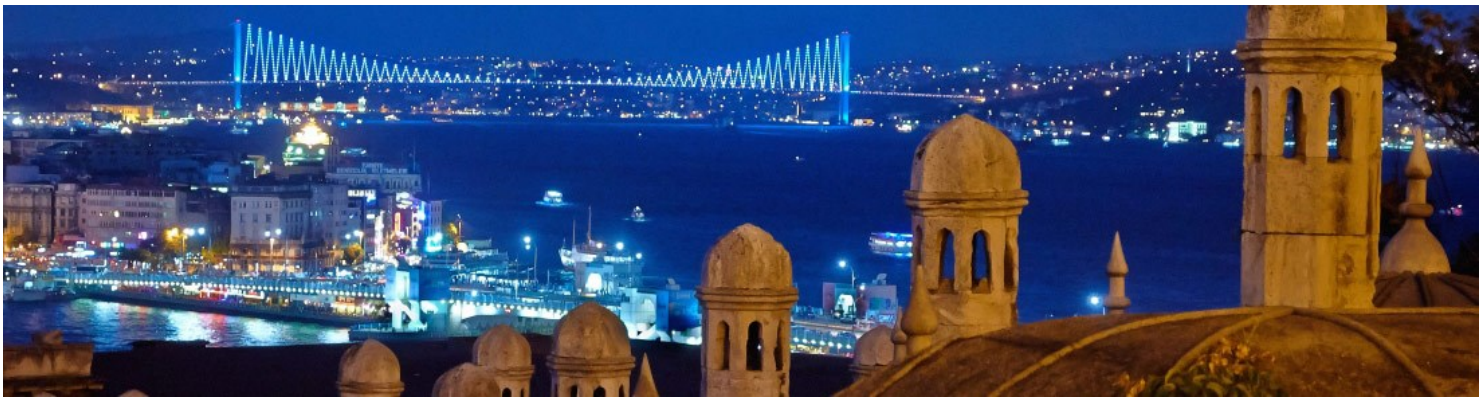
2nd IEEE/IFIP International Workshop on Security for Emerging Distributed Network Technologies (DISSECT)
Istanbul // Turkey // 25 or 29 APRIL 2016

Managing Security of Emerging Networking Paradigms for a Smart and Hyper connected World



IEEE/IFIP DISSECT 2016 – CALL FOR PAPERS

The emergence of networking technologies and paradigms, such as software defined networking and network function virtualization, has completely transformed the way networks are designed, deployed, and managed, and has brought a multitude of challenges to the spotlight of worldwide research. In this context, security has been one of the areas of major concern and thus research interest, especially with the growing demands of the general public for secure, trustworthy, and privacy-preserving data communication and management.

In its second edition, the main goal of DISSECT will be to put focus on security issues and challenges arising with the emergence of novel networking technologies and paradigms. 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) present and discuss work-in-progress security-related research on cutting-edge technologies, and (3) strengthening collaboration and research ties among peers.

TOPICS OF INTEREST

In this workshop, the research community from industry and academia 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 networking architecture design
- Intrusion detection and mitigation for emerging networks
- Trust and privacy in social networks
- Security and trust management in cloud environments
- Security challenges in the Internet of Things
- Secure design of SDN and NFV solutions
- Networked, distributed systems security
- Security and privacy of mobile systems
- Privacy-enhancing technologies
- Security measurement and analysis
- Wireless and *ad-hoc* network security
- Networks forensics
- Collaborative network security
- Security for smart X
- Security for large system and critical infrastructure

IMPORTANT DATES

Paper Submission Deadline
December 15th, 2015

Notification of Acceptance
January 30th, 2016

Camera-ready papers
February 15th, 2016

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 http://jems.sbc.org.br/dissect2016.

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.

ORGANIZING COMMITTEE

Carol Fung
Virginia Commonwealth University

Mohamed Faten Zhani
ÉTS, Canada

Weverton Cordeiro
UFRGS, Brazil

For more information, please visit
http://www.dissect.vcu.edu/2016