오픈소스 IDS/IPS Suricata를 활용한 SDN 보안 강화 연구

남기호, 한근희, 김기천
건국대학교 컴퓨터정보통신공학과
e-mail:namgeo@konkuk.ac.kr

A Study on SDN security enhancement using open source IDS / IPS Suricata

Kiho Nam, Keun-Hee Han, Keecheon Kim
Dept of Computer Science & Engineering,, Konkuk University

요 약

소프트웨어 정의 네트워크(Software Defined Network)는 기존의 네트워크 벤더 중심의 폐쇄적인 네트워크 환경을 추상화를 통해 단순화하여 프로그래밍이 가능한 유연한 소프트웨어 기반의 중앙 집중적인 관리 환경으로 전환해 주는 차세대 네트워킹 기술이다. 이러한 장점을 활용해 기존 네트워크보다 일부 보안 문제에 강점을 가질 수는 있으나 기존 네트워크의 보안 문제와 취약점들 대부분이 그대로 존재하고 이를 대상으로 한 다양한 공격이 발생하고 있다. 본 논문에서는 이러한 보안 문제에 대하여 SDN 기술을 활용하여 어떻게 네트워크 보안 기능을 구현할 수 있는지 확인하고, 기존 오픈소스 IDS/IPS 소프트웨어 Suricata와의 연동을 통해 SDN의 보안기능을 강화하는 구조를 제안한다.

1. 서론

최근 네트워크 분야에서 이슈인 소프트웨어 정의 네트워크(Software Defined Network)는 기존의 네트워크 하드웨어 벤더 중심의 고정된 하드웨어와 소프트웨어 기반의 폐쇄적인 네트워크 환경을 네트워크 추상화를 통해 단순화하여 프로그래밍이 가능한 유연한 소프트웨어 기반의 중앙 집중적인 관리 환경으로 전환해 주는 차세대 네트워킹 기술이다. 네트워크 관리자는 이러한 기능을 이용해 소프트웨어적으로 제어 플레인을 프로그래밍 해 데이터 플레인에서 이루어지는 통신기능을 네트워크의 관리목적에 맞게 다양하게 제어할 수 있으므로 일반적인 네트워크 제어와 경로설정이나 복잡한 운용관리 기능도 쉽게 처리하고 Load Balancing, QoS 같은 고급 기능도 쉽게 구현할 수 있다. SDN 환경의 이런 유연한 기술과 기능들은 많은 부분에서 네트워크 보안을 위해 사용이 가능하다. 또한 소프트웨어적으로 제어가 가능한 유연한 SDN 환경 특성으로 기존의 다양한 오픈소스 소프트웨어 보안 솔루션과 소프트웨어를 구조적으로 연동하면 그 기능을 더욱 강력하게 확장하여 SDN의 보안성을 강화할 수 있을 것이다. 그러나 이러한 SDN의 기술을 네트워크 보안의 관점에서 접근하여 분석/구현하거나 기존의 오픈소스 보안 솔루션과 연동하여 보안성을 강화하려는 사례는 많지가 않다.

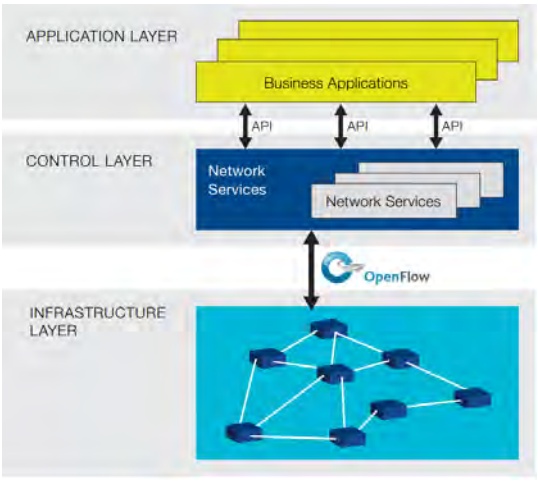
본 논문은 SDN 환경에서 SDN 기술을 활용하여 어떻게 네트워크 보안 기능을 구현할 수 있는지 확인하고, 기존 Open Source IDS/IPS 소프트웨어 보안 솔루션 Suricata와 소프트웨어적으로 연동하는 구조를 통하여 보안성을 강화하는 방법을 알아보고 SDN의 보안기능을 강화하는 구조를 제안하고자 한다.

2. 연구 배경 및 관련 연구

가. SDN

소프트웨어 정의 네트워크(Software Defined Network)는 SDN은 고정된 하드웨어와 소프트웨어 중심의 폐쇄적인 네트워크를 추상화하여 데이터 플레인, 제어 플레인, 애플리케이션 플레인의 3개 플레인 구조로 모델링한다. 데이터 플레인은 SDN의 특정 인터페이스를 통해 제어를 받는 계층으로서, 데이터 흐름의 전송을 담당한다. 제어 플레인은 데이터의 흐름을 제어하는 계층으로 애플리케이션과 네트워크 서비스를 통하여 데이터 흐름을 라우팅 할지, 전달할지, 거절할지를 결정한다. 또한 데이터 플레인의 동작들을 API형태로 애플리케이션 계층에 전달한다. 끝으로 애플리케이션 플레인은 제어 플레인에서 제공한 API들을 이용해 네트워크의 다양한 기능을 수행한다. 그리고 각각의 플레인 사이에는 이들을 연결하는 사우스바운드 인터페이스와 노스바운드 인터페이스로 불리는 개방형 인터페이스를 정의해 각각 디바이스/자원 추상화와 제어 추상화, 서비스 추상화를 지원한다. 그림1은 SDN의 개념 구조

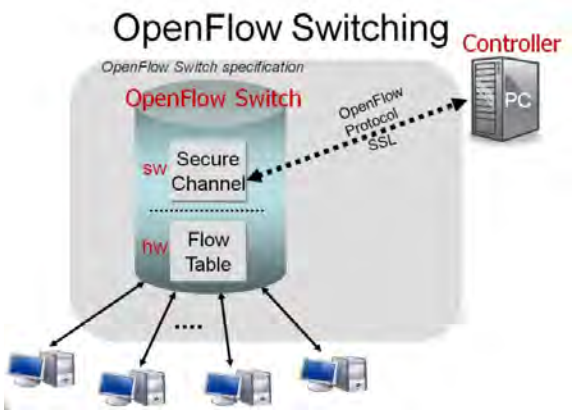
[1]를 간단하게 나타내 주는 그림이다.



(그림 1) SDN Architecture

나. OpenFlow

OpenFlow는 SDN 개념을 구현하기 위해서 스탠포드 대학을 중심으로 하는 프로젝트[2]로 시작되었고, 현재는 다수의 벤더들이 ONF(Open Networking Foundation)에 참여하여 연구를 진행하고 있다.



(그림 2) OpenFlow Switching

OpenFlow[3]는 콘트롤러와 네트워크 장치간의 사우스 바운드 인터페이스 규격으로, 이를 구현한 오픈 소스 소프트웨어로 콘트롤러인 FloodLight[4]와 스위치인 Open vSwitch[5]가 제공되고 있다.

3. 제안하는 SDN 보안 방안

기존 네트워크 환경의 보안에서 방화벽과 네트워크 스캔, 비정상 트래픽 탐지, 침입 탐지 및 차단 기술은 필수 불가결한 요소이고 하드웨어와 비용이 많이 요구되는 주요한 요소다. 이러한 내용은 SDN 환경도 크게 다르지 않다. 여기서는 일반적인 보안환경에서 중요시하는 방화벽과 네트워크 스캔, 비정상 트래픽 탐지, 침입 탐지 및 차단 기술을 별도의 하드웨어의 추가 없이 SDN의 OpenFlow 기술을 기본적으로 사용하고[6] 필요에 따라 오픈소스 IDS/IPS인 Suricata를 연동하여 OpenFlow 차단 자동화 프로그램을 구현하는 방법으로 SDN 환경의 보안성을 강화하는 방안을 제안한다. 그 내용은 아래 <표1>의 SDN 보안 구현 시 필요사항을 참고하도록 한다.

	SDN (OpenFlow)	Suricata IDS/IPS	자동차단 프로그램	미러링
방화벽	가능	불필요	불필요	불필요
스캔탐지	가능	부가기능	불필요	부가기능
비정상 트래픽탐지	가능	부가기능	불필요	부가기능
침입탐지 (IDS)	불가능	필요	불필요	필요
침입차단 (IPS)	불가능	필요	필요	필요

<표 1> SDN 보안 구현 시 필요 사항

가. SDN OpenFlow를 활용한 보안 구현

1) 방화벽 구현

기존 네트워크 장비들과는 별개의 장비로 구현되었던 방화벽을 SDN에서는 필요한 보안 정책을 SDN의 응용 프로그램에서 지원하고 OpenFlow 기능 중 패킷 포워드와 드랍 기능을 이용하여 이를 OpenFlow를 지원하는 네트워크 장비들로 전달하여 방화벽 기능을 매우 쉽게 구현할 수 있다. 이는 OpenFlow 기능을 지원하는 네트워크 장비들이들이 모두 방화벽 기능을 할 수 있다는 것이며 이를 이용하면 분산방화벽 기능도 어렵지 않게 구현할 수 있다.

2) 네트워크 스캔 탐지

네트워크 스캔중에서, Threshold Random Walk[7] 탐지 방법은 TCP 연결의 성공과 실패 여부를 모니터링 하여 통계적으로 성공보다 실패가 많이 발생한 경우 이를 스캔 공격으로 간주하는 탐지 방식이다. SDN 기술에서는 각 TCP 세션의 성공과 실패 여부를 알아내야하기 때문에 TCP 세션을 처음 시작하는 패킷들을 구분할 수 있도록 각 네트워크 플로우를 세션 별로 감시할 수 있도록 플로우 룰을 제어하는 것으로 구현이 가능하다. 그리고 대부분의 네트워크 스캔 공격이 TCP 프로토콜을 기반으로 하지만 ICMP 나 UDP 등과 같은 프로토콜을 이용하여 네트워크 스캔을 시도하는 경우도 있다. 이들 프로토콜은 세션 정보가 없기 때문에 서버로 전달되는 패킷의 양 등을 분석하여 스캔을 탐지한다.

3) 비정상 트래픽 탐지

네트워크 비정상 트래픽 탐지 시스템에서 이용되는 네트워크 정보들은 첫째, TCP 프로토콜의 세션 정보(각 TCP 세션의 성공, 실패, 특정 사용자의 특정 네트워크 상대 TCP 세션 시도 횟수와 성공, 실패 횟수 등의 정보), 둘째로 특정 사용자의 초당 전달 된 패킷 수(PPS)나 바이트 수(BPS), 셋째, 트래픽이 전달 될 때 BPS와 PPS의 변

화의 양 등의 정보들이 가장 일반적이다. 이 정보들을 OpenFlow를 이용하여 첫째는 스캔 탐지와 같이 TCP 세션을 모니터링하고 둘째는 BPS와 PPS를 구하기 위해 네트워크 장비들에게 주기적으로 거쳐 간 네트워크 패킷 수와 바이트 수를 요청하고, 셋째는 이 정보들을 응용 프로그램 내에 있는 별도의 자료구조에 저장하면 얻어낼 수 있다. 추후 이 정보들을 바탕으로 다양한 알고리즘을 이용해 비정상 트래픽을 탐지하고 이를 기반으로 관리자에게 보고하거나 혹은 직접 관련된 비정상 트래픽을 차단하거나 자동 차단 시스템과 연동하도록 구성할 수 있다.

나. SDN과 Suricata의 연동을 통한 보안 강화

1) Suricata 연동을 통한 침입 탐지 및 자동 차단

침입 탐지 시스템은 패킷 내용을 분석해 공격 패턴이 있는지 확인하기 때문에 데이터 플레인에 있는 패킷 내용을 SDN 응용 프로그램으로 전달해야 한다. 하지만 현재 OpenFlow에서는 패킷 내용을 Controller로 전달하는 방법이 쉽지 않으므로 IDS 구현이 단순하지 만은 않다. 만약 장비의 플로우 룰에 매치되는 패킷이 들어오면 네트워크 장비는 패킷을 Controller로 전달하지 않고 바로 룰에 따라서 처리하므로 패킷 내용을 Controller로 전달하지 못하는 경우가 발생하므로 이를 해결하기 위해서는 미러링 방식을 이용해야 한다. 이는 SDN 기술을 이용 하지 않는 기존 네트워크 침입 탐지 시스템에서도 많이 이용 하는 기술로 미러링은 네트워크 장비를 거쳐 가는 모든 패킷을 복사하여 특정 서버로 전달하는 방식을 말한다. 이때 네트워크 침입 탐지 기능을 하는 Open Source IDS/IPS Suricata를 특정 서버에 위치시켜, 미러링된 내용들을 분석하여 공격과 관련한 패턴이 있는지 확인하고 만약 있다면 이를 공격으로 판단하도록 한다. 그리고 이때 Suricata의 탐지 내역을 모니터링하여 네트워크 장비로 OpenFlow 명령을 보내 SDN의 방화벽 기능을 연동하여 차단할 수 있는 프로그램 작성을 통해 자연스럽게 네트워크 침입 차단 시스템을 구현할 수 있다. 이를 네트워크 구조로 표현하면 아래 (그림 3)의 구조와 같다.

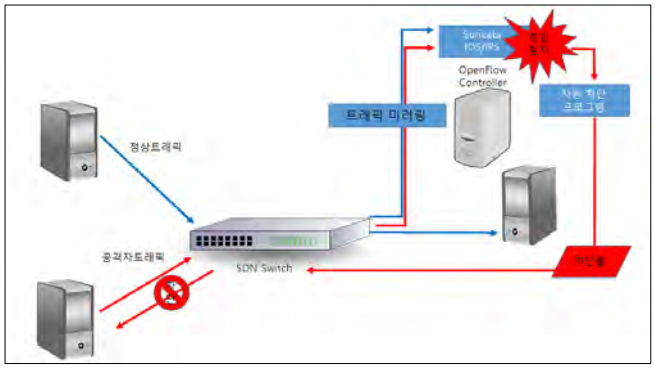


그림 3 SDN과 Suricata의 연동 보안 구조

4. 결론

본 논문에서는 SDN의 OpenFlow를 활용하여 기존 네트워크 환경의 방화벽과 네트워크 스캔과 비정상 트래픽 탐지를 구현하는 방법을 알아보았고 현재 OpenFlow에서는 패킷 내용을 Controller로 전달하는 방법이 쉽지 않기 때문에 구현이 힘든 네트워크 침입 탐지 기능을 미러링을 통한 Suricata 연동으로 해결하고 탐지된 내역을 모니터링하여 OpenFlow 명령으로 자동차단하는 프로그램을 통하여 침입 탐지 및 자동 차단을 통한 침입 차단 시스템 구조를 구현할 수 있다.

ACKNOWLEDGEMENT

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00279, 안전한 IoT 전용망 구축을 위한 LPWAN 침해 방지 기술 개발)

참고문헌

[1] ONF, "Software-Defined Networking: The New Norm for Networks," ONF White Paper(https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[2] J. Pettit, J. Gross, B. Pfaff, and M. Casado, "Virtual Switching in an Era of Advanced Edges," Proc. of the 2nd Workshop on Data Center-Converged and Virtual Ethernet

[3] ONF, "OpenFlow Switch Specification",(https://www.opennetworking.org/software-defined-standards/specifications/)

[4] Floodlight Project, http://www.projectfloodlight.org

[5] Open vSwitch, http://openswitch.org

[6] 신승원, 송용주, "SDN 기술을 이용한 네트워크 보안 기술 설계 및 구현 방법", Telecommunications Review, vol.23, no.5, pp. 627-640 (14 pages), 2013.

[7] SCHECHTER, Stuart E.; JUNG, Jaeyeon; BERGER, Arthur W. Fast detection of scanning worm infections. In: Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2004. p. 59-81.