인터넷 키 관리 프로토콜 IKE와 IKEv2에 관한 비교 연구

임수현°, 박용진
한양대학교 대학원 네트워크 컴퓨팅 연구실
shlim@nclab.hanyang.ac.kr°, park@nclab.hanyang.ac.kr

A study for internet key management protocols : IKE & IKEv2

Su-Hyoun Lim°, Yong-Jin Park
Network Computing Lab., Hanyang University

요 약

IPsec는 IP layer에서의 보안을 제공하기 위해 제안된 프로토콜이다. 이를 구현하는데 있어서 아직은 여러가지 문제점들이 있다. 그 중 하나가 키 관리 프로토콜인 IKE의 복잡성과 보안 상의 허점 때문이다. IETF IPsec WG에서는 이러한 문제점을 해결하기 위한 프로토콜들을 제안해 왔으며 최근에, IKE를 대체할 프로토콜로 결정한 것이 IKEv2이다. IKEv2는 IKE를 기반으로 하여 보다 단순하고 강건하게 설계된 프로토콜이다. 본 논문에서는 현 IKE와 IKEv2를 소개하고 개선된 점을 위주로 비교 분석한다.

1. 서 론

인터넷의 이용이 증대됨에 따라 여러 가지 영역에서 활용되고 있다. 사용 영역이 확대되면서 많은 이슈들이 대두되고 있다. 그 중 하나가 보안이다. 전자상거래나 가상 사설망(VPN, Virtual Private Network)등의 구축에 핵심이 되는 분야가 인터넷 보안에 관한 것이다. IP VPN 구축에 있어서 IPsec는 핵심 보안 프로토콜로 인식되고 있다. IPsec[1]는 암호 알고리즘 및 프로토콜을 이용하여 통신 쌍방이 안전하게 IP Packet을 전달할 수 있도록 한다.

IPsec는 IP 패킷에 대한 무결성(data integrity)과 기밀성(confidentiality)을 제공하는 보안 프로토콜인 AH (Authentication Header) Protocol[1], ESP (Encapsulation Security Payload) Protocol[2]과 이들 보안 프로토콜의 안전한 키 교환과 관리를 담당하는 응용계층의 IKE(Internet Key Exchange) Protocol[3]로 구성된다.

IP VPN을 구축하는데 있어서 IPsec은 강력한 보안을 제공할 수 있다. 하지만 IPsec으로 VPN을 구현하는데 있어서 몇 가지 문제점들이 있다. 그 중 하나가 현재 키 관리 프로토콜의 표준안인 IKE의 복잡성 때문에 생기는 것들이다. 구현이 어렵고 보안에 허점이 생길 가능성이 많다. 또, 다른 IPsec 구현 제품과의 상호 연동성에 문제가 발생할 수 있으며, DoS(Denial of Service)에 취약한 한계가 있다.

이러한 문제들을 해결하기 위해 IETF IPsec WG에서는 2001년 8월에 복잡한 현 IKE 프로토콜을 대체할 수 있는 후속 키 관리 프로토콜(Son of IKE)을 개발하기로 하여 제안된 SOI로는 2개의 공식 후보안(WG draft : IKEv2, JFK)과 1개의 비공식 후보안(individual draft : SIGMA)이 있으며, 2002년 7월에 IKEv2를 중심으로 JFK의 장점을 취하는 최종안을 발표하여 지금까지 draft문서의 수정 작업을 진행하고 있다. 현재의 최종 draft는 draft-ietf-ipsec-ikev2-10.txt 이다.

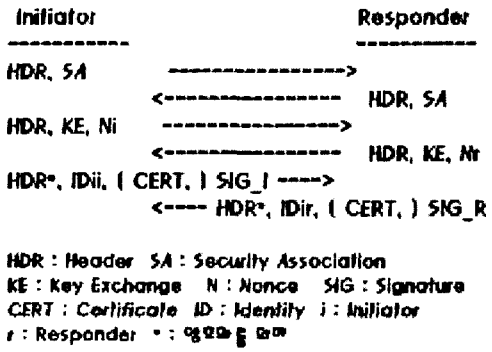
2. IKE 프로토콜

IPsec이 보안 서비스를 제공하기 위해서는 보안 통신을 하는 양단에 필요한 상태정보를 담고 있는 SA(Security Associate)를 사전에 설정하고 관리해 줄 필요가 있다. SA는 수동적인 방법으로 설정이 가능하나 대규모 네트워크에서는 사실상 불가능하기 때문에 자동으로 설정해 줄 프로토콜이 필요하다. 이를 위해서 개발된 프로토콜이 IKE이다. IETF에서 1998년에 표준으로 제정된 IKE(Internet Key Exchange)는 ISAKMP(Internet Security Associate Key Management Protocol)[4], Oakley, SKEME(Secure Key Exchange Mechanism)을 부분적으로 수용하고 있다. ISAKMP에서는 프레임 워크와 메시지 교환방식, phase개념 등을, Oakley 프로토콜에서는 키 교환 모드를, SKEME에서는 융통성 있는 키 교환 기법을 가져왔다.

IKE는 두 가지 phase로 동작한다. phase1에서는 IPSsec 통신을 위한 최초의 보안 채널을 형성하는 단계이며, IKE-SA의 협상과 통신 양단을 인증한다. Phase 2에서는 phase 1에서 생성된 보안 채널을 통해 실제 IPsec통신에 필요한 SA를 생성, 관리하는 역할을 한다.

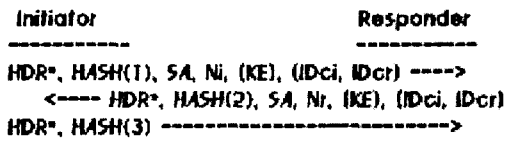
IKE의 메시지 교환 모드에는 phase1에 6개의 메시지를 교환하는 main mode, 3개의 메시지를 교환하는 aggressive mode, phase2에 2개의 메시지를 교환하는 quick mode가 있다. IKE phase1에서는 또한 양단간의 인증을 수행하는데, 이 인증 방식에는 네 가지가 있다. 디지털 서명 방식(authentication with digital signature), 공개키 방식(authentication with public key encryption),

공개키 변형방식(A revised method of authentication with public key encryption), 공유키 방식 (authentication with pre-shared key)이 그것이다.
위에서 기술한 것들을 조합해 보면 IKE 메시지 교환 방식에는 phase1에 8개 phase2에 1개로 총 9가지가 존재한다. 이는 다양한 방식을 지원하고자 제안되었지만, 결과적으로 IKE의 복잡성을 가중시킨다.
[그림1]은 phase1에서 디지털 서명 방식을 이용한 main mode의 메시지 교환을 보여준다.



[그림1] phase1 메인 모드의 메시지 교환(서명인증방식)

메시지 1과 2의 교환으로 SA 협상이 수행되고, 메시지 3, 4에서 키 분배를 위한 DH(Diffie-Hellman) 공개값(KE)이 교환된다. 메시지 5, 6에서는 상호 인증을 위한 과정이 수행되는데, identify(ID)와 signature(SIG-I/R), 그리고, 선택적으로 인증서([CERT])가 교환된다. 5, 6번 메시지는 이전 4단계까지의 메시지를 통해 교환된 SA와 키로 암호화 된다.

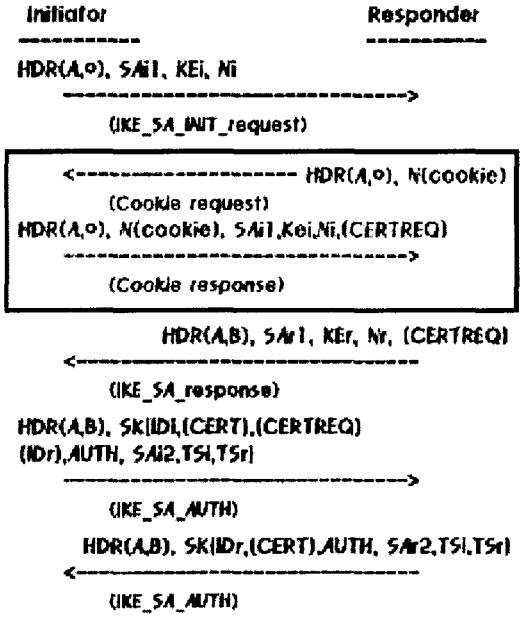


[그림2] phase2 Quick mode 메시지 교환

phase1에서 IKE-SA가 수립되면, 이 IKE-SA를 바탕으로 IPsec-SA를 위한 phase2의 메시지가 교환된다. 아래 (그림2)는 phase2의 Quick 모드 메시지 교환을 보여준다. Phase2에서는 IPsec를 위한 SA를 협상하고, 키 값과 ID를 교환한다.

3. IKEv2

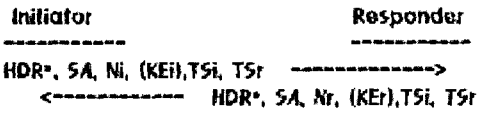
IKEv2는 IKE의 후속 프로토콜로서 IETF IPsec WG에서 여러 가지 IKE의 문제점들을 보완하기 위해 2001년 8월부터 논의된 프로토콜이다. IKEv2는 IKE의 대부분의 속성들(identity, hiding, PFS, Two phases, Cryptographic negotiation 등) 유지하면서 효율성과 안전성, 강건성, 유연성을 증대시키는 방향으로 재구성 되었다.
IKEv2는 IKE의 2 phase 방식과 SA negotiation을 계승한다. 반면에, 인증방식을 디지털 서명 방식 하나로 간소화 했으며, phase1에서도 IPsec-SA negotiation이 가능하게 했다. DoS 공격에 대응하는 메커니즘으로 공격이 예상 되면 Cookie 정보를 가진 추가 메시지 교환을 하도록 되어있다.



[그림3] IKEv2 phase1 메시지 교환(with DoS 예방)

Phase1은 기본적으로 4개의 메시지로 구성되며 첫번째 메시지 쌍인 IKE_SA_INIT에서는 IKE_SA의 협상 및 설정에 필요한 D-H 키 교환을 수행하고 nonce 값과 필요한 parameter들을 교환한다. IKE_SA_INIT이 완료된 이후의 메시지는 설정된 IKE_SA에 의해 암호학적 보호를 받게 된다. 두번째 메시지 쌍인 IKE_AUTH에서는 상호 인증을 위한 식별정보와 인증 정보를 교환하고 Child-SA 설정에 필요한 parameter들을 협상한다. 이 때 child-SA를 협상함으로써 IPsec-SA의 생성 지연을 최소화 할 수 있다.
Dos 공격이 예상되는 경우에는 IKE_SA_INIT의 첫번째 메시지를 받은 responder는 initiator에게 initiator의 IP 주소와 ISAKMP의 cookie 값, 그리고, 자신만이 아는 비밀값의 해쉬 코드를 암호화 하여 cookie를 생성하여 응답하고, initiator는 받은 cookie 정보에 메시지 1을 덧붙여

responder 에게 반환함으로써 responder 가 정당한 initiator 와 암호 통신을 시작하는 것임을 확인한다.



[그림 4] IKEv2 phase2 의 child-SA 생성 메시지 교환

[그림 5] IKEv2 phase2 의 정보 메시지 교환

[그림 4]와 [그림 5]는 Subsequence exchange 를 보여준다. 이는 두 개의 메시지로 구성되며, child-SA 를 설정하거나[그림 4], 프로토콜 수행 중에 발생한 오류 정보 및 이벤트 발생 정보 등을 교환[그림 5]한다. 또한 SA 의 재설정에도 사용된다. Subsequence exchange 는 그 용도에 따라 child-SA 를 설정하거나 기존 SA 를 재설정하는 create-child-SA 와 오류정보 및 이벤트 발생정보를 교환하기 위한 informational exchange 로 구분한다.

[표 1] IKE vs IKEv2

	IKE	IKEv2
Phase	Phase1 : IKE-SA negotiation Phase2 : IPsec-SA negotiation	Phase1 : SA negotiation Phase2 : rekeying (child-SA negotiation) Information change
mode	Main/Aggressive/Quick mode	Initial exchange Subsequence exchange
Negotiation	허용 initiator가 암호 suit 제안, responder는 이 중 하나 선택 새로운 암호 메커니즘을 수용하기에 용이하나 복잡해짐	
인증방식	4가지	1가지
DoS 공격에 대한 대응방안	취약	필요시 cookie 교환 공격검출 메커니즘 필요

[표 1]은 개략적인 IKE와 IKEv2의 특성들을 도표화 한 것이다.

4. 결론

IPsec은 IP layer에서 IP Packet 에 대한 보안 서비스를 제공하는 프로토콜로, IP VPN 구축뿐만 아니라 앞으로 모바일 인터넷 보안 등을 위한 핵심 보안 프로토콜이다. 그러나 IPsec의 key management protocol인 IKE의 복잡성으로 야기되는 구현상의 어려움과 낮은 상호 연동성, 그리고 DoS 공격에 취약함 등의 문제가 있다. 또, 모바일 네트워크에 적용하기에는 적합하지 않다. 이러한 문제점들을 해결하기 위한 방안으로 제시된 것이 IKEv2이다. IKEv2는 IKE의 개념을 그대로 계승하여 phase 1/2로 나누어 메시지를 전달하며, SA 협상 과정을 거친다. 이는 융통성을 유지하기 위한 방안이다. IKE와의 가장 큰 차이점은 두 가지로 볼 수 있다. 그 하나는 자주 사용되지 않는 옵션들을 없애서 프로토콜을 단순화 하였다는 것이고, 두번째는 Cookie 메시지를 교환 함으로서, DoS 공격에 대응하는 메커니즘을 추가 하였다는 점이다. 이것은 DoS 공격을 검출해 내야 하므로, 구현 시에 DoS 공격 검출 메커니즘의 추가가 필요하다. 앞으로 ikev2를 적용하는데 있어서 Dos의 효율적인 검출 방법의 적용이 IPsec 시스템의 적용에 관건이 될 것이다.

[참고문헌]

[1] S. Kent 외," IP Authentication Header" RFC2402,1998
[2] S. Kent 외," IP Encapsulating Security Payload" , RFC 2406, 1998
[3] Dan Harkins 외, " The Internet Key Exchange(IKE)" , RFC 2409,1998
[4] D. Maughhan 외, " Internet Security Association and Key Management Protocol (ISAKMP)" , RFC 2408, 1998
[5] IETF, " IETF IPsec WG Chapter" , http://www.ietf.org/html.charters/ipsec-charter.html
[6] Charlie Kaufman, " Internet Key Exchange (IKEv2) Protocol" draft-ietf-ipsec-ikev2-10.txt, 2003