Enhancing Critical Infrastructure Protection with innovative SECyurity framework

Manos Athanatos
FORTH-ICS, Distributed Computing Lab
H2020 SAINT Project Workshop
20/03/2018

The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.
• Project overview
• Consortium
• Work Description – Milestones
• Pilots
Overview

• **Project name:** Enhancing Critical Infrastructure Protection with innovative SECurity framework

• **Grant Agreement no.:** 700378

• **Start day:** May 1\textsuperscript{st} 2016

• **Duration:** 36 months

• **Call identifier:** H2020-DS-2015-1

• **Topic:** DS-03-2015. The role of ICT in Critical Infrastructure Protection.

• **Cost:** 5.613.788,00 €
Making a long story short

- **The critical point**: CI are an integrated part of our lives as they provide services to citizens, businesses and government.

- The main aim of CIPSEC is to create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection (detect, identify and mitigate threats) in IT (information technology) and OT (operational technology) departments of CIs.

- CIPSEC will offer a complete security ecosystem of additional services that can support the proposed technical solutions to work reliably and with professional quality. These services include vulnerability tests and recommendations, key personnel training courses, forensics analysis, standardization and protection against cascading effects.

- All solutions and services will be validated in three pilots performed in three different CI environments (transportation, health, environment).

- CIPSEC will also develop a marketing strategy for optimal positioning of its solutions in the CI security market.
<table>
<thead>
<tr>
<th>Objectives</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified security framework for CI</strong></td>
<td>Anomaly detection, anti-malware, cyber-security, data privacy, distributed denial of service, hardware security. Easy integration of heterogeneous systems to the CIPSEC framework.</td>
</tr>
<tr>
<td><strong>Security Ecosystem</strong></td>
<td>System vulnerability tests and recommendations, contingency plans based on PPPs, training courses and certification, updating/patching mechanisms, and forensics analysis.</td>
</tr>
<tr>
<td><strong>Transportation, health and environment pilots</strong></td>
<td>Validate our proposed solution under real conditions: System modules level (in each industrial section and security aspect), and system level (the complete framework).</td>
</tr>
<tr>
<td><strong>Links and standardizations bodies</strong></td>
<td>EPCIP (European Program for Critical Infrastructure Protection). ERNCIP (European Reference Network for Critical Infrastructure Protection).</td>
</tr>
<tr>
<td><strong>Ready to market</strong></td>
<td>Security frameworks for transportation, health or environmental monitoring CIs TRL 7/8. Industrial partners will bring to the CIPSEC project their own market products services (up to TRL 8/9)</td>
</tr>
</tbody>
</table>
Roadmap

- Project overview
- Consortium
- Work Description – Milestones
- Pilots
Partners

- Consortium: 13 partners
- Webpage: www.cipsec.eu
- Project coordinator: ATOS
Roadmap

• Project overview
• Consortium
• Work Description- Milestones
• Pilots
Work plan

■ **WP1**: Analyzing specific CI security requirements clearly assessing weak points and current limitations.
■ **WP2**: Setting the whole CIPSEC solution tailored to CI scenarios.
■ **WP3**: Integrating the CIPSEC solution to the three pilot scenarios proposed in the project for validation.
■ **WP4**: Final adjustments turning into a close to market solution running on real operational scenarios.
■ **WP5**: Starting from the very beginning, capturing and collecting all project contributions for communication, exploitation, and standardization purposes.
■ **WP6**: Dealing with overall project management aspects.
## Milestones - Achievements

### Already Achieved

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Description</th>
<th>Milestone</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS1</td>
<td>Security Analysis</td>
<td>M6</td>
<td>D1.1</td>
</tr>
<tr>
<td>MS2</td>
<td>Market review and analysis</td>
<td>M6</td>
<td>D1.1</td>
</tr>
<tr>
<td>MS3</td>
<td>Functionality building blocks</td>
<td>M6</td>
<td>D1.2</td>
</tr>
<tr>
<td>MS4</td>
<td>CI taxonomy</td>
<td>M6</td>
<td>D1.3</td>
</tr>
<tr>
<td>MS18</td>
<td>The exploitation and dissemination plan is ready</td>
<td>M6</td>
<td>D5.1</td>
</tr>
<tr>
<td>MS21</td>
<td>Committees Setting</td>
<td>M3</td>
<td></td>
</tr>
<tr>
<td>MS22</td>
<td>Project management strategy</td>
<td>M6</td>
<td>D6.1</td>
</tr>
<tr>
<td>MS23</td>
<td>Project report: First year</td>
<td>M12</td>
<td>D6.2</td>
</tr>
<tr>
<td>MS5</td>
<td>Architecture system design</td>
<td>M9</td>
<td>D2.1</td>
</tr>
<tr>
<td>MS6</td>
<td>First release preliminary version of the CIPSEC security platform</td>
<td>M18</td>
<td>D2.2-D2.4</td>
</tr>
<tr>
<td>MS9</td>
<td>Preliminary report for the pilots’ integration</td>
<td>M18</td>
<td>D3.1-D3.3</td>
</tr>
<tr>
<td>MS10</td>
<td>Preliminary report on CI intra/Inter-dependencies</td>
<td>M18</td>
<td>D3.4</td>
</tr>
</tbody>
</table>

### Next inline...

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Description</th>
<th>Milestone</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS7</td>
<td>Prototype ready for operation and environment tests</td>
<td>M24</td>
<td>D2.5-D2.6</td>
</tr>
<tr>
<td>MS11</td>
<td>Adapted and optimized solution for the selected pilots</td>
<td>M24</td>
<td>D3.5-D3.7</td>
</tr>
<tr>
<td>MS12</td>
<td>Final report on the CI's intra/Inter-dependencies analysis</td>
<td>M24</td>
<td>D3.8</td>
</tr>
<tr>
<td>MS13</td>
<td>list of policies for the CIPSEC prototype</td>
<td>M24</td>
<td>D3.9</td>
</tr>
<tr>
<td>MS14</td>
<td>Trials settings and configuration</td>
<td>M24</td>
<td>D4.1</td>
</tr>
<tr>
<td>MS24</td>
<td>Project Report: Second year</td>
<td>M24</td>
<td>D6.3</td>
</tr>
</tbody>
</table>
“CIPSEC project has successfully passed the 1st technical review”
Barcelona, Spain, 22th of November 2017
Roadmap

- Project overview
- Consortium
- Work Description - Milestones
- Pilots
Pilot Critical Infrastructure Areas

- CIPSEC focuses on three Critical infrastructures
  - Pilot 1 – Health (Spain)
  - Pilot 2 – Environmental Monitoring (Italy)
  - Pilot 3 – Transportation (Germany)
The Hospital Clinic de Barcelona (HCB) is one of the most recognized and representative largest public tertiary university hospitals in Spain and in the EU. Some of the most representative OT in HCB are:

- Monitoring and therapeutic equipment
- Imaging equipment
- High interventionist areas
- Surveillance cameras
- Access control
- Temperature and gas concentration active RFID sensors
- Voice over IP
- Patient’s bedside multimedia monitors
Network AQDRS (Air Quality Detection Regional System)

The Net is composed of:

- 7 COP Operating Provincial Center
- 78 fixed public stations
- 6 mobile public stations
- 900 sensors
- Connected to several other IT systems (apps and databases)
- The system records 25 million data entries per year.
Pilot 3- Railway transportation

Biggest business premises in Germany – with public access
- 5,700 Stations (in Germany) as gate to railway transportation
- 33,500 km rail network
- 48,800 heated railway switches (of 70,000 total)
- Approx. 3,300 interlocking systems of various types
- 1,323 electronic interlockings (ESTW)

Main objective
Safe railway operation

© CIPSEC Project, Mar 2018
CIPSEC community - Contact

Web site:
http://www.cipsec.eu/ (subscription)

YouTube presentation:
https://www.youtube.com/watch?time_continue=2&v=JdZ8IFMLFIQ

Twitter account:
CIPSEC Project@CIPSECproject

LinkedIn account:
https://www.linkedin.com/in/cipsec-project/

Project Coordinator (ATOS):
Antonio Alvarez Romero (antonio.alvarez@atos.net)

Scientific Coordinator (FORTH):
Sotiris Ioannidis (sotiris@ics.forth.gr)
Thank you!!
Questions??

Manos Athanatos
Contact: thanat@ics.forth.gr