



IFIP IoT 2022 Special Session Cybersecurity in IoT

Scope

Current critical and complex ICT ecosystems address multidimensional and heterogeneous components and systems, including multi-actors and different technologies, communicating and generating an exchange of data. This emerging complexity, which includes IoT environments, has been evolving fast, empowering the emergence of system vulnerability to malicious attacks. In the new landscape of fast deployment of new technologies, cybersecurity has become a major concern requiring continuous monitoring, testing, assessment, and improvement of digital ecosystems to assure their integrity, security and privacy. Current research is focusing on the development of measures for improving resilience, trust, and security and privacy within ICT supply chains, including IoT security and privacy standards and certification as one of the major challenges. In this regard, this special session aims addressing the current research in cybersecurity in IoT, enabling the discussion and knowledge generation fostering security and trust within ICT ecosystems across their entire lifecycle. For such, a set of topics for this special session can be found below, but not limited to such list.

Session Organizers

- José Barata, Uninova-CTS/Nova School of Science & Technology, Portugal, jab@uninova.pt
- Ricardo Peres, Uninova-CTS/Nova School of Science & Technology, Portugal, ricardo.peres@uninova.pt
- Ovidiu Cosma, Technical University of Cluj-Napoca, Romania, ovidiu.cosma@cunbm.utcluj.ro
- Eda Marchetti, National Research Council, Italy, eda.marchetti@isti.cnr.it
- Emilia Cioroaiuca, Fraunhofer-IESE, Germany, Emilia.Cioroaiuca@iese.fraunhofer.de
- Ana Inês Oliveira, Uninova-CTS/Nova School of Science & Technology, Portugal, aio@uninova.pt
- Filipa Ferrada, Uninova-CTS/Nova School of Science & Technology, Portugal, faf@uninova.pt

Topics/ Keywords

- Trust in ICT supply chains
- Vulnerability assessment and testing
- Achieving resilience (in ecosystems formed by unreliable components)
- Extending auditing (evaluation of interconnected ICT systems)
- Advanced risk analysis
- Security, safety, and privacy assurance
- Safety and security Co-engineering
- Industrial validation
- Ontologies for cybersecurity
- Cybersecurity prediction and maintenance
- Security-by-design
- IoT Security standards and certification
- Internet of Behaviour (IoB)
- Functional and non-functional monitoring

Submission procedure

Special sessions are included in the main Conference and follow the same reviewing process.

Short abstracts submission (100-150 words): NOW

Full papers submission: May 6th, 2022

Acceptance Notice: Jun 17th, 2022

Final version Submission: Jul 1st, 2022

Acceptance of papers is based on the **full paper** (up to **18** pages). Each paper will be evaluated by three members of the International Program Committee.

When submitting on the web site, you have to indicate the name of the special session.

Submission procedure via EasyChair available on: <http://ifip-iotconference.org>, with copy by email to the chairs of the special session.

Special Session Sponsored by



www.bieco.org