Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.4, Aug. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.4.661

NIKEv2 AR : IKE v2 실시간 분석 기술 연구

박 정 형,[1†] 유 형 열,[1] 류 재 철[2‡]
[1]국가보안기술연구소 (책임연구원), [2]충남대학교 (교수)

A Study on IKE v2 Analysis Method for RealTime

Junghyung Park,[1†] Hyungyul Ryu,[1] Jaecheol Ryou[2‡]
[1]National Security Research Institute (Principal Researcher),
[2]Chungnam National University (Professor)

요 약

코로나19 팬데믹으로 인해 재택근무와 온라인 교육이 활성화되고 이에 따라 IPsec VPN 사용이 급속히 증가하고 있다. VPN 확산에 따라 VPN 취약점은 공격자들에게 중요 공격 대상이 되고 있으며, 이와 관련된 연구가 활발히 진행되고 있다. IKE v2 분석은 IPsec VPN 시스템 개발과 구축 뿐만 아니라 안전성 분석을 위해서 필요하며, 이를 위해서 Wireshark, Tcpdump 등 네트워크 패킷 분석 도구를 이용한다. Wireshark는 네트워크 분석을 위한 대표적인 도구 중 하나이며, IKE v2 분석을 지원하지만 이를 위해서는 IPsec VPN 시스템 관리자 권한을 알아야하는 등 여러 한계점이 존재한다. 본 논문에서는 Wireshark의 한계점을 분석하고 이를 해결할 수 있는 새로운 분석 기법을 제안한다. 제안하는 분석 기법은 세션키 교환 과정부터 암호화된 모든 IKE v2 메시지를 실시간으로 분석할 수 있다. 이뿐만 아니라 제안하는 분석 기법은 네트워크 패킷 포워딩 기능을 이용하여 패킷을 조작할 수 있기에 퍼징 등과 같은 동적 테스팅에 활용될 수 있을 것으로 기대된다.

ABSTRACT

Due to the COVID-19 pandemic, remote working, e-learning, e-teaching and online collaboration have widely spread and become popular. Accordingly, the usage of IPsec VPN for security reasons has also dramatically increased. With the spread of VPN, VPN vulunerabilities are becoming an important target of attack for attackers, and many studies have been conducted on this. IKE v2 analysis is an essential process not only for developing and building IPsec VPN systems but also for security analysis. Network packet analysis tools such as Wireshark and Tcpdump are used for IKE v2 analysis. Wireshark is one of the most famous and widely-used network protocol analyzers and supports IKE v2 analysis. However Wireshark has many limitations, such as requiring system administrator privileges for IKE v2 analysis. In this paper, we describe Wireshark's limitations in detatil and propose a new analysis method. The proposed analysis method can analyze all encrypted IKE v2 messages in real time from the session key exchange In addition, the proposed analysis method is expected to be used for dynamic testing such as fuzzing as packet manipulation.

Keywords: IPsec VPN, IKE v2, MITM, Wireshark

I. 서 론

코로나19 바이러스 감염병이 전 세계적으로 대유행함에 따라 재택근무와 온라인 교육이 활성화되고 있다[10, 11]. 이에 따라 보안 솔루션이 보다 요구되고 있으며, 이를 위해 가상 사설망(VPN: Virtual Private Network) 사용이 급속히 증가하고 있다[3]. VPN 구축을 위해서는 널리 알려진 시스코 社의 ASA(Adaptive Security Appli-

Received(05. 23, 2022), Accepted(07. 04. 2022)
† 주저자, junghyung@nsr.re.kr
‡ 교신저자, jcryou@cnu.ac.kr(Corresponding author)

ance) 소프트웨어[17]와 같은 솔루션을 도입하거나 StrongSwan[14]과 같은 오픈소스 기반 IPsec VPN 솔루션을 활용할 수 있다. 또는 IPsec 표준을 참고하여 필요에 따라 최적의 솔루션을 자체 개발할 수도 있다. IPsec VPN 개발과 환경 구축 과정에서 네트워크 패킷 분석은 필요한 부분 중 하나이다. 하지만 IPsec VPN 네트워크 패킷들은 암호화되어 있어 사실상 이를 실시간 분석하기란 쉽지 않다.

VPN 사용이 증가함에 따라 VPN 취약성은 공격자들에게 중요한 공격 대상이 되고 있으며, 이와 관련된 다양한 연구가 수행되고 있다[3,4,5,6,7,8]. Y. Cui 등[4]은 IKE v2 프로토콜에 대한 퍼징을 수행하였으며, J. Guo 등[6]은 IKE v2 인증 과정에서 인증서의 ID 검증 방식에 대한 구현 결함을 확인했다. T. Kai 등[5]은 차분 퍼징 기법을 이용하여 서로 다른 솔루션의 결과 비교를 통해 구현 오류를 확인하였다. 위의 연구들에서는 IKE v2 프로토콜 분석을 위해 이를 실제 구현하여 확인하였다. 이러한 과정에서 암호화된 IKE v2 패킷 분석은 반드시 필요한 부분이며, 이를 위해서 다양한 방법을 활용했을 것으로 추측이 된다. 이 외에도 IPsec VPN에서 대두되고 있는 서비스 거부 공격 가능성[3,6]과 서비스 공격 시 시스템 성능 평가[9]에 대한 연구들도 진행되었다.

IPsec은 VPN 중 대표적인 프로토콜로서, 네트워크 계층에서 IP 패킷에 대한 인증과 기밀성을 위한 AH(Authentication Header)와 ESP (Encapsulating Security Payload), 그리고 보안 서비스 제공을 위한 SA(Security Association)를 자동으로 설정하는 IKE(Internet Key Exchange) 프로토콜로 구성된다. IKE v2는 기존 IKE v1보다 키 교환 과정을 줄여 더 가볍고 효율적이며, 서비스 거부 공격에 대한 안전성이 강화되었다[1]. 또한 IoT 디바이스와 같이 소비전력, 메모리, 처리 능력 등 리소스가 제한된 환경에서 상호 운영이 가능한 최소 구현 방법에 대해서도 제안되었다[2].

Wireshark[13]는 네트워크 분석에 활용되는 대표적인 도구로서, ICMP, TCP/UDP, HTTP, SMTP 뿐만 아니라 IKE, ESP 등 다양한 네트워크 프로토콜을 실시간으로 분석할 수 있다. IKE는 버전 1과 버전 2로 나뉘며, Wireshark에서 이를 분석하기 위해 요구되는 파라미터는 각각 다르다. IKE v1의 경우에는 Initiator의 쿠키 값과 암호키가 요구되며, IKE v2의 경우에는 Initiator와 Responder의 SPI와 세션키, 암호 알고리즘, 무결성 알고리즘이 요구된다. IKE v2 분석을 위해 요구되는 세션키는 시스템의 기밀성과 무결성 보장을 위한 가장 중요한 요소이기 때문에 안전하게 관리되어야 한다. 따라서 이를 획득하기란 쉽지 않으며, 이를 위해서는 IPsec VPN 시스템 관리자 권한이 반드시 필요하다. 하지만, 일부 장비에서는 세션키 획득이 불가능할 수도 있다.

IKE v2 실시간 분석은 IPsec VPN 시스템 개발, 분석 및 운영 중 발생 가능한 문제를 해결하는데 중요하다. Wireshark을 이용하여 IKE v2 프로토콜 분석은 가능하지만 이를 위해서는 세션키 획득과 같은 한계점이 존재한다. 본 논문에서는 이러한 한계점을 해결하는 새로운 분석 기법을 제안한다. 제안하는 기법은 MITM 방식으로 Initiator와 Responder 사이에 위치하여 송수신 패킷을 실시간으로 분석할 수 있다.

본 논문의 구성은 다음과 같다. II 장에서는 IKE v2에서의 세션키 공유 및 상호 인증과정에 대해 기술하고, III장에서는 대표적인 네트워크 분석 도구인 Wireshark에서 IKE v2를 분석하는 방법에 대해 상세히 기술하고 이에 대한 한계점을 분석한다. IV장에서는 제안하는 분석 기법과 실험 결과에 대해 분석하고 V장에서 결론으로 마무리 한다.

II. IKE v2

IKE v2는 네트워크 트래픽 보호를 위한 세션키와 여러 보안 파라미터(SA: Security Association)를 자동으로 설정하는 키 관리 프로토콜이다. IKE v2에서 SA 설정은 요청과 응답 패킷(메시지) 쌍으로 이루어지며, Fig. 1.과 같이 IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL로 구성된다.

IKE_SA_INIT 교환 과정에서는 이후 교환되는 메시지들을 보호하기 위한 세션키와 암호 알고리즘 등의 IKE SA를 결정한다. 세션키는 Diffie-Hellman 키 교환 프로토콜과 몇 가지 암호연산을 통해 생성되며, 사용할 암호 알고리즘은 Initiator와 Responder에서 지원하는 암호 수트(cipher suites)를 서로 확인하여 결정한다.

IKE_AUTH 교환 과정에서는 상호 인증과 CHILD SA를 결정한다. IKE_AUTH 메시지는 IKE_SA_INIT 교환 과정에서 결정된 SA(세션키

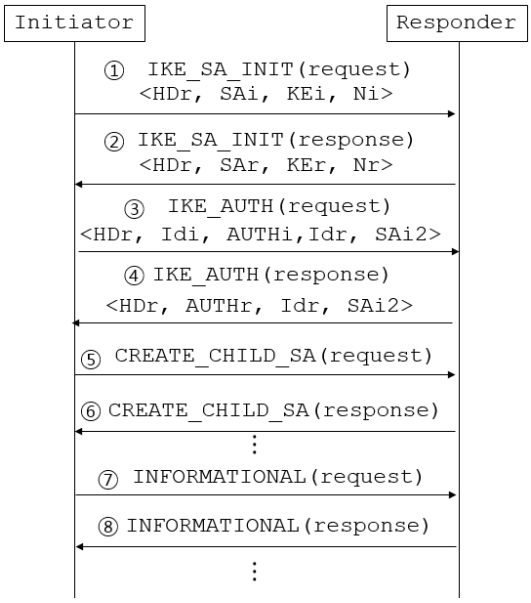


Fig. 1. An example of IKE v2 session

및 암호 알고리즘)로 암호화되며, 상호 인증은 사전 공유키(PSK: Pre-shared key) 방식 또는 디지털 서명 방식으로 이루어진다.

CREATE_CHILD_SA 교환 과정은 두 가지 목적에 따라 사용된다. 첫 번째는 기존 IKE SA를 새로운 IKE SA로 갱신하는 것이며, 두 번째는 새로운 CHILD SA를 생성하거나 기존 CHILD SA를 갱신하는 것이다.

INFORMATIONAL 교환은 오류 통지 또는 세션 종료, IPsec VPN 노드들 사이의 환경설정 등을 위해 선택적으로 사용한다.

본 장에서는 IKE v2에서 IKE_SA_INIT과 IKE_AUTH 교환 과정에서 이루어지는 세션키 생성과 상호 인증 과정에 대해 상세히 기술한다. Table 1.은 이후 사용할 IKE v2 표기법을 나타낸다.

Table 1. Notation of IKE v2

Notation	Meaning
HDr	IKE header
i	Initiator
r	Responder
AUTH**α**	Authentication payload of user **α**
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
m | s	concatenation of m and s
Enc(k, msg)	symmetric encryption of msg using key k
prf(k, msg)	pseudorandom function of msg using key k

2.1 IKE_SA_INIT

IKE v2에서 세션키는 Fig. 1과 같이 IKE_SA_INIT(①, ②) 교환 과정 이후 생성한다. Initiator는 ① IKE_SA_INIT 메시지에 암호 알고리즘을 포함하는 SA**i**와 함께 Diffie-Hellman 공개키 KE**i**, 난수 N**i**를 Responder에게 전송한다. Responder는 Initiator가 제공한 암호 알고리즘 중에서 지원 가능한 것을 선택하고 이를 포함하는 SA**r**과 Diffie-Hellman 공개키 KE**r**, 난수 N**r**을 Initiator에게 전송한다. 이 과정에서 Initiator와 Responder는 서로 난수 N**i**, N**r**과 Diffie-Hellman 공유 키, PRF(pseudorandom function)을 이용하여, SKEYSEED를 계산한다.

$$SKEYSEED = prf(N\mathbf{i}|N\mathbf{r}, g\hat{}ir)$$

이후, 세션키는 SKEYSEED를 이용하여 계산한다.

$$\{SK\_d|SK\_ai|SK\_ar|SK\_ei|SK\_er|SK\_pi|\ SK\_pr\} = prf+(SKEYSEED, N\mathbf{i} \mid N\mathbf{r} \mid SPI\mathbf{i} \mid SPIr)$$

여기서, prf+ 함수는 다음과 같다.

$$prf+(K, S) = T1 \mid T2 \mid T3 \mid T4$$
$$T1 = prf(k, s|\ 0x01)$$
$$T2 = prf(k, T1 \mid s \mid 0x02)$$
$$T3 = prf(k, T2 \mid s \mid 0x03)$$
$$T4 = prf(k, T3 \mid s \mid 0x04)$$
$$\cdots$$

총 7개의 세션키가 생성되며, 이 중 SK_d는 인증 페이로드(AUTH payload)와 CHILD SA 생성에 필요하며, SK_ei, SK_er은 데이터 암호화에

사용된다. SK_ai, SK_ar은 암호화된 데이터 인증에 필요하며, SK_pi, SK_pr은 인증 페이로드 생성에 사용된다.

2.2 IKE_SA_AUTH

IKE_AUTH 교환 과정에서는 사용자 상호 인증과 CHILD SA를 결정한다. 사용자 상호 인증은 사전 공유키(PSK) 또는 디지털 서명 방식으로 이루어진다. 본 논문에서는 사전 공유키 방식의 상호 인증에 기반하여 설명한다. 인증 페이로드 계산을 위해서는 IKE_SA_INIT 교환 과정에서 각각 송신한 INE_SA_INIT 메시지와 난수, 세션키, 사전 공유키 등이 필요하며, AUTH 계산 방식은 아래와 같다.

octet = IKE_SA_INIT|Nonce|prf(SK_p, Id)
AUTH = prf(prf(PSK, "Key Pad for IKEv2"), octet)

따라서, Initiator의 AUTH**i**는

octet**i** = ①IKE_SA_INIT|N**r**|prf(sk_pi, Id**i**)
AUTH**i** = prf(prf(PSK, "Key Pad for IKEv2"), octet_i)

이며, Responder의 AUTH_r은

octet**r** = ②IKE_SA_INIT|N_i|prf(sk_pr, Id**r**)
AUTH**r** = prf(prf(PSK, "Key Pad for IKEv2"), octet**r**)

이렇게 계산된 결과는 IKE_AUTH 메시지의 AUTH payload로 전송된다.

IKE_AUTH 메시지는 IKE_SA_INIT 교환 과정에서 결정된 암호 알고리즘과 세션키로 암호화되며, 메시지 무결성과 인증을 위한 MAC Tag도 함께 생성된다.

III. IKE v2 분석

본 절에서는 대표적인 네트워크 패킷 분석 도구인 Wireshark에서 IKE v2를 분석하는 방법에 대해 상세히 설명한다. 이를 위해 우선 실험 환경 구성하고 세부 분석 과정을 설명한다. 이후 Wireshark이 가지는 한계점에 대해 분석한다.

3.1 실험 환경 구성

IKE v2 분석을 위한 실험 환경은 Fig.2와 같이 Windows 10 호스트 PC 상에 VMware 15 pro를 이용하여 가상환경을 구성하여 Ubuntu 20.04 운영체제와 오픈소스 IPsec VPN 솔루션 StrongSwan 5.8.2를 설치하였다. 네트워크는 VMware에서 제공하는 가상 네트워크(VMnet)로 구성하였으며, 상세 내용은 다음과 같다. VM1과 VM2는 VMnet1에 서로 연결하고, VM1의 내부 네트워크는 VMnet11, VM2의 내부 네트워크는 VMnet10에 각각 연결하였다. VMnet의 경우 네트워크 허브와 같이 동작하기에 Wireshark는 호스트 PC에 설치하였다. 가상환경이 아닌 실제 IPsec VPN 시스템 사이에 Wireshark를 설치할 경우 스

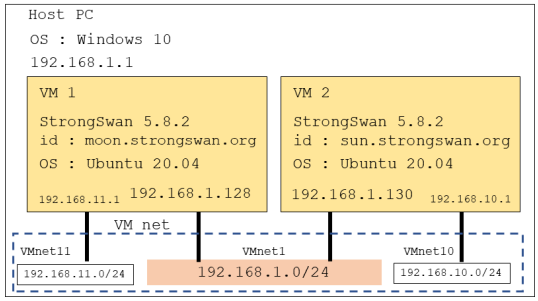


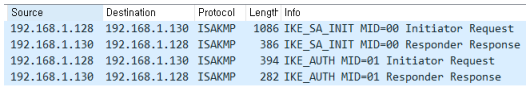
Fig. 2. IKE v2 Experimental environment

```
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        authby=secret
        ike=aes256-sha256-modp1024
        keyexchange=ikev2
        mobike=no

conn net-net
        left=192.168.1.128
        leftsubnet=192.168.11.1/24
        leftid=@moon.strongswan.org
        right=192.168.1.130
        rightsubnet=192.168.10.1/24
        rightid=@sun.strongswan.org
        auto=add
```

Fig. 3. Configuration of StrongSwan IPsec VPN



Source	Destination	Protocol	Length	Info
192.168.1.128	192.168.1.130	ISAKMP	1086	IKE_SA_INIT MID=00 Initiator Request
192.168.1.130	192.168.1.128	ISAKMP	386	IKE_SA_INIT MID=00 Responder Response
192.168.1.128	192.168.1.130	ISAKMP	394	IKE_AUTH MID=01 Initiator Request
192.168.1.130	192.168.1.128	ISAKMP	282	IKE_AUTH MID=01 Responder Response

Fig. 4. IKE v2 message exchange for tunnel in Wireshark

위치의 포트 미러링 기능 또는 전용 네트워크 탭 장비를 이용하여 연결해야 한다.

StrongSwan은 Site-to-Site 방식으로 설정하였으며, 상세 설정은 Fig.3과 같다. 인증은 사전 공유키(authby=secret) 방식이며, IKE 버전은 IKE v2(keyexchange=ikev2)로 설정하였다.

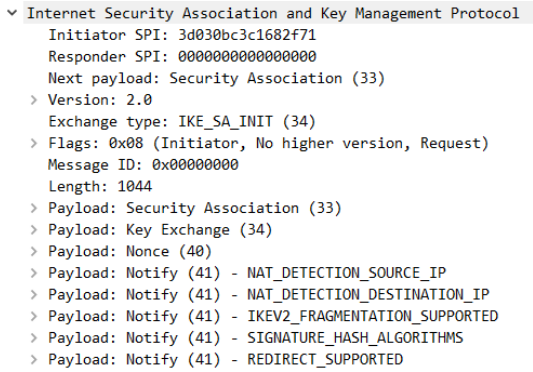
IPsec VPN 터널을 생성하고 이를 호스트 PC에 설치한 Wireshark로 그 과정을 확인하면 Fig.4와 같으며, IKE_SA_INIT과 IKE_AUTH 교환 과정을 통해 터널이 생성되었음을 확인할 수 있다. 이때, VM1은 Initiator로, VM2는 Responder로 동작하였다.

3.2 Wireshark를 이용한 분석

Wireshark는 Tcpdump[15]와 함께 대표적인 네트워크 분석도구이며, 네트워크 문제 분석, 소프트웨어 및 통신 프로토콜 개발 및 교육 등에 널리 활용되고 있다. Wireshark는 IKE v2 뿐만 아니라 TCP/UDP, SMTP, SIP 등 다양한 통신 프로토콜 분석을 지원한다.

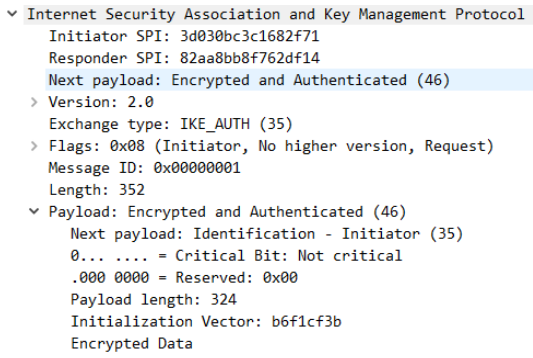
IKE_SA_INIT 메시지는 Fig.5와 같이 IKE 헤더, SA, KE, Nonce 등으로 구성된다.

IKE_SA_INIT 교환 과정을 거친 후 Initiator와 Responder는 암호 알고리즘을 결정하고, Diffie-Hellman 키 정보를 이용하여 세션키를 생성한다. 이후 교환되는 IKE_AUTH 메시지를 Wireshark에서 확인하면 Fig.6과 같이 IKE 헤더 이후 페이로드는 암호화되어 세부 정보를 확인할 수 없다. 이뿐만 아니라 이후 송수신되는 CREATE_CHILD_SA, INFORMATIONAL 메시지 또한 암호화되어 Wireshark로는 그 내용을 확인할 수 없다. 하지만, Wireshark는 IKE_AUTH와 같이 암호화된 IKE v2 메시지를 분석할 수 있는 기능을 제공한다. 이를 위해서는 IKE 헤더의 SPI, 결정된 암호 및 무결성 알고리즘, 세션키(SK_er, SK_er, SK_ai, SK_ar)를 알아야 한다. SPI와 암호 및 무결성 알고리즘은 IKE_SA_INIT 교환 과정을 확인



```
Internet Security Association and Key Management Protocol
    Initiator SPI: 3d030bc3c1682f71
    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: 1044
  > 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. IKE_SA_INIT exchange message



```
Internet Security Association and Key Management Protocol
    Initiator SPI: 3d030bc3c1682f71
    Responder SPI: 82aa8bb8f762df14
    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: 352
  v Payload: Encrypted and Authenticated (46)
      Next payload: Identification - Initiator (35)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 324
      Initialization Vector: b6f1cf3b
      Encrypted Data
```

Fig. 6. IKE_AUTH exchange message

하여 알 수 있으나, 세션키 정보는 쉽게 확인할 수 없다. 세션키는 IKE v2의 기밀성과 무결성을 보장하기 위한 가장 중요한 정보이기에 안전하게 관리되기 때문이다.

StrongSwan의 경우 시스템 관리자 권한으로 로그 레벨을 상향 조정하여야 세션키 정보를 확인할 수 있다. Fig.7은 StrongSwan의 로그 레벨을 상향 조정 후 IPsec VPN 터널 생성 과정에서 획득한 세션키 정보이다. Ubuntu 20.04는 기본적으로 AppArmor 기능이 활성화되어 로그 파일 생성이 차단된다. 따라서 로그 파일 생성을 위해서는 AppArmor 기능을 비활성화해야 한다.

Wireshark에서 IKE v2에서 암호화된 메시지를 분석하기 위해서 Edit → Preferences → Protocol → ISAKMP(IKEv2) 순으로 메뉴를 선택하고, Initiator's SPI, Responder's SPI, SK_ei, SK_er, Encrypt algorithm, SK_ai, SK_ar, Integrity algorithm을 차례로 입력해야 한다.

```
SKEYSEED => 32 bytes @ 0x7f595c001930
   0: 60 15 8D 63 7C 56 47 39 61 65 4E 17 62 6F 1A 18
  16: E2 E0 B8 75 78 4D AA 48 72 C1 26 1C 57 8A F9 E7
Sk_d secret => 32 bytes @ 0x7f595c001930
   0: CC 31 41 CC 94 EE 80 E5 C0 B8 96 8B DF 2D 07 F8
  16: 92 62 ED 3D AF 5A 0F 6D 4B EB 4C 56 CF F7 2E DF
Sk_ai secret => 32 bytes @ 0x7f595c0025a0
   0: 27 F2 C5 FD 7B FD C8 20 E9 F1 74 F4 46 42 35 66
  16: A7 8C B6 3E 80 16 DD D4 9C B4 93 8A BA 95 01 FB
Sk_ar secret => 32 bytes @ 0x7f595c004820
   0: 29 C4 16 DB 19 54 0E 8C A2 99 00 03 FF 57 A8 FC
  16: 90 84 63 8C 79 C2 F0 8F 85 D5 DF DD EC D4 D6 AA
Sk_ei secret => 32 bytes @ 0x7f595c004850
   0: C2 1D 58 9E D7 B6 67 5F 09 07 FA 61 C8 E1 5B DC
  16: 00 D6 61 D0 DA DE BC 10 21 18 24 CB B1 AC 03 96
Sk_er secret => 32 bytes @ 0x7f595c004ac0
   0: 08 D7 96 5F DD 7A D1 96 56 E4 23 E7 CB FA F1 10
  16: D8 B8 07 F6 12 10 3E 8B 16 F3 9D ED B4 39 71 9F
Sk_pi secret => 32 bytes @ 0x7f595c004ac0
   0: 01 4B CD 78 7E 6F 5A 05 11 69 64 ED 90 AF 8A 1A
  16: E6 70 9A BD 8B 3D 42 C1 8B CE 12 56 92 03 76 10
Sk_pr secret => 32 bytes @ 0x7f595c004850
   0: 3A 08 0A AA E8 8D AC BA 4A E2 11 F5 B1 1C D8 1D
  16: 53 5D 07 06 E8 01 5A 4B 3C F0 65 67 46 7C 63 46
```

Fig. 7. Log for session key in StrongSwan

3.3 Wireshark를 이용한 분석 결과

Wireshark에서 분석한 IKE_AUTH 메시지는 Fig.8과 같으며, Fig.6에서 Ecrypted Data 부분이 복호화되어 각각의 페이로드를 확인할 수 있다. 또한, 암호화된 메시지에 대한 무결성을 위한 Integrity Checksum Data도 확인할 수 있다.

```
▾ Internet Security Association and Key Management Protocol
    Initiator SPI: 3d030bc3c1682f71
    Responder SPI: 82aa8bb8f762df14
    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: 352
  ▾ Payload: Encrypted and Authenticated (46)
      Next payload: Identification - Initiator (35)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 324
      Initialization Vector: b6f1cf3b55768d9be2aed53b5524baf
      Encrypted Data (288 bytes) <AES-CBC-256 [RFC3602]>
    ▾ Decrypted Data (288 bytes)
      ▾ Contained Data (273 bytes)
          › Payload: Identification - Initiator (35)
          › Payload: Notify (41) - INITIAL_CONTACT
          › Payload: Identification - Responder (36)
          › Payload: Authentication (39)
          › 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_SUPP
        Padding (14 bytes)
        Pad Length: 14
      Integrity Checksum Data: 17ed7ef660964063a946dfde13eff
```

Fig. 8. The result of decrypted IKE_AUTH by Wireshark

Wireshark에서 IKE_ATUH 메시지를 분석한 결과 Initiator와 Responder ID, 사용자 인증을 위한 Authentication, CHILD SA, Traffic Selector 등으로 구성되어 있음을 확인하였다.

3.4 Wireshark 한계점

Wireshark에서 암호화된 IKE v2 패킷 분석이 가능하였다. 하지만 이러한 과정에서 몇가지 한계점을 확인하였다.

Wireshak는 IKE v2 분석을 위해 세션키 정보가 반드시 필요하다. 하지만 세션키는 시스템의 기밀성과 무결성 보장을 위해 안전하게 보호되어야 할 자산이기 때문에 시스템 관리자 이외에는 접근이 불가하며, 특히 하드웨어 장비의 경우 접근이 불가능할 수도 있다.

만약, 세션키를 시스템으로부터 획득할 수 있더라도 분석을 위해서는 매 세션마다 세션키를 수동으로 입력해 주어야 한다. 또한 Wireshark을 이용하기 위해서는 스위치의 포트 미러링 기능 또는 전용 네트워크 탭 장비를 사용해야 하며, 이 경우에도 네트워크 패킷 모니터링 기능만 제공한다.

IV. MITM 방식을 이용한 실시간 분석 기술

본 장에서는 IKE v2 분석에 있어 Wireshark가 가지는 한계점을 해결할 수 있는 새로운 분석 기술에 대해 제안한다.

4.1 제안하는 분석 기법(NIKEv2 AR: New IKEv2 Analyzer for Realtime) 개요

Wireshark 한계점을 해결하기 위해서는 다음과 같은 3가지 조건을 만족해야 한다.

1. IPsec VPN 시스템으로부터 세션키 획득을 하지 않아야 한다.
2. 매 세션마다 세션키를 자동 갱신할 수 있어야 한다.
3. 모니터링 기능 뿐만 아니라 캡쳐된 패킷을 동적 테스팅에도 활용 가능해야 한다.

기존 네트워크 스위치 및 전용 탭 장치 대신 제안하는 기술은 IPsec VPN 시스템 사이에서 네트워크 패킷 포워딩 기능을 활용한다. 이를 위해 물리적 네

트워크 카드를 2개 사용하며, 각각 IPsec VPN 시스템과 연결한다. 네트워크 패킷 포워딩 이용하여 Initiator에서 수신한 패킷은 Responder로, 반대로 Responder에서 수신한 패킷은 Initiator로 전송한다. 이를 기반으로 MITM 방식으로 Initiator에게는 Responder로, Responder에게는 Initiator로 동작하여 세션키를 생성한다. 이러하기에 제안하는 분석 기법은 매 세션마다 세션키를 시스템으로부터 획득할 필요가 없다.

하지만 제안하는 기법은 상호 인증을 위해 Initiator와 Responder의 ID, 사전 공유키를 알고 있어야 한다. 사전 공유키는 시스템 관리자 권한으로만 접근이 가능하나, 분석을 위해 단 한번만 확인하면 되기에 매 세션마다 확인이 필요한 Wireshark보다 효율적이다.

4.2 패킷 포워딩

패킷 포워딩은 들어온 패킷의 헤더 정보를 이용하여 최종 목적지 네트워크를 향해 패킷을 내보내 주는 일련의 단계를 말한다. 본 논문에서는 맥주소 기반의 패킷 포워딩 기능을 이용한다. 즉, IPsec VPN 시스템 사이에서 Initiator로부터 수신한 네트워크 패킷은 Responder로 전달하고, Responder로부터 수신한 네트워크 패킷은 Initiator로 전달한다. 이를 위해서는 두 가지 방법이 있다. 첫 번째는 IPsec VPN들 사이에 물리적으로 직결하는 방법이고, 이 경우에는 이더넷 어댑터 1에서 수신한 패킷을 어댑터 2로 단순 전달만 하면 된다. 두 번째는 Fig.9와 같이 IPsec VPN 시스템의 외부 네트워크에서 게이트웨이로 동작하는 방식이다. 이 경우, Initiator에서 수신한 네트워크 패킷의 수신 맥주소가 어댑터1이고 송신 맥주소가 Initiator이기에 수신 맥주소는 Responder로, 송신 맥주소는 어댑터2로 각각 변경하고 어댑터2를 이용해 Responder로 전송해야 한다. Responder에서 수신한 패킷 또한 동일한 방법으로 맥주소를 변경하여 Initiator로 전달한다.

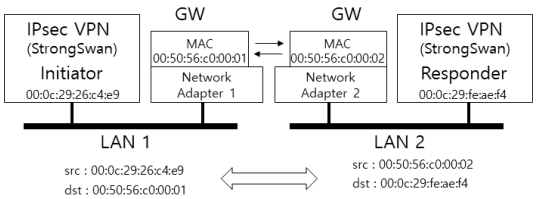


Fig. 9. Packet forwarding in Proposed method

제안하는 분석 기법은 네트워크 패킷 포워딩 기능을 이용하기에 IKE v2 패킷에 대한 실시간 변조 뿐만 아니라 드롭, 재전송을 가능하게 한다. Y. Cui 등은 [4]에서 IPSec 시스템인 ASA에 대해 IKEv2 패킷 변조를 통한 퍼징을 수행하였다. 제안하는 분석 기법 또한 IKEv2 패킷의 페이로드와 필드를 변조할 수 있으며, 패킷 재전송 및 순서 변경 등의 기능을 제공하기에 IPsec VPN 시스템에 대한 퍼징과 같은 테스팅에 활용할 수 있다.

4.3 IKE_SA_INIT 교환 과정

Initiator는 IKE SA를 위해 IKE_SA_INIT 메시지를 Responder에게 전달한다. IKE_SA_INIT 메시지는 암호 알고리즘 등을 포함하는 SA(security association)와 세션키 공유를 위한 KE(key exchange), Nonce 등으로 구성된다.

제안하는 분석 기법(NIKEv2 AR)은 Initiator와 Responder 사이에서 네트워크 패킷 포워딩 기능을 기반으로 Fig.10과 같은 과정을 수행한다.

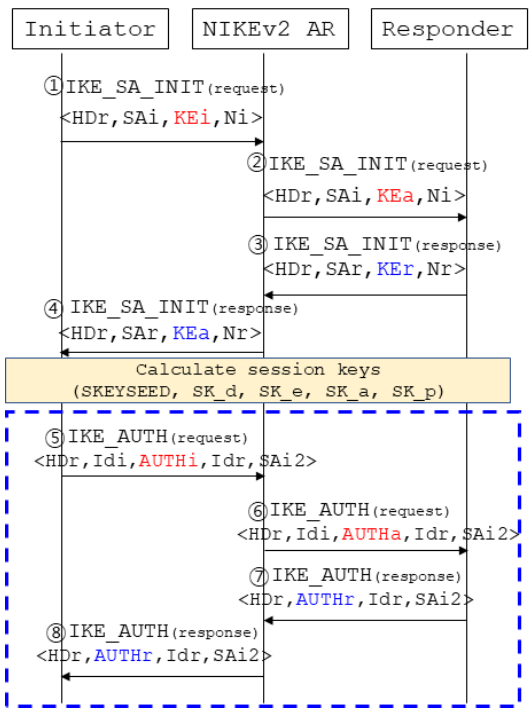


Fig. 10. Proposed method(NIKEv2 AR)

① Initiator로부터 IKE_SA_INIT을 수신하면 NIKEv2 AR은 KE를 생성한다. ② 수신한 IKE_SA_INIT 메시지의 KE 페이로드를 생성한 KE로 변경하여 Responder에게 전송한다. ③ Responder로부터 IKE_SA_INIT을 수신하면 ①과 같은 방식으로 KE를 생성하고, ④ 수신한 IKE_SA_INIT 메시지의 KE 페이로드를 생성한 KE로 변경하여 Initiator에게 전송한다.

IKE_SA_INIT 단계를 마치면 제안하는 분석 기법(NIKEv2 AR)은 각각 Initiator, Responder와 세션키를 공유한다.

4.4 IKE_AUTH 교환 과정

Initiator와 Responder는 IKE_SA_INIT 교환 이후 각각 세션키를 생성한다. 이후 Initiator는 공유한 세션키 정보와 자신의 ID를 이용하여 인증값을 계산하고 이를 인증 페이로드(AUTH payload)로 전송한다.

IKE_AUTH 메시지는 IKE 헤더, 세션키(SK_e, SK_a)로 암호화된 페이로드와 암호화된 메시지에 대한 무결성 코드로 구성된다. 제안하는 분석 기법(NIKEv2 AR)은 Fig.10과 같이 ⑤ Initiator로부터 IKE_AUTH 메시지를 수신하면 다음과 같은 과정을 수행한다. a. 수신한 IKE_AUTH 메시지에 대한 무결성 코드를 계산하고 수신한 값과 비교하여 무결성 여부를 확인한다. b. 세션키를 이용하여 암호화된 페이로드를 복호화하고 수신한 인증 페이로드를 자신이 계산한 인증 페이로드로 교체한다. c. Responder와 공유한 세션키로 페이로드를 암호화한다. d. 암호화된 메시지에 대한 무결성 코드를 계산하여 메시지 마지막에 추가한다. 이러한 과정을 거친 후 ⑥ Responder로 메시지를 전송한다.

Responder로부터 IKE_AUTH 메시지를 수신하면 위와 동일한 과정을 거친 후 Initiator에게 메시지를 전송한다.

4.5 구현 및 실험 결과

본 논문에서 제안하는 분석 기법에 대한 실험 환경은 Fig.11과 같다. Initiator와 Responder를 서로 다른 로컬 네트워크로 연결하고, 호스트 PC를 게이트웨이로 설정한다. 그 밖의 설정은 기존 Wireshark 분석 환경과 동일하다.

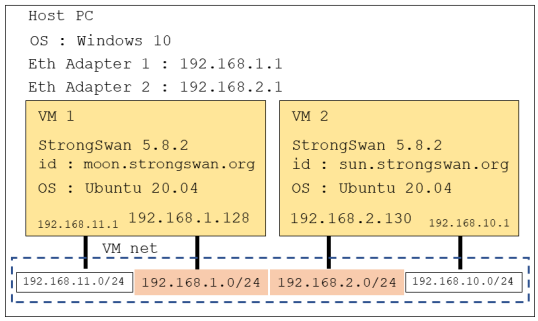


Fig. 11. Experimental environment for NIKEv2 AR

제안하는 분석 기법은 python 3.9 기반으로 scapy[12]와 pycryptodome[16] 모듈을 활용하여 구현하였다. 키교환은 Diffie-Hellman Group 중 modp 1024, 암호 알고리즘은 AES256 CBC, 무결성 알고리즘은 SHA256기반 HMAC을 각각 사용하였다.

이 외의 암호학적 알고리즘에 대해서도 IKE SA 결정을 위한 IKE_SA_INIT 또는 CREATE_CHILD_SA 메시지의 SA 페이로드를 확인하여 적용할 수 있다.

제안하는 분석 기법(NIKEv2 AR)은 Intiator와 Responder에게 송수신하는 모든 패킷들을 실시간으로 저장할 수 있으며, 이를 확인하면 Fig.12와 같다.

①번 과정에서 NIKEv2 AR은 Initiator로부터 IKE_SA_INIT을 수신하면, Fig. 13과 같이 KE를 새로 생성하고, 이를 Responder에게 전달한다.

②번 과정도 ①번과 같은 방식으로 Responder로부터 수신한 IKE_SA_INIT 메시지를 Initiator에게 전달한다.

③번 과정에서 NIKEv2 AR는 Initiator로부터 IKE_AUTH를 수신하면 Fig.14과 같이 이를 복호화하고 AUTH payload를 Fig.15와 같이 변경한 후 암호화하여 Responder에게 전송한다.

④번 과정도 ③번과 같은 방식으로 Responder로

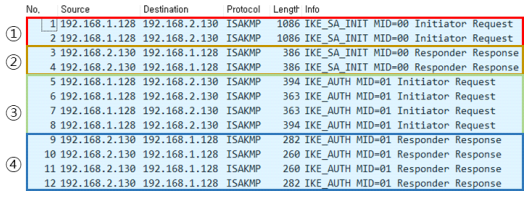


Fig. 12. Saved packet in Proposed method

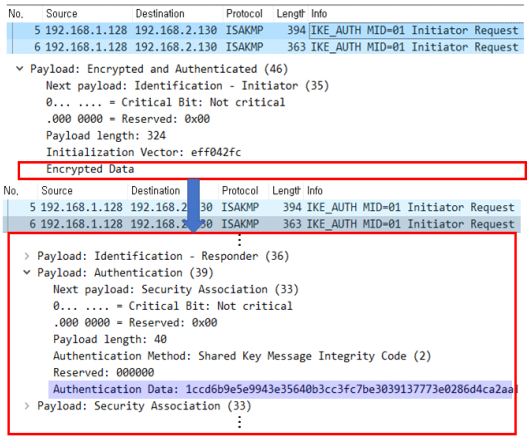


Fig. 13. Generate KE and replace IKE_SA_INIT

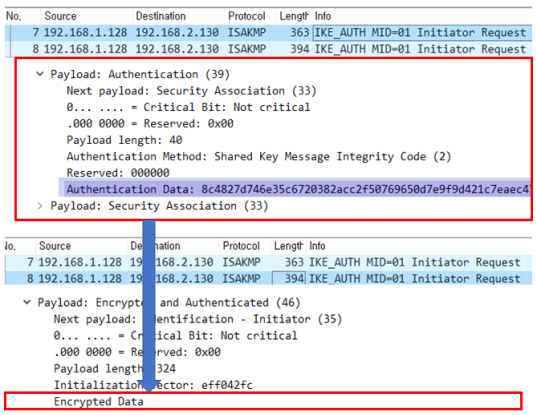


Fig. 14. Decrypted payload of received IKE_AUTH from Initiator

부터 수신한 IKE_AUTH 메시지를 Initiator에게 전달한다.

실험 결과를 통해 Initiator와 Responder ID와 인증을 위한 사전 공유키만 알고 있다면 제안하는 분석 기법(NIKEv2 AR)은 시스템으로부터 세션키 획득 없이도 IKE v2를 실시간 분석할 수 있다.

4.6 고찰

실험 결과를 통해 제안하는 분석 기법은 IKE v2 프로토콜의 모든 패킷에 대해 실시간으로 분석하고, Wireshark이 가지는 한계점을 극복함을 보였다. Wireshark의 한계점에 대해 정리하면, ① 매 세션마다 관리자 권한으로 세션키를 확보해야 하며, ② IKE v2 프로토콜에 대해 실시간 분석이 어렵다. 또

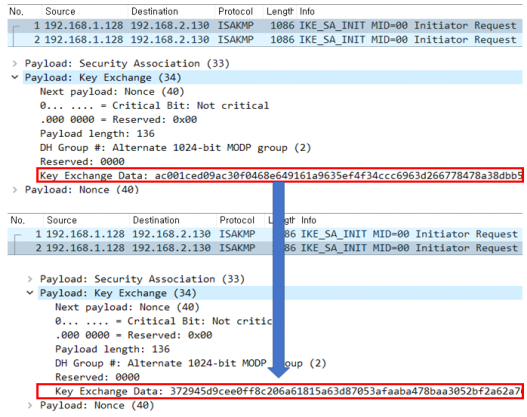


Fig. 15. Replacement AUTH payload and encryption of IKE_AUTH payload

한 ③ 패킷 캡처를 위해 네트워크 스위치 미러링 기능 또는 전용 탭 장비가 필요하다. 이에 비해 제안하는 분석 기법은 사전 공유키 획득을 위해 단 1회만 관리자 권한이 필요하며, IKE v2 프로토콜 실시간 분석이 가능하다. 또한 IPsec 시스템 사이에 직접 연결이 가능하여 추가적인 네트워크 장치가 필요하지 않을 뿐만 아니라 IPsec 시스템 간 송수신되는 네트워크 패킷을 드롭, 재전송, 변조할 수 있어 IPsec 시스템 테스팅에 활용할 수 있다.

본 논문에서 네트워크 포워딩 환경에서 MITM을 이용하여 분석 기법을 적용하였다. 이러한 방식은 IKE v2 이외에도 다양한 보안 프로토콜에도 적용할 수 있을 것이다.

V. 결 론

IKEv2 프로토콜은 IPsec VPN을 위한 키 관리 프로토콜이다. IKEv2 프로토콜은 IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL로 구성된다. IKE_SA_INIT 교환 과정에서는 IKE SA를 위한 정보가 교환되고, 이를 통해 세션키가 생성된다. 세션키 생성 이후에는 모든 메시지들이 암호화되어 전송되기 때문에 각 메시지의 payload를 확인하기는 힘들다.

Wireshark는 IKEv2 프로토콜 뿐만 아니라 SIP, SMTP 등 다양한 네트워크 프로토콜 분석에 활용된다. Wireshark를 이용해 IKEv2 프로토콜을 분석하기 위해서는 Initiator와 Responder의 ID, IKE_SA_INIT 교환 과정에서 생성된 세션키

SK_ei, SK_er, SK_ai, SK_ar와 암호 및 무결성 알고리즘을 알아야 한다. Initiator와 Responder ID, 암호 알고리즘은 IKE_SA_INIT 메시지를 통해 확인할 수 있으나, 세션키 정보는 IPsec VPN 시스템 관리자 권한이 필요하며, 특정 시스템에서는 세션키 획득이 불가능할 수 있다. 세션키는 매 세션마다 확인하고 매번 Wireshark에 수동으로 입력해야 한다. 또한 Wireshark을 이용하기 위해서는 네트워크 스위치의 포트 미러링 기능 또는 전용 탭 장치가 필요하며, 이 경우에도 단순 모니터링만 가능하다.

본 논문에서 제안하는 분석 기법(NIKEv2 AR: New IKEv2 Analyzer for Realtime)은 Initiator와 Responder의 사이에서 MITM 방식을 이용한다. 이를 통해 패킷 모니터링 기능만 제공하는 Wireshark과 달리 패킷을 실시간 조작 가능하여 퍼징 등 동적 분석에 활용할 수 있다. 네트워크 패킷 포워딩 기능을 기반으로 제안하는 분석 기법은 Initiator에게는 Responder로, Responder에게는 Initiator로 동작하여 세션키 생성 단계부터 IKE v2 모든 메시지를 실시간 분석할 수 있다. 뿐만 아니라 다양한 보안 프로토콜 분석에도 활용할 수 있을 것으로 기대된다.

References

[1] RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2), Internet Engineering Task Force (IETF)

[2] RFC 7815: Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation, Internet Engineering Task Force (IETF)

[3] Sawalmeh, H., Malayshi, M., Ahmad, S., Awad, A., "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements," In 2021 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) pp. 236-241. Sep. 2021

[4] Y. Cui, T. Yu and J. Hu, "IKEv2 Protocol Fuzzing Test on Simulated ASA," IEEE International Conference on Smart Internet of Things, pp. 111-116, Aug. 2018

[5] Tian, Kai, et al. "Analysis of Vulnerability of IPsec Protocol Implementation Based on Differential Fuzzing," International Conference on Security and Privacy in New Computing Environments, pp.282-293, Dec. 2021

[6] T. Ninet, A. Legay, R. Maillard, L. -M. Traonouez and O. Zendra, "The Deviation Attack: A Novel Denial-of-Service Attack Against IKEv2," 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 66-74, Aug. 2019

[7] Jiaxing Guo, Chunxiang Gu, Xi Chen, Siqi Lu, Fushan Wei, "Automated State-Machine-Based Analysis of Hostname Verification in IPsec Implementations," Information Technology and Control vol 50(3), pp. 570-587, Sep. 2021

[8] D. Felsch, M. Grothe, J. Schwenk, A. Czubak, and M. Szymanek, "The dangers of key reuse: Practical attacks on IPsec IKE," Proceedings of the 27th USENIX Security Symposium, pp. 567 - 583, Aug. 2018

[9] Streun, F., Wanner, J., & Perrig, A., "Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing," In Network and Distributed System Security Symposium (NDSS), Apr. 2022

[10] B. Pranggono, A. Arabo, "COVID-19 pandemic cybersecurity issues," Internet Technology Letters, 4(2), e247, 2021

[11] Favale, T., Soro, F., Trevisan, M.,

Drago, I., Mellia, M., "Campus traffic and e-Learning during COVID-19 pandemic," Computer networks, vol. 176, July, 2020
〔12〕 Scapy, "scapy" https://scapy.net, May 22, 2022
〔13〕 Wireshark, "wireshark" https://www.wireshark.org, May 22, 2022
〔14〕 StrongSwan, "strongswan" https://strongswan.org, May 22, 2022
〔15〕 Tcpdump, "tcpdump website" https://www.tcpdump.org, May 22, 2022
〔16〕 PyCryptodome, "PyCryptodome's documentation" https://pycryptodome.readthedocs.io/en/latest/index.html, May 22, 2022
〔17〕 Cisco ASA Software, "cisco asa software" https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html, May 22, 2022

〈저자소개〉

박 정 형 (Junghyung Park) 정회원
2005년 2월: 경북대학교 전자전기공학부 졸업
2007년 2월: 포항공과대학교 전자전기공학과 석사
2007년 2월~2010년11월: LIG넥스원
2010년12월~현재: 국가보안기술연구소
2020년 3월~현재: 충남대학교 컴퓨터공학과 박사과정
〈관심분야〉 네트워크 보안, 시스템 보안

유 형 열 (Hyungyul Ryu) 정회원
1999년 2월: 연세대학교 전자공학과 졸업
2001년 2월: 포항공과대학교 전자전기공학과 석사
2003년 3월~2007년 9월: 팬택&큐리텔
2007년 9월~현재: 국가보안기술연구소
〈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