소프트웨어 정의 네트워킹 기술의 보안 위협 및 보안 요구사항에 대한 연구

강용혁*

*극동대학교

A Study of Security Threats and Security Requirements of Software Defined Networking Technology

Yong-Hyeog Kang*

*Far East University

E-mail : yhkang@kdu.ac.kr

요 약

소프트웨어 정의 네트워킹 기술은 네트워크 처리 부분과 제어 부분을 분리하여 중앙집중적이고 강력하게 네트워크를 제어할 수 있다. 하지만 소프트웨어 정의 네트워킹 기술은 강력함과 함께 보안 위협이 크고 영향도 크다. 대부분의 소프트웨어 정의 네트워킹에 대한 보안 연구는 네트워크 취약점을 발견하고 방어하는 데 중점을 두고 있다. 하지만 이러한 기술 자체에 대한 보안 연구는 많지 않다. 본 논문에서는 이러한 네트워킹 기술에서 발생할 수 있는 보안 취약점들을 분석하고 보안도를 높이기 위해 필요한 사항을 제안한다. 가장 큰 위협은 컨트롤러에 대한 서비스 거부 공격 및 보안 위협들이며 컨트롤러와 스위치간 신뢰성 문제도 있으며 설정 정보를 조작하여 오동작하게 하는 공격을 탐지하기 위한 기법도 필요하다.

ABSTRACT

Software defined networking technology allows centralized and powerful network control by separating packet processing and network control. However, powerfulness of software-defined networking technology threats the network itself. Most security researches of software-defined networking focus on discovering and defending network vulnerabilities. But, there is not much security for this technology itself. In this paper, the security vulnerabilities that can occur in this networking technology are analyzed and the security requirements of it are proposed. The biggest threats are the threats to the controller, the reliability problem between the controller and the switch must be solved, and a technique to detect attacks that malfunction by manipulating configuration information are needed.

키워드

소프트웨어 정의 네트워킹, 보안 위협, 보안 요구사항, 공격 탐지

Ⅰ. 서 론

소프트웨어 정의 네트워킹(SDN: Software Defined Networking) 기술은 혁신 기술이며 다양한 응용에 활용되고 있다. 하지만 SDN은 공격자에게 기존 네트워크 공격 목표 외에 SDN 컨트롤러와 가상 하부구조(Infrastrucutre) 등이 추가적인 공격 목표로 노출되어 있다[1]. 또한, 이러한 기술이 공격 받으면 네트워크에 대한 강력한 제어 능력을 갖게 되어 더 위험하다.

소프트웨어 정의 네트워킹 기술에 대한 보안 논문은 주로 이것을 이용한 보안 향상에 대한 논문이 많으며, 자체 기술에 대한 방어도 이것을 이용하여 보안도를 높이는 논문들이 많다[2]. 하지만, 이러한 기술이 공격받으면 이러한 기술을 이용하여 보안도를 높이는 기술은 무용지물이 된다.

본 논문에서는 SDN 기술에 대한 보안 위협과 보안 요구사항을 조사하고 분석한다. 본 논문의

구성은 다음과 같다. 2장에서 관련연구를 기술하고, 3장에서 SDN의 보안 위협과 보안 요구사항을 제시하고, 4장에서 결론 및 향후 연구 과제를 제시한다.

Ⅱ. 관련 연구

SDN 기술에 대한 보안 연구에 대한 조사도 많이 이루어져 있다[3,4]. SDN은 논리적으로 중앙 집중화된 제어를 가지며 개방되어 있으며 스위치를 관리하는 프로토콜로 실제적으로는 Openflow 프로토콜이 사용된다[1]. Openflow 프로토콜에 대한 STRIDE 위협 분석으로 보안 취약점들을 분석한 연구도 있다. Openflow 명세는 TLS를 사용하는 것과 컨트롤러와 스위치간의 상호 인증을 제시하지만, 필수 요구사항이 아니며, 명확한 표준이 제시되지 않아서 대부분의 벤더가 채택하지 않고 있다[2].

SDN의 취약점을 분석하여 악의적인 전파, 플러딩 공격, 핑거프린팅 공격, 서비스 거부 공격(DoS)의 가능성이 제시되었다. 특히, DoS 공격은 컨트롤러에 대한 공격과 플로우 테이블을 통한 DoS 공격이 있다. 상위 계층의 분석을 통해 중앙 집중 제어와 네트워크 프로그래밍 가능성의 위협을 분석하였고 컨트롤러 복제 및 다양화와 응용 수준에서 컨트롤러의 관리 및 제어 기법을 제공하여 해결하는 방안이 제시되었다[2].

Ⅲ. SDN의 보안 위협과 보안 요구사항

본 논문에서 SDN의 보안 위협을 분석한 내용을 토대로 하여 가장 중요한 보안 위협을 정리하면 다음과 같다.

- 컨트롤러 보안 위협
- 컨트롤러와 스위치간 통신 위협
- 컨트롤러 또는 스위치의 비정상 행위

SDN은 컨트롤러에 의한 중앙 집중 제어 기법으로 컨트롤러가 단일 장애점(single point of failure)가 될 수 있다. 이로 인해 컨트롤러에 대한 DoS 공격으로 전체 네트워크를 마비시킬 수 있다. 또한, 컨트롤러에 대한 침입을 통해 네트워크에 대한 악의적인 제어를 할 수 있다.

컨트롤러와 스위치 간 통신은 TLS를 통해 인증 및 무결성을 제시하는 기법이 제시되었지만 대부분의 벤더에서 채택하지 않아서 가짜 컨트롤러 문제, 가짜 스위치를 통해 네트워크에 악의적인 행위를 할 수 있다.

본 논문에서는 다음과 같은 SDN의 보안 요구사항을 제시한다.

- 컨트롤러의 복제와 협력으로 침입 탐지 및 방지
- 컨트롤러와 스위치간의 DTLS 의무화를 통한 상호 인증과 무결성
- 컨트롤러와 스위치의 설정 정보 검증으로 비정상 행위 탐지

첫 번째 요구 사항은 현재 진행 중인 SDN을 이용한 보안 기법과 유사하게 연구하여 수행할 수 있다. 두 번째 요구 사항은 보안 정책적으로 수행해야 하지만, 자원 제약적인 스위치의 특성을 이용하여 UDP를 사용하는 TLS를 적용하는 것이 자원 효율적이다. 세 번째 요구 사항은 응용 계층에서 설정 정보들을 모두 수집하여 종합적으로 분석하여 비정상 행위를 탐지하는 방식으로 수행하면 된다.

Ⅳ. 결론 및 향후 연구과제

본 논문에서는 SDN 자체 기술의 주요한 보안 위협들을 제시하고 보안 위협들을 방지할 수 있는 보안 요구사항을 제시하였다. 또한, 보안 요구사항에 대한 간략한 해결방안을 제시하여 보안 위협들을 완화할 수 있는 방안을 제시하였다. 향후 연구 과제로는 본 논문에서 간략히 제시된 보안 기법들을 연구하여 상세화하는 것이다. 또한, 구체적인 기법을 제시하고 제시된 기법에 대한 성능 분석을 수행하는 것이다.

참고문헌

[1] H. Fei, Network Innovation Through OpenFlow and SDN: Principles and Design, CRC Press, 2014.

[2] S. Scott-Hayward, S. Natarajan, and S. Sezer, A survey of security in software defined networks, IEEE Commun. Surveys & Tutorials, 2015.

[3] M. Sazena, R. Kumar, A recent trends in software defined networking (SDN) security. In Proceedings of the Computing for Sustainable Global Development, 2016.

[4] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, Security in software-defined networking: Threats and countermeasures, Mobile Netw. Appl. 2016.