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

SPEAR NEWSLETTER

SPEAR Kick-off Meeting **May 2018**

The SPEAR objectives

The SPEAR proposal aims at:

a) detecting and responding to cyber-attacks using new technologies and capabilities

b) detecting threat and anomalies timely

c) developing all-in-one security detection solutions

d) leveraging advanced forensics subject to privacy preserving

e) confronting Advanced Persistent Threat (APT) and targeted attacks in smart grids

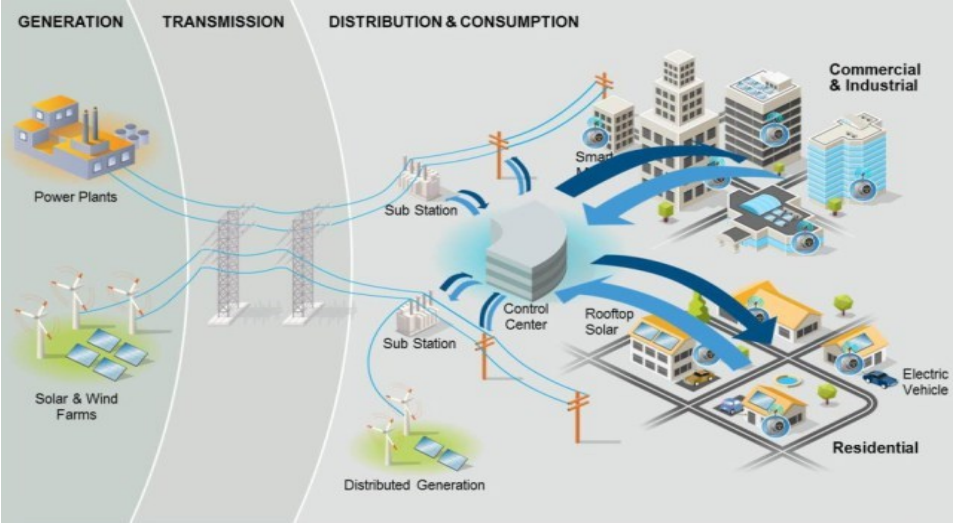
f) increasing the resilience of the smart grid innovation

g) alleviating the lack of trust in smart grid operators and

h) empowering EU-wide consensus.

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)



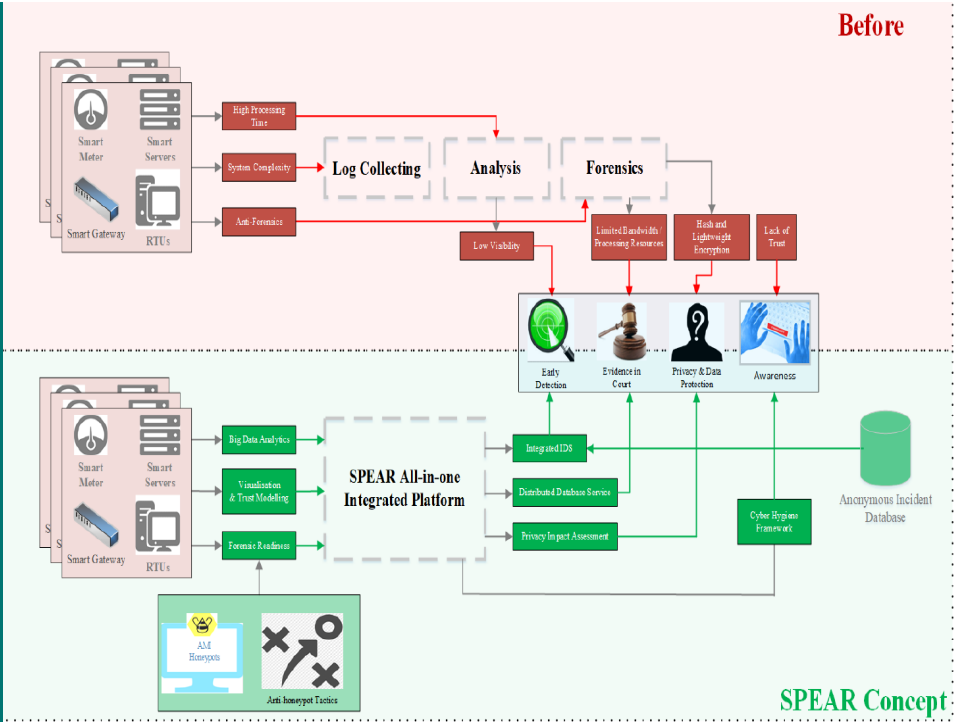
Smart Grid System

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

SPEAR Kick-Off meeting

The SPEAR kick-off meeting

The project's kick-off meeting took place in Thessaloniki, Greece at the Centre for Research and Technology from 10 to 11 May 2018. The kick-off meeting was attended by all partners from the academic and industry section and by the Project Officer (PO).

The Project Coordinator Dr. Panagiotis Sarigiannidis of UOWM welcomed the participants to the SPEAR Kick-Off meeting in Thessaloniki and opened the meeting.

The coordinator presented the Project identity and explained the motivation and challenges of the SPEAR project which comes to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern smart grid.

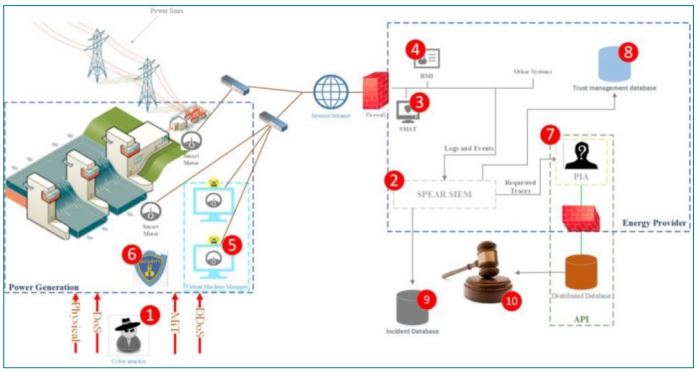
Presentation from PO

The Project Officer (PO), Mr. Nikolaos Panagiotarakis, participation in the kick-off meeting allowed to draw conclusions on the maturity of the project plan, the appropriateness of work-distribution among beneficiaries and the overall quality of the partnership proposing the project.

SPEAR Use Cases

Use Case 1: The Hydro Power Plant Scenario

The use case will validate the efficiency of the SPEAR platform in hydro smart grid in terms of a) response time to the attack, b) accuracy of the SPEAR SIEM tool, i.e., of the BDAC component, c) effectiveness of the AMI honeypots operating at the power generation premises and d) robustness of the SPEAR platform to DoS, DDoS, MiT and physical attacks.

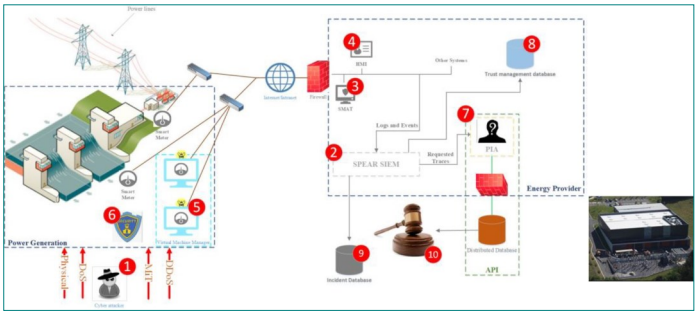


Use case 1: Hydro Plant Scenario

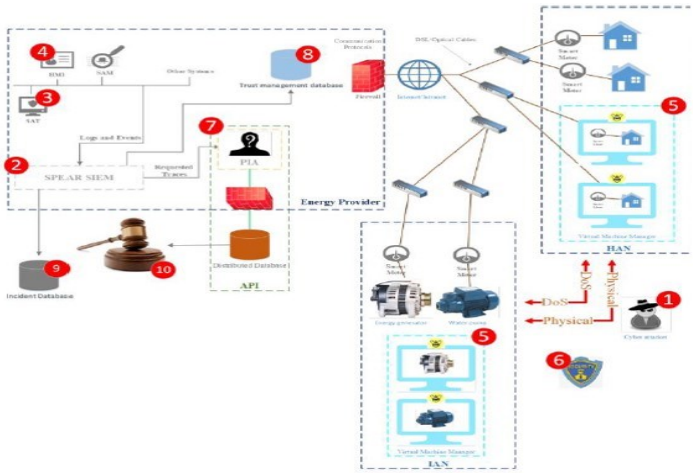
Use Case 2: The Substation Scenario

The substation scenario will address one of the critical infrastructures defined by the European Program for Critical Infrastructure Protection (EPCIP). Electrical substations today are characterized by different mixes of Information Technology (IT) and Operational Technology (OT). When bolstering the security of a substation network, IT infrastructure components such as PC hosts, network devices (e.g., switches, routers, and firewalls) are a logical first step for protection. However, the protection of OT-based devices can be more difficult to achieve. Most embedded devices and power systems applications were not designed with security monitoring in mind.

This scenario will provide insights on how the SPEAR platform confronts cyber-attacks against RTUs and will validate the feasibility of SPEAR platform to protect operator sensitive data within the control center.



Use case 2: Substation Scenario



Use case 3: The combined IAN & HAN Scenario

Use Case 3: The combined IAN and HAN scenario

PPC governs many power production units, where most of them are steam electric power plants, across Greece. Towards selecting a legacy power plant which is now evolving to a modern power grid, PPC was selected by the SPEAR consortium to validate its integrated platform in newly power grid systems that will be ready up to the project beginning.

The SPEAR platform will be validated in the PPC premises in Greece subject to its ability to detect and respond to cyber attacks in Industrial Area Network (IAN) and Home Area Network (HAN). The equipment in these areas is designed to aim the grid obtain valuable information about the operation status of the equipment in the IAN and to collect the consumers' power consumption in the HAN. Hence, both area are crucial for the grid credibility and reliability.

Use case 4: The Smart Home Scenario

Use Case 4: The Smart Home Scenario

The goal of this scenario is to perform extensive trials on the SPEAR technologies to smart home and micro-generation scenarios, where IoT devices and multi-sensorial networks have been already installed, as well as a PhotoVoltaic (PV) system of 10kW for energy production, supporting also demand response strategies and net metering services. The overall aim of is to showcase that SPEAR technologies can safeguard smart grid availability, integrity, confidentiality.

Upcoming Events

In October 2018, the first 6-month meeting will take place in Bilbao where the first results will be presented in the consortium partners

Communication

The SPEAR project is funded by HORIZON 2020 under the call "H2020-DS-2016-2017", Contract No. 787011

Website

https://www.spear2020.eu

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

E-mail:

psarigiannidis@uowm.gr

SPEAR