The Sixth International Workshop on Security in NFV-SDN (SN-2019) in conjunction with the 5th IEEE NFV-SDN conference,

12 November 2019, Dallas, Texas, USA

Scope

Network Function Virtualization (NFV) and Software Defined Network (SDN) have changed the networking industry dramatically. NFV virtualizes network services by utilizing virtualization technologies to reduce the dependency on underlying hardware. NFV provides many benefits such as faster service enablement, ease of resource management and lower OPEX and CAPEX. SDN separates the control functions from the underlying physical network by decoupling the control and data planes. SDN provides many benefits such as reduced costs, ease of deployment and management, better scalability, availability, flexibility and fine-grain control of traffic and security. Like traditional networks, they are subject to various security threats and attacks. In this workshop, we invite high-quality submissions in the areas of NFV and SDN security and other related areas. Submitted papers should highlight methods and approaches that can be used to analyse the security risks and requirements, threats and techniques related to NFV and SDN and to provide novel methods and approaches to assure security in NFV and SDN.

Topics of interest include but are not limited to the following areas:

- Security, reliability and privacy through SDN and NFV in 5G networks
- Management and orchestration of NFV and SDN elements for security
- Secure design of NFV and SDN solutions, security enablers
- Security threats and vulnerabilities introduced by NFV and SDN technologies
- Threat detection and mitigation through SDN and NFV
- Security policy specification and management in SDN and NFV systems
- Security related monitoring and analytics in SDN and NFV solutions
- 5G security architecture, trust and confidence
- Authentication, authorization and Accounting in SDN
- Secure SDN with Blockchain
- Security of applying SDN to wireless and mobile network
- Security of applying NFV and SDN to IoT
- Security of applying NFV and SDN to cloud computing
- Security of SDN API
- Risk and compliance issues in SDN
- Securing SDN infrastructure
- Security architecture for SDN
- Security standard of SDN
- Security of SDN data plane
- Security of SDN control plane
- Security of SDN application plane
- Security of Routing in SDN
- Security of network slicing
- Security as a service for SDN
- SDN security using artificial intelligence

All submitted papers will be peer-reviewed and included in IEEE-NFV-SDN Proceeding in IEEE Xplore. The manuscripts must be prepared in English, following IEEE two-column Manuscript Templates for Conference Proceedings with a maximum length of six (6) printed pages (10-point font), including figures.

The workshop deadlines:

- Workshop Paper Submission: July 26, 2019
- Notification of Acceptance: August 30, 2019
- Camera-ready Submission: September 20, 2019
- Paper Presentation: November 12, 2019

Edas Submission Link : https://edas.info/N26379

For more info visit: https://www.pasiphae.eu/SN-2019

The Workshop Chairs:

Dr Shao Ying Zhu - Department of Electronics, Computing and Mathematics, University of Derby, UK

Dr. Evangelos Markakis – Department of Electrical & Computer Engineering, Hellenic Mediterranean University, Hellas

Dr Yacine Rebahi – Fraunhofer Fokus, Germany