소프트웨어 정의 네트워킹에서 발생하는 취약점들에 대한 새로운 보안 분류 방법 제시

서민재, 강한이, 신승원

카이스트

ms4060@kaist.ac.kr, haney1357@kaist.ac.kr, claude@kaist.ac.kr

Novel Security Classification for Software Defined Networking

Minjae Seo, Haney Kang, Seungwon Shin

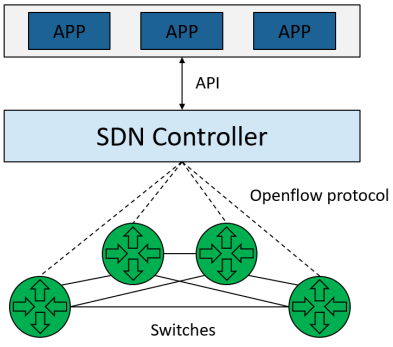
KAIST

요 약

최근 데이터 센터, 클라우드 네트워크 그리고 광역 네트워크 (Wide Area Network, WAN)의 사용이 증가함에 따라 비약적으로 증가하는 트래픽에 대한 유연한 관리를 위해 소프트웨어 정의 네트워킹 (Software Defined Networking, SDN)이 제시되었다. 하지만 계속해서 소프트웨어 정의 네트워킹의 보안에 대한 취약점이 발견되었고, 기존의 보안 3요소 기밀성 (Confidentiality), 무결성 (Integrity), 가용성 (Availability)으로는 최근의 보안 이슈들을 전부 포함할 수 없었다. 따라서 소프트웨어 정의 네트워킹의 보안에 대한 새로운 분류 방법이 야기되었다. 본 논문에서는, 기존의 보안 3요소뿐만 아니라 새로운 2가지 요소인 인증 (Authentication)과 부인방지 (Non-repudiation)를 집합하여 새로운 보안 분류 방법을 제시한다. 따라서 우리는 새로운 보안 분류 방법으로 최근 떠오르는 소프트웨어 정의 네트워킹 취약점들을 포함할 수 있는 방법론을 제시하도록 한다.

Ⅰ. 서 론

최근 급부상하는 서비스들에 대한 유동적인 트래픽의 증가 문제와 네트워크 장비 관리의 유연함을 위한 해결 방법 중 하나로 소프트웨어 정의 네트워킹 (Software Defined Networking, SDN)이 제시되었다. SDN은 기존의 네트워크 장비에서 라우팅 (Routing)을 담당하던 제어 평면 (Control Plane)과 포워딩 (Forwarding)을 담당하던 데이터 평면 (Data Plane)을 분리한 컨트롤러 중앙 집권형 구조로써, 사용자에게 여러 가지 프로그래머블 (Programmable)한 환경을 제공한다. 따라서 오늘날 데이터 센터, 클라우드 네트워크 그리고 광역 네트워크에 적극적으로 활용되고 있다. 논리적 중앙 집권형 구조인 SDN 컨트롤러는 SDN 스위치들과 통신을 하기 위해 라우팅 경로와 같은 메시지들을 사우스바운드 프로토콜 (South Bound Protocol)인 오픈플로우 프로토콜 (Openflow Protocol)을 이용하여, 컨트롤 채널을 통해 SDN 스위치에 전달한다. SDN의 많은 구성 요소들 중 Control Plane은 SDN의 두뇌 역할로써 SDN의 환경과 구성 요소들을 제어 및 관리하고, 사용자들에게 보다 편리한 서비스들을 유연하게 효과적으로 제공한다 [1]. 하지만 제어 평면은 아직까지 보안에 취약하고, SDN의 핵심 부분이기 때문에 많은 연구자들이 SDN 제어 평면의 보안과 취약점에 초점을 두고 연구를 진행하고 있다.



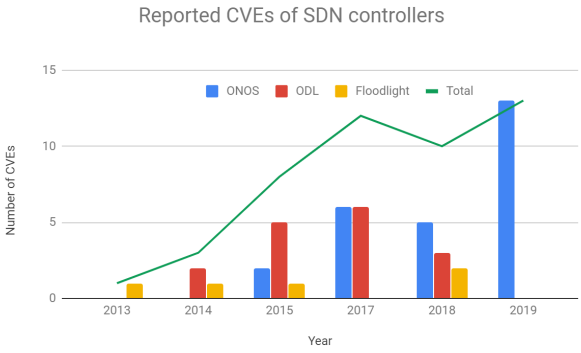
<그림 1> SDN 제어 평면과 데이터 평면 구조

이러한 연구가 진행될수록, SDN의 많은 취약점들이 밝혀졌고 최근에는 많은 연구자들이 공통 취약성 및 노출 (Common Vulnerabilities and Exposures, CVE)시스템에 취약점들을 등록하고 있다. CVE는 공개적으로 알려진 컴퓨터 보안 결함 목록이다. CVE는 IT 전문가들이 이러한 취약점에 우선 순위를 지정하고 해결하기 위해 협력하여 컴퓨터 시스템을 보다 안전하게 관리하도록 지원한다.

최근까지도 많은 SDN의 취약점들이 CVE 시스템 등록과 함께 밝혀지면서 기존의 보안 3요소로는 이러한 취약점들을 구성할 수 없게 되었고 새로운 보안 분류 방법이 강구되었다. 따라서 기존보다 더 포괄적인 분류를 위해 새로운 2가지 요소인 인증 (Authentication)과 부인방지 (Non-repudiation)를 포함하여 기존보다 포괄적인 보안 분류 방법을 제시한다.

Ⅱ. 본론

본론에서는 최근 CVE 시스템에 등록된 여러 컨퍼런스 논문들을 바탕으로 현재 SDN 보안의 취약성을 분석하고 앞서 말한 보안 5가지 요소를 바탕으로 새로운 보안 분류 방법을 제시한다.



<그림 2> SDN 컨트롤러(ONOS, ODL, Floodlight)의 CVE 증가 추세

Security Category	Attack	CVE ID	Reference
Confidentiality	AT-4-firewall	CVE-2017-1000406	AIM-SDN (CCS '18)[2]
	AT-6	CVE-2018-1078	AIM-SDN (CCS '18)[2]
	DC-7	CVE-2018-1000614	SVHunter (S&P '20)[3]
	DC-8	CVE-2018-1000616	SVHunter (S&P '20)[3]
Integrity	AT-2-general impact	CVE-2017-1000411	AIM-SDN (CCS '18)[2]
	AT—2-controller core	CVE-2017-1000406	AIM-SDN (CCS '18)[2]
	AT-4-firewall	CVE-2017-1000406	AIM-SDN (CCS '18)[2]
	DC-10	CVE-2018-1999020	SVHunter (S&P '20)[3]
	DC-1, 2	CVE-2017-1000078	SVHunter (S&P '20)[3]
Availability	AT-2-general impact	CVE-2017-1000411	AIM-SDN (CCS '18)[2]
	AT-2-controller core	CVE-2017-1000406	AIM-SDN (CCS '18)[2]
Authentication	DC-9	CVE-2018-1000615	SVHunter (S&P '20)[3]
	Data Plane Access Control Bypass	CVE-2019-11189	EventScope (NDSS '20)[4]
Non-repudiation	virtualbng	CVE-2019-16298	EventScope (NDSS '20)[4]

표 1. 보안 5요소와 새로운 SDN 보안 분류 방법

2.1 새로운 SDN 보안 분류 방법

<그림 2>와 같이 ONOS, ODL, Floodlight과 같은 SDN 컨트롤러 내에서 다양한 취약점과 더불어 CVE 등록이 완료되었고, 기존의 CIA 보안 3요소는 충분하게 새로운 취약점들을 포함시킬 수 없었다. 따라서 위의 표 1과 같이 CIA 보안 3요소에서 인증 (Authentication)과 부인방지 (Non-repudiation)이 추가되었다. AIM_SDN (CCS '18) [2]에서는 여러 가지 공격 시나리오 중 방화벽 (firewall), 접근제어목록 (Access Control List, ACL)일 때 Confidentiality 요소에 포함되었고, general impact, controller core 그리고 firewall 상황일 때 Integrity 요소에 포함되었다. 마지막으로 general impact, controller core 상황일 때 Availability 요소에 포함되었다.

또한 SVHunter (S&P '20) [3]에서는 Data dependency Creation 공격 7번과 8번이 Confidentiality에 포함되었고, 공격 1번과 2번 그리고 10번이 Integrity에 포함되었다. 마지막으로 공격 9번이 Authentication 요소에 포함되었다.

마지막으로 EventScope (NDSS '20) [4]에서는 여러 가지 공격 시나리오 중 데이터 평면 우회 기법이 Authentication 요소에 포함되었고, 마지막으로 virtualbng를 이용한 공격 기법이 Non-repudiaton 요소에 포함되었다.

III. 결론

최근 계속해서 여러 SDN 보안 문제들이 발견되었고, 연구자들은 발견한 문제들을 바탕으로 CVE 시스템에 그 취약점들을 등록하였다. 하지만 기존의 보안 3요소만을 이용하여 최근 발견된 SDN의 취약점을 분류하는 데는 큰 한계가 있었고 새로운 방법의 SDN 보안 분류 방법을 제시하였다. 이러한 방법으로 여러 SDN 보안 문제들을 효율적으로 분류할 수 있었고, 현재 발견되고 있는 SDN 보안 문제들을 한눈에 볼 수 있었다. 악의가 있는 송신자가 인증된 사용자로 가장하여 데이터 전송을 하는 위험이 있는 Authentication 요소를 추가하였고, 송신자가 정보를 보낸 후, 보낸 사실을 부인하지 못하게 하는 장치의 역할을 하는 Non-repudiation 요소를 추가하여, 최근 지속적으로 발견되어지는 SDN 보안 취약성의 트렌드를 한눈에 볼 수 있었다는 점은 이번 논문의 큰 강점이라고 생각한다. 그러나 아직까지 계속해서 새로운 취약점들이 발견되고 있기 때문에 향후 더욱 넓은 범위의 취약점들을 포괄 할 수 있는 SDN 보안 분류 방법을 연구 할 것이다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크 기술 특화연구센터 사업의 일환으로 수행되었습니다.(UD190033ED)

참 고 문 헌

[1] Jain, S, et al. B4: Experience with a globally-deployed software defined wan. ACM SIGCOMM Computer Communication Review. 2013. p. 3-14.

[2] Dixit, Vaibhav, et al. "AIM-SDN: Attacking Information Mismanagement in SDN-datastores", Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communication Security (CCS'18), January 2018.

[3] Xiao, Feng, et al. "Unexpected Data Dependency Creation and Chaining: A New Attack to SDN", Symposium on Security and Privacy IEEE S&P 2020.

[4] Ujcich, Benjamin, et al. "Automated Discovery of Cross-Plane Event-Based Vulnerabilities in Software-Defined Networking", In: Network and Distributed Systems Security (NDSS), 2020.

[5] Cao, Jiahao, et al. "The CrossPath Attack: Disrupting the SDN Control Channel via Shared Links", 28th USENIX Security Symposium 2019.