# 소프트웨어 정의 네트워크 기반 위협 대응 프레임워크

이승현, 신승원
한국과학기술원 전산학부 네트워크 및 시스템 보안 연구실
e-mail:coksm1963, claude@kaist.ac.kr

# Threat Response Framework based on Software Defined Network

Seunghyeon Lee, Seungwon Shin
KAIST, School of Computing, NSS laboratory

요 약

소프트웨어 정의 네트워크(SDN)의 등장은 학계와 산업계에 큰 영향을 주었다. SDN은 물리적인 장치를 변경하지 않고 네트워크 관리자의 의도대로 대상 네트워크를 관리 할 수 있기 때문에, 능동적이고 유연한 관리환경을 제공한다. 보안측면에서 SDN 기반의 네트워크는 다양한 공격을 탐지하는 데 유용하게 쓰인다. 하지만 대부분의 SDN을 이용한 보안 연구는 네트워크에만 집중되어 있고, 호스트를 고려하지 않고 있다. 이와 더불어 SDN 기반의 보안 애플리케이션을 제작하기 위해서는, SDN을 운용하는 컨트롤러와 다양한 지식이 요구된다. 본 연구에서는 SDN 기반의 호스트와 네트워크를 모두 고려하는 보안 애플리케이션 제작의 어려움을 해결하기 위해, 소프트웨어 정의 네트워크 기반 위협 대응 프레임워크를 제안한다.

## 1. 서론

SDN [1] 기반의 네트워크는 물리적으로 정해진 기능만 하는 기존 네트워크와는 달리, 프로그래밍이 가능한 환경을 통하여 물리적인 장치를 바꾸지 않고 다양한 기능을 적용할 수 있는 환경을 제공해 준다. 보안관점에서의 SDN은 동적으로 변하고 빠른 대응이 필요한 다양한 보안 위협에서 현존하는 문제를 해결할 수 있는 기회를 제공한다. 이러한 이점에도 불구하고 현대 공격은 네트워크와 시스템 각각의 측면만을 고려한 공격이 아니므로 프로그래밍이 가능한 네트워크만으로는 모든 위협을 방어할 수 있는 기반시설을 갖추고 위협에 대응하기에는 한계점을 가진다.

위협 대응을 한쪽 측면에서만 했던 기존 연구들과는 다르게, 본 연구에서 제안하는 SDN 기반의 위협 대응 프레임워크는 SDN환경에서 호스트와 네트워크의 협업을 통하여 효과적으로 위협을 탐지하고 대응할 수 있는 기반 시설 및 개발 환경을 제공해 준다. 개발자는 위협 대응 프레임워크를 통하여 위협에 대비한 호스트와 네트워크의 협업 시스템을 사전지식이나 인프라 구축 없이 개발할 수 있다. 본 연구에서 제안한 프레임워크가 가지는 이점은 다음과 같다.

- SDN 환경을 사용하기 위해 필수적으로 알아야 할 네트워크 OS에 대한 지식 없이 시스템을 구축
- 네트워크와 호스트를 모두 고려한 협업 시스템을 통하여 양 영역간의 정보전달의 부재 해결 및 효과적인 대응
- 개발자가 원하는 애플리케이션을 위협 대응 프레임워크에서 제공하는 스크립트 언어를 통하여 구축
- 호스트와 연계를 위해 네트워크 OS와 호스트 간에 필요한 환경 구축 없이, 프레임워크에 필요한 모듈 개발 가능

본 논문의 구성은 다음과 같다. 2장에서는 위협 대응에 대한 문제점을 다루고, 해당 문제를 해결하기 위하여 3장에서 위협 대응 프레임워크의 디자인을 제안한다. 4장에서는 본 연구에서 제안한 위협 대응 프레임워크를 이용한 보안 애플리케이션의 동작 예제에 관하여 기술한다. 끝으로 5장은 결론으로 구성되어 있다.

## 2. 위협 대응에 대한 문제점

SDN은 프로그래밍이 가능한 네트워크를 제공하므로 보안 위협에 능동적이고 즉각적으로 대응할 수 있는 장점을 가진다. 하지만 SDN기반의 네트워크를 구성하기 위해서는, SDN기반의 네트워크를 제어하는 컨트롤러 및 스위치에 대한 다양한 지식을 습득해야 한다는 문제가 있다. 보안 관리자 입장에서는 SDN 기반의 네트워크가 위협 대응에 다양한 기회를 마련해 주지만, 보안 자체에 집중하지 못하고 SDN 기반의 제어 자체에 많은 시간소모를 할 수밖에 없는 것이 현재 SDN 기반 위협대응의 문제점이다.

또한, 궁극적인 위협 탐지 및 대응에 있어 VMI 연구영역의 메모리 시맨틱 갭 문제와 유사하게 호스트와 네트워크의 정보전달 부재로 현존하는 위협에 대한 정확한 판단 및 대응을 못 하는 문제가 있다. 예를 들어 DDoS 공격을 탐

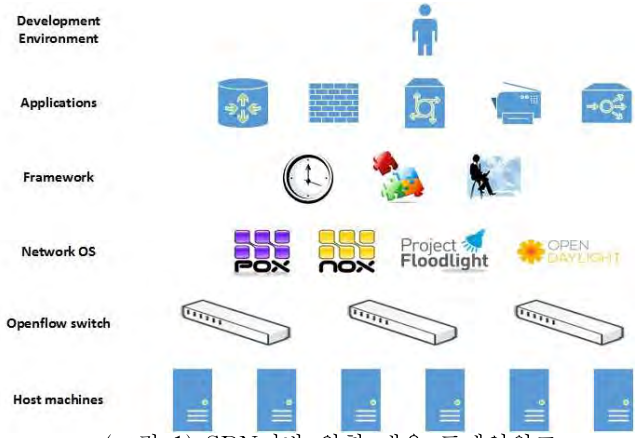
지하기 위한 네트워크 단의 트래픽 감지를 통하여 DDoS를 탐지한 경우, 네트워크 안에 있는 호스트들에 대한 전후사정을 알 수 있기 때문에 해당 사이트에 대한 트래픽 증가가 정상적인 사용자의 일반적인 접근인지 아닌지 구분할 수 있는 구체적인 증거가 없다.

Fresco [4]는 SDN 기반의 보안 애플리케이션을 쉽게 만들 수 있도록 와주는 대표 프레임워크지만 호스트를 고려하는 보안 애플리케이션을 만들 수 없다. 이처럼 현존하는 협업 프레임 워크의 부재를 해결 하기 위해 본 연구에서는 호스트와 네트워크를 모두 고려하고, SDN 기반의 보안 애플리케이션을 쉽게 만들 수 있도록 도와주는 위협 대응 프레임워크를 제안한다.

## 3. SDN 기반 위협 대응 프레임워크

2절에서 언급한 문제점을 해결하기 위하여 본 연구에서는 SDN 기반의 위협 대응 프레임워크를 제안한다. 본 연구에서 제안하는 위협 대응 프레임워크는 개발자로 하여금 쉽게 자신이 원하는 협업 애플리케이션을 제작할 수 있도록 도와준다. 협업 시스템을 쉽게 구축할 수 있도록 도와주는 위협 대응 프레임워크의 주된 기능은 아래와 같다.

- 협업 시스템을 구축하기 위한 인프라 제공
- 협업 시스템을 통한 공격 탐지 및 대응 기능 제공
- 제공되는 모듈을 이용하여 원하는 협업 애플리케이션을 만들 수 있는 환경 제공
- 부수적으로 필요한 다양한 구현이슈를 없애 주고, 간단한 스크립트를 통하여 원하는 애플리케이션을 제작할 수 있는 환경 제공



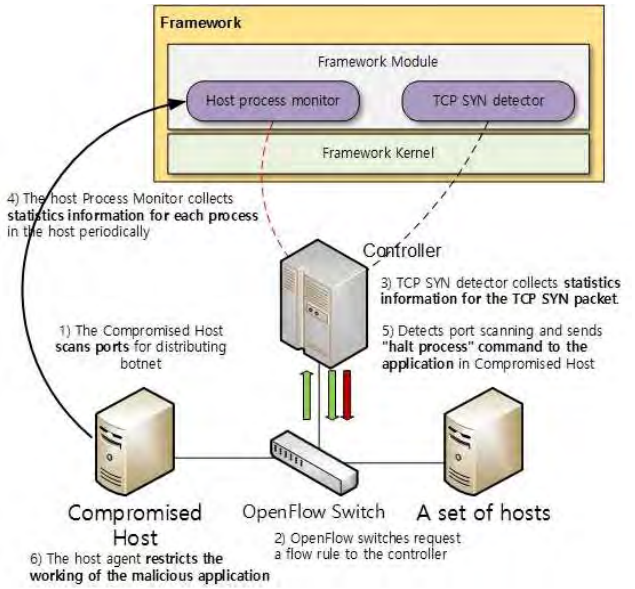

(그림 1) SDN기반 위협 대응 프레임워크

SDN 기반의 위협 대응 프레임워크는 SDN 기반의 네트워크에서 동작한다. 그림1은 전체적인 위협 대응 프레임워크의 논리 구조에 대하여 나타내고 있다. 위협 대응 프레임워크는 네트워크를 제어하기 위하여 네트워크 OS위에 동작하게 되고, 각각의 호스트 머신에 프레임워크 에이전트를 통해 호스트를 제어한다. 네트워크 OS 위에는 실제 프레임워크의 코어부분인 프레임워크단이 존재하고 해당 프레임워크 단에서는 협업을 위한 보안 애플리케이션 제작에 필요한 다양한 모듈을 제공한다. 협업 프레임워크에서 제공하는 다양한 모듈 및 개발환경을 이용하여 간략한 스크립트 언어를 통하여 보안 애플리케이션을 작성하고 위협 대응 프레임워크상에 자신이 원하는 협업 보안 애플리케이션을 동작시킬 수 있다.

위협 대응 프레임워크의 프로토타입은 네트워크 OS 중 안전성이 높고 확장성이 용이한 OpenDayLight[2] 네트워크 OS위에 구현되어 있다. 네트워크 OS위에 동작하는 위협 대응 프레임워크의 코어 부분에서는 전체 네트워크를 제어하고, 호스트에서 동작하는 위협 대응 프레임워크 에이전트는 호스트에서 다양한 정보를 모으고 코어와 통신을 하여 위협 탐지 및 대응을 하는 역할을 한다.

## 4. 포트스캐닝 공격 탐지 및 대응

본 절에서는 협업 대응 프레임워크를 이용하여 포트스캐닝 공격을 탐지하고, 공격에 대한 효과적인 대응에 관한 예제를 다룬다. 포트 스캐닝 공격은 다양한 공격에서 정보수집을 위한 공격단계로 쓰인다. 또한, 취약점을 찾아 봇을 확신시키는 봇넷 시스템에도 쓰이게 된다. 본 절에서는 봇 확산을 위한 포트스캐닝 공격을 협업 대응 시스템을 통하여 방어하는 프로세스에 대해 다루고 협업 대응 시스템을 통한 애플리케이션이 가지는 이점에 대하여 서술한다.




(그림 2) 위협 대응 프레임워크를 이용한 포트스캐닝 공격 탐지 및 대응

그림 2는 봇에 감염된 호스트 (Compromised Host)가 포트스캐닝을 시작했을 때, 위협 대응 프레임워크가 해당 공격을 감지하고 감염된 호스트에서 포트스캐닝 공격을 수행한 프로세스를 종료시키는 예제를 다루고 있다. 먼저 봇에 감염된 호스트 (Compromised Host)가 봇 확산을 위하여 포트스캐닝 수행하면, SDN 기반의 네트워크에서 동작하는 OpenFlow 스위치 [3]는 해당 정보를 네트워크 OS에게

보내게 된다. 또한, 호스트에서 동작하는 위협 대응 프레임워크 에이전트는 감염된 호스트에서 발생하는 네트워크 트레픽 정보를 위협 대응 프레임워크로 전달해 주게 된다. 위협 대응 프레임워크에서 제공하는 호스트 프로세스 모듈과, TCP 감지 모듈이 네트워크 OS와 호스트에서 제공하는 네트워크 사용 정보를 분석하여 포트스캐닝 공격이 이루어지고 있는지 판단한다. 그 후 포트스캐닝 공격이 이루어졌다고 판단이 되면 위협 대응 프레임워크 위에서 동작하는 보안 애플리케이션은 해당 공격에 대한 대응으로 감염된 호스트에서 포트스캐닝 공격을 수행하는 프로세스를 종료한다.

## 5. 결론

환경에 따라 유동적으로 동적으로 대응할 수 있는 SDN 기반의 네트워크는 기존 네트워크 환경에서 할 수 없었던 많은 일을 가능하게 하였다. 하지만 상대적으로 네트워크 관리에 용이한 SDN 환경이지만 원하는 보안 애플리케이션 만들기엔 다양한 지식이 필요하다. 또한, 유동적이고 유연한 환경을 제공하는 SDN 기반의 네트워크라도, 호스트와 네트워크의 협업을 통한 위협 탐지 및 대응 시스템을 구축하기에는 기반시설 확충 등 다양한 문제점들이 존재한다.

본 연구에서 제안한 위협 대응 프레임워크는 호스트와 네트워크의 협업을 통하여 관리자가 쉽게 원하는 애플리케이션을 제작할 수 있는 환경을 제공해 준다. 호스트와 네트워크의 협업을 통한 공격 대응 및 탐지 시스템 구축에 있어 개발자는 사전지식, 프로그래밍 노력, 구현 노력 등 인적자원이 필요한 다양한 측면에서 이점을 얻을 수 있다. 본 프레임워크를 통하여 기존 연구에서 수행하기 힘들었던 호스트와 네트워크 기반의 시스템을 쉽게 구축함으로서, 본 연구에서 제안한 프레임워크가 협업 위협 대응 시스템의 기반 연구로 자리매김 할 수 있다.

## 참고문헌

[1] McKeown, Nick, et al. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38.2 (2008): 69-74.

[2] Linux Foundation. OpenDaylight. http://www.opendaylight.org/

[3] Openflow, http://archive.openflow.org/wp/learnmore/

[4] Shin, Seungwon, et al. "FRESCO: Modular Composable Security Services for Software-Defined Networks." NDSS. 2013.