Securing Europe's IoT Devices and Services

Dr. Evangelos OUZOUNIS | Head of Unit - Secure Infrastructure and Services

Validation Workshop | Berlin | 16 October 2015

Positioning ENISA activities

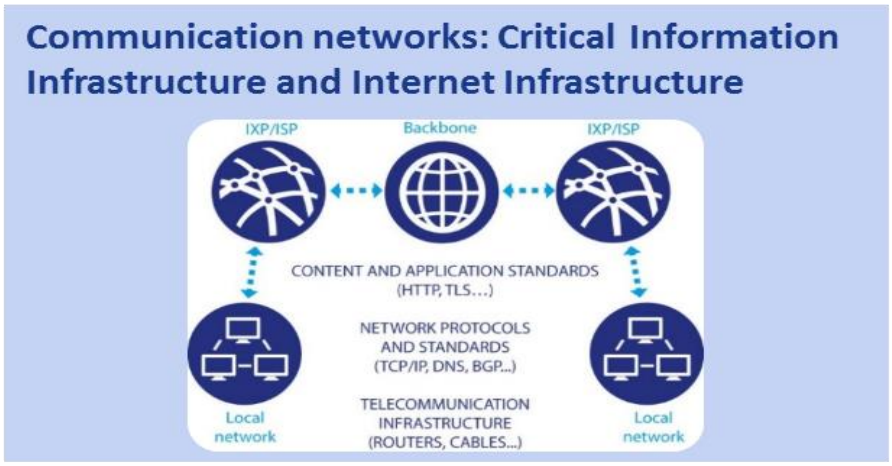
Emerging Threat Environment

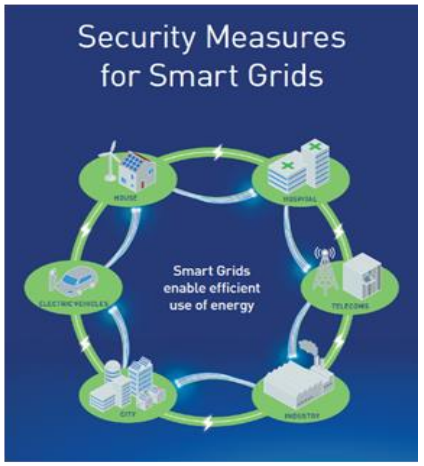
- significant physical disasters affecting CIIs
- complex networks and services
- low quality of software and hardware
- asymmetric threats allowing remote attacks
- increasing organised cybercrime and industrial espionage
- lack of international agreements and regimes,
- lack of well functioning, international operational mechanism

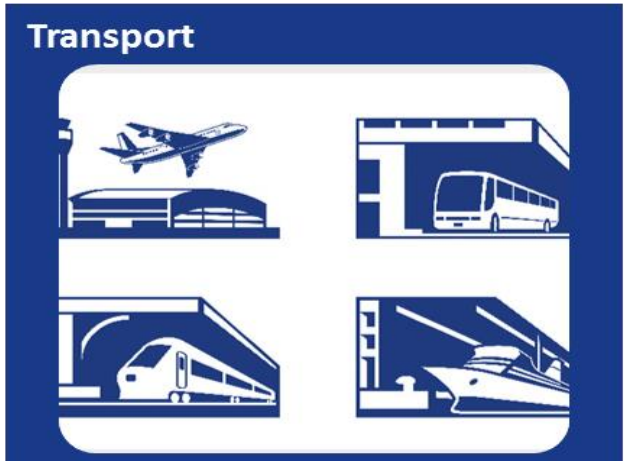
EU Policy Context – Resilience and CIIP

- ENISA II – new mandate ☑
- Proposal for a NIS Directive 👍
- eIDAs Directive – article 19 ☑
- EU Cyber Security Strategy (COM) ☑
- EU Cloud Computing Strategy and Partnership (COM) ☑
- Telecom Package – article 13 a, art. 4 ☑
- EU's CIIP action plan ☑
- Digital Single Market ☑
- Alliance for Internet of Things Innovation ☑

Secure Infrastructure and Services







Like curling

Secure Infrastructure and Services

Policy implementation

- Incident Reporting (Article 13a, Article 19), technical expertise

Enhance the level of security

- Minimum security measures, recommendations

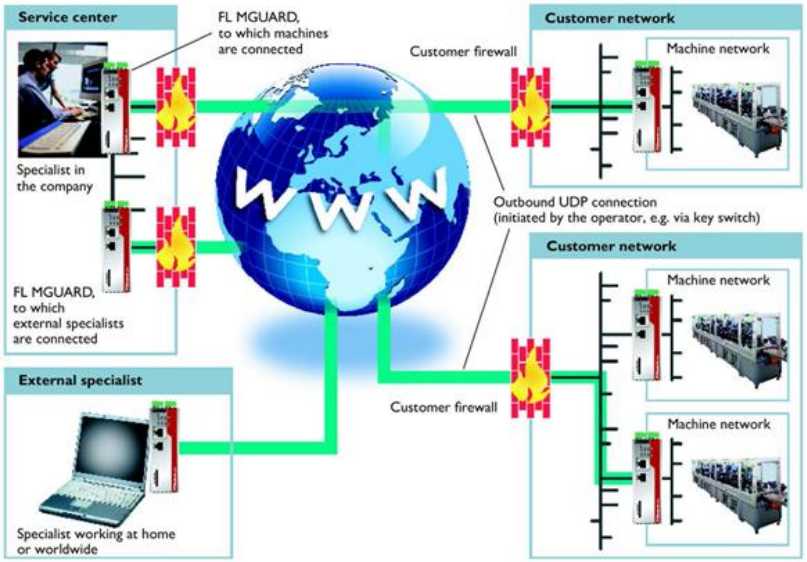
Community engagement

- Expert reference groups, workshop organisation

Domains of expertise

- ICT systems (Cloud, electronic communications)
- Critical infrastructure (Transport, Smart Grids, Finance, ICS/SCADA)
- Emerging technologies (Smart Cities, Smart Homes, eHealth)

Industry 4.0



Increased connectivity to the Internet

Great impact in case of attack

New types of attacks (APT…)

Cascading effects due to interconnection of critical infrastructures

eHealth Cyber Security

Security and Resilience in eHealth infrastructures and services

- Critical information infrastructures protection (incident-impact)

Scope

- Health information networks as critical infrastructures
- Health jurisdictions responsible
- Electronic health records (focusing mostly on availability and integrity of the data stored and exchanged)

ENISA's domains of interest

- eHealth and Cloud Computing
- Smart hospitals
- Big Data for health records

Smart Infrastructures Cyber Security

Threats with consequences on the society

- ICT Dependency generalised
- Data exchange integrated into business processes
- Cohabitation between legacy and new systems

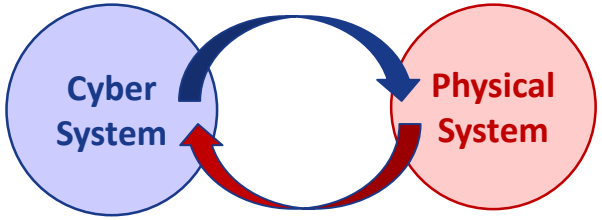
Cyber Security for Smart Infrastructures

- Raise awareness on existing threats
- Provide security guidance to industry
- Importance of cyber security for safety

ENISA's domains of interest

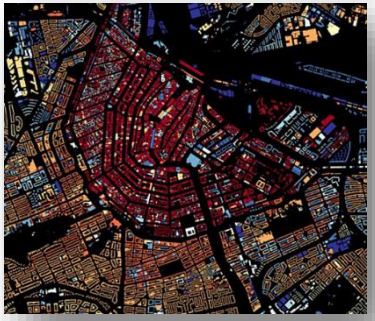
- Intelligent Transportation Systems
- Smart cars and connected roads
- Smart Homes
- Smart Airports

Defining IoT Security



IoT is a Smart Infrastructure

- Rely on data exchange and data processing
- Usage of cyber-physical systems (sensors/actuators)



Objectives

- Dynamic adaption of services
- Reduction of operational expenditure
- Improvement of the global quality of life

Following a sectorial/service driven approach

Important to secure Smart Infrastructures and citizens against cyber threats

IoT Security at ENISA

Smart Cities

Smart Homes

Intelligent Transportation Systems

SCADA and Industry 4.0

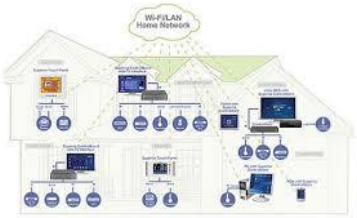
eHealth

Emerging threats target

- Data collection, data exchange and data processing
- Cyber-physical systems with a potential impact on citizens
- Dependences and existing technologies (Cloud, ICS/SCADA…)

ENISA engages in several communities with specific cyber security needs

ENISA's Threat Landscape for Smart Homes (2014)



Source: nanjingiot.wordpress.com

Smart Home is unsecure

- Several cyber threats to Smart Home Environments
- Multiple devices, OS, networks, protocols…
- Interdependences between devices and services

Several limitations to Smart Home security

- Limited knowledge of security by manufacturers/vendors
- Difficult to implement security for many reasons: technical, economical, lack of harmonisation…
- No regulatory framework for liabilities

Good Practices and Recommendations for Smart Homes (2015)

Basic measures increase security in Smart Homes

⇨ Need to promote and extend security good practices

Conclusion

Importance of IoT in Europe

- New business models appear with IoT
- Usage increases in critical sectors
- Yet, lack of harmonisation for security

ENISA promotes Cyber Security for IoT

- Developing sectorial expertise
- Promoting security good practices
- Engaging stakeholders

Cyber Security of IoT is an opportunity for the European Union

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu