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

SPEAR NEWSLETTER

Fourth newsletter **June 2020**

Dear reader,

You are reading the fourth issue of our newsletter, published by the SPEAR project, a Horizon 2020 program funded by European Union.

In this issue we inform you about our latest achievements, project activities, blog posts and scientific publications. In particular:

- An extensive review about cybersecurity in SCADA systems has been published in **IEEE Communications Surveys and Tutorials**, the top journal for Computer Science and Electronics, according to Guide2Research.
- An overview of our **latest blog posts** is provided.
- **Project status**: Entering its third year, our project reaches its final stage, towards the integration and the final validation in the pilots.
- SPEAR consortium co-organizes the **EPESec Workshop.**
- Our latest **deliverables**

Zenodo collection of SPEAR publications

Towards increasing the impact of our work and scientific publications as well as to ensure open access to all scientific work produced in the context of the project, we are utilising the Zenodo platform to upload and index our publications.

Zenodo is an **open access repository** of scientific data, including publications, datasets, multimedia content and software, that is operated by CERN and developed under the European OpenAIRE program.

A collection has been created on the platform for the SPEAR project, that is maintained by the consortium and gathers all the scientific work affiliated by the project. You can access the collection by visiting the following link: https://zenodo.org/communities/h2020_spear_project

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)

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

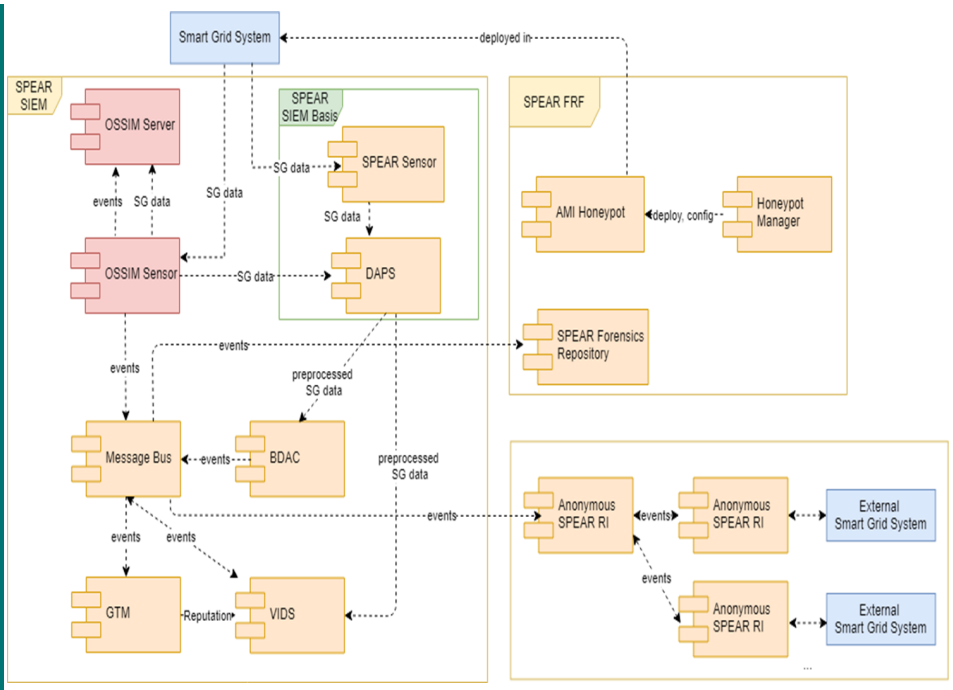
SPEAR Architecture

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.

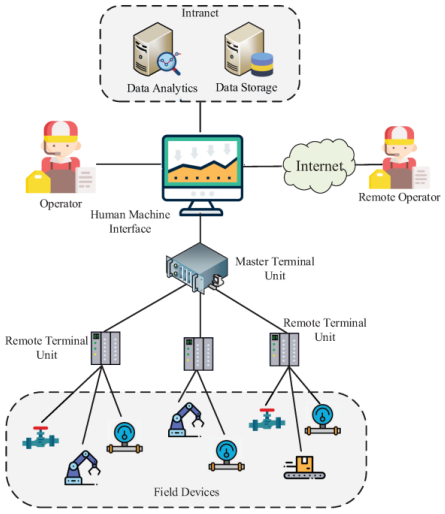
Anonymous SPEAR-RI: The SPEAR Anonymous Repository of Incidents enables communication and transaction of security incidents among energy providers and operators in Europe. Anonymisation techniques guarantee that the participating organisations will not get exposed.



SPEAR Architecture

Publication in IEE Communications Survey and Tutorials

Supervisory Control and Data Acquisition (SCADA) systems are widely deployed to monitor and control critical infrastructures, including transportation, telecommunication networks, factories and power grids. Although, SCADA systems are characterised by severe security vulnerabilities that can expose critical infrastructures to new risks.



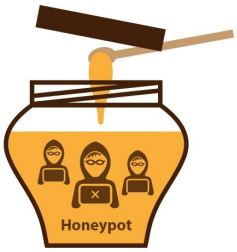
Our recent work entitled "**A Survey on SCADA Systems: Secure Protocols, Incidents, Threats, and Tactics**" provides an overview of the SCADA architecture and the utilised communication protocols, along with specific security incidents and threats. Moreover, an extensive review of security strategies to secure SCADA systems is carried out as well as the current research trends and future advancements are presented.

The research paper has been published in IEEE Communications Surveys & Tutorials, the top journal for Computer Science and Electronics with Impact Factor of 22.973, according to Guide2Research (http://www.guide2research.com/journals/).

You can read our article by visiting our project's collection on Zenodo: https://zenodo.org/record/3834801

Latest Blog Posts

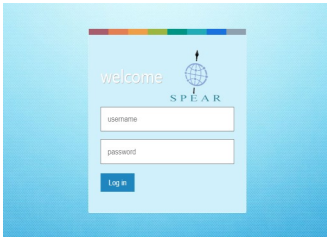
Deception Technologies for Smart Grid Protection



One of the focus of SPEAR project work is placed on deception technologies which are part of the overall cyber defense strategy of an organization. These technologies aim at fulfilling multiple purposes at the same time; they are set up to act as a decoy to lure cyber-attackers, and to support the detection and learning about zero-day cyber threats and other types of attacks. Therefore, they lead to improved decision making about cyber security strategies.

You can read the full article in the following link: https://www.spear2020.eu/News/Details?id=99

The SPEAR Early Integrated Prototype is Coming Soon



The SPEAR components (SPEAR SIEM, SPEAR FRF and SPEAR RI) developed in the technical work packages are currently being integrated towards a complete functional prototype in the framework of the Integration work-package (WP6). The SPEAR platform that is built on a novel three-tier approach, unifies the different modules and converges into an overall system that provides to security administrators of the Smart Grid (SG) systems not only a friendly and useful but also a more effective and reliable tool to detect, respond and take countermeasures against advanced cyber threats and attacks.

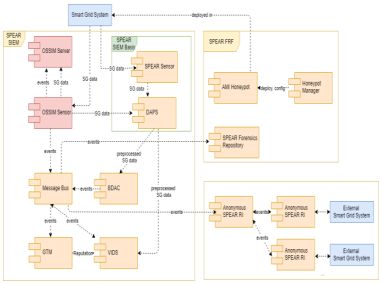
You can access the full article in the following link: https://www.spear2020.eu/News/Details?id=97

Enel in the SPEAR project

The Smart Grids, among other things, remotely manage the elements maneuvers on the electrical substations that allow to transport and to distribute the electric power of the network. This enables control in different environments like the System of Control of Supervision and the Acquisition of Information (SCADA), Distribution Manager Systems (DMS), and other small configurations of control systems as Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) often found in the critical infrastructures sector.

You can read the full article in the following link: https://www.spear2020.eu/News/Details?id=98

Secure and Private Smart Grids: The SPEAR Architecture



The SPEAR solution, proposed by this project, aims to provide the ability to energy operators to timely detect cyber-threats against their infrastructures, considering in parallel privacy-related issues and the collection of forensic-related data. Moreover, SPEAR intends to enhance situational awareness of energy-related stakeholders by establishing an anonymous repository of incidents .

You can read more about the SPEAR architecture by visiting the following link: https://www.spear2020.eu/News/Details?id=92

SPEAR co-organizes the EPESec workshop

SPEAR is co-organising the **EPESec workshop** in conjunction with the ARES EU Projects Symposium 2020 at the 15th International Conference on Availability, Reliability and Security (ARES 2020 - http://www.ares-conference.eu/). The EPESec 2020 workshop aims at collecting the most relevant ongoing research efforts in the Electrical Power Energy Systems (EPES) security field. It will also serve as a forum for relevant projects in order to disseminate their security-related results, boost cooperation, and foster the development of the EPES Security Community.

Read more about the workshop in our website: https://www.spear2020.eu/News/Details?id=95

SPEAR Deliverables

The SPEAR consortium continuously updates the SPEAR website about new deliverables that are approved by the European Commission. Until now, you can find in our website the following deliverables:
(https://www.spear2020.eu/Deliverables)

- D1.4 - Data Management Plan
- D2.4 - Public Version of User, Security and Privacy Requirements
- D2.5 - Public Version of System Specifications and Architecture
- D4.1 - Forensic Law and Regulations
- D8.1 - SPEAR web site, social network pages and open access server
- D8.2 - Plans for Dissemination and Communication