단순화된 IKE 프로토콜의 설계

윤희준, 김형국, 최준욱, 김재영, 정선화, 박석천
경원대학교 소프트웨어학부

Design and Evaluation of Simplified IKE Protocol

Hee-Jun Yoon, Hyung-Kuk Kim, Joon-Wook Choi, Jae-Young Kim, Sun-Hwa Jung, Seok-Cheon Park
Division of Software, Kyungwon University
E-mail : scpark@kyungwon.ac.kr

요 약

IP 기반에서 보안 서비스를 제공하는 IPsec은 IP 패킷에 대한 기밀성과 무결성 그리고 인증과 같은 보안 서비스를 제공하는 국제 표준 프로토콜이며, IPsec의 키 관리 프로토콜은 IKE이다. 그러나 기존의 IKE 프로토콜은 구현이 복잡하고 1단계와 2단계의 SA 설정에 총 9번의 과다한 메시지 교환으로 인해 실제 시스템간의 상호 운용성이 떨어질 뿐만 아니라 기존 시스템의 성능을 저하시키는 단점이 꾸준히 제기되어 왔다. 또한 서비스 거부 공격에 대해 매우 취약한 구조를 가지고 있다. 따라서 본 논문에서는 이를 해결하기 위해 IKE가 가지고 있는 대부분의 특징과 속성을 유지하면서 프로토콜을 단순화하고 효율성과 안전성, 유연성을 증대시킬 수 있도록 기존 IKE 프로토콜을 개선하여 단순화된 IKE 프로토콜을 설계하였다.

1. 서론

IP 기반에서 보안 서비스를 제공하는 IPsec(Internet Protocol security)은 IP 패킷(packet)에 대해 기밀성과 무결성 그리고 인증과 같은 보안 서비스를 제공하는 국제 표준 프로토콜이다. IPsec은 AH(Authentication Header)와 ESP(Encapsulating Security Payload), 그리고 IKE(Internet Key Exchange)라는 세부 프로토콜들로 구성되어 있으며 강력한 암호학적 알고리즘과 프로토콜을 이용하여 안전한 보안 서비스를 제공해주고 있다. IPsec의 AH와 ESP를 통해 제공되는 무결성과 기밀성은 송수신자가 같은 키를 공유한 후 공유된 키를 이용해 대칭키 암호 알고리즘, 또는 HMAC(Hash Message Authentication Code)와 같은 함수를 통해 제공된다. 이때 송수신자가 같은 키를 공유할 수 있도록 해주는 메커니즘이 IKE이다. IKE는 공유키의 생성뿐만 아니라 생성된 키의 소멸과 재생성(re-keying)과 같은 키 관리 기능, IPsec에서 사용될 프로토콜 및 알고리즘의 협상기능, 그리고 송수신 양단 간의 사용자 인증 기능 등을 동시에 제공하며, IKE의 자동화된(automated) 메커니즘은 중앙 집중화된 키 분배나 수동 조작(manual setup)을 통한 키 분배의 제약을 극복하여 보다 손쉽고 폭넓은 응용을 가능하게 한다.

그러나 IPsec이 대표적인 보안 프로토콜로 자리를 잡은 오늘날까지 IPsec에 대한 크고 작은 문제점들은 끊임없이 제기되어 왔다. IPsec의 가장 큰 문제점은 전체적인 시스템의 복잡성(complexity)이었다. IPsec의 지나친 복잡성은 시스템의 구현은 물론 구현된 시스템의 상호 호환(interoperability)을 어렵게 할 뿐만 아니라, 구현과정에서 눈에 보이지 않는 보안상의 약점(security holes)을 포함할 수 있다. 그 외에도 IPsec 시스템의 많은 선택사항(IKE의 4가지 인증모드, AH/ESP의 2가지 전송모드 등)들은 개발자나 사용자에게 혼란을 가져올 수 있으며 IPsec 자체는 물론 각 프로토콜의 목적과 응용분야, 설계의 타당성을 언급하는 표준문서의 부재는 이러한 혼란을 더욱 가중시키고 있음을 지적하였다. IKE와 관련되어서는 시스템의 복잡성과 함께 서비스 거부 공격(DoS : Denial-of-Service)에 취약하다는 문제점을 비롯해 보다 향상된 안전성의 보장이 중요한 해결과제로 지적되고 있다.

따라서 본 논문은 이러한 문제점을 해결하기 위하여 IKE가 가지고 있는 대부분의 특징과 속성들을 유지하면서 프로토콜을 단순화하고 효율성과 안전성, 유연성을 증대시킬 수 있도록 기존 IKE 프로토콜을 개선한 단순화된 IKE 프로토콜을 설계하였다.

2. IKE 프로토콜

2.1 IKE 개요

IKE는 IPsec에서 사용할 SA나 ISAKMP에서 사용하기 위한 인증된 키 재료들을 얻기 위하여 ISAKMP와 연계하여 Oakley의 일부와 SKEME(Security Key Exchange Mechanism)의 일부를 이용한 합성 프로토콜이다. ISAKMP는 인증 및 키 교환을 위한 프레임워크로서 1단계와 2단계를 제공하고, Oakley는 각각의 대상이 자신의 속도에 맞게 프로토콜의 상태를 진행해 나갈 수 있는 자유로운 형식의 키 교환 모드를 정의하며, SKEME는 키 공유 및 re-keying 기법을 제공한다. IKE는 중간자 공격(man-in-the-middle-attack)을 방지하며 PFS(Perfect Forward Secrecy)를 제공하도록 설계되었다.

IKE 프로토콜의 목적은 안전한 방법으로 인증된 필수적인 키를 협상하고 제공하는 것이다. 그리고 IKE로 구현된 프로세스는 VPN(Virtual Private Network)을 협상하는데 사용할 수 있고, 원격 사용자에게 안전한 호스트나 네트워크에 대한 접속을 제공할 수 있다.

Oakley와 SKEME 같은 프로토콜은 IKE에서 전체를 구현하는 것이 아니고 단지 IKE의 목적에 부합하는 부분만을 구현하면 된다. 즉, IKE는 Oakley와 SKEME 프로토콜과는 독립적이다.

2.2 IKE 키 교환

IKE 프로토콜은 기본적으로 두 개의 인증된 키 교환으로 이루어지는, 메인(main) 모드와 어그레시브(aggressive) 모드로 이루어진다. 이 두 모드는 DH 키 교환에 의해서 키 교환을 위한 두 IKE 개체간의 SA를 생성하기 위한 것이다. 메인 모드에는 6개의 메시지가 교환되며, 어그레시브 모드에서는 3개의 메시지만 교환된다. 이 외에 퀵(quick) 모드가 정의되어 있는데, 퀵 모드는 IKE 프로토콜이 아닌 다른 프로토콜(IPsec 프로토콜)을 위한 SA를 생성하기 위한 것이다. 퀵 모드는 IKE SA에 의해 메시지 교환이 암호화되어 보호된다. 따라서 퀵 모드로 IPsec SA를 생성하기 위해서는 메인 모드나 어그레시브 모드 메시지 교환을 통하여 IKE SA가 이전에 설정되어 있어야 한다.

따라서 IKE는 IKE SA를 생성하는 1단계 키 교환과 실제 IPsec 프로토콜이 사용할 SA를 정의하는 2단계 키 교환으로 이루어진다. 그리고 1단계에서 생성된 SA는 방향성이 없고, 2단계에서 생성된 SA는 방향성이 있다. 즉, IKE 객체 둘 중 하나가 시작하여 IKE SA가 생성되었다면, 응답자가 2단계 키 교환 보호를 위해서 보내는 메시지도 이 IKE SA에 의해서 보호할 수 있다. 2단계 SA(IPsec SA)는 방향성이 있으므로, 수신하기 위한 SA와 송신하기 위한 SA가 따로 설정되어야 한다. 그림 1은 이러한 IKE의 처리 절차도를 나타낸다.

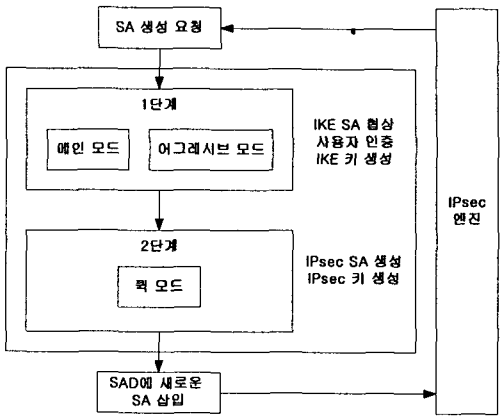

그림 1. IKE 처리 절차도

메인 모드나 어그레시브 모드를 위해서는 4가지의 인증방법이 가능한데, 전자서명, 두 가지 형태의 공개키 암호화에 의한 인증, 사전공유(pre-shared) 키 방법이 있다.

3. 단순화된 IKE 프로토콜 설계

3.1 설계시 고려사항

단순화된 IKE 프로토콜 설계시 고려되어야 할 요구사항은 다음과 같다.

① 프로토콜의 단순화 : IKE 프로토콜의 많은 선택사항(IKE의 인증 모드와 인증 방법)들은 개발자나 사용자에게 혼란을 줄 수 있으므로, 불필요한 선택사항을 제거하여 프로토콜을 단순화하여 설계하여야 한다.

② 프로토콜의 효율성 증가 : IKE의 메인 모드의 6단계 메시지 교환은 처리 시간을 낭비하고, 어그레시브 모드는 ID hiding 기능을 제공하지 못한다. 따라서 메시지 교환을 수정하여 프로토콜의 효율성이 증가되도록 설계하여야 한다.

③ 프로토콜의 보안 기능 개선 : IKE의 취약점인 공격자가 수백 개의 랜덤 IP를 이용해 응답자에게 연결 설정 메시지를 요청하여 응답자의 리소스를 점유하는 DoS 공격에 대응할 수 있는 메커니즘이 추가되어야 한다.

④ 기존의 IKE에 대한 불필요한 변화의 최소화 : 기존 IKE가 가지고 있던 대부분의 특징 및 속성들(identity hiding, PFS, two phases 등)을 유지하면서 최소한의 수정만으로 설계되어야 한다.

따라서, 본 논문에서는 위에서 제시된 요구사항을 모두 수용할 수 있는 새로운 IKE 프로토콜을 설계하였다.

3.2 단순화된 IKE 프로토콜 동작 절차

3.2.1 1 단계 통신

1단계는 IKE_SA_INIT과 IKE_AUTH라는 2개의 라운드로 구성되어있으며 각 라운드는 request와 response의 메시지 쌍을 가지기 때문에 총 4개의 메시지를 주고받도록 설계하였다. 이는 기존의 IKE가 많은 상이한 키 교환을 지원하기 위한 프레임워크를 다룬 ISAKMP의 "ID Protection" 메시지 교환 절차를 따르다보니 실제 IKE에서는 불필요한 과도한 6번의 메시지 교환으로 인해 비효율적이어서 이를 개선하여 설계한 것이다. 1단계 첫 번째 쌍(IKE_SA_INIT)은 IKE 메시지를 보호하기 위한 암호화 알고리즘, 서명, 해쉬 알고리즘 등의 SA를 협상하고, nonce 값과 함께 DH 키 교환에 필요한 값을 주고받는다. 첫 번째 라운드가 끝나면 송신자와 응답자는 암호 알고리즘에 사용할 키 값을 계산할 수 있으며 이후 전송되는 모든 메시지들은 여기서 계산된 키 값과 협상된 암호 알고리즘에 의해 보호받는다.

기존의 IKE 프로토콜은 중간자 공격에 대비해 4가지의 인증 방식(전자서명, 공개키 암호화, 수정된 공개키 암호화, 사전공유 키)을 제공한다. 하지만 공개키 암호화와 수정된 공개키 암호화 방식을 이용한 인증 방식은 통신을 하려는 모든 노드에 수동으로 자신의 공개키를 모두 복사해야하는 문제점이 있다. 만약 n개의 노드와 통신을 하려고 한다면 노드 개수별 키의 수는 n(n-1)/2개가된다. 이 경우 관리자가 모든 노드에 키를 안전하게 분배하기란 결코 쉽지 않다. 이로 인해 현재 공개키 암호화를 이용한 방식과 수정된 공개키 암호화를 이용한 방식은 사용되지 않고 있다. 따라서 본 논문에서 설계한 IKE 프로토콜에서는 인증 방식을 전자서명을 이용한 방식과 사전공유 키를 이용한 방식으로 단일화하여 설계하였다. 또한 AUTH 페이로드를 이용하여 2가지 인증 방식이 가능하게 하면서도 1단계 통신의 전체적인 구조를 동일할 수 있도록 설계하였다.

다음에 수행되는 1단계의 두 번째 쌍(IKE_AUTH_request / response)은 서로를 확인하기 위한 정보와 인증(메시지/사용자 인증)에 사용될 정보를 교환한다. 또한, AH, ESP 등의 프로토콜과 해당 프로토콜에서 사용할 암호 알고리즘에 대한 협상이 가능하다. 두 번째 라운드의 메시지들은 첫 번째 라운드에서 설정된 키 값에 의해 보호받는다. 1단계 통신의 메시지 교환은 그림 2와 같다.

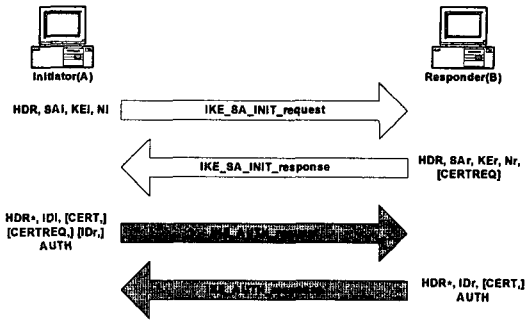

그림 2. 1단계 통신의 메시지 교환

IKE_SA_INIT을 수행하고 나면 A와 B는 IKE_SA에 사용될 키 생성에 필요한 SKEYSEED 값을 공유하게 된다. SKEYSEED를 통해 생성되는 키의 용도로는 SK_e는 이후에 전송되는 메시지들의 암호화에 사용되고, SK_a는 이후에 전송되는 메시지들의 인증(무결성 검증)에 사용된다. 그리고 SK_d는 IPsec_SA를 위한 다른 키 값 생성에 사용된다.

따라서, IKE_SA_INIT 이후에 전송되는 모든 메시지들은 SK_e와 SK_a에 의해 보호를 받는다. 즉, SK_e에 의해 헤더를 제외한 모든 페이로드가 암호화되며 SK_a를 통해 헤더를 포함한 모든 페이로드가 인증 함수에 입력되어 불법적인 도청이나 메시지 위변조로부터 보호를 받는다. 3, 4번 메시지의 HDR*는 헤더를 제외한 해당 데이터들이 SK_e와 SK_a에 의해 암호화되고 인증(무결성 보장)된다는 것을 뜻한다.

메시지 3과 4를 수신한 B와 A는 상대방을 인증하기 위한 AUTH 페이로드를 검증하고 ID 페이로드의 내용이 AUTH 페이로드의 생성에 사용된 키와 일치하는지를 확인해야한다.

3.2.2 DoS 공격에 대응한 1단계 통신

IKE 프로토콜은 위조된 IP 주소들을 이용해 무수히 많은 연결을 시도하여 응답자의 메모리와 CPU를 소모시키는 형태의 DoS 공격이 있을 수 있다.

이 경우 응답자는 IKE_SA_INIT_request의 응답으로 IKE_SA_INIT_response 메시지를 전송하고, KEi와 KEr을 이용해 많은 연산이 필요한 DH 값을 계산해야 할 뿐만 아니라 송신자의 IKE_SA_INIT_request와 관련된 상태 정보(IP, SPI, nonce 등)들을 저장해야한다. 이러한 방식은 응답자의 리소스를 점유함으로써 응답자가 정상적인 연결 요청에 응답 못하게 하는 결과를 초래할 수도 있다. 이와 같은 공격은 연결을 시도하는 당사자가 주장하는 IP가 유효한(실제로 IKE 통신을 원하는) 주소인지가 확인되기 전까지 어떠한 상태 저장이나 CPU 소모(공개키의 지수 연산 등)를

하지 않게 함으로써 예방할 수 있으며 "stateless cookie"를 이용해 이를 설계하였다. DoS 공격을 대응한 1단계 통신의 메시지 교환은 그림 3과 같다.

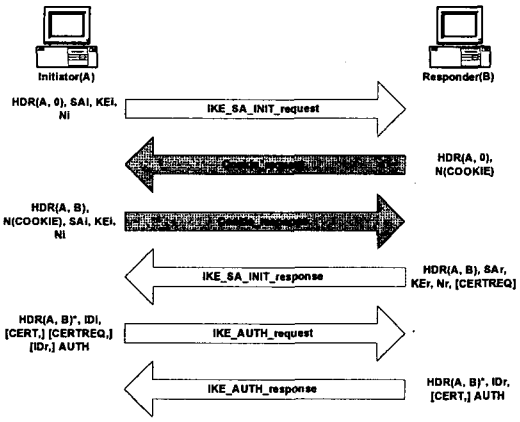

그림 3. DOS 공격에 대응한 1단계 통신

응답자는 많은 수의 IKE_SA 설정 요청을 받게 되었을 때 cookie 값을 포함하는 notify 페이로드를 이용해 요청 메시지(IKE_SA_INIT_request)들을 거부할 수 있다. 자신의 요청에 이러한 응답을 받은 개시자는 응답자가 보내온 cookie 값을 첫 번째 페이로드로 하여 이전의 요청 메시지(IKE_SA_INIT_request)를 재전송하게 된다. 즉, 2번의 메시지 교환을 하는 기본 1단계에 비해 1번의 메시지 교환(cookie exchange)이 추가된다.

IKE를 구현할 때에는 cookie 계산 및 검증시 어떤 정보의 저장 없이도 가능하도록 해야한다. 또한 cookie는 상대방의 IP 주소와 공격자가 예측할 수 없는 랜덤한 값을 반드시 포함해야한다.

4. 결론

IPsec은 IP 패킷에 대해 기밀성과 무결성 그리고 인증과 같은 보안 서비스를 제공하는 국제 표준 프로토콜이다. IPsec의 AH와 ESP를 통해 제공되는 무결성과 기밀성은 송수신자가 같은 키를 공유한 후 공유된 키를 이용해 대칭키 암호 알고리즘, 또는 HMAC과 같은 함수를 통해 제공된다. 이때 송수신자가 같은 키를 공유할 수 있도록 해주는 메커니즘이 IKE이다. 그러나 기존 IKE는 구현이 복잡하고, 서비스 거부 공격(DoS)에 대해 매우 취약한 구조를 가지고 있다. 이러한 IKE의 복잡성은 IKE 구현 제품에 보안 허점의 존재 가능성을 높인다. 이러한 문제점을 해결하기 위해서는 IKE가 가지고 있는 대부분의 특징과 속성들을 유지하면서 프로토콜을 단순화하고 효율성과 안전성, 유연성을 증대시킬 수 있도록 기존 IKE 프로토콜을 개선할 필요가 있으며, 본 논문에서는 위에서 제시된 요구사항을 모두 수용할 수 있는 새로운 IKE 프로토콜을 설계하였다.

본 논문에서는 이를 위해 먼저 기존 IKE 프로토콜의 2가지 모드(메인, 어그레시브)와 4가지 인증 방법(전자서명, 공개키 기반, 수정된 공개키 기반, 공유된 비밀키) 중 사용되지 않는 어그레시브 모드와 공개키 기반, 수정된 공개키 기반의 인증 방법을 제거하고 전자서명과 공유된 비밀키에 기반한 방식으로 단일화시켰다. 또한 DoS 공격시 연결을 시도하는 당사자가 주장하는 IP가 유효한 주소인지 확인되기 전까지 어떠한 상태 저장이나 CPU 소모를 하지 않게 함으로써 DoS 공격을 예방할 수 있도록 설계하였다. 그리고 기존 IKE가 가지고 있던 대부분의 특징 및 속성들을 그대로 유지하면서 최소한의 수정만으로 단순화된 IKE 프로토콜을 설계하였다.

향후 연구방향으로는 설계한 IKE 프로토콜의 성능을 평가하기 위하여 기존 IKE 프로토콜의 동작을 모니터링한 후, 각 단계별 메시지 교환 시간을 측정하고 이를 토대로 새로운 IKE 프로토콜과 성능 비교를 수행할 예정이다.

[참고문헌]

[1] S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, Nov 1998
[2] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, Nov 1998
[3] D. Maughan, "Internet Security Association and Key Management Protocol", RFC 2408, Nov 1998
[4] D. Harking and D. Carrel, "The Internet Key Exchange", RFC2409, Nov 1998
[5] N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPsec", Counterpane, 1999
[6] P. Hoffman, "Features of Proposed Successors to IKE", IETF WG, May 31. 2002
[7] 강권학, "ISAKMP 프로토콜", 안철수연구소, 2002
[8] 강권학, " VPN-IKE 프로토콜", 안철수연구소, 2002
[9] 이정훈 외, "VPN을 위한 자동 키 관리", 비트프로젝트 67호