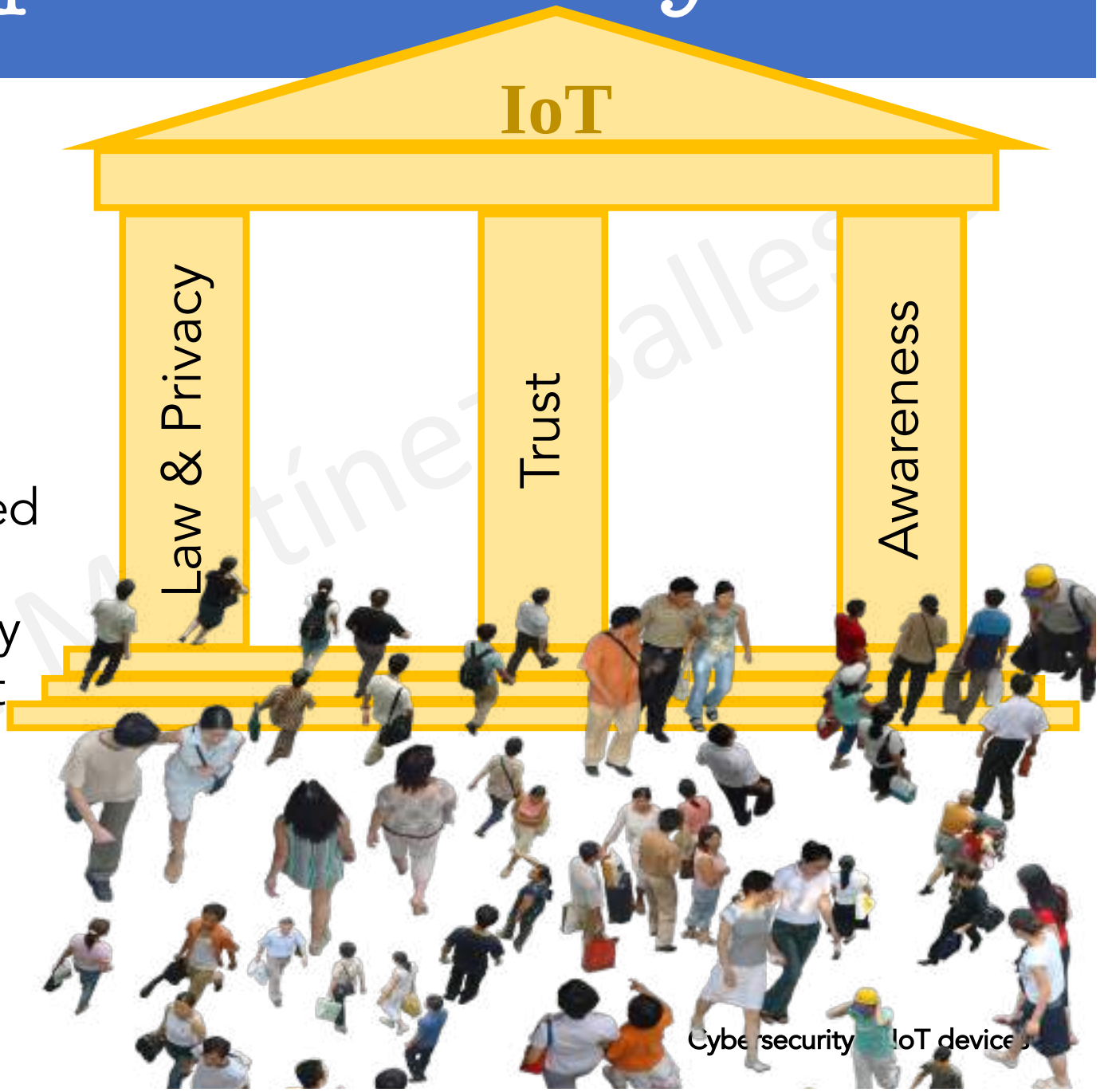
Content

- The Internet of Things
- Some real threats
- How to address cybersecurity
- IoT under attack
- **People and society**
- Guidelines

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

People and Society

The IoT creates a new social, economic, political, and ethical landscape that needs new enhanced legal and ethical measures for privacy protection and trust improvement…



Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

smart technologies research group

People and Society

- **Addressing user privacy**
  - "Privacy by design" principles: privacy must be taken into account throughout the whole engineering process.

General Data Protection Regulation

L 119/48 EN Official Journal of the European Union 4.5.2016

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

  - Privacy Enhancing Technologies.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

People and Society

- **Addressing trust in IoT**

The OTA IoT Trust Framework

IoT services are trustworthy if…

- **Authentication** of devices and users.
- **Encryption** of data.
- **Security** in all areas (devices, apps, backend services) with regular **testing** and **updates**.
- Inform users about **updates**, and deliver them with minimal impact.
- Disclose **privacy-related policies** about data collection and sharing, presented in down-to-earth language to users.
- Users have choices and **control regarding their data** collected.
- Communications between provider and users must use best practices to **limit social engineering attacks**.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

People and Society

- **Raising awareness**

kaspersky

…Additional research shows 84% of cyberattack victims attribute the attack, at least in part, to human error, …

1. Opening emails from unknown people
2. Having weak login credentials
3. Leaving passwords on sticky notes
4. Having access to everything
5. Lacking employee training
6. Not updating antivirus software
7. Using unsecured mobile devices

Organisations are doing a great effort but…

…awareness **must be spread** in education, mass media, by governments…

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Content

- The Internet of Things
- Some real threats
- How to address cybersecurity
- IoT under attack
- People and society
- **Guidelines**

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Guidelines

- **Applus+**
  - Innovative approaches to testing, inspection and certification.
  - Cybersecurity for IoT certification:
    - **Data protection:** evaluation of communication security and storage mechanisms.
    - **Interface security:** proper identification of interfaces and certification of authentication mechanisms (user interfaces, APIs, network ports, physical interfaces).
    - **Secure updates:** integrity of new binaries, avoid faux updates.
    - **Safe boot:** certification of a secure and reliable device boot system.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Guidelines

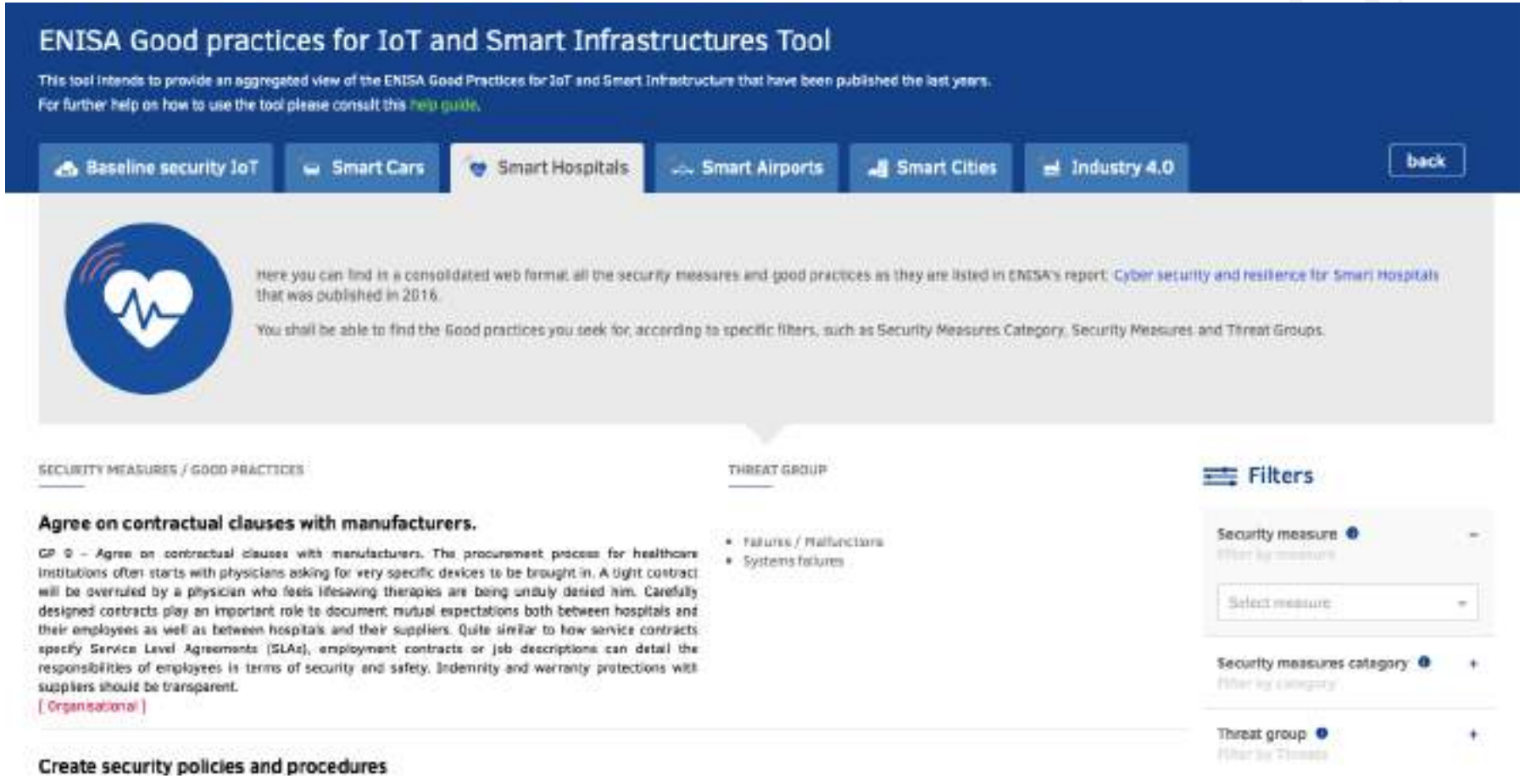
- **OWASP**
  - Open Web Application Security Project, collect/disseminate tools for cybersecurity. 10 checkpoints for IoT security:

1. Weak, guessable, hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanisms
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Guidelines

- **ENISA** (European Union Agency for Cybersecurity)



Guidelines

- ISO/IEC 27000
  - Family of standards about information security
    - **27000.** Description of concepts used in the standards.
    - **27001.** Information technology - Security Techniques - Information security management systems — Requirements
    - **27002.** Code of practice for information security controls.
    - **27004.** Information security management — Monitoring, measurement, analysis and evaluation.
    - **27033.** Network security
    - **27034.** Application security
    - **27035.** Information security incident management
    - …

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Guidelines

- ISO/IEC 27000
  - Family of standards about information security
    - **27000.** Description of concepts used in the standards.
    - **27001.** Information technology - Security Techniques - Information security management systems — Requirements
    - **27002.** Code of practice for information security controls.
    - **27004.** In
      measuren
    - **27033.** N
    - **27034.** A
    - **27035.** In
    - …

27030. Guidelines for security and privacy in IoT (under development)

The standard will provide guidance on the principles, risk and controls for IoT security and privacy.
To be published in 2022, project proposed in 2018.

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Conclusions

- We have reviewed security concerns related to IoT devices: device security, information security, user privacy and user (physical) security. But some other relevant concerns must be considered: regulation, trust, awareness, …
- Technology can be protected, companies count with guidelines and certifications, governments are enacting regulations… **the IoT can be a safe place!**

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Conclusions

… well, the IoT can be
at least as safe
as our real world can be!

Antoni Martínez Ballesté – Universitat Rovira i Virgili – SMART research group

Cybersecurity in IoT devices

Antoni Martínez Ballesté
Universitat Rovira i Virgili

smart research
Universitat Rovira i Virgili