Securing Smart Infrastructures – From Smart Homes to Smart Cities

Udo Helmbrecht | Executive Director

Summer School | Hersonissos | 2 July 2015

European Union Agency for Network and Information Security

Sommaire

1 Introduction

2 Securing Smart Infrastructures: several approaches

3 From Smart Homes to Smart Cities

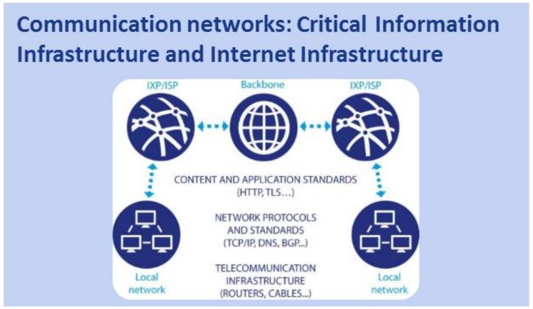
4 Conclusion

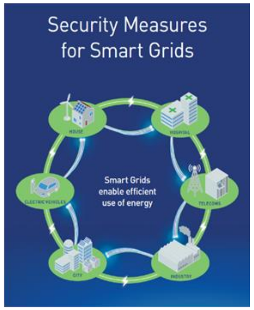
Introduction

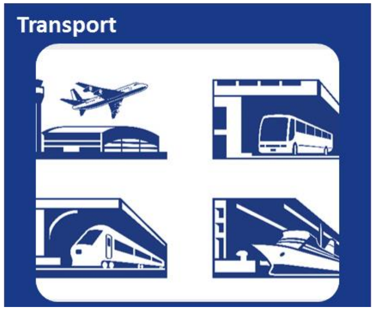
Securing Infrastructures and Services

- Critical Infrastructures
- Critical Information Infrastructure

enisa
Annual studies
Community engagement
SECURING EUROPEAN NETWORKS
Workshops
INFRASEC ENISA Internet infrastructure security and resilience reference group


Communication networks: Critical Information Infrastructure and Internet Infrastructure
IXP/ISP
Backbone
IXP/ISP
CONTENT AND APPLICATION STANDARDS (HTTP, TLS…)
NETWORK PROTOCOLS AND STANDARDS (TCP/IP, DNS, BGP…)
TELECOMMUNICATION INFRASTRUCTURE (ROUTERS, CABLES…)
Local network
Local network


Security Measures for Smart Grids
HOUSE
HOSPITAL
ELECTRIC VEHICLES
TELECOMS
Smart Grids enable efficient use of energy
CITY
INDUSTRY

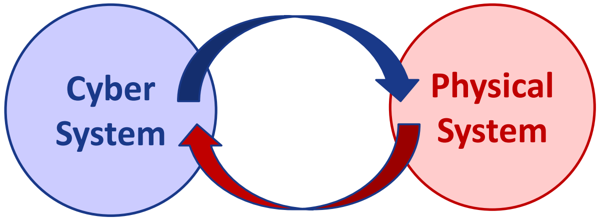


ENHANCING THE SECURITY OF ICS SCADA IN EUROPE
ENERGY
WATER
TRANSPORT
SHIPPING
CHEMICALS
MANUFACTURING
INDUSTRIAL CONTROL SYSTEMS
SUPERVISORY CONTROL AND DATA ACQUISITION

Overview of critical infrastructures (UE28 + EFTA)

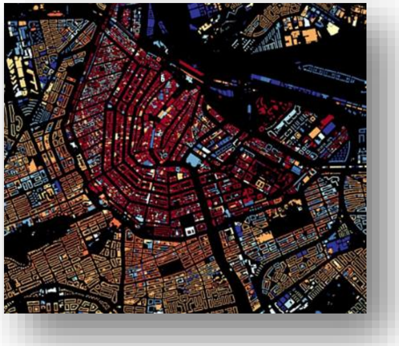
Sectors	Energy	ICT	Water	Food	Health	Financial	Public & Legal Order	Civil Admin.	Transport	Chemical & Nuclear Industry	Space & Research	Other
AU	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
BE	✓	✓				✓			✓			
CZ	✓	✓	✓	✓		✓		✓	✓			Emergency services
DK	✓	✓		✓	✓				✓			
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓			Rescue services
FI	✓	✓	✓	✓	✓	✓	✓		✓			
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	Industry
DE	✓	✓	✓	✓	✓	✓	✓		✓			Media & Culture
EL	✓								✓			
HU	✓	✓	✓	✓	✓	✓	✓		✓			Industry
IT	✓								✓			
MT	✓	✓			✓	✓		✓	✓			
NL	✓	✓	✓	✓		✓	✓	✓	✓	✓		
PL	✓	✓	✓	✓	✓	✓		✓	✓	✓		Rescue systems
SK	✓	✓	✓		✓				✓			Industry Postal
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
UK	✓	✓	✓	✓	✓	✓		✓	✓			Emergency services
CH	✓	✓	✓	✓	✓	✓		✓	✓			Industry

Defining a Connected Infrastructure



A connected infrastructure…

- Data exchange between services
- Usage of cyber-physical systems (sensors/actuators)
- Examples : Smart Grids, Smart cities…



Objectives

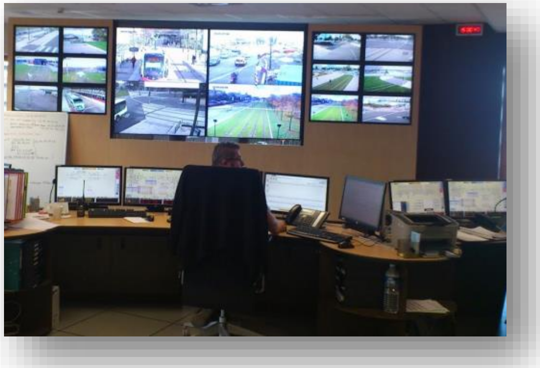
- Dynamic adaption of services
- Reduction of operational expenditure
- Improvement of the global quality of life

Important to secure Smart Infrastructure against cyber threats

Securing Smart Infrastructures

Several approaches

On the importance of securing smart infrastructures



New and emerging risks

- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (*legacy*) systems

Threats with consequences on the society

- Economical consequences, but not only
- Smart Infrastructures' operators' are not security experts
- Lack of clarity on the concept of "cyber security"

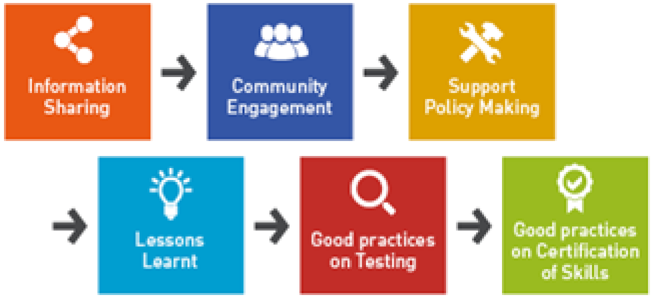
Cyber security measures are not only technical but also operational and organisational

How to secure Smart Infrastructures?

Several actions are possible

- Usually, after a risk assessment
- Who is responsible? What role for everyone?
- Who invest? Why invest?

ENISA is leading several actions in this direction



- Threat landscape
- Regulation and incident sharing
- Good practices and recommendations
- Collaboration with all stakeholders

Smart Operator secure their infrastructures and services
Citizens are protected from cyber threats

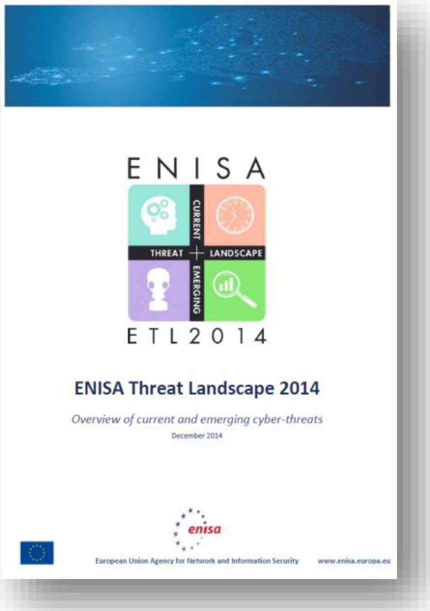
ENISA Threat Landscape

Threats are always evolving

- Target: all sectors of our life

This document to help risk assessment

- Evaluate the assets exposed
- Prioritise investments



ENISA

CURRENT

THREAT LANDSCAPE

EMERGING

ETL2014

ENISA Threat Landscape 2014

Overview of current and emerging cyber-threats

December 2014

enisa

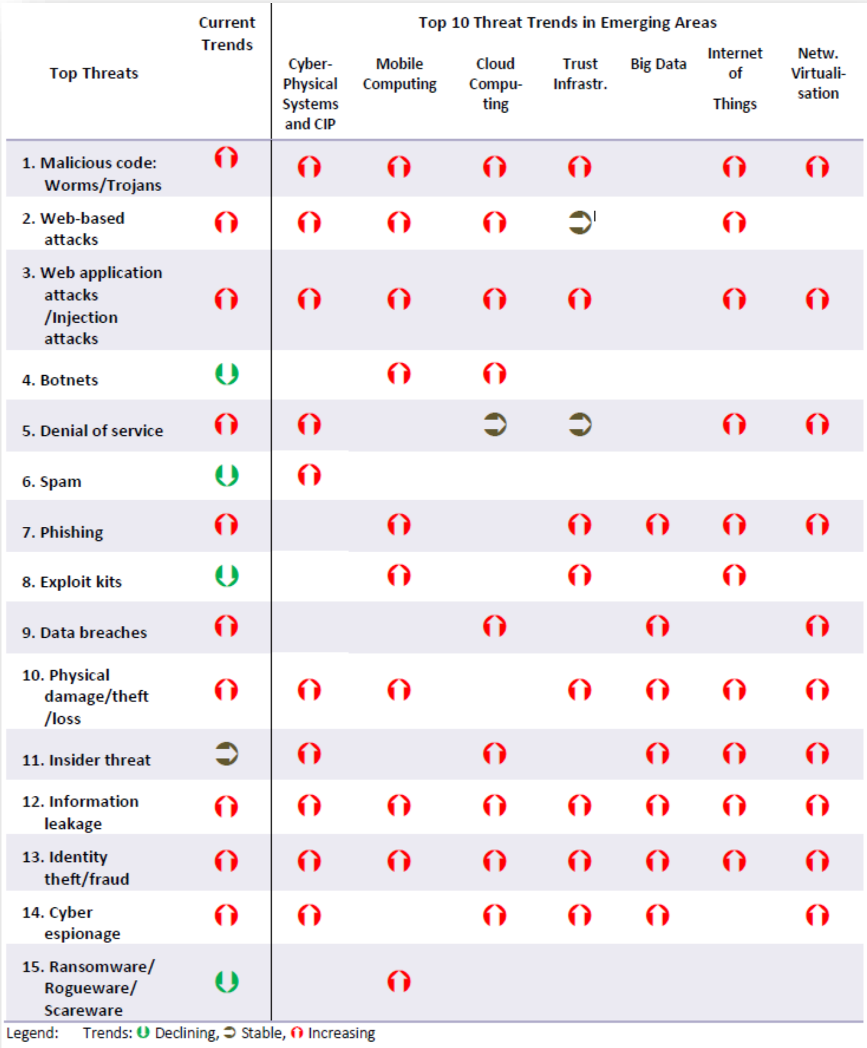
European Union Agency for Network and Information Security

www.enisa.europa.eu

ENISA “Threat Landscape” 2014

- Focus on current and emerging threats per type of technology
- Two technical “deep dives”: Internet Infrastructure and Smart Homes

Top Threats 2014



Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

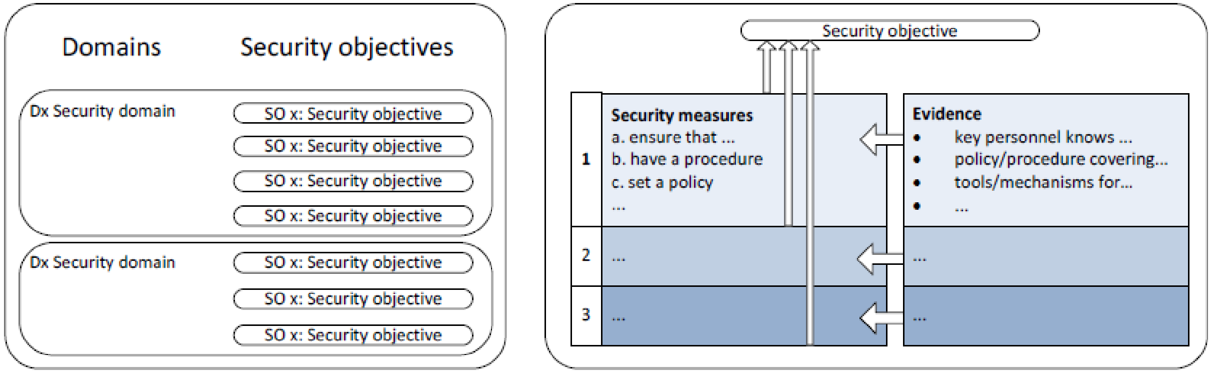
Regulation

Regulation provides high level requirements

- Prone to interpretation
- No tangible action

ENISA provides guidance to the public and private sectors

- Coordination at EU level
- Definition of security objectives and associated security measures



Domains

Security objectives

Dx Security domain

SO x: Security objective

SO x: Security objective

SO x: Security objective

SO x: Security objective

Dx Security domain

SO x: Security objective

SO x: Security objective

SO x: Security objective

Security objective

	Security measures	Evidence
1	a. ensure that ... b. have a procedure c. set a policy ...	• key personnel knows ... • policy/procedure covering... • tools/mechanisms for... • ...
2	...	...
3	...	...

Structure for security objectives and associated security measures

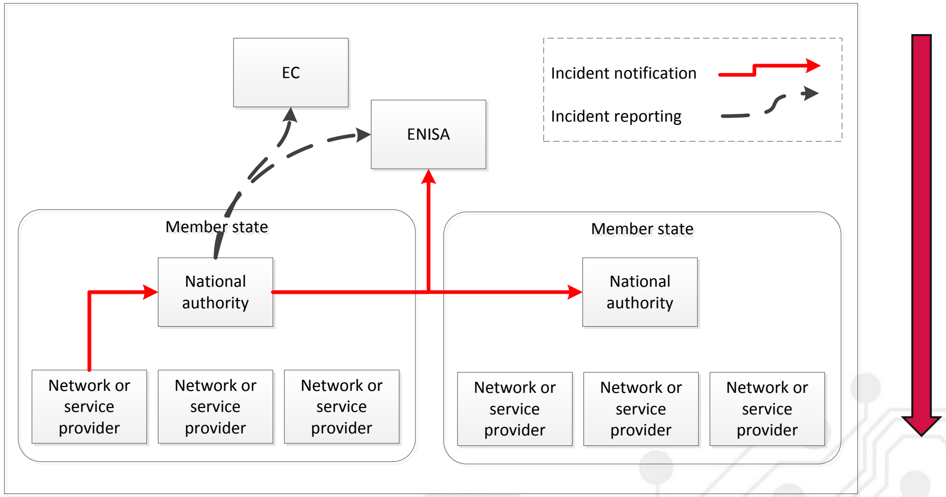
Incident sharing

Obligation to report incidents

- Electronic Communications — Article 13a of the Telecom Framework Directive (2009/140/EC)
- Personal Data Breach — Article 4 of the Privacy Directive (2002/58/EC)

Incident sharing can improve security

- Root causes analysis
- Dissemination of good practices


EC
ENISA
Incident notification
Incident reporting
Member state
National authority
Network or service provider
Network or service provider
Network or service provider
Member state
National authority
Network or service provider
Network or service provider
Network or service provider

Incidents are analysed and conclusions are shared with electronic communication operators

Good practices and recommendations

Methodologies for the identification of Critical Information Infrastructure assets and services

Guidelines for charting electronic data communication networks

December 2014

enisa

European Union Agency for Network and Information Security

www.enisa.europa.eu

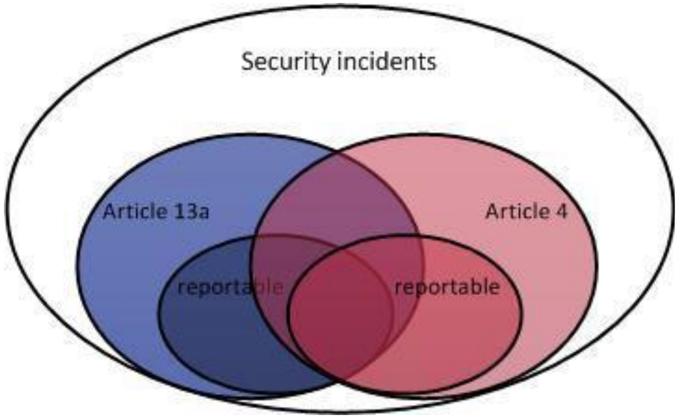
Enhance the baseline security level

- Sectorial approach
- List security measures and their level of applicability
- Validation by experts

Objectives of these recommendations

- Reduce the existing needs and gaps
- Addressed to one or several stakeholders
- Can be high level or very technical

Collaboration between stakeholders



Collaboration before regulation

- Share incidents and good practices
- Incentive to invest

Collaboration in Europe

- Public Private Partnerships (*e.g.* NIS Platform)
- Sectorial ISACs (*e.g.* FI-ISAC)
- Trust groups (*e.g.* ENISA Reference groups)

Preparatory to future regulations (*e.g.* NIS Directive)

- Enhance the global security level
- Spread investments over time
- Facilitate future compliance

From Smart Homes to Smart Cities

What is a Smart Home?

Connected devices

- Data acquisition and processing
- Actions on the environment

Connected users

- Interface for command & control
- Adaption to the environment

Towards an automation of the home
for an improved quality of life (comfort, energy reduction…)

Why secure Smart Homes?

Integration of several devices in one shared environment

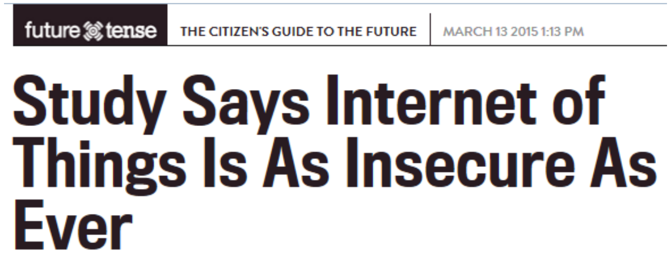
- Several manufacturers
- Different economical models
- Heterogeneity of software, protocols, architectures

Security is limited

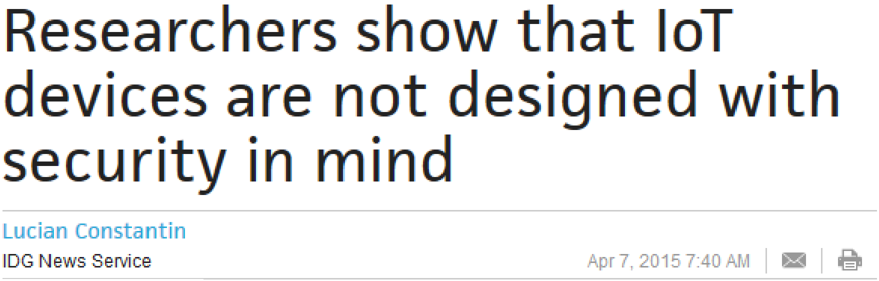
- Multiple vulnerabilities
- Lack of investment (manufacturers and buyers)
- Lack of transparency for security management

A cyber attack has consequences (direct or indirect) on the Smart Home and its inhabitants

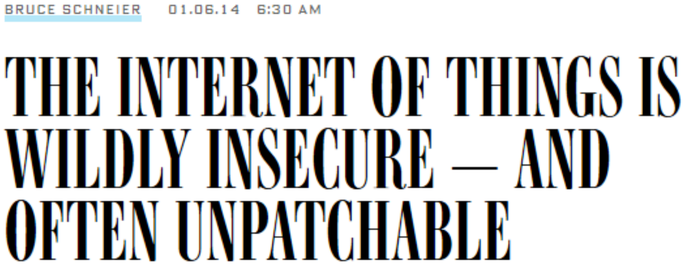
In the press, and it's worrying…


future tense | THE CITIZEN'S GUIDE TO THE FUTURE | MARCH 13 2015 1:13 PM

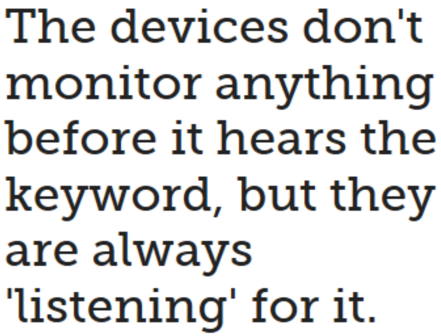
Study Says Internet of Things Is As Insecure As Ever

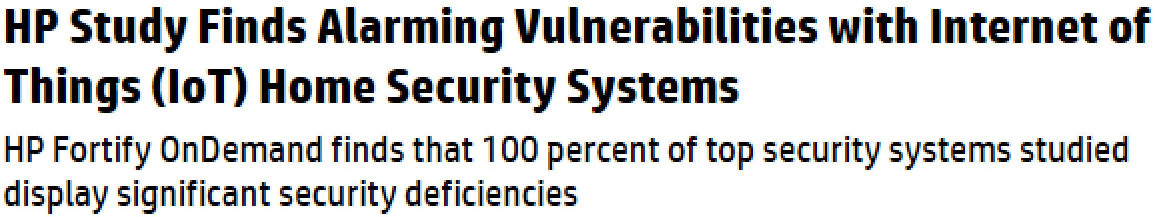

Researchers show that IoT devices are not designed with security in mind

Lucian Constantin
IDG News Service
Apr 7, 2015 7:40 AM


BRUCE SCHNEIER 01.06.14 6:30 AM

THE INTERNET OF THINGS IS WILDLY INSECURE — AND OFTEN UNPATCHABLE

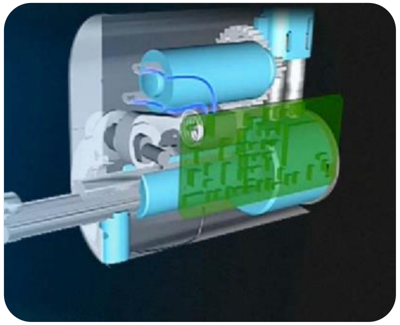

The devices don't monitor anything before it hears the keyword, but they are always 'listening' for it.


HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems

HP Fortify OnDemand finds that 100 percent of top security systems studied display significant security deficiencies

ENISA Threat Landscape for Smart Homes

TV recording all conversations



Hacking Smart Locks to open doors

No device is fully secured

- Dependency to external services
- Design of IoT/connected devices
- Vulnerabilities of protocols

Non-technical threats

- Cost reduction during design/manufacturing
- Economical model (*e.g.* selling private data…)
- Potential risks on health and safety

By design, a Smart Home is prone to several threats

Real physical threats

Impact on life, health and safety

- Failure or attack on devices?

Criminal usage of IoT and Smart Homes

- “Virtual” crime
- Physical crime difficult to prove (e.g. robbery with no proof)

Continuity of service in case of a disaster

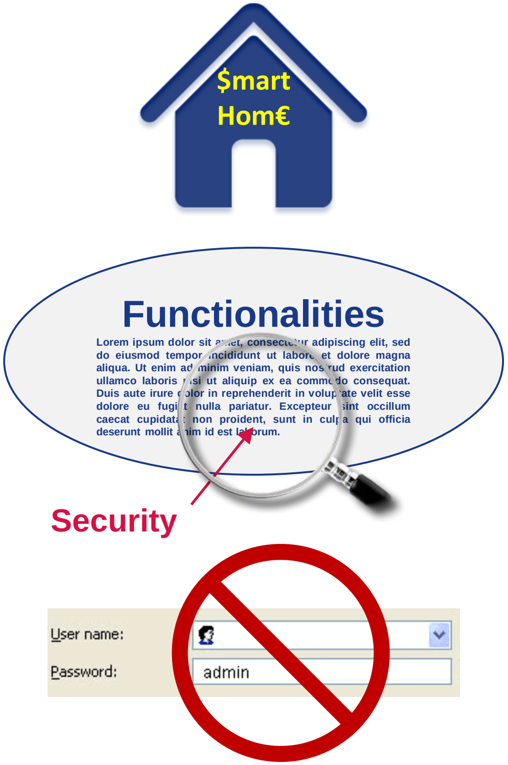
- Impact on the Smart Home environment?

Usage in case of emergency?

- How could IoT devices help first aid / emergency services?

A lack of legal framework defining liabilities in Smart Homes

A questionable approach of security



Technical

- Choice and implementation of protocols

Economical

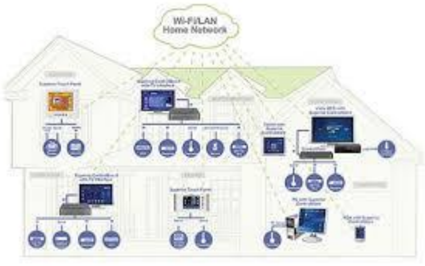
- Low incentive to integrate security
- Long term support of devices vs rapid evolution

Cultural

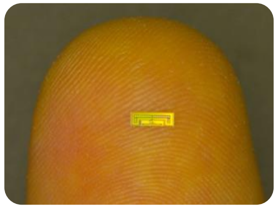
- Functionalities before security (product before end-user)
- Lack of collaboration industry/research. On the contrary, several lawsuits were initiated against security researchers.

No major attack to this day
⇨ Limited integration of security in the lifecycle of IoT

A need of harmonisation in security



Source: nanjingiot.wordpress.com



IoT Radio (Stanford)

The life cycle of Smart Home devices

- Conception: security of components and frameworks?
- Integration: security of the whole system?
- Disposal: confidentiality of private data?

Mobility and pervasiveness of IoT devices

- Multiple networks and protocols
- Interdependences between devices and services

Components limitations

- Low processing power, lack of bandwidth capacity
- Evolution and patching against vulnerabilities?

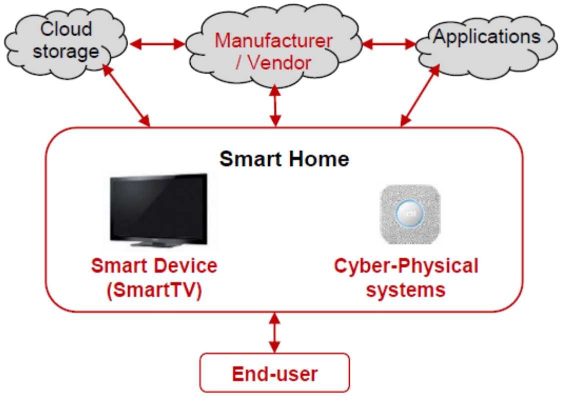
Basic measures increase security in Smart Homes

⇨ Need to consider security by design

ENISA's work to secure Smart Homes

Secure interconnection of devices

- Access to private data
- Possible risk for health and safety
- Limited security in existing devices



Objectives and scope (in red)

- Secure the life cycle of IoT devices
- Raise awareness for manufacturers, vendors
- Advise buyers

ENISA's work to secure Smart Cities

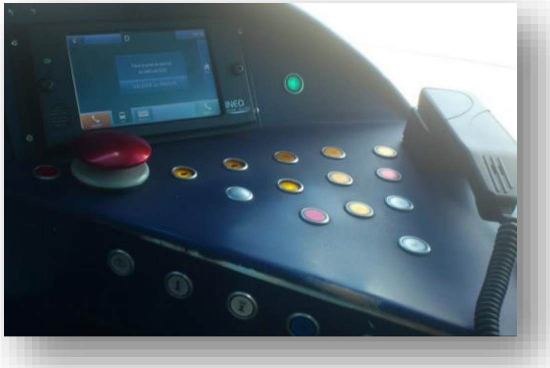
A wide range of operators

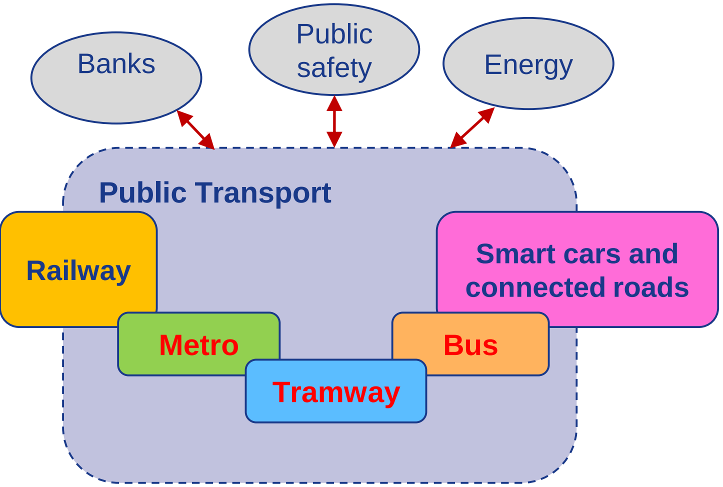
- Cohabitation between different systems
- Data gathering, processing, exchange
- Cyber physical systems

Secure different domains of Smart Cities

- Public Transport Systems
- Smart Cars and connected roads
- Smart Grids and energy systems

ENISA's work to secure Public Transport





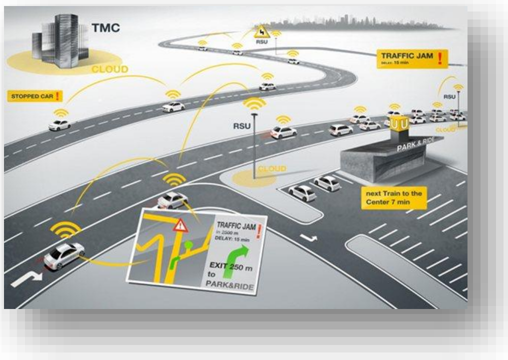
Current status of cyber security

- Diversity of systems
- Independence between sub-systems
- Lack of UE-wide harmonisation

Objectives and scope (in red)

- Secure exchanges in the Smart Cities between transport operators and other operators
- Secure critical systems for transport operators
- Raise awareness for manufacturers/vendors
- Advise policy makers

ENISA's work to secure smart cars and connected road infrastructure



Several systems to secure

- In-car systems
- Connected road infrastructure (Speed regulation, Traffic lights…)
- Autonomous cars

Objectives and scope

- Promote good practices for security
- Focus on security by design
- Advise policy makers
- Protect EU citizens

Conclusion

Conclusion

ENISA aims at enhancing the baseline level of cyber security

- A practical approach
- Beyond technical measures
- Integrating all stakeholders

Security of Smart Infrastructures is important

- Rapid technological evolution
- Impact on the economy and on EU citizens
- Need for harmonisation across the EU

ENISA promotes a pragmatic approach for enhanced cyber security

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu