인터넷 키 관리 프로토콜에 관한 연구

이 계 상†

요 약

IPSEC의 표준 키 관리 프로토콜인 IKE는 복잡성으로 야기되는 여러 알려진 문제점을 갖고 있다. 이 문제점을 해결하기 위한 유력한 후속 프로토콜로 IKE 버전 2 프로토콜과 Just Fast Keying 프로토콜이 IETF에서 논의 중이다. IKE 후속 프로토콜의 설계 요구사항으로는 프로토콜의 단순성 이외에, 서비스 거부 공격 대응력, PFS 제공 여부, identity 보호, 암호 협상 및 인증 방식 등이 있다. 본 고에서는 이 두 프로토콜을 IKE 후속 프로토콜이 만족시켜야 할 주요 요구사항별로 각 프로토콜의 특징과 그 내포 의미를 분석한다.

A study on the key management protocols for the Internet

Kye Sang Lee†

ABSTRACT

IKE, which is the standard key management protocol for IPSEC, is said to have several known problems. To resolve the problems of the IKE, two protocol proposals are being discussed in the IETF : the IKE version 2 and Just Fast Keying protocols. They should satisfy several protocol design requirements such as the protocol simplicity, the endurability against DOS attacks, the degree of the PFS, the identity protection, the cryptographic negotiation, and the authentication methods. In this paper, we summarize the characteristics of these two protocols and try to analyze their implications according to the protocol design requirements.

키워드 : 인터넷 보안(Internet Security), IPSEC, 키관리 프로토콜(Key Management Protocol), IKEv2, JFK

1. 서 론

인터넷의 이용이 전자상거래 등 기업활동 영역으로 확산되어 가면서 인터넷 정보 보안이 점점 더 중요한 이슈가 되어 가고 있다. 최근에는 인터넷을 통한 가상 사설망(VPN, Virtual Private Network), 즉, IP VPN의 구축이 기업 망의 경제적이며 안전한 구축 방식으로 관심을 모으고 있다. IPSEC(IP Security)은 안전한 IP VPN 구성을 위한 핵심 보안 프로토콜 요소로 이용된다. IPSEC은 임의의 통신 쌍방이 암호 알고리즘 및 프로토콜을 이용하여 제 3자의 보안 공격으로부터 안전한 IP 패킷 전달을 보장한다.

IPSEC은 네트워크 계층의 보안 프로토콜인 AH(Authentication Header) 프로토콜[1]과 ESP(Encapsulating Security Payload) 프로토콜[2], 그리고 응용 계층의 키관리 프로토콜인 IKE(Internet Key Exchange) 프로토콜[3]로 구성된다. AH 프로토콜과 ESP 프로토콜은 각각 IP 패킷에 대한 무결성과 기밀성 보안 서비스를 제공한다. IKE 프로토콜은 AH와 ESP 프로토콜의 보안 서비스 제공을 위한 안전한 키 교환을 주 임무로 수행한다. 이러한 IPSEC 프로토콜은 1993년부터 IETF(Internet Engineering Task Force)의 IPSEC WG에서 논의되어 1998년말 RFC로 표준화된 바 있다[4].

하지만, IPSEC 표준을 따르는 IP VPN의 구축은 예상했던 것 만큼 활발히 전개되어 오지 않았다. 그 중요한 한 이유는 IKE 프로토콜의 복잡성에 기인한다[5]. IKE의 복잡성으로 인하여 표준에 따른 정확한 구현이 어렵고, 이로 인해 서로 다른 IPSEC 프로토콜 구현 제품간에 상호 연동성이 제대로 확보되지 않고 있는 것이다. 또한 IKE의 복잡성으로 인하여 구현시 보안 허점의 존재 가능성이 높다. 게다가, 최근 들어 빠른 발전을 보이고 있는 모바일 VPN 클라이언트의 경우 소형 단말기가 대부분으로 현재의 복잡한 IKE 프로토콜을 수용하는데 한계를 갖고 있다. 현 IKE 프로토콜은 두 지역간 VPN 게이트웨이의 연결을 주 목적으로 설계되었기 때문이다.

이와 같은 현 IKE 프로토콜의 문제점을 해결하기 위해 IETF의 IPSEC WG은 2001년 8월 복잡한 현 IKE 프로토콜을 대체할 수 있는 후속 키 관리 프로토콜(Son of IKE)을 개발키로 하였다[6]. 단순성을 첫 번째 요구사항으로 만

※ 본 연구는 2000년도 동의대학교 교내 연구비 지원에 의해 수행되었음.
† 정 회 원 : 동의대학교 정보통신공학과 교수
논문접수 : 2002년 9월 9일, 심사완료 : 2003년 3월 11일

족시켜야 하는 후속 키 관리 프로토콜은 최근 두 가지 제안, 즉, IKEv2(IKE version 2)[7]와 JFK(Just Fast Keying)[8] 프로토콜로 나뉘어 논의 중이다.

본 고에서는 현 IKE 프로토콜의 개요와 문제점을 2장에서 먼저 살펴보고, 3장에서는 최근 제안되어 논의 중인 두 후속 IKE 프로토콜인 IKEv2와 JFK 프로토콜의 개요를 살펴본다. 4장에서는 이 두 후속 프로토콜이 만족시켜야 할 요구사항 측면에서 그 특징과 내포 의미를 분석한다.

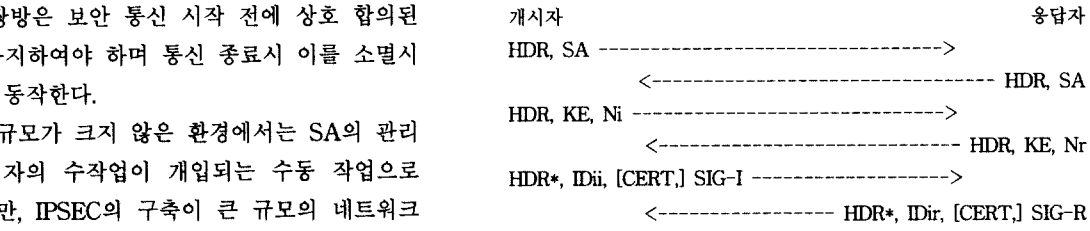
2. IKE 프로토콜

IP 계층의 보안 엔진 프로토콜인 AH와 ESP 프로토콜의 동작에는 통신 양쪽에 동일한 암호 키가 존재하는 것이 전제가 된다. IPSEC 프로토콜 표준에서는 이 암호 키를 포함한 보안 통신 쌍방의 사전 합의 사항을 security association (SA)으로 관리한다. 즉, IPSEC을 이용하여 보안 통신을 하고자 하는 통신 쌍방은 보안 통신 시작 전에 상호 합의된 SA를 생성하고 유지하여야 하며 통신 종료시 이를 소멸시키는 단계를 거쳐 동작한다.

보안 네트워크 규모가 크지 않은 환경에서는 SA의 관리를 네트워크 관리자의 수작업이 개입되는 수동 작업으로 할 수 있다. 하지만, IPSEC의 구축이 큰 규모의 네트워크로 확대되는 단계에 이르면 SA의 관리를 더 이상 수동으로 할 수 없고 확장성을 위해 자동화하여야 한다. 즉, 보안 통신을 하고자 하는 임의의 통신 쌍방은 SA의 생성, 유지, 소멸 등 SA 관리 작업을 자동적으로 수행해 낼 수 있는 수단을 가져야 한다. IKE 프로토콜은 이러한 IPSEC SA 관리 작업을 자동화하기 위한 목적으로 IETF에서 고안된 IPSEC의 표준 키 관리 프로토콜이다.

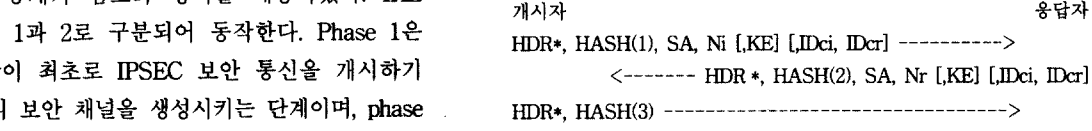
IKE 프로토콜은 ISAKMP, Oakley, SKEME의 세 프로토콜이 결합된 하이브리드 프로토콜이다. ISAKMP 프로토콜[9]에서는 프레임워크, 메시지 포맷, phase 개념 등을 따 왔고, Oakley 프로토콜[10]에서는 키 교환 모드를, SKEME 프로토콜[11]에서는 공개키 암호화 방식을 채용하였다. IKE 프로토콜은 phase 1과 2로 구분되어 동작한다. Phase 1은 임의의 통신 쌍방이 최초로 IPSEC 보안 통신을 개시하기 전, 그 들간 최초의 보안 채널을 생성시키는 단계이며, phase 2에서는 phase 1에서 생성된 보안 채널을 통해, 실제 IP 트래픽 보안 채널, 즉, IPSEC SA의 생성 및 관리를 위한 메시지 교환이 일어난다.

Phase 1에서는 특히 통신 쌍방의 인증 작업이 수행되어야 한다. IKE에서는 이를 위해 네 가지 인증 방식을 지원한다. 공유키 방식, 디지털 서명 방식, 공개키 방식과 공개키 변형 방식이 그 것이다. 또한, IKE는 phase 1의 메시지 교환 모드로 6개 메시지 교환으로 이루어지는 메인 모드와 3개 메시지 교환으로 이루어지는 어그레시브 모드를 지원한다. (그림 1)은 디지털 서명 인증 방식을 채용한 메인 모드 phase 1 메시지 교환을 보인다. 여기서, HDR은 ISAKMP 메시지 헤더를, SA는 SA 페이로드를, KE는 Diffie Hellman (DH) 키 교환 페이로드를 나타내고, Ni와 Nr은 각각 개시자와 응답자의 nonce 값을 의미한다. 메시지 1과 2의 교환에서 SA 협상이 수행되고, 메시지 3와 4에서 키분배를 위한 DH 공개값 교환, 그리고, 메시지 5와 6에서는 이상의 통신 내용을 상호 인증하는 작업이 수행된다. 메시지 5와 6에서, ID는 identity 페이로드를, SIG는 signature 페이로드, CERT는 선택적으로 사용될 수 있는 인증서를 나타낸다. 이 두 메시지는 암호화되어 교환되는데 HDR 다음의 기호 '*'이 이를 의미한다. 암호화를 위한 세션 공유키는 메시지 3과 4의 교환 후 양단에서 계산된다. 결국, phase 1은 임의의 통신 쌍방이 보안 통신을 위해 최초로 상호 인증된 보안 채널인 IKE SA가 수립되는 단계이다.



(그림 1) IKE의 phase 1 메인모드 메시지 교환(서명 인증방식 경우)

이와 같이 phase 1에서 IKE SA가 수립되면, phase 2에서는 이 인증된 보안 채널을 사용하여 실제 IP 트래픽을 보호할 수 있는 IPSEC SA가 수립되어 진다. IPSEC SA는 IKE SA의 보호 아래 (그림 2)와 같이 세 개의 메시지 교환으로 생성된다. IPSEC SA 수립을 위한 이러한 phase 2 메시지 교환 모드는 퀵 모드로 불린다. 그림에서 각 페이로드에 대한 자세한 설명은 본 논문의 논의에 영향을 미치지 않으므로 생략한다.



(그림 2) IKE의 phase 2 퀵 모드 메시지 교환

이상에서 살펴 본 것과 같이 IKE 프로토콜에서는 phase 1에 두 가지 모드와 네 가지 인증 방식이 있을 수 있으므로, phase 1에서만 8가지 메시지 교환 방식이 가능하다. 이에 phase 2의 퀵 모드를 더하면 모두 9가지 메시지 교환 방식이 존재하는 셈이다. 또한, 메인 모드의 경우, 6개의 메시지 교환으로 IKE SA가 수립되는데 이로 인한 전송 대역폭의 소모와 통신 개시 전 긴 지연시간이 소요된다. 또한,

IKE 프로토콜은 이 프로토콜의 표준화 이후 증가하고 있는 서비스 거부 공격(Denial of Service Attack)에 대해 매우 취약한 구조를 갖는다. 즉, 메인 모드의 경우, 메시지 5와 6을 통한 인증 과정 전에 값비싼 계산을 필요로 하는 세션 키의 생성이 요구되어 지기 때문이다. 또한, 현재 IKE 프로토콜은 RFC 2407[12], RFC 2408[9], RFC 2409[3]의 세 RFC에 분산되어 기술되어 있는 상당히 복잡한 프로토콜이기도 하다.

이러한 IKE 프로토콜의 문제점으로 인해 서로 다른 벤더 간 상호연동성이 최근까지도 확보되지 못하고 있다. 게다가 프로토콜의 복잡성은 IKE 구현 제품에 보안 허점의 존재 가능성을 높인다. 이러한 결과의 예로 IPSEC을 이용한 VPN 구축이 예상보다 많이 지연되고 있다. 또한, IKE 프로토콜의 복잡성은 최근 들어 활발한 발전을 보이고 있는 모바일 인터넷 분야의 IPSEC 프로토콜 적용에 장애물이 되고 있다. 모바일 인터넷 분야에서는 소형 단말기들이 많이 사용되며 이들의 계산 능력은 대부분 상당히 제한적이기 때문에 복잡한 IKE 프로토콜의 적용이 당장은 어렵기 때문이다. 이러한 배경에서 IKE 후속 프로토콜의 표준 개발이 IETF에서 진행 중이다. 다음 장에서는 유력한 IKE 후속 프로토콜 안을 살펴본다.

3. IKE 후속 프로토콜

IKE 후속 프로토콜은, 앞장에서 살펴 본 기존 IKE 프로토콜의 문제점을 해결하고 최근 대두된 새로운 요구사항을 만족할 수 있도록, 기존 IKE 프로토콜에 비해 그 기능이 대폭 간소화되고 한 문서에 간결히 기술될 수 있도록 단순하게 설계되어야 한다. 다음절에서 현재 IETF에서 후속 프로토콜 표준으로 개발 중인 IKEv2 프로토콜과 JFK 프로토콜을 간략히 기술한다.

3.1 IKEv2 프로토콜

IKEv2 프로토콜은 기존 IKE 프로토콜에서 거의 사용되지 않는 기능, 또는 문제가 있는 기능 등을 생략하여 IKE 프로토콜의 축약 형태로 개발되었다. 하지만, IKE를 계승하는 프로토콜이므로 주요 개념을 또한 계승하고 있다. 프로토콜의 동작에 있어 phase 1과 2로 나뉘는 것이 한 예이다.

(그림 3)은 IKEv2의 phase 1에서 개시자와 응답자간 메시지 교환을 보인다. 모두 네 개의 메시지 교환이 일어난다. HDR은 IKE에서와 같이 ISAKMP 포맷을 따르는 메시지 헤더를 표시하며, HDR*은 헤더를 제외한 나머지 부분이 암호화된 메시지임을 나타낸다. 첫 번째와 두 번째 메시지는 각각 IKE SA 수립을 위한 요청과 응답 메시지이다. SA 페이로드를 통해 IKE SA 협상이 일어나고, KE 페이로드를 통해 DH 값이 교환된다.

```
개시자                                              응답자
HDR, SAi, KEi, Ni, [CERTREQ] ---------->
                    <---------- HDR, SAr, KEr, Nr, [CERTREQ]
HDR*, IDi, [CERT,] AUTH, SAi2, TSi, TSr -------->
                    <-------- HDR*, IDr, [CERT,] AUTH, SAr2, TSi, TSr
```

(그림 3) IKEv2 phase 1 메시지 교환

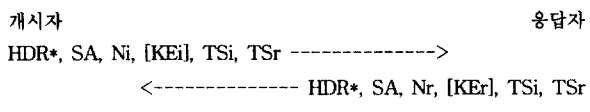
두 메시지의 교환으로 IKE SA가 초기화되고 난 후, 다음은, 세 번째와 네 번째 메시지를 통해 상호 인증이 수행되는데, 이들 메시지의 암호화를 위해 우선 세션 공유키가 다음과 같이 계산된다.

```
SKEYSEED = prf(Ni | Nr, g^ir)
SK_d = prf(SKEYSEED, g^ir | Ni | Nr | CKY-I |
       CKY-R | 0)
SK_a = prf(SKEYSEED, SK_d | g^ir | Ni | Nr |
       CKY-I | CKY-R | 1)
SK_e = prf(SKEYSEED, SK_a | g^ir | Ni | Nr |
       CKY-I | CKY-R | 2)
```

여기서, prf(X, Y)는 키 X를 사용하여 Y에 pseudo random function을 취함을 의미하며, 기호 '|'는 스트링 연결을 의미한다. g^ir은 g^i 또는 g^r을 수신하여 자신의 비밀 i와 r을 멱승한 것으로 개시자와 응답자간의 DH 공유값이 된다. 첫 째 식에서 DH 공유값 g^ir로부터 SKEYSEED를 먼저 계산하여, 이 결과를 다음 식들에서 키로 활용하여 SK_d, SK_a와 SK_e를 차례로 계산한다. SK_a와 SK_e는 IKE SA의 인증과 암호용 키로 각각 사용하며, SK_d는 IPSEC SA 키를 유도하는 키로 사용한다.

세션 공유키로 암호화된 세 번째와 네 번째 메시지는 상호 인증을 수행한다. AUTH 페이로드는 이를 위한 인증 데이터를 포함한다. RSA나 DSA와 같은 signature 방식 또는 MAC 방식이 이 페이로드의 발생과 확인에 이용된다. 이 두 메시지는 또한 SAi2와 SAr2를 통해 IPSEC SA의 생성 협상을 수행함으로써 IPSEC SA의 생성 지연을 최소화한다.

IKEv2의 phase 2에서는 두 가지 형태의 메시지 교환이 일어난다. 하나는 IPSEC SA와 같은 child SA를 생성하기 위한 메시지 교환으로 (그림 4)와 같다. HDR*의 기호 '*'의 의미는 (그림 3)에서와 같이 이들 메시지가 IKE SA에 의해 보호됨을 뜻한다. 실제로 키 SK_e로 헤더 다음 부분이 암호화되며, 키 SK_a로 헤더를 포함한 메시지 전체의 무결성이 보장된다. SA 페이로드를 통하여 IPSEC SA가 협상된다. KE 페이로드는 PFS(perfect forward secrecy)가 필요할 때 사용된다. PFS는, 이전키가 노출되었을지라도 새로 갱신된 키에 의한 데이터 보안이 아무런 영향을 받지 않는, 키 생성 방식의 성질을 말한다. 이 교환은 IKE SA의 자체 rekeying에도 사용된다.



(그림 4) IKEv2 phase 2의 child SA 생성 메시지 교환

Phase 2 메시지 교환의 또한 형태는 SA 제어 정보 교환을 위한 메시지 교환으로 (그림 5)와 같다. 교환되는 메시지에는 오류 상황을 상대편에 알리는 페이로드 N(Notification)이 포함되거나, 특정 SA의 소멸을 위한 페이로드 D(Delete)가 포함된다. 페이로드 없이 헤더만으로 구성된 메시지의 교환을 통해 상대방이 동작 중임을 확인할 수도 있다.

(그림 5) IKEv2 phase 2의 정보 메시지 교환

3.2 JFK 프로토콜

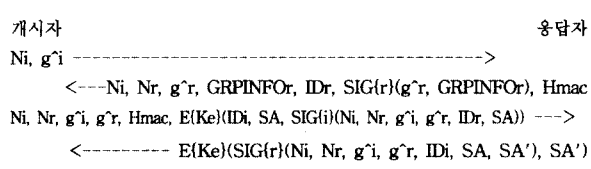
JFK 프로토콜은 기존 IKE 프로토콜과는 별개의 간결한 새로운 프로토콜로 설계되었다. JFK 프로토콜은 (그림 6)과 같이 언제나 네 개의 메시지 교환으로 동작한다. 응답자의 DH 그룹을 이미 알고 있는 개시자는 이 그룹에 속한 DH값 g^i를 생성하여 메시지 1에 실어 응답자에 전달한다. 응답자는 DH값 g^r과 자신의 identity IDr, 그리고 이의 인증을 위한 signature SIG를 메시지 2에 포함시켜 응답한다. 메시지 2에는 또한 응답자만이 아는 비밀키(HKr)로 다음과 같이 생성한 HMAC 코드, Hmac을 포함한다. 이 코드는 개시자에 의해 메시지 3에 그대로 에코우된다.

$$Hmac = HMAC\{HKr\}(Ni, Nr, g^i, g^r)$$

메시지 3에서 개시자는 자신의 identity IDi와 SA 제안, 그리고signature를 세션 키 Ke로 암호화하여 전달한다. 메시지 3의 암호화를 위한 세션 공유키 Ke와 IPSEC용 공유키 Kir은 다음과 같이 계산된다. 여기서, g^ir은 DH 공개값 교환 후 계산된 DH 공유값을 의미한다.

$$Ke = HMAC\{g^ir\}(Ni, Nr, 1)$$
$$Kir = HMAC\{g^ir\}(Ni, Nr, 0)$$

마지막으로, 응답자는 메시지 4를 그림과 같이 생성하고, 이를 개시자와 같은 방식으로 계산한 세션 공유키로 암호화하여 전송함으로써 지금까지의 통신 내용을 확인한다.

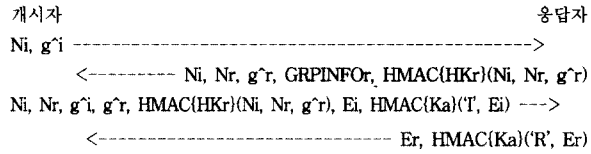


(그림 6) JFKi 메시지 교환

이상의 (그림 6)의 JFK는 응답자의 identity가 먼저 노출되고 개시자의 identity는 적극적으로 보호되는 방식으로 JFKi로 불리워지며, 만약 응답자의 identity 보호가 중요한 경우를 위해 고안된 약간 변형된 방식인 JFKr은 (그림 7)과 같다. 그림에서 Ei와 Er은 각각 다음과 같이 계산된다.

$$Ei = E\{Ke\}(IDi, SA, SIG\{i\}(Ni, Nr, g^i, g^r, GRPINFO))$$
$$Er = E\{Ke\}(IDr, SA', SIG\{r\}(Ni, Nr, g^i, g^r))$$

이 방식에서는 응답자의 identity IDr이 마지막 메시지에 실려 전달되므로 응답자의 identity를 적극적인 공격자로부터 보호할 수 있다. 세션 공유키인 Ke와 IPSEC 공유키 Kir의 계산은 JFKi에서와 동일하고, Ka는 Ka = HMAC{g^ir}(Ni, Nr, 2)로 계산된다. JFKi와 JFKr의 identity 보호 방식의 내포 의미는 다음 장에서 더 자세히 기술한다.



(그림 7) JFKr 메시지 교환

4. IKE 후속 프로토콜 분석

이 장에서는 앞장에서 기술한 IKEv2와 JFK 프로토콜을, 서비스 거부 공격 대응력, PFS, identity 보호, 암호 협상, phase 유무, 인증방식 등 프로토콜 설계의 주요 요구사항별로 그 특징과 내포 의미를 분석한다.

4.1 IKEv2 프로토콜 분석

(그림 3)에 보인 IKEv2 프로토콜 메시지 교환은 정상 상태의 경우이며, 서비스 거부 공격이 탐지된 경우는 메시지 1에 대해 응답자가 쿠키를 생성하여 응답하고 개시자는 이를 다시 새로운 메시지 1에 포함시켜 응답자에 반환하는 방식으로 서비스 거부 공격에 대응한다. 이 경우 2개의 메시지 교환이 추가되어 phase 1이 총 6개의 메시지 교환으로 이루어지게 된다. 응답자는 개시자의 IP 주소와 ISAKMP 쿠키 값 그리고 응답자만이 아는 비밀값의 해쉬 코드를 암호화하여 쿠키를 생성한다. 응답자는 이를 개시자에 주었다 돌려 받음으로써 자신이 선의의 개시자와 암호 통신을 시작하는 것임을 확인하게 된다. 이 방식의 이점은 평상시 phase 1을 위해 교환되는 메시지의 길이를 짧게 유지시킬 수 있다는 것이다. 이 점은 서비스 거부 공격을 위해 JFK 프로토콜에서는 메시지 3이 항상 해쉬 정보를 포함하여 그 길이가 길어진다는 단점과 비교된다. 또한 JFK의 경우 메시지 3이 부분적으로 암호화되어야 하고 이는 구현을 복잡하게 하는데 반해 IKEv2에서는 그럴 필요가 없게 되는 점

이 또 다른 이점이 된다. 하지만, IKEv2의 경우, 서비스 거부 공격의 시작을 검출해 내야 하는 일이 구현자의 부담으로 남는다.

IKEv2는 phase 1에서 DH 값을 교환하는데, 매번 새로운 값을 생성하여 사용한다고 가정하면, PFS가 보장된다. 또한 phase 2에서도 새로운 DH 값을 사용함으로써 IPSEC SA에서도 PFS가 보장될 수 있다. 하지만, IKEv2 프로토콜은 서로 다른 IKE SA간에도 같은 DH 값을 재사용할 수 있도록 하여 불완전한 PFS를 허용하였다. 즉, 암호화 수준과 서비스 거부 공격 대응력이 서로 절충될 수 있음을 허용한다.

IKEv2는 (그림 3)의 메시지 3에서 개시자의 identity가 전달되고 메시지 4에 응답자의 identity가 전달된다. 두 identity 모두 암호화되어 전달되므로 수동적 공격자로부터 보호된다. 하지만, 개시자의 identity는 응답자 것 보다 먼저 제시되어야 하므로 적극적 공격자로부터 보호는 불가능하다. 즉, 공격자가 응답자를 가장하는 man-in-the-middle인 경우 개시자의 identity는 노출될 수 있다. 반면, 응답자의 identity는 항상 개시자의 인증과정을 거친 후 제시되므로 적극적 공격자로부터의 보호가 가능하다. IKEv2의 identity 보호 형태는 다음절에서 기술할 JFKr 프로토콜의 보호 형태와 동일하다.

기존 IKE의 후속 버전으로 개발 중인 IKEv2는 기존 IKE의 암호 협상 기능을 계승하고 있다. IKEv2에서는 phase 1의 메시지 1과 2를 통해 개시자가 일련의 IKE SA 암호 suite을 제안하고 응답자는 이 중 가장 선호하는 암호 suite을 선택한다. DH group의 경우, 개시자가 제안한 group을 응답자가 지원하지 않는 경우, 개시자는 다른 group으로 프로토콜을 다시 시작한다. IKEv2는 phase 1의 키교환 암호 suite 협상뿐만 아니라, phase 2의 IPSEC SA 생성을 위해서도 협상을 허용한다. 즉, IPSEC SA를 위한 암호 suite도 개시자와 응답자가 가장 선호하는 파라미터로 선택될 수 있게 한다. 이를 위해 개시자는 일련의 암호 suite을 제안하고 응답자가 선택하는 방식으로 협상이 지원된다. 이러한 IKEv2의 협상 기능은 새로운 프로토콜로의 진화와 알고리즘의 추가를 용이하게 한다. 예를 들어, 개시자가 새로운 암호 알고리즘을 채용하고 이를 암호 제안 목록에 추가하여 응답자에게 제시하는 경우, 응답자가 아직 이 알고리즘을 이해하지 못한다면, 응답자는 목록 중 자신이 선호하는 기존의 알고리즘을 선택하면 된다. 이렇게, 암호 협상 기능은 상호연동성의 범위를 넓히는 장점이 있으나, 그 만큼 프로토콜을 복잡하게 하는 단점을 갖는다.

IKEv2는 역시 기존 IKE의 phase 1/2 개념을 계승한다. IKE SA가 phase I에서 수립되면, 이것은 다음에 계속해서 다수의 IPSEC SA의 생성에 이용될 뿐만 아니라, 여러 가지 SA 제어 기능의 구현에 활용될 수 있다. 실제로 IKEv2 phase 2의 정보 메시지 교환은 이를 위한 도구로 고안되었다. (그림 5) 참조. 우선, SA 소멸의 경우, 정보 메시지 교환으로 교환되는 메시지에 D 페이로드를 실어 SA를 소멸시킨다. IPSEC SA 뿐 아니라, IKE SA도 이를 통해 소멸된다. SA rekeying은 다음절에서 기술할 JFK에서와 같이 기존 SA와 동등한 새로운 SA를 생성한 후, 기존 SA는 소멸시키는 방식으로 달성한다. 여기서도 역시 rekeying은 IPSEC SA 뿐 아니라, IKE SA에도 적용된다. 또한, IKE SA는 dead peer detection에도 활용될 수 있다. JFK 프로토콜에서와 같이 phase 구분 개념이 없는 경우 일반 SA 트래픽을 통해서만 dead peer detection을 수행할 수 있는 것에 반해, IKEv2는 IKE SA 트래픽의 응답 유무를 통해 dead peer를 검출할 수 있다. IKEv2의 정보 메시지 교환은 또한 N 페이로드를 규정함으로써 이를 통해 자신의 오류 상황과 같은 정보를 상대방에 전달할 수 있다. 이러한 메시지 교환은 IKE SA의 보호아래 전달되고 확인됨으로써, 안전하고 인증된 오류 정보 교환이 이루어지는 것이다. 정보 메시지 교환은 아무런 페이로드를 갖지 않는 메시지 교환을 통해 liveliness 검사를 수행할 수도 있다.

IKEv2는 인증서 또는 공유 비밀을 사용하여 상호 인증을 수행한다. 상호 인증을 위해 교환되는 (그림 3)의 메시지 3과 4의 CERT 페이로드는 디지털 서명키가, ID 페이로드에 기재된 name의 소유라는 사실을 증명한다. IKEv2는 인증서나 공유 비밀을 사용하지 않는 기존 인증 방식(legacy authentication system)을 간접적으로 지원한다. 이 경우 IKEv2 시스템은 기존 인증 방식을 통하여 identity와 공유 비밀을 생성하고 이를 안전하게 전달받을 수 있는 안전한 메커니즘을 가져야 한다.

4.2 JFK 프로토콜 분석

JFK 프로토콜은 서비스 거부 공격에 대해 잘 견딜 수 있도록 설계되었다. 이 프로토콜은 (그림 6)에서 응답자는 메시지 3을 수신하여 정당한 개시자임이 확인된 후에나, 많은 연산을 요하는 공유키 계산을 수행한다. DH 값의 발생도 모든 새로운 세션 마다 매번 수행되는 것이 아니라 일정한 기간 동안 같은 값을 재사용할 수 있도록 하여 서비스 거부 공격에 대한 대응성을 제고하였다. 따라서, 응답자가 메시지 2의 준비에 있어 매번 연산을 필요로 하는 부분은 nonce Nr과 HMAC으로서, 이에 필요한 주 계산은 HMAC 코드 발생을 위한 두 번에 걸친 해쉬 알고리즘의 연산 정도로 국한된다. 또한, 응답자는 자신과 상대방의 nonce와 DH 값들을 메시지 2에 실어 보냈다가 메시지 3에 의해 돌려 받음으로써, 이 때 까지 프로토콜 상태를 유지하고 있을 필요가 없게 된다. 이와 같이 함으로써, JFK 프로토콜은 서비스 거부 공격에 대해 응답자의 계산처리 능력이나 메모리 용량의 고갈 가능성을 최소화한다.

위의 서비스 거부 공격에 대한 저항력 제고를 위한 DH 값 재사용은 한편 세션간 PFS를 달성하지 못하는 절충 요소가 된다. DH 값의 갱신은 새로운 세션을 기준으로 하지 않고 그와는 별도의 forward secrecy 기간을 기준으로 한다. 그 결과, 같은 DH 값을 재사용하는 세션간에는 기밀이 보장되지 않고, 다른 DH 값이 사용되는 서로 다른 forward secrecy 기간에만 기밀이 보장된다. 따라서, PFS의 정도는 forward secrecy 기간의 길이에 의존하게 되는데 이는 다시 상세 구현에 따라 달라지게 된다. 결국, 서비스 거부 공격의 저항력을 위한 반대 급부로 세션간에 불완전한 PFS가 제공된다.

JFK 프로토콜은 앞장에서 언급한 바와 같이 통신자 identity 보호에 있어 두 가지 다른 방식, JFKi와 JFKr을 제안하고 있다. (그림 6)의 JFKi에서는 메시지 2에서 응답자가 먼저 자신의 identity IDr을 제시한다. 개시자는 응답자의 IDr과 signature 코드를 통해 응답자의 identity를 확인하고 난 후, 메시지 3에 자신의 identity IDi를 암호화하여 응답자에 제시한다. 이와 같이 하여 JFKi에서는 응답자 identity는 아무런 보호를 하지 않지만, 개시자 identity는 적극적인 공격자로 부터의 공격에도 보호될 수 있다. JFKi 프로토콜은, 응답자가 잘 알려진 서버로 identity 보호가 중요치 않으며, 개시자인 클라이언트 쪽에는 적극적인 identity 보호가 꼭 필요한 클라이언트-서버 모델에 적합하다.

반면에, (그림 7)의 JFKr에서는 응답자의 identity가 적극적으로 보호된다. 그림의 메시지 3에서 보는 바와 같이, 먼저 identity를 제시하는 쪽은 개시자로서 identity IDi가 암호화되어 전달되어 수동적인 공격자로부터 identity가 보호될 수 있다. 하지만, 상대방이 적극적인 공격자인 경우 개시자의 identity는 노출될 수 있는 여지가 있다. 한편, 응답자는 메시지 3에 포함된 개시자의 identity IDi를 통해 개시자의 신원을 확인하고 나서야 자신의 identity IDr을 메시지 4에 전송하기 때문에 응답자의 identity는 적극적으로 보호될 수 있다. JFKr은 응답자에게는 적극적인 identity 보호, 개시자에게는 수동적인 보호가 필요한 피어(peer) 모델에 적합하다.

한편, JFKr에서와 반대로, 개시자에게는 능동적인 보호와 응답자에게는 수동적인 보호가 제공될 수 있을지 생각해 볼 수 있지만, 이는 서비스 거부 공격에 대한 보호를 네 개의 메시지 교환으로 동시에 제공해야 한다는 조건하에서는 불가능한 것으로 다음과 같이 분석된다. 서비스 거부 공격으로부터 응답자를 보호하기 위하여, 응답자는 전송할 첫 번째 메시지 준비를 위해 공유키를 계산해서는 안된다. 왜냐하면, 공유키 계산에는 상당한 연산이 필요하기 때문이다. 이는 결국 응답자의 identity는 암호화되지 않은 상태로 첫 번째 메시지 (메시지 2)에 실려 가거나, 두 번째 메시지(메시지 4)에 실려 갈 수밖에 없음을 의미한다. 전자는 바로 JFKi의 identity 보호 방식에 해당하며, 후자의 경우는 개시자의 identity 제시가 응답자의 identity 보다 먼저 일어날 수 밖에 없는 JFKr의 보호 방식에 해당하게 된다.

단순성을 가장 중요한 설계 목표의 하나로 세운 JFK 프로토콜에서는 이를 달성하기 위해 암호 suite에 대한 협상을 하지 않는다. 암호 suite의 협상은 키 교환을 위한 것과 IPSEC SA를 위한 것으로 나누어 생각할 수 있다. 전자의 경우, 응답자는 한 세트의 암호 알고리즘, 서명 알고리즘과 해쉬 알고리즘 만을 사용하고 있어, 만일 개시자가 이를 지원하지 않으면 통신은 종료된다. DH group의 경우는 응답자가 여러 group을 지원할 수 있고, 개시자는 이중의 하나를 선택한다. 개시자는 응답자의 이러한 정보를 사전에 알고 있다고 가정되거나, 그렇지 않은 경우 메시지 2의 GRPINFOr 메시지 요소를 통해 통지된다. 따라서, JFK 프로토콜은 응답자가 지정한 키교환 암호 suite외에 다른 suite는 필요 없는 환경에서 사용이 가정된다. 또한, 만약 이 암호 suite이 바뀔 필요가 있을 경우, 응답자와 모든 개시자는 이 사실이 프로토콜과는 별개의 통로로 통지되어야 함을 의미한다.

후자의 IPSEC SA 협상의 경우, 개시자가 IPSEC SA 암호 suite를 제시하면, 응답자는 이를 단지 수락하거나, 거절할 수만 있다. 거절되는 경우, 개시자는 새로운 메시지 3에 다른 암호 suite를 제시한다. 이 경우도 개시자와 응답자 간에 암호 suite이 미리 정의된 상황이 가정된다.

JFK 프로토콜은 또한 프로토콜의 단순성을 위해 기존 IKE 프로토콜의 phase 1과 2 분리 개념을 따르지 않는다. 모든 SA는 언제나 (그림 6) 또는 (그림 7)과 같은 네 개의 메시지 교환을 통해 독립적으로 생성된다. IKE 프로토콜의 IKE SA와 같은 별도의 제어 채널을 갖지 않는 이 개념은 몇 가지 제어 기능의 구현에 있어 다음과 같이 별도의 방식들이 고안되어야 한다. SA 소멸은 AH나 ESP 암호 suite을 우회(bypass)하는 새로운 SA를 생성시키고, 새 SA로 기존 SA를 대체하여 수행한다. 이와 유사하게 SA rekeying도 동일한 SA를 생성한 후 기존 SA를 소멸시키는 방식으로 달성한다. 또한, 별도의 제어 채널을 갖지 않음으로 인하여 dead peer detection에도 방도가 강구되어야 한다. 한 방법으로 패킷의 마지막 성공 수신이후 일정 시간이 경과하면 dead peer로 의심하고 탐색 패킷의 송신으로 이를 확인하는 방법을 생각할 수 있다.

인증 방식은 JFK 프로토콜을 가능한한 간단하게 만들기 위해 의도적으로 여러 선택을 최소화하였다. JFK 프로토콜은 상대의 인증을 위해 인증서 방식만을 채택하고 있다. 즉, 공유 비밀, 토큰기반 인증 및 기존 인증 방식 등을 프로토콜에 포함시키지 않음으로써 프로토콜의 단순성을 유지하였으며, 그 결과 프로토콜의 보안 분석에서 이들을 분리시킬 수 있는 장점을 갖는다. (그림 6)과 (그림 7)에 나타

난 메시지의 IDi와 IDr은 각각 개시자와 응답자의 인증서를 의미한다. 통신 쌍방은 이 인증서와 signature 코드를 통해 상대방을 인증한다.

5. 결 론

IPSEC은 인터넷 IP 패킷 레벨에서 보안 서비스를 제공할 수 있는 프로토콜로서 IP VPN의 구축을 위한 핵심 보안 프로토콜로서 뿐 아니라, 모바일 인터넷 보안, storage network 보안 등을 위해서도 유력한 보안 프로토콜 후보로 기대되어 왔다. 하지만, IPSEC의 키관리 프로토콜인 IKE 프로토콜의 복잡성으로 인해 야기되는 낮은 상호연동성, 구현 제품의 보안 허점, 서비스 거부 공격의 취약성 등과, IKE 프로토콜이 표준으로 채택되고 난 후 급격히 발전하고 있는 모바일 네트워크 환경에서 오는 새로운 요구사항 들을 제대로 수용하지 못하고 있는 점 등으로, IPSEC의 적용과 구축이 예상만큼 활발히 이루어지고 있지 않다.

본 고에서는 이러한 기존 IKE 프로토콜의 문제점을 해결하기 위해 IETF에서 논의 중에 있는 IKE 후속 프로토콜인 IKEv2와 JFK 프로토콜을 프로토콜 설계 요구사항 측면에서 비교 분석하였다. 분석 결과의 간략한 요약은 <표 1>과 같다.

IKEv2는 기존의 IKE 프로토콜의 개념을 그대로 계승하면서 기능을 대폭 축약한 형태인데 반해, JFK 프로토콜은 완전히 새로 설계한 프로토콜이라는 점에서 서로 대비된다.

IKEv2와 JFK는 전혀 다른 프로토콜이지만, 새로운 키 관리 프로토콜이 만족시켜야 하는 요구사항을 거의 대등하게 만족시키고 있다. 우선, 두 프로토콜 모두 정상시 4개의 메시지 교환에 의해 통신 쌍방이 인증된 보안 채널을 수립한다. 기존 IKE가 6개의 메시지 교환으로 이를 달성하는 것에 비해 경제적이다. 또한, 두 프로토콜은 모두 기존 프로토콜이 갖지 못한 서비스 거부 공격(DOS)에 대한 대응력을 갖고 있다. IKEv2는 DOS 공격시 2개의 메시지 교환을 추가함으로써, JFK는 메시지에 DOS 대응 기능을 항상 포함함으로써 이를 달성한다. DOS 공격 대응력을 높이기 위해 두 프로토콜 모두 PFS(Perfect Forward Secrecy)를 타협할 수 있도록 허용하였다. 또한, 두 프로토콜은 모두 IKE에서와 같이, 개시자 identity의 수동적 보호와 응답자 identity의 적극적 보호를 도모할 수 있다. 하지만, 암호 협상과 phase 개념 면에서는 두 프로토콜이 차이를 보인다. IKEv2가 IKE에서 보다는 훨씬 선택 사항이 줄어들긴 했지만 아직도 암호 협상을 허용하는데 반해, JFK는 암호 협상을 허용하지 않음으로써 간결성을 강조하였다. 또한, IKEv2는 기존 IKE의 phase 1/2 개념을 계승하여 phase 1에서 수립된 IKE SA를 후속 IPSEC SA 수립과 관리시 제어 채널로 활용할 수 있게 한데 비해, JFK는 phase 구분을 없애 프로토콜의 간결성을 제고하였다. 인증 방식면에서는 두 방식 모두 인증서에 의한 인증을 기본으로 하지만, IKEv2는 공유 비밀 사용도 지원하고, 기존 인증 시스템의 사용도 간접 지원한다. 결과적으로, JFK는 좀 더 간결한 프로토콜이며, IKEv2는 약간 더 융통성 있는 프로토콜이라 할 수 있으나, 주요 특성에서는 그 차이가 크지 않은 것으로 보인다.

〈표 1〉 IKEv2와 JFK 분석 요약

프로토콜 설계 요구사항	IKEv2	JFK
서비스 거부 (DOS) 공격에 대한 대응력	• 필요시 쿠키 교환으로 대응. 즉, 필요시 stateless operation • DOS 공격시 2개 메시지 교환이 추가됨 • DOS 공격 개시 검출 필요	• 항상 해쉬 코드로 대응. 항상 stateless operation • 이 결과, 메시지의 길이가 길어짐 • 항상 4개 메시지 교환
Perfect Forward Secrecy	• phase 1에서 매번 새로운 DH 값을 사용하면 보장 • DOS 대응력을 높이기 위해 DH 값 재사용으로 불완전한 PFS 허용	• DOS 대응력 제고를 위해 불완전한 PFS 제공 • PFS의 정도는 같은 DH 값을 재사용하는 forward secrecy 기간에 의존
Identity 보호	• 개시자에 대한 수동적 보호, 응답자에 대한 적극적 보호	• JFKi는 개시자에 대한 적극적 보호만 제공 • JFKr은 개시자에 대한 수동적 보호, 응답자에 대한 적극적 보호
암호 협상	• 허용 • Phase 1과 2 모두, 개시자가 암호 suite을 제안하고, 응답자는 이 중 하나를 선택 • 진화가 용이하나, 복잡해짐	• 프로토콜을 간단하게 하기 위해 허용하지 않음 • 키 교환과 IPSEC SA 수립시, 응답자가 천명한 암호 suite만 사용 가능
Phase 개념	• IKE의 phase 1/2 승계 • Phase 1은 다수의 phase 2 메시지 교환 또는 여러가지 SA 제어 용도로 사용 가능	• 프로토콜을 보다 간단하게 하기 위해 사용하지 않음 • 제어 채널이 없으므로 SA 제어를 위한 별도의 수단 필요
인 증	• 인증서 또는 공유 비밀 사용 • legacy authentication system 지원	• 인증서 방식만 사용함으로써 프로토콜의 단순성 유지
계산량 및 통신량	• DOS 공격을 검출하기 위해 구현 복잡도 증가 • 평상시는 4개의 메시지 교환, DOS 공격시에는 6개의 메시지 교환	• 메시지의 일부분을 암호화함으로 구현 복잡도 증가 • 교환되는 메시지 개수는 항상 4개

참 고 문 헌

[1] S. Kent외, "IP Authentication Header," RFC 2402, 1998.

[2] S. Kent 외, "IP Encapsulating Security Payload," RFC 2406, 1998.

[3] Dan Harkins 외, "The Internet Key Exchange (IKE)," RFC 2409, 1998.

[4] IETF, "IETF IPSEC WG Charter," http://www.ietf.org/html.charters/ipsec-charter.html.

[5] W. Simpson, "IKE/ISAKMP Considered Dangerous," draft-simpson-danger-isakmp-01.txt, 1999.

[6] M. Leech, "Position Statement on IKE Development," mailing list of IPSEC WG, 2001.

[7] Dan Harkins 외, "Proposal for the IKEv2 Protocol," draft-ietf-ipsec-ikev2-01.txt, IETF, 2002.

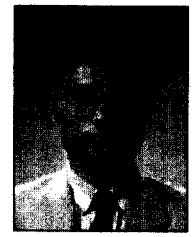
[8] W. Aiello 외, "Just Fast Keying (JFK)," draft-ietf-ipsec-jfk-01.txt, IETF, 2002.

[9] D. Maughhan 외, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, 1998.

[10] H. Orman 외, "The Oakley Key Determination Protocol," RFC 2412, 1998.

[11] H. Krawczyk 외, "SKEME : A versatile Secure Key Exchange Mechanism for Internet," IEEE proc. Of 1996 Symposium on Network and Distributed Systems Security, 1996.

[12] D. Piper 외, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, 1998.



이 계 상

e-mail : ksl@dongeui.ac.kr

1979년 서울대학교 공대 졸업(공학사)

1981년 서울대학교 대학원 전자공학과 (공학석사)

1997년 KAIST 전기및전자공학과(공학박사)

1982년~1997년 한국전자통신연구원 선임연구원

1997년~현재 동의대학교 정보통신공학과 조교수

관심분야 : 인터넷 보안, IPSEC, VPN, 광인터넷 등