7th IEEE/IFIP International Workshop on Security for
Emerging Distributed Network Technologies (DISSECT)
May 17 or 21, 2021 // Bordeaux, France

Intelligent Management of Open and Highly Programmable Networks: Security and Computation

IEEE/IFIP DISSECT 2021 – CALL FOR PAPERS

The computer networking landscape is subject to a multitude of changes that occur very rapidly. First, paradigm shifts such as Internet of Things (IoT), cloud and fog computing, and emerging networking technologies such as Programmable Networks and 5G/6G are reshaping the way networks are designed, deployed, and managed. The benefits are manifold, including an unprecedented flexibility for network operation and management, and a favorable environment for delivering innovative network applications and services. However, those paradigm shifts bring a multitude of security challenges that have to be addressed to provide secure, intelligent, trustworthy, and privacy-preserving data communication and network services. Second, large scale and distributed deployment of IoT, Self-Driving Networks, etc. has become real but also emphasizes particular privacy and security issues to be overcome, especially when interconnected with the Internet.

Addressing all these challenges may require not only revisiting existing solutions (e.g., for intrusion detection, privacy preserving, and resilience against attacks), but also designing novel security and resilience schemes tailored to the specific design of open networking technologies and infrastructures. New types of attacks and threats also appear against usual services over the Internet such as DNS or routing. DISSECT 2021 follows the track of its six previous editions, and will put focus on security issues and challenges arising with the emergence of novel networking technologies and paradigms but also on new threats emerging against former services and technologies, towards a secure cognitive management in a cyber-world. The workshop will shed light on new challenges and present state-of-the-art research on the various security aspects of next-generation networking technologies and service management frameworks.

The 7th edition of DISSECT will focus on Intelligent Management of Open and Highly Programmable Networks: Security and Computation. It will offer a venue for bringing together students, researchers, and professionals sharing common interest on security challenges related to the design and management of distributed networks and infrastructures. DISSECT is intended to (1) discussing these challenges as well as future trends on security management, (2) presenting and discussing work-in-progress security-related research, and (3) strengthening collaboration and research ties among peers.

TOPICS OF INTEREST

We invite our community to contribute with manuscripts describing novel, work-in-progress research on the design of solutions to relevant security issues on a wide variety of next generation networking technologies. The topics of interest include:

Blockchain and distributed consensus

Security of Next-generation Networks

AI for Network Security

Federated and Deep learning for Privacy protection of emerging Networks

Secure and resilient solutions for open networking technologies

Privacy-preserving solutions

Vulnerability analysis

Digital forensic

Security models and threats

Security and privacy properties and policies

Verification and enforcement of security properties

Trust and identity management

NFV-based security functions and services

Security of software-defined infrastructures, protocols and interfaces

Threat modeling

Security and availability management

Privacy and security for Internet of Things
Intrusion detection, resilience, and prevention
Honeypots

Network forensics and auditing

Detection and resilience against large-scale distributed attacks

Security of programmable components

Security-related business and legal aspects

Security challenges and trends for open networking technologies

Secure programmable data plane

Collaborative intrusion detection

Security measurement and monitoring

Industrial Control System security

Threat Intelligence

Large-scale security experimentation

Reproducible research in security

Lightweight computing resources

Lightweight security protocols in distributed networks

AUTHOR INSTRUCTIONS

Paper submissions must present original, unpublished research or experiences. Papers under review elsewhere must not be submitted to the workshop. All contributions must be submitted in PDF format via JEMS submission system.

All papers must be limited to 6 pages in an IEEE 2-column style and will be subject to a peer-review process. The accepted papers will be submitted for publication in the IEEE Xplore Digital Library. Papers will be withdrawn from IEEE Xplore in case the authors do not present their paper at the workshop.

Authors of distinguished papers will be invited to submit an extended version of their manuscripts to the International Journal on Network Management (IJNM).

IMPORTANT DATES

Paper Submission: *Jan 22, 2021*

Acceptance: *Feb 18, 2021*

Camera-ready: *Mar 15, 2021*

ORGANIZING COMMITTEE

Moayad Aloqaily
xAnalytics Inc., Canada

Weverton Cordeiro
UFRGS, Brazil

PC CHAIR

Ouns Bouachir
Zayed University, Dubai, UAE

STEERING COMMITTEE

Jérôme François
Inria Nancy Grand Est, France

Carol Fung
VCU, USA

Mohamed Faten Zhani
ETS, Canada

For more information, please visit
http://www.inf.ufrgs.br/dissect/2021