5th IEEE/IFIP International Workshop on Security for
Emerging Distributed Network Technologies (DISSECT)
8 April 2019 // Washington DC, USA

Security for the Next Wave of Cyber and Social Networks

IEEE/IFIP DISSECT 2019 – CALL FOR PAPERS

The computer networking landscape is subject to a multitude of changes that occur very rapidly. First, paradigm shifts such as fog computing, mobile edge computing, Named Data Networking (NDN) and emerging open networking technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Programmable Networks 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 in order to provide secure, trustworthy, and privacy-preserving data communication and network services. Second, large scale and distributed deployment of mobile communications, Internet-of-Things (IoT), Intelligent Transport Systems, smart grids or industrial systems has become real but also emphasizes particular privacy and security issues to be overcome, especially when interconnected with 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 Internet such as DNS or routing. DISSECT 2019 follows the track of its four 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.

DISSECT will offer a venue for bringing together students, researchers, and professionals from academia and industry sharing common interest on security challenges related to the design and management of the 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 on cutting-edge technologies, and (3) strengthening collaboration and research ties among peers.

TOPICS OF INTEREST

The industry and academia research community will be invited 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 of the workshop include, but are not limited to

Secure and resilient design and deployment of open networking technologies
Privacy-preserving solutions
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 measurement and monitoring
Industrial Control System security

Security and availability management
Security for Internet of Things
Intrusion detection, tolerance, 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
Blockchain and distributed consensus

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 https://submissoes.sbc.org.br/im2019_dissect.

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 the best papers in DISSECT2019 will be invited to submit an extended version of their papers to a Special Issue of the International Journal on Network Management (IJNM) on Advanced Security Management.

IMPORTANT DATES

Paper Submission Deadline
Dec 15, 2018

Notification of Acceptance
Jan 5, 2019

Camera-ready papers
Jan 25, 2019

ORGANIZING COMMITTEE

Mohamed Faten Zhani
École de Technologie Supérieure, Canada

Jérôme François
Inria Nancy Grand Est, France

Emmanouil Vasilomanolakis
TU Darmstadt, Germany

Hsu-Chun Hsiao
National Taiwan University, Taiwan

For more information, please visit
http://www.inf.ufrgs.br/dissect/2019