Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach

Athanasios Liatifis[†], Pedro Ruzafa Alcazar[‡], Panagiotis Radoglou Grammatikis[†], Dimitris Papamartzivanos[§], Sofianna Menesidou[§], Thomas Krousarlis[§], Molinuevo Martin Alberto[¶], Iñaki Angulo[¶], Antonios Sarigiannidis[‖], Thomas Lagkas[**], Vasileios Argyriou[††], Antonio Skarmeta[‡] and Panagiotis Sarigiannidis[†]

***Abstract*—The digitisation of the typical electrical grid introduces valuable services, such as pervasive control, remote monitoring and self-healing. However, despite the benefits, cybersecurity and privacy issues can result in devastating effects or even fatal accidents, given the interdependence between the energy sector and other critical infrastructures. Large-scale cyber attacks, such as Indostroyer and DragonFly have already demonstrated the weaknesses of the current electrical grid with disastrous consequences. Based on the aforementioned remarks, both academia and industry have already designed various cybersecurity standards, such as IEC 62351. However, dynamic risk assessment and certification remain crucial aspects, given the sensitive nature of the electrical grid. On the one hand, dynamic risk assessment intends to re-compute the risk value of the affected assets and their relationships in a dynamic manner based on the relevant security events and alarms. On the other hand, based on the certification process, new approach for the dynamic management of the security need to be defined in order to provide adaptive reaction to new threats. This paper presents a combined approach, showing how both aspects can be applied in a collaborative manner in the smart electrical grid.**

***Index Terms*—Certification, Cybersecurity, Energy, Honeypot, Power Grid, Risk Assessment, Software Defined Networking**

I. Introduction

Electrical Grids and Electrical Power and Energy Systems (EPES) in general, are undergoing a radical reformation and evolve into new smart and complex Cyber-Physical Systems (CPS) with modern communication, control and signal processing technologies. This evolution leads to efficient management of diverse energy resources including renewable ones and lower overall carbon emissions. Despite all the benefits, the introduction of smart systems and processes is accommodated by new security concerns in form of cyber attacks that aim to cause large scale disruptions [1]. These cyberattacks may induce different several impacts such as the performance of unauthorized actions by systems devices [2] or loss of productivity and revenue. Based on this both, academia and industry design various cybersecurity standards such as IEC TC57 or IEC 62351.

Neverthless, dynamic risk assessment and management of security consist crucial aspects of modern systems. Recent studies [3] related to risk assessment in CPS focus on the operation of power grids only. There are also studies [4] about the risk assessment analysis in power grid regarding network communication attacks such as Denial of Service (DoS) attacks.

Software Defined Networking (SDN) aims to revolutionise how networks operate and are managed. SDN was originally targeted towards large and complex networks, though it met wide adoption by several other industries and sectors like smart grid communications [5]. SDN offers enhanced monitoring and control over the data plane. This can benefit other services like security tools such as Security Information and Event Management (SIEM) systems, and risk assessment tools with rich and real-time statistics.

On the other hand, there are lines of research in dynamic security policies mostly in the Internet of Things (IoT) architectures [6] which are trying to make different frameworks to cover the entire life cycle of IoT devices due to their constraints and heterogeneity nature. This line is focused on a continuous evaluation of the device security, in this sense, exist different proposals addressing this, such as Manufacturer Usage Description (MUD) standardized by IETF [7], its version Threat MUD [8] and cyber threat intelligence sharing [9].

This work is focused on the development of a new approach for the dynamic evaluation of the devices security and the dynamic risk assessment in a collaborative manner, to give full coverage during all life cycle of all power grid components, combining the continuous risk re-calculation based on alert monitoring and network topology information with the persistent evaluation of the devices security using the knowledge of cyber intelligence, updated risk assessment and updated

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936.

†A. Liatifis, P. Radoglou-Grammatikis and P. Sarigiannidis are with the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece - E-Mail: {aliatifis, pradoglou, psarigiannidis}@uowm.gr

‡P. Rufaza Alcazar and A. Skarmeta are with the Department of Information and Communications Engineering, University of Murcia, Murcia 30100, Spain - E-Mail: {perdro.ruzafaa, askarmeta}@um.es

§ D. Papamartzivanos, S. Menesidou, and T. Krousarlis are with UBITECH Limited, 26 Nikou & Despinas Pattchi, Limassol 3071, Cyprus - E-mail: {dpapamartz, smenesidou, tkrousarlis}@ubitech.com

¶M. Alberto and I. Angulo are with TECNALIA, Basque Research and Technology Alliance (BRTA), Parque Cientifico Y Tecnologico De Bizkaia, Astondo Bidea, Edificio 700, Derio Bizkaia 48160, Spain - E-mail: {Alberto.Molinuevo, inaki.angulo}@tecnalia.com

‖A. Sarigiannidis is with the Sidroco Holdings Ltd, Nicosia, Cyprus - E-Mail: asarigia@sidroco.com

**T. Lagkas is with the Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Greece - E-Mail: tlagkas@cs.ihu.gr

††V. Argyriou is with the Department of Networks and Digital Media, Kingston University London, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE, UK - E-Mail: vasileios.argyriou@kingston.ac.uk

manufacturer security information. Section II provides related work in the scientific areas of Risk Assessment, Certification, Honeypots and SDN intrusion detection in the broader domain of Smart Grid communications. In Section III a dynamic risk assessment framework that incorporates the aforementioned technologies is presented. Finally, Section IV concludes our work and list next steps of our work. In future we plan realising the proposed approach in a real EPES environment and provide experimental results.

II. Related Work

Several studies investigate the security issues of the smart electrical grid. Some of them are listed in [10]–[13]. In [10] the authors present a comprehensive survey with respect to the role of the Intrusion Detection and Prevention Systems (IDPS) in the energy sector. In [13], N. Komninos et al. discuss security issues and challenges with respect to smart homes and the power grid. In [11], A. Ghosal and M. Conti analyse study and analyse key management systems for Advanced Metering Infrastructures (AMIs). Similarly, in [12], the author presents an overall architectural design that takes full advantage of the SDN technology in order to mitigate and prevent potential cybersecurity incidents in a timely manner. In [14], M. Asghar et al. focus on the privacy issues related to the smart meters. In [15], M. Hassan et al. analyse the various differential privacy techniques, considering the unique characteristics of the CPS. Subsequently, we give more emphasis to similar works related to (a) risk assessment, (b) cybersecurity certification, (c) industrial honeypots and (d) SDN-based mitigation techniques.

A. Risk Assessment in the Power Grid

R. Habash et al. in [16] developed a risk assessment framework targeted towards Smart Grid (SG) environments. They start by addressing the issues related to standardisation and ICT integration to the SG paradigm focusing on communication technologies, metering solutions and new energy generation and storage technologies that focus on distributed approaches. Afterwards, an analysis of SG standardisation efforts is presented. The concept of risk is introduced and explained while also a mathematical formulation to estimate the risk is presented. An evaluation of health issues related to wireless technologies is also presented. Finally, the authors present a complete risk management framework suitable for SG. The authors conclude that integrated risk management approaches are needed to efficiently optimize SG processes of risk identification, management and minimize it.

In [17] the author propose a continuous risk management methodology suitable for complex SG environments that include multiple components. The proposed solution can quantify the risk and uses Attack Defence Trees (ADTs) a special type of Directed Acyclic Graph. Specifically, the system consists of five phases, namely, ADT modelling of the system (1), risk assessment (2) and sensitivity analysis (3), optimization (4) and continuous monitoring and adjustment of the system (5). By performing the various operation on the ADT the proposed system can realise the above-mentioned functions. To demonstrate the proposed system, feasibility the authors created the ADToolRisk and ADMind software tools and evaluated it in a real environment of a smart building.

Authors in [18] developed a risk assessment framework for three Synchrophasor Communication Network (SCN) topologies, namely, a. dedicated, b. shared and c. hybrid, which relies on hardware and data reliability to evaluate the risk. A generic hardware reliability model is presented and for each SCN type, a simplified model is developed, while the data integrity reliability model remains the same. Regarding the risk assessment framework, for each type, a dedicated model is developed. To evaluate the proposed system the authors designed various SCN topologies using QualNet simulator, a discrete event simulator. The results indicate that data reliability has a higher impact on the overall risk than hardware reliability. Depending on the end-goals of the CPS one solution may be favored over the others.

The authors in [12] present the SDN-microSENSE architecture, a three tier architecture consisting of a. risk assessment framework (S-RAF), b. an intrusion detection and correlation framework (XL-EDPS) and c. a self-healing framework (SDN-SELF). S-RAF is responsible for collaborative risk assessment and honeypot deployment management. XL-EDPS undertakes the role of reliable and fast detection of cyber attacks against EPES/SG. It is integrated with a Security Information and Event Management (SIEM) system and an anonymous repository of security incidents. The SDN-SELF framework is tasked with enforcing the mitigation strategy to the data plane and the efficient energy balancing after the mitigation process is realised. Finally, the SDN controller responsible for communication with the networking devices that forward traffic in the data plane, and provide statistics to other SDN-microSENSE components.

B. Cybersecurity Certification in the Power Grid

The industry and academy have been designing and developing frameworks to protect themselves against cyber threats in IoT architectures [19], most of these frameworks are based on risk assessment [3], and Intrusion Detection System (IDS) among others [20]. There are a few works regarding the dynamic evaluation of cyber threats that could affect a specific IoT device and build the corresponding countermeasures. These works focus in to define the limitations of its IoT architecture in the deployment phase but do not take special attention to the rest of the IoT device's life cycle, being weak against new potential threats that could appear and affects the normal working of these devices or be a potential risk for possible intrusions and cyber attacks.

In [21] the authors explain that in the power grid sector when false meter data is injected through a cyberattack the control center will be misled and may potentially make an erroneous decision. The authors also explain another way that an intruder can affect the communication network attempting to connect a remote terminal which can allow them to wiretap telecommunication attacking the corporate information system and gain backdoor access to the system. Authors explain a

strategy to detect cyber intrusions such as a network-based cyber intrusion detection system that uses multicast messages in substation automation systems to monitor anomalies and malicious activities.

Authors in [22] propose certain items to attack mitigation in the power grid such as access controls, encryption, and authentication, all of these measures are fine to identify devices and protect the traffic through the network but don't consider that most device manufacturers build devices without thinking about deployment future. For this, the authors explain an extra item to apply regular security patches and updates to the devices. The problem with this is the time gap between one threat is discovered, reported, and then build the consequent patch or update, this update or patch may be applied late and a malicious attacker could take advantage of that threat. This update process should be addressed continuously by all end users that are using that device and the manufacturer device making a continuous certification process of the devices.

C. Honeypots in the Power Grid

D. Pliatsios et al. [23] develop an interactive honeypot able to emulate real Remote Terminal Unit (RTU) devices that operate using the Modbus protocol. The proposed honeypot receives as input a Modbus only traffic capture file in pcap format, extracts RTU device measurements and stores them internally. Moreover, the honeypot properly configures itself using that traffic. file When an attacker interacts with the honeypot, reply messages requesting measurement values are crafted using the stored values. To demonstrate the effectiveness of their work, the authors utilised data from a real hydro plant and a real RTU device.

Authors in [24] provide an extensive survey work on honeypots and their place in the Industrial Control System (ICS) security domain. Starting with the current state in the ICS domain the authors highlight the impact and side-effects of ICS attacks on society. Afterwards, they explore the current legislation, starting from a national level, and specifically the UK, then moving to other well-known organisations like ISO and IEC and finally mentioning other national organisations like NIST. The importance and placement of honeypots in the aforementioned legislation bodies are also investigated and noted. The two final sections of the surveys work related to existing honeypot solutions and their taxonomy, and finally, a proposed framework called HoneyPlant. The proposed framework consists of two sections, the external network and the organisation network. The first one includes honeypots over the internet that monitor blacklisted domains and IP addresses collecting valuable information while the latter includes honeypots deployed inside an organisation's network with the ultimate goal of timely detection of attacks.

HoneyPLC [25] is a high-level interaction flexible honeypot designed for ICS environments that emulates many Programmable Logic Controller (PLC) devices out-of-the-box. HoneyPLC was designed to be easily extensible, emulating the internal memory of PLC devices easily and offering support for many protocols used by PLC devices. To evaluate HoneyPLC, the authors conducted several experiments using multiple tools for profiling, scanning and interaction with HoneyPLC. The tests were designed to test HoneyPLC's memory and behaviour emulation and ease of extensibility. HoneyPLC was able to trick multiple tools and the wide range of PLC devices already supported prove the above-mentioned statements.

It is evident that the previous works provide useful methodologies and mechanisms. However, the dynamic risk assessment and cybersecurity certification remain critical issues. In [12], the authors provide a dynamic risk assessment process based on Common Vulnerability Scoring System (CVSS). However, CVSS is characterised by some operational limitations [26]. For instance, the current risk assessment methodologies do not consider the disastrous effects of Advanced Persistent Threats (APTs). APTS refer to coordinated cyber-physical attacks targeting a specific goal for a long period.

A characteristic example of an APT campaign against the energy sector was Crashoverride. In particular, Crashoverride resulted in a power outage for more than 220000 people in Ukraine. Consequently, based on the dynamic risk assessment outcomes, the sensitive nature of the power grid requires also the presence of a dynamic certification mechanism that will ensure whether industrial entities/devices can participate or not in the lifecycle of the power grid. Finally, both honeypots and SDN can act as security mechanisms that can mitigate or prevent a potential risk. However, a honeypot is also a security hole that can endanger the production network of an EPES organisation. Based on the aforementioned remarks, in this paper, we present a collaborative framework explaining how risk assessment and cybersecurity certification can be applied in the smart electrical grid. For this purpose, both honeypots and SDN are utilised as a combined security mechanism redirecting the malicious network traffic to cloud honeypots.

D. SDN-based Intrusion Mitigation

In [27] the auuthors highlight the security concerns around IEC 60 870-5-104 protocol, provide a quantitative threat model using ADTs and CVSS v3.1 and an Machine Learning (ML) based IDPS that resides in the control plane utilizes the SDN paradigm to efficiently mitigate malicious actions. In particular, the proposed IDPS captures data plane traffic and extract network flows aimed at detecting malicious actions and mitigating them using the northbound Application Programming Interface (API) of the SDN controller. The mitigation strategy is generated using the Thomson Sampling Reinforcement Learning (RL) method. ML-based detection outperforms other solutions while the RL-based mitigation system is efficient.

P. Manso et al in [28] developed a generic SDN-based IDS solution for efficient detection and mitigation of DDoS attacks, especially Mirai-like ones, without interrupting the QoS of users. The proposed IDS block an attack at the nearest point to the source, thus minimizing any negative effects. A blacklist of IPs is used to block any malicious actions. The authors used the Ryu SDN controller and snort IDS to validate the proposed

system. Results indicate the proposed system is feasible and can successfully mitigate DDoS attacks in a timely manner.

Authors in [29] attempt to translate MUD policies into data plane rules and combine it with SDN technology and also identify current limitations of the derived rules. The suggested system includes an inspection engine that analyses mirrored traffic of IoT devices through an internal signature-based IDS and is responsible for fetching MUD profiles of IoT devices connected to the network and translating them into networking policies. These policies are enforced to the switch through the SDN controller. Evaluation results show that flow rules produce from MUD profiles are able to capture many botnet attempts but they are not able to detect other types of attacks. This could be complemented by properly configuring the internal IDS in the inspection engine though.

T. Xing et al. [30] present a detection and prevention system called SDNIPS designed specifically for cloud environments is a based on snort IDS and OVS virtual switch tools. More specifically, SDNIPS consists of four modules, the cloud cluster hosting all computing resources the OVS responsible for the traffic forwarding and routing, the snort ids and the SDN controller. Comparison tests against a traditional networking approach that uses iptables shows that the SDN-based approach can handle more traffic since it operated in a privileged domain bypassing the user space overhead.

T. Lukaseder et al. in [31] suggest a three-phase SDN-based framework to mitigate slowloris attack. The proposed framework constantly monitors the state of the servers (detection phase). When a server is not reachable the SDN controller instructs the data plane to mirror traffic to IDS instances for further analysis (identification phase). If an attack is recognised the SDN controller pushes instructions to the data plane and block any further communication between the attacker and that server machine. The authors investigate two attacker models, one in which the attacker has a large number of devices under their control and one in which the attacker performs more sophisticated attacks. Two data sets were used to measure the effectiveness of the proposed frameworks. Despite the fact that HTTP attacks were conducted only, the authors state that the proposed framework is feasible.

III. Proposed Architectural Model and Implementation Details

The proposed collaborative framework assumes the presence of a SIEM that can detect, normalise and correlate various security events. A security event is considered as any normalised security-related information identified by the sensors of the SIEM. The SIEM sensors refer to any security-related tool such as an IDPS and firewall that send information to the SIEM. In other words, the SIEM acts as an umbrella of various security tools that send their logs to the SIEM. Next, the SIEM receives the various security logs and undertakes to normalise them in a common format. The normalised secure logs are named *security events*. Each *security event* is characterised by a risk value defined by Equation 1. In particular, *Asset Value* (ranging between 0-5) is defined by the security administrator or the security operator and denotes how significant an asset is. Next, *Event priority* (ranging between 0-5) expresses how severe the impact of the corresponding event is. Finally, *event reliability* (ranging between 0-10) represents the probability of occurrence related to this event.

$$Risk = (Asset\ Value \times Event\ Priority \times Event\ Reliability)/25 \quad (1)$$

Next, the SIEM correlates the various security events with each other, producing security alerts. Consequently, a security alert refers to a set of security events related logically to each other. A security alert is also characterised by a risk value defined by the average of the corresponding security events' risk values. Based on the aforementioned remarks, the proposed collaborative framework receives the security alerts of a SIEM system and based on their risk values, it can calculate in a dynamic manner the risk values of the involved assets (i.e., EPES entities) and certify whether they can participate or not in the production network of an EPES organisation. In particular, as illustrated in Fig. 1, the proposed framework relies on three main modules (a) Risk Assessment Module (RAM), (b) Cybersecurity Certification Module (CCM) and (c) SDN-enabled HaaS. Each module is further analysed below.

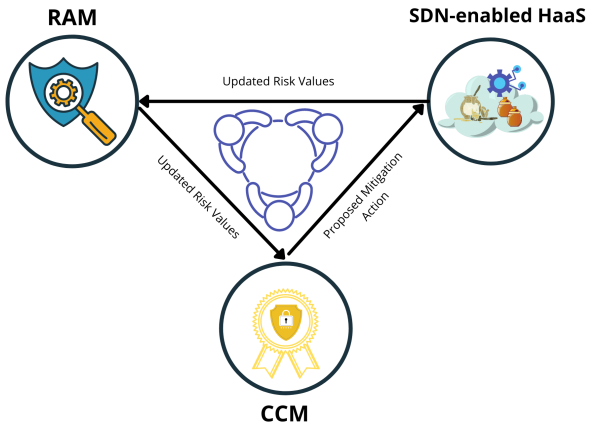

Fig. 1: Architecture of the proposed collaborative framework

A. RAM: Risk Assessment Module

RAM is responsible for the dynamic risk assessment. As mentioned, it receives the various security alerts and re-calculates the risk value of the related assets (i.e., EPES entities/devices) and their relationships (connections with other assets). To this end, first, RAM takes into account all the new energy-related cyberthreats and vulnerabilities published in various repositories, such as vulnerability databases and cybersecurity incidents. A special emphasis is given to MITRE ATT&CK, Common Vulnerability Exposures (CVEs), Common Weakness Enumeration (CWE) and MISP repositories.

Next, seven phases follow: (a) asset identification, (b) threat identification, (c) vulnerability analysis, (d) likelihood calculation, (e) countermeasure analysis, (f) impact analysis and (g) risk calculation. Regarding the threat identification, a Common Attack Pattern Enumeration and Classification (CAPEC)-based threat taxonomy is used, including also APT campaigns from MITRE ATT&CK. The threat identification and vulnerability analysis consider the aforementioned sources, and also special emphasis is given to deep and dark web sources. Next, both Open Web Application Security Project (OWASP) and CVSSS are combined with respect to (d) likelihood calculation, (e) countermeasure analysis, (f) impact analysis and (g) risk calculation.

B. CCM: Cybersecurity Certification Module

Cybersecurity Certification Module (CCM) is responsible to certify whether an EPES asset is eligible to reside in the production network. CCM makes use of the updated risk estimation values of the RAM module for each asset and combines these values with MUD Manager outputs.This module is in charge of continuous evaluation and revisioning of power grid devices security, this will be addressed by MUD and Threat MUD. Finally, CCM concludes if traffic destined to a highly risky device should be redirected to Honeynet-as-a-Service (HaaS) honeynets. This module will be composed of the following subcomponents:

- **MUD Manager**: MUD Manager is composed by two subcomponents and is allocated in the local architecture.
  - MUD Manager: MUD Manager receives the MUD URL from the device where the MUD file is allocated, then the MUD Manager retrieves the MUD file from MUD Server. This file will be translated by the policies translator into MUD policies, then these policies will be enforced to the infrastructure through the management components (e.g. SDN controller, orchestrating tools etc.).
  - Threat MUD Manager: Eventually Threat MUD Manager will receive new vulnerability records by other Cyber Threat Intelligence (CTI) Sharing modules, this makes Threat MUD Manager retrieve the associated Threat MUD file from the manufacturer Threat MUD Server, this file will be translated into policies and enforced to the orchestrator.
- **Local Threat Signaling Server**: This component is composed also by two subcomponents and is allocated in the local architecture.
  - DNS: All power grid components will resolve their domains against this DNS server, this DNS server will respond as a normal DNS but will respond null if the domain requested is a possible compromised domain.
  - Threat Agent: When there is a null DNS response, this component will call the CTI Sharing module to try to find out what kind of vulnerability or threat has compromised the domain.
- **Threat MUD Server**: This component will be in charge to allocate all the Threat MUD files, this component is allocated on the manufacturer's side and will be replicated in every device manufacturer. This component will respond to every request from the Threat MUD Manager and also will receive new updates from the Update Server.
- **MUD Server**: This server will be allocated on the manufacturer's side and will be also replicated in every device manufacturer that the power grid contains. This component will respond to the MUD Manager with the MUD file requested. This component will also receive updated MUD files from the Update Server.
- **Policies Translator**: This component will be in charge to takes the MUD or Threat MUD files and translating them into policies. This component will be allocated in the local architecture

C. SDN-enabled Honeynet-as-a-Service

The SDN-enabled HaaS is an *-as-a-Service model approach to honeypot deployment and management lifecycle that resides in the cloud. EPES sites often lack adequate computing resources to accommodate fully-fledged deployments. To this end a collaborative EPES-to-Cloud approach will be levered. Cloud-based honeynets are deployed and configured properly to accommodate the needs of the EPES site in which the CCM has identified high risk assets. Taking full advantage of the SDN technology the HaaS can properly instruct the SDN networking layer (i.e. the SDN Controller) to redirect traffic from the EPES site to cloud-based honeynets achieving and EPES-to-Cloud continuum. Moreover, if deemed necessary, malicious host isolation actions can be taken to minimize potential threats. The HaaS consists of the following components:

- **Honeypot Manager**: This component is responsible for managing honeynet deployment. Appropriate choice of honeypots and proper configuration of them constitute its main tasks.
- **HaaS Gateway**: This component is deployed in the EPES site and is responsible to properly instruct the SDN controller to redirect traffic to honeypot when the attacker is identified.
- **Low, Medium, High Level Interactions Honeypots**: Multiple honeypots(low, medium and high interaction) will be available as ready-to deploy base images. After proper configuration by the Honeypot Manager, these honeypot instances will be able to emulate real devices and interact with attackers through industrial protocols like Modbus, IEC 61850 or IEC-104.

Finally, despite not being component of the HaaS, the SDN controller is responsible for translating high-level policies and commands issued by other management components (i.e. Honeypot Manager and MUD Policies Translator) to low level data plane commands.

IV. Conclusions

Despite the fact that the smart technologies offer valuable services and benefits with respect to the digitisation of the

conventional electrical grid, critical cybersecurity and privacy risks remain. Based on the various cybersecurity incidents in the energy sector, it is obvious that a dynamic risk assessment and certification mechanisms are necessary. Consequently, in this paper, we present a collaborative risk assessment and cybersecurity certification approach that can update the risk value of each asset and its relationships in a dynamic manner. Moreover, the proposed solution can certify whether each asset can remain in the production network of the EPES organisation or not. To this end, three modules, namely RAM, CCM and SDN-enabled HaaS, are described.

V. ACKNOWLEDGEMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936.

REFERENCES

[1] P. R. Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, A. Sarigiannidis, O. Nikolis, D. Ioannidis, V. Machamint, M. Tzifas, A. Giannakoulias *et al.*, "Secure and private smart grid: The spear architecture," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 450–456.

[2] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[3] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[4] G. Dondossola, F. Garrone, and J. Szanto, "Cyber risk assessment of power control systems — a metrics weighed by attack experiments," in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1–9.

[5] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 61–68. [Online]. Available: https://doi.org/10.1145/2732198.2732203

[6] Y. Li, F. Björck, and H. Xue, "Iot architecture enabling dynamic security policies," in *Proceedings of the 4th International Conference on Information and Network Security*, ser. ICINS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 50–54. [Online]. Available: https://doi.org/10.1145/3026724.3026736

[7] E. Lear, R. Droms, and D. Romascanu, "Manufacturer usage description specification," *IETF RFC8520*, 2019.

[8] D. Dodson, D. Montgomery, W. Polk, M. Ranganathan, M. Souppaya, S. Johnson, A. Kadam, C. Pratt, D. Thakore, M. Walker *et al.*, "Securing small-business and home internet of things (iot) devices: Mitigating network-based attacks using manufacturer usage description (mud)," National Institute of Standards and Technology, Tech. Rep., 2021.

[9] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101589, 2019.

[10] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[11] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[12] P. R. Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz *et al.*, "Sdn-based resilient smart grid: The sdn-microsense architecture," *Digital*, vol. 1, no. 4, pp. 173–187, 2021.

[13] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[14] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[15] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[16] R. W. Y. Habash, V. Groza, D. Krewski, and G. Paoli, "A risk assessment framework for the smart grid," in *2013 IEEE Electrical Power Energy Conference*, 2013, pp. 1–6.

[17] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using attack defense trees," *Sensors*, vol. 20, no. 16, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/16/4404

[18] A. V. Jha, B. Appasani, A. N. Ghazali, and N. Bizon, "A comprehensive risk assessment framework for synchrophasor communication networks in a smart grid cyber physical system with a case study," *Energies*, vol. 14, no. 12, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/12/3428

[19] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for internet of things-based energy internet," *Future Generation Computer Systems*, vol. 93, pp. 849–859, 2019.

[20] T. Shekari, C. Bayens, M. Cohen, L. Graber, and R. Beyah, "Rfdids: Radio frequency-based distributed intrusion detection system for the power grid." in *NDSS*, 2019.

[21] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87 592–87 608, 2020.

[22] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, 2019.

[23] D. Pliatsios, P. Sarigiannidis, T. Liatifis, K. Rompolos, and I. Siniosoglou, "A novel and interactive industrial control system honeypot for critical smart grid infrastructure," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[24] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ics in honey: How do honeypots fit within industrial control system security," *Computers & Security*, vol. 114, p. 102598, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821004211

[25] E. López-Morales, C. Rubio-Medrano, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G.-J. Ahn, "Honeyplc: A next-generation honeypot for industrial control systems," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 279–291.

[26] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke, "Can the common vulnerability scoring system be trusted? a bayesian analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1002–1015, 2016.

[27] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.

[28] P. Manso, J. Moura, and C. Serrão, "Sdn-based intrusion detection system for early detection and mitigation of ddos attacks," *Information*, vol. 10, no. 3, 2019. [Online]. Available: https://www.mdpi.com/2078-2489/10/3/106

[29] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "Combining mud policies with sdn for iot intrusion detection," in *Proceedings of the 2018 Workshop on IoT Security and Privacy*, ser. IoT S & P '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–7. [Online]. Available: https://doi.org/10.1145/3229565.3229571

[30] T. Xing, Z. Xiong, D. Huang, and D. Medhi, "Sdnips: Enabling software-defined networking based intrusion prevention system in clouds," in *10th International Conference on Network and Service Management (CNSM) and Workshop*, 2014, pp. 308–311.

[31] T. Lukaseder, L. Maile, B. Erb, and F. Kargl, "Sdn-assisted network-based mitigation of slow ddos attacks," in *Security and Privacy in Communication Networks*, R. Beyah, B. Chang, Y. Li, and S. Zhu, Eds. Cham: Springer International Publishing, 2018, pp. 102–121.