5rd Workshop on Internet of Things Security and Privacy (WISP) (in conjunction with Global IoT Summit 2023)

Organizing Committee

Program Chair:

- **Antonio Skarmeta** (University of Murcia, Spain) - skarmeta@um.es
- **Konstantinos Loupos** (Inlecom, Greece)
- **Christos Xenakis** (University of Piraeus, Greece)
-

Important Dates

Paper submission deadline: **April 1st, 2023**
Acceptance Notification: May 10, 2023
Camera-Ready Paper Submission: May 30, 2023

Paper Submission Guidelines

Final submissions must not substantially overlap papers already or simultaneously submitted to a journal or a conference with proceedings. Their contents should be written in English with a maximum paper length of six (6) printed pages see web conference for instructions. Papers must be submitted through EDAS.

Technical Program Committee

- **Gianmarco Baldini** (European Commission, Joint Research Centre, Italy)
- **Jose Luis Hernández-Ramos** (European Commission, Joint Research Centre, Italy)
- **Jorge Bernal** (University of Murcia, Spain)
- **Konstantinos Loupos** (Inlecom, Greece)
- **Hui Song (**SINTEF, Norway**)**
- **Nicolas Ferry (**SINTEF, Norway**)**
- **Paul-Emmanuel Brun** (AIRBUS, France)
- **Konstantinos Votis** (ITI, Greece)
- **George Baroutas** (Inlecom, Greece)
- **Bruno Crispo** (University of Trento, Italy)

Call for Papers

The enforcement of security and privacy notions are widely considered as the main barriers for the design and development of IoT-enabled scenarios. With the massive deployment of wireless communication technologies and the integration of IA techniques, IoT devices are becoming more autonomous and pervasive in our surrounding environment. On top, the already increasing number and heterogeneity of IoT devices is further increasing needs on a harmonized security and privacy layer. This aspect will be reinforced with the integration of 5G technologies to realize a data-driven society. In this context, current digital and physical infrastructures will be the target of potential attackers, in order to get access to the information provided by such devices. This trend toward hyperconnectivity also means an increase of security and privacy risks, since IoT systems will often operate on behalf of their owners by disclosing potentially sensitive data.. These concerns must be tackled by joint efforts involving manufacturers, regulatory bodies, policy makers and end users to increase trust in the future digital society. For that reason, there is a need to develop joint strategies addressing the identification and mitigation of security and privacy risks to promote the deployment of IoT systems on a broad scale.

This workshop is aimed to bring together experts from different EU projects working in cross-layer issues in the areas of user-centric security, privacy and trust in the IoT. The goal is to present the recent results to the research community, the industry and standardisation bodies and exchange ideas for joint research activities in the future. Finally, the threats of the IoT for the citizens will be identified analysed, discussing also how the results of the projects can help mitigating these threats.

The technical topics of interest include, but are not limited to:

- Security and privacy challenges of interoperable and usable IoT
- Lightweight IoT security protocols and architectures
- Privacy enhancing and anonymization techniques in IoT
- Trust and identity management in IoT
- Privacy data protection in Smart Cities applications
- Secure discovery and authentication in IoT
- IoT security lifecycle and Data Governance models
- Security and privacy framework for IoT platforms
- Case studies of new or existing IoT security technologies
- Novel architectures, protocols, and applications for security and interoperability
- Testbeds, and experimental results in IoT domains
- Blockchain-based identity management and access control systems
- Smart contracts for enhancing trust and security in IoT
- Security and privacy aspects on the integration of LPWAN in IoT systems
- Incentive mechanisms for enhancing security and privacy
- Cognitive Systems for IoT platforms
- Formal models to represent IoT systems, attacks and vulnerabilities
- Automated IoT security testing
- Security certification and standardization activities

This workshop is supported by EU projects:

- ERATOSTHENES; CERTIFY; ENTRUST, CROSSCON