Enhancing infrastructure cybersecurity in Europe

Rossella Mattioli
Secure Infrastructures and Services

European Union Agency for Network and Information Security
Securing Europe’s Information society
Positioning ENISA activities
Secure Infrastructure and Services

Communication networks: Critical Information Infrastructure and Internet Infrastructure

- CONTENT AND APPLICATION STANDARDS
  - (HTTP, TLS...)
- NETWORK PROTOCOLS AND STANDARDS
  - (TCP/IP, DNS, BGP...)
- TELECOMMUNICATION INFRASTRUCTURE
  - (ROUTERS, CABLES...)

Transport

- eHealth and Smart Hospitals

Finance
Cybersecurity for ICS SCADA

Protecting Industrial Control Systems. Recommendations for Europe and Member States

Can we learn from SCADA security incidents?

Window of exposure... a real problem for SCADA systems?

Good Practices for an EU ICS Testing Coordination Capability

Certification of Cyber Security skills of ICS/SCADA professionals

EuroSCSIE

ICS Security Stakeholder Group

Good practices on Testing

Good practices on Certification of Skills

Information Sharing

Community Engagement

Support Policy Making

Lessons Learnt

https://www.enisa.europa.eu/scada
Communication network dependencies for ICS SCADA

- **Outlined scope and perimeter with EICS SG and EUROSCSIE experts**
- Map assets and threats via desktop research and interviews with security researchers and asset owners
- List all possible attacks coming from network exposure
- Examine protocols vulnerabilities
- List good practices
- Develop 3 attack PoCs and mitigation actions
- Define recommendations for
  - Infrastructure operators
  - Vendors
  - EU Member States
  - European Commission
IoT and Smart
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

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
An increasing number of threats

Study Says Internet of Things Is As Insecure As Ever

08 IoT Reality: Smart Devices, Dumb Defaults

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

The Internet of Things has a vision problem

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

“Internet of Things” security is hilariously broken and getting worse
Threat taxonomy for IoT

- Failures
  - Malfunctions
- Acts of Nature
  - Disasters
- Physical attacks
- Unintentional damage
  - (accidental)
- Damage/Loss
  - (IT Assets)
- Nefarious Activity
  - Abuse
- Outages
- Eavesdropping
  - Interception
  - Hijacking
- Legal
- Insider threat
How to secure IoT?

Generic good practices

- Raise awareness of manufacturers and suppliers
- Define security management at organisational level
- Develop information exchange on threats and risks
- Promote a common cyber security framework
- Reuse existing good practices from other domains

ENISA to provide guidance to secure the lifecycle of IoT

- Develop cross-sector baseline security measures
- Develop sectorial good practices
- Foster information exchange through ENISA Experts Groups

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

• Manufacturers don’t invest in security
• Security and privacy are closely linked
• Difficult to secure the entire lifecycle of products

ENISA proposes to:

• Establish security procurement guidelines
• Define a framework to evaluate the security of products
• Support security-driven business models

https://www.enisa.europa.eu/smartinfra
Securing Smart cities and transport infrastructure
Smart Cities as a “system of systems”

New and emerging risks
- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (legacy) systems
- Data exchange integrated into business processes

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
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 IPT 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
Existing status of security for IPT is limited

- Safety does not integrate security
- Security is not well integrated in organisations
- Awareness level is low

Yet, it is possible to act today

- Understand the threats to critical assets
- Assess applicable security measures
- Collaborate to enhance cyber security

ENISA aims at providing pragmatic solutions to secure transport infrastructure in Europe
Cybersecurity for Smart Cars

- Increased attack surface
- Insecure development in today’s cars
- Security culture
- Liability
- Safety and security process integration
- Supply chain and glue code
Preliminary Findings - Smart Cars

- Improve cyber security in smart cars
- Improve information sharing amongst industry actors
- Improve exchanges with security researchers and third parties
- Clarify liability among industry actors
- Achieve consensus on technical standards for good practices
- Define an independent third-party evaluation scheme
- Build tools for security analysis
The objective of this study is to improve the security and resilience of airports and air traffic control to prevent disruptions that could have an impact on the service being delivered and on the passengers.

Workshop November 2016
Publication Q4 2016
Perimeter of the study

The goal is to cover the entire IT perimeter of smart airports:

- Assets inside the airport
- Connected assets outside the airport
- Dependencies on the airway
Threat modelling

- **Human Errors**
  - Configuration errors
  - Operator/user errors
  - Loss of hardware
  - Non compliance with policies or procedures

- **Third Party Failures**
  - Internet service provider
  - Cloud service provider (SaaS / PaaS / SaaS)
  - Utilities (power / gas / water)
  - Remote maintenance provider
  - Security testing companies

- **Malicious Actions**
  - Denial of Service attacks
  - Exploitation of (known or unknown) software vulnerabilities
  - Misuse of authority / authorisation
  - Network interception attacks
  - Social attacks
  - Tampering with devices
  - Breach of physical access controls / administrative controls
  - Malicious software on IT assets (including passenger and staff devices)
  - Physical attacks on airport assets

- **System Failures**
  - Failures of devices or systems
  - Failures or disruptions of communication links (communication networks)
  - Failures of parts of devices
  - Failures or disruptions of the main supply
  - Failures or disruptions of the power supply
  - Malfunctions of parts of devices
  - Malfunctions of devices or systems
  - Failures of hardware
  - Software bugs

- **Natural Phenomena**
  - Earthquakes
  - Floods
  - Solar flare
  - Volcano explosion
  - Nuclear incident
  - Pandemic (e.g. ebola)
  - Industrial actions (e.g. strikes)
  - Fires
  - Shortage of fuel
  - Space debris & meteorites
Attack scenarios

- Drone intercept as mobile vehicle for jamming and spoofing aircraft-airport and traffic control- airline communications
- Tampering with airport self-serving e-ticketing systems
- Network attack to the baggage handling

- Drone intercept as mobile vehicle for jamming and spoofing aircraft-airport and traffic control- airline communications
- Tampering with airport self-serving e-ticketing systems
- Network attack to the baggage handling
Preliminary Findings – Smart airports

- Variety of cyber security practices in airports
- Lack of EU regulations on cyber security of airports
- Lack of guidelines on network architecture, ownership, and remote management
- Evidence-based vulnerability analysis metrics and priorities
- Threat modelling and architecture analysis
- Information sharing
- Multi-stakeholder enable security technologies
- Appropriate Security Governance model
- Skillset of experts – safety vis a vis security
Recommendations

ENISA recommendations

• Propose solutions to enhance cyber security
• Targeted at Policy makers, transport Operators, Manufacturers and Service providers

Key recommendations (excerpt)

• Promote collaboration on cyber security across Europe
• Integrate security in business processes
• Develop products integrating security for safety

Cyber security for Transport requires a global effort
How you can get involved

• Studies

• Events:
  • Network attacks to ICS SCADA - 27th of September - Frankenthal
  • Securing Smart Cars – 10th of October - Munich
  • NISD and ICS SCADA skills - 26/28th of October - Stockholm

Open call for experts:

• CARSEC Smart Car security expert group
• TRANSSEC - Intelligent Public Transport Resilience and Security Expert Group
• ENISA ICS Security Stakeholder Group
• EuroSCSIE - European SCADA and Control Systems Information Exchange

https://resilience.enisa.europa.eu/
The road ahead
The Network and Information Security Directive

**Scope:** to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

**Status:** 17 May 2016, the Council approved its position at first reading. The next step is approval of the legal act by the European Parliament at second reading. The directive entered into force in August 2016. 21 months after entry into force from transposition

**Provisions:**

- Obligations for all MS to adopt a national NIS strategies and designate national authorities.

- Creates first EU cooperation group on NIS, from all MS.

- Creates a EU national CSIRTs network.

- Establishes security and notification requirements for operators of essential services and digital service providers
The NIS Directive

Digital Service Providers

- Cloud Computing Services
- Online Marketplaces
- Search Engines

Operators of Essential Services

- Incident Reporting
- Security Requirements

Strategic Cooperation Network

Tactical/Operational CSIRT Network

National Cyber Security Strategies

- Transport
- Energy
- Healthcare
- Banking and Financial market infrastructures
- Digital Infrastructure

ENISA’s overall role and contribution

- Assist MS and EU Comm by providing expertise/advice and by developing/facilitating exchange of good practices, e.g.
  - assist MS in developing national NIS Strategies (NCSS)
  - assist EU Commission and MS in developing min security requirements for ESOs and DSPs
  - assist EU Commission and MS in developing incident reporting frameworks for ESOs and DSPs
  - assist MS in the defining criteria for the designation of ESOs
- Be the secretariat of the CSIRT network and develop with members the network
- Participate/contribute to the work of the Cooperation Group (CG)
- Elaborate advices and guidelines regarding standardization in NIS security, together with MS
# NISD Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>entry into force + ...</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2016</td>
<td>-</td>
<td>Entry into force</td>
</tr>
<tr>
<td>February 2017</td>
<td>6 months</td>
<td>Cooperation Group begins tasks</td>
</tr>
<tr>
<td>August 2017</td>
<td>12 months</td>
<td>Adoption of implementing on security and notification requirements for DSPs</td>
</tr>
<tr>
<td>February 2018</td>
<td>18 months</td>
<td>Cooperation Group establishes work programme</td>
</tr>
<tr>
<td>May 2018</td>
<td>21 months</td>
<td>Transposition into national law</td>
</tr>
<tr>
<td>November 2018</td>
<td>27 months</td>
<td><strong>Member States to identify operators of essential services</strong></td>
</tr>
<tr>
<td>May 2019</td>
<td>33 months (i.e. 1 year after transposition)</td>
<td><strong>Commission report assessing the consistency of Member States' identification of operators of essential services</strong></td>
</tr>
<tr>
<td>May 2021</td>
<td>57 months (i.e. 3 years after transposition)</td>
<td>Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers</td>
</tr>
</tbody>
</table>
Goals

01 Raise the level of awareness on Infrastructure security in Europe

02 Support Private and Public Sector with focused studies and tools

03 Facilitate information exchange and collaboration

04 Foster the growth of communication networks and industry

05 Enable higher level of security for Europe’s Infrastructures
Thank you,

Rossella Mattioli

resilience@enisa.europa.eu

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