IEEE Workshop on Security in Virtualized Networks

SEOUL, KOREA - June 10 2016

http://www.sec-virtnet.org

CALL FOR PAPERS

SCOPE

The IEEE International Workshop on Security in Virtualized Networks (**Sec-VirtNet 2016**) will be held on June 10, 2016 in Seoul Korea along with the 2nd IEEE International Conference on Network Softwarization (**NetSoft 2016**, sites.ieee.org/netsoft). Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies fundamentally change the network architecture as well as the way networks (e.g., mobile or transport networks) will be deployed and operated. This new generation of virtualized and multi-tenant networks comes with various promises (e.g., CAPEX and OPEX optimization) but also raises several new security challenges, in particular because network functions will no longer be embedded and thus "protected" within network equipments. Besides, network virtualization also brings various opportunities for security such as the possibility to offer software-based security appliances or Security as a Service.

The **Sec-VirtNet 2016** workshop focuses on novel research topics dealing with security in these virtualized networks. Submitted papers should provide theoretical or practical approaches to identify and address the critical security issues of such virtualized networks or, conversely, to exploit these promising virtualization and SDN technologies in order to offer innovative security services.

TOPICS OF INTEREST

Authors are invited to submit papers that fall into the area of software-defined and virtualized infrastructures.
Topics of interest include, but are not limited to, the following:

- Security of Software Defined Networking (SDN)
- Security of virtualized network applications
- Security of SDN controllers
- SDN protocol hardening
- Security of Network Function Virtualization (NFV)
- Security of multi-tenant virtualized networks
- SDN/NFV-based security deployment
- Dynamic security assessment & testing
- Security assurance in virtualized networks
- SDN-based analytics for security
- Security-aware network service chaining and orchestration
- Security of network slicing
- Security of 5G network infrastructure including IoT & verticals
- Security services based on SDN and network virtualization
- Virtualization of security appliances (eg firewall, IDS)
- Security as a Service (SECaaS)
- Trusted computing in SDN and NFV environments
- Security & privacy policy management in virtualized network
- Enforcement of sovereignty policies in virtualized networks
- Regulation & liability management in software-based networks

PAPER SUBMISSION

Authors are invited to submit only original papers (written in English) not published or submitted for publication elsewhere. Papers can be up to 6 pages. Papers should be in IEEE 2-column US-Letter style using IEEE Conference templates (http://www.ieee.org/conferences_events/conferences/publishing/templates.html) and submitted in PDF format via JEMS at: https://jems.sbc.org.br/sec-virtnet2016.

Papers exceeding these limits, multiple submissions, and self-plagiarized papers will be rejected without further review. All submitted papers will be subject to a peer-review process. The accepted papers will be published in the Sec-VirtNet 2016 Proceedings and appear in IEEE Xplore®.

IMPORTANT DATES

- Paper Submission: February 14, 2016 (Extended)
- Notification of Acceptance: February 29, 2016
- Camera-ready Submission: March 13, 2016

WORKSHOP CO-CHAIRS

- Stéphane Betgé-Brezetz, Nokia Bell Labs, France
- Emmanuel Dotaro, Thales, France
- Hervé Debar, Telecom SudParis, France

NETSOFT GENERAL CHAIR

- James Won-Ki Hong, POSTECH, Korea

NETSOFT WORKSHOP CO-CHAIRS

- Burkhard Stiller, University of Zurich, Switzerland
- Noura Limam, University of Waterloo, Canada
- Younghan Kim, Soongsil University, Korea

TECHNICAL SPONSORS

The technical sponsors are IEEE Communications Society, IEEE Computer Society, IEEE Signal Processing Society, and IEEE Consumer Electronics Society.