1ST WORKSHOP ON DEPENDABILITY AND SAFETY EMERGING CLOUD & FOG SYSTEMS (DeSECSys)

September 17, 2020 — Virtual Workshop

IMPORTANT DATES

Submission Deadline:
July 5th, 2020

Notification to Authors:
August 2nd, 2020

Camera-ready Versions:
August 9th, 2020

SUBMISSION

We invite the following types of papers:

Regular papers: (18 pages, including the bibliography but excluding well-marked appendices; Template

Short research papers: (submissions of up to 8 pages, using the same template)

Submission platform: **EasyChair**

PROGRAM COMMITTEE

GENERAL CHAIRS:

Liqun Chen
(University of Surrey, UK)

Christos Xenakis
(University of Piraeus, GR)

PROGRAM CO-CHAIRS:

Thanassis Giannetsos
(Technical University of Denmark, DK)

Christoforos Ntantogian
(Ionian University, GR)

Panagiotis Gouvas
(UBITECH Limited, GR)

All projects have received funding from the European Union's Horizon 2020 research and innovation programme

CALL FOR PAPERS

desecsys.futuretpm.eu

The goal of the DeSECSys workshop is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various applications, opportunities and possible shortcomings of these technologies and their integration. Effectively we aim to produce a collection of state-of-the-art research about emerging security technologies, their applications, their shortcomings and their verification with a focus on their uncompromised, in terms of security, safety and dependability, integration. Industry experience reports and empirical studies are also welcome.

TOPICS OF INTEREST

(not limited to)

- Emerging security and privacy technologies and solutions
- Next-generation trustworthy computing security solutions and attacks (e.g., TPMs, TEEs, SGX, SE), and their impact
- Utilization of novel artificial intelligence and machine learning based technologies in the context of security
- Blockchain / Smart contracts for auditability & accountability
- Fog Computing
- Runtime risk assessment
- Vulnerability Analysis
- Formal Verification/Validation of design
- wAdvanced cryptographic techniques (e.g., homomorphic encryption, secure multi-party computation and differential privacy)
- Impact of quantum computing on cyber-security (not limited to cryptography)
- Novel attacks & protection solutions in mobile, IoT and Cloud
- Standardization of cyber security and trust techniques
- Novel schemes for Trust and Reputation in Distributed Environments
- Policy languages for advanced Access and Usage Control
- Consensus mechanisms
- Security in 5G networks

SPONSORS:

ASTRID CUREX SECURE AND PRIVATE HEALTH DATA EXCHANGE FutureTPM INCOGNITO SECONDO