Chapter 11
Software-Defined Network Security

Ahmed Demirpolat
Middle East Technical University, Turkey

Doğanalp Ergenç
Middle East Technical University, Turkey

Esref Ozturk
Middle East Technical University, Turkey

Yusuf Ayar
Middle East Technical University, Turkey

Ertan Onur
Middle East Technical University, Turkey

ABSTRACT

The future networks are expected to lead a hyper-connected society with the promise of high social and economic value. The goal is to solve today's network problems and provide satisfactory security. Thus, the future networks require a flexible infrastructure that is secure against cyberattacks. Software defined networking (SDN) can be considered as one of the building blocks of upcoming networking technologies. In this chapter, first, the limitations of today's networks are presented. Then, solutions to secure the networks with SDN components are given. This concept is referred to as "SDN for Security." While SDN facilitates securing networks in general, it introduces additional challenges, mainly, the vulnerabilities of the SDN components such as the controller have to be addressed. Security for SDN aims at securing SDN assets and is discussed in the sequel. After reading this chapter, readers will obtain a comprehensive overview of the limitations of traditional networks, such as how SDN overcomes those limitations and the security issues thereof.

DOI: 10.4018/978-1-5225-6023-4.ch011

INTRODUCTION

Changing business and consumer demands in technology have transformed the perspective of networking. Rather than the former person-to-person or person-to-computer interactions, with the rapidly spreading Internet of Things (IoT) and smart devices, the world has become a complete "anything-to-anything" connected network. From this perspective, connection to anything anytime and anywhere is perceived as the most basic requirement for very near future. All these paradigm changes entail quite significant improvements to adopt requirements of the future networks. For example, the key performance indicators (KPI) of 5G networks directly infer the technological exigence of the near future. These indicators include more than 1 Gbps data rate with ultimately 1ms end-to-end latency. 99% availability and reliability are also expected even in high-device density which supports nearly 10,000 per km^2 (Fallgren, Spapis, Qi, Martín- Sacristán, Carrasco, … Fresia, 2016). However, it is not possible for present mobile networks to address the 1000x key performance requirements of 5G because of their limitations.

Today, the networking infrastructures are very complex and hard-to-be-operated as they reflect outdated technological requirements which belong a decade ago. They lack common control functions and interfaces and network operators have to separately configure network devices using vendor-defined commands to apply the high-level management policies (Kim & Feamster, 2013). It obliges the existing mobile networks to be structured with vendor locked-in and the dedicated hardware and software. These components implement such network functions which are not only prone to misconfiguration but also costly and require trained/expert administrators (Goransson, Black & Culver, 2016). Besides, from a security point of view, since network policies are tightly bundled to physical resources instead of services and applications, today's solutions are strained to deploy, manage, program and scale the security throughout heterogeneous equipment from multiple vendors. To enforce consistent security policies through computing, storage, and network domains and especially across multiple data centers is very difficult. It should be noted that there is no end-to-end solution for security orchestration across data center networks today (Ahmad, Namal, Ylianttila, & Gurtov, 2015). Eventually, all those limitations significantly reduce flexibility and slow down the evolution of the infrastructure for the future networks (McBride, Cohn, Deshpande, Kaushik, Mathews, & Nathan, 2013; Liyanage, Ylianttila, & Gurtov, 2015).

Software-defined networking is a novel technique that may overcome the limitations of traditional networks. It is, for instance, expected to be used in the implementation of 5G networks since SDN perfectly compromises the logical and functional architecture of 5G which targets modularity, flexibility, and scalability in the first place. Besides, considering the significantly complex architecture of the future networks, it is very natural to take advantage of "softwarization" for more manageable, reusable, high-performance and optimized systems. To provide those conditions, SDN architecture fundamentally abstracts lower-level functionality by detaching the control plane from the data plane. As shown in Figure 1, a software-defined network can be described in three levels; application, control and infrastructure levels. The most significant level in SDN is the control level (controller) that is responsible for implementing the network control logic. It implements the southbound, northbound and east/west interfaces for intercommunication between the SDN application, controller, and infrastructure at different levels. The southbound interface is between the controller and infrastructure levels and mainly specifies functionalities to manage switching devices residing at data plane. Advising packet forwarding rules and taking feedback of current network status could be example capabilities accomplished over this interface. Similarly, for communication between the application level and the controller, the northbound interface establishes a service access generally through an API. For example, using the information gathered from