CIPSEC 3rd newsletter – Spring 2018

The second year of the CIPSEC project is coming to an end on April 30 and with many new milestones to have been successfully achieved. A brief report of the main achievements since our last newsletter published in September 2017 is presented here split into two main sections, dissemination activities and technical advances.

DISSEMINATION ACTIVITIES

Blog
6 new CIPSEC blog entries have been released with monthly periodicity:

- When IT and OT Collide by COMSEC.
- Critical Infrastructure Security Starts with Endpoints by Bitdefender.
- Aspects on end to end and link encryption by Empeloros.
- Introduction to Digital Forensics by AEGIS.
- Most common attack vector over Critical Infrastructures by ATOS.
- Private data in Critical Infrastructures: a security threat or a business opportunity? by WoS.

YouTube
Tutorial videos from the 1st CIPSEC Critical Infrastructure Protection Training Session held in Heraklion on July 3rd, 2017 have been uploaded to YouTube:

Liaisons and related events

During the duration of the project, CIPSEC has established new liaisons with the projects: Cyberwatching, SMESEC, ReCRED and SAINT. A summary of these fruitful collaboration activities is the following:

- CIPSEC was included in the Cyberwatching catalogue of services.
- On 31st of January Ilias Spais from AEGIS presented the CIPSEC project in the H2020 clustering event organized by ReCRED with more than 16 project presentations.
• Manos Athanatos from FORTH presented the CIPSEC project in the SAINT workshop on 20th of Mach:

CIPSEC General Assembly Meetings
• CIPSEC Fifth General Assembly Meeting. The meeting was held successfully in October, 2018 in Bucharest, Romania and was organized by Bitdefender.
• CIPSEC Sixth General Assembly Meeting. The meeting was held successfully in February 21-22, 2018 in Athens, Greece and was organized by AEGIS.

2nd CIPSEC workshop
The 2nd CIPSEC Workshop International Workshop on Securing Critical Infrastructures (S-CI 2017) was organized by TUD in collaboration with UoP, in conjunction with the ARES EU Projects Symposium 2017. It was a full day Workshop collocated with ARES 2017 conference held in Regio Calabria on 29th of August 2017. The S-CI 2017 workshop technical program included two invited talks by CIPSEC members, Aljosa Pasic from ATOS and Christian Schlehuber from DB, as well as six peer reviewed research papers organized in two technical sessions.

Review meeting
The first CIPSEC review meeting, covering months 1-18 of the project, took place on November 22nd, at the Hospital Clínica de Barcelona (HCB) in Barcelona. The review meeting was led by our Project Officer Cristina Longo, assisted by Jose Araujo from the French Network and Information Security Agency and Filipe Caldeira from the Escola Superior de Tecnologia de Viseu.

The consortium presented the progress and the milestones achieved during the first phase of the project to the EC, including an early prototype of the CIPSEC framework, which has integrated a number of tools such as XL-SIEM (ATOS), antimalware tool (Bitdefender), Honeypot tool (FORTH), Forensics Visualization Tool (AEGIS) and DoSSensing Antijamming tool (Worldsensing).
COMSEC acted as an attacker, performing numerous vulnerability tests like attacking well known exploitable bugs, uploading a malicious file to the web server and more in order to demonstrate how the CIPSEC framework can effectively detect the attempted attacks and visualise them through the XL-SIEM (ATOS). A demo specifically designed for the the health pilot was successfully carried out with the CIPSEC framework being able to detect attack attempts to assets like infusion pumps, security cameras and more.

**Publications**

Six new conference papers:


**Journals:**


**Press releases:**

On a yearly basis, the ATOS web booklet is released including updated information about the diverse research lines and related projects ATOS participates to. CIPSEC is a strategic project for the Research and Innovation area of ATOS, and it is reflected as such in this [web booklet](#).

**TECHNICAL ADVANCES**

**Workpackages and milestones**
WP2
The main milestone of this workpackage is:

- **First release: preliminary version of the CIPSEC security platform**
  verified by the following deliverables D2.2-D2.3-D2.4:
  - D2.2: CIPSEC Unified Architecture First Internal Release
  - D2.3: CIPSEC products integration on the Unified Architecture
  - D2.4: CIPSEC services integration on the Unified Architecture

The reference architecture that has been designed in CIPSEC is able to protect critical infrastructures against cybersecurity threats. The design process followed an exhaustive methodology that feed from the context analysis carried out in WP1 (critical infrastructure requirements and commonalities, market analysis, etc.), as well as the initial system design created in D2.1. The design process of the architecture an incremental progress where the level of granularity of the design was progressively increased, adding details and components that fulfil the expected requirements. To this end, the design methodology started with an analysis of the management of data in critical infrastructures, which defined the data lifecycle. This data lifecycle was used for the creation of a high level architecture, which consisted of a layered model where data flows from the acquisition layer (network, devices, sensors, etc.), of the architecture, to the analysis and processing layers in order to generate reports, recommendations and contingency plans presented to the system security admin staff. This high-level architecture was refined with an additional level of granularity, that defined components for every layer and interconnections between the different layers, resulting to the CIPSEC reference architecture. Such components and interactions were defined by using:
  1. The security requirements and commonalities specified in WP1,
  2. The characteristics of the CIPSEC tools and services provided by CIPSEC partners,
  3. The foreseen extensions of such tools and services.

The CIPSEC reference architecture also mapped the tools and services from CIPSEC partners inside the reference architecture. This mapping will guide the implementation of the prototype in WP3 along with the deployment of the framework to three pilots of CIPSEC. The architecture is envisioned to be flexible and extensible, so that additional services and tools can be plugged to any layer of the CIPSEC architecture (for example, to retrieve new types of data from the acquisition layer).

Regarding the products integration in this architecture, the transformation from initial security products to the CIPSEC security products has been divided into two subsections/phases.

- **Phase 1**: Transformation (through innovation) from the initial form of the products and their state just before the beginning of the integration into the overall architecture. This phase includes the description of all applications, hardware and software modules/submodules, APIs etc. required to be modified to make each individual product “ready to integrate”.
- **Phase 2**: Transformation during/after the integration. This phase documents the innovation that each solution provider plans to introduce to his solution in order to be appropriately integrated it to the CIPSEC overall framework.
Finally, CIPSEC will deploy all the appropriate services in order to create a robust security framework for Critical Infrastructures (CIs) that will have the ability to orchestrate an assortment of heterogeneous products and services from different providers. Numerous services in CIPSEC framework include vulnerability tests and recommendations, technicians training courses, public-private partnerships (PPPs) for advanced contingency plan, forensic analysis, preliminary certification, and protection against cascading effects.

CIPSEC DASHBOARD

In WP2 we have been also working in creating a unified dashboard. The main objectives of the CIPSEC dashboard are:
- To provide a unified, harmonised view of the CIPSEC framework
- To integrate all the CIPSEC framework functionalities and heterogeneous products.
- To ease the usability of the CIPSEC framework

The CIPSEC dashboard is a unified, harmonised and consistent application where the user/administrator of the infrastructure is able to: i) check for the current infrastructure status; ii) easily access to all tools and services provided by the CIPSEC framework, and; iii) be warned about current or future threats in the system.

WP3

In this workpackage we are still working in tasks T3.1, T3.2 T3.3 and T3.4 that started on February and June 2017 respectively, and a new task started on November 2017 namely, T3.5 Complexity analysis and policies definition.

The main milestone of this workpackage for this period has been:
• **Preliminary report for pilots integration** verified by means of deliverables:
  
  o **D3.1: Preliminary Pilot I Integration: Incident Discovery and Response for Railway use case**
  o **D3.2: Preliminary Pilot II Integration: Hospital’s Operational Technology Management System use case**
  o **D3.3: Preliminary Pilot III Integration: Air quality Monitoring System use case**

This milestone documents the preliminary efforts carried out to integrate the CIPSEC platform into the three pilots. It aims at defining three robust solutions with capabilities to improve the resilience of the critical infrastructures in the three specific pilots from Environmental, Railway and Health domain.

The methodology for the integration followed a sequence of steps:

1. Understanding the pilot.
2. A list of security features is accurately defined.
3. Pilot providers choose the security features they believe suits them to their pilot’s device / resource, justifying their choice.
4. Once the pilots defined their needs based on their assets, and the product providers analyzed how their products can provide the required security features, a matching between these two lists is generated, reporting any kind of tool modification required for its integration with the specific pilot.
5. With the analysis of the coverage of security features by the products, the pilot owner can choose the products to be used to secure the critical infrastructure.
6. The tool providers specify the hardware and software requirements each solution requires.
7. The pilot analyses the feasibility of using the products on the infrastructure in question, according to the specs obtained in the previous step.
8. The pilot proceeds to adapt their infrastructure to accommodate the solutions.
9. Subsequently the pilot produces the final detailed definition of the infrastructure map with all the associated technical details.
10. Both pilot and solution providers work together to determine how and where the different selected products are going to be deployed within the pilot infrastructure.
Detail of the CIPSEC tools integration in the railway pilot.

- **Preliminary report on CI intra/interdependencies** verified by deliverable:
  - D3.4: CIPSEC Intra/Inter-dependencies Analysis Preliminary Report

This milestone and its related document describes a preliminary analysis on intra/inter-dependencies analysis, highlighting the potential cascading effects. Firstly an analysis in the three pilots (Environmental, Railway and Health) was performed denoting differences both in the areas of day to day operation and the safety aspects that must be taken into account. Also, the possible Cascading Effects that can be generated as a result of computer incidents are different for each pilot. Following these pilot descriptions, an evaluation of the real Cascading Effects took place, distinguishing between Inter and Intra Dependencies of each pilot. The first are dependencies between macro systems, while the latter is related to internal relationships within the CIs. Based on the definitions of Inter and Intra Dependencies, a concrete identification of the possible Cascading Effects of each Pilot was documented.

**WP4**

WP4 started on November 2017. This WP focuses on the efforts required to build a working prototype to run on operational CI scenarios. In this sense task T4.1 Setup and configuration of the trials that started in November 2017, defines the details of different scenarios for the trial of the system framework; Task T4.2 Field configuration for pilot deployment started on January 2018, undertakes the preparatory actions for the field trial as well as the integration of the system modules for the pilot implementations.