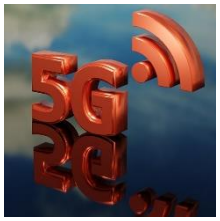
ECCWS 2024

23rd European Conference on Cyber Warfare and Security
27-28 June 2024, University of Jyväskylä, Finland

Mini Track on Evolved Cyber-Physical Systems Cybersecurity and Cyber-Ranges
Chairs: Dr Paulo Simões and Dr Tiago Cruz, University of Coimbra, Portugal



Deployments of evolved wireless WAN (WWAN) technologies, ranging from private/virtual 5G or hyperlocal cellular networks to LoRaWAN, are spreading worldwide at a fast pace, introducing new models for network architectures. Together with the adoption of edge computing and cloud-to-edge continuum models, such trends are fostering new ecosystems for the deployment of novel services and applications. This will enable connection of millions of devices in consumer or industrial IoT applications, constituting a milestone towards the emergence of new Cyber-Physical Systems (CPS) paradigms.

Due to the importance of the involved application domains, these developments will naturally increase the interest of malicious actors, providing fertile ground for many kinds of threats, such as malware, API/service-targeting attacks, data stealing, or ransomware, among others. This situation requires the introduction of suitable intrusion detection, prevention and mitigation mechanisms but also to increase awareness through training and testing. This cannot be undertaken in production environments, calling for the development of realistic cyber-ranges to provide safe grounds for R&D activities.

This mini-track, realized under the auspices of the P2020 POWER and NEXUS Projects, addresses these challenges, encompassing all the relevant aspects that are involved in such domains. Suggested topics include but are not limited to:

- Mechanisms for data collection to leverage edge computing models.
- Contributions towards the development of secure computing continuum solutions.
- Algorithms and techniques for security anomaly detection and protection.
- Security of Machine-to-Machine (M2M) communications and network infrastructure security.
- Security (auditing, protection, reaction).
- Risk and interdependency modelling.
- Threat lifecycle and profiling analysis.
- Development of cyber-range and testbed environments for security R&D and training.

Dr Paulo Simões received his Ph.D. degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2002. He is an Associate Professor in the Department of Informatics Engineering, University of Coimbra. His research interests include network and infrastructure management, security, critical infrastructure protection.

Dr Tiago Cruz received his Ph.D. degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2012. He is an Assistant Professor in the Department of Informatics Engineering, University of Coimbra. His research interests include areas such as management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, Internet of Things.

Submission Details
In the first instance, a 300–350-word abstract is required, submissions must be made using the online submission form at https://www.academic-conferences.org/conferences/eccws/eccws-abstract-submission/
If you have any questions about this track, please email: psimoes@dei.uc.pt , tjcruz@dei.uc.pt

See more about ECCWS 2024 at http://www.academic-conferences.org/conferences/eccws