Lessons learned from EU funded projects SECRET and CYRAIL

CYBERSECURITY4RAIL,
Brussels, 04 October 2017

Marie-Hélène Bonneau, UIC Security Division
UIC today

- 200 Members in 100 countries
- Cooperation with over 100 institutions
- 700 UIC Leaflets, new International Railway Solutions (IRS)
- 85 congresses, conferences, workshops
Security at UIC

- Security platform: global level
  Current chair: DB AG
  Current vice chair: VIA RAIL CANADA

- 5 Working groups
  Human factors, Technologies, Strategy and regulation, Border crossing and international corridors, Sabotage-Intrusions-Attacks

- An annual worldwide congress and an annual security week
  2017 security congress in Potsdam, Germany on “Rail freight security door to door”
  2018 security congress will focus on “crisis management & resilience

- Research projects
  Provide rail companies with recommendations/toolbox
  Develop cooperation with other sectors at international level
Cyber security on rail: the challenges

- Rail Network is a critical infrastructure
- Rail Systems are more and more connected and open
- Rail Technologies are becoming more and more interoperable and harmonized
- Threats (human and technology based) are adapting quicker than traditional security detection methods
EU SECRET project

- Protection of railway infrastructure against EM attacks

  Duration: 01 August 2012 for 36 Months
  Budget: 4,268 M€ (3,059 M€ funding by EU)
  Coordinator: IFSTTAR (France)
  Partners: 10 Partners from 5 countries
EM attacks: definition

Case 1: The target is an electronic device
Permanent or Temporary Default on electronic devices = damaging or disrupting, confusing

Case 2: The target is to avoid the data transmission
Jamming the data transmission between the devices = disrupting or confusing the system
Objectives

- To assess the risks and consequences of EM attacks on the rail infrastructure
- To identify preventive and recovery measures
- To develop protection solution for EM attacks
- To produce technical recommendations to reinforce the railway infrastructure
About 40 recommendations

- Organisation
- Standardization
- Technical

3 categories of recommendations

- Prevention from EM jamming effects
- EM attack detection solution
- Mitigation of EM jamming effect

Available at http://www.secret-project.eu
Cybersecurity in the RAILway sector

- Duration: 1 Oct. 2016 - 30 Sept. 2018
- Estimated Budget: 1,500 000
- Coordinator: Evoleo
- Consortium: 6 partners from 5 countries
Goal

- Perform a cyber security assessment of the Railway systems
  - *What are the most critical railway services, zones and communications?*

- Deliver a taxonomy of threats targeting rail management and control systems
  - *What are the threats?*

- Assess and select innovative rail management systems attack detection techniques
  - *How to detect attacks targeting rail management systems?*

- Specify Countermeasures and Mitigation strategies for improved quality levels;
  - *How to prevent, how to make the system resilient*

**CYRAIL Structure**

**WP1 - Project Management**

<table>
<thead>
<tr>
<th>Study &amp; Assess</th>
<th>Detect</th>
<th>Act</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP2 - Operational Context and Scenarios</td>
<td>WP4 - Threat analysis, attack detection and early warning</td>
<td>WP5 - Mitigation and Countermeasures Specification</td>
<td>WP6 - Protection Profiles</td>
</tr>
<tr>
<td>WP3 - Security Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WP7 - Dissemination and Outreach**
On-going work: operational scenario

- Work led by UIC Rail System Department
- Definition of the operational scenario based on
  - different communication systems
  - smart rail transport technologies such as automatic train Location, train movement management, train data management, smart ticketing, ..
- Focus on signaling and communication system
Security Assessment Methodology for the railway domain

- Work led by the university of the Basque country: euskoiker

- No common European standard to define a security assessment methodology for rail

- Analysis of existing Cyber Security Assessment Methodologies

- Definition of a Security Risk Assessment Methodology based on ISO 62443 standard and ETSI TVRA
Added value

- Preventing cyber-attacks
- Improving the operational security level of the different rail segments
- Enhancing the robustness of the railway information, control and signalling sub-systems
Further information

- Secret project: [www.secret-project.eu](http://www.secret-project.eu)
- Cyrail project: [www.cyrail.eu](http://www.cyrail.eu)
- UIC Security division: [www.uic.org/security](http://www.uic.org/security)
- Contact point: [security@uic.org](mailto:security@uic.org)