Session 4 TELECOM

Security aspects and transition management when introducing IP in the railway domain

Pierpaolo Di Labio
Finmeccanica
What are threats on the network?

- Disruption
- Malware
- Physical Attacks
- Ddos
- Network Intrusions
- Spoofing
- Fraud
- Disruption
What is on board

- Ddos
- WiFi for Internet and Intranet access

- Public Announcement System

- Network Intrusions & error reporting
  Especially if WiFi service are active

- Passenger Information System

- Server

- CCTV & video recorder

- Train Control Network

- Managed IP Gigabit Ethernet Backbone

- Entertainment Server

- Diagnoses & error reporting

- Passenger Information System

- Public Announcement System

- WiFi for Internet and Intranet access
Cyber Security is achieved when

- **CONFIDENTIALITY**
- **INTEGRITY**
- **AUTHENTICATION**
- **AVAILABILITY**
Cyber Security methodology

We suggest 3 main steps to protect your networks:

Define with experts a secure system through the threat analysis and risks assessment in terms of cyber-attacks scenarios

Introduce Railway specific solutions and resilient architecture against cyber-attacks

Security Guideline for the Railways
1st step

Security assessment

<table>
<thead>
<tr>
<th>Objective</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What has to be protected first

<table>
<thead>
<tr>
<th>Threat Detection and Prevention</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Result</td>
</tr>
<tr>
<td>threats.</td>
<td></td>
</tr>
</tbody>
</table>

What are threats and risks

<table>
<thead>
<tr>
<th>Incident management</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Result</td>
</tr>
<tr>
<td>identified and prevented where possible.</td>
<td></td>
</tr>
</tbody>
</table>

How to prevent and react

<table>
<thead>
<tr>
<th>incidents.</th>
<th></th>
</tr>
</thead>
</table>
## Security Guideline for the railways

### 2nd step - Cyber Security system

<table>
<thead>
<tr>
<th>Objective</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and prevent external and internal attacks to the Railway ICT Infrastructure.</td>
<td>Safe and secure railway ICT Infrastructure, thanks to identification and prevention of attacks.</td>
</tr>
<tr>
<td>Deep Protocol Behaviour Inspection</td>
<td>• The purpose is the identification of malicious software or content introduced into the network.</td>
</tr>
<tr>
<td>Network packet analysis</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>• It allows the identification of network based attacks.</td>
</tr>
<tr>
<td>Fraud Management</td>
<td></td>
</tr>
<tr>
<td>Vulnerability and security incident management systems.</td>
<td>• It is based on the detection of hardware or software vulnerabilities.</td>
</tr>
<tr>
<td>Log correlator</td>
<td>• Centrally collect all log files, correlate the information and provide alerts to the CERT if suspicious behaviour is detected.</td>
</tr>
<tr>
<td>Vulnerability and Threat prediction</td>
<td>• Quick reaction to intrusion/anomaly with rapid analysis of large amounts of information (public and/or private).</td>
</tr>
<tr>
<td>Early warning</td>
<td></td>
</tr>
<tr>
<td>Cross Correlation</td>
<td>• an Intelligent distributed defence model that cross correlate operational information to optimize decision making, increasing the speed of reaction.</td>
</tr>
</tbody>
</table>
**Combining expertise – Designing a holistic knowledge base**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circle of experts that cover a holistic view on the problem.</td>
<td>Development of a working group of experts from all (needed) fields that is able to communicate efficiently and unambiguously.</td>
</tr>
<tr>
<td>Common terminology and taxonomy.</td>
<td></td>
</tr>
</tbody>
</table>

**Railway Security Operation Center (SOC)**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up a SOC/CERT dedicated to railway at national level.</td>
<td>Structure for a SOC/CERT dedicated to Railway.</td>
</tr>
<tr>
<td>Bundling the expert know-how</td>
<td></td>
</tr>
</tbody>
</table>
Security on SCADA and Industrial Control System

IT Systems
- IT System
  - Confidentiality
  - Integrity
  - Availability
  - ISO standards
  - International regulations
  - Well known methodologies
  - Architecture and protocols
  - Standard architectures / protocols
  - Proprietary/unknown to a certain extent
- PRIORITY

ICS Systems
- ICS Systems
  - Availability
  - Integrity
  - Confidentiality
  - Importance C(35%), I(35%), A(30%)
  - Patches are released quite slowly
  - Local standards
  - Local regulations
  - Not well known methodologies
  - Architecture and protocols
  - No standardized architectures / protocols
- PRIORITY

INDUSTRY GROUP
Sierra Wireless Proprietary and Confidential
Lesson Learned

35% are Cyber

The real danger

The industry is facing more classic problem like managing access to the resources (remote workers, contractors etc.), device misconfiguration and software behaving badly.

•  Operational mistakes
•  Sw update going wrong
•  Misuse & misconfiguration
•  Malware & exploits: zero-days
CONCLUSION

- Industry can provide solutions that are available for IT& ICT but railway is a specific domain
- Cyber-Security cannot be driven only by manufacturers, Railways community should work on guidelines and technical recommendations, standards/norm to reinforce the railway infrastructure.
- Some top-down initiatives should be re-enforced, like in France with ANSSI (National Agency for Information System Security) that has identified VIO (Vital Importance Operators) which includes also the main rail/metro operators and publishes some RECCOMENDATIONS step by steps and will formalize very soon some obligations through state law. **Such an approach should be extended at EU level.**

**WE ARE READY FOR SOLVING EXISTING ISSUES RIGHT NOW WORKING TOGHETER**
Thank you

Contact

Pierpaolo.dilabio@finmeccanica.com