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

SPEAR NEWSLETTER

Fifth newsletter **September 2020**

Dear reader,

You are reading the fifth issue of our newsletter, published by the SPEAR project, a Horizon 2020 program funded by European Union under grant agreement No. 787011.

In this issue we inform you about the following topics:

- The demonstrations that were carried out during the **second SPEAR review**;
- Highlights of our **latest publications**;
- Highlights of our **latest** public **deliverables**;
- Highlight of our latest **blog posts**;
- **Upcoming events**;

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
* **Project Start date:** May 1st, 2018 (36 months duration)

SPEAR Deliverables

The SPEAR consortium continuously updates the SPEAR website about new deliverables that are approved by the European Commission. Recently, we have uploaded the following deliverables, that summarise the majority of scientific and technical work performed within the project: (https://www.spear2020.eu/Deliverables)

- D3.2 - Multi-factor and Open Analytics Engine for Smart Grid Ecosystem
- D3.3 - Open Visual-aided Intrusion Detection System
- D3.4 - Node-centric Reputation Models and Algorithms
- D4.5 - SPEAR Smart Grid Database & Interfaces
- D8.4 - Interim Impact Creation Report

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

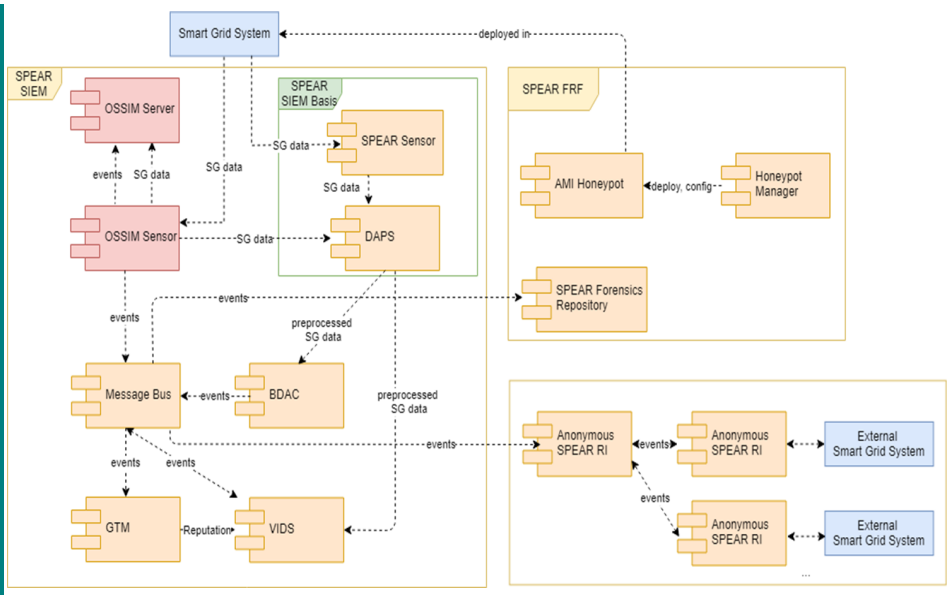
SPEAR Architecture

The SPEAR project 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 needs 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.



SPEAR Architecture

Second SPEAR Review

The second review of the SPEAR project took place at 18th of June 2020. As an impact of the ongoing COVID-19 pandemic, the review meeting was held online via teleconference, while the technical demonstrations were performed in the nZEB Smart House of CERTH, requiring the minimum physical presence of SPEAR technical partners at CERTH premises.

The review meeting was attended online by all SPEAR partners from the academic and industry section, and by the Project Officer, *Nikolaos Panagiotarakis*. 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

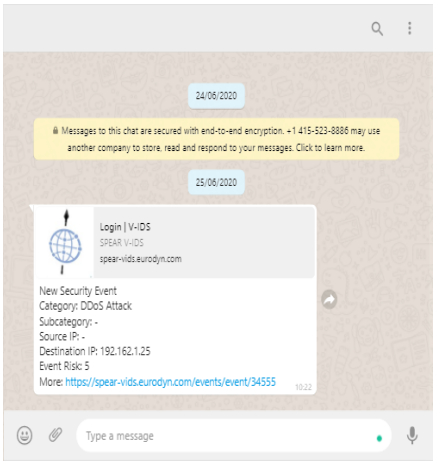
The review meeting started with the greeting of the Project Coordinator, *Dr. Panagiotis Sarigiannidis*, who introduced the project's concept, the achievements during the second year of the project as well as the next steps and plans, towards the end of the project.

Considering the maturity of the SPEAR project at the end of its second year, extensive end-to-end demonstrations were carried out in order to showcase the project's technical achievements so far. Highlights of the demo sessions are provided bellow.

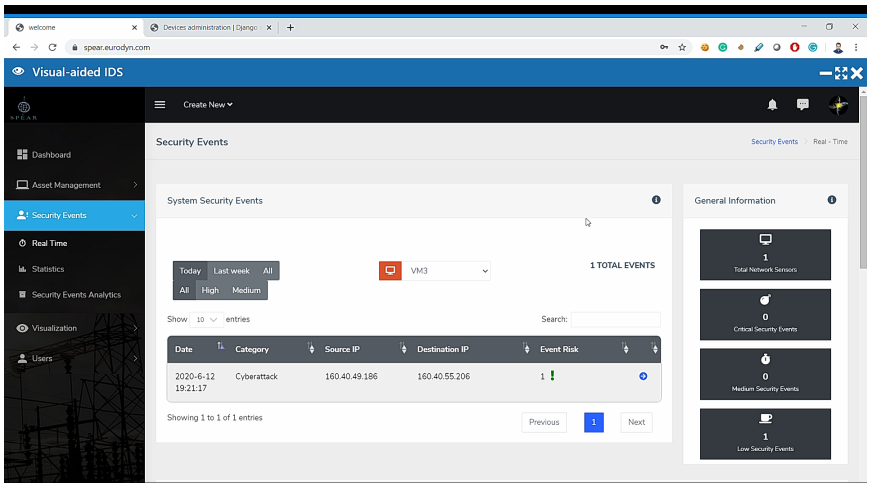
End-to-end Detection of Cyberattacks Demo

The capability of SPEAR to detect a variety of cyberattacks was demonstrated during the first demo session. The session concerned the detection of attacks against smart grid protocols, including Modbus TCP and MQTT.

The demonstration was carried out in a realistic environment of the CERTH Smart Home pilot, where smart devices and the cyberattacker were connected to a port-mirroring switch, that was copying and forwarding network traffic directly to the SPEAR platform. The complete SPEAR solution was deployed locally in the Smart Home premises.



Real-time notification on WhatsApp



The V-IDS dashboard showing security events in real time

During the demo session, DoS and reconnaissance attacks were performed live by researchers of CERTH against the smart devices of the pilot infrastructure. SPEAR received the generated network traffic and, by employing the appropriate AI methods, it successfully detected the cyberattacks. The detection generated the corresponding security events, which were finally appeared in the V-IDS dashboard as well as in a WhatsApp application, in order to ensure instant acknowledgment about the cybersecurity incident.

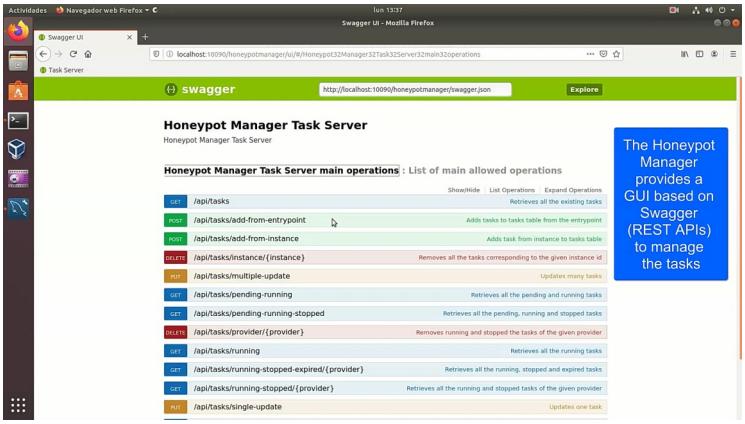
Game Theoretic Intelligence and Honeypot Manager

The SPEAR Honeypot Manager was also demonstrated during the second SPEAR review, including the following two major components:

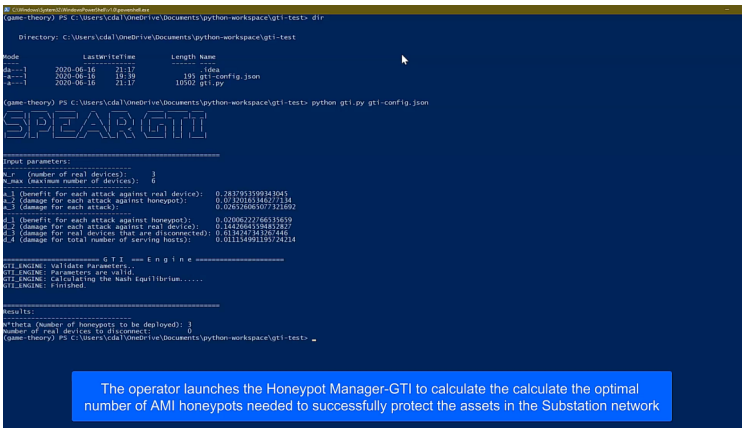
Game Theory Intelligence (GTI): This is the brains of honeypot manager, undertaking to calculate the optimal number of honeypots that need to be deployed in order to efficiently protect the network, while minimising the operational costs.

Honeypot Deployer: This is the GUI (based on Swagger) that allows the user to navigate through the Honeypot Manager REST API and performs various tasks, including deployment of new honeypots according to the GTI recommendations as well as management and removal of the deployed honeypots.

During the demo session, the complete workflow of the Honeypot Manager was showcased, starting from loading the preferred configuration via the Manager GUI and proceeding to the deployment of the corresponding honeypots as VMs to a VirtualBox hypervisor. The deployment was followed by automatic remote configuration of their communications and the automatic retrieval of the generated logs, via SSH.



The Honeypot Manager GUI



The SPEAR GTI Engine

Our Latest Blog Posts

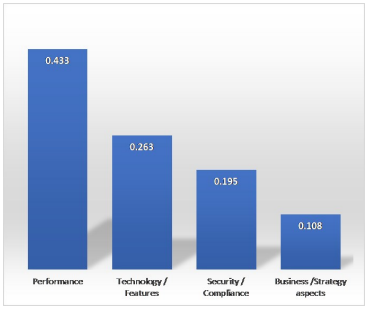
ENISA Guidelines in the Energy Domain and its Synergy with the SPEAR Project

The energy sector is one of the vital areas of any economy. While the integration of IT and power grid brings many benefits in terms of efficiency, it also raises significant cybersecurity threats. It is in this regard that the work of the European Union Agency for Cybersecurity (ENISA) in the energy sector is relevant .

You can read the full article in the following link: https://www.spear2020.eu/News/Details?id=101

Factors affecting the SPEAR market adoption

To identify the main factors and the main criteria that would affect the adoption of SPEAR by the market, a survey using the Fuzzy Analytic Hierarchy Process (AHP) method has been conducted within the project.



You can read the full article in the following link: https://www.spear2020.eu/News/Details?id=102

Our Latest Publications

Game Theoretic Honeypot Deployment in Smart Grid

This papers presents a game theoretic model that is solved to find and deploy the optimal number of honeypots in the smart grid infrastructure, considering resource constraints as well as the activity of the attacker. This research provides the mathematical framework and evaluation results that prove the effectiveness of the proposed model

You can read the full article in the following link: https://zenodo.org/record/3967314

ARIES: A Novel Multivariate Intrusion Detection System for Smart Grid

A novel anomaly-based IDS, called ARIES, is introduced in this paper, which is capable of protecting efficiently smart grid communications. ARIES combines three detection layers that are devoted to recognizing possible cyberattacks and anomalies against network flows, Modbus/TCP packets and operational data, relying on multiple Machine Learning models.

You can read the full article in the following link: https://zenodo.org/record/4036224

Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees

This research proposes a comprehensive methodology that enables informed decisions on security protection for smart grid systems by the continuous assessment of cyber risks. The solution is based on the use of attack defense trees and allows system risk sensitivity analysis to be performed with respect to different attack and defense scenarios.

You can read the full article in the following link: https://zenodo.org/record/4035771

Secure and Private Smart Grid: The SPEAR Architecture

This papers introduces the Secure and PrivatE smArt gRid (SPEAR) architecture which constitutes an overall solution aiming at protecting SG, by enhancing situational awareness, detecting timely cyberattacks, collecting appropriate forensic evidence and providing an anonymous cybersecurity information-sharing mechanism. Operational characteristics and technical specifications details are analysed for each component, while also the communication interfaces among them are described in detail.

You can read the full article in the following link: https://zenodo.org/record/4019723

Upcoming Events

Towards its final stage, the SPEAR final demonstrations are planned to start on November 2020. which will assess the final integrated SPEAR platform at the end user's premises. The demonstrations will last for 4 months (until February 20201) and will take place at the following locations:

- Belitsa, Bulgaria (**MVETS Lenishta**) - Hydro Power Plant Use Case
- Bizkaia, Spain (**Tecnalia** Smartgrid Cybersecurity Laboratory) - Substation Use Case
- Athens, Greece (**PPC** Testing, Research and Standards Centre Laboratories) - Combined IAN/HAN Use Case
- Lavrio, Greece (Unit no5 of the **PPC** Lavrio Power Plant) - Combined IAN/HAN Use Case
- Thessaloniki, Greece (nZEB Smart House of **CERTH**) - Smart-Home Use Case