A Playground for Software-Defined Networking Security

Seunghyeon Lee, Chanhee Lee, Hyeonseong Jo, Jinwoo Kim, Seungsoo Lee, Jaehyun Nam, Taejune Park, Changhoon Yoon, Yeonkeun Kim, Heedo Kang, and Seungwon Shin
GSIS, School of Computing, KAIST
{coksm1963, mitzvah, hsjjo, jinwoookim, lss365, namjh, taejune.park, chyoon87, yeonk, kangheedo, claude}@kaist.ac.kr

ABSTRACT

Although Software-Defined Networking (SDN) is being considered as a promising future networking technology, it has non-negligible security issues to be solved. Despite the necessity for overcoming the security issues, however, there is no well-organized references that contain what the security issues are. To promote and accelerate SDN security studies, we have recently constructed a public knowledge repository, called as **SDNSecurity**, which has systematized SDN security vulnerabilities with lots of useful resources (e.g., Animations, demo-vids, source codes and so forth) and proposed feasible research projects to handle the security issues. In this paper, we briefly introduce overall research projects and available resources as a knowledge repository.

1. INTRODUCTION

Software-Defined Networking (SDN) has steadfastly brought innovation to manage enterprise network as a centralized manner. The application can handle varying network conditions through programmable network environment with cost efficient and operational flexibility as a brain of a network. Although it has already been *de facto* standard for enterprise network with the advantages, people who adopt SDN to manage a network have been worried about security issues that cause security problems. Researchers have tried to address the security issues. However, they are hard to find well-organized knowledge to follow up what kinds of security issues must be solved. Previously, OpenFlowSec [3] has covered to security issues and proposed feasible solutions, however, it is not sufficient to address newly open security issues.

In this work, we present a playground named **SDNSecurity** (sdnsecurity.org) [4] as a comprehensive knowledge repository to cope with various practical security issues. As SDNSecurity is inspired from OpenFlowSec [3], we have systematized open security questions with comprehensive attack vectors including unrevealed attacks including useful resources. To overcome the open questions, we also have proposed feasible solutions with reference implementations that help to build security-enhanced SDN operational environment. We believe that SDNSecurity helps people easily understand what kinds of security issues there are in SDN and gives opportunities to solve open problems in an SDN security area.

2. SDNSECURITY

As a comprehensive knowledge repository, SDNSecurity has covered open security issues through providing useful resources such as animations, demo-vids, source codes, detail descriptions, presentations, and so forth. Besides to the resources, SDNSecurity has continuously proposed feasible solutions as a security project. The given projects are categorized into two parts: on-going projects (Security-mode ONOS [2], sCARF, SDN Vulnerability Genome, and POSEIDON) and completed projects (FRESCO [8], Rosemary [9], AVANT-GUARD [10], SE-Floodlight [6], Security Actuator, OpenFlow BotHunter [1, 5], and FortNOX [7]). The rest of this section, we briefly summarize those projects we provide in SDNSecurity and currently available resources.

2.1 Ongoing Security Projects

Given projects in SDNSecurity has mainly focused on revealing and mitigating threats in SDN. Here, we first introduce ongoing projects for secure and robustness SDN environment:

sCARF: While FRESCO provides an ease-of-use development environment for building up security applications, it still has some limitations (e.g., lack of supporting multi-applications running, useful modules, closed source, and limited features). To overcome the limitations of FRESCO, we newly propose sCARF which is a comprehensive security application framework supporting powerful and useful features such as multiple application environment, dynamic application loader, distributed database, collaboration with host, efficient message delivery and other useful features. Especially, compared with FRESCO, sCARF has concerned both network and host features to react more intelligently against threats. Currently, sCARF is under development on ONOS.

Security-Mode ONOS: The goal of this project is to provide a secure SDN application execution environment to Open Network Operating System (ONOS), which an open-source distributed SDN controller platform. In networks managed by ONOS, it is possible to deploy diverse ONOS applications to enable various network control functions by leveraging the powerful APIs offered by ONOS platform. At the same time, ONOS applications with such powerful authority may also be abused or misused to cause security problems. To eliminate such abuse or misuse opportunities, Security-Mode ONOS enforces security policies to constrain ONOS applications. This project is currently under development.

SDN Vulnerability Genome Project: In this project, we address vulnerabilities of SDN environments and the corresponding attacks. We classify SDN related attacks into three major categories (control plane, control channel, and data plane). For the control plane specific attacks, we focus on vulnerabilities of controllers (e.g., ONOS, OpenDaylight, and FloodLight). While the channel encryption is highly recommended, it is hardly used due to the performance issue.

Thus, for the control channel specific attacks, we concentrate on the lack of encryption. For the data plane specific attacks, we focus on the hardware restriction such as TCAM and firmware. With the careful analysis of each point, we demonstrate already-known attacks as well as newly discovered attacks by our group. For the given attacks, this project provides the source codes, demonstration videos, conceptual animations, and detail descriptions for each attack.

POSEIDON: POSEIDON is an automated penetration testing framework that reproduces 20 known attack scenarios with well-known SDN elements and provides fuzzing features to find unknown attacks. POSEIDON supports diverse well-known controllers such as ONOS, OpenDaylight, and Floodlight. We newly found five undiscovered attack scenarios through the fuzzing functions by POSEIDON (we keep finding new attack scenarios in diverse SDN environments). POSEIDON allows security managers to systemically and automatically measure the security quality of their networks without significant efforts.

2.2 Completed Security Projects

Due to space constraints, we only provide a brief description of each project that has been completed. More information is available on our website (sdnsecurity.org).

Rosemary: While the control plane operates as the critical middleware facilitator between the data plane and network applications, even small and basic flaws in network applications can lead to the crash of the control plane and loss of network functionality. Rosemary employs several strategies (e.g., application containment, resource management, and application sandboxing) to construct a robust, secure, and high-performance network operating system.

AVANT-GUARD: OpenFlow network is susceptible to *a control plane saturation attack*, which exploits the bottleneck that arises between the control plane and the data plane. Furthermore, OpenFlow offers limited support for *effective network monitoring*, which is a crucial feature required for implementing diverse security services. AVANT-GUARD implements the data plane extensions that enable scalable and vigilant switch flow management to allow the development of more scalable and resilient SDN security services ultimately.

FRECSO: Developers encounter difficulties to build up security application on SDN due to it require complex logic to be implemented. For the developers who wish to devise network security applications easily and effectively, FRESCO attempts to provide an effective, efficient, and easy programming framework for implementing various security detection and mitigation modules.

SE-Floodlight: SE-Floodlight is a security-enhanced version of Floodlight. The key features of SE-Floodlight include authentication, role-based authorization, a permission model for the data plane access, flow rule conflict resolution and more. SE-Floodlight adds security enforcement kernel (SEK) between the control and data plane to support the features listed above.

2.3 Available Resources

To spread the open security questions and feasible solutions, SDNSecurity is ready to open various type of resources including reference implementations. To date, we not only give written descriptions but also provide animated SDN attack scenarios, demonstration video clips, code samples, and more. We also provide presentation videos to give a better understanding of some research projects. Also, SDNSecurity includes an online forum to form an SDN security research community.

3. CONCLUSION AND FUTURE WORK

While SDN has emerged as the innovative technology for enabling programmable network environment to realize a network with efficient and dynamic, open security issues in SDN has been still left untouched. Moreover, due to less attempt for building up knowledge repository that deals with security issues in SDN, people cannot catch up the open security questions not solved yet and solutions were covering some parts of the issues. In this work, we present **SDNSecurity** that provides a diverse information about the security of SDN. Through SDNSecurity, we organize SDN threat vectors that current SDN environments have and address some of the security issues by proposing feasible solutions. Our ultimate goal is to make SDN secure and robust. To achieve it, we will keep discovering newly security challenges and provide open reference solutions that improve the security of SDN. We believe that SDNSecurity would be the starting point to understand and participate the SDN security area.

4. REFERENCES

[1] Bothunter :a network-based botnet diagnosis system. http://www.bothunter.net/.

[2] Onos security: Security-mode onos. https://wiki.onosproject.org/display/ONOS/ONOS+Security+Security-mode+ONOS.

[3] Openflowsec.org. http://www.openflowsec.org.

[4] Sdnseucirty.org. http://www.sdnsecurity.org.

[5] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. In *Usenix Security*, volume 7, pages 1–16, 2007.

[6] M. F. K. S. Phillip Porras, Steven Cheung and V. Yegneswaran. Securing the software-defined network control layer.

[7] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu. A security enforcement kernel for openflow networks. In *Proceedings of the first workshop on Hot topics in software defined networks*, pages 121–126. ACM, 2012.

[8] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson. Fresco: Modular composable security services for software-defined networks. In *NDSS*, 2013.

[9] S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. B. Kang. Rosemary: A robust, secure, and high-performance network operating system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 78–89. ACM, 2014.

[10] S. Shin, V. Yegneswaran, P. Porras, and G. Gu. Avant-guard: Scalable and vigilant switch flow management in software-defined networks. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 413–424. ACM, 2013.