IPv6 네트워크 토폴로지 기반 IPsec과 MACsec 구현 및 공격시나리오 방어

전현호, 김종석, 정세원, 문현정

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

Hyun-ho Jun, Jong-seok Kim, Se-won Jung, Hyun-jeong Mun

요 약

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

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 IPsec and MACsec, IP layer and data link layer security protocols in IPv6 network environment. This suggested that the use of IPsec and MACsec 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 : IPsec, MACsec, 네트워크 보안, 공격 시나리오

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

Ⅰ. 서 론

IPv4 주소 고갈 문제로 인하여 IPv6 주소체계에 대해서 관심이 급증하고 있다. IPv6는 새로운 프로토콜인 ND 프로토콜을 포함하고 있는데 이것은 기존의 IPv4의 ARP 프로토콜을 대체하는 프로토콜이다. 하지만, ND 프로토콜이 사용되면서 여러 취약점들이 발견되었는데, MITM, DOS 공격이 대표적이다. 본 논문에서는 ND 프로토콜을 이용한 공격기법에 대해서 조사하고, 본 공격에 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. ND 프로토콜 소개 및 취약점

2.1. NDP 소개

NDP는 IPv4의 ARP와 같은 유사한 역할을 수행한다. 즉, 이더넷 환경에서 상대방의 IPv6 주소를 통해 MAC 주소를 알아내고 이를 바탕으로 상대방과의 통신을 가능케 하는 역할을 수행한다.

인터넷 모델의 링크 계층에서 동작하며, 호스트의 주소 자동구성, 다른 노드의 링크 계층 주소 결정, 중복 주소 탐지, 사용 가능한 라우터 및 DNS(Domain Name System) 서버탐지, 주소 접두사 검색, 유지관리 등을 담당한다. 다른 활성화 되어있는 인접 노드로의 경로에 대한 접근성 정보 NDP는 목적에 따라서 총 5개의 ICMPv6 패킷 유형으로 정의되는데, 라우터 요청(RS), 라우터 광고(RA), 이웃 요청(NS), 이웃 광고(NA), 리다이렉트 메시지가 있다.

Neighbor Discovery 과정은 출발지 라우터와 목적지 라우터가 통신하기 위해 상대방의 MAC 주소를 알아야 한다. 이를 위해 출발지 라우터는 이더넷 링크를 이용하여 NS 메시지를 전송한다. 이때 출발지 IPv6 주소는 자신의 IPv6 주소를 사용하고, 목적지 IPv6 주소는 출발지 IPv6 주소를 기반으로 하는 노드 멀티캐스트 주소(FF02::1) 를 사용한다. 전송된 패킷은 네트워크의 모든 활성화된 링크 로컬 주소에 도달하게 된다. 그러나 이러한 IPv6 통신에서 ICMPv6 메시지를 교환하는 형식은 서비스 거부공격(Dos) 또는 중간자 공격(MITM) 또는 기타 악의적인 목적을 위해 조작된 가짜 응답 메시지를 보내서 악용될 수 있다.

2.2. MITM

중간자 공격(man in the middle attack, MITM)은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격기법이다. 중간자 공격은 통신을 연결하는 두 노드 사이 중간에 위치하여, 두 노드는 상대방에게 연결했다고 생각하지만 실제로 두 노드는 중간자에 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달하는 공격이다.

2.2.1. 스니핑(Sniffing)

스니핑 공격은 공격자가 네트워크상의 데이터를 도청하는 행위를 말한다. 스니핑 공격은 수동적 공격이라고 말하는데 이는 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문이다. LAN 상에서 개별 호스트를 식별하기 위한 방법으로 이더넷 인터페이스는 MAC 주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC 주소는 서로 다른 값을 가진다. 따라서 로컬 네트워크상에서 각 호스트는 유일하게 식별이 가능하다. 이더넷은 로컬 네트워크 내의 모든 호스트가 같은 선을 공유하도록 되었는데, 이로 인해서 같은 네트워크 내의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다. 하지만 이더넷 인터페이스는 자신의 MAC 주소를 갖지 않는 트래픽을 무시하는 필터링을 가진다. 하지만 스니핑 공격은 이러한 필터링을 무시하고, MAC주소를 위장하는 방법이나 모든 트래픽을 볼 수 있는 Promiscuous 모드를 설정하여 트래픽을 도청하는 방식을 취한다.

2.2.2. 스푸핑(Spoofing)

스푸핑은 도용하다 라는 의미가 있는데, 신분을 도용하거나 위조하여 진행하는 공격을 스푸핑이라고 한다. 링크 로컬 네트워크에서, 두 노드 사이의 통신은 NS와 NA 두 종류의 ICMPv6 메시지를 교환함으로써 정상적으로 수행될 수 있다. 두 가지 유형의 ICMPv6 메시지는 네트워크에서 IPv6 주소의 MAC 바인딩에 사용된다. 그러나, 이 교환은 완전히 안전하지 않고 공격자가 링크의 다른 호스트에 속한 자신의 2계층 주소를 광고하는 NA를 생성하는 것을 방지하기 위한 대책이 마련되어 있지 않다.

2.3. 서비스 거부 공격(Dos)

Dos는 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다. 수단, 동기, 표적은 다양할 수 있지만, 보통 인터넷 사이트 또는 서비스의 기능을 일시적 또는 영구적으로 방해 및 중단을 초래한다.

2.3.1. ICMPv6 Flood Attack

IPv6의 새로운 유형의 확장 헤더, 새로운 ICMPv6 메시지 및 IPv6의 멀티캐스트 주소에 대한 의존성은

flood공격에 새로운 방법을 제공할 수 있다. ICMPv6 패킷을 피해자의 수신처로 보내는 것 또는 세션이 삭제되도록 하여 이미 경로가 확립된 통신을 교란하는 오류 메시지를 보내는 것 등 여러 가지 방법으로 Dos 공격을 발생시키는데 사용할 수 있다. 또한, 가짜 통신망 구축 또는 유지보수 메시지를 링크에 침투시킬 수 있다면, 합법적인 주소를 무효로 하거나 인터페이스를 비활성화할 수 있다.

이렇듯 ND 프로토콜에 발생할 수 있는 취약점에는 서비스 거부 공격(Dos) 또는 중간자 공격(MITM) 또는 기타 악의적인 목적을 위해 조작된 가짜 응답 메시지를 보내서 악용으로 인한 방어 기법이 필요하다. 이에 네트워크 계층별로 네트워크 보안 프로토콜을 살펴보며 보안 기법에 대해 알아본다.

Ⅲ. 계층별 보안 프로토콜

3.1. IPsec

3.1.1. IPsec 개요

IPSec은 Internet Protocol Security의 약어로서 네트워크 계층에서의 보안을 위한 표준이다. IPSec은 인터넷상에서 VPN(Virtual Private Network)을 구현하는데 사용될 수 있도록 IETF (Internet Engineering Task Force)에서 개발된 프로토콜이다. 이는 네트워크상의 Network Layer에서의 보안에 중점을 두었으며, 사설 및 공중망을 사용하는 TCP/IP 통신을 보다 안전하게 유지하기 위한 End-to-End encryption과 authentication을 제공한다. IPSec은 인증 헤더(AH : Authentic-ation Header)와 캡슐 보안 페이로드(ESP : Encapsulating Security Paylaod) 2개의 프로토콜로 구성돼 있다. ESP는 데이터를 암호화하고 인증하는 데 사용할 수 있지만, AH는 데이터를 인증하는 데만 사용할 수 있습니다. 두 옵션은 함께 사용할 수 있지만 일반적으로 별도로 사용된다.

3.1.2. AH 헤더

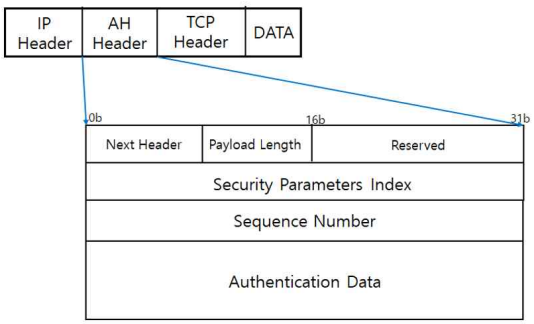


그림 1 IP sec AH 헤더

메시지 인증 코드(MAC)를 이용하여 인증을 제공해주는 프로토콜로 기밀성은 제공하지 않는다. 송신 측에서 MAC 알고리즘과 인증키를 통해 인증 데이터를 계산하여 전송하고 수신 측에서 이를 검증한다. 인증 데이터 계산에는 IP 헤더의 변경 가능한 필드를 제외한 IP 패킷 전체를 대상으로 한다. 전송 모드는 IP 헤더의 전송 중 변경 가능한 필드를 제외한 IP 패킷 전체를 인증한다. 터널 모드는 New IP 헤더의 전송 중 변경 가능한 필드를 제외한 New IP 패킷 전체를 인증한다.

3.1.3. ESP 헤더

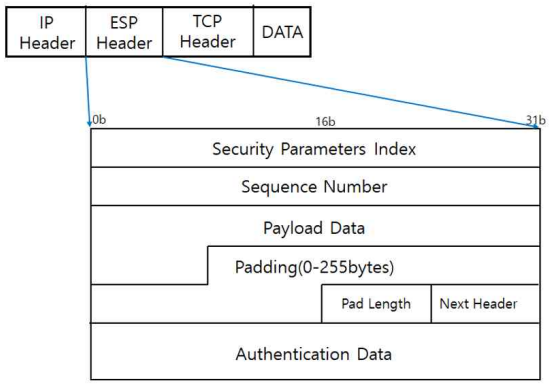


그림 2 IPsec ESP 헤더

MAC와 암호화를 이용하여 인증과 기밀성을 제공한다. 인증과 암호화를 선택적으로 적용할 수 있다. 인증에 있어서 AH는 변경 가능한 IP 헤더 필드를 제외한 IP 패킷 전체를 인증하지만, ESP는 IP 헤더를 인증하지 않는다. 전송모드는 IP 페이로드와 ESP 트레일러를 암호화하고 암호화된 데이터와 ESP 헤더를 인증한다. 터널 모드는 원본 IP 패킷 전체와 ESP 트레일러를 암호화하고 암호화된 데이터와 ESP 헤더를 인증한다.

3.1.4. VPN

IPsec 프로토콜은 VPN 연결하고, 두 개 이상의 지점 사이의 모든 트래픽을 암호화 및 인증하는 데 사용할 수 있다. VPN을 포함한 IPsec 회로는 다음 두 가지 모드를 사용할 수 있다.

터널 모드는 일반적으로 호스트가 다른 게이트웨이 뒤에 있는 호스트와 안전하게 통신할 수 있도록 한다. IPsec 터널은 두 게이트웨이 호스트 사이에 설치되지만, 터널 자체는 보호된 네트워크 내의 모든 호스트로부터 트래픽을 전송할 수 있다. 터널 모드는 양쪽 끝에 서로 다른 호스트로부터 두 네트워크 사이의 모든 트래픽을 보호하기 위한 메커니즘 구현에 유용하다.

전송 모드는 두 개의 개별 호스트가 직접 연결된 IPsec VPN 연결을 설정할 때, 이 회로는 전송 모드 IPsec 회로의 예라고 할 수 있다. 전송 모드 IPsec은 한 호스트가 다른 호스트와 상호 작용해야 하는 경우에 사용된다. 두 호스트는 IPsec 회로를 서로 직접 협상하며, 세션이 완료된 후 회로가 일반적으로 중단된다.

3.1.4. 구현 동작

IPsec 연결의 첫 번째 단계는 호스트가 IPsec을 사용

하여 패킷을 전송해야 한다는 것을 인식할 때 발생한다. 이는 소스 또는 대상의 IP주소를 정책 구성에 관해 확인하여 IPsec의 경우 트래픽이 "흥미로운" 것으로 간주되어야 하는지를 결정하여 수행한다. 이런 트래픽은 패킷에 대한 보안 정책을 트리거하므로 패킷을 보내는 시스템이 패킷에 적절한 암호화 및/또는 인증을 적용하게 된다. 들어오는 패킷이 "흥미롭다"라고 판단되면 호스트는 인바운드 패킷이 암호화되었는지 또는 제대로 인증되었는지 검증한다.

IPsec 연결의 두 번째 단계는 IPsec을 사용하여 보안 회로에 사용하는 정책을 협상하고 서로 인증하며 두 호스트 간의 보안 채널을 시작할 수 있도록 한다. 이 단계에서, IPsec을 사용하여 호스트 간에 초기 보안 채널을 설정한다. 그런 다음 보안 채널은 IPsec 회로가 IPsec 회로에서 전송된 데이터를 암호화 및 인증하는 방식을 안전하게 협상하는 데 사용된다.

IPsec 연결의 세 번째 단계, 그 자체는 두 번째 단계의 보안 채널 설정을 통해 수행된다. 두 호스트가 실제 네트워크 데이터를 전달하는 IPsec 회로에 대한 보안 연결을 협상하고 시작해야 한다. 두 번째 단계에서는 두 호스트가 세션에서 사용할 암호화 알고리즘 유형을 협상하고 해당 알고리즘에 사용할 비밀 키에 동의한다. IPsec 연결의 네 번째 단계는 새로 생성된 IPsec 암호화 터널에서 실제 데이터 교환이다. 이 시점부터 패킷은 이전 세 단계의 IPsec SA 설정을 사용하여 두 엔드 포인트에 의해 암호화되고 해독된다.

마지막 단계는 IPsec 터널의 종료로, 대개 호스트 간의 통신이 완료되거나 세션이 시간 초과되거나 이전에 지정한 바이트 수가 IPsec 터널을 통과했을 때이다. IPsec 터널이 종료되면 호스트는 해당 보안 연결을 통해 사용된 키를 삭제한다.

3.2. MACsec

3.2.1. MACsec 개요

MACsec 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 CA에서 구성된다. CA는 인터페이스에서 인바운드 트래픽용과 아웃바운드 트래픽용으로 각각 하나씩, 두 개의 보안 채널을 생성하기 위해 사용되는 MACsec 속성 집합이다. 보안 채널은 MACsec 보안 링크에서 데이터를 전송하고 수신하는 역할을 담당한다.

CA는 point-to-point Ethernet link의 양쪽에 있는 MACsec 지원 인터페이스에 할당되어야 한다. 여러 이더넷 링크에서 MACsec을 사용하도록 설정하려면 각 링크에서 개별적으로 MACsec을 구성해야 한다. MACsec을 사용하려면 MAC 주소 또는 포트와 같은 다른 사용자 구성 가능한 매개 변수들도 링크의 각 측면에 있는 인터페이스에서 일치해야 한다. MACsec이 활성화되면 연결된 두 장치 간의 보안 키 교환 및 검증 후 양방향 보안 링크가 설정된다. 즉, MACsec이 활성화되면 링크의 양쪽 끝에 있는 인터페이스 간에 일치하는 보안 키를 교환하고 확인한 후 링크가 보안된다. 키는 MACsec을 활성화하는 데 사용되는 보안 모드에 따라 수동으로 구성하거나 동적으로 생성할 수 있다. 전송된 데이터를 보호하기 위해 데이터 무결성 검사와 암호화의 조합이 사용된다. 전송 장치는 전송할 모든 이더넷 프레임에 헤더와 테일을 추가하고 프레임 내의 데이터 페이로드를 암호화한다. 수신 장치는 헤더와 테일의 무결성을 확인한다. 검사에 실패하면 트래픽이 삭제되고 확인이 성공하면 프레임이 해독된다.

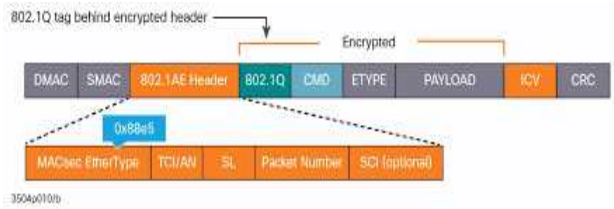


그림 3 MACsec 패킷 구조

3.2.2. 패킷 구조

MACsec은 L2 이더넷 프레임의 MAC 주소 다음 부분을 암호화한다. 기본적인 이더넷 프레임 구조에 암호화를 위해 MACsec 파라미터를 포함한 보안 태그(SecTag)가 추가되며, 프레임의 뒤에 무결성 체크를 위한 값(ICV)이 추가된다. L2 프레임의 마지막에 들어가는 FCS는 ICV까지 반영하여 다시 계산된다. MACsec에서 실제 데이터 부분인 Payload를 암호화할 것인가는 옵션 사항으로 암호화하지 않을 수도 있다. 보안 태그의 암호화 필드의 값을 E: 0x01 설정하면 암호화를 사용할 수 있다. MACsec Header의 필드는 다음과 같다.

- TCI/AN: TAG 제어 정보/관련 번호
- SL: 암호화된 데이터의 길이
- PN: 재생 보호에 사용되는 패킷 번호
- SCI : CA 의 보안 채널 식별자, MAC 주소 및 16bit 포트 ID 연결

3.2.3. 제공 기능

MACsec Offers	Explanation
Device-to-device security	MACsec은 개입 장치 또는 네트워크와 관계없이 두 장치 간에 데이터를 안전하게 전송한다. 이를 통해 LAN, MAN 및 WAN에서 MACsec을 사용하여 데이터 통신을 보호할 수 있다.
Connectionless data integrity	무단으로 데이터를 변경하는 것을 감지할 수 있다. (데이터의 무결성을

	보장한다) 각 MAC 프레임은 별도의 무결성 확인 코드를 전달하므로 Connectionless 라는 용어가 사용된다.
Data origin authenticity	수신된 MAC 프레임은 인증된 장치에서 전송된 것임을 보장한다.
Confidentiality	각 MAC 프레임의 데이터 페이로드가 암호화되어 권한이 없는 이가 도청하는 것을 방지한다.
Replay protection	공격자가 네트워크에서 복사한 MAC 프레임은 탐지되지 않고는 네트워크로 재전송 될 수 없다. 하지만, 특별한 구성에서는 네트워크 내에서 프레임 순서를 변경할 수 있으므로 제한된 재생이 허용될 수 있다.
Bounded receive delay	MAC 프레임은 중간자 공격으로 가로챌 수 없으며, 감지되지 않고 몇 초 이상 지연될 수 없다.

표 1 MACsec 제공 기능

Ⅳ. 계층별 공격 및 보안 프로토콜 적용

4.1. Parasite6 공격

Parasite6 명령어는 IPv6에 대한 "ARP Spoofer"로, 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 거쳐 가게 되어 공격자가 패킷을 볼 수 있게 된다.

Parasite6 공격 테스트를 위한 네트워크 환경은 GNS3와 Virtual Box를 연동한 그림 1과 같은 토폴로지의 가상 테스트 베드 환경에서 실행한다. 희생을 위한 호스트 2대의 Virtual Machine과 네트워크 공격을 위한 Virtual Machine 1대(Kali Linux)로 구성되었다. 각 Virtual Machine의 환경은 표 2와 같다.

	IPv6 Address	MAC Address
Host1	2001:DB8:1F:A::2/64	00:0c:29:b8:a2:64
Host2	2001:DB8:1F:A::3/64	00:0c:29:b8:b2:65
Kali	2001:DB8:1F:A::11/64	00:0c:e1:e1:e1:e1

표 2 Parasite6 토폴로지 네트워크 환경

Parasite 명령어는 fake-mac을 지정할 경우 지정된

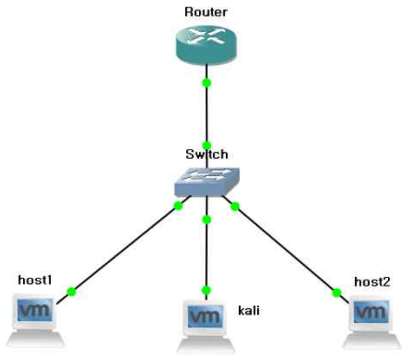


그림 4 Parasite6 토폴로지

MAC 주소로 리다이렉션 된다. 이외의 옵션으로 5개를 지정할 수 있다. -I 옵션은 패킷을 5초마다 반복 전송하고, -R 옵션은 목적지를 주입한다. 나머지는 네트워크 보안을 우회하는 옵션으로 -F 옵션은 fragment, -H 옵션은 hop-by-hop, -D옵션은 large destination header 이다.

```
Kali#parasite6 [-lRFHD] interface [fake-mac]
```

구성된 네트워크 환경에서 공격자(Kali)가 parasite6 공격을 수행하면 모든 LAN 안의 기기들의 ND Table이 이와 같이 변하게 된다. 즉, ND Table에서 모든 IPv6 Address에 대한 MAC 주소가 공격자의 MAC 주소로 변하게 된다.

IPv6 Address	MAC Address
2001:DB8:1F:A::3	00:0c:29:b8:b2:65
2001:DB8:1F:A::11	00:0c:e1:e1:e1:e1

표 3 공격 전 Host1 ND Table

IPv6 Address	MAC Address
2001:DB8:1F:A::3	00:0c:e1:e1:e1:e1
2001:DB8:1F:A::11	00:0c:e1:e1:e1:e1

표 4 공격 후 Host1 ND Table

IPv6 Address	MAC Address
2001:DB8:1F:A::2	00:0c:29:b8:a2:64
2001:DB8:1F:A::3	00:0c:29:b8:b2:65
2001:DB8:1F:A::11	00:0c:e1:e1:e1:e1

표 5 공격 전 Router ND Table

IPv6 Address	MAC Address
2001:DB8:1F:A::2	00:0c:e1:e1:e1:e1
2001:DB8:1F:A::3	00:0c:e1:e1:e1:e1
2001:DB8:1F:A::11	00:0c:e1:e1:e1:e1

표 6 공격 후 Router ND Table

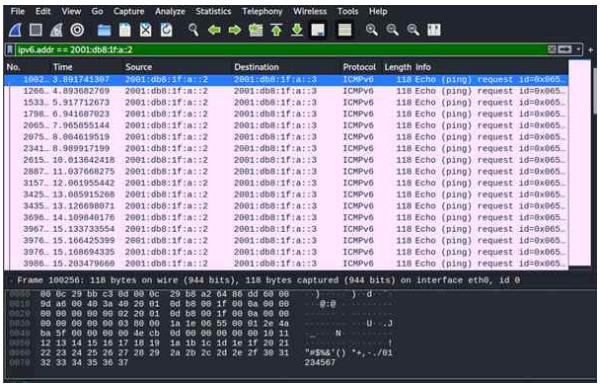


그림 5 스푸핑 된 Host 패킷

ND Table 변화 이후 Host1가 패킷을 Host2에게 패킷을 전송하면 이는 공격자를 거쳐 가게 되며, 이후 답신 역시 공격자를 거치게 된다.

4.2. MACsec 구현 및 Parasite6 공격

4.2.1. 리눅스의 MACsec 지원

리눅스는 리눅스 4.5 이후, 2016년 Red Hat 엔지니어 Sabrina Dubroca가 도입한 drivers/net/macsec.c에서 MACSec의 소프트웨어 구현을 사용할 수 있다. MACSec 지원은 상위 네트워크 장치에 연결된 전송 보안 채널당 전체 가상 네트워크 장치로 구현된다. 상위 인터페이스는 보호되거나 암호화된 콘텐츠가 있는 MACsec의 경우, 암호화된(혹은 보호된) 그대로 이더넷 패킷에 있는 원래 패킷만 확인한다. 이러한 설계는 VLAN과 같이 Linux에서 지원되는 다른 프로토콜과 매우 유사하다. 커널의 다양한 네트워크 구성을 목표로 하는 유틸리티 모음인 iproute2에도 MACsec 지원되었다.

4.2.2. MACsec 구현

MACSec은 데이터 링크 계층의 이더넷으로 연결된 장치 간의 데이터 보안을 제공한다. MACSec 구현 및 성능 테스트를 위한 시나리오는 GNS3과 Virtual Box를 연동한 그림 6과 같은 토폴로지의 가상 테스트베드 환경에서 실행한다. MACsec 통신을 위한 호스트 2대의 Ubuntu와 공격을 위한 Kali Linux로 구성되었다. 각 가상머신의 네트워크 환경은 표 7와 같다. 리눅스에서의 MACSec 구현을 위해 유틸리티 모음 iproute2를 사용한다.

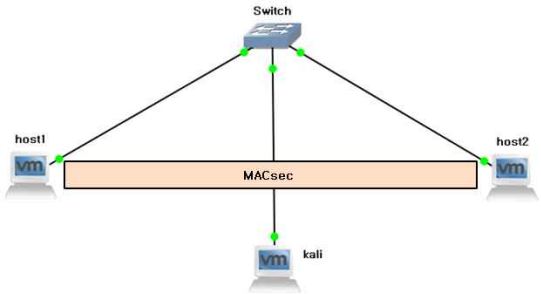


그림 6 MACsec 구현 토폴로지

	IPv6 Address	MAC Address
Host1	2001:DB8:1F:A::2/64	00:0c:29:b8:a2:64
Host2	2001:DB8:1F:A::3/64	00:0c:29:b8:b2:65
Kali	2001:DB8:1F:A::11/64	00:0c:e1:e1:e1:e1

표 7 MACsec 구현 토폴로지 네트워크 환경

두 호스트 사이에 보안 채널을 구성하려면 먼저 물리적 네트워크 인터페이스 위에 두 호스트 모두에 가상 MACsec 인터페이스(전송 보안 채널)를 만들어야 한다. 두 호스트 모두에서 ens33을 사용하고, MACsec 트래픽을 암호화하려고 한다고 가정한다.

전송 보안 연결을 위해, SA 및 키를 통해 전송된 패킷의 시작 ID로 사용될 패킷 번호를 구성한다. 또한, 수신 채널을 구성하고 상대의 MAC 주소, 포트 번호, 예상되는 첫 번째 패킷 번호 및 키를 기반으로 연결한다. 모든 MACsec 구성이 완료되면 MACsec 인터페이스를 이용하여 암호화된 패킷을 사용하여 Host1과 Host2간에 트래픽을 교환할 수 있다.

4.2.2. MACsec 환경 Parasite6 공격

두 MACsec이 적용된 PC가 데이터를 공유하면 MACsec은 Layer 2 페이로드를 암호화한다. 암호화된 데이터는 MACsec 프로토콜에 대한 정보를 제공하는 보안 태그(SecTag)와 전송된 암호화된 패킷이 변경되지 않았음을 확인하는 ICV(Integrity Check Value)의 두 헤더로 캡슐화 된다. 이 필드의 길이는 헤더 정보에 따라 8-16바이트 사이이며, ICV에 추가된 것은 패킷의 새로운 CRC이다.

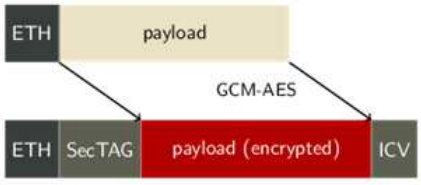


그림 7 MACsec Tag

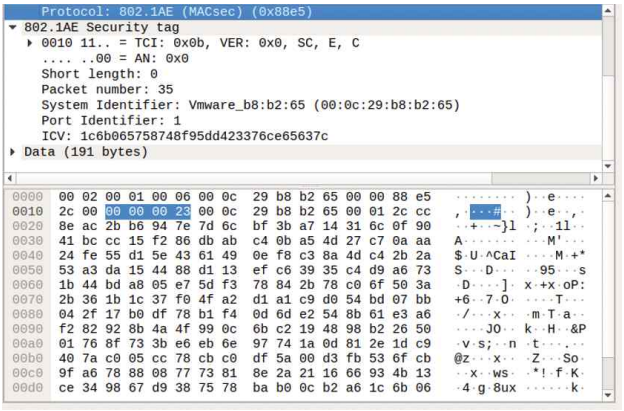


그림 8 MACsec 패킷

따라서 MACSec이 구현된 토폴로지에서는 Host1과 Host2의 MAC Address가 공격자의 ND Spoofing 전후로 변하지 않았다. 이를 통해 MACSec 프로토콜이 2계층 공격에 대응하기 위한 방어책으로 유효하다는 것을 알 수 있다. 그러나 스위치의 상위계층 장비인 라우터의 ND Table을 참조하면 라우터의 ND 테이블은 바뀐 것을 알 수 있다. 이를 통해 MACsec은 레이어 2에서만 작동하므로 단일 LAN만 보호할 수 있으며 트래픽이 라우팅 될 때 보호 기능을 제공하지 않다는 것을 알 수 있다. 예를 들어 ARP 스푸핑 또는 IP 리디렉션을 사용하여 트래픽을 다른 인터페이스에서 강제로 나가는 공격은 MACsec만으로는 방지할 수 없다. 즉 내부 LAN의 공격에 대해서는 유효하지만, 외부 LAN으로부터의 공격에 대해서는 유효하지 않는 한계를 지니고 있다.

4.2.3. IPsec 구현

ipsec 은 VPN으로 연결된 두 개 이상의 지점 사이의 지나가는 트래픽들을 암호화 및 인증하는데 사용할 수 있다. IPsec 회로는 두 가지 모드를 사용할 수 있는데, 본 논문에선 그림 9와 같이 터널모드를 사용한 토폴로지를 구성하였다. 네트워크 환경은 표 8과 같다.

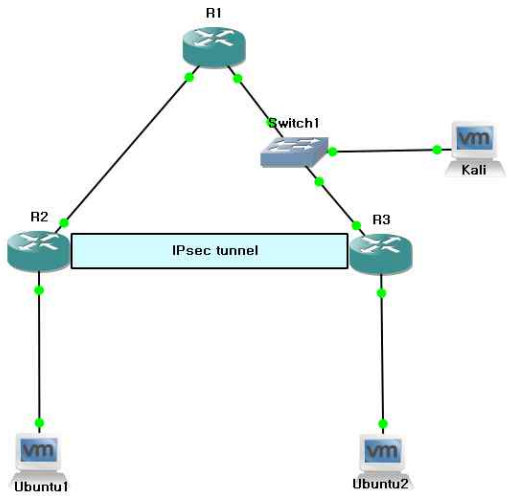


그림 9 IPsec 구현 토폴로지

	IPv6 Address	MAC Address
ubuntu1	2001:DB8:1F:A::1/64	00:0c:29:b8:a2:64
ubuntu2	2001:DB8:1F:B::1/64	00:0c:29:b8:b2:65
Kali	2001:DB8:1F:23::11/64	00:0c:e1:e1:e1:e1

표 8 IPsec 구현 토폴로지 네트워크 환경

IPsec을 구현하기 위해 IKE 정책 및 사전 공유 키 구성(키는 1234로 구성하였다.), IPsec 변환 세트 및 IPsec 프로파일 구성, IPv6에서 ISAKMP 프로파일 구성, IPsec IPv6 VTI 구성을 라우터 R2와 R3에 각각 설정 해준다..

그림 10 양단 라우터 터널 IPsec 적용 확인

이제 그림 9에서 보이듯이 IPv6 IPSec ESP Tunne을 생성하여 두 개의 떨어진 라우터가 인접한 라우터가 된 것과 같이 터널링 작업이 완료됐다. 따라서 좌측 R2 라우터에서 R3 라우터로 터널을 사용하여 패킷을 보내면 중간에 다른 라우터에서는 그림 11과 같이 ESP로 암호화된 된 패킷을 볼 것이다.

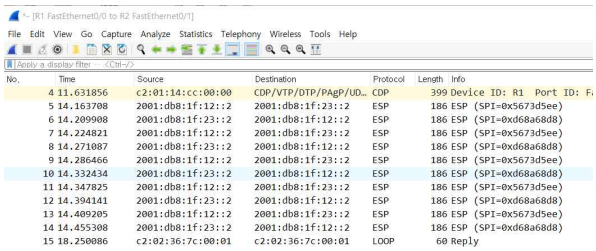


그림 11 ESP 패킷 캡쳐

4.2.2 IPsec 환경에서 parasite6 공격

ESP 패킷으로 감싸지는 부분인 R1과 R3 라우터 사이에 칼리 리눅스를 추가해주고, 5초마다 NA 패킷을 보내 같은 LAN에 구성되어있는 라우터들의 MAC 주소를 바꾸는 공격을 진행하여 패킷을 spoofing 하는 parasite6 공격을 진행하였다. 이때, 칼리 리눅스의 MAC 주소는 00:0c:e1:e1:e1:e1이다.

칼리 리눅스에서 공격을 시작하고 R3의 ND 테이블을 확인해보면 MAC 주소가 공격자의 MAC 주소로 변환되어있는 것을 확인할 수 있다. (그림 12)

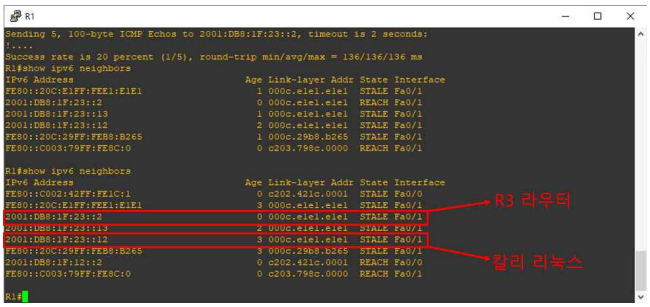


그림 12 R1의 ND 테이블

이때 ubuntu1에서 ubuntu2로 ping을 날려 패킷을 전송해 보면 그림 13 과 같이 칼리 리눅스는 암호화된 ESP 패킷을 spoofing하여 정상적으로 공격을 수행할 수 없게 된다.

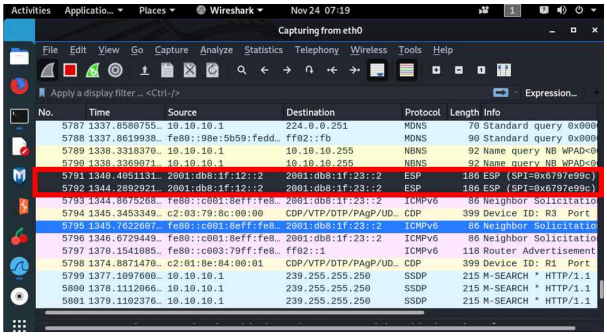
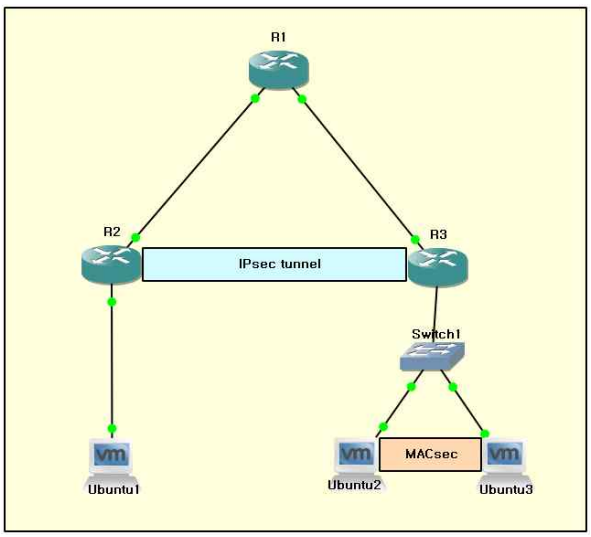


그림 13 공격자의 패킷 스푸핑

따라서 IPsec 토폴로지에서 터널 사이 외부 랜에서의 MITM 공격은 라우터의 MAC 주소를 변환시키는 데는 성공하였지만, 암호화된 패킷을 감지하므로 성공적으로 방어하였다고 볼 수 있다. 하지만 터널모드에서의 IPsec은 외부 LAN에서는 패킷이 암호화되지만, 내부 LAN에서는 그대로 ICMPv6 패킷이 감지되기 때문에 보안에 취약점이 있다고 할 수 있다.

4.2.4. MACsec+IPsec 구현

앞서 Parasite6를 통한 외부 LAN과 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. Ubuntu2와 Ubuntu3를 기준으로 어디에 공격자가 들어와서 ICMPv6 공격 패킷을 보내도 두 개의 보안 프로토콜의 사전 방어 기법을 통해 방어할 수 있고 네트워크 안전성을 유지할 수 있다.



Ⅴ. 결론 및 향후 계획

5.1. 결론 및 향후 계획

최근 네트워크 기술을 이용한 다양한 응용 분야의 증가와 기하급수적인 요구로 인한 공급으로 인한 여러 보안 취약점이 생겨나면서 이에 대응할 보안이 요구되고 있다. 특히 IPv4 주소 자원의 부족으로 IPv6 공급의 증가가 예상되면서 IPv6 주소 메커니즘의 보안 강화는 충분히 고려되어야 한다.

본 논문은 IPv6 네트워크 환경에서 IP 계층과 데이터 링크 계층 보안 프로토콜인 IPsec과 MACsec을 구현하면서 각 보안 프로토콜의 방어 기법과 성능을 확인했다. 이를 통해 IPsec와 MACsec의 병행 사용으로 외부 LAN의 데이터 기밀성과 무결성을 유지하고 내부 LAN의 Dos Attack, MITM Attack을 방어하는 강력한 보안 기법임을 제시하였다.

하지만, 두 개의 보안 프로토콜을 함께 사용하는 것은 유지비용과 효율적인 측면에서 바라보았을 때 적절한지 고민해야 한다. MACsec의 경우 주요 네트워크 장비에서는 키 교환을 위해 RADIUS 서버 구축이 필요하며 이는 고가의 장비를 구매해야 한다. 또한, 유지보수하는 입장에서 두 개의 보안 프로토콜을 관리한다는 것은 때에 따라서 비효율적일 수도 있다. 따라서 기업과 개인은 최적화 된 보안 프로토콜을 사용하여 미래 IPv6 네트워크 환경에서의 안전하고 신뢰할 수 있는 네트워크 기술을 유지해야 한다.

또한, 앞으로 IPsec과 MACsec의 보안 프로토콜이 개선되어야 할 점을 고쳐나가야 한다. IPsec의 경우 IPv6의 방대한 주소 공간을 효율적으로 관리하기 위해 주소 자동 설정 방식을 제공하는데 이는 관리자의 수동적인 조작 없이 호스트에서 자동으로 주소를 설정하게 된다. 이때, 인터페이스 주소를 사용하면서 NIC(Network Interface Card)가 교체되지 않는 한 동일한 주소가 설

정되는 문제가 있다. 또, IPv6 주소에 네트워크 주소가 암호화나 수정 없이 그대로 사용되어 위치 정보가 노출될 수 있다. 또한, IPsec의 ISAKMP 프로토콜의 구현상의 오류로서 영향받는 플랫폼의 원격 공격자가 악의적으로 조작된 IKE 패킷을 전송하여 서비스 거부가 발생하거나, 포맷 스트링, 버퍼 오버 플로우 취약점이 나타날 수 있다. MACse의 경우에도 하드웨어 ACL(Access Control Lists)은 MACsec 처리 후 수신 트래픽에 적용되기 때문에 ACL에 MACsec 캡슐화가 표시되지 않거나 MACsec에 의해 프레임이 차단된 경우 ACL 작업이 수행되지 않는다. 이외에도 Port mirroring, VCStacking, MRU(Maximum Receive Unit) 보안 문제가 있다. 향후 연구로는 IPsec과 MACsec의 보안 문제를 파악하고 해결하여 미래 네트워크 기술을 안전하고 유지할 수 있는 보안 대책을 마련한다.