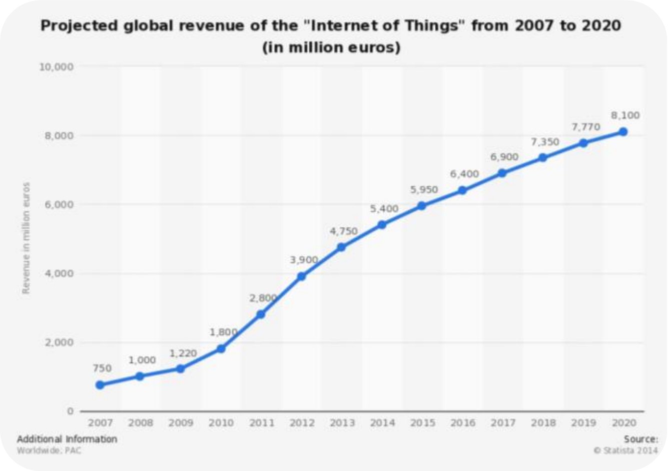
BoR (17) 14

IoT and Smart Infrastructure efforts in ENISA

Dr. Dan Tofan | IoT workshop BEREC | 01.02.2017, Brussels

Everything becomes connected



Projected global revenue of the "Internet of Things" from 2007 to 2020 (in million euros)

Additional Information
Worldwide; PAC

Source:
© Statista 2014

Manufacturers have an economic interest

- Data collection and processing
- New business models: data reseller, targeted ads, etc.
- Competitors do IoT, hence we must do IoT
- Competitors don't do IoT, let's be the first one!

Customers have their own interests (do they?)

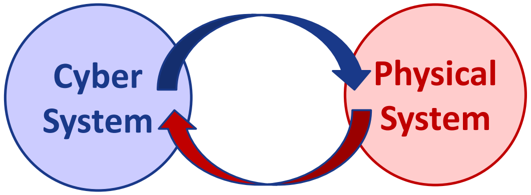
- Connectivity is needed, mobility is important
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities than non-IoT product, reasonable price
- Non-connected version is not available

Connected products are the new normal

Why IoT security matters?

No device is fully secured

- Reliance on third-party components, hardware and software
- Dependency to networks and external services
- Design of IoT/connected devices
- Vulnerabilities in protocols
- Security by design NOT the norm.



IoT security is currently limited

- Investments on security are limited
- Functionalities before security
- Real physical threats with risks on health and safety
- No legal framework for liabilities

IoT brings smartness and new security challenges

Securing Europe’s smart infrastructures

SMART cars, cities, homes, hospitals and transport studies

Just published

- Understand threats and assets
- Highlight security good practices in specific sectors
- Provide recommendations to enhance cyber security

Demos

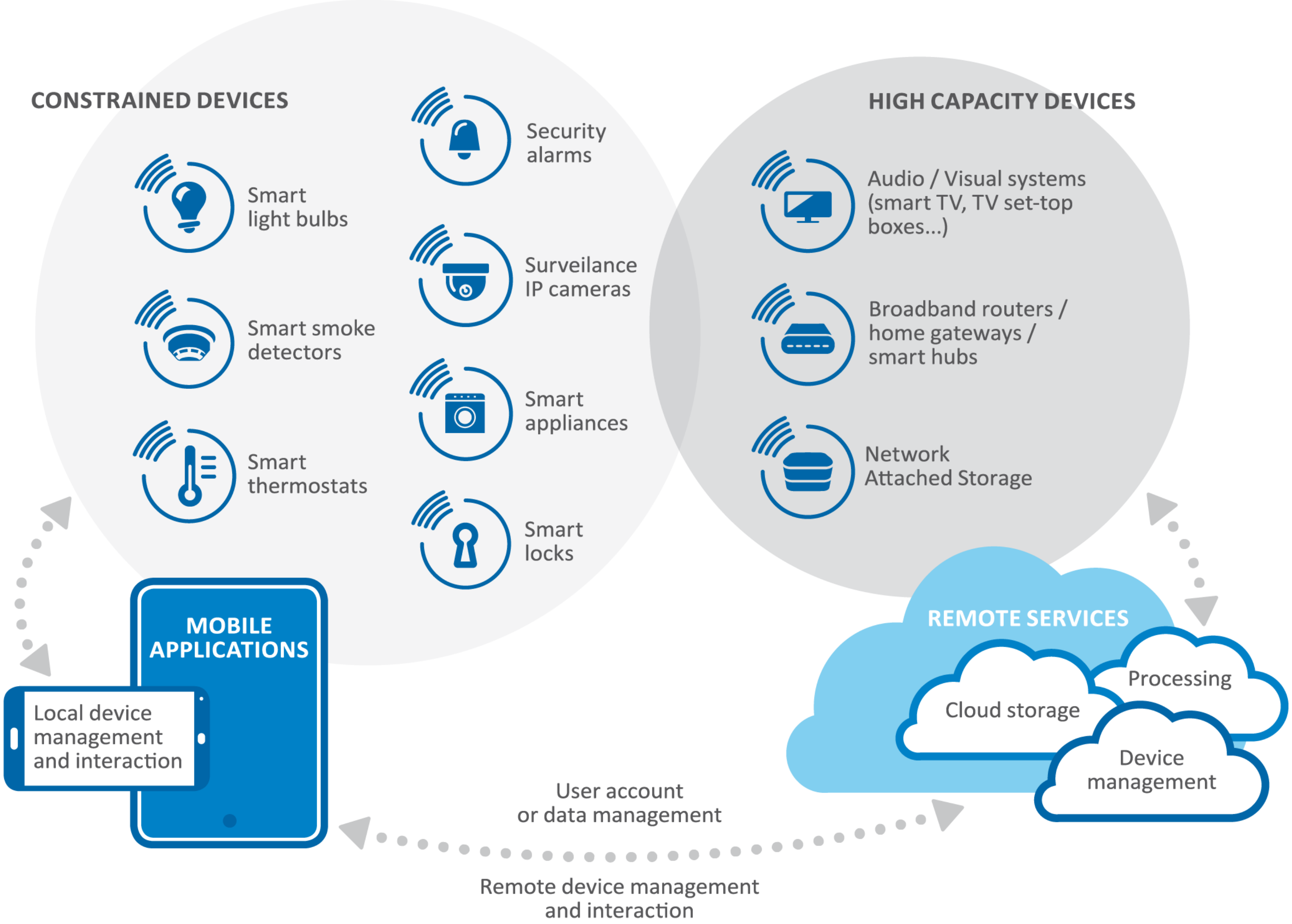
- Hands on Bluetooth lock demo
- Live hacking attack and countermeasures

Expert groups with renowned subject matter experts

- Engage with communities
- Smart Cars, Intelligent Public Transports and eHealth expert group

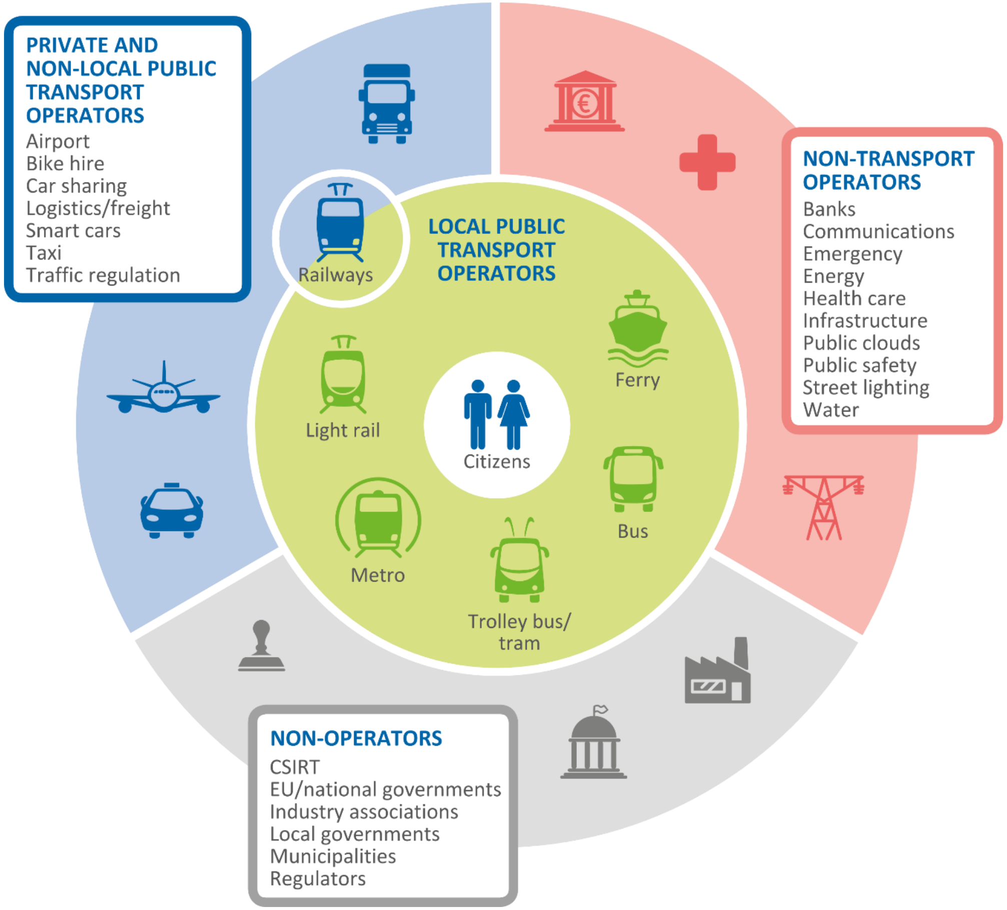
http://enisa.europa.eu/smartinfra

IoT in Smart Homes: devices



https://www.enisa.europa.eu/smartinfra

Securing transport infrastructure



2015 studies

- **Architecture model of the transport sector in Smart Cities**
- **Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations**

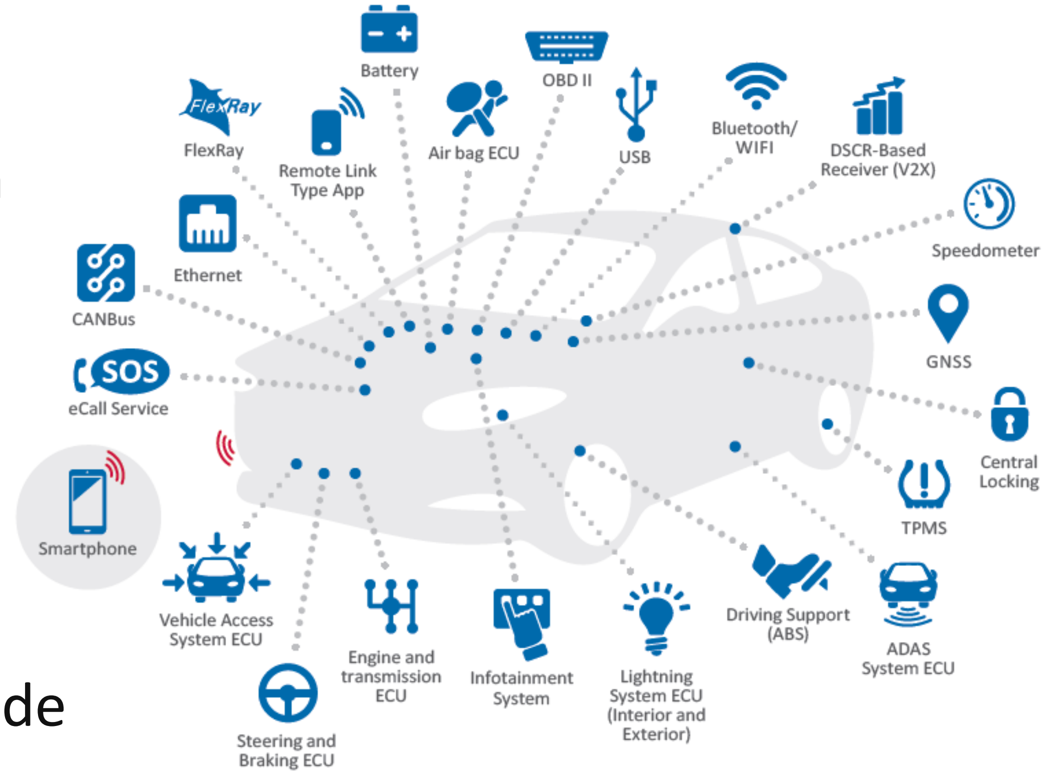
Objectives

- Assist operators in their risk assessment
- Raise awareness to municipalities and policy makers
- Invite manufacturers and solution vendors to focus on security

https://www.enisa.europa.eu/smartinfra

IoT in Smart Cars

- Increased attack surface
- Insecure development in today's cars
- Security culture
- Liability
- Safety and security process integration
- Supply chain and glue code



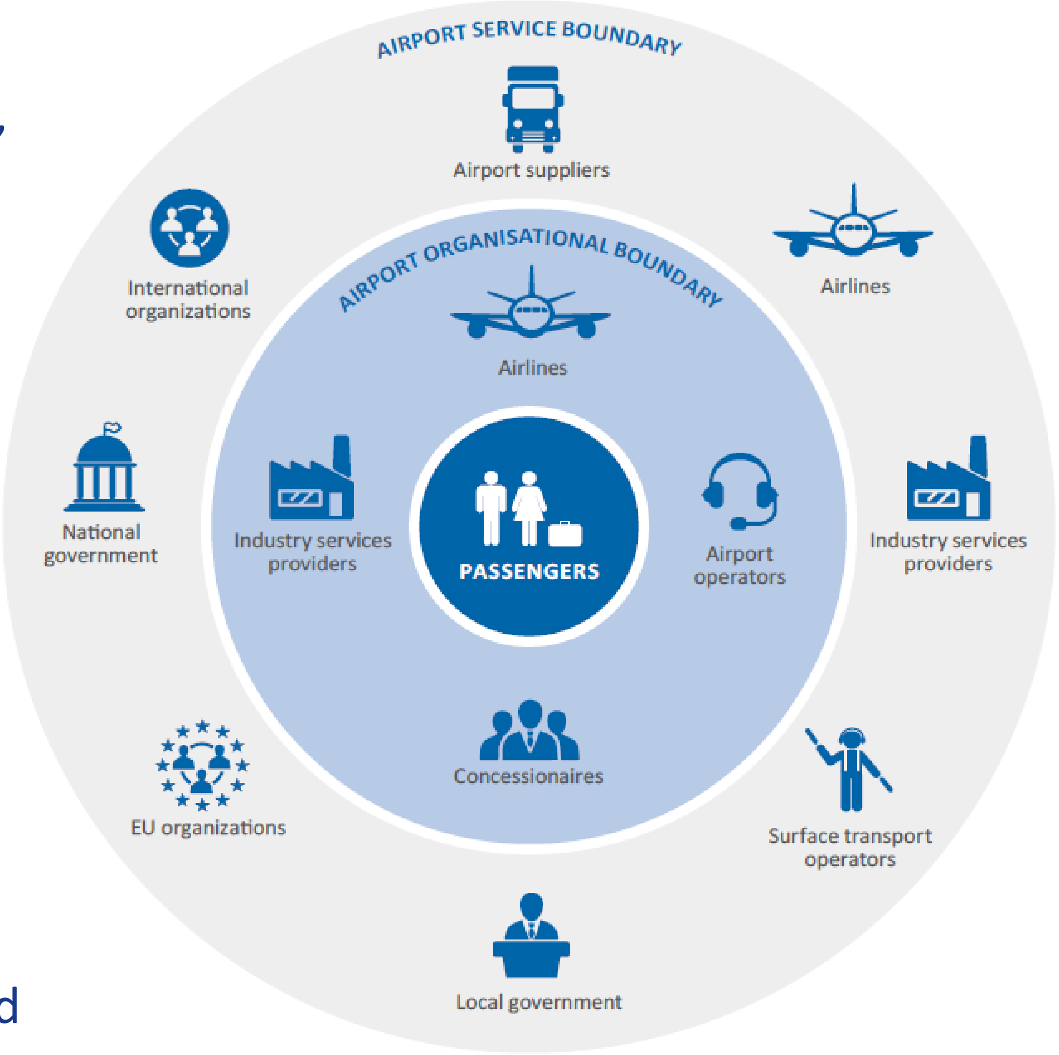
Secure Smart Cars today
for safer autonomous cars tomorrow

IoT in Smart Airports

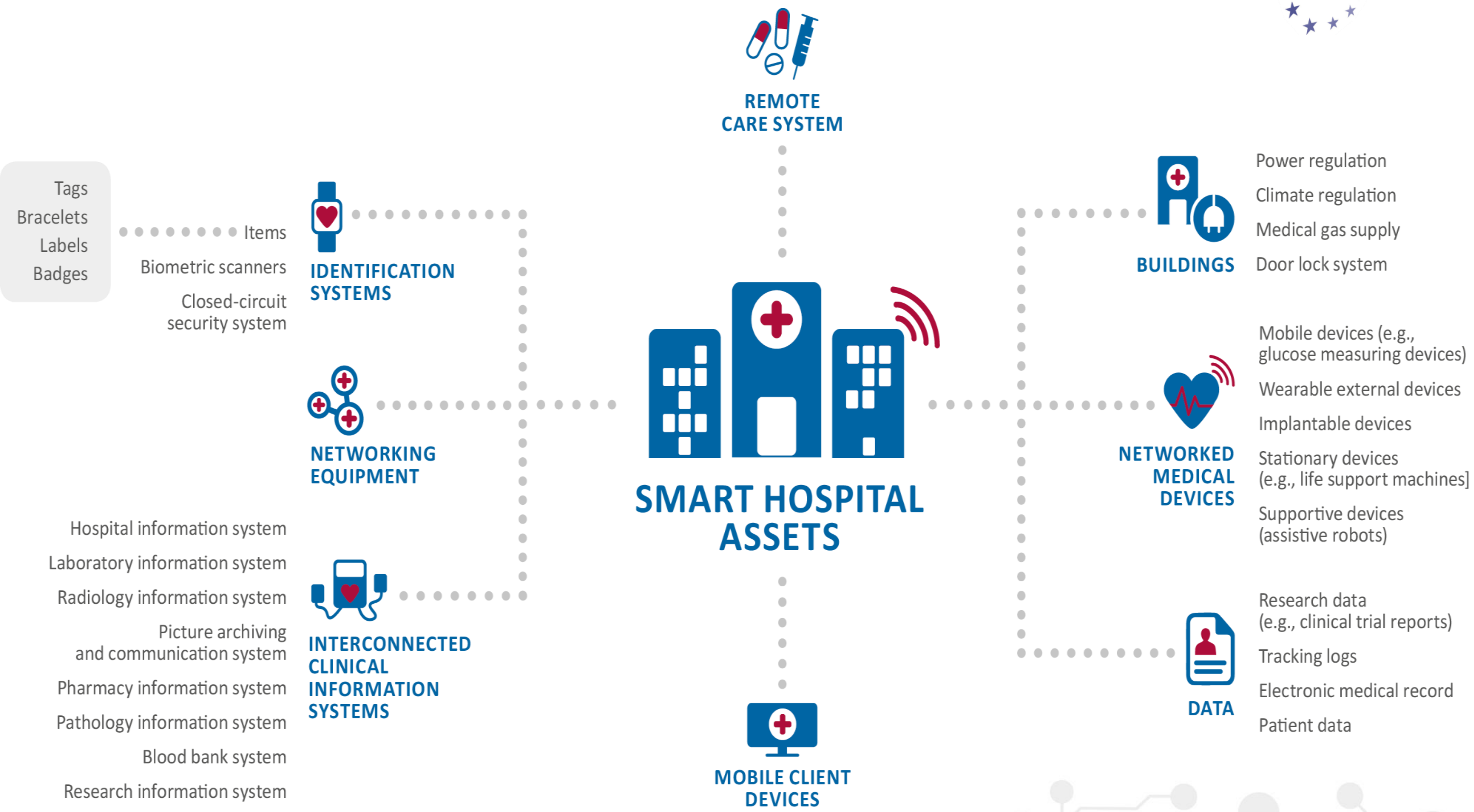
Smart airports are those airports making use of networked, data driven response capabilities that, on the one hand, provide travellers with a **better and seamless travel experience** and, on the other hand, aim to guarantee **higher levels of security for the safety** of the passengers and operators.

Smart services can be:

- self check-in
- flight booking management
- way finding services
- automated border control and security checks.



Smart Hospitals



REMOTE CARE SYSTEM

Tags
Bracelets
Labels
Badges

Items

Biometric scanners

Closed-circuit security system

IDENTIFICATION SYSTEMS

NETWORKING EQUIPMENT

Hospital information system

Laboratory information system

Radiology information system

Picture archiving and communication system

Pharmacy information system

Pathology information system

Blood bank system

Research information system

INTERCONNECTED CLINICAL INFORMATION SYSTEMS

SMART HOSPITAL ASSETS

MOBILE CLIENT DEVICES

BUILDINGS

Power regulation

Climate regulation

Medical gas supply

Door lock system

NETWORKED MEDICAL DEVICES

Mobile devices (e.g., glucose measuring devices)

Wearable external devices

Implantable devices

Stationary devices (e.g., life support machines]

Supportive devices (assistive robots)

DATA

Research data (e.g., clinical trial reports)

Tracking logs

Electronic medical record

Patient data

Secure devices and systems to improve patients’ safety

Security incidents involving IoT– examples (1)

Home routers taken over and used for DDoS:

- Oct. 2016 Dyn attach: large DNS service provider attacked through network of compromised routers; several popular websites affected worldwide.

Security incidents involving IoT– examples (2)

DDoS attack halts heating in Finland

- Nov. 2016: DDoS attacks disabled the computers that were controlling heating distribution in at least in two properties in the city of Lappeenranta.
  - Statements: convenience and ease of use it often opens up vulnerabilities; building automation security is often neglected; security in general tends to be lax.
  - Devices attacked because they were vulnerable and the attackers scanned network to find more of them.

Giant Heating System Hacked In Finland

Security incidents involving IoT– examples (3)

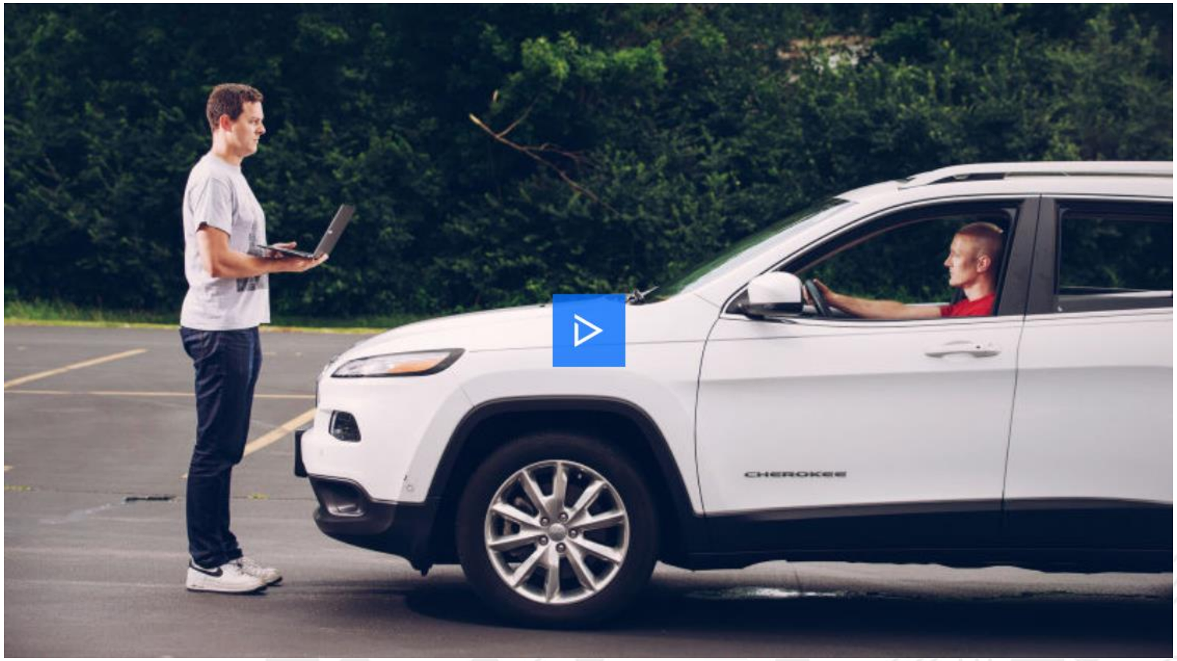
The vulnerable fridge

- Security researchers have discovered a potential way to steal users’ Gmail credentials from a Samsung smart fridge.
- Vulnerability discovered during an IoT hacking challenge at a recent DEF CON hacking conference.

Security incidents involving IoT–examples (4)

The laptop driven car

- Hackers Remotely Kill a Jeep on the Highway
- Hackers remotely toyed with the brakes, air-conditioning, radio, and windshield wipers via an xploit in its Uconnect infotainment system.



Security incidents involving IoT– examples (5)

Internet-connected Hello Barbie doll can be hacked

- several vulnerabilities in the toy, the worst of which could allow an attacker to intercept a child’s communications.

IoT Security – main challenges

- **Very large attack surface**
- **Widespread deployment**
- **Limited device resources**
- **Security by design not a top priority**
- **Lack of standards and regulations**
- **Lack of expertise**
- **Lack of security updates**
- **Insecure development**
- **Unclear liabilities**

IoT Security Recommendations (1)

- **Smart operators need to include security in their governance model in order to define liabilities.**
- **Need to develop a harmonized scheme to ensure/evaluate security.**
- **Security to be included in all stages of the life cycle of products and services.**
- **IoT Security should reuse existing good practices from other sectors.**
- **Consider network connectivity in regard to IoT security.**
- **Operators and other IoT stakeholders often do not have security expertise, awareness must be raised.**

IoT Security Recommendations (2)

- **New provision of GDPR, NISD and future telecom code must be taken into account:**
  - **NISD**: NO special mentions about IoT; NISD focus on services, same treatment applied when IoT is involved.
  - **New Telecom Code**: NO special mentions about IoT; Code focuses on services, networks + OTT; same treatment applied when IoT is involved.
  - **GDPR**: NO special mentions, but we must consider:
    - User consent must be obtained
    - Data protection by design and by default
    - Right of access by the data subject (+erasure, right to be forgotten …)
    - Processing data relating to children
    - Security breaches notification

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu