Secure and private smart grid: the SPEAR project

Panagiotis Radoglou-Grammatikis and Panagiotis Sarigiannidis

The digital world we currently enjoy with intelligent environments and smart devices has not been accomplished without difficulty. Intelligent objects make our lives comfortable, more straightforward and automated. However, this digital reality comes with severe cybersecurity and privacy issues due to the vulnerabilities of smart and legacy technologies.

Adobe Stock © Felix

Cyberattacks are socially or politically motivated malicious actions carried out primarily via the weaknesses of the typical internet model. A decade ago, the cyber-defensive mechanisms focused mainly on mitigating and preventing cyberattacks targeting websites and web applications. Now, given the digital era of the industrial internet of things (IIoT), a cyberattack against a critical infrastructure (CI) could significantly affect human lives.

Since our society is explicitly dependent on CIs, the cybersecurity mechanisms should be adapted and optimised appropriately to meet the security requirements of CIs, taking into account their sensitive nature and the continuous operation. Detecting and preventing intrusions carried out by a highly-skilled, persistent and coordinated group of cyberattackers remains a challenging task. The smart grid (SG) is one of the most vulnerable CIs where malicious cyber activities can lead to disastrous consequences, cascading effects or even fatal accidents (Radoglou-Grammatikis & Sarigiannidis, 2019).

In particular, the SG is considered as the next-generation electrical grid promising multiple benefits and services, such as self-healing, improved resilience and pervasive control. However, since this paradigm is adopted globally among various energy stakeholders, more and more intruders try to violate the security of the SG assets. In parallel, the SG incorporates legacy assets, such as supervisory control and data acquisition (SCADA)/industrial control systems (ICS), that are vulnerable to a plethora of unauthorised activities due to the necessary presence of insecure communication protocols (Gunduz & Das, 2020). Characteristic examples are Modbus and IEC 60870-5-104. According to the European Network and Information Security Agency (ENISA): "A cybersecurity incident against electrical power and energy systems (EPES) is considered as any security event, which aims to affect the essential cybersecurity principles related to the involved assets originating either from the electrical engineering sector or the information and communication technology (ICT) area." Consequently, it is evident that the SG evolution generates enormous cybersecurity and privacy challenges.

Currently, the cybersecurity incidents against CIs have been seriously intensified. One example is the cyberattack on a Ukrainian power station that caused a power outage for over 225,000 people. Other advanced persistent threats (APTs) are DragonFly, Dugu, Flame, Stuxnet, TRITON and DragonFly2. The current detection and mitigation solutions do not consider the unique characteristics and peculiarities of the modern electrical grid. Furthermore, they do not consider the capacity of advanced visualisation methods capable of recognising anomalous events and situations. Moreover, the forensic mechanisms are limited only to monitoring and logging (Gunduz & Das, 2020) activities without extracting clear evidence that can be used in court. Therefore, stealthy attacks can evade the typical countermeasures. Hence, the following challenges are identified: *(a)* enhancing the EPES/SG resiliency and reliability; *(b)* detecting and mitigating timely and accurately EPES/SG cyberattacks; *(c)* addressing multi-step attack scenarios, such as APTs; *(d)* enhancing digital forensic solution taking into account privacy concerns; *(e)* optimising the trust among the EPES/SG assets; and *(f)* empowering EU-wide consensus.

SPEAR objectives

SPEAR (Secure and PrivatE smArt gRid) is a Research and Innovation Action (RIA) project funded by the Horizon 2020 framework programme of the European Union, aiming to provide an integrated solution capable of: *(a)* detecting timely potential cyberattacks/anomalies (e.g. disturbances) against the SG environments; *(b)* ensuring the presence of sufficient forensic mechanisms collecting the necessary attack traces and preparing the appropriate legal processes; *(c)* providing an anonymous repository of cybersecurity incidents for the energy sector; and *(d)* introducing a cyber hygiene framework, evaluating the cybersecurity readiness level of the EPES personnel and providing a web-based training environment, which will continually inform and educate the EPES personnel about the best practices in the cybersecurity domain. SPEAR focuses on the following primary objectives.

Objective #1: define the SPEAR system architecture, the security components and the privacy framework for situational awareness provisioning in relation to cybersecurity threats

The first objective is related to defining the architecture of the SPEAR solution, which will constitute an integrated platform, comprising: *(a)* detection and correlation components; *(b)* a forensic repository; *(c)* deception components; *(d)* an anonymous repository of incidents; and *(e)* a cyber hygiene framework. To this end, the ARCADE framework (Radoglou-Grammatikis, *et al.*, 2020) will be adopted, identifying the functional and non-functional requirements, the data model, the various components and their interfaces.

Objective #2: build attack detection mechanisms and promote resilience operations in SG

A significant aspect of SPEAR is to accurately detect the various cyberattacks and anomalies against the EPES assets in a timely manner. To this end, machine learning (ML) and deep learning (DL) models have been implemented, detecting a plethora of cyberattacks against a plethora of multiple EPES industrial protocols, such as Modbus, Distributed Network Protocol 3 (DNP3), IEC 60870-5-104, IEC 61850/Manufacturing Message Specification (MMS), Message Queuing Telemetry Transport (MQTT), BACnet, Network Time Protocol (NTP), Secure Shell (SSH), RADIUS and Hypertext Transfer Protocol (HTTP). The various ML/DL detection models are incorporated into a common component called a big data analytics component (BDAC).

Moreover, SPEAR includes a visual-based intrusion detection system (VIDS) capable of distinguishing electrical disturbances and other kinds of anomalies, using advanced visual analytics with operational data (i.e. time series electricity measurements).

Objective #3: increase situational awareness in SG networks

After the detection processes, SPEAR aims to enhance situational awareness, utilising correlation mechanisms. To this end, based on the various security events detected by BDAC, VIDS and AlienVault OSSIM, the Grid Trusted Module (GTM) re-calculates the reputation score of each EPES assets, utilising fuzzy logic rules. The reputation score represents the trust level of each EPES asset within a sub-network.

Objective #4: create and maintain an anonymous repository of SG incidents

SPEAR also intends to contribute to global situational awareness by creating and maintaining a repository of SG incidents. The rationale behind the creation of this repository is to broadcast, inform and exchange critical information about cyberattack incidents in SG environments across Europe. To this end, the SPEAR Repository of Incidents (SPEAR RI) will be implemented and compliant with the best practices designed by relevant organisations, such as the European Energy - Information Sharing & Analysis Centre (EE-ISAC) and the European Smart Metering Industry Group (ESMIG). SPEAR RI incorporates appropriate anonymisation mechanisms, thus protecting the reputation of the EPES organisations related to cybersecurity incidents. Simultaneously, it maintains the technical details behind the cybersecurity incidents.

Objective #5: provide smart network forensics subject to data protection and privacy

SPEAR intends to provide a forensic readiness framework (FRF), which will guarantee the digital forensic actions and collection of the evidence, taking into account the privacy of the involved entities. To this end, the OSCAR methodology will be followed—obtain information, strategise, collect evidence, analyse and report. Moreover, a data privacy impact assessment (DPIA) procedure will be determined, considering the data flows related to the SPEAR components. Finally, in the context of the SPEAR FRF, a forensic repository (FR) will be developed, including visualisation capabilities, thus facilitating the work of the forensic investigator.

OSCAR
Obtain information
Strategise
Collect evidence
Analyse
Report

Objective #6: empower EU-wide consensus of cybersecurity in SG systems

Based on the guidelines of NIST SP 800-53 and NIST SP 800-82, there is no current EU-wide consensus on the minimum range of capabilities required for smart devices and meters. A risk assessment is needed in all layers of security (physical, smart metering, networking and application) to increase society's resilience to significant threats. In the context of the SPEAR architecture, authorities and energy utilities can anonymously share information about their vulnerabilities without exposing critical geographical or technical details. SPEAR RI will bring together multiple EPES organisations across Europe, thus forming a network of trust where the various entities can exchange information about the various cybersecurity incidents.

Objective #7: validate the SPEAR architecture capabilities in proof-of-concept use cases

The SPEAR consortium has selected four high-impact use cases to validate the objectives of the SPEAR architecture, namely the:

- hydropower plant
- substation
- combined use case
- smart house use case.

Each use case is characterised by different needs and security requirements that are met by SPEAR. Thus, SPEAR can satisfy various EPES cases and stakeholders in detecting, correlating, and mitigating cyberattacks and anomalies.

Objective #8: design an innovative business model and conduct a techno-economic analysis to strengthen the role of European SG and the cybersecurity industry in the global market

One of the main goals of SPEAR is to strengthen the role of the European SG security domain in the global market. SPEAR aims to provide the European Union (EU) SG security industry with the necessary innovation capacity to increase its leading role in the world business field. The main rationale behind this objective is to seek exploitation opportunities of the SPEAR results by identifying potential market sectors and including a revenue prediction.

SPEAR architecture

As illustrated by Figure 1, the architecture of SPEAR consists of three main components: *(a)* SPEAR Security Information and Event Management System (SIEM); *(b)* SPEAR FRF; and *(c)* SPEAR RI.

SPEAR SIEM is the flagship of SPEAR, integrating the intrusion/anomaly detection and correlation mechanisms (Radoglou-Grammatikis, *et al.*, 2021). First, SPEAR SIEM uses AlienVault OSSIM with respect to its signature/specification-based intrusion detection systems (i.e. OSSEC and Suricata). SPEAR sensors are deployed throughout the EPES subnets, collecting the network traffic and operational data.

Next, the Data Acquisition Processing and Storage (DAPS) receives and normalises the data from the various SPEAR sensors. The normalised data is used by BDAC and VIDS in order to detect potential cyberattacks and anomalies. BDAC applies ML/DL detection models to recognise security violations against EPES industrial protocols, while VIDS uses dimensionality reduction techniques to identify anomalies concerning the operational data.

GTM then receives the security events generated by BDAC, VIDS and AlienVault OSSIM and re-calculates the reputation value of each EPES asset. Finally, the message bus represents an asynchronous communication system, which facilitates communication among the aforementioned SPEAR SIEM components.

On the other side, SPEAR FRF includes three main components: *(a)* honeypots; *(b)* honeypot manager; and *(c)* SPEAR forensic repository (FR). Honeypots are intentional security holes that aim to trap potential cyberattackers. In the context of SPEAR, the honeypots are deployed through the honeypot manager, which applies a strategic game theory model, taking into account the benefits and the costs of the defender and the attacker side. The SPEAR FR collects the necessary forensic information related to the various security violations, including the honeypots' logs and security events generated by SPEAR SIEM. Finally, SPEAR RI receives, anonymises and distributes the security events generated by SPEAR SIEM of various EPES organisations. To this end, SPEAR RI uses the Malware Information Sharing Platform (MISP) platform. It is noteworthy that the aforementioned SPEAR components are consolidated into an integration environment with a common dashboard.

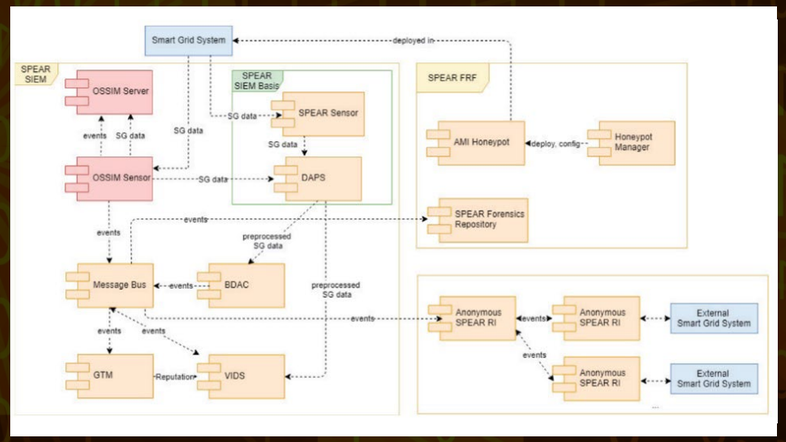

Figure 1: SPEAR architecture.

References

Gunduz, M. Z. & Das, R., (2020) 'Cyber-security on smart grid: Threats and potential solutions', *Computer Networks*, p. 107094.

Radoglou-Grammatikis, P. & Sarigiannidis, P. (2019) 'Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems', *IEEE Access*, pp. 46595–46620.

Radoglou-Grammatikis, P., Iturbe, E., Rios, E., Sarigiannidis, A., Nikolis, O., Ioannidis, D. Machamint, V., Tzifas, M., Giannakoulias, A., Angelopoulos, M., Papadopoulos, A. and Ramos, F. (2020) *Secure and Private Smart Grid: The SPEAR Architecture.* s.l., s.n.

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M. and Ramos, F. (2021) 'SPEAR SIEM: A Security Information and Event Management system for the Smart Grid', *Computer Networks*, p. 108008.

Adobe Stock © Irina

SPEAR

PROJECT SUMMARY

The rapid evolution of the smart technologies has digitised the electrical grid into a new paradigm called smart grid (SG). Despite the multiple benefits, this reality raises severe cybersecurity concerns. SPEAR provides a global cybersecurity solution, which *(a)* detects SG-related cyberthreats, *(b)* provides an advanced forensic readiness framework; and *(c)* introduces an SG cyber hygiene framework.

PROJECT LEAD

SPEAR provides a global cybersecurity solution, which *(a)* detects SG-related cyberthreats, *(b)* provides an advanced forensic readiness framework; and *(c)* introduces an SG cyber hygiene framework. The main achievements of SPEAR are: *(a)* SPEAR Security Information and Management System, *(b)* SPEAR Repository of Incidents (SPEAR RI), *(c)* RTU Honeypot; and *(d)* NeuralPot.

PROJECT PARTNERS

University of Western Macedonia (UOWM)
European Dynamics Luxembourg SA (ED)
Fundacion Tecnalia Research & Innovation (TEC)
Enel Iberia SRL (ENEL)
Public Power Corporation S.A. (PPC)
Eight Bells Ltd (8BL)
Incites Consulting SA (INC)
G.E. Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine (PIMEE)
Gottfried Wilhelm Leibniz Universitaet Hannover (LUH)
Sidroco Holdings Ltd (SID)
0 Infinity Ltd (0INF)
Technical University of Sofia (TUC)
MVETS Lenishta OOD (VETS)
Schneider Electric Espana SA (SCHN)

CONTACT DETAILS

Panagiotis Sarigiannidis
Karamanli & Ligeris, Kozani, Greece 501 00

https://ithaca.ece.uowm.gr

/panagiotis-sarigiannidis-7636901a

FUNDING

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