

Call for Papers

The First International Workshop on Security in NFV-SDN (SNS2016) in conjunction with the 2nd IEEE NFV-SDN conference, 7-9 November, Palo Alto, California, USA

Workshop website: <http://computing.derby.ac.uk/sns2016/>

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

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
- 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

Submission

Paper submissions will be handled on-line through the EDAS system at <https://edas.info/newPaper.php?c=22175&track=81343>. All submitted papers will be peer-reviewed. 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. You can find the IEEE Computer Society Proceedings Author Guidelines at <http://www.computer.org/web/cs-cps/>. To be published in the Workshop Proceedings and to be eligible for publication in IEEE Xplore, at least one author of an accepted paper is required to register and present the paper at the workshop. The IEEE reserves the right to exclude a paper from distribution after the conference (including its removal from IEEE Explore) if the paper is not presented at the conference. Papers are reviewed on the basis that they do not contain plagiarized material and have not been submitted to any other conference at the same time (double submission). These matters are taken very seriously and the IEEE Communications Society will take action against any author who engages in either practice. Authors of selected papers will be invited to submit an extended version of their work as a book chapter for Springer book Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications (<http://computing.derby.ac.uk/gssnoa2016/>).

Important Dates

The workshop deadlines:

- Paper Submission: July 31, 2016
- Notification of Acceptance: September 7, 2016
- Camera Ready: October 7, 2016

Workshop Chairs

- Shao Ying Zhu, University of Derby, UK
- Eleni Trouva, NCSR Demokritos, Greece
- Richard Hill, University of Derby, UK
- Collin Allison, University of St Andrews, UK
- Muhammad Shuaib Siddiqui, Fundació i2CAT, Spain
- Linas Maknavicius, Nokia Bell Labs, France

Technical Program Committee (TPC)

- Sandra Scott-Hayward - Queen's University Belfast, UK
- Roberto Bifulco - NEC Labs Europe, Germany
- Ludovic Jacquin - Hewlett Packard Labs, UK
- Marco Anisetti - University of Milan, Italy
- Augusto Ciuffoletti - University of Pisa, Italy
- Colin Allison - University of St Andrews, UK
- Rhonda L. Farrell- Booz Allen Hamilton, USA
- Jianxin Li-Beihang University, China
- Ljiljana Trajkovic - Simon Fraser University, Canada
- Eleni Trouva, Harilaos Koumaras, Michail-Alexandros Kourtis - NCSR Demokritos, Greece
- Muhammad Shuaib Siddiqui, Eduard Escalona, Jordi Ferrer, Amaia Legarrea - i2CAT, Spain
- Carolina Canales, Miguel Angel Garcia, Miguel-Angel Monjas, Manuel Lorenzo - Ericsson, Spain
- Felix Klaedtke - NEC Labs Europe, Germany
- Linas Maknavicius, Abdelkader Outtagarts - Nokia, Bell Labs, France
- Nicolae Paladi - SICS, Sweden
- Gergely Biczók - Budapest Univ. of Technology and Economics, Hungary

Contacts

Shao Ying Zhu - s.y.zhu@derby.ac.uk

Eleni Trouva - trouva@iit.demokritos.gr