Workshop on Internet of Things Security and Privacy (WISP)
(in conjunction with Global IoT Summit 2019)

Organizing Committee

Program Chair:

- **Antonio Skarmeta**(University of Murcia, Spain)

General Co-Chairs:

- **Jose Luis Hernández** (JRC, Italy)
- **Juan Antonio Martínez** (OdinS, Spain)
-

Technical Program Committee

- **Gianmarco Baldini** (JRC, Italy)
- **Jose Luis Hernández** (JRC, Italy)
- **Jorge Bernal** (University of Murcia, Spain)
- **Prof. George Polyzos** (AUEB-RC, Greece)
- **Prof. Vasilios Siris** (AUEB-RC, Greece)
- **Martin Strohbach** (AGT International. Germany)
- **Dmitrij Lagutin** (Aalto, Finland)
- **Konstantinos Loupos** (Inlecom, Greece)
- **Hui Song (**SINTEF, Norway**)**
- **Nicolas Ferry (**SINTEF, Norway**)**
- **Enrico Ferrera** (Istituto Superiore Mario Boella - ISMB, Italy)
- **Giuseppe Pacelli** (Istituto Superiore Mario Boella - ISMB, Italy)
- **Saddek Bensalem (**Université Grenoble Alpes, France)
- **Ralf Tönjes** (University of Applied Science Osnabrück, Germany)
- **Nikolaos Petroulakis** (Forth, Greece)
- **Andrea Detti** (University of Rome "Tor Vergata", Italy)

More to be added…

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.

"IEEE reserves the right to exclude a paper from distribution after the conference, including IEEE Xplore® Digital Library, if the paper is not presented by the author at the conference."

Important Dates

Paper submission deadline: **February 22, 2019**
Acceptance Notification: March 31, 2018
Camera-Ready Paper Submission: April 30, 2019

Call for Papers

IoT technologies are not designed and applied in a secure and safe way, they can be vulnerable to many types of attacks, which can cause serious problems in the physical world. Since IoT devices are not only monitoring (e.g., through sensors) but also controlling physical objects (e.g., through actuators), the impact of security attacks can be devastating, including serious safety impacts as in the case of connected vehicles and smart healthcare. Thus, the IoT brings new challenges regarding security, privacy and mainly "trust" in order to protect the safety of the citizens in smart city environments. Since IoT devices are monitoring the physical world, they can be monitoring citizens and their behaviour too. Having a large numbers of devices installed in, e.g., homes, offices, busses, and on the streets, that monitor everyday activities of citizens raises issues regarding the privacy of the citizens and the access to sensitive information.

This workshop to bring together experts from different EU projects and the Internet of Things Research Cluster (IERC) that are 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
- Identity Management and IoT
- Privacy data protection in Smart Cities applications
- Secure discovery and authentication in IoT
- IoT Security Life cycle
- Data Governance on IoT
- Security and Privacy Framework for IoT Platforms
- Access control for shared data and IoT devices
- Case studies of new or existing IoT security technology
- Novel architectures, protocols, or applications that achieve both security and interoperability (usability)
- Testbeds, and experimental results in IoT domains
- Blockchain based identity management and access control systems
- Smart contracts for enhancing trust and security in IoT
- Distributed trust models

		• Incentive mechanisms for enhancing security and privacy • Cognitive Systems for IoT Platforms • IoT Safety, Security and Privacy • Blockchain and PKI • DevOps for secure IoT • Resilience of IoT Systems • Secure and privacy-savvy exchange of personal information • Privacy and Data Integrity This workshop is supported by EU projects IOTCrawler, Fed4IoT, ENACT, SOFIE, CHARIOT