토폴로지 스캐닝 무력화를 위한 SDN 기반 거짓 IP 주소 응답 기법

김진우, 신승원
한국과학기술원

jinwoo.kim@kaist.ac.kr, claude@kaist.ac.kr

A Method for Neutralizing Topology Scanning using SDN-based Fake IP Address Reply

Jinwoo Kim, Seungwon Shin
KAIST

요 약

최근 네트워크 보안 연구자들은 공격자들이 다양한 형태의 토폴로지 스캐닝(Topology Scanning) 기법을 사용하여 네트워크 토폴로지 내의 취약한 병목 지점(Bottleneck point)을 찾고 이를 공격할 수 있는 가능성을 제시하였다. 본 논문에서는 이러한 형태의 공격을 방어하기 위해 SDN 기반 거짓 IP 주소 응답 기법을 제안한다. SDN 환경에서는 중앙집중화된 SDN 컨트롤러가 네트워크의 모든 토폴로지 스캐닝 패킷을 탐지하고 스위치가 임의의 거짓 IP 주소를 가지는 패킷을 전송하도록 할 수 있다. 본 논문은 SDN 의 표준 프로토콜인 OpenFlow 를 활용하여 이러한 기술을 구현하는 방법에 대해 소개하도록 한다.

Ⅰ. 서 론

오늘날 전 세계 네트워크 망은 다양한 네트워크 애플리케이션의 요구 및 발전에 따라 규모 및 구조 측면에서 매우 복잡하게 변해가고 있다. 이러한 추세에서 네트워크 토폴로지들의 형태는 한가지 뚜렷한 특징을 나타내는데, 소수의 노드, 즉 라우터들이 다른 많은 노드들과 연결되어 있어 해당 네트워크의 연결성에 매우 중요한 부분을 차지한다는 점이다. 특히 WAN 과 같은 네트워크 망에서는 소수의 코어 라우터들이 많은 LAN 의 네트워크 백본 연결을 담당하고 있다. 따라서 만약 이와 같은 소수 노드 또는 링크들이 다운된다면 해당 네트워크의 대부분 연결성에 심각한 영향을 끼칠 수 있다. 먼저 본 논문에서는 이러한 지점을 네트워크 병목 (Network Bottlenecks) 이라고 가정한다.

네트워크 병목 지점은 공격자들에게 주요한 타겟이 될 수 있는데 소수의 공격 트래픽으로 다수의 네트워크 연결성을 저해하는 큰 효과를 낼 수 있기 때문이다. 이러한 점에 착안하여 제안된 공격 시나리오가 링크 플러딩 공격(Link Flooding Attacks) 이다[1,2]. 공격자는 다수의 봇을 이용하여 네트워크 병목 지점을 찾고, 해당 지점을 통과하는 공격 플로우를 집중적으로 보내어서 공격하는 방식이다(그림 1).

링크 플러딩 공격과 같은 방식은 공격자가 병목 지점을 네트워크 토폴로지 스캐닝 기법을 이용하여 정확하게 찾아내는 것이 요구된다. 본 논문에서는 이와 같은 토폴로지 스캐닝 패킷을 탐지하고 공격자가 병목 지점을 탐지하지 못하도록 응답 패킷을 임의의 거짓 IP 주소로 전송하는 기법을 제안하도록 한다. 특히 이를 SDN 의 표준 프로토콜인 OpenFlow 의 두가지 메시지인 *Packet_In* 과 *Packet_Out* 을 이용하여 구현하는 방법을 제시하도록 한다.

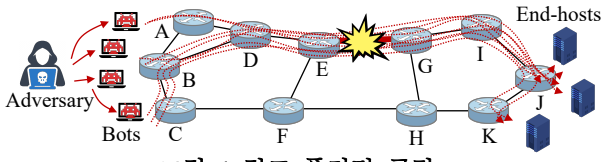

그림 1 링크 플러딩 공격

Ⅱ. 본론

Traceroute. 대표적인 토폴로지 스캐닝 기법으로 여러 플랫폼에서 네트워크 경로 추적에 널리 사용되는 traceroute 를 들 수 있다. Traceroute 는 IP 프로토콜의 특징을 이용한 것으로, 중간 라우터 또는 호스트가 IP TTL=1 인 패킷을 감지하였을 때, 이를 파기하고 ICMP Time Exceeded 패킷으로 응답하는 특성을 이용한 것이다[3]. Traceroute 는 TTL 값을 1 씩 증가시키며 임의의 더미 패킷을 목적지까지 지속적으로 보내면서, 응답한 패킷들의 IP 주소를 나열하는데, 이를 통해 목적지까지의 중간 홉 IP 주소들을 알 수 있다.

OpenFlow. SDN 은 기존 네트워크의 고질적인 문제였던 벤더 의존적 제어 평면을 해결한 새로운 네트워크 패러다임이다. 각 라우터마다 각기 다른 제어 평면을 가졌던 기존 환경과는 달리, SDN 환경에서는 제어 평면이 통합되어 하나의 중앙집중화된 컨트롤러가 전체 네트워크를 제어한다. 컨트롤러는 OpenFlow 라는 사실상의 SDN 표준 프로토콜을 이용하여 데이터 평면의 라우터를 제어하고, 네트워크 정책 등을 OpenFlow 메시지로 라우터에 전달하여 구현한다. 그림 2 는 OpenFlow 의 작동 예제를 나타낸 것으로 만약 Host A 가 SDN Switch 에 패킷을 전송할 시, SDN Switch 는 이 패킷을 어떻게 처리할지를 SDN Controller 에 *Packet_In* 메시지로 질의한다. SDN Controller 는 이에 대한 룰을 스위치 테이블에 *Flow_Mod* 로 보내 설치하고, *Packet_Out* 을 보내 해당 패킷을 Host B 로 보내도록 SDN 스위치에 지시하여 처리하도록 한다.

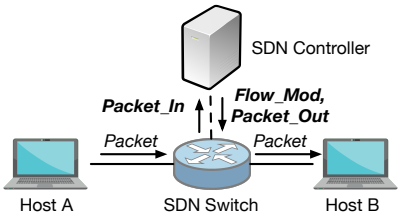

그림 2 OpenFlow 프로토콜 작동 예제

거짓 IP 주소 응답 기법. 본 논문이 제시하는 SDN 기반 MTD 기법을 설명하기 위해 그림 3 의 간단한 시나리오를 활용하도록 한다. 토폴로지 상의 Host A 는 10.0.0.1 의 IP 주소를 가지고 있으며 IP 주소가 10.0.0.2 인 Host B 를 목적지로 하는 traceroute request 패킷을 보내는 상황이다. 이때 해당 패킷이 expired 되는 첫번째 홉인 SDN Switch 는 10.0.1.1 의 주소가 지정된 인터페이스를 가지고 있다. 실제로 예제와 같이 Host A 와 해당 인터페이스가 인접한다면 같은 서브넷 주소를 가져야 하지만 본 예제에서는 두 지점이 실제로 각기 다른 네트워크에 속해있다고 가정한다.

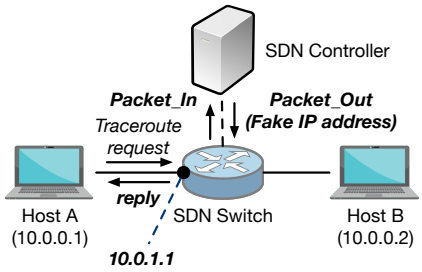

그림 3 시나리오 예제

SDN 스위치가 traceroute request 를 수신하면 이를 Packet_In 메시지로 SDN 컨트롤러에 전송하게 된다. SDN 컨트롤러는 traceroute 요청에 따라 Packet_Out 을 통해 SDN 스위치가 reply 패킷을 Host A 에 전송하도록 명령하는데, 이때 10.0.1.1 이 아닌 다른 IP 주소를 임의로 선택하여 전송하게끔 한다. 결과적으로 Host A 는 실제 스위치 인터페이스의 IP 주소가 아닌 다른 IP 주소를 가진 traceroute 응답 패킷을 수신하게 된다.

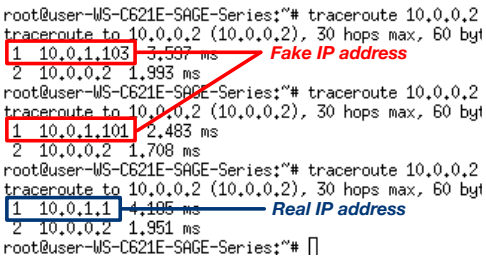

그림 4 거짓 IP 주소 응답 예제

그림 4 는 이러한 시나리오에 따라 SDN Switch 가 거짓패킷으로 응답하였을 때 Host A 의 traceroute 프로세스가 나타내는 주소 리스트를 나타낸 것이다. 그림 상에서 빨간색으로 표시된 주소는 임의로 만들어낸 거짓 인터페이스 주소이며, 파란색으로 표시된 주소는 실제 인터페이스의 주소이다. 거짓 주소들은 실제 인터페이스 주소와 같은 서브넷 주소인 10.0.1/24 에서 가용한 IP 주소 중에서 선택하도록 한다. 만약 공격자에게 실제 인터페이스 주소인 10.0.1.1 을 공격자에게 전혀 보여주지 않는다면, 다른 두 거짓 주소가 실제 주소가 아니라고 여길 수 있으므로, 본 기법에서는 매 traceroute 패킷 탐지 시 마다 거짓 주소들과 실제 주소를 랜덤하게 선택하여 응답 패킷을 작성하도록 한다.

검증. Traceroute 는 각 홉에서 응답한 패킷이 도착한 시간을 기록하는데 이를 RTT (Round Trip Times)라고 한다 (그림 5 참조). 만약 본 기법을 적용한 후에 이러한 RTT 수치가 크게 증가한다면, 공격자는 컨트롤러가 임의로 조작한 IP 주소가 실제 주소가 아니라고 여길 수 있다. 이러한 가설을 검증하기 위해 실제 하드웨어 SDN 스위치인 EdgeCore 4610-54T 모델에서 본 제안 방법을 테스트하였다. 특히 같은 모델의 다른 2 대의 하드웨어 스위치에서 실험함으로써, 다른 네트워크 디바이스에서 RTT 가 어떻게 변하는지를 검증하고자 하였다.

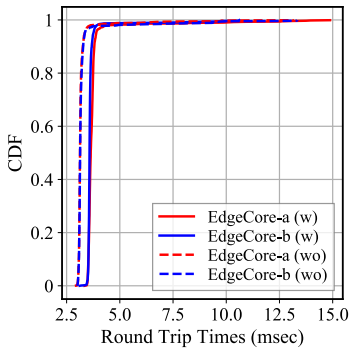

그림 5 RTT 측정 결과

그림 6 은 시나리오 예제와 같은 토폴로지에서 Host A 가 1,000 개의 Traceroute 패킷을 전송하고 RTT 를 기록한 결과를 나타낸 것이다. 각 두 하드웨어 스위치 장비를 EdgeCore-a, EdgeCore-b 로 표시하였으며, w(with)는 본 기법이 적용된 상태, wo(without)는 본 기법이 적용되지 않은 상태를 의미한다. 기록된 RTT 값 중 약 90%가 4ms 이내로 나타나 오버헤드가 크지 않은 것으로 관찰되었으며, 적용되지 않은 상태와 약 0.3ms 의 지연시간이 차이나는 것을 알 수 있었다. 따라서 공격자는 본 기법의 적용 여부를 판단하기 매우 힘들 것이라고 예상된다.

Ⅲ. 결론

본 논문에서는 토폴로지 스캐닝 공격 방어를 위한 SDN 기반 거짓 IP 주소 방법을 제안하였다. 시나리오를 통해 실제 traceroute 툴에서 본 기법이 유효하게 적용되는 것을 보였으며, 실시한 하드웨어 테스트베드에서 성능 오버헤드가 크지 않음을 보일 수 있었다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00254, SDN 보안 기술개발)

참 고 문 헌

[1] Kang, Min Suk, Soo Bum Lee, and Virgil D. Gligor. "The crossfire attack." 2013 IEEE symposium on security and privacy. IEEE, 2013.
[2] Studer, Ahren, and Adrian Perrig. "The coremelt attack." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2009.
[3] “Traceroute for linux”, http://man7.org/linux/man-pages/man8/traceroute.8.html.