IPv6 네트워크 토폴로지 기반 MACsec과 IPsec 공격 및 방어 시나리오에 대한 연구

김종석, 정세원, 문현정, 전현호

Implement MACsec and IPsec based on IPv6 network topology and defend against attack scenario

Jongseok-Kim, Sewon-Jung, Hyunjeong-Mun, Hyunho-Jun

요 약

최근 네트워크 기술을 이용한 다양한 응용 분야의 증가와 기하급수적인 요구로 인한 공급으로 인한 여러 보안 취약점이 생겨나면서 이에 대응 할 보안이 요구되고 있다. 특히 IPv4 주소 자원의 부족으로 IPv6의 공급의 증가가 예상되면서 IPv6 주소 메카니즘의 보안 강화는 충분히 고려되어야 한다. 본 논문은 IPv6 네트워크 환경에서 IP 계층과 데이터 링크 계층 보안 프로토콜인 MACsec과 IPsec을 구현하면서 각 보안 프로토콜의 방어 기법과 성능을 확인했다. 이를 통해 MACsec와 IPsec의 병행 사용으로 외부 LAN의 데이터 기밀성과 무결성을 유지하고 내부 LAN의 Dos Attack, MITM Attack을 방어하는 강력한 보안 기법임을 제시한다.

ABSTRACT

Security is required to respond to the recent increase in various applications using network technology and supply from exponential demands. Strengthening the security of IPv6 address mechanisms should be fully considered, especially as the supply of IPv6 is expected to increase due to a lack of IPv4 address resources. This paper confirmed the defense techniques and performance of each security protocol, implementing MACsec and IPsec, IP layer and data link layer security protocols in IPv6 network environment. This suggested that the use of MACsec and IPsec in parallel is a powerful security technique that maintains the data confidentiality and integrity of the external LAN and defends the Dos Attack, MITM Attack on the internal LAN.

키워드 : MACsec, IPsec, 네트워크 보안, 공격 시나리오

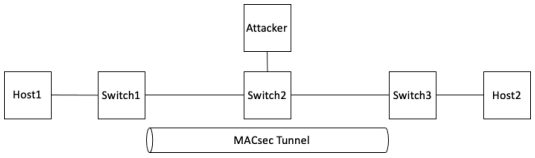
Key word : MACsec, IPsec, Network security, Attack scenario

Ⅰ. 서 론

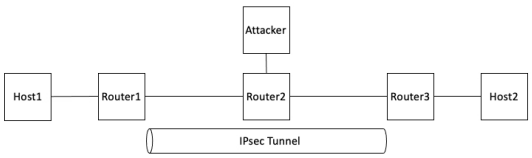
IPv4 주소 고갈 문제로 인하여 IPv6 주소체계에 대해서 관심이 급증하고 있다. IPv6 현재 국내에 5,260개 할당되어 있고, 4,273,677,318개가 미할당 되어있다. 이는 IPv4 미할당분인 22,314,080개 보다 충분히 많은 숫자이며 주소 고갈 문제를 해결할 수 있을것이다. 또한, 할당 추이도 꾸준히 증가하는 추세이다. IPv6에 관심이 높아짐에 따라서 보안문제가 대두되고 있는데, IPv6는 새로운 프로토콜인 ND 프로토콜을 포함하고 있다. 이것은 기존의 IPv4의 ARP 프로토콜을 대체하는 프로토콜이다. 하지만, ND 프로토콜이 사용되면서 여러 취약점들이 발견되었는데, MITM, DOS 공격이 대표적이다. 이러한 공격에 대한 방어기법으로 MACsec, IPsec등이 소개되어 있지만 취약점을 여전히 가지고 있다. 본 연구에서는 대표공격에 대한 방어기법을 GNS3 가상환경에서 적용하여 가상 공격 시뮬레이션을 통해 실제로 공격과 방어가 이루어지는지 확인한다. 또한 보안기법에 취약점을 보안할 융합된 형태의 토폴로지를 소개하고 향후 보안기법 개발 방향을 제시한다

Ⅱ. IPsec과 MACsec 공격 및 방어 시나리오

2.1. IPsec과 MACsec 공격 및 방어 시나리오



(a)



(b)

그림1. MACsec과 IPsec 공격 및 방어 시나리오

그림1은 MACsec과 IPsec 프로토콜으로 구성된 각 토폴로지에서 공격 및 방어 시나리오를 나타낸다.

MACsec(Media Access Control Security) 프로토콜은 이더넷 연결 장치 간의 데이터 보안을 제공하며, IEEE 표준 802.1AE에 의해 정의된다. 원래 MACSec은 물리적으로 연결된 두 장치 사이의 연결을 확보했지만, 현재 형태에서는 간섭되는 장치나 네트워크의 수에 관계없이 두 장치 간의 데이터 통신을 보호할 수 있다. MACsec은 서비스 거부, 침입, 중간자, 가장, 수동 도청 및 재생 공격을 포함한 대부분의 보안 위협을 식별하고 방지 할 수 있다. 본 연구서는 2계층 중간자 공격을 방어하기 위해 MACsec을 사용하였다(그림1a).

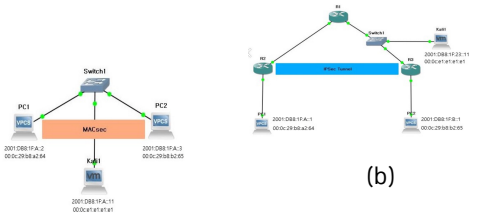
IPSec(Internet Protocol Security) 프로토콜은 인터넷상에서 VPN을 구현하는데 사용될 수 있도록 IETF에서 개발된 프로토콜이다. 동작 방식으로는 전송 모드와 터널모드로 나뉘며 사설 및 공중망을 사용하는 TCP/IP보다 안전하게 유지하기 위해 인증 헤더인 AH(Authentication Header)와 캡슐 보안 페이로드인 ESP(Encapsulating Security Payload)로 2개의 프로토콜로 구성된다. 본 연구에서는 IP 패킷 전체를 보호하는 것이 목적이기 때문에 터널모드의 ESP 프로토콜을 사용하였다(그림1b).

2.2. 공격 방법

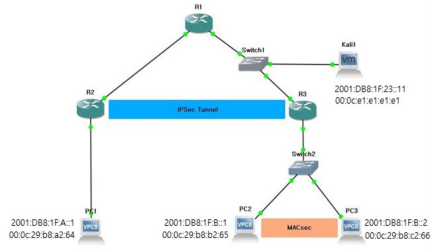
본 논문에서 공격방법으로 칼리 리눅스에서 공격도구로 제공되는 parasite6 명령어를 사용한다. Parasite6 명령어는 IPv6에 대한 ARP Spoofer로 Neighbor Solitication 요청에 거짓으로 응답하여 모든 로컬 트래픽을 자신의 시스템으로 리디렉션하는 공격이다. 즉, Parasite6를 사용해 공격하게 되면 LAN 안의 모든 기기의 ND Table의 MAC 주소가 공격자의 MAC 주소로 바뀌게 되고 이후 패킷을 전송하면, 모든 패킷은 공격자를 거쳐가게 되어 공격자가 패킷을 볼 수 있게 된다.

Ⅲ. 실험

3.1. 네트워크 토폴로지



(a) (b)



(c)

그림2. 네트워크 토폴로지

실험을 위한 네트워크 환경은 GNS3와 Virtual Ware를 연동한 그림 2과 같은 토폴로지의 가상 테스트 베드 환경에서 실행한다. 희생을 위한 호스트 3대의 Virtual Machine와 네트워크 공격을 위한 Virtual Machine 1대(Kali Linux)로 구성되었다.

3.2. MACSec이 구현된 토폴로지

그림2a는 MAC이 구현된 토폴로지를 나타낸다. MACsec이 적용된 PC1과 PC2가 데이터를 공유하면 MACsec은 Layer 2 페이로드를 암호화한다. 암호화된 데이터는 MACsec 프로토콜에 대한 정보를 제공하는 보안 태그(SecTag)와 전송된 암호화 패킷이 변경되지 않았음을 확인하는

ICV(Integrity Check Value)의 두 헤더와 함께 캡슐화 된다(그림3). 따라서 MACSec이 구현된 PC1과 PC2는 MAC 주소가 공격자의 ND Spoofing 전후로 변하지 않았다. 이를 통해 MACSec 프로토콜이 2계층 공격에 대응하기 위한 방어책으로 유효하다는 것을 알 수 있다. 하지만 MACsec은 레이어 2에서만 작동하므로 단일 LAN만 보호할 수 있어 트래픽이 라우팅 될 때 보호 기능은 제공하지 않는다. 예를 들어 ARP 스푸핑 또는 IP 리디렉션을 사용하여 트래픽을 다른 인터페이스에서 강제로 나가는 공격은 MACsec만으로는 방지할 수 없다.

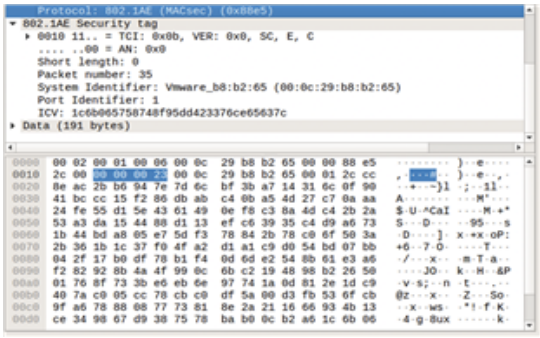


그림3. MACSec 패킷

3.3. IPSec이 구현된 토폴로지

그림2b는 IPsec이 구현된 토폴로지를 나타낸다. 공격자는 Switch1에 연결된 장비의 ND테이블 목적지를 본인으로 변경하기 위해 본인이 도착지 라우터라는 가짜 패킷을 무한히 보낸다. 따라서, R3의 ND테이블을 확인해보면 MAC주소가 공격자 MAC주소로 바뀌게 된다(그림4).

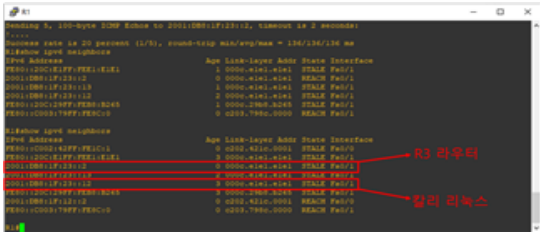


그림4. R1의 ND 테이블

이때 PC1에서 PC2로 ping 명령어를 통해 패킷을 전송해 보면 그림 와 같이 공격자는 암호화된 ESP패킷을 spoofing하여 내용을 알 수 없게 되어 공격을 수행할수 없게된다. 따라서 IPsec 터널사이 외부 LAN에서 MITM 공격은 라우터의 MAC주소는 변환되지만 암호화된 패킷을 감지하므로 성공적으로 방어했다고 볼 수 있다. 하지만 터널모드에서의 IPsec은 외부 LAN에서는 패킷이 암호화되지만 내부 LAN에서는 그대로 ICMPv6 패킷이 감지되기 때문에 내부 2계층 보안 취약점은 여전히 남아있다.

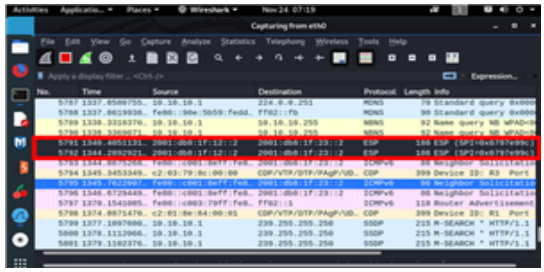


그림5. 칼리 리눅스에서 스푸핑한 패킷

3.4. MACSec과 IPSec이 구현된 토폴로지

앞서 Parasite6를 통한 외부 LAN(그림2 c)과 내부 LAN에서의 스푸핑 공격을 시도하고 결과를 봤다. IPsec은 외부 LAN(라우터 터널링) 보안의 강력함이 있지만 내부 LAN에서의 보안 취약점이 있었다. 반면에, MACsec은 내부 LAN 보안의 강력함이 있지만 외부 LAN 보안의 취약점이 보였다. 따라서 IPsec과 MACsec의 보안 프로토콜 병행 사용을 통한 내외부 LAN의 보안성을 높이고자 아래 토폴로지를 제안한다.(그림2 d) PC1와 PC2로 어디에 공격자가 들어와서 ICMPv6 공격 패킷을 보내도 두 개의 보안 프로토콜의 사전 방어 기법을 통해 방어할 수 있고 네트워크 안전성을 유지할 수 있다.

Ⅳ. 결론

본 논문은 IPv6 네트워크 환경에서 IP 계층과 데이터 링크 계층 보안 프로토콜인 MACsec과 IPsec을 구현고 이를 공격하면서 각 보안 프로토콜의 방어 기법과 성능을 확인했다. 이를 통해 MACsec과 IPsec의 병행 사용으로 외부 LAN의 데이터 기밀성과 무결성을 유지하고 내부 LAN의 MITM 공격을 방어하는 강력한 보안 기법임을 제시하였다.

Ⅴ. 참고문헌

[1] 한국인터넷정보센터(KRNIC). cn.d. cited 20210114. IP주소/AS번호-국내현황 국가승인 일반통계 제329001호(2021); Available from https://xn--3e0bx5euxnjje69i70af08bea817g.xn--3e0b707e/jsp/statboard/IPAS/inter/pos/currentV6Addr.jsp