CIPSEC 5th Newsletter – Final Recap

This Newsletter summarizes all the progress done since December 2018, until the finalization of the project. Moreover, the final CIPSEC framework developed during the project life is presented.

CIPSEC framework

At the beginning of the project, different partners, providing heterogeneous cybersecurity solutions, joined forces to propose a solution to the increasing weakness of critical infrastructures, against cyber-attacks. The main goal was to integrate them into a single, unique product, capable of providing strong protection to critical infrastructures belonging to a wide range of verticals.

The first step was to identify a set of requirements, that is present to most critical infrastructures regardless of the sector they belong to. Subsequent to that process, we identified those requirements that are applicable on each vertical that was involved, from the very beginning of CIPSEC, namely the three CIPSEC pilots: *Hospital Clinic de Barcelona*, from Health Sector, *Consorzio per il Sistema Informativo*, from Environmental Monitoring Sector, and *Deutsche Bahn AG*, from Transportation Sector.

From the analysis of these requirements, the design of the CIPSEC Framework came up, with a reference architecture for critical infrastructure protection against cyber-attacks, integrating each product and creating new services in the novel CIPSEC framework.

After thorough work, the CIPSEC solutions were deployed to the three pilot sites. From this process, we concluded that each critical infrastructure is unique and there were not two identical deployments. CIPSEC's modularity allowed us to deploy customized solutions for each of the pilot sites.

Once the deployments were working correctly, a thorough testing process was carried out to check that CIPSEC behaves as expected against a wide range of attack scenarios.

As a summary, we can conclude that CIPSEC, as an integrated solution, is a product whose value is much higher than the sum of that of the individual products and services included. CIPSEC can be applied to critical infrastructures in different verticals, and is flexible enough to be adapted to the needs of the client. It can be deployed fully-on-premises, but also supports deployments using public cloud with minimum installation on the premises of the client. Finally, a hybrid approach is supported which is amid the two other approaches. The client can select the products and services that better fit their case.

Regarding the activities in the last period of the project, we present a brief report of the main achievements of CIPSEC emphasizing into the dissemination and the technical aspects of the work that has been performed.

DISSEMINATION ACTIVITIES

Blog

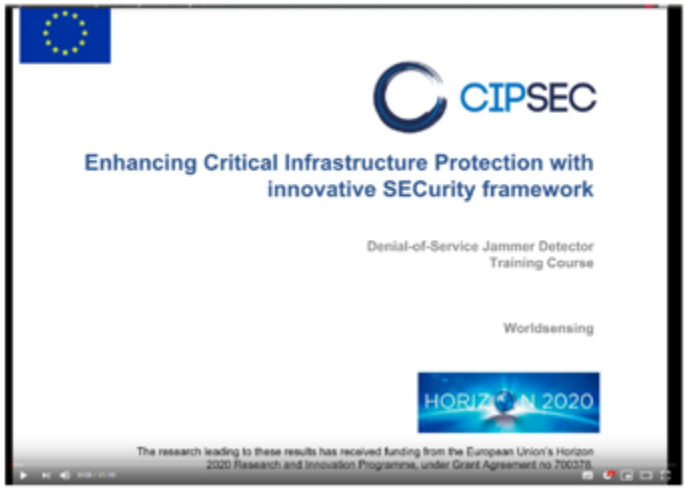
New 5 CIPSEC blog entries (http://www.cipsec.eu/auto/blog) have been released with monthly periodicity:

- How Blockchain Technology Can Improve Defence In Critical Infrastructures by Panagiotis Sifniadis from Empeloros, January 2019.
- The Importance of Critical Infrastructure Security by Liviu Arsene from Bitdefender, February 2019.
- Visualisations against challenges in Digital Forensics by Leonidas Kalipolitis from AEGIS, March 2019.
- General considerations regarding exploitation in EU-funded project by Denis Guilhot from Worldsensing, April 2019.
- The CIPSEC Project comes to an end: final recap and concluding thoughts by Antonio Álvarez from ATOS, May 2019.

YouTube

During these last 5 months of the project we have produced two new CIPSEC videos:

- A video with a DoSSensing training course produced by WoS was released on February 2019.



- A video with the CIPSEC Framework dashboard training course produced by UPC was released on May 2019.

Liaisons and related events

During the last five months, CIPSEC has been present in the following events:

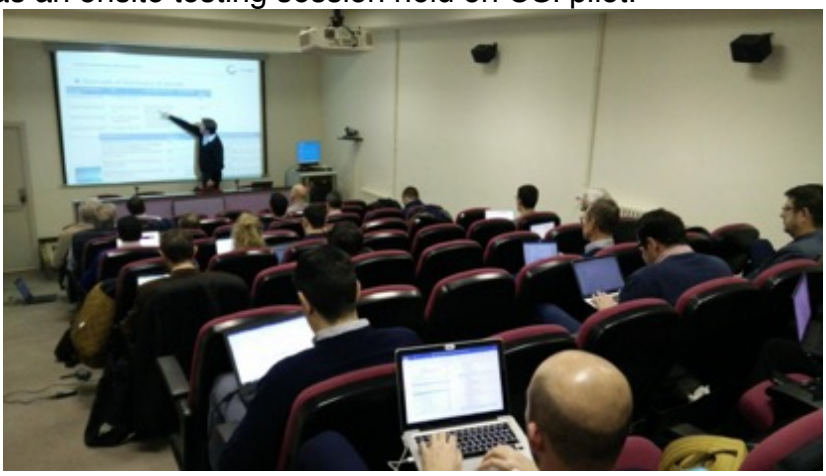
- COMSEC attended Cybertech 2019, on January 2019, which is the cyber industry's foremost B2B networking platform conducting industry-related events all around the globe. COMSEC had a booth in the exhibition and assigned a part for promoting the CIPSEC project.

- Worldsensing has also attended the 4YFN2019 and MWC2019, and the framework was presented to companies with strong focus on the IoT field, both small and large, and also to potential integrators of cybersecurity solutions.
- TUD presented CIPSEC's technical approach at:
  - Fifth annual IRSE presidential programme technical meeting in Darmstadt, on February 2019.
  - The EU-AsiaPacific CIP Forum (April 2019)

CIPSEC General Assembly Meetings

- CIPSEC Eight General Assembly hosted by HCPB in Barcelona on January 22nd-23rd-24th 2019, including a training course offered to the HCPB staff and the follow-up meeting with the Advisory Board; as well as an on-site testing session took place at the HCPB pilot site and also another testing session carried out to fix and improve things in the prototype.

- CIPSEC Ninth General Assembly hosted by CSI in Turin on March 13th-14th 2019; also including a training course offered to several members of CSI staff: as well as an onsite testing session held on CSI pilot.



Publications
During this period, the CIPSEC consortium achieved the publication of:

3 new conference/ papers:

- "Red-Zone: Towards an IntrusionResponse Framework for Intra-Vehicle System", Mohammad Hamad, Marinos Tsantekidis, and Vassilis Prevelakis, presented at the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS), Crete, Greece, May 2019.
- "Anonymizing Cybersecurity Data in Critical Infrastructures: The CIPSEC Approach ", Ana Rodríguez-Hoyos, Jose Antonio Estrada-Jimenez, David Rebollo-Monedero, Jordi Forné, Ruben Trapero, Antonio Alvarez, Rodrigo Diaz, presented at the 16th International Conference on Information Systems for Crisis Response and Management, Valencia, Spain, May 2019.
- "Balancing Security Guarantees vs QoS Provisioning in Combined Fog-to-cloud systems", Sarang Kahvazadeh, Xavi Masip, Rodrigo Diaz, Eva Marín Tordera , Alejandro Jurnet, Jordi Garcia, Ana Juan Ferrer, Ester Simó, to be presented at 10th IFIP International Conference on New Technologies, Mobility & Security, on June 2019.

3 journals publication or acceptance:

- Louiza Papachristodoulou, Apostolos P. Fournaris, Kostas Papagiannopoulos, Lejla Batina, "Practical Evaluation of Protected Residue Number System Scalar Multiplication", on the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), vol.1, December 2018.
- "Design and Leakage Assessment of Side Channel Attack Resistant Binary Edwards Elliptic Curve Digital Signature Algorithm Architectures", Apostolos P.Fournaris, Charalambos Dimopoulos, Athanassios Moschos and Odysseas Koufopavlou from UoP, on the Microprocessors and Microsystems, Volume 64, February 2019, Pages 73-87.

- Kubilay Demir, Ferdaus Nayyer, Neeraj Suri, “MPTCP-H: A DDoS Attack Resilient Transport Protocol to Secure Wide Area Measurement Systems“,on the International Journal of Critical Infrastructure Protection, Volume 25, June 2019, Pages 84-101.

1 book chapter:

- Antonio Álvarez, Rubén Trapero, Denis Guilhot, Ignasi García-Milà, Francisco Hernández, Eva Marín-Tordera, Jordi Forné, Xavi Masip-Bruin, Neeraj Suri, Markus Heinrich, Stefan Katzenbeisser, Manos Athanatos, Sotiris Ioannidis, Leonidas Kallipolitis, Ilias, Spais, Apostolos Fournaris and Konstantinos Lampropoulos, “CIPSEC-Enhancing Critical Infrastructure Protection with innovative SECurity framework”, in Challenges in Cybersecurity and Privacy - the European Research Landscape, River Publishers, ISBN: 9788770220880

TECHNICAL ACTIVITIES

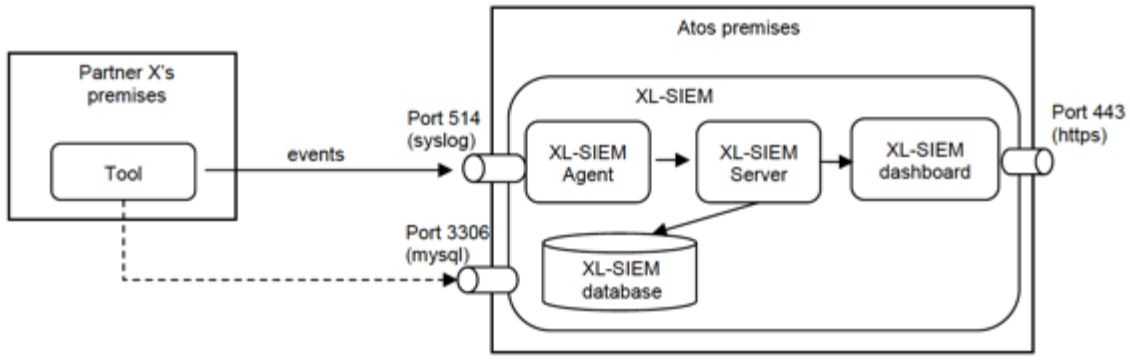
Work packages and milestones

WP2

The main milestone of this work package in this period was:

- ***Final CIPSEC security framework*** verified by means of deliverable D2.7:
  - D2.7. CIPSEC Framework Final Version

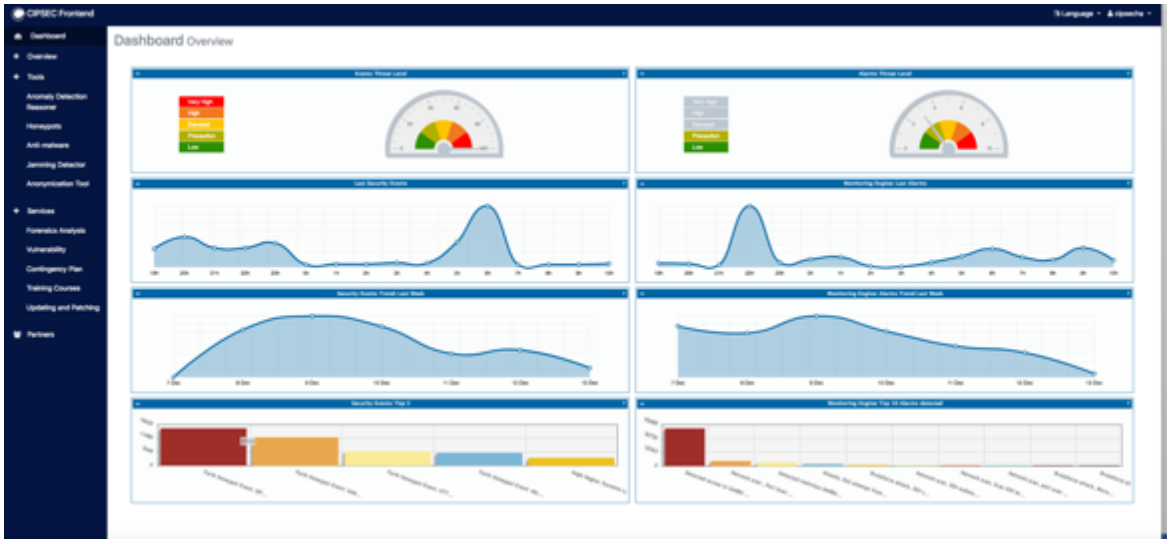
Deliverable D2.7 describes the final integrated CIPSEC Framework summarizing all the activities that took place in Task 2.5, “From the prototype to the final CIPSEC security framework”. It describes the final Integrated Framework, as it was developed throughout the duration of CIPSEC project, the core components of the framework developed, the interconnection between the different components, the final deployed services; as well as the adjustments to each tool through the lessons learned from the deployment to the different pilot Infrastructures and the final evaluation settings with an overall assessment summary of the framework.



- **CIPSEC Dashboard**

The CIPSEC dashboard is completely finalized, including all the integrated tools and services. Furthermore, we produced two versions of the dashboard, one of them deployed in cloud, accessed through Internet; and with users created for each one of the pilots. The other version of the dashboard is offline, and we created a unique

user. However, the idea is to customize the dashboard deployed on-premises just by adding those tools that are relevant for every customer needs.



WP4

This WP focuses on the efforts required to build a working prototype to run on operational CI scenarios, and the milestones achieved for this period have been:

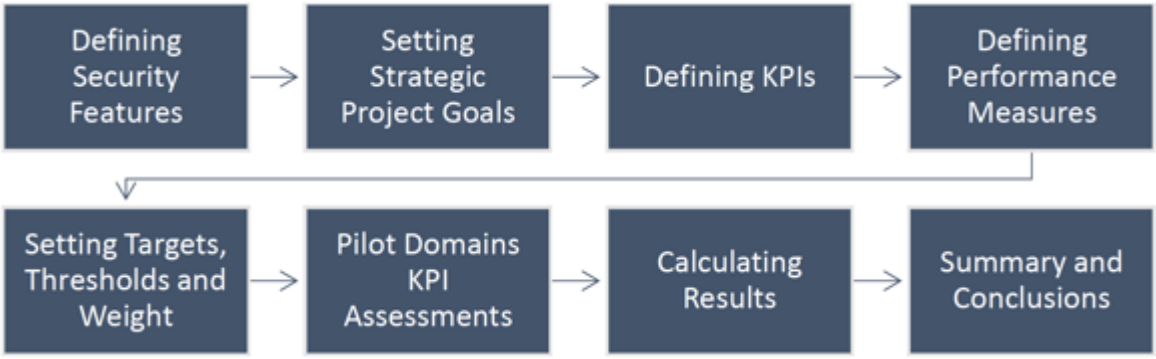
- ***Prototype demonstration successfully conducted*** verified by means of the deliverable:
  - D4.3 CIPSEC Prototype Demonstration: Field trial results

  This milestone and deliverable reports all the tests conducted to validate the functionalities of the CIPSEC prototype installed at each of the test sites. The definition of the test cases has been already reported at D4.1 and D4.2; and the session definition and test session reporting were documented with the same standard (IEEE 829) used in D4.1 and D4.2.
  DB test site required two on-sites sessions to validate their test cases. HCPB site required seven online sessions to validate their test cases. CSI required five online sessions to validate their test cases completely.
  All the test cases and test plans and designs were successfully validated.

- ***Final CIPSEC framework capabilities in TRL8: results*** verified by means of deliverable:
  - D4.4. Use-case evaluation and recommendations

  This milestone and deliverable describe the evaluation (i.e. assessment) of the CIPSEC framework in a quantitative manner, both by evaluating the framework's performance and by estimating the potential expected savings of deploying the solution. In general terms, the deliverable's goal is to acknowledge the CIPSEC framework as a close to market solution, running in real operational scenarios.
  As a conclusion, most of the security features were fully achieved, i.e. their

KPIs have met the target value.



Solution assessment process

WP5

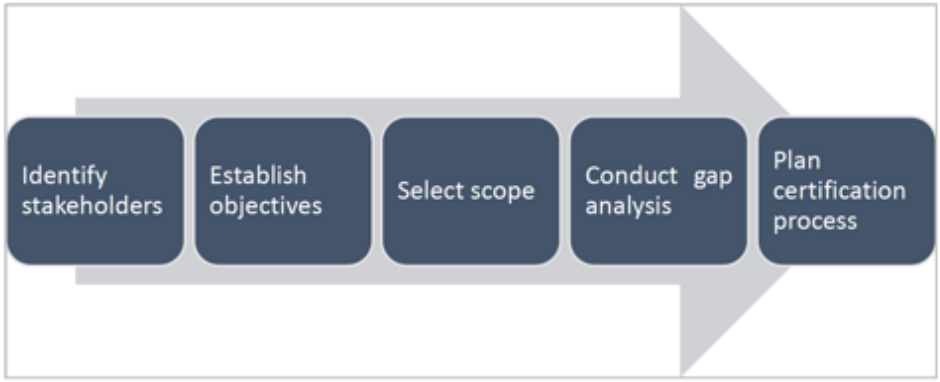
In this technical description of the CIPSEC activities we also include work done in WP5 related to business model definition and certification activities.
The main milestones achieved during this period in these areas are:

- ***The business model for impact creation and exploitation is ready*** verified by means of the deliverable:
  - D5.5: Business Plans Definition

  In this deliverable, we have analyzed possible business processes to deliver the solutions to the customer segments. As a result of this analysis CIPSEC has proposed 10 different business models that adapt each of the solutions and business processes to the targeted markets and clients. These business models are:
  - 6 individual business models: Business models designed to outline the commercial and service models of the following individual solutions: DoSSensing, XL-SIEM, SECOCARD, Forensics Visualization Tool, Antivirus and the Vulnerability assessment tool.
  - 3 verticals business models: These business models have been designed considering the pilots' vertical market. A set of tools has been considered to protect the IT/OT infrastructures of each of the markets according to the different customer segments and their needs.
  - Free version business model: The free version integrates some of the solutions developed within the CIPSEC project, offering limited capabilities.
- ***Preliminary certification activities*** verified by means of the deliverable:
  - D5.6 Preliminary certification activities

  As it is known a world-wide respected method to guarantee and present compliance with security controls for CIs is to have an information security certification by an accredited third party. In this deliverable we analyze the potential certification options with and for CIPSEC framework, underlying different angles:
    1) **Certification of CIPSEC as one framework**
    2) **Certification of the separate CIPSEC components**
    3) **Compliance with (the help of) CIPSEC framework**

Although, not concluding with clearly identified stakeholders for CIPSEC certification, we propose a plan to follow for certifying CIPSEC shown in the figure below.



Preliminary certification activities process