DOI: 10.19729/j.cnki.1673-5188.2018.04.001
http://kns.cnki.net/kcms/detail/34.1294.TN.20181029.1705.002.html, published online October 29, 2018

Editorial

Security and Availability of SDN and NFV

▶ Guest Editor

CHEN Yan received the Ph.D. degree in computer science from the University of California at Berkeley, USA, in 2003. He is currently a professor with the Department of Electrical Engineering and Computer Science, Northwestern University, USA. Based on Google Scholar, his papers have been cited over 10,000 times and his h-index is 49. His research interests include network security, measurement, and diagnosis for large-scale networks and distributed systems. He received the Department of Energy Early CAREER Award in 2005, the Department of Defense Young Investigator Award in 2007, the Best Paper nomination in ACM SIGCOMM 2010, and the Most Influential Paper Award in ASPLOS 2018.

Software defined networking (SDN) and network function virtualization (NFV) have attracted significant attention from both academia and industry. Fortunately, by virtue of unique advantages of programmability and centralized control, SDN has been widely used in various scenarios, such as home networking, enterprise networking, telecommunication networking, data center, and cloud networking. Meanwhile, through adopting virtualization technology to realize various network functions, NFV delivers high-performance networks with greater scalability, elasticity, and adaptability at reduced costs compared to networks built from traditional networking equipment. NFV covers a wide range of network applications, including video, Software Defined Wide Area Network (SD-WAN), Internet of Things (IoT), and 5G.

With SDN and NFV, the flexibility of networks is increased, the utilization of resources is improved, the network operation and maintenance cost is cut down, and the time-to-market of new service is considerably decreased. However, these benefits bring new security challenges for network at the same time. Besides traditional inherent security issues (Distributed Denial of Service (DDoS) attack; Man-in-the-Middle attack), various new attacks are introduced by the new architecture and technology, such as data-to-control plane saturation attack, control plane reflection attack, and control-data plane view inconsistency. Thus, new countermeasures for this new scenario are necessary to defend against attacks and make the whole system more secure and reliable.

This special issue aims at giving a bird view to the concept of SDN and NFV, then analyzing the potential security issues and proposing feasible countermeasures.

Since the birth of SDN, academia and industry have invested a lot of energy in research. However, the deployment of SDN has faced several security issues which put a severe threat to crucial resources of the SDN infrastructure, including resources of the control plane, data plane, and in-between downlink channel. The first paper "Survey of Attacks and Countermeasures for SDN" by BAI et al. analyzes the vulnerability of SDN, presents two kinds of SDN-targeted attacks, namely data-to-control plane saturation attack and control plane reflection attack, and finally proposes the corresponding defense frameworks.

With the development and revolution of network in recent years, traditional hardware based network security solutions have shown some significant disadvantages in cloud computing based Internet data centers (IDCs), such as high cost and lack of flexibility. With the implementation of SDN, network security solutions could be more flexible and efficient, such as SDN based firewall service and SDN based DDoS-attack mitigation service. The second paper "SDN Based Security Services" by ZHANG et al. analyzes some typical SDN based network security services, and provides a research on SDN based cloud security service and its implementation in IDC network.

SDN has been well researched in both academia and industry. The main reason SDN is so concerned is its ability to dynamically change the network states in response to the global view. In particular, the control message processing capability on switches, especially the prevailing Ternary Content Addressable Memory (TCAM) based flow tables on physical SDN switches, proves to be the bottleneck along the policy update pipeline. The limitation has slowed down network updates

Editorial

CHEN Yan

and hurt network visibility, which further constrains the control plane applications with dynamic policies significantly. To solve this serious problem, the third paper "Optimization Framework for Minimizing Rule Update Latency in SDN Switches" by CHEN et al. presents a SDN update optimization framework RuleTris to minimize rule update latency for TCAM-based switches.

NFV is a new network technology which will be widely popularized and used in the foreseen future. Therefore, how to build a secure architecture for NFV is an important issue. Trusted computing has the ability to provide security for NFV and it is called trusted NFV system. The fourth paper "A New Direct Anonymous Attestation Scheme for Trusted NFV System" by CHEN et al. proposes a new NFV Direct Anonymous Attestation (NFV-DAA) scheme based on trusted NFV architecture. It is based on the Elliptic curve cryptography, and transfers the computation of variable D from the Trusted Platform Module (TPM) to Issuer. With the mutual authentication mechanism that those existing DAA schemes do not have and an efficient batch proof and verification scheme, the performance trusted NFV system is optimized. According to the experiment results, NFV-DAA scheme has higher security level and efficiency than those existing DAA schemes.

The aforementioned four excellent works comprehensively set forth the security challenges faced by SDN and NFV from different perspectives, and propose countermeasures and defense frameworks to effectively improve the security and availability of SDN and NFV.

Finally, we would like to thank all the authors, the external reviewers and the staff at *ZTE Communications* for contributing their excellent research work, precious time and energy to this special issue.