Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.41

콘텐츠 감사를 위한 IPsec VPN 패킷 분석 기술 연구

박 정 형,[1†] 윤 재 남,[1] 류 재 철[2‡]
[1]ETRI 부설연구소 (책임연구원), [2]충남대학교 (교수)

IPsec VPN Encrypted Packet Analysis Method for Contents Auditing

Junghyung Park,[1†] Jaenam Yoon,[1] Jaecheol Ryou[2‡]
[1]Affiliated Institute of ETRI (Principal Researcher),
[2]Chungnam National University (Professor)

요 약

IPsec VPN에 대한 보안 감사는 구현 결함이나 설정 오류로 인한 취약점을 점검하고 사고 발생에 대한 조사 등을 위해 매우 중요하다. 하지만 IPsec VPN은 기밀성, 무결성, 인증 등을 보장하기 위해 네트워크 콘텐츠가 암호화되어 있어 보안 감사에 큰 어려움이 있다. 이를 해결하기 위해 중간자 공격 방식을 이용한 분석 기법들이 이전 연구들에서 제안되었다. 중간자 공격 기법을 적용하기 위해서는 상호 인증을 위한 사전 공유키를 알고 있어야 하며, 네트워크에 직접 참여해야 한다. 이는 보안 감사를 위해 일시적으로 네트워크 단절을 유발하며, 감사 이전에 수집된 데이터에 대한 분석이 불가능하다. 본 논문에서는 네트워크 연속성을 보장하며, 특정 IPsec VPN 연결 방식과 인증 방식에 한정되지 않는 새로운 분석 기법을 제안한다. 따라서, 제안하는 분석 기법은 IPsec VPN 보안 감사를 위해 실제적으로 활용될 것으로 기대된다.

ABSTRACT

Security audits of IPsec VPNs are crucial for identifying vulnerabilities caused by impleme- ntation flaws or misconfigurations, as well as investigating incidents. Nevertheless, auditing IPsec VPN presents noteworthy challenge due to the encryptiong of network contents which ensere confidentiality, integrity, authentications and more. Some researchers have suggested using man-in-the-middle(MITM) techniques to overcome this challenge. MITM techniques require direct participation in the network and prior knowledge of the pre-shared key for authentication. This causes temporary network disconnection for security audits, and it is impossible to analyse data collected before the audit. In this paper, we present an analysis technique aimed at ensuring network continuity without relying on a specific IPsec VPN topologies or authentication method. Therefore, it is anticipated that this approach will be effective, practical and adaptable for conducting IPsec VPN security

Keywords: Audit, IPsec VPN, IKEv2, ESP

I. 서 론

VPN(Virtual Private Networks)은 두 네트워크 또는 호스트 간 보안을 위해 공용 네트워크에 암호와 인증을 추가하여 데이터를 안전하게 전송하는 사설 통신망이다. IPsec VPN은 대표적인 VPN 중 하나이며, IP 계층을 보호하는 가장 오래되었지만, 여전히 가장 널리 사용되는 인터넷 보안 프로토콜이다. IPsec VPN은 보안 서비스 제공을 위한 SA (Security Association)을 설정하는 IKE(Internet Key Exchange)와 인증과 기밀성을 위한 AH(Authentication Header), ESP(Encap-

Received(09. 15. 2023), Modified(11. 22. 2023), Accepted(12. 13. 2022)
† 주저자, junghyung@nsr.re.kr
‡ 교신저자, jcryou@cnu.ac.kr(Corresponding author)

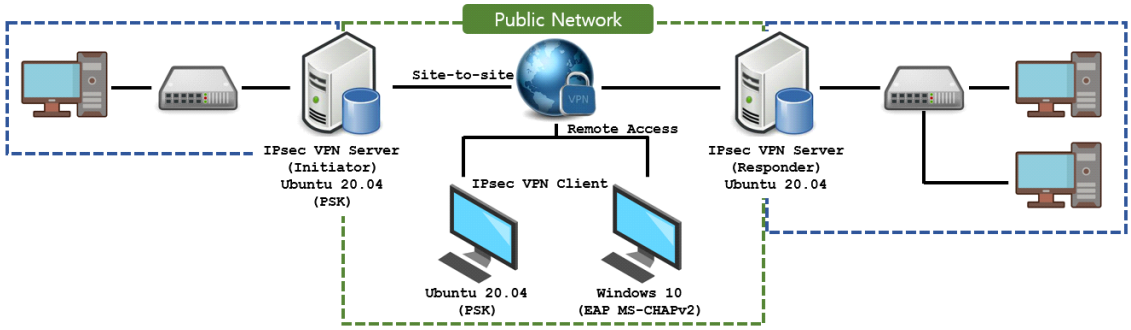


Fig. 1. Network topology of experimental environment

sulating Security Payload) 프로토콜로 구성된다. IKE는 두 가지(IKEv1, IKEv2) 버전이 있으며, IKEv2[1]는 키 교환 과정을 줄이고 서비스 거부 공격에 대한 보안을 강화하여 기존 IKEv1보다 가볍고 효율이다.

네트워크 환경이 복잡하고 다양해짐에 따라 클라우드 컴퓨팅, 가상 네트워크, SDN 환경이 더욱 보편화되고 있다. 이러한 가상 네트워크와 SDN 환경에서 보안을 강화하고 데이터를 안전하게 관리하기 위해 IPsec VPN에 대한 연구가 진행되고 있다. [8][9][10][11]

IPsec VPN 보안 감사는 데이터 보호와 기밀성 유지, 취약점 사전 식별 및 조치, 사고 대응 및 조사를 위해 필수적인 활동이다. IPsec VPN 보안 취약점에 관한 많은 연구가 수행되고 있으며, 보안 감사에 관한 연구 또한 진행되고 있다.

[7]은 VPN 솔루션에 대해 보안, 성능, 감사, 및 관리 기능을 기반으로 종합적으로 평가하기 위한 지표를 제안하였다. [5][6]는 IKEv1와 IKEv2에 대해 중간자 공격 기법을 이용한 분석 기법을 제안하였다. IPsec VPN은 서버 간 보안 터널을 생성하는 Site-to-Site 방식과 서버와 클라이언트 간 보안 터널을 생성하는 Remote Access 방식이 있다. 또한 상호 인증을 위해 사전 공유키 방식(Pre-shared Key, PSK)과 인증서 기반 방식이 있다. [5]는 Remote Access와 사전 공유키 방식, [6]는 Site-to-Site와 사전 공유키 방식의 환경에 대해 고려하였다. 중간자 공격 기반 분석 방법은 네트워크에 직접 참여하기 때문에 분석을 위해서는 일시적으로 네트워크 단절이 불가피하다. 또한, 감사 이전의 데이터를 확보할 수 없어 사고 대응 및 조사에 활용할 수 없다.

본 논문은 Site-to-Site, Remote Access 방식과 사전 공유키 방식과 인증서 기반 방식을 고려한 새로운 분석 기법을 제안한다. 제안하는 분석 기법은 네트워크에 직접 참여하지 않으며, 감사 시점 이전의 데이터에 대한 분석이 가능하여 IPsec VPN 감사에 효과적으로 사용할 수 있을 것으로 기대한다.

본 논문의 구성은 다음과 같다. II장에서는 IPsec VPN에 대해 소개하고, III장에서는 중간자 공격 기반 분석 기법들을 분석한다. IV장에서는 제안하는 분석 기법에 대해 상세히 다루고, V장에서 결론으로 마무리 한다.

II. IPsec VPN

IPsec VPN은 네트워크 보안과 데이터 프라이버시를 확보하기 위한 가장 널리 사용되는 가상 사설 네트워크 프로토콜 중 하나이다. IPsec VPN은 보안 터널을 설정하고 암호키를 교환하기 위한 IKE (Internet Key Exchange)와 데이터 기밀성과 무결성을 보장하는 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 프로토콜로 구성된다. 본 절에서는 IPsec VPN 터널모드를 위한 IKEv2와 ESP에 대해 소개한다.

IKEv2는 기존 IKEv1보다 효율적이며, 서비스 공격에 대한 안전성이 강화되었으며, ESP는 IP패킷에 대해 기밀성과 데이터 인증, 무결성을 동시에 지원한다.

2.1 IKEv2

IKEv2는 안전한 통신을 위한 키 교환과 보안 연결 설정을 위한 프로토콜이며, Fig.2와 같이 각각의 단계는 요청과 응답 메시지 쌍으로 이루어진다.

IKE_SA_INIT 메시지 쌍은 암호 알고리즘, 논스

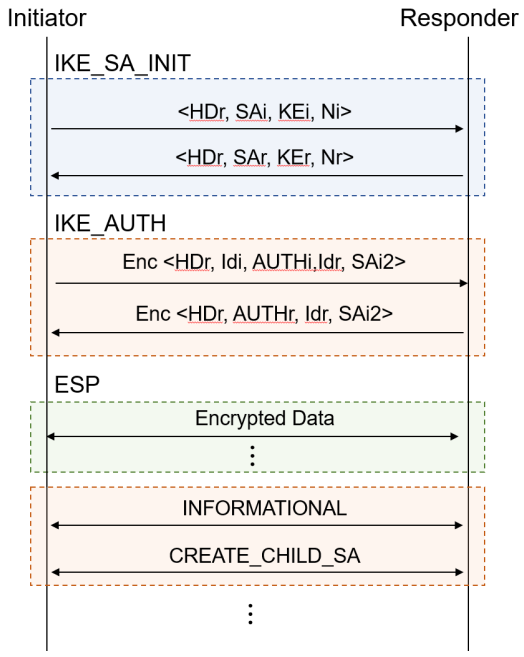


Fig. 2. IPsec VPN Establishment Process with IKEv2 and ESP

(nonce), Diffie-Hellman 파라미터 등을 교환하며, 이 과정은 IKEv2 프로토콜 최초에 수행된다. 이후, 모든 메시지들은 INIT_SA_INIT 교환 과정에서 협상된 SA(세션키, 암호 알고리즘 등)로 암호화된다.

IKE_AUTH 메시지 쌍은 Initiator와 Responder 사이에 상호 인증을 수행하고 CHILD SA를 생성한다. IKE_AUTH 메시지는 IKE_SA_INIT 단계에서 결정된 SA로 암호화되며, 상호 인증은 사전 공유키(PSK: Pre-shared Key) 방식 또는 인증서 기반 인증 방식으로 이루어진다.

CREATE_CHILD_SA 메시지 쌍은 기존 IKE SA를 새로운 IKE SA로 갱신하거나 새로운 CHILE SA를 생성 또는 갱신할 때 사용된다.

INFORMATIONAL 메시지 쌍은 설정 오류 통보, 세션 종료, IPsec VPN 노드들 사이의 환경설정 등을 위해 선택적으로 사용한다.

Table 1은 이후 사용할 IKEv2에 대한 표기법을 나타낸다.

Table 1. Notation of IKEv2

Notation	Meaning
i	Initiator
r	Responder
SA**α**	IPsec SA of user **α**
KE**α**	Diffie-Hellman public key of user **α**
N**α**	nonce of user **α**
Id**α**	Identification of user **α**
g^*ir*	Diffie-Hellman shared key
Auth**α**	Authentication payload of user **α**
m || s	concatenation of m and s
$Enc(k, msg)$	symmetric encryption of msg using key k
$prf(k, msg)$	pseudo-random function of msg using key k

2.2 ESP(IP Encapsulating Security Payload)

ESP는 IPsec VPN에서 안전한 데이터 전송을 목적으로 데이터에 대한 기밀성, 무결성 및 인증을 제공하는 보안 프로토콜이다. IPsec 터널을 통과하면 Fig. 3과 같이 New IP 헤더, ESP 헤더, 암호화된 데이터, ESP Auth 형태의 패킷이 생성된다. ESP 헤더는 Security Parameter Index(SPI)와 Sequence Number로 구성되고 원본 패킷은 ESP Trailer와 함께 암호화된다. ESP Auth는 ESP 헤더부터 암호화된 데이터까지를 인증하기 위한 코드(MAC)이다.

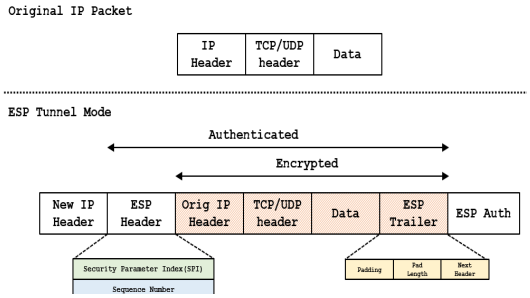


Fig. 3. IPsec ESP Packet Fomat

2.3 SA 협상 및 세션키 교환

IKEv2에서 SA와 세션키는 IKE_SA_INIT 교환 과정 이후 결정된다. Initiator는 지원 가능한 SA와 Diffie-Hellman 파라미터(KE*i*), 난수(N*i*)를 Responder에게 전달하고, Responder는 전달받은

SA 중에 지원 가능한 SA를 선택하고, 자신의 Diffie-Hellman 파라미터(KE***r***)와 난수(N***r***)를 Initiator에게 전달한다.

SA는 기밀성을 위한 암호 알고리즘, 무결성 및 인증을 위한 알고리즘(MAC), PRF(Pseudo-random Function), Diffie-Hellman 그룹 등으로 구성된다.

Initiator와 Responder는 결정된 SA를 바탕으로 Diffie-Hellman 공유키(g^***ir***)를 계산하고, N***i***, N***r***, PRF를 이용하여 SKEYSEED를 계산한다.

$$SKEYSEED = prf(N_i \| N_r, g^{ir})$$

세션키는 $SKEYSEED$를 이용하여 계산한다.

$$SK_d \| SK_{ai} \| SK_{ar} \| SK_{ei} \| SK_{er} \| SK_{pi} \| SK_{pr} = prf^{+}(SKEYSEED, N_i \| N_r \| SPI_i \| SPI_r)$$

여기서, prf^{+} 함수는 다음과 같다.

$$prf^{+}(K,S) = T1 \| T2 \| T3 \| T4$$
$$T1 = prf(K, S \| 0x01)$$
$$T2 = prf(K, T1 \| S \| 0x02)$$
$$T3 = prf(K, T2 \| S \| 0x03)$$
$$T4 = prf(K, T3 \| S \| 0x04)$$
$$\cdots$$

총 7개의 세션키가 생성되며, SK_{ei}, SK_{er}은 IKE 메시지 암호화에 사용되며, SK_{ai}, SK_{ar}은 암호화된 메시지 인증에 사용된다. SK_{pi}, SK_{pr}은 IKE_AUTH 메시지의 인증 페이로드 생성에 사용되며, SK_d는 패킷 암호화(ESP)를 위한 CHILD SA 생성에 사용된다.

IKE_SA_INIT 교환 이후 IKE_AUTH 교환 과정에서 Initiator와 Responder 사이의 상호 인증과 CHILD SA가 결정된다. 상호 인증은 사전 공유키(PSK), 디지털 서명, EAP 등의 방식이 있으며, 본 논문에서는 [5][6]과 비교를 위해 사전 공유키 방식의 상호 인증에 대해 설명한다. 인증값(Auth) 계산을 위해서는 IKE_SA_INIT 교환 과정에서 각각 송수신한 IKE_SA_INIT 메시지와 난수, 세션키, 사전 공유키 등이 필요하며, 인증값 계산은 다음과 같다.

$$octet = IKE\_SA\_INIT \| nonce \| prf(SK_p, id)$$
$$Auth = prf(prf(PSK, Key\,Pad\,for\,IKEv2), octet)$$

IKE_AUTH 과정에서 Initiator는 자신의 ID와 Responder의 ID, 인증값, 지원 가능한 SA 등을 Responder에게 전달하고, Responder는 수신한 인증값과 자신이 계산한 값과 비교하여 인증하며, Initiator 인증이 성공하면, 자신의 ID, 인증값, CHILD SA를 위한 SA를 Initiator에게 전달한다. Initiator 또한 수신한 Responder의 인증값을 인증한 후 CHILD SA를 위한 세션키와 암호 알고리즘들을 설정한다. 만약 상호 인증이 실패할 경우 통신을 종료한다.

CHILD SA를 위한 세션키는 다음과 같이 계산한다.

$$KEYMAT = prf^{+}(SK_d, N_i \| N_r) = SK_{ei} \| SK_{ai} \| SK_{er} \| SK_{ar}$$

ESP에 사용할 암호키 크기는 상호 협의된 암호 알고리즘에 따라 결정된다.

IPsec VPN은 안전성을 높이기 위해 일정 시간이 경과하면 터널에 대한 세션키(암호키)와 SA 정보를 갱신하는 키 재교환 기능이 있다. 이는 시스템에 설정된 유효기간에 따라 일정 시간이 경과하면 새로운 세션키와 SA 결정을 위해 위의 과정을 반복 수행한다.

III. 사전 연구

보안 감사는 시스템이 올바른 보안 정책을 적용하고 있으며, 암호 알고리즘, 프로토콜 등 표준을 준수하고 있는지를 확인하고, 보안 사고 발생 시 이를 분석하는 등 시스템 안전성 및 보안 진단을 위해 필요하다.

IPsec VPN은 사용자들에게 기밀성, 무결성, 인증 등을 보장하여 적은 비용으로 사설망을 구축하는 효과를 제공하지만, 네트워크 콘텐츠가 암호화되어 있어 보안 감사에는 큰 어려움이 있다. 따라서, 안전하고 효과적으로 IPsec 관리를 위해서 콘텐츠 보안 감사는 필요하다.

보안 감사는 정보 기술이 빠르게 발전하는 시대에 점점 더 중요해지고 있으며, 특히 데이터베이스 관

리, 로그 분석, 클라우드 컴퓨팅과 같은 분야에서 보안 사고에 대한 조사와 취약한 보안 구성요소에 대한 사전 조치 등에 직접 활용된다. 많은 연구자들은 IPsec VPN에 대한 취약한 구성 모드, 시간 동기화, 초기화 벡터 관련 결함[12][13][14] 등의 취약점을 조사하였다.

[5][6]은 보안 감사를 위해 중간자 공격 기법을 활용한 IPsec VPN 분석 기법을 제안하였다. 본 절에서는 중간자 공격을 이용한 분석 기법에 대해 분석한다.

3.1 중간자 공격 기반 분석 기법

중간자 공격 기반 분석 기법은 Fig. 4와 같이 분석 시스템이 Initator와 Responder 네트워크 사이에서 직접 참여한다. 이를 위해서 분석 시스템은 Initiator, Responder 사이에 공유된 키(PSK)를 사전에 알고 있어야 하며, Initiator, Responder와 각각 IKE_SA_INIT 과정을 통해 Diffie-Helleman 키교환을 수행한다. 이후, INIT_AUTH 과정에서 상호 인증을 위한 인증값(Auth)을 계산하고, 인증을 수행한다. INIT_AUTH 과정부터 ESP 패킷까지 모두 세션키로 암호화되어 있어, 분석을 위해서 복호화와 재 암호 과정이 필요하다.

3.2 사전 연구 대한 분석

중간자 공격 기반 분석 기법은 분석 시스템이 Initiator와 Responder 사이 네트워크에 직접 참여하여 Initiator, Responder와 각각 DH 공유키를 교환하고, 상호 인증값을 계산하는 등 IKE 과정에 필요한 모든 내용을 알고 있어야 한다. 중간자 공격 기반 분석 기법은 사전 공유키만 알고 있다면, Initiator와 Responder 사이의 모든 데이터에 대한 분석이 가능하지만 네트워크 성능저하, 불연속성 등과 같은 단점이 있다.

- 네트워크 성능 저하 : Initiator와 Responder 사이에서 DH 키 교환, 인증값 계산 등 세션키 및 SA 협상 단계 뿐만 아니라 INIT_AUTH 과정부터 이후 전 단계에서 복호, 재 암호 과정이 추가로 필요하기에 네트워크 성능 저하는 불가피하다.
- 네트워크 불연속성: 중간자 공격 기반 분석 기법을 적용하기 위해서는 일시적인 네트워크 단절이 필요하다. 또한 보안 감사 이전의 데이터에 대해서는 분석이 불가능하여, 사고 조사에 활용이 힘들다.
- 데이터 무단 분석: 보안 감사가 모든 데이터에 대해 항상 허용된다면 이는 도청과 같은 도덕성에 위배될 수 있다. 이전 연구는 네트워크에 적용된 이후 모든 데이터에 대해 분석이 가능하다. Remote Access 방식일 경우, VPN 서버(Responder)는 동일 사전 공유키를 사용한다. 이는 모든 클라이언트에 대한 분석이 가능함을 의미한다. IPsec VPN은 안전성을 높이기 위해 재키교환 기능이 있어, 일정 기간이 지나면 터널을 다시 생성하는데 이전 연구는 이를 무력화할 수 있다.
- 높은 수준의 구현 난이도 : 이전 연구는 Initiator와 Responder 각각과 IPsec VPN 터널을 직접 생성해야 하기에 IPsec VPN에 대한 전반적인 이해와 이를 구현할 수 있어야 한다. 또한 프로토콜 진행 상태와 이에 따른 데이터 관리가 중요하고, 통신을 위한 여러 대상을 동시에 관리해야한다.

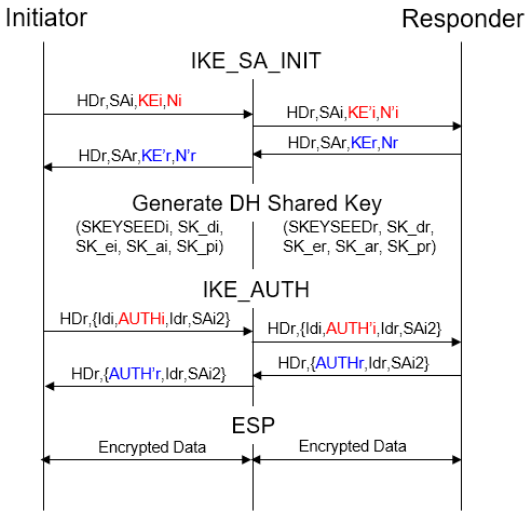


Fig. 4. Analysis Method with MITM

중간자 공격 기반 분석 기법은 네트워크 단절이 불가피하며, 성능 저하를 초래할 수 있다. 또한 사전 공유키를 통한 IPsec VPN 터널을 직접 생성할 수 있기 때문에 권한 남용 등 악용될 수도 있으며, 구현

난이도 또한 높다.

IV. 제안하는 암호화 패킷 분석 기법

본 논문은 콘텐츠 감사를 위한 새로운 분석 기법을 제안한다. 제안하는 분석 기법은 IPsec VPN 구성 방법과 상호 인증 방식에 제한되지 않으며, 보안 감사 이전에 수집된 데이터들을 분석할 수 있다. 또한, 네트워크에 직접 참여하지 않아 네트워크 연속성을 보장하며, 성능 저하를 유발하지 않는다.

제안하는 분석 기법은 ① 송수신 IP를 바탕으로 패킷을 필터링하여 분류하고, ② IKEv2 프로토콜을 분석하여 IKE SA와 CHILD SA를 위한 세션키를 계산하고, ③ 이를 이용하여 ESP 패킷을 복호화하는 절차로 이루어진다. 이전 연구와 달리 제안하는 분석 기법은 SKEYSEED(Diffie-Hellman 공유키)를 필요로 하며, 이는 IPsec VPN 서버로부터 획득이 가능하다. SKEYSEED는 터널을 생성할 때마다 만들어지기 때문에 이를 통해 감사 대상과 기간을 제한할 수 있다. 또한 제안하는 분석 기법은 수집된 IPsec VPN 패킷 분석을 자동화할 수 있다.

실험 환경은 Fig. 1과 같이 IPsec VPN 서버를 Site-to-site 방식을 구성하고, 호스트 클라이언트는 Ubuntu 20.04와 Windows 10 운영체제이며 Remote Access 환경으로 구성하였다. 상호 인증 방식은 사전 공유키 방식(PSK)과 인증서 기반 인증 방식(EAP MSCHAPv2)으로 설정한다.

4.1 패킷 분류 방법

IPsec VPN 서버는 수많은 클라이언트와 서버와 터널을 생성한다. 그에 따라 저장된 패킷들은 다양한 송·수신 IP를 가지며, 여러 프로토콜 패킷들로 구성된다. 분석을 위해서는 우선 송·수신 IP와 프로토콜(ISAKMP, ESP)에 따라 패킷들을 분류해야 할 필요가 있다.

수신한 패킷들에 대해 첫 번째로 ISAKMP(IKE) 또는 ESP 패킷인지 아닌지를 확인한다. 만약 수신한 패킷의 프로토콜이 이와 다를 경우 다음 패킷으로 넘어간다. 패킷이 ISAKMP 또는 ESP 패킷인 경우, 분류 대상 IP 쌍(송신 IP, 수신 IP)과 패킷의 IP를 비교하여 (송신 IP, 수신 IP) 또는 (수신 IP, 송신 IP)인지 확인한다. 이와 다를 경우 수신한 패킷의 송·수신 IP를 분류 대상 IP 쌍에 추가하고, 새로운 파일을 생성한다. 만약 패킷 IP가 분류 대상 IP 쌍과 동일하면 분류 대상 IP 쌍에 해당하는 파일에 추가한다. 이러한 방법으로 모든 패킷에 대해 순차적으로 적용하면 IPsec VPN 터널별로 파일이 분류된다.

이러한 방법 이외에도 패킷 필터링 도구 및 방법들을 이용하여 패킷을 분류할 수 있다.

4.2 IKEv2 분석 방법

IKEv2에서 IKE_SA_INIT 패킷은 UDP 500번 포트를 사용하며, ISAKMP 페이로드 헤더의 SPI, Version, Exchange type, Flag, Message ID 필드 값을 통해 Initiator와 Reponder를 구분할 수 있다. Fig. 5는 IKE_SA_INIT 요청 메시지로, UDP 포트는 500이며, ISAKMP 헤더에서 Responder SPI(=0), Version(=2.0), Exchange type(=IKE_SA_INIT, 34), Flag(=0x8, Initiator), Message ID(=0)를 확인할 수 있다. 또한 SA(Security Association)와 KE(Key Exchange), Nonce 페이로드에서 암호알고리즘, DH 파라미터, 난수 등을 확인할 수 있다.

Fig. 6은 이에 대한 IKE_SA_INIT 응답 메시지로 요청 메시지와 유사하나, ISAKMP 헤더의 Responder SPI와 Flag(=0x20, Responder)가 다르다. Initiator는 IKE_ SA_INIT 요청 메시지에 지원 가능한 암호 알고리즘들을 SA 페이로드를 통해 제안한다. Responder는 Initiator가 제안한 SA 중 Fig. 7과 같이 IKE SA를 결정하여 Initiator에게 응답한다. 암호 알고리즘은 AES-CBC-256, 메시지 인증은 HMAC-SHA2-256-

```
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 60c75883f20bda2b
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
  > Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  > Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000000
    Length: 1300
  > Payload: Security Association (33)
  > Payload: Key Exchange (34)
  > Payload: Nonce (40)
  > Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
  > Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
  > Payload: Notify (41) - IKEV2_FRAGMENTATION_SUPPORTED
  > Payload: Notify (41) - SIGNATURE_HASH_ALGORITHMS
  > Payload: Notify (41) - REDIRECT_SUPPORTED
```

Fig. 5. An example of IKE_SA_INIT Request

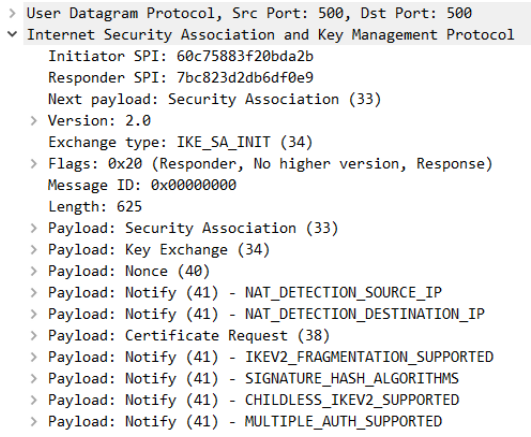


Fig. 6. An example of IKE_SA_INIT Response

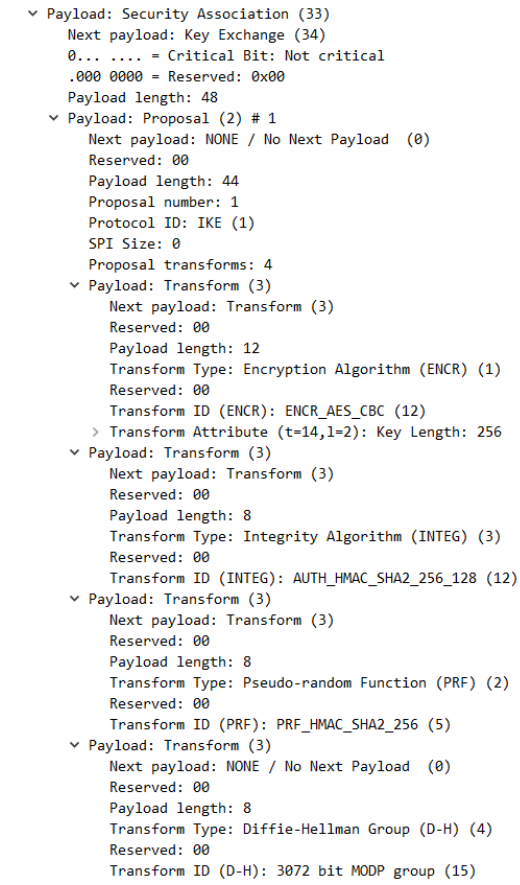


Fig. 7. SA payload of IKE_SA_INIT Response

128, PRF는 HMAC-SHA2-256, Diffie-Hellman 그룹은 3072 bits(15)로 결정됨을 알 수 있다.

IKE_SA_INIT 요청/응답 메시지 쌍으로부터 Initiator와 Responder 각각의 SPI, 난수, 그리고 암호 알고리즘들을 알 수 있다. 하지만 세션키를 계산하기 위해서는 IPsec VPN 서버로부터 SKEYSEED를 획득해야 한다. 이는 IPsec VPN 취약점 점검, 설정 확인 또는 침해사고 조사와 같은 이유로 감사가 필요한 경우, 충분히 가능하다.

IKE_SA_INIT 분석은 Initiator의 요청 메시지에서 Initiator SPI, Exchange type, Flag, Message ID를 확인하고, Initiator SPI와 Nonce를 저장한다. 이후 Responder의 응답 메시지에서 Responder SPI, Exchange type, Flag, Message ID를 확인하고, Responder SPI와 Nonce, SA를 저장한다. 이와 함께 서버로부터 획득한 SKEYSEED를 이용하여 3.3. 절에서의 계산식으로 세션키를 계산한다.

계산된 세션키과 저장된 Responder SA의 암호 알고리즘들을 이용하여 INIT_SA_INIT 이후 교환되는 메시지(IKE_AUTH, INFORMATIONAL, CHILD_SA)들을 복호화한다.

Fig. 8과 Fig.는 IKE_AUTH 메시지이며, ISAKMP 프로토콜의 페이로드 부분이 암호화되어 있다. 암호 데이터의 첫 16바이트는 암호를 위한 IV(Initial Vector)이며, 마지막 16바이트는 메시지 인증을 위한 HMAC Tag로 구성된다. IKE_AUTH 분석은 저장된 SPI를 비교하여, 동일 세션임을 확인하고, 계산한 세션키와 IV, 암호 알고리즘(AES-CBC- 256)을 이용하여 복호화를 수행한다. 암호화된 페이로드를 복호화된 페이로드로 대체하면 Fig. 9과 같이 평문 형태로 확인할 수 있다.

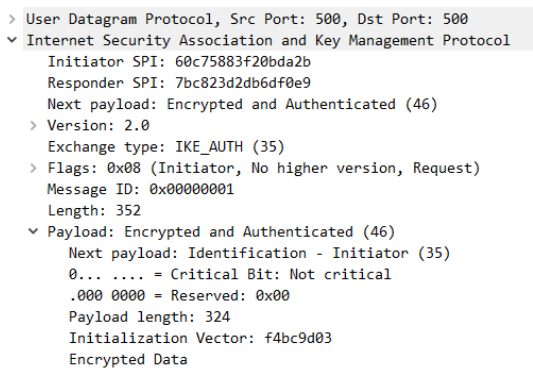


Fig. 8. Encrypted IKE_AUTH Request

```
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 60c75883f20bda2b
    Responder SPI: 7bc823d2db6df0e9
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
    Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000001
    Length: 336
  > Payload: Encrypted and Authenticated (46)
  > Payload: Identification - Initiator (35)
  > Payload: Notify (41) - INITIAL_CONTACT
  > Payload: Identification - Responder (36)
  v Payload: Authentication (39)
      Next payload: Security Association (33)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 40
      Authentication Method: Shared Key Message Integrity Code (2)
      Reserved: 000000
      Authentication Data: adf9b039806d525ab591ca959b147b41bea32c5
  > Payload: Security Association (33)
  > Payload: Traffic Selector - Initiator (44) # 1
  > Payload: Traffic Selector - Responder (45) # 1
  > Payload: Notify (41) - MULTIPLE_AUTH_SUPPORTED
  > Payload: Notify (41) - EAP_ONLY_AUTHENTICATION
  > Payload: Notify (41) - IKEV2_MESSAGE_ID_SYNC_SUPPORTED
    Extra data: 6b704b06274107a26704a40e0c470e
```

Fig. 9. Decrypted IKE_AUTH Request

4.3 ESP 분석 방법

복호화된 IKE_AUTH 메시지 Fig. 9와 Fig. 10 에서 보여주듯이 IKE_AUTH 메시지는 Initiator와 Responder의 ID, 인증값, IPSec SA 등으로 구성된다. IKE_AUTH 교환 과정에서 상호 인증이 성공하면, IPsec VPN 터널이 생성되고 이를 통해 암호통신(ESP)이 가능하다.

ESP 분석은 IKE SA 결정와 같은 방식으로 IPsec SA를 결정한다. 세션키는 3.3.절에서의

```
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 60c75883f20bda2b
    Responder SPI: 7bc823d2db6df0e9
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
    Exchange type: IKE_AUTH (35)
  > Flags: 0x20 (Responder, No higher version, Response)
    Message ID: 0x00000001
    Length: 224
  > Payload: Encrypted and Authenticated (46)
  > Payload: Identification - Responder (36)
  v Payload: Authentication (39)
      Next payload: Security Association (33)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 40
      Authentication Method: Shared Key Message Integrity Code (2)
      Reserved: 000000
      Authentication Data: 3e4929b7046c7eca0e7989e134a9594923ccdb8
  > Payload: Security Association (33)
  > Payload: Traffic Selector - Initiator (44) # 1
  > Payload: Traffic Selector - Responder (45) # 1
  > Payload: Notify (41) - AUTH_LIFETIME
    Extra data: 82cb53be04
```

Fig. 10. Decrypted IKE_AUTH Response

```
v Payload: Security Association (33)
    Next payload: Traffic Selector - Initiator (44)
    0... .... = Critical Bit: Not critical
    .000 0000 = Reserved: 0x00
    Payload length: 44
  v Payload: Proposal (2) # 1
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 40
      Proposal number: 1
      Protocol ID: ESP (3)
      SPI Size: 4
      Proposal transforms: 3
      SPI: c576da15
    v Payload: Transform (3)
        Next payload: Transform (3)
        Reserved: 00
        Payload length: 12
        Transform Type: Encryption Algorithm (ENCR) (1)
        Reserved: 00
        Transform ID (ENCR): ENCR_AES_CBC (12)
      > Transform Attribute (t=14,l=2): Key Length: 128
    v Payload: Transform (3)
        Next payload: Transform (3)
        Reserved: 00
        Payload length: 8
        Transform Type: Integrity Algorithm (INTEG) (3)
        Reserved: 00
        Transform ID (INTEG): AUTH_HMAC_SHA2_256_128 (12)
    v Payload: Transform (3)
        Next payload: NONE / No Next Payload  (0)
        Reserved: 00
        Payload length: 8
        Transform Type: Extended Sequence Numbers (ESN) (5)
        Reserved: 00
        Transform ID (ESN): No Extended Sequence Numbers (0)
```

Fig. 11. SA payload of IKE_AUTH Response

KEYMAT 계산 방식으로 구하고, 암호 알고리즘들은 Fig. 11과 같이 Responder의 IKE_AUTH 응답 메시지의 SA 페이로드로 확인한다. SA 페이로드는 ESP 프로토콜 SPI, 암호 알고리즘(AES-CBC-128), 인증 알고리즘(HMAC- SHA-256-128) 등으로 구성된다.

세션키는 결정된 암호 알고리즘의 키 크기에 따라 달라지기 때문에 알고리즘을 확인한 후 KEYMAT으로부터 구한다.

Fig. 12는 ESP 패킷이며, SPI와 Sequence Number를 제외한 부분들이 암호화되어 있으며, 첫 16바이트는 IV이며, 마지막 16바이트는 메시지 인

```
> Internet Protocol Version 4, Src: 192.168.1.128, Dst: 192.168.1.130
v Encapsulating Security Payload
    ESP SPI: 0xc47a0d96 (3296333206)
    ESP Sequence: 6

0000  00 0c 29 fe ae f4 00 0c  29 26 c4 e9 08 00 45 00   ··)····· )&····E·
0010  00 9c e8 38 40 00 40 32  cd a4 c0 a8 01 80 c0 a8   ···8@·@2 ········
0020  01 82 c4 7a 0d 96 00 00  00 06 97 f8 e8 12 a9 77   ···z···· ·······w
0030  2e fd 5a 64 12 d8 8f 41  1a 28 0e 44 8a 30 06 8e   ··Zd···A ·(·D·0··
0040  c9 49 71 c0 8a 4a f2 88  cf c2 24 21 39 fb 48 8b   ·Iq··J·· ··$!9·H·
0050  a2 5f a5 96 0c a5 b9 56  ae 94 8f 2c b7 cb 90 fb   ·_·····V ···,····
0060  e6 1a a6 c8 1b 01 91 17  64 f4 10 5c 85 eb 73 7b   ········ d··\··s{
0070  eb 83 3d 9f 5f eb 52 5f  ab ad a4 13 c8 05 d0 ab   ··=·_·R_ ········
0080  b9 45 5f c1 b2 fb 6f 6a  5b 11 98 55 15 6f 34 a9   ·E_···oj [··U·o4·
0090  cc dc 43 36 fe 6b 17 a8  6f 44 82 fb eb e5 8c 42   ··C6·k·· oD·····B
00a0  cd 12 6b a4 7c 43 f3 59  91 ba                    ··k·|C·Y ··
```

Fig. 12. An Example of ESP Packet

```
> Internet Protocol Version 4, Src: 192.168.4.100, Dst: 192.168.3.128
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d4d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 14 (0x000e)
    Sequence Number (LE): 3584 (0x0e00)
    [Response frame: 8]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656
      [Length: 32]
```

Fig. 13. Decrypted Packet of ESP(ICMP Packet)

증을 위한 HMAC Tag로 구성된다. 따라서, KEYMAT로부터 획득한 세션키와 IV, 암호 알고리즘(AES-CBC-128)을 이용하고, 복호화를 수행한다. 복호화된 패킷은 Fig. 13와 같다.

4.4 구현 및 실험 결과

본 논문에서 제안하는 분석 기법은 Fig. 14과 같다. IPsec VPN 연결은 VM1과 VM2 서버 간 연결하는 Site-to-Site 방식과 Cilent(VM3, VM4)와 서버(VM1) 간 연결하는 Remote Access 방식을 고려하였으며, 상호 인증은 PSK와 EAP MS-Chapv2 방식으로 설정하였다. Initiator (VM2,VM3,VM4)는 Responder(VM1)와 IPsec VPN 터널을 생성하고, VM1 보호대역에 있는 VM5와 ICMP를 통해 정상적으로 터널이 생성되고 암호통신이 가능하다.

이를 분석하기 위해 IKEv2와 ESP 패킷들은 VMnet1 네트워크에서 Wireshark를 이용하여 수집하고, 감사 대상 서버의 로그 파일에서 SKEY SEED(Diffie-Hellman 공유키)을 획득하였다.

제안하는 분석 기법은 python 3.10 기반으로 scapy[15]와 pycryptodome[17] 모듈을 활용하여 구현하였다. 전체 수집된 패킷들을 분류하기 위해 순차적으로 패킷을 읽어서 IKEv2 또는 ESP 패킷 여부를 판단하고, 만약 IKEv2 또는 ESP 파일이면 송·수신 IP에 따라 패킷을 분류한다.

패킷이 보안 터널에 따라 분류된 이후 IKEv2 분석과 ESP 패킷 분석 단계를 수행한다. IKEv2 분석 단계는 IKE_SA_INIT 요청 패킷을 찾는 순으로 진행된다. UDP 포트(500), Reponder SPI(0), Exchange Type(0x22), Flags(0x08), Message ID(0)를 확인하여 IKE_SA_INIT 요청 패킷 여부를 판단한다. IKE_SA_INIT 요청 패킷인 경우, IKE_SA 인스턴스를 생성하고 Initiator Header와 Nonce 정보를 저장한다. 이후, UDP 포트(500), Initiator SPI, Exchange Type (0x22), Flags(0x20), Message ID(0)를 확인하여 IKE_SA_INIT 응답 패킷 여부를 판단한다. IKE_SA_INIT 응답 패킷일 경우, IKE_SA 인스턴스에 Responder Header, SA, Nonce 정보를 추가한다. INIT_SA_INIT 요청/응답 패킷 확인 이후 서버로부터 획득한 SKEYSEED와 IKE_SA 정보 (SPI, Nonce)를 이용하여 세션키를 계산하고, 이를 IKE_SA 인스턴스에 저장한다. IKE_AUTH 패킷은 IPsec VPN 연결방식에 따라 UDP 포트가 상이하다. Site-to-Site 방식일 경우는 500번 포트를 사용하지만, Remote Access 방식은 NAT traversal로 인해 4500번 포트를 사용하며, ESP

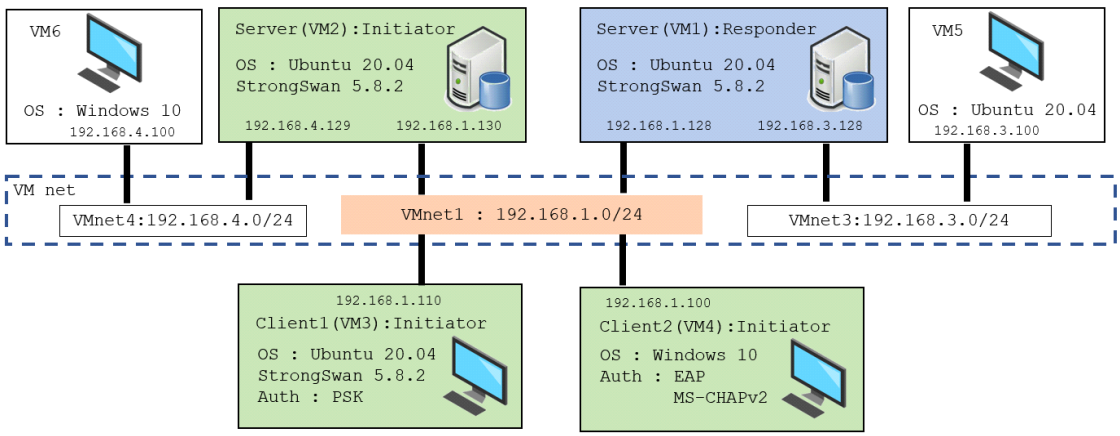


Fig. 14. Experimental environment with Virtual Machine

spi는 '0'으로 설정된다.[18] Scapy는 UDP 포트 4500번을 ESP 패킷으로 판단하기에 우리는 ESP 패킷인 경우 spi를 확인하여 '0'인 경우에는 IKEv2 패킷으로 판단하고 IKEv2 패킷으로 변환하여 처리한다.

IKE_SA_INIT 단계 이후 Initiator와 Reponder의 SPI는 동일하며, 이값은 IKA_SA 인스턴스에 저장된다. Exchange type(=0x23), Flag (=8), Message ID(=1)인 경우 IKE_AUTH 요청 패킷으로 판단하고 IKE_SA에 저장된 암호 알고리즘과 세션키를 이용하여 복호화한다. Flag (=0x20)인 경우 IKE_ AUTH 응답 패킷에 대해서도 동일한 알고리즘과 키를 이용하여 복호화한다. 복호화된 IKE_AUTH 응답 패킷의 SA 페이로드를 확인하여 ESP spi과 암호 알고리즘, 세션키를 계산하고, IPsec SA 인스턴스에 생성하고, 이에 저장한다.

이후, 수신된 ESP 패킷에 대해서 IPsec SA 인스턴스에 저장된 ESP spi를 확인하고 이에 해당하는 암호 알고리즘과 세션키를 이용하여 복호화한다.

Fig. 15는 서버 간(Site-to-site) IPsec VPN 통신에 대한 분석한 결과이며, Fig. 16는 Client와 서버 간(Remote Access) IPsec VPN 통신을 분석한 결과이다. Fig. 15은 PSK 방식이며, Fig. 16는 인증서 기반의 EAP MSCHAPv2 방식으로 EAP 프로토콜을 확인할 수 있다.

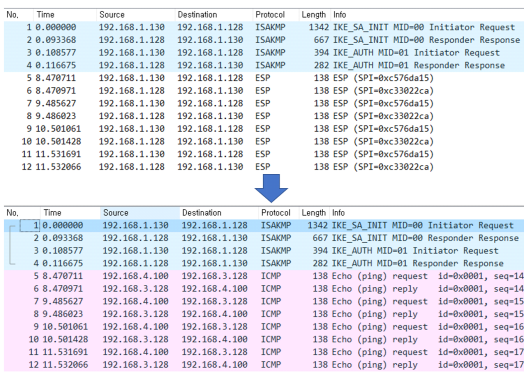


Fig. 15. Analysis Result of Site-to-site

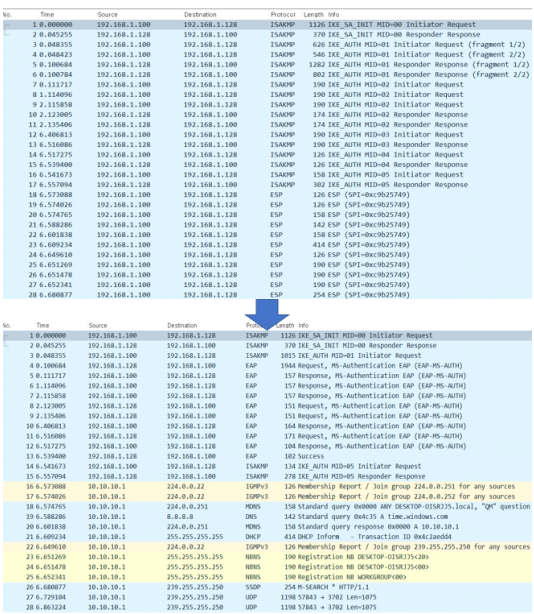


Fig. 16. Analysis Result of Remote Access

4.5 고찰

EAP MSCHAPv2과 같은 인증 방식에서 IKE_AUTH 과정에서 인증서로 인해 패킷 파편화가 발생한다. 분석 시스템은 이를 위해 데이터 파편화 여부를 확인하고 파편화가 발생한 경우 이를 합치는 과정을 필요하다. Site-to-site와 달리 Remote Access 방식일 경우에는 NAT travesal로 인해 UDP 포트가 바뀌는 부분에 대해 추가 고려가 필요하다.

본 실험에서 제안하는 분석 기법은 네트워크에 직접 참여할 필요가 없으며, IPsec VPN 서버로부터 SKEYSEED를 획득하면 IKE SA 뿐만 아니라 IPsec SA에 대한 분석이 가능함을 보였다. 또한, 실험을 통해 제안하는 분석 기법은 Site-to-site Remote Access 연결 방식과 PSK와 EAP MSCHAPv2 인증 방식에 대한 분석이 가능함을 보였다.

제안하는 분석 기법은 Initiator와 Responder 네트워크 사이에 직접적으로 참여할 필요가 없어 네트워크 연속성을 보장하고, 성능저하가 없다. 또한 보안 감사는 목적에 따라 대상과 기간이 제한되어야 한다. 제안하는 분석 기법은 보안 감사 대상과 기간에 따라 SKEYSEED에 제공함으로써 권한을 제한할 수 있다. 또한 네트워크 직접 참여로 인해 발생 가능한 실시간성과 성능 등을 고려한 구현 비용 등이 필요하지 않으며 수집된 패킷을 대상으로 자동화가 가능하다.

V. 결 론

IPsec VPN에 대한 보안 감사는 데이터 보호와 기밀성 유지를 위한 설정 정보를 확인하여 잘못된 설정 또는 구현 오류 등으로 인해 발생 가능한 취약점 사전 식별하고 조치할 수 있도록 한다. 또한, 사고 발생 시 이를 조사하기 위해 반드시 필요하다. 하지만 IPsec VPN은 사용자들에게 기밀성, 무결성, 인증 등을 보장하기 위해 네트워크 콘텐츠가 암호화되어 있어 보안 감사에는 큰 어려움이 있다.

본 논문은 암호화된 네트워크 콘텐츠를 감사하기 위해 네트워크에 직접 참여하지 않고, 효율적이고 실제적인 IPsec VPN 분석 기법을 제안한다. 수집된 대용량 암호화 데이터를 송·수신 IP와 IKEv2, ESP 프로토콜에 따라 분류하고, IKEv2 프로토콜의 각 단계별로 패킷을 분석하여 결정한 IKE SA와 서버로부터 획득한 SKEYSEED를 이용해 IKEv2를 분석한다. IKEv2 분석을 통해 IPsec SA를 결정하고, 암호화된 ESP 패킷을 복호화한다.

IPsec VPN은 목적에 따라 Site-to-site, Remote Access 등 구성방식이 다르며, 상호 인증 방식도 사전 공유키 방식, 인증서 기반 방식 등 다양하게 설정할 수 있다. 제안하는 분석 기법은 실험을 통해 특정 구성 방식과 인증 방식에도 제한되지 않으며, 네트워크 연속성을 보장하고 자동화가 가능하다. 이를 통해 효율적이고 실제적으로 활용 가능할 것을 기대한다.

References

[1] Kaufman, Charlie, et al. "RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)." (2014).

[2] Kivinen, T. "RFC 7815: Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation." (2016).

[3] Kent, Stephen. "RFC 4303: IP encapsulating security payload (ESP)." (2005).

[4] Migault, D., and T. Guggemos. "RFC 9333: Minimal IP Encapsulating Security Payload (ESP)." (2023).

[5] G. Wang, Y. Sun, Q. He, G. Xin and B. Wang, "A Content Auditing Method of IPsec VPN," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 634-639, 2018.

[6] J. Park, H. Ryu, and J. Ryou, "A Study on IKE v2 Analysis Method for RealTime," Journal of the Korea Institute of Information Security & Cryptology, 32(4), pp. 661-671, Aug. 2022.

[7] Abbas, Haider, et al. "Security Assessment and Evaluation of VPNs: A Comprehensive Survey," ACM Computing Surveys vol. 55 no. 13s, pp. 1~47, 2023.

[8] Hauser, Frederik, et al. "P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn." IEEE Access vol. 8, pp. 139567-139586, 2020

[9] Lopez-Millan, Gabriel, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia, "Towards a standard SDN-based IPsec management framework," Com- puter Standards & Interfaces, vol. 66 p. 103357, 2019.

[10] López-Millán, Gabriel, et al. "Analysis and practical validation of a standard SDN-based framework for IPsec management." Computer Standards & Interfaces, vol. 83, p.103665, 2023.

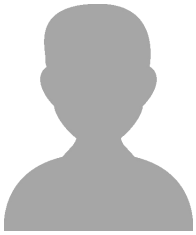
[11] Parra-Espín, José Antonio, et al. "Sdn-based automated rekey of ipsec security associations: design and practical validations." Computer Networks, vol. 233, p.109905, 2023.

[12] Hamed, Hazem, Ehab Al-Shaer, and Will Marrero, "Modeling and verification of IPSec and VPN security policies," 13th IEEE International Conference on Network Protocols (ICNP'05). pp.10, 2005.

[13] Fang, Dongxiang, Peifeng Zeng, and Weiqin Yang. "Attacking the IPsec

standards when applied to IPv6 in confidentiality-only ESP tunnel mode," 16th International Conference on Advanced Communication Technology. pp. 401-405, 2014.
〔14〕 Mizrahi, Tal. "Time synchronization security using IPsec and MACsec." 2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication. pp. 38-43, 2011.
〔15〕 Scapy, https://scapy.net, 31. Jan. 2024.
〔16〕 StrongSwan, https://www.strongswan.org, 31. Jan. 2024.
〔17〕 PyCryptodome, https://www.pycryptodome.org, 31. Jan. 2024.
〔18〕 Huttunen, A., et al. "RFC 3948: UDP encapsulation of IPsec ESP packets." (2005).

〈저자소개〉



박 정 형 (Junghyung Park) 정회원
2005년 2월: 경북대학교 전자전기공학부 졸업
2007년 2월: 포항공과대학교 전자전기공학과 석사
2007년 2월~2010년11월: LIG넥스원
2022년 2월: 충남대학교 컴퓨터공학과 박사수료
2010년12월~현재: ETRI 부설연구소
〈관심분야〉 네트워크 보안, 시스템 보안

윤 재 남 (Jaenam Yoon) 정회원
1998년 2월: 경희대학교 컴퓨터공학과 졸업
2000년 2월: 한국과학기술원 정보통신공학 석사
2000년 2월~2007년 12월: ㈜텔리언
2007년 12월~현재: ETRI 부설연구소
〈관심분야〉 네트워크 보안, 시스템 보안

류 재 철 (Jaecheol Ryou) 종신회원
1985년 2월: 한양학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남학교 컴퓨터공학과 교수
〈관심분야〉 모바일 보안, 금융보안, 블록체인