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

Christos Tryfonopoulos
Spiros Skiadopoulos
Angelos Marnerides

Publicity chairs

Paraskevi Raftopoulou

Contact us

trifon@uop.gr
spiros@uop.gr
angelos.marnerides@glasgow.ac.uk

Over the years cyber-threats have increased in numbers and sophistication; adversaries now use a vast set of tools and tactics to attack their victims with their motivations ranging from intelligence collection to destruction or financial gain. Lately, the introduction of IoT devices on a number of applications, ranging from home automation to monitoring of critical infrastructures, has created an even more complicated cyber-defense landscape. The sheer number of IoT devices deployed globally, most of which are readily accessible and easily hacked, allows threat actors to use them as the cyber-weapon delivery system of choice in many today's cyber-attacks, ranging from botnet-building for DDoS attacks, to malware spreading and spamming.

Staying on top of these evolving cyber-threats has become an increasingly difficult task that nowadays entails the collection, analysis, and leveraging of huge volumes of data and requires methodologies and techniques located at the intersection of statistics, data mining, machine learning, visualization and big data. Although the application of Data Science methodology to the Cyber Security domain is a relative new topic, it steadily gathers the interest of the research community as showcased by the utilization of data science techniques in a variety of cyber-defense facets that include proactive technologies (e.g., cyber-threat intelligence gathering and sharing), platform profiling (e.g., trust calculation and blacklisting), attack detection/mitigation (e.g., active network monitoring, situational awareness, and adaptable mitigation strategies), and others. This workshop aims to spotlight cutting-edge research in data science driven cyber-security in academia, business and government, as well as help in the alignment of these endeavors.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Big data-driven cyber-security (incl. analytics, management)
- Machine and deep learning methods for cyber-security (incl. malware/phishing/botnet/spam/intrusion/anomaly detection)
- Visualization methods (incl. visual situation awareness, VR & AR visualization, real-time visualization)
- AI-driven cybersecurity
- Private information retrieval
- Cyber-threat intelligence collection, identification and sharing at scale
- Private/sensitive information protection
- Machine-learning powered traffic analysis and attack modelling
- Machine learning-based platform profiling and trust management
- Advanced attack detection and mitigation

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/ds4cs.

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