Call for Papers

Important dates

Workshop papers' deadline:
~~April 22~~ May 20, 2022
Workshop authors' notification:
~~May 13~~ June 10, 2022
Camera-ready submission:
~~May 27~~ June 24, 2022
Early registration deadline:
June 24, 2022
Workshop's date:
July 27–29, 2022

Workshop chairs

Panagiotis Sarigiannidis

Organizing committee

George Karagiannidis
Dimosthenis Ioannidis
Thomas Lagkas
Valeri Mladenov
Erkuden Rios
Igor Kotsiuba

Publicity chairs

Panagiotis Radoglou-Grammatikis

Contact us

psarigiannidis@uowm.gr

The smart technologies digitize the conventional model of the Electrical Power and Energy Systems (EPES) into a new architectural paradigm, known as the Smart Grid (SG), thus introducing multiple services, such as two-way communication, pervasive control and self-healing. However, despite the benefits, this progression leads to challenging cybersecurity issues due to the vulnerabilities of the new technologies and the necessary presence of legacy and insecure systems, like Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS).

On the other side, anticipating the critical issues of EPES/SG, both academia and industry have developed appropriate countermeasures, considering the advances in the Artificial Intelligence (AI) and the networking domains. AI and especially Machine Learning (ML) and Deep Learning (DL) allow the implementation of detection mechanisms capable of discriminating malicious behaviors as well as zero-day vulnerabilities. Emerging solutions in this sector include Security Information and Event Management (SIEM) systems and Intrusion Detection and Prevention Systems (IDPS). Other emblematic technologies that can mitigate or even prevent cyberattacks are honeypots, Software-Defined Networking (SDN), Network Function Virtualization (NFV) and intentional islanding.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Intrusion/anomaly detection and mitigation in EPES/SG
- SDN/NFV-based architectures for resilient EPES/SG
- EPES/SG honeypots and honeynets
- SIEM systems in EPES/SG
- Self-healing in EPES/SG
- Federated learning solutions for anomaly and cyberattack detection in EPES/SG
- Security management and risk assessment in EPES/SG
- Threat modelling and vulnerability analysis in EPES
- Security management and risk assessment in EPES/SG
- Emerging privacy-preserving mechanisms and techniques in EPES/SG

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. The workshop's proceedings will be published by IEEE and will be included in IEEE Xplore. Detailed information about the paper submission and guidelines to authors can be found at the workshop's website https://www.ieee-csr.org/epes-spr.

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION