Security by Software Defined Networking (SDN)

Dr.-Ing. Rahamatullah Khondoker
Researcher, Mobile Networks, Fraunhofer SIT
Darmstadt, Germany
rahamatullah.khondoker@sit.fraunhofer.de

I. Goal

The aim of this session is to assist communication network researchers especially those who are located in Bangladesh by providing theoretical background and hands-on on Software-Defined Networking (SDN) and OpenFlow capabilities i.e., automatic detection and mitigation of network attacks.

II. Scale of Network Attackers

According to the statistics of Deutsche Telekom[1], the number of network attackers per month were increased from 100K to 550K in the last one year (June 2015 - June 2016). Traditional defense mechanisms where the strategy is automatically detect and manually mitigate are inefficient to detect and mitigate attacks.

III. SDN

Software-Defined Networking (SDN) decouples control plane of a networking device (called controller) from the data plane (called switch) where the planes communicate with each other by an open interface such as OpenFlow[1] so that the data plane can be directly programmed. Among others, these centralized monitoring and control features of SDN might be used wisely to detect and mitigate network attackers automatically.

IV. Security by SDN

The aim of "Security by SDN" is to utilize the capabilities of SDN to improve security of traditional networks. The work in this topic might be divided into three categories: 1, developing security applications within the controllers to increase performance (i.e., Defense4All), 2, developing security applications outside the controllers to increase flexibility (i.e., OrchSec shown in Fig.1, more details in [2], and AutoSec [3]), and 3, developing frameworks to write security applications easily (i.e., FRESCO). The result of the security applications is to automatically detect and mitigate different types of network attacks including (D)DoS, Scanning, ARP Spoofing, and Cache Poisoning.

V. Security for SDN

SDN itself is not immune to security vulnerabilities which currently exist in the legacy system or which may newly arise due to change in the network design. The target of "Security for SDN" is to analyze vulnerabilities of the SDN applications [4], architectures, and protocols [6] including controllers, North Bound Interfaces (NBIs), and South Bound Interfaces (SBIs) and develop/propose methods to defend and mitigate against those vulnerabilities and attacks (i.e., AVANT-GUARD).

[1]http://www.sicherheitstacho.eu/statistics

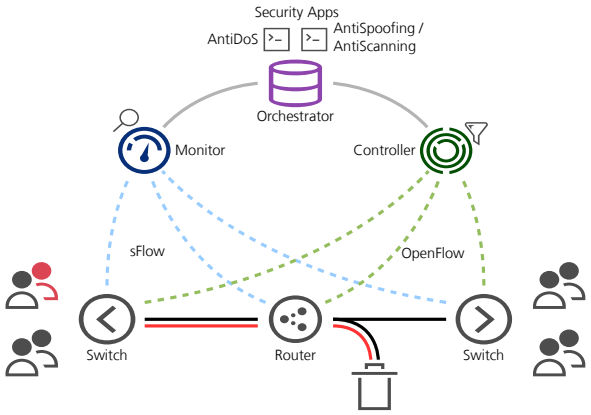

Fig. 1: OrchSec Architecture

VI. Recommendation

Before deploying SDN into a network, both aspects of security "Security by SDN" and "Security for SDN" should be considered to support "Security by Design" and to reduce different types of risks including ROI, security threats, and company reputation.

References

[1] M. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev*, vol. 38, no. 2, 2008.

[2] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, ser. IEEE NOMS 2014, pp. 1–9.

[3] R. Khondoker, P. Larbig, D. Senf, K. Bayarou, and N. Gruschka, "Autosecsdndemo: Demonstration of automated end-to-end security in software defined networks," in *IEEE Conference on Network Softwarization*, ser. IEEE NetSoft 2016.

[4] D. Magin, R. Khondoker, and K. Bayarou, "Security analysis of openradio and softran using stride framework," in *The 24th International Conference on Computer Communications and Applications*, ser. ICCCN 2015.

[5] M. Brandt, R. Khondoker, R. Marx, and K. Bayarou, "Security analysis of software defined networking protocols—openflow, of-config and ovsdb," in *Special Session on «Software-Defined Networking»*, ser. IEEE ICCE 2014.