Workshop Title: Key challenges in global cybersecurity: Efforts and trends in EU **(KCYEU-2022)**

The Workshop will be held on 28 March, 2022, as a remote event, co-located with the DRCN2022 Conference.

Workshop Organizers

Dora Kallipolitou, Zelus P.C.

Anna Marton, Safepay Systems

Eva Marín Tordera, Universitat Politécnica de Catalunya

Nelly Leligou, SYNELIXIS

Organization

TPC Members

Cataldo Basile (POLITO)
Henrique Santos (UMinho)
Nelly Leligou (Synelixis Solutions S.A.)
Admela Jukan (TUBS)
Diego López (Telefónica I+D)
Grigorios Kalogiannis (STS)
Sergio Sánchez López (UPC)
Danijela Tešendić (University of Novi Sad)
Srdjan Škrbić (University of Novi Sad)
Danijela Boberić Krstićev, (University of Novi Sad)
Dr. Konstantinos Georgopoulos, (Research Associate, Telecommunication Systems Institute)
Dr. Grigorios Chrysos, (Research Associate, Telecommunication Systems Institute)
Prof Christos Douligeris (University of Piraeus)
Prof. Erol Gelenbe (IITIS-PAN - Institute of Theoretical and Applied Informatics of the Polish Academy of Sciences)
Prof. Tadeusz Czachórski (IITiS PAN - Institute of Theoretical and Applied Informatics of Polish Academy of Sciences)
Dr. Mohammad Heydari (Stockholm University)

Call for Papers and Work-in-Progress Presentations

According to the World Economic Forum[1], Cybersecurity is one of the biggest concerns worldwide, being also one of the top five identified risks. The European Union is not indifferent to this concern and need, and different projects have been funded from the European Union's Horizon 2020 research and innovation programme. Among these projects FISHY (https://fishy-project.eu/), CYRENE (https://www.cyrene.eu/) and IoTAC (https://iotac.eu/), are organizing a joint workshop trying to track current research in cybersecurity, especially in the fields of IoT and supplychain but also open to other cybersecurity research areas and projects. The topics identified for this workshop are, although not limited to:

Cybersecurity certification schemes
How to assess Risk in a Supply Chain Service?
Identity and access management in IoT environments
AI based attack detection
AI attacks modeling
Certification of IoT architectures
Vulnerability prediction and secure software development
Supply chain vulnerability and impact assessment
Control access and authentication on supply of chains
Cybersecurity prediction maintenance
Trust and incident management on supply of chains

Authors are invited to submit original contributions that have not been published or submitted for publication elsewhere.

Two types of submissions are solicited:

1. **Original unpublished papers**. They should be in pdf. IEEE 2-cloumn conference style, limited to six (6) pages. The DRCN 2022 conference is technically Co-Sponsored by the IEEE Communications Society. All accepted and presented papers will be included in the DRCN 2022 proceedings and will be subsequently submitted to IEEE Xplore for publication. At least one author is required to register, at the full rate (for online workshop), to present accepted papers at the conference and for the paper to appear in the conference proceedings and in IEEE Xplore.
2. **Work-in-Progress presentations.** One page (1) summary in Calibri 11pt style, plus no more than 10 ppt slides, sent in pdf format. The paper will not appear in IEEE Xplore and the registration for work-in-progress presentations will be different.

Important dates:

Deadline for workshop paper submission: **February 10, 2022**

Acceptance/rejection notification: **February 18, 2022**

Final workshop papers due: **February 25, 2022**

Submit your paper through:

1. **Original unpublished papers through EDAS: https://www.edas.info/newPaper.php?c=28793&track=110494**

2. **Work-in-progress presentation to the email: submitworkshop@iotac.eu**

[1] https://www.weforum.org/