Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D8.3 – Initial Impact Creation Report

2019-04-30

Version 1.0

Published by the SPEAR Consortium
Dissemination Level: Public

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

Document Control Page

Document Details

Document Version	1.0
Document Owner	INC
Contributors	INC, PPC
Work Package	WP 8 - Dissemination and Exploitation
Deliverable Type	[R]
Task	Task 8.1 - Dissemination and Communication
Document Status	Final
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	INC	2019-03-15	Initial ToC
0.2	Christos Dalamagkas (PPC)	2019-04-02	Contribution to the “Communication Tools” section
0.3	Christos Dalamagkas (PPC)	2019-04-14	Updated publication abstracts, media, plans for second year
0.4	Theodoros Rokkas (INC)	2019-04-22	Updated with content from ENEL, CERTH, INC
0.5	Theodoros Rokkas (INC), Christos Dalamagkas (PPC)	2019-04-25	Updated with content from SURREY, 0 IFN, PPC, UOWM
0.6	Theodoros Rokkas (INC),	2019-04-26	Updated with content from Tecnalia

Internal Review History

Reviewed By	Date	Summary of Comments
Anton Hristov (VETS)	2019-05-02	Minor syntax and grammar corrections.
Alkiviadis Giannakoulias	2019-05-02	Minor syntax and grammar corrections.

Legal Notice

The information in this document is subject to change without notice.

The Members of the SPEAR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

The Members of the SPEAR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects only the author's view and that the Agency and the Commission are not responsible for any use that may be made of the information it contains.

Table of Contents

Acronyms

Acronym	Explanation
AICC	Anonymous Incident Communication Channel
AMI	Advanced Metering Infrastructure
BD	Big Data
CI	Critical Infrastructure
CPS	Cyber-Physical Systems (CPS
DDoS	Distributed Denial of Service
DoS	Denial of Service
ESG	Electric Smart Grid
GA	Google Analytics
ICT	Information and Telecommunication Technologies
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IoT	Internet of Things
MCS	Mobile Crowd-Sensing applications
PC	Project Coordinator
SCADA	Supervisory Control and Data Acquisition
SEO	Search Engine Optimisation
SG	Smart Grid
UOWM	University of Western Macedonia

1. Executive Summary

This document is the third deliverable coming out of WP8 and covers the dissemination and communication activities that took place during the first year of SPEAR. The dissemination and communication strategy was introduced in D8.2 and was the guide for the organization of the associated activities.

Until now results and outcomes coming from SPEAR has been published in four conference papers and in one Journal while four more papers have been submitted for publication. A newsletter has been published on the project's website while two interviews have been given to the media. SPEAR was presented in three events and is co-organizing a workshop along with the IEEE NetSoft 20129 conference.

Most of the KPIs during the first year are on track with the original plan and preventive plans were made to achieve those that were not in track.

2. Introduction

All SPEAR partners are engaged to the dissemination and communications activities according to the ignition plan that was included in D8.2. According to that, partners will participate in the dissemination activities of the project while they will interact with other projects to organize special events, workshops. Academic partners will be mainly responsible for publishing papers in journals and conferences, while industrial partners for participating in exhibitions.

This deliverable presents all the activities performed during the first year of the project along with the plan of activities for the second year. It records the achievements made in the KPIs in order to evaluate the initial strategy and propose changes where is needed.

The document is structured as followed: chapter 3 presents the communication tools that were used along with their impact. Chapter 4 continues with the dissemination and communication activities during the first year while chapter 5 presents the KPIs. Finally, the plan for dissemination and communication activities for the second year of the project is presented in chapter 6.

3. Communication tools

SPEAR realizes numerous communication channels that assist the consortium in disseminating the project's outputs. Those channels are namely, the SPEAR's official website, a LinkedIn page, a YouTube channel and leaflets that are posted on the website and the LinkedIn page.

3.1 SPEAR website impact

The website is the central dissemination tool of the SPEAR consortium and it is developed in order to inform stakeholders and the general audience about the project's objectives, outcomes and progress.

The Google Analytics (GA) service has been deployed on the website in order to measure the detailed impact of SPEAR's dissemination strategy. Figure 1, screenshot from the "Audience Overview" of GA, provides an overview of visitor's activity on the website. From 1 May 2018 to 31 March 2019, approximately 464 unique visitors have visited our website. By examining the audience overview graph, we notice an increasing trend of the number of visitors.

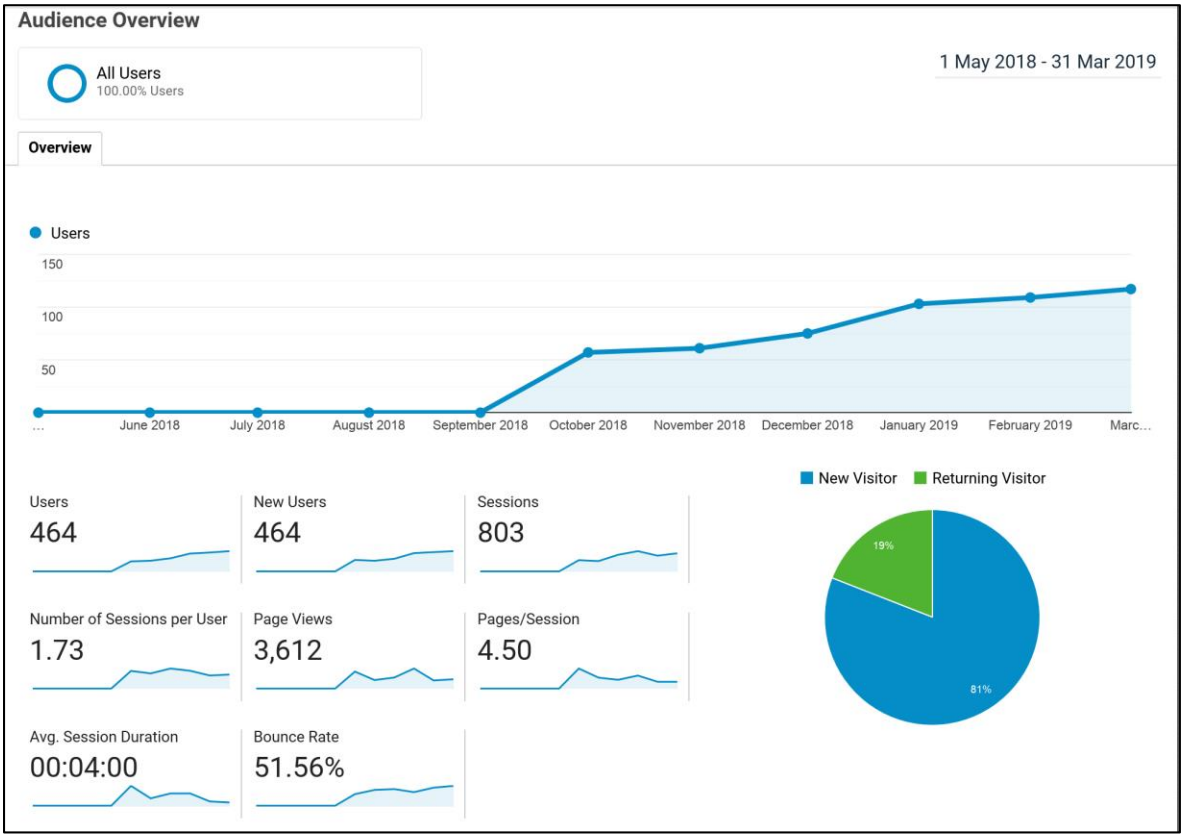


Figure 1: Website - Audience Overview

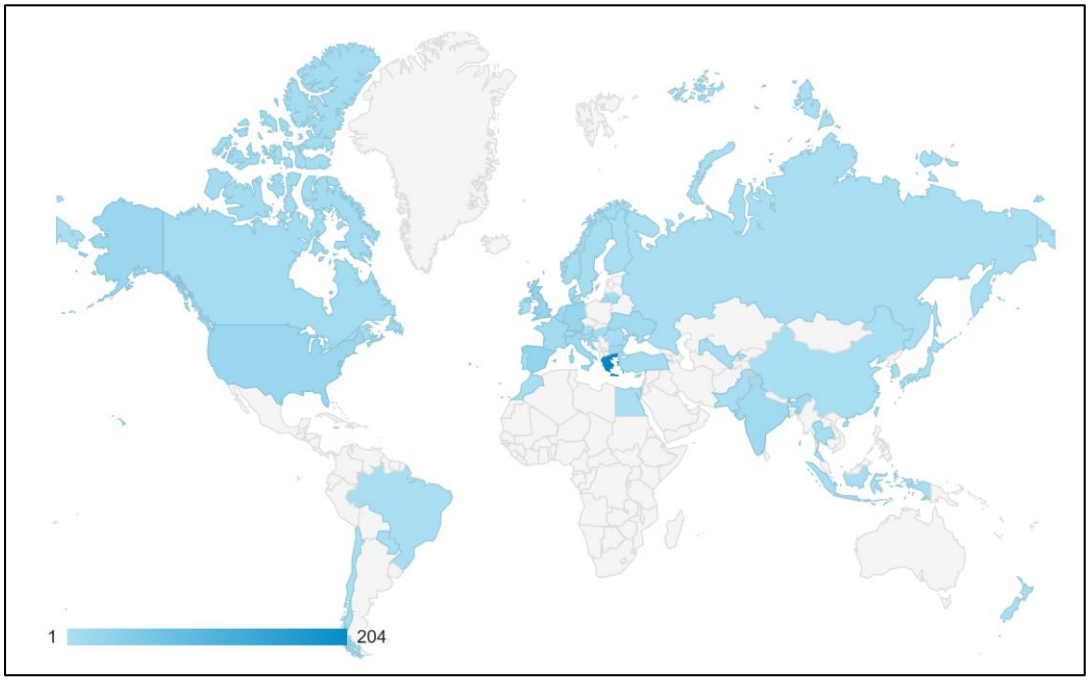


Figure 2: SPEAR Website - Geolocation overview

Figure 2 is a screenshot of the “Location” menu of GA and illustrates the visitor’s geolocation distribution. Most visitors originate from Greece, which is reasonable since the dissemination tools are operated by the Public Power Corporation (PPC), which is based in Greece. Nevertheless, there are many visitors originating from a variety of countries, such as United Kingdom, Spain, Germany and the United States of America.

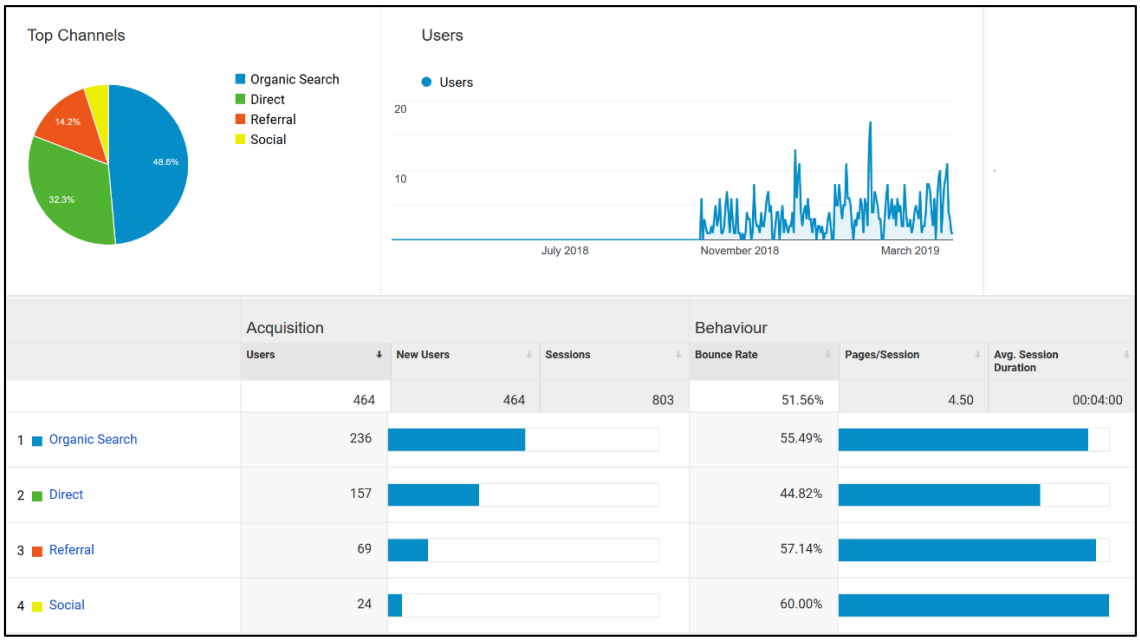


Figure 3: SPEAR Website – Acquisition overview

Figure 3 is a screenshot from the “Acquisition overview” menu and provides a summary of the channel sources of our visitors. The majority of our visitors reached the website by organic search, meaning that they found our website through search engines. The second source of generated traffic comes directly from visitors that type the website URL or click their bookmark (Direct), while the third source of incoming visitors is clicks of the website link from third-party websites and social media (Referral and Social).

The fact that the organic search precedes other sources indicates the efficiency of the website’s Search Engine Optimisation (SEO) that has been deployed.

3.2 Social media impact

The SPEAR LinkedIn page has totally 32 followers as of 04/04/2018. LinkedIn provides an Analytics functionality, similarly to GA, that gives a deeper insight of user activities and the impact that posts have to followers. Figure 4 provides an overview of visitor’s metrics, since the project started. Peaks are observed during project’s events, like plenary meetings.

Figure 5 displays the number of interactions that were observed in the SPEAR LinkedIn page. Examples of such interactions are likes, shares, comments and clicks. Peaks of activities are observed during SPEAR events, like a plenary meeting, and lows during holidays, for example during August, December and January.

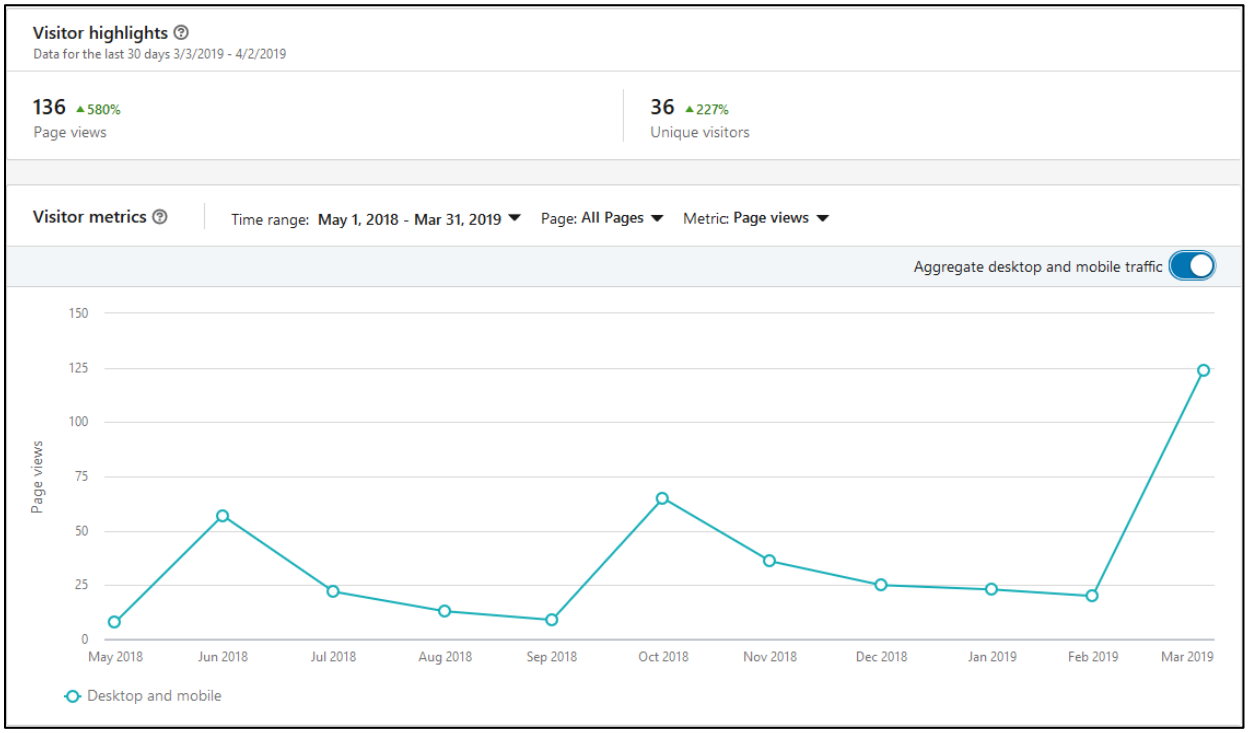


Figure 4: LinkedIn - Visitors Overview

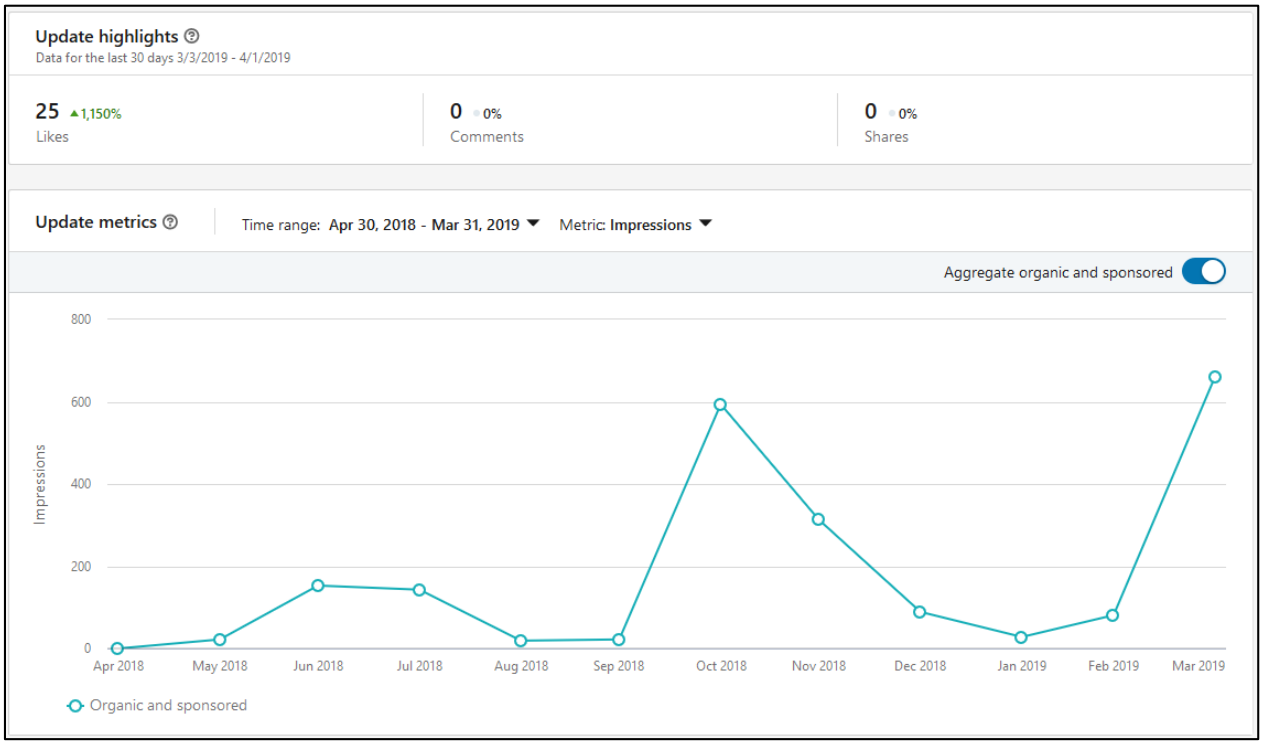


Figure 5: LinkedIn - Updates Overview

3.3 Other tools

During the first year of SPEAR, a light leaflet has been published that describes the SPEAR objectives and use cases. The leaflet is presented in figures 6-9 while is available for download in the following link:

https://www.spear2020.eu/cmsMedia/Uploads/UserFiles/News/SPEAR_Newsletter_May18.pdf

The SPEAR newsletter uses the main project's colour, emerald green, with light grey and the front page always includes the SPEAR logo, a list of project details, the SPEAR objectives, an image that illustrates a smart grid and a menu that has the characteristic emerald green background. The frontpage also includes an acknowledgment of the European Union funding and a proper disclaimer, according to the Grant Agreement.

A periodic Newsletter, intended to be issued every three months, will provide information on project progress and results, as well as contain links to public deliverables and articles and interviews for external communications. It will be made available on the project website and social media in order to improve the visibility of the project via electronic means and also will be sent to consortium partners and other registered stakeholders.

A detailed plan was made for the second and third year of the project with blog publications assigned each month to specific partners. Each partner will be the editor for these blog publications that will be uploaded to the website of the project.

Partners have already announced their participation in the project and its objectives and context in their respective websites. For example:

- https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/spear.jsp by SCHN.
- https://www.cyberssbytecnalia.com/content/spear-secure-and-private-smart-grid by Tecnalia.
- https://ipme.kiev.ua/en/2018/02/03/spear-secure-and-private-smart-grid/ by PIMEE.
- http://www.8bellsresearch.com/projects.html by 8BELLS.
- https://www.eurodyn.com/european-dynamics-was-awarded-a-cyber-digital-security-contract/ by ED.
- https://iri.uni-hannover.de/forschung/spear.html by TUH.
- https://www.surrey.ac.uk/secure-systems-research-group/research/secure-communications SURREY.
- https://www.certh.gr/358BEA28.el.aspx by CERTH.

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

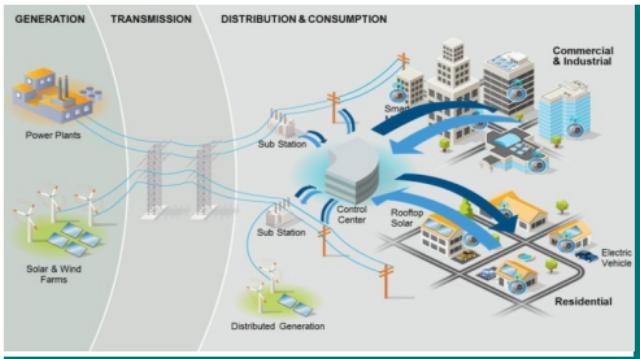
f) increasing the resilience of the smart grid innovation

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

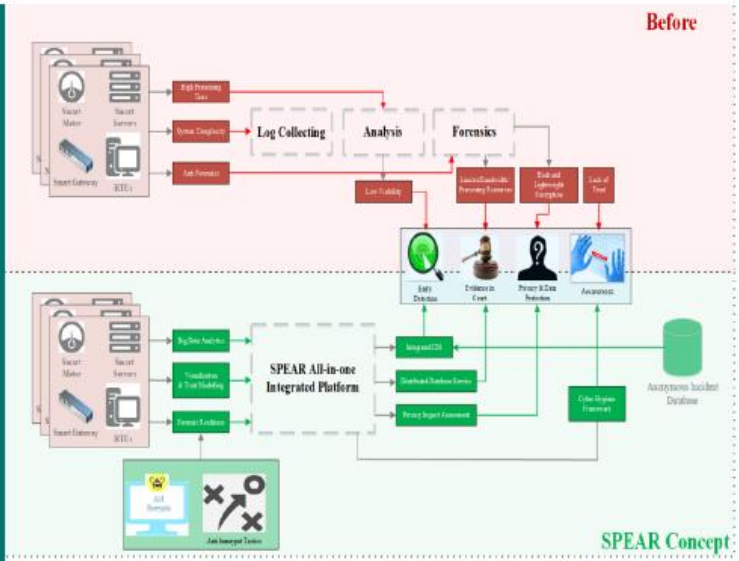
Contents:

Figure 6: 1st page of the newsletter

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

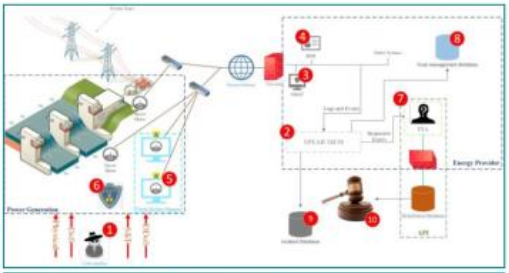
The Project Officer (PO), Mr. Nikolaos Panagiotarakis, participation in the kick-off meeting allowed to draw conclusions on the maturity of the project plan, the appropriateness of work-distribution among beneficiaries and the overall quality of the partnership proposing the project.

Figure 7: 2nd page of the newsletter

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.

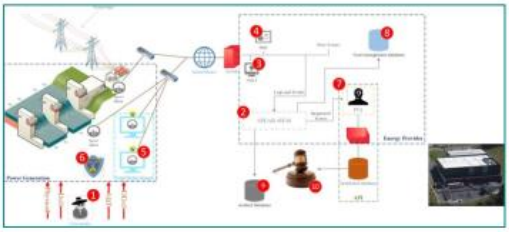


Use case 1: Hydro Plant Scenario

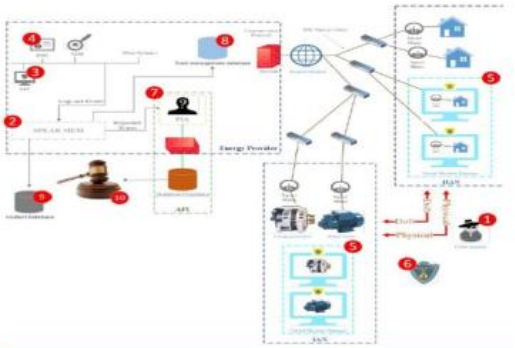
Use Case 2: The Substation Scenario

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.

Figure 8: 3rd page of the newsletter

Figure 9: 4th page of the newsletter

4. Dissemination and communication activities

4.1 Publications

During the first year of the project five publications were accepted for publications. The detailed list is the following:

- N. Banerjee, T. Giannetsos, E. Panaousis and C. C. Took, "Unsupervised Learning for Trustworthy IoT," 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Rio de Janeiro, 2018, pp. 1-8. doi: 10.1109/FUZZ-IEEE.2018.8491672

- Triantafyllou, P. Sarigiannidis, A. Sarigiannidis, E. Rios, and E. Iturbe, “Towards an anonymous incident communication channel for electric smart grids,” in Proceedings of the 22nd Pan-Hellenic Conference on Informatics - PCI ’18, 2018, pp. 34–39. doi: 10.1145/3291533.3291559
- P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos, and S. Oikonomou, “An Overview of the Firewall Systems in the Smart Grid Paradigm,” in 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, October, pp. 1–4. doi: 10.1109/GIIS.2018.8635747
- P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree,” in 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, no. October, pp. 1–5. doi: 10.1109/GIIS.2018.8635743
- P. Radoglou-Grammatikis and P. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, IEEE Access. doi: 10.1109/ACCESS.2019.2909807

Furthermore, four more articles were submitted for publication and are now in the review process:

- D. Pliatsios, P. Sarigiannidis, A. Sarigiannidis, G. Sakellari, E. Panaousis, “Revisiting the Arsenal of Smart Grid Against Security Threats: Big Data, Analytics, Anomaly Detection and Requirements”, IEEE Access
- D. Pliatsios, P. Sarigiannidis, T. Lagkas, A. Sarigiannidis, “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics”, IEEE Communications Surveys and Tutorials
- P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. N. Kafetzakis, E. Panaousis, "Risk Assessment of the IEC 60870-5-104 Protocol in the Smart Grid", submitted to 2019 1st Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined and Virtualized Infrastructures.
- C. Dalamagkas, P. Sarigiannidis, D. Ioannidis, E. Iturbe, O. Nikolis, F. Ramos, E. Rios, A. Sarigiannidis and D. Tzovaras, "A Survey On Honeypots, Honeynets And Their Applications On Smart Grid", submitted to 2019 1st Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined and Virtualized Infrastructures.

The abstracts of both the published and submitted applications are presented in Table 1.

Table 1: Abstract of submitted publications

Title	Abstract
Unsupervised Learning for Trustworthy IoT	The advancement of Internet-of-Things (IoT) edge devices with various types of sensors enables us to harness diverse information with Mobile Crowd-Sensing applications (MCS). This highly dynamic setting entails the collection of ubiquitous data traces, originating from sensors carried by people, introducing new information security challenges; one of them being the preservation of data trustworthiness. What is needed in these settings is the timely analysis of these large datasets to produce accurate insights on the correctness of user reports. Existing data mining and other artificial intelligence methods are the most popular to gain hidden insights from IoT data, albeit with many challenges. In this paper, we first model the cyber trustworthiness of MCS reports in the presence of intelligent and colluding adversaries. We then rigorously assess, using real IoT datasets, the effectiveness and accuracy of well-known data mining algorithms when employed towards IoT security and privacy. By taking into account the spatio-temporal changes of the underlying phenomena, we demonstrate how concept drifts can masquerade the existence of attackers and their impact on the accuracy of both the clustering and classification processes. Our initial set of results clearly show that these unsupervised learning algorithms are prone to adversarial infection, thus, magnifying the need for further research in the field by leveraging a mix of advanced machine learning models and mathematical optimization techniques.
Towards an Anonymous Incident Communication Channel for Electric Smart Grids	The Electric Smart Grid (ESG) is an intelligent Critical Infrastructure (CI) aiming to create an automated and distributed advanced energy delivery network, while preserving information privacy. This study proposes the implementation of an Anonymous Incident Communication Channel (AICC) amongst smart grids across Europe to improve situational awareness and enhance security of the new electric intelligent infrastructures. All participating organizations will have the ability to broadcast sensitive information, stored anonymously in a repository, without exposing the reputation of the organisation. This work focuses on the requirements of establishment, the possible obstacles and proposed data protection techniques to be applied in the AICC. Furthermore, a discussion is conducted regarding the documentation of cyber-incidents. Last but not least, the benefits and the potential risks of this AICC concept are also provided.
Unsupervised Learning for Trustworthy IoT	The advancement of Internet-of-Things (IoT) edge devices with various types of sensors enables us to harness diverse information with Mobile Crowd-Sensing applications (MCS). This highly dynamic setting entails the collection of ubiquitous data traces, originating from sensors carried by people, introducing new information security challenges; one of them being the preservation of data trustworthiness. What is needed in these settings is the timely analysis of these large datasets to produce accurate insights on the correctness of user reports. Existing data mining and other artificial intelligence methods are the most popular to gain hidden insights from IoT data, albeit with many challenges. In this paper, we first model the cyber trustworthiness of MCS reports in the presence of intelligent and colluding adversaries. We then rigorously assess, using real IoT datasets, the effectiveness and accuracy of well-known data mining algorithms when employed towards IoT security and privacy. By taking into account the spatiotemporal changes of the underlying phenomena, we demonstrate how concept drifts can masquerade the existence of attackers

Title	Abstract
	and their impact on the accuracy of both the clustering and classification processes. Our initial set of results clearly show that these unsupervised learning algorithms are prone to adversarial infection, thus, magnifying the need for further research in the field by leveraging a mix of advanced machine learning models and mathematical optimization techniques.
An Overview of the Firewall Systems in the Smart Grid Paradigm	The multiple interconnections and the heterogeneity of the devices and technologies into the Smart Grid (SG) generate possible cyber-physical security vulnerabilities that can be exploited by various cyber-attackers. The cyberattacks in SG, usually target the availability and the information integrity of the systems. Replay attacks, Denial of Service (DoS), Distributed Denial of Service (DDoS) and botnets are typical examples. Furthermore, the hacking tools have been largely automated, so even a novice can execute destructive cyberattacks. These situations make it necessary to develop efficient firewall systems that can prevent possible cyberattacks. In this paper, we present an overview of the various firewall systems in the SG paradigm and also, we provide new research directions in this field.
An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree	The SG paradigm constitutes the new technological evolution of the traditional electrical grid, providing remote monitoring and controlling capabilities among all its operations through computing services. These new capabilities offer a lot of benefits, such as better energy management, increased reliability and security, as well as more economical pricing. However, despite these advantages, it introduces significant security challenges, as the computing systems and the corresponding communications are characterized by several cybersecurity threats. An efficient solution against cyber-attacks is the Intrusion Detection Systems (IDS). These systems usually operate as a second line of defence and have the ability to detector even prevent cyberattacks in near real-time. In this paper, we present a new IDS for the Advanced Metering Infrastructure (AMI) utilizing machine learning capabilities based on a decision tree. Decision trees have been used for multiple classification problems like the distinguishment between the normal and malicious activities. The experimental evaluation demonstrates the efficiency of the proposed IDS, as the Accuracy and the True Positive Rate of our IDS reach 0.996 and 0.993 respectively
Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems	The SG paradigm is the next technological leap of the conventional electrical grid, contributing to the protection of the physical environment and providing multiple advantages such as increased reliability, better service quality, as well as efficient utilisation of the existing infrastructure and the renewable energy resources. However, despite the fact that it brings beneficial environmental, economic and social changes, the existence of such a system possesses important security and privacy challenges, since it includes a combination of heterogeneous, co-existing smart and legacy technologies. Based on the rapid evolution of the Cyber-Physical Systems (CPS), both academia and industry have developed appropriate measures for enhancing the security surface of the SG paradigm by, for example, integrating efficient, lightweight encryption and authorisation mechanisms. Nevertheless, these mechanisms may not prevent various security threats, such as DoS attacks that target on the availability of the underlying systems. An efficient countermeasure against several cyberattacks is the Intrusion Detection and Prevention System (IDPS). In this paper, we examine the contribution of IDPS in the SG paradigm, providing an analysis of 37 cases. More detailed, these systems can be considered as a secondary defence mechanism, which

Title	Abstract
	enhances the cryptographic processes, by timely detecting or/and preventing potential security violations. For instance, if a cyberattack bypasses the essential encryption and authorisation mechanisms, then the IDPS systems can act as a secondary protection service, informing the system operator for the presence of the specific attack or enabling appropriate preventive countermeasures. The cases we study focused on the AMI, Supervisory Control and Data Acquisition (SCADA) systems, substations and synchrophasors. Based on our comparative analysis, the limitations and the shortcomings of the current IDPS systems are identified, while appropriate recommendations are provided for future research efforts.
Revisiting the Arsenal of Smart Grid Against Security Threats: Big Data, Analytics, Anomaly Detection and Requirements	The environmental concerns, the limited availability of conventional energy sources, the integration of alternative energy sources and the increasing number of power-demanding appliances and electric vehicles progressively change the way electricity is generated and distributed. SG is an appealing concept, which was developed in response to the emerging issues of electricity generation and distribution. It utilizes information and communications technologies, offering thus significant benefits to energy providers, retailers and consumers. However, SG is vulnerable to cyber-attacks, which could cause critical economic and ecological consequences. An effective way to mitigate cyber-attacks is through traditional IDSs. These though are starting to become less efficient due to their limited capabilities of analysing the constantly increasing amount of network traffic. Therefore, the need for analysing vast amount of data has led to the use of machine learning and more recently Big Data (BD) concepts within intrusion detection mechanisms. In this paper we provide an extensive overview of the related work on BD-enabled IDS mechanisms and the most efficient classification methods in detecting anomalies in the SG systems. We also propose a BD-IDS architecture, which features high scalability, distributed deployment, utilization of honeypots and novel real-time traffic classification. The innovation behind this paper lies in the interconnection between SG and BD subject to security and privacy requirements, while a novel architecture is presented as a way of implementing a secure and privacy-preserving SG paradigm.
A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics	SCADA systems are the underlying monitoring and control components of CIs, such as power, telecommunication, transportation, pipelines, chemicals and manufacturing plants. Legacy SCADA systems operated on isolated networks, which made them resistant to cyber-attacks. However, the increasing integration of SCADA systems with the Internet introduces severe security issues. Security considerations for SCADA systems are gaining higher consideration as the number of security incidents against these CIs is increasing. In this survey, we provide an overview of the general SCADA architecture, along with a detailed description of the SCADA communication protocols. Additionally, we discuss certain high-impact security incidents, objectives, and threats. Furthermore, we carry out an extensive review of the security proposals and tactics that aim to secure SCADA systems. We also discuss the state of SCADA system security. Finally, we present the current research trends and future advancements of SCADA security.
A Survey on Honeypots, Honeynets And Their Applications on	Power grid is a major part of modern CI. The rapid evolution of Information and Communication Technologies (ICT) enables traditional power grids to encompass advanced technologies that allow them to monitor their state, increase their reliability, save costs and provide ICT services to end customers, thus converting them into smart grids. However, smart grid is

Title	Abstract
Smart Grid	exposed to several security threats, as hackers might try to exploit vulnerabilities of the industrial infrastructure and cause disruption to national electricity system with severe consequences to citizens and commerce. This paper investigates and compares honey-x technologies that could be applied to smart grid in order to distract intruders, obtain attack strategies, protect the real infrastructure and form forensic evidence to be used in court.

4.2 Presence at events

During the first year, SPEAR partners participated in the event presented in Table 2 while more details for each of these events are presented next.

Table 2: Presence at events

Title	Date	Location	Presenter
EPRI advisory meeting	23/05/2018	Madrid, Spain	Pablo Gómez-Calvente (ENEL)
3rd Energy Tech Forum	15/11/2018	Athens, Greece	Panagiotis Sarigiannidis (UOWM), George Kakamoukas (UOWM), Dimitris Pliatsos (UOWM), Panagiotis Radoglou-Grammatikis (UOWM) and Anna Triantafyllou (UOWM)
GHOST H2020 Clustering workshop	28/03/2019	Athens, Greece	Theodoros Rokkas (INC)

EPRI advisory meeting

The EPRI Power Delivery & Utilization (PDU) International Advisory meeting focused on challenges in the International Electricity Industry pertaining to Energy Utilization, Distribution, Transmission and Sub-stations, Information and Communication Technology, Cyber Security, Power Quality and Energy Storage and Efficiency. The meeting offered insight into the dynamic research EPRI is doing in these areas and will also highlight how some International utilities are preparing for and adapting to the evolution of the electric power industry. Guest speakers from across Europe, Asia and the Middle East shared their utility and regional perspective on challenges, potential improvements and their vision for the future as they collaborate with EPRI on solutions. Enel participated with a presentation regarding to the European Initiatives on Smart Grid Cyber Security, among them, the SPEAR project.

3rd Energy Tech Forum

The third "Energy Tech Forum", organised by energia.gr, focused on energy technologies and innovation. The event took place on October 16, 2018 at the Eugenides Foundation in Athens, Greece. The forum had representatives from energy projects towards increasing efficiency in electric power consumption. Representing SPEAR, Panagiotis Sarigiannidis from UOWM participated and presented an overview of the SPEAR project. The audience includes 30 persons and were composed of electrical, mechanical engineers and researchers from academic institutions and SMEs.

GHOST H2020 Clustering workshop

GHOST project organized a clustering workshop at 28th of March 2019 Athens, Greece. The workshop had representatives from 25 projects in the area of ICT security. Representing SPEAR, Theodoros Rokkas from

INC was present and presented an overview of the SPEAR. The audience includes 30 persons and were composed from security experts and researchers from academic institutions and SMEs.

4.3 Media

A radio interview of the Project Coordinator (PC), Dr. Panagiotis Sarigiannidis, was given during the first year of the project to the Hellenic Broadcasting Corporation. During this interview, Dr. Sarigiannidis, was asked and talked about the motivation of the SPEAR project, the need for cyber-security frameworks that shield the Critical Infrastructure and the innovation as well as the SPEAR's impact to society and Critical Infrastructure protection. The interview was in the Greek language and the full audio of the interview has been uploaded on the SPEAR's YouTube channel and is available on the following link: https://www.youtube.com/watch?v=9I1VQAfTe-A

In the same concept, a similar interview was given by the PC to the local newspaper "ThessNews" of Thessaloniki, Greece, about the SPEAR project and how it can help to secure the next generation smart grids. The full text of this interview is available on the following link: https://www.linkedin.com/feed/update/urn:li:activity:6418884764400381952

5. Dissemination KPIs (INC)

The monitoring of dissemination and communication activities is an essential process to evaluate the success and efficiency of the plan. SPEAR defined a set of Key Performance Indicators (KPIs) that monitor the progress and impact of the dissemination and communication activities and act as guidance to take proper actions. Table 3 presents the KPIs that introduced in D8.2 and an update on the current achieved status.

Table 3: KPIs

No	KPI	Audience	Objective (min value)	Values at end of fist year
1	Organization and/or Attendance to exhibitions	Strategic stakeholders, Industry	200 visitors	SPEAR was present at 3 events with an estimated number of 150 people
2	Workshops co-located with major conferences	Research community, Strategic stakeholders, Industry, Other Projects	1-2 workshops per year	SPEAR was present in 1 workshop at first year
3	On-site demonstrations	Research community, Strategic stakeholders, Industry	3 demonstrations	This activity is planned to take place during the third year of the project
4	Publications in workshops,	Research community	Workshop papers (1-3 per year)	4 conferences 1 journal

	conferences and journals		Conference papers (1-2 per year) Journal papers (1-2 per year)	
5	Online publications (magazines, newspapers, blogs)	Research community, Strategic stakeholders, Industry, Public	10 publications per year 500 views	
6	Posts to social networks	Research community, Strategic stakeholders, Industry, Public	10 posts 100 contacts 50 likes/share 5 comments	8 posts 32 followers 89 likes, 4 shares 1 comment
7	Participation in CeBIT	Research community, Strategic stakeholders, Industry, Public	5 brochure copies delivered	-
8	Project website	Research community, Strategic stakeholders, Industry, Other Projects, Public	Top 5 SEPR	• spear • spear project • spear security • www spear • h2020 cybersecurity project
9	Inclusion of light content for non-specialized audience in the project website, blog, social media, as well as publishing "lighter" versions of project newsletters, leaflets, flyers, etc.	Public	5 material 100 reads	1 newsletter has been published in the SPEAR website
10	Summer schools / open events with free access, where visitors will realize in a lively way the SPEAR benefits.	Research community, Strategic stakeholders, Industry, Other Projects, Public	1 summer school 50 attendees 1 open event	-

11	Participation in media (TV, newspapers, radio) events	Public	10 media appearances	2 appearances in media

The following section provides information about each of the KPIs along with the plan to meet them.

KPI 1: Organization and/or attendance to exhibitions

SPEAR has participated in three events (see section 4.2), with an estimated audience of 150. This KPI is on track.

KPI 2: Workshops co-located with major conferences

SPEAR results were presented in one workshop that was organized by the GHOST project. The 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures is co-organized by SPEAR. (see section 6).

KPI 3: On-site demonstrations

This activity is planned to take place during the final year of the project.

KPI 4: Publications in workshops, conferences and journals

There were four conference publications and one Journal publication during the first year while there are two more submitted in workshops and two submitted in Journals (see section 4.1). The KPI for the first year has been met.

KPI 5: Online publications (magazines, newspapers, blogs)

This KPI is low during the first year, as a preventive meter in order to achieve it a detailed plan was created for the next year activities. (see section 3.3)

KPI 6: Posts to social networks

The KPI is on track for the first year. More specifically, the LinkedIn account of SPEAR has in total 32 of 100 followers, 8 of 10 posts and 1 of 5 comments. The target of posts and shares has been met since 89 likes and 4 shares have been gathered.

KPI 7: Participation in CeBIT

Since CeBIT 2019 was cancelled the consortium plans to identify an alternative exhibition to participate, this will happen at the last year of the project.

KPI 8: Project website (SEPR)

The Google Search Console platform has been employed in order to measure the SEPR KPI. The platform shows the following top-5 SEPR keywords that visitors search in search engines in order to find our website:

- spear
- spear project
- spear security
- www spear
- h2020 cybersecurity project

KPI 9: Light content for general public

One newsletter has been published until now (see section 3.3). Four more are planned to be produced every year (every three months) in order to achieve this KPI.

KPI 10: Summer schools/open events

This activity is planned to take place during the final year of the project.

KPI 11: Media appearances

Two appearances took place in the first year, their number is expected to increase the second and third year as more results are produced.

6. Plans for second year (all)

Two one-page posters are planned to be published in electronic form and uploaded to the SPEAR website and social media. Those posters will be market-oriented, addressed mainly to the general public and stakeholders, and will illustrate the SPEAR's platform components and the use cases that the SPEAR consortium realises and stakeholders will be interested in.

In addition, more leaflets are planned to be published upon public deliverables and outputs dissemination activities are available. Future leaflets will inform the general public and stakeholders about accepted publications related to the SPEAR project, the context of new public deliverables as well as upcoming dissemination activities.

Moreover, the SPEAR consortium plans to enhance the media content of its YouTube channel by uploading videos that demonstrate some components of the SPEAR platform as well as cyberattacks or methods that are produced in the context of SPEAR's dissemination activities and publications.

To share the project progress with the scientific community, the consortium will draft articles and other contributions for the technical literature and dedicated journals. Such contributions will be written by academic and technology partners, through peer-reviewed journals and magazines and also through papers presented at conferences and other events. A list of Journals that are covering the research areas of SPEAR has been compiled and presented in Table 4 while a list of future conferences is presented in Table 5.

Table 4: list of Journals

Journals	Link
Applied Energy	**http://www.sciencedirect.com/science/journal/0306261**
Computers & Electrical Engineering	**http://www.sciencedirect.com/science/journal/0045790/open-access**
Computers, Environment & Urban Systems	**http://www.sciencedirect.com/science/journal/01989715/open-access**
Computers in Human Behavior	**http://www.sciencedirect.com/science/journal/07475632**
The Electricity Journal	**http://www.sciencedirect.com/science/journal/10406190**
Electric Power Systems Research	**http://www.sciencedirect.com/science/journal/03787796**
Energy - an international journal	**http://www.sciencedirect.com/science/journal/03605442**

Energy Policy	**http://www.sciencedirect.com/science/journal/03014215**
Energy Reports	**http://www.sciencedirect.com/science/journal/23524847**
Energy Research & Social Science	**http://www.sciencedirect.com/science/journal/22146296**
Energy Strategy Reviews	**http://www.sciencedirect.com/science/journal/22146296**
Energy Conversion & management	**http://www.journals.elsevier.com/energy-conversion-and-management**
Journal of Electrical Systems and Information Technology	**http://www.journals.elsevier.com/journal-of-electrical-systems-and-information-technology**
Journal of Environmental Management	**http://www.journals.elsevier.com/journal-of-environmental-management**
Sustainable cities and societies	**http://www.journals.elsevier.com/sustainable-cities-and-society**
Sustainable Energy Technologies and Assessments	**http://www.journals.elsevier.com/sustainable-energy-technologies-and-assessments**
Utilities Policy	**http://www.journals.elsevier.com/utilities-policy**
IEEE Transactions on Industry Applications – Special Issue, Security, Reliability, Privacy, and Quality in Industrial Automation and Control	**https://ias.ieee.org/publications/ieee-transactions-on-industry-applications.html** **http://jolfaei.info/IEEE-Trans-IAS.html**
IEEE Transactions on Power Systems	**https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=59**
IEEE Transactions on Industrial Informatics	**https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424**
Pattern Recognition Elsevier	**https://www.journals.elsevier.com/pattern-recognition**
Information Sciences Elsevier	**https://www.journals.elsevier.com/information-sciences**

Table 5: List of conferences

Conference	Timing	Place
European Utility Week	12-14/11 2019	Paris, France
Innogrid2020+ (2020)	Not available yet	-
ETP SmartGrids General Assembly	Not available yet	-
European Sustainability Energy Week 2020	Not available yet	-
International Council on Large Electric Systems CIGRE 2020	Not available yet	-
International Conference on Electricity Distribution - CIRED 2020	Not available yet	-
Protection, Automation & Control World Conference – PAC World	17-20/06	Glasgow, UK
4th International Conference on Digital Signal Processing (ICDSP 2020)	21-24/02/2020	Chengdu, China
25th International Conference on Pattern Recognition	Not available yet	Milan, Italy

Presence at events

For the second year SPEAR will have a presence at the following events:

- CERTH - Smart Home expo Indelex, 11th - 13th of May 2019: This event will present the Smart-Home innovations. Part of the innovation is the SPEAR Smart-Home use case in a wider context of the cyber-security in Home/Work environments.

- CERTH - Open Day 2019, 10th of May: This event is open to the public and is organized in the premises of CERTH. In this event, the main objectives, the goals and the innovative technologies developed and used in the SPEAR project are going to be presented.

- An open event titled “Seminar on Smart Grids Cybersecurity and challenges – The SPEAR project” will be organised at the end of May 2019 by the Public Power Corporation (PPC) and “IIEK ALFA”, in the context of the Education Festival 2019 (https://www.education-festival.edu.gr). The event is mainly addressed to the general public, students, professionals and individuals interested in automation and cybersecurity in IoT, industrial networks and smart grids. The lecturers, Solon Athanasopoulos (PPC) and Christos Dalamagkas (PPC) will talk about modern smart grids, the ongoing transition from conventional power grids to modern smart grids and the challenges that are faced during this transition. In the context of this seminar, the SPEAR project will be introduced, particularly what is its motivation and how SPEAR can help to address the cybersecurity and privacy challenges of smart grids.

- Igor Kotsiuba will give a speech on June 5th for "The cyberhygiene in Smart Grids" at the Malware Forum. https://www.nsm.stat.no/norcert/norcertforum2019/

Workshops

The 1st Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft) is a joint initiative from the H2020 EU Projects ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD, and 5GENESIS to create a dialogue about emerging cyber-security paradigms for virtualized environments and critical infrastructures. The workshop is co-located with IEEE NetSoft 2019, will be held on June 24, 2019, in Paris, France.

SPEAR participates in the organizing committee of SecSoft 2019 with the following members:

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

The workshop will take place in Paris, France on June 24th. More details can be found in: https://www.astrid-project.eu/secsoft/cfp.html

Table of Figures

Table of Tables