Guest Editors' Introduction: Special Section on Security in Emerging Networking Technologies

Gail-Joon Ahn, *Senior Member, IEEE*, Guofei Gu, *Senior Member, IEEE*, Hongxin Hu, *Member, IEEE*, and Seungwon Shin, *Member, IEEE*

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.

In response to the call for papers, this special section has collected 14 submissions and the following 4 papers were included in this special section after rigorous peer review and careful revision.

The first paper "*Dynamic Packet Forwarding Verification in SDN*" by Qi Li, Xiaoyue Zou, Qun Huang, Jing Zheng, and Patrick P.C. Lee proposes a robust and lightweight packet forwarding verification mechanism that is able to detect various sophisticated attacks against packet forwarding in SDN. The proposed mechanism leverages dynamic packet sampling to verify integrity of packets on networks to detect various attacks violating packet integrity in SDN. Extensive experiments have been done with real trace to demonstrate that the proposed system can achieve more than 97 percent verification accuracy, while only incurring around 0.2 percent packet collection rate and less than 5 percent throughput degradation.

The second paper "*SDN-based Privacy Preserving Cross Domain Routing*" by Qingjun Chen, Shouqian Shi, Xin Li, Chen Qian, and Sheng Zhong presents a privacy-preserving cross-domain routing optimization protocol in multi-domain SDN environments. The proposed solution provides two fundamental routing functions, policy-compliant shortest path computing and bandwidth allocation, to ensure strong protection for the private information of domains. Experimental evaluation shows that the proposed system is efficient in computation and communication costs based on real ISP network topologies.

The third paper "*Detecting and Mitigating Target Link-Flooding Attacks Using SDN*" by Juan Wang, Ru Wen, and Jiangqi Li introduces a novel defense system for the link-flooding attack (LFA), leveraging some key features, such as programmability, network-wide view, and flow traceability, of SDN. The proposed solution includes a target link selection approach and a congestion monitoring mechanism to effectively detect LFA, and a multiple traffic rerouting method and a malicious traffic blocking approach to mitigate LFA. Experimental results show that the proposed system can accurately detect and rapidly mitigate LFA, but only imposes minimal communication overhead.

The fourth paper "*Dependability Integration in Cloud-hosted Telecommunication Services*" by Wiem Abderrahim and Zied Choukair proposes a Dependability Broker Architecture in Telco Clouds (DBA-Telco), which is a broker architecture

- *G.-J. Ahn is with the Security Engineering for Future Computing (SEFCOM) Laboratory, Arizona State University, Tempe, AZ 85287. E-mail: gahn@asu.edu.*
- *G. Gu is with the Secure Communication and Computer Systems (SUCCESS) Laboratory, Texas A&M University, College Station, TX 77843. E-mail: guofei@cse.tamu.edu.*
- *H. Hu is with the School of Computing, Clemson University, Clemson, SC 29634. E-mail: hongxih@clemson.edu.*
- *S. Shin is with the School of Electrical Engineering, KAIST, Daejeon 34141, South Korea. E-mail: claude@kaist.ac.kr.*

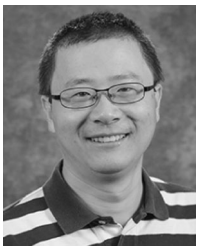
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TDSC.2019.2906921

based on an SDN controller that operates on NFV environments, to guarantee dependability in telecommunication services hosted in cloud environments according to the Service Availability Level (SAL) fixed by European Telecommunications Standards Institute (ETSI). Experimental results demonstrate that that the proposed approach provides reliable and maintainable bottlenecks for the different SALs but with the restriction on the arrival rate range.

The Guest Editors would like to thank all of the authors who have submitted their research to this special section. They also would like to thank the many experts in this field who have participated in the review process and provided helpful suggestions to the authors for improving their work.

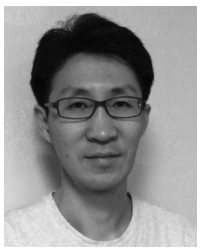
Gail-Joon Ahn
Guofei Gu
Hongxin Hu
Seungwon Shin
Guest Editors

Gail-Joon Ahn received the PhD degree in information technology from George Mason University, Fairfax, Virginia, in 2000. He is a professor with the School of Computing, Informatics, and Decision Systems Engineering, Ira A. Fulton Schools of Engineering and the director of security engineering for Future Computing Laboratory, Arizona State University. His research has been supported by the U.S. National Science Foundation, National Security Agency, U.S. Department of Defense, U.S. Department of Energy, Bank of America, Hewlett Packard, Microsoft, and Robert Wood Johnson Foundation. He is a recipient of the U.S. Department of Energy CAREER Award and the Educator of the Year Award from the Federal Information Systems Security Educators Association. He is a senior member of the IEEE.



Guofei Gu received the PhD degree in computer science from the College of Computing, Georgia Institute of Technology, in 2008. He is an associate professor with the Department of Computer Science & Engineering, Texas A&M University. His research interests include network and systems security, such as malware and APT defense, software-defined programmable security (e.g., SDN/NFV), mobile and IoT security, and intrusion/anomaly detection. He is a recipient of 2010 NSF CAREER Award, 2013 AFOSR Young Investigator Award, 2010 IEEE S&P Best Student Paper Award, 2015 ICDCS Best Paper Award, Texas A&M Dean of Engineering Excellence Award, Charles H. Barclay Jr. '45 Faculty Fellow, TEES Select Young Fellow, TEES Research Impact Award, and a Google Faculty Research Award. He is a senior member of the IEEE.

Hongxin Hu received the PhD degree in computer science from Arizona State University, Tempe, Arizona, in 2012. He is an assistant professor with the School of Computing, Clemson University. His current research interests include security in emerging networking technologies, security in Internet of Things (IoT), security and privacy in social networks, and security in cloud and mobile computing. He is a recipient of 2019 NSF CAREER Award. His research has been featured by the IEEE Special Technical Community on Social Networking and received wide press coverage including ACM TechNews, InformationWeek, Slashdot, NetworkWorld, etc. He is a member of the IEEE.



Seungwon Shin received the BS and MS degrees in electrical and computer engineering from KAIST, and the PhD degree in computer engineering from the Electrical and Computer Engineering Department, Texas A&M University. He is an associate professor with the School of Electrical Engineering, KAIST. Before joining KAIST, he spent nine years at industry, where he devised several mission critical networking systems. He is currently a member of editorial board of the *Elsevier Computers and Security*. His research interests span the areas of software defined networking security, Internet of Things (IoT) security, and Botnet analysis/detection. He is a member of the IEEE.