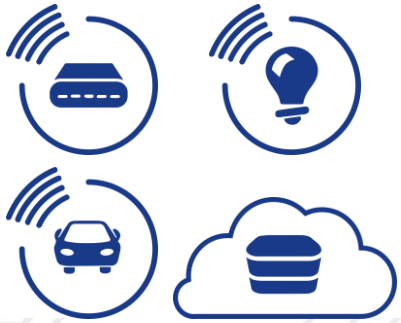


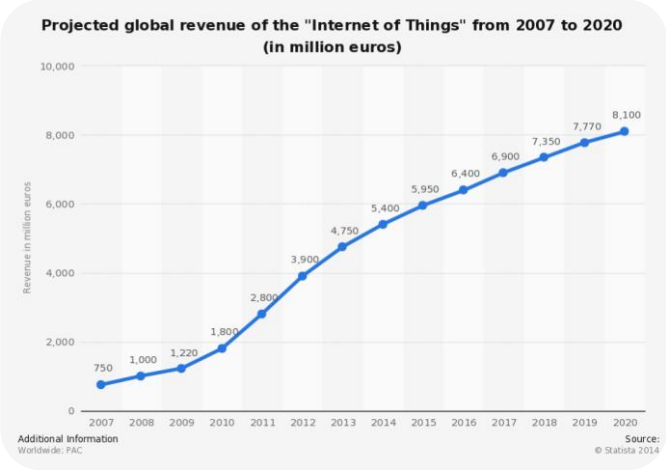
ENISA work to secure IoT

ENISA - NLO Meeting | Athens | 8 June 2016

Dr. Cédric LÉVY-BENCHETON | NIS Expert | @clevybencheton

European Union Agency for Network and Information Security

Everything becomes connected



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?)

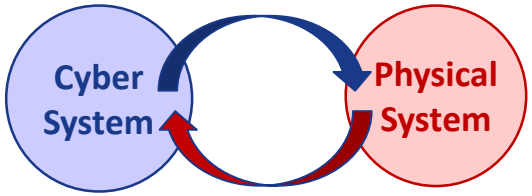
- Connectivity is needed, mobility is important
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities than non-IoT product, reasonable price
- Non-connected version is not available

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



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

ENISA and IoT security

Smart Cities

SCADA
and Industry 4.0

Smart Homes

eHealth

Intelligent
Public Transport

Smart Cars

Smart Airports

Definition of the perimeter

- Devices
- Data exchange (including network infrastructure)
- Local and remote services (*e.g.* Cloud, etc.)

ENISA develops expertise to secure IoT

- Evaluation of threats
- Promotion of security good practices
- Stakeholders engagement
- Awareness raising
- Community expert groups
- Liaison with policy makers

ENISA provide guidance to secure IoT against cyber threats

Security measures for IoT

Common IoT security measures

- Employ security and privacy by design
- Integrate security in the governance model
- Improve the awareness level at every level of the organisation
- Do not redevelop cryptography!
- Collaborate and exchange information with other actors

Sectorial aspects

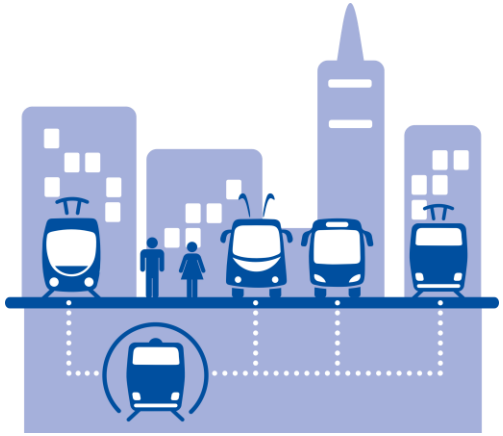
- Identify critical assets
- Define minimum security measures for procurement
- Separate critical systems from non-critical
- Coordinate with CSIRTs
- Engage in staff training

IoT security goes beyond technical

Challenges toward a secure IoT

Future actions to enhance IoT security

- Identify good security practices per sector (ENISA)
- Promote harmonisation
- Need for specific risk assessment methods
- Establish a framework to assess IoT security



Incentives for IoT security

- Consider security as a business enabler
- Improve the preparedness level
- Anticipate regulation (e.g. NIS Directive)

IoT security will lead to a safer society

ENISA work to secure Smart Cars

Actions

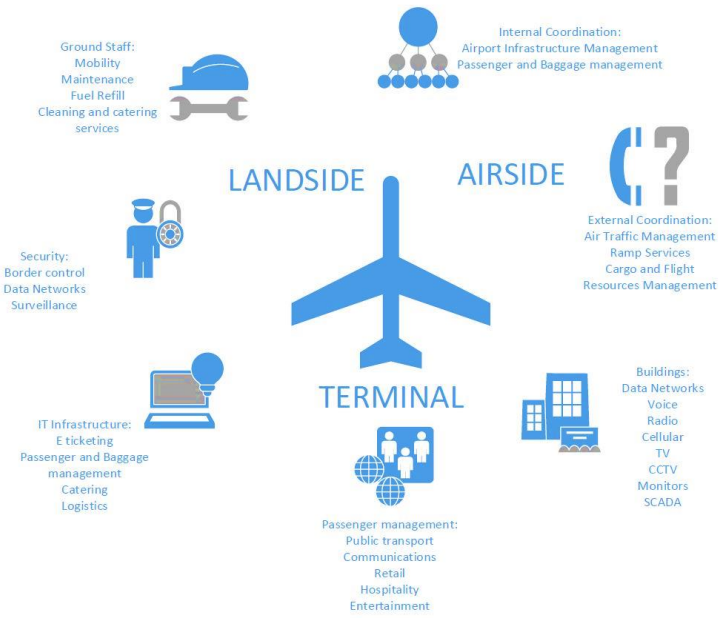
- Deliverable: good practices and recommendations
- Engage with the community: validation workshop, CaRSEC expert group
- Collaboration with the European Commission (C-ITS, AIOTI)

Objectives

- Secure the entire life cycle of smart cars
- Security measures go beyond technical (organisation, policy)
- Raise awareness of manufacturers and suppliers

Secure Smart Cars to ensure the safety of citizens

ENISA work to secure Smart Airports



Actions

- Deliverable: good practices and recommendations
- Validation workshop

Objectives

- Improve security and resilience of airports and air traffic control
- Prevent disruptions that could have an impact on the service and on the passengers

Secure assets and dependencies to ensure safety of air travel

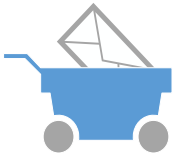
ENISA work to secure Smart Hospitals

Hospital Staff:
Mobility
Tele monitoring
Collaboration

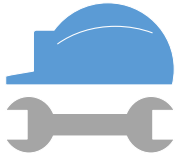
Devices
Surgical devices
Bedside medical devices
Monitoring devices

Core Systems:
Health Information
Laboratory Info
Radiology Info
Referral & Discharge
ePrescription

SMART HOSPITALS



Data
Electronic Health Record
Clinical data repository
PACS



Core Infrastructures
High speed reliable network
Identification technology
Sensor networks
Embedded systems

Actions

- Deliverable: good practices and recommendations
- Validation workshop

Objectives

- Improve security and resilience of hospitals information systems
- Identify common cyber security threats and challenges and,
- Present mitigation measures to address them

Secure devices and systems to improve patients' safety

Conclusions

IoT security is not a *one-size fits all* solution

- Common security measures
- Specific sectorial measures
- No real guidance today

ENISA promotes IoT Security

- Develop awareness and training on IoT threats and risks
- Assume that dependencies are/can be compromised
- Anticipate future regulation
- Make security a feature!

IoT security is not an option!

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu