*****Call for Papers*****

Security in Emerging Networking Technologies

Special Issue in IEEE Transactions on Dependable and Secure Computing (TDSC)

Network infrastructure is undergoing a major shift away from ossified hardware-based networks to programmable software-based networks. One compelling example of this paradigm shift is the advent of Software-Defined Networking (SDN). A traditional network mixes control and traffic processing logic in single hardware devices, making the network more complex and harder to manage. SDN has addressed this issue by decoupling the control plane in network devices from the data plane to simplify production networks. On the other hand, enterprise networks are populated with a large number of proprietary and expensive hardware-based middleboxes, such as firewall, IDS/IPS, and load balancing. Hardware-based middleboxes present significant drawbacks such as high costs, management complexity, slow time to market, and unscalability. Network Function Virtualization (NFV) was proposed as another new network paradigm to address those drawbacks by replacing hardware-based network functions with virtualized software systems running on generic and inexpensive commodity hardware. Given their benefits, SDN and NFV have recently attracted significant attention from both academia and industry.

SDN and NFV introduce significant granularity, visibility, flexibility, and elasticity to networking, but at the same time bring forth new security challenges. For example, decoupling the data plane and the control plane in SDN essentially opens a door to attackers for exploiting the vulnerabilities of SDN controllers, APIs, applications, and protocols, and further break their trust relations. Meanwhile, both SDN and NFV could be leveraged to strengthen network defense. The aim of this special issue is to encompass research advances in all areas of security in emerging networking technologies. The special issue intends to provide a venue for interested researchers and practitioners to share their novel research ideas and results.

Topics

This special issue calls for original, high-quality, high-impact research papers related to the following broad topics, but are not limited to:

- SDN/NFV-enabled security architecture
- SDN/NFV-based automated network security
- SDN/NFV-based mitigation for attacks
- SDN/NFV-based network forensics and auditing
- Authentication/confidentiality in SDN/NFV-based networks
- Proofs of security in SDN/NFV-based networks
- Logic flaws in SDN/NFV implementations
- Attacks/defense to SDN controllers, protocols, and APIs
- SDN/NFV-oriented security policy enforcement
- Trust management of SDN applications and controllers
- Development and deployment of NFV-based security functions (virtual firewalls, virtual IDSs, virtual DDoS mitigation, etc.)
- SDN/NFV-enabled security for Internet of Things
- Safe state migration in NFV
- Network security as a service
- Privacy-preserving solutions for SDN/NFV
- Security of programmable components

Important Dates
Submission deadline: September 31, 2017
First round of reviews: December 15, 2017
Revised papers due: January 31, 2017
Final notification: February 28, 2018
Final manuscript due: April 15, 2018
Expected inclusion in issue: September 2018

Submission & Major Guidelines
Papers submitted to this special issue for possible publication must be original and must not be under consideration for publication in any other journal or conference. TDSC requires meaningful technical novelty in submissions that extend previously published conference papers. Extension beyond the conference version(s) is not simply a matter of length. Thus, expanded motivation, expanded discussion of related work, variants of previously reported algorithms, incremental additional experiments/simulations, may provide additional length but will fall below the line for proceeding with review. Submissions must be directly submitted via the IEEE TDSC submission web site at *https://mc.manuscriptcentral.com/tdsc-cs*, and must follow instructions for formatting and length listed there.

Guest Editors
Gail-Joon Ahn, Arizona State University, USA, ahn@asu.edu
Guofei Gu, Texas A&M University, USA, guofei@cse.tamu.edu
Hongxin Hu, Clemson University, USA, hongxih@clemson.edu
Seungwon Shin, KAIST, Korea, claude@kaist.ac.kr