IPsec 시스템에서 IKE 프로토콜 적용에 관한 연구

*홍용근, 이승윤, 박기식, **이달원, 조인준

*한국전자통신연구원, **배재대학교

A study on Application of IKE protocol in IPsec System

*Yongkeun Hong, Seungyun Lee, Kishik Park, **Dalwon Lee, Injune Jo

*ETRI, **Paichai Univ.

요 약

IPsec은 차세대 IP 프로토콜인 IPv6에서 필수 구현 사항이며, 네트워크 계층에 적용되어 보안 서비스를 제공하며, 모든 인터넷 서비스를 대상으로 일관된 보안 서비스 제공이 가능하다는 특징을 지닌 국제 표준 프로토콜이다. 이러한 IPsec 시스템에서 키 분배 및 관리를 위해 사용되고 있는 IKE 프로토콜은 시스템의 복잡성 문제와 함께 DoS 공격에 취약하다는 문제점이 발견되어 이를 해결하고자 IPsec WG에서 개선 작업 중에 있다. 본 논문에서는 기존 IKE 프로토콜(IKEv1)의 문제점과 IPsec WG에서 개선 작업중인 IKEv2와 JFK 두가지 후보안의 분석된 내용을 정리하였으며, 분석 정리된 내용들이 기존 IKE 프로토콜에 적용시 보안기능 관점에서 고려해야할 사항들을 정리하였다.

I. 서론

정보시스템 내에서 처리, 축적, 전달되는 정보는 전기적 현상을 이용하여 디지털화, 대용량화되고 있어 정보에 대한 적절한 보호조치가 없으면 전송, 처리 혹은 기억장치에 보관된 상태에서 불법 유출 삭제 및 수정 등의 위험에 노출되기 쉽다. 이러한 원치 않는 불법적인 사고로 인하여 개인 사생활 침해뿐만 아니라 막대한 경제적 손실을 당할 우려가 있어 정보보호에 대한 관심은 점점 고조되고 있는 상황이다. 이러한 중요성은 이미 국제 표준화기구인 IETF(Internet Engineering Task Force)에서도 인식되었고, 특히 본 논문에서 언급한 IPsec WG는 이미 1993년 6월부터 작업을 시작하여 현재 IPsec 아키텍쳐를 기술한 RFC2401을 비롯하여 21개의 RFC를 작성하였다[1]. 1995년 IPsec이 처음으로 발표되었고, 이전까지 IP 계층의 보안을 위해 제안되었던 swIPe와 SIPP(Simple Internet Protocol Plus)을 근간으로 제정되었던 1995년의 표준(RFC1825-1829)에는 키 분배를 위한 표준이 제시되지 못하였으나, 1998년에 개정된 표준에 비로서 현재의 AH(Authentication Header)와 ESP(Encapsulation Security Payload), IKE(Internet Key Exchange)로 이루어진 IPsec(Internet Protocol security)이 발표되었다[2].

IPsec은 네트워크 계층에 대해 confidentiality, data origin authentication, connectionless integrity, protection against replays, limited traffic flow confidentiality, access control 등과 같은 보안 서비스를 제공하는 국제 표준 프로토콜로서 공개된 네트워크상에서 VPN(Virtual Private Network)을 구현하거나 종단간 보안(end-to-end security)을 위해 응용되고 있다. IPsec이 제공하고 있는 정보보호 서비스가 응용 계층 또는 전송 계층 프로토콜과 독립적으로 네트워크 계층에서 제공되어 일반 인터넷 사용자에게는 투명한 상태로 처리되며, 기존의 응용 소프트웨어에 대한 변경을 필요로 하지 않으며, 모든 인터넷 서비스를 대상으로 편리하면서도 일관된 보안 서비스를 제공할 수 있기 때문에 한 호스트 내에서 일관된 방식의 정보보호 서비스 설정이 가능하다. 또한 현재의 IPv4에서는 선택사항으로 되어 있으나 차세대 IP 프로토콜인 IPv6에서는 필수 구현 사항으로 되어 있다는 특징을 가지고 있다.

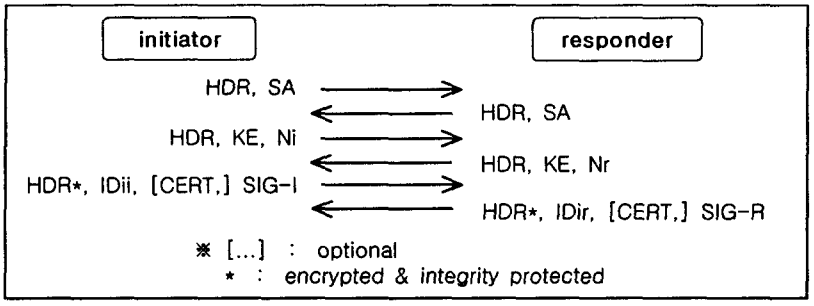
이러한 특징으로 인해 대표적인 보안 프로토콜로 자리를 잡은 IPsec에 대해 1999년 Counterpane 사의 Ferguson과 Schneier는 IPsec의 전체적인 문

제점과 함께 AH, ESP 및 IKE/ISAKMP(Internet Security Association and Key Management Protocol) 각각의 프로토콜에서 개선되어야할 요소들을 지적하였다. 또한 IPsec WG의 메일링 리스트에서 AH 프로토콜과 transport mode의 불필요성 등은 많은 논쟁을 불러일으켰으며, IKE와 관련되어서는 시스템의 복잡성과 함께 DoS(Denial Of Service) 공격에 취약하다는 문제점을 비롯해 보다 향상된 안정성의 보장이 중요한 해결과제로 지적되어 이러한 문제점들을 개선하기 위한 구체적인 작업들을 진행하고 있다[2]. 이 에 본 논문에서는 IKE 프로토콜의 문제점과 IPsec WG에서 개선작업중인 IKEv2와 JFK(Just Fast Keying) 두가지 후보안의 분석된 내용을 정리하였으며, 분석정리된 내용들이 기존 IKE 프로토콜에 적용시 보안기능 관점에서 고려해야할 사항들을 정리하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 표준인 IKEv1과 보안 문제점들을 정리하였고, 3장에서는 IKEv1을 대체하고자 작업중인 SoI(Son of IKE)의 해결방안에 대해 분석된 내용들을 정리하였다. 4장에서는 앞서 살펴본 내용들을 바탕으로 기존 IKE 프로토콜에 적용시 고려해야할 사항들을 보안기능 관점에서 정리하고, 5장에서는 결론을 내린다.

그리고 IKE에서 키교환의 근본을 이루는 메커니즘으로는 Diffie-Hellman 알고리즘이 사용되었다. IKE 프로토콜은 두 단계로 이루어져 있는데 phase 1에서는 phase 2에서의 협상에 필요한 안전하고 인증된 통신 채널을 생성하고 인증된 키 교환을 수행한다. 이 단계에서 수립되는 SA를 IKE SA라고 하며, 상대방에 대한 인증을 위한 메커니즘으로 Digital signature, Preshared Keys, Public key encryption, Revised public key encryption 이렇게 4가지 방식이 지원된다. phase 1 단계에서 지원되는 모드는 두가지로서 identity에 대한 보호(ID hiding)를 제공하지만 메시지 교환회수가 3라운드(6메시지)인 main mode와 identity 보호를 제공하지는 못하지만 메시지 교환 회수를 줄인 aggressive mode가 있다. [그림 1]은 Digital signature 인증 메커니즘이 적용된 main mode를 보여주고 있다. phase 2는 실제로 IPsec에서 사용될 보안 서비스, 암호 알고리즘, 키 등의 정보를 협상하고 교환하는 단계이며 이 단계에서 수립되는 SA를 IPSEC SA라고 하며, quick mode가 사용된다. 결국 quick mode의 통신 내용은 phase 1에서 협상된 보호 메커니즘에 의해 보호를 받게 된다[3,4,5].

1999년 Counterpane사의 Ferguson과 Schneier는 IPsec의 전체적인 문제점과 함께 AH, ESP 및 IKE/ISAKMP 각각의 프로토콜에서 개선되어야 할 요소들을 지적하였다. Ferguson과 Schneier가 지적한 IPsec의 가장 큰 문제점은 전체적인 시스템의 복잡성(complexity)이었다. IPsec의 지나친 복잡성은 시스템의 구현은 물론 구현된 시스템의 상호호환(interoperability)을 어렵게 할 뿐만 아니라, 구현과정에서 눈에 보이지 않는 보안상의 약점(security holes)을 포함할 수 있다고 하였다. 그 외에도 IPsec 시스템의 많은 선택사항(IKE의 4가지 인증모드, AH/ESP의 2가지 전송모드 등)들은 개발자나 사용자에게 혼란을 야기시킬 수 있으며



[그림 1] Main mode with Signatures(Phase1 of IKEv1)

II. IKEv1

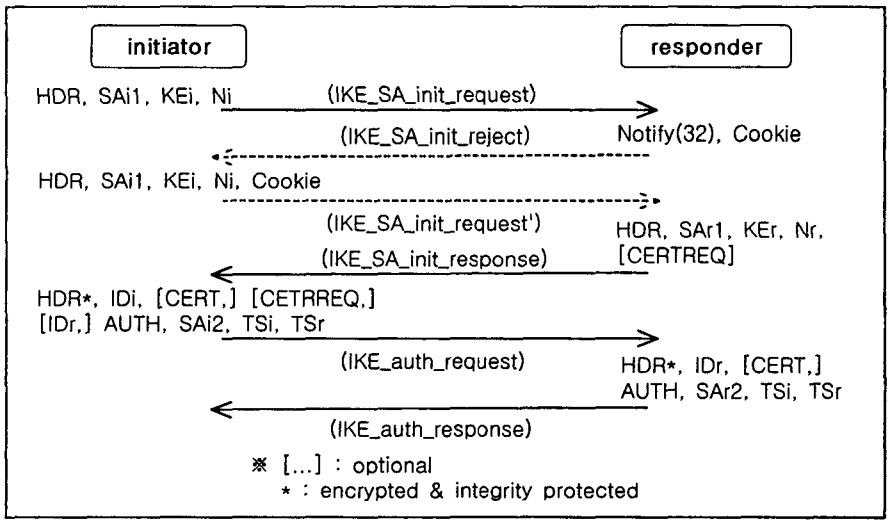
IKE는 IPsec을 위하여 기본으로 설정되어 있는 자동화된 키 관리 프로토콜로서 자동화된 SA협상, 분배 및 갱신, 키 생성을 담당하며 이를 위해 ISAKMP(RFC2408), Oakley(RFC2412), SKEME 등의 프로토콜로부터 만들어 졌다. ISAKMP는 인증 및 키 교환을 위한 프레임 워크를 제공하며 Oakley는 키 교환 모드를 정의하는데 사용되고 SKEME는 키 공유 및 rekeying 기법을 제공한다.

IPsec 자체는 물론 각 프로토콜의 목적과 응용 그리고 설계의 타당성을 언급하는 표준문서의 부재는 이러한 혼란을 더욱 가중시키고 있음을 지적하였다. AH 프로토콜과 트랜스포트 모드의 불필요성 등은 IPsec WG의 메일링 리스트에서 많은 논쟁을 불러일으켰다. IKE와 관련되어서는 시스템의 복잡성과 함께 DoS 공격에 취약하다는 문제점을 비롯해 보다 향상된 안전성의 보장이 중요한 해결과제로 지적되고 있다. IPsec의 개선과 관련되어 IPsec WG의 활동은 AH/ESP와 차세대 IKE(SoI)의 두가지 영역으로 나누어 살펴볼 수 있다. AH나 ESP는 공통적으로 기존의 메커니즘과 포맷을 개선하는데 초점이 맞추어져 있다는 것이 새로운 시스템과의 대체를 고려하고 있는 IKE와의 가장 큰 차이점이다. IKE의 경우에는 기존의 IKE를 대체하기 위해 대체될 프로토콜의 요구사항과 함께 각각의 후보안들을 별도의 draft로 공개함으로써 직접적인 비교, 평가 과정을 공개적으로 진행하고 있다. 이러한 과정을 통해 SoI 후보안들 중 individual draft로 제안되었던 SIGMA(SIGnature Mode of Authentication)를 제외한 IKEv2와 JFK는 지금까지 꾸준한 개정작업이 진행되어오고 있다. 당초 IPsec WG에서는 프로토콜 설계에 대한 타당성 논의를 통해 적당한 후보안을 채택하려 하였으나 아직까지 어떠한 결정도 내리지 못하고 있는 상황이며 현재까지도 계속적인 논의 과정이 이루어지고 있다[2].

III. SoI

IPsec WG에서 기존의 IKE를 새로운 프로토콜로 대체하기 위해 제일 먼저 시작한 작업은 다음 버전의 IKE(SoI)에서 필요로 하는 요구사항들을 정의하는 것이었다. IPsec의 응용 시나리오와 프로토콜, 정책, 보안 요구사항 등 다양한 IKE 요구사항들 중 보안 요구사항에 대해서만 살펴보면 다음과 같다. IKEv1에서 키 동의를 위해 기존 안정성에 충분한 검증을 받았지만 키 교환시 발생하는 고비용 때문에 DoS 공격에 취약한 Diffe-Hellman 방식을 사용하였는데 이와같은 키 동의 요구사항, 키 길이 등을 포함하는 키 생성 요구사항 명시와 키 확장에 대한 상세 명세 요구사항, IKEv1에서 허용하고 있는 다양한 인증 방식에 대한 각각의 분리와 처리방안 그리고 완전한 명세 포함 요구사항, DoS 공격에 대한 대응력 요구사항, replay attack에 대한 예방 요구사항, 구현 권고안에 대한 요구사항, 협상에 필요한 파라미터의 수를 줄이거나 negotiation suites 등의 대안 사용에 대한 요구사항, 수동 공격자(passive attacker)와 더불어 능동 공격자(active attacker)에 대한 ID 정보의 보호에 대한 요구사항, 부인봉쇄에 대한 요구사항, IKE 메시지 전체에 대한 보호 수단 요구사항, 키의 노출로 인해 과거의 session key 안전을 의미하는 PFS(Perfect Forward Secrecy) 보장 요구사항 등이 존재한다.

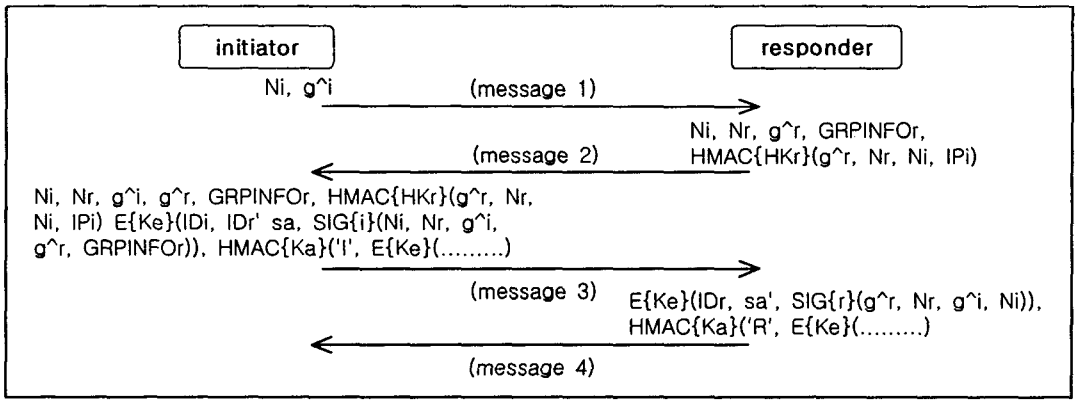
IKEv2는 IKEv1을 작성했던 D.Harkins가 C.Kaufman, S.Kent, T.Kivinen, R.Perlman 등과 함께 IKEv1을 단순화하고 안전성을 강화하는데 초점을 맞추어 설계하였다. 기존 4가지 인증방법 중 signature와 preshared key에 기반한 방식으로



[그림 2] Phase 1 of IKEv2 against DoS

단일화하였으며 ID hiding 기능을 제공하면서도 2 라운드(4메시지)만으로 프로토콜이 가능하도록 하였다. IKEv1과 같이 2-phase 방식을 사용하고 있으나 phase 1을 통해 IKE SA 뿐만 아니라 AH, ESP, IPcomp에 필요한 SA의 설정이 가능하도록 piggybacking 기능이 제공되면서 DoS 공격에 안전하도록 설계되었으며 기존 RFC2407, 2408, 2409 문서들을 하나의 문서에 포함시키고 있다. IKEv2의 phase 1은 4개의 메시지(2개의 request/response 쌍)로 이루어졌으며 IKE SA를 설정한다. 2개의 메시지(1개의 reuest/response 쌍)로 이루어진 phase 2에서는 child SA의 설정 외에 child SA의 삭제, IKE SA의 삭제 및 재생성(rekeying) 그리고 에러나 이벤트 발생과 같은 정보 전달이 가능하다. DoS 공격에 대한 의심이 있을 경우에는 OAKEY 프로토콜에서 적용되었던 stateless cookie를 사용하여 [그림 2]에서와 같이 responder는 자신이 송신한 cookie 값을 돌려 받고 그 값을 확인하기 전까지는 어떠한 상태정보에 대한 저장이나 계산과정을 필요로 하지 않기 때문에 DoS 공격을 막을 수 있을 뿐만 아니라 fragmentation DoS 공격을 막을 수 있다[2].

계에 의한 새로운 접근방법을 사용하고 있다. JFK에서는 JFKi와 JFKr 2개의 프로토콜을 제안하고 있는데 [그림 3]에서 볼 수 있듯이 JFKr은 SIGMA와 IKEv2의 암호학적 설계에 맞춰 JFKi를 변형한 방식으로서 능동 공격자로부터 responder의 identity를 보호하고 initiator의 identity는 수동 공격자에게 안전한 반면, JFKi는 ISO 9798-3 프로토콜을 변형한 방식으로서 능동 공격자로부터 initiator의 identity를 보호한다. JFKi가 JFKr과 다른 점은 2번째 메시지에서 DoS 공격을 예방하기 위한 cookie 값과 함께 자신의 비밀키로 생성한 서명을 함께 전송한다는 것이며 JFKi는 responder의 identity 보다는 initiator의 identity 보호가 중요시되는 client-server 모델에 적합하고 JFKr은 P2P(peer-to-peer) 모델에 더 적합한 방식이라고 설명하고 있다. DoS 공격의 예방은 IKEv2와 같이 stateless cookie를 사용하고 있으나 cookie를 선택적으로 교환하는 IKEv2와 달리 항상 cookie를 교환하는 Photuris의 아이디어를 따르고 있으며, 특이한 점은 initiator가 IKE SA 협상에 필요한 SA를 전송하지 않는다는 차이점을 볼수 있다[2,4].



[그림 3] JFKr protocol

JFK는 프로토콜의 단순성과 효율성 그리고 DoS 예방과 privacy 보장, PFS의 보장 등 안전성의 강화를 목표로 하여 AT&T와 IBM의 연구원, Columbia 대학 교수 등 7명의 보안 전문가들이 공동으로 작성한 SoI 후보 프로토콜이다. IKEv1과의 가장 큰 차이점은 2-phase 방식이 아닌 1-phase 방식을 사용하고 있으며 2번의 라운드(4번의 메시지 교환)만으로 IKE SA는 물론, child SA를 함께 설정할 수 있다는 것이며 인증모드의 경우 signature 기반 방식만을 사용한다는 것이다. IKEv2가 기존의 IKEv1 형식을 유지하면서 개선하는 접근 방식을 취한 반면, JFK는 전혀 다른 설

IV. IKE 구현시 고려사항

SoI 후보안의 가장 큰 차이점으로 IKEv2의 경우에는 단일 방식의 프로토콜을 제시하고 있으나, JFK는 JFKi와 JFKr 두가지 변형된 방식을 제공하고 있다는 것이다. 그리고 각 후보안의 구체적인 보안 요구사항별 해결방안에 대해 정리하면, 우선 두 후보안에서 공통적으로 제공하고 있는 해결방법으로는 PFS의 보장과 DoS 공격에 대한 대응력 강화 이렇게 두가지가 있으며, 나머지 요구사항에 대해서는 차이를 보이고 있다. 다음 [표 1]에 두 후보안의 해결방안에 대해 공통점과 차이점

으로 나누어 정리하였다.

[표 1] SoI 후보안 비교

요구	IKEv2	JFK
공통 제시 해결방안		
DoS	선택적 stateless cookie 적용	모든 메시지에 stateless cookie 적용
PFS	phase 1에서 새로운 DH값 사용	DH값 재사용 기간에 의존
서로 다른 해결방안		
ID hiding	initiator에 수동공격자로 부터 보호, responder는 능동공격자로부터 보호	JFKi(initiator 능동공격로부터 보호, responder 수동공격자로부터 보호) 와 JFKr(JFKi와는 반대) 두가지 제공
IKE SA	협상기능 제공	단순화위해 제공하지 않음
phase	유연성위해 제공	역시 단순화위해 제공하지 않음
인증 방법	signature, preshared 제공	signature만 제공
코드 재사용	IKEv1의 변형으로 가능	새로운 방법 적용으로 불가능

위에서 살펴본것과 같이 두 후보안에서 공통적으로 지원되는 해결방안에 대해서는 기존 IKE에 구현시 보안기능으로 적극 고려해야 할것으로 판단된다, 그리고 새로운 코딩보다는 기존의 코드들을 재사용할 수 있는 코드 유지성면에서 볼 때 JFK 보다는 IKEv2가 우수하다고 판단된다.

[표 2] IKE 구현시 고려사항

요구	IKEv1	IKEv2	JFK	구현
DoS	취약	선택보장	보장	필수
PFS	미약	보장	보장	필수
ID hiding	mode별 제공	부분 제공	부분 제공	용도별
IKE SA	허용	허용	없음	용도별
phase	허용	허용	없음	용도별
인증 방법수	6	2	1	1-2
코드 재사용	-	가능	불가능	고려

또한 IPsec WG에서 후보안에 대한 표준화 작업이 계속 진행중이지만 phase 개념을 이용한 협상의 유연성과 표준문서에서 제공해야할 완전한 명세와 구현 권고안 등을 고려하여 두가지 후보안 중 IKEv2를 기본으로 JFK의 장점을 추가하는 방향으로 표준화 될것으로 판단되기 때문에 이 또한 구현시 고려해야할 사항으로 판단된다. [표 2]에 기존 IKE 프로토콜에 보안 요구사항에 대한 해결방안 적용시 고려해야할 사항들을 정리하였다.

V. 결론

인터넷의 대표적인 보안 표준 프로토콜로 자리잡고 있는 IPsec의 키 분배 및 관리를 위해 사용되고 있는 IKEv1과 보안 문제점 그리고 IKEv1을 해결하기 위해 제안된 IPsec WG의 대표적인 두가지 후보안 IKEv2와 JFK를 보안 관점에서 살펴봄으로서 기존 IKE 프로토콜에 구현 적용시 고려해야할 사항들에 대하여 살펴보았다.

IKE 프로토콜 제품의 경우 raccon(KAME, BSD 계열)과 Pluto(FreeS/WAN, Linux 계열) 등이 존재하며 이들 소스가 공개되어 있지만 이들 제품들을 그대로 수용하여 사용하는데 문제가 있으며 이들을 변경하여 사용할 경우와 직접 제품을 구현할 경우 IPsec WG의 SoI 표준화 작업 과정을 충분히 반영하여야 할것으로 판단된다.

IPsec WG의 SoI 표준화 작업과정을 예의주시하면서, IKE 프로토콜의 전체적인 요구사항에 대해 분석, 반영하여 새로운 IKE 프로토콜을 설계하거나 기존 제품에 반영할 수 있도록 포괄적인 연구가 계속 진행되어야 한다고 판단된다.

참고문헌

[1] 이형규, 나재훈, 손승원, "IPSec 시스템에서 IKE 프로토콜 엔진의 연동에 관한 연구", 정보보호학회논문지, pp.27-35, 2002년 10월.

[2] 최승복, 김해숙, "차세대 IKE(SOI: Son Of IKE) 후보안의 비교", Technical Report, (주) 퓨처시스템, 2002년 6월.

[3] 이만영, 손승원, 조현숙, 정태명, 채기준, 차세대 네트워크 보안기술, 생능출판사, 2002년.

[4] 김한철, 이계상, "IP-based VPN의 키교환 메시지 IKE와 JFK의 성능 비교 분석", 한국통신학회 하계종합학술발표회, 2002년.

[5] 이광수, 신은경, 이홍섭, "IPSec 제품의 적합성 및 상호운용성 시험", 통신정보보호학회지, pp.17-19. 2001년 4월.