This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787011.

SPEAR NEWSLETTER

Second newsletter **September 2019**

The SPEAR Architecture

The SPEAR programme aims to introduce a three-tier platform architecture that is able to ensure confidentiality, integrity and availability of smart-grid oriented data and services. The SPEAR architecture consists of the following major layers:

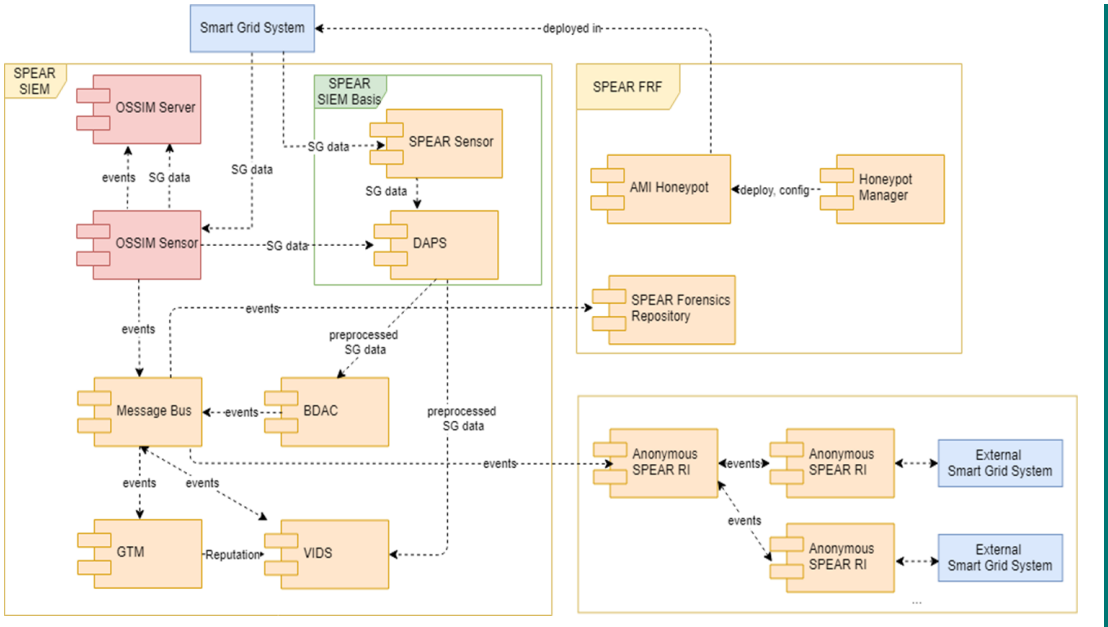
SPEAR SIEM: The SPEAR system information and event management framework aims at detecting and illustrating anomalies on operational data and network traffic that could indicate a cyber-attack or any kind of anomaly that need immediate action.

SPEAR FRF: The SPEAR Forensic Readiness Framework encompasses tools that process forensic data and prepare evidences which can be used in courts. In addition, FRF realizes the optimal deployment of honeypots to trap attackers and collect precious evidences.

Anonymous SPEAR-RI: The SPEAR Anonymous Repository of Incidents enables communication and transaction of security incidents among energy providers and operators in Europe. Anonymisation techniques guarantee that the participating organisations will not get exposed.

Project Details

* **Project no.** 787011
* **Research and Innovation Action:** Co-funded by the Horizon 2020 Framework Programme of the European Union
* **Call identifier:** H2020-DS-2016 -2017 (Digital Security Focus Area)
* **Topic: DS-07-2017:** Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
* **Start date of project:** May 1st, 2018 (36 months duration)



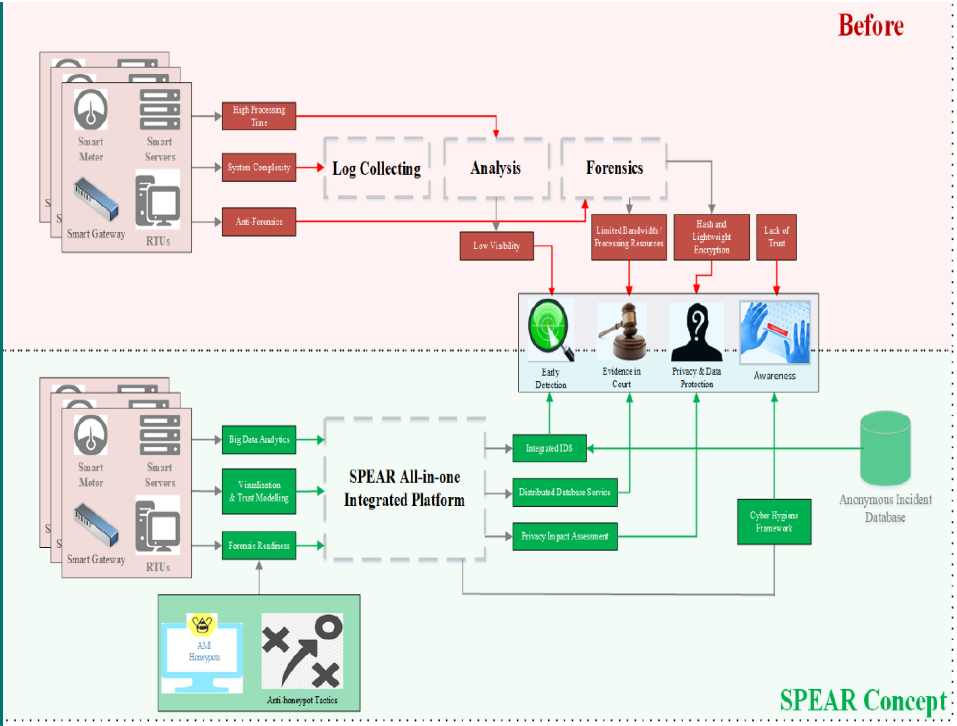
The SPEAR architecture

Contents

SPEAR Concept

Compared to traditional IT networks, where confidentiality is the most important, smart grid is prioritised in availability. Any form of disruption occurring to the grid can be highly dangerous and it can cost human lives, major economical disturbance, major gaps in national defence, reputation degradation and personal information leaking. Even though modern security solutions that have sufficiently protected IT infrastructure, such as IDS and firewalls, they are incapable of directly deploying in smart grid systems without critical redesign and modifications due to grid inherent features.

SPEAR platform relies in the basic concept that cyber security must be considered in all domains, components and subsystems of the smart grid and at all phases of the grid lifecycle. The transformation of the legacy power industry to modern smart grid has led to a complex system that involves both IT and electricity operation and administration which is apparently presents many and arduous challenges in security, privacy and data protection.



SPEAR Concept

The SPEAR First Review Meeting

The project's first review meeting took place in Brussels, at the Headquarters of the European Research Executive Agency from 27 to 28 May 2019. The review was attended by all partners from the academic and industry section and by the Project Officer (PO). In addition, two reviewers from the energy industry and the energy market, *Stamatis Karnouskos* and *Sigitas Rokas*, reviewed the progress of the project so far.

Agenda

The review process started with the greeting of the Project Coordinator, *Dr. Panagiotis Sarigiannidis*, who described the project's vision, the progress and the achievements so far as well as the next steps and plans.

Next, the development progress for each work package was presented by the partners as well as the involvement of end users with the rest of the consortium.

Demo presentations

Preliminary work on machine learning algorithms and software components was presented. The presentation was focused on the following:

- Big Data Analytics (BDAC) demo
- Visual-based IDS demo
- AMI honeypots demo
- Grid Trusted Module (GTM) demo
- Honeypots demo

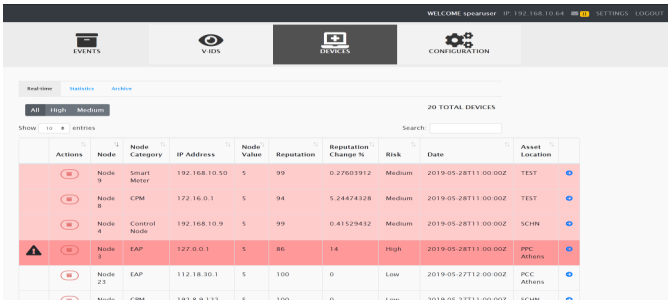
Demo presentations

Demo 1: The BDAC demo

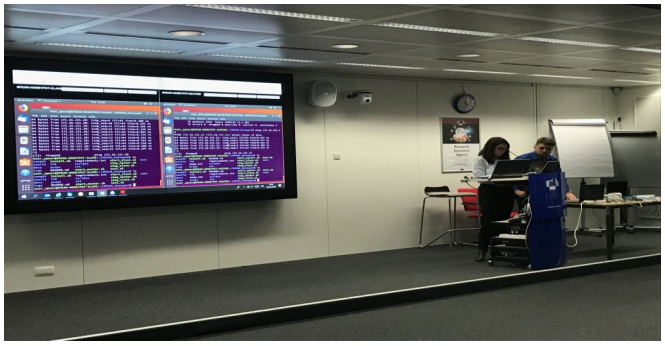
The SPEAR platform is powered by strong Machine Learning algorithms that aim to detect anomalies on network traffic and operational data that could indicate a cyber-attack or any kind of anomaly. During the review, a comparison between several anomaly detection algorithms applied on public and SPEAR end-user's data was presented.

Demo 2: The Visual-based IDS demo

During the second demo, an early version of the visual-based Intrusion Detection System user interface was presented, which is capable to display all the important information for the security status of the critical infrastructure.



Demo 2: The start page of the Visual-IDS



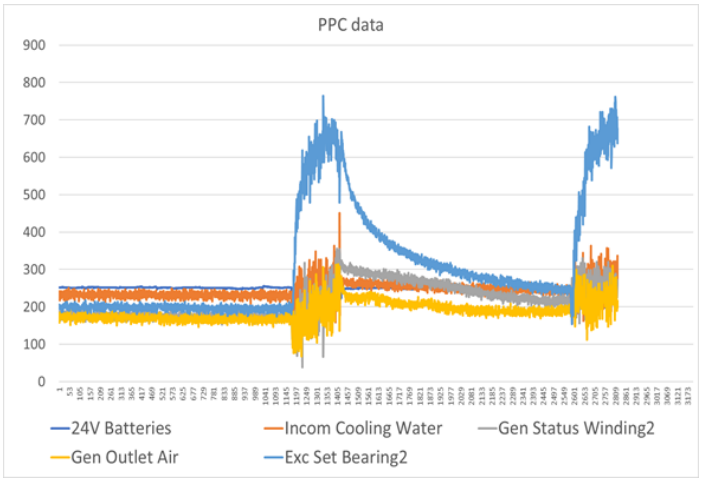
Demo 3: Presenting the AMI Honeypots Demo

Publications

During the first year of the SPEAR project, 7 scientific publications have been accepted and 2 are under revision, to conferences and journals that concern cybersecurity, privacy and machine learning applied on smart grid use cases.

A great success of the SPEAR consortium was it's first journal publication. "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems", which was published to the prestigious IEEE Access journal.

You can find all our publications in PDF format by visiting our website: https://www.spear2020.eu/Publications/



Demo 1: Big Data Analytics on operational data

Demo 3: The AMI Honeypots demo

Honeypots are a powerful tool that SPEAR project realizes and are used as a decoy to trap attackers and gather intelligence about their activity as well as to protect the real infrastructure from the intruders. During the review, a demo interaction between two honeypots as well as some preliminary work on the game-theoretic model that aims to orchestrate the honeypots in the most efficient way.

Demo 4: The GTM demo

The last demo was dedicated to the Grid Trusted Module, a software component that receives events from the BDAC component and applies calculations to estimate the reputation of each asset of the infrastructure. Critical assets that are possibly under attack or present an unusual behavior, appear on the Visual-based IDS user interface.

The SecSoft workshop

On June 24, 2019, SPEAR co-organized the 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft).

SPEAR participated in the organising committee of SecSoft 2019 with the following members:

- Panagiotis Sarigiannidis (SPEAR coordinator) from the University of Western Macedonia, Greece, served as TPC co-chair and Scientific sessions co-chair
- Manos Panaousis from the University of Surrey, UK, served as Panel co-chair

Upcoming Events

In 24-25th of September, 2019, the 4th plenary meeting will take place in Sevilla, Spain, where the progress of the SPEAR project will be presented in the consortium partners

Communication

Website

https://www.spear2020.eu

LinkedIn

https://www.linkedin.com/company/spear2020

YouTube

https://www.youtube.com/channel/UCw6-d5G01ToBhCmaUnHIcpw

Project Coordinator:
Dr. Panagiotis Sarigiannidis
University Of Western Macedonia, Greece

E-mail:

psarigannidis@uowm.gr

SPEAR