CALL FOR ABSTRACTS

IFIP WG 11.4 Workshop – iNetSec 2020

Open Problems in Network Security
September 22-23, 2020, Maribor, Slovenia
co-located with IFIP SEC 2020

GENERAL INFORMATION. In the past decade, mobile networks have fundamentally influenced the ways in which information is exchanged and handled. Pervasive electronic devices make our everyday life easier, e.g., by helping us to connect with other people while being mobile, to use services available online, or to pay and use tolls and tickets. Many of the components employed routinely manage and distribute large amounts of data for different purposes. As these processes involve sensitive information, protecting information and the network with suitable security measures is more important than ever.

The objective of this one-day workshop (noon to noon) is to bring together researchers in the field of network security to discuss the open problems and future research directions. We think that workshop discussions can contribute additional insights to the research community and should be an integral part of the paper publication process. Therefore, we encourage authors to submit abstracts of open problems that can be presented and discussed at the workshop. Authors of accepted abstracts will receive the opportunity to integrate suggestions induced by the discussions in their full papers after the workshop.

INSTRUCTIONS FOR AUTHORS. To this end, we solicit papers describing interesting unsolved problems and issues in (a certain area of) network security. Example areas include:

- Reliable Secure Network Systems
- 5G Security and Privacy
- Wireless mesh networks and protocols
- Sensor nets & embedded systems
- Identity & trust management
- Cryptographic primitives & services
- Security definitions and proofs
- Anonymous networks
- Cross layer security
- Usage control
- Trusted platforms
- Forensics
- Security policies
- Dynamic composition of services

We ask authors to submit 1-2 page extended abstracts. They must be submitted electronically by **June 01, 2020 (AoE)**, using *https://cmt3.research.microsoft.com/iNetSec2020*. Late submissions and non-electronic submissions will not be considered. Notification of acceptance or rejection will be sent to authors by July 06, 2020. Authors of accepted abstracts must guarantee that they will submit a **full paper by September 01, 2020**, and that their paper will be presented at the workshop. Papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference. More information is available at *https://itsec.ur.de/inetsec2020/*.

CONFERENCE PROCEEDINGS. Copies of the papers will be available at the workshop. Authors will be able to revise their papers after the workshop. Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. These final papers will be published as post-proceedings by Springer in the series of IFIP Advances in Information and Communication Technology (IFIP AICT).

Submission (extended abstract):	June 01, 2020 (AoE)
Acceptance:	July 06, 2020
Conference Version (full paper):	September 01, 2020
Post Proceeding (full paper):	To be announced

PROGRAM CHAIR.
Doğan Kesdoğan (University of Regensburg)
Contacting the chair: inetsec2020@mailman.uni-regensburg.de

VENUE. The iNetSec 2020 workshop will be co-located with IFIP SEC 2020 in Maribor, Slovenia. Travel information will be available at *https://sec2020.um.si/*.