IPsec용 차세대 키관리 프로토콜의 동향 및 분석

김진, 이상원, 최철준, 김광조

국제정보보호기술연구소

한국정보통신대학원대학교, 공학부

A Study on Next Generation Key Management Protocol for IPsec

Zeen Kim, Sang-won Lee, Chul-Joon Choi and Kwangjo Kim

International Research center for Information Security (IRIS)

School of Engineering, Information and Communications Univ. (ICU)

요 약

최근 VPN의 구축이 늘어남에 따라, 안전한 VPN을 구축하는 데 있어 강력한 보안기능과 터널기능을 제공하는 핵심 프로토콜인 IPsec의 중요성은 더욱 부각되고 있다. 현재 사용되고 있는 IKE 프로토콜은 기능이 복잡하고 표준규격의 기술(description)이 난해해서 이를 구현한 이기종 제품간에 상호 연동성이 아직까지도 제대로 확보되지 않고 있다. 또한 서비스거부공격에 대한 취약점을 드러내고 있으므로 이들에 대한 보완이 필요하다. 본 논문에서는 이 취약점을 보완하기 위하여 제안된 두 개의 프로토콜 IKEv2와 JFK에 대한 소개와 두 프로토콜의 비교를 한 후, 차세대 키관리 프로토콜로 적합한 것은 이 중 어떤 프로토콜인지 고려해본다.

I. 서론

1. 동향

최근 VPN의 구축이 늘어남에 따라, 안전한 VPN을 구축하는 데 있어 강력한 보안기능과 터널기능을 제공하는 핵심 프로토콜인 IPsec의 중요성은 더욱 부각되고 있다. IPsec 프로토콜의 국제표준화는 IETF(The Internet Engineering Task Force)의 IPsec WG을 중심으로 IPSRA(IP Security Remote Access) WG와 IPSP(IP Security Policy) WG에서 진행하고 있다. IPsec WG은 1999년 발족하여 AH(Authentication Header), ESP(Encapsulation Security Payload), IKE(Internet Key Exchange) 등 주요 IPsec 프로토콜의 표준을 수립하였다. IPSRA, IPSP WG는 2000년 3월 발족되었고, 각각 IPsec을 이용한 원격접속 이슈와 정책 이슈를 다루고 있다.

키관리 프로토콜인 IKE의 문제점을 해결하기 위해 IPsec WG는 새 키관리 프로토콜을 개발하기로 하였고, 두 개의 프로토콜이 제안되어 현재까지 경합하고 있다. 제안된 두 개의 프로토콜이 본 문서에서 설명할 IKEv2와 JFK이다. IKEv2는 기존의 IKE 프로토콜의 개념을 그대로 계승하면서 기능을 대폭 축약한 형태인데 반해, JFK 프로토콜은 완전히 새로 설계한 프로토콜이라는 점에서 서로 대비된다. 다음 장에서 상세히 다루겠지만 결론적으로 JFK는 좀 더 간결한 프로토콜이며, IKEv2는 약간 더 융통성 있는 프로토콜이라 할 수 있다.

당초 IPSEC WG은 올 3월 단일 표준안을 수립할 예정이었으나, 이 두 프로토콜이 기술적으로 대등하여 최근까지 팽팽한 경합을 벌여 표준화 일정이 계획보다 지연되고 있다. 이 두 프로토콜은 기술적으로 거의 대등한 특성을 갖고 있어 기술적으로는 우열을 가리기 힘든 것으로 보인다. 올 여름 몇 주간 메일링 리스트에서 진행된 기능별 두 프로토콜의 비교작업에 대한 7월 일본 요코하마 회의에서의 요약결과도 마찬가지였다. 하지만, 이 회의를 통한 WG의 전체적인 분위기는 이 두 프로토콜에 대한 논의가 충분히 진행된 것으로 보고, 이제는 이 중 어느 한가지로 결정해야될 시점에 왔다고 보는 것이 지배적이었다. 따라서, 요코하마 회의에서 WG 의장은 후속 키관리 프로토콜 표준화를 다음 미국 아틀란타 회의 때까지는 마무리짓는다는 목표로 다음과 같은 표준화 추진일정을 제시하였다.

즉, 8월말까지는 프로토콜 특성에 대한 논의를 종결짓고, 9월 말까지는 후속프로토콜에 대한 단일문서를 완성하여, 10월 중 논의를 마무리한 후, 11월 초까지는 문서를 갱신하여, 같은달 중순에 있을 아틀란타 회의에서 마무리한다는 일정이었

다.

2002년 아틀란타 IETF 회의의 최대 쟁점은 지난 1년여 동안 계속 논의해온 IKE의 후속 프로토콜 표준에 관한 것이었다. 이 회의직전 IKEv2와 JFK 프로토콜은 하나의 문서로 단일화됐으나 여러가지 기술적 문제들이 해결되지 않아 이번 회의의 주요 의제로 논의됐다.

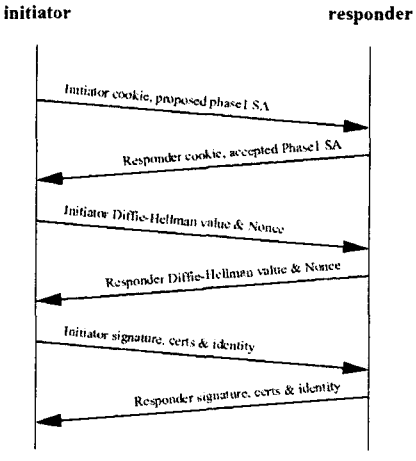
대략 7가지 기술 이슈 가운데 교환메시지의 개수문제와 알고리듬 협상방식에 대해서는 이번 회의에서 합의됐으나 나머지는 뒤로 미뤄졌다. IETF 집행부는 2003년까지 워킹그룹 내 합의를 촉구했다.

2. IKE의 문제점과 새로운 키관리 프로토콜의 요구사항

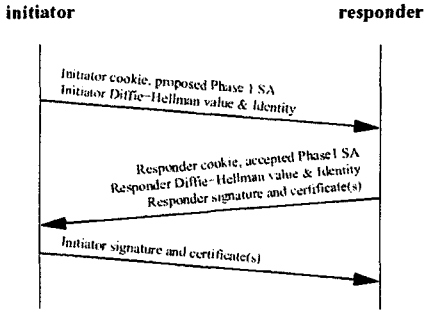
현재 사용되고 있는 IKE 프로토콜은 기능이 복잡하고 표준규격의 기술이 난해해서 이를 구현한 이기종 제품간에 상호 연동성이 아직까지도 제대로 확보되지 않고 있다. 또한 서비스거부공격에 대한 취약점을 드러내고 있으므로 이들에 대한 보완이 필요하다.

자세히 살펴보면, (그림 1)에서와 같이 IKE는 많은 메시지 교환작업을 통해서 비효율적이라는 점이 지적되어 있었다. 그렇다고하여 (그림 2)의 Aggressive 모드를 사용하는 경우는 안전성에 취약점을 드러낸다.

이 때문에 IKE의 이후의 새로운 IPsec 키관리 프로토콜의 요구사항으로는 크게 두가지를 들 수 있다. 첫째, 프로토콜에 대한 기술을 명확히 하여 구현, 실행, 동작하는 데 있어서 어려운 점이 없어야 한다. 둘째, 서비스거부 공격에 대한 안전성을 반드시 확보하고 있어야 한다. 는 것이 바로 그 두 가지 요소이다.



(그림 1) IKE Main Mode



(그림 2) IKE Aggressive Mode

3. 논문의 구성

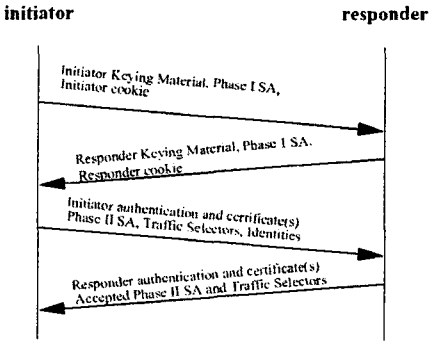
본 논문은 IPsec의 새로운 키관리 프로토콜이 될 두 개의 후보 프로토콜인 IKE version 2 (IKEv2)와 Just Fast Keying (JFK)관련 동향과 각 프로토콜의 특성을 소개한다. 또한 현재 진행중인 고속암호기술 과제에 적합한 프로토콜로는 이들 중 어떤 프로토콜인지 고려해본다.

서론에서 관련 표준화 동향의 소개와 IKE의 문제점과 후속 키관리 방법에 대한 요구사항을 소개한다. 2장에서는 후보 알고리즘 IKEv2를 간략히 소개하고, 3장에서 후보 알고리즘인 JFK를 상세히 소개하며, 4장에서 두 알고리즘을 비교·분석한다.

II. IKEv2

IKEv2는 IKE와 용어가 동일하고, 기본적인 틀이 IKE와 같으므로 간략하게 소개하도록 하겠다.

IKEv2의 Phase I은 (그림 3)과 같이 4회의 교환으로 이루어진다. 이들 과정을 통해 SA 협상을 완료하고, Phase II에서 사용될 키 합의까지 얻는다.



(그림 3) IKEv2

Phase I에서 기본적으로 교환되는 메시지는 4개이지만, 서비스거부공격이 있을 시에는 2개의 메

시지 교환을 더하여 그에 대응토록 되어 있다.

III. JFK

JFK 프로토콜의 디자인 목표는 다음의 일곱 가지를 들 수 있다.

첫째, 키 교환시 생성된 키는 암호학적인 안전성의 표준 측정기준에 만족하는 정도의 안전성을 보장해야 한다.

둘째, 가능한 간단하고 효율적이며 정확한 구현을 보장하는 간결성(simplicity)을 가져야 한다.

셋째, 응답자에 대한 메모리 고갈공격이나 응답자에 대한 CPU 고갈 공격 등의 서비스거부공격에 대해 대응을 할 수 있어야 한다.

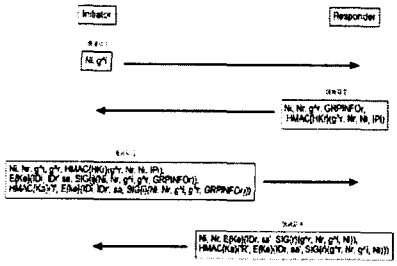
넷째, 개시자와 응답자의 ID에 대한 비밀성을 보장하여야 한다.

다섯째, 계산량, 대역폭, 라운드 횟수에 대하여 효율적이어야 한다.

여섯째, 협상(negotiation)은 복잡도와 라운드 횟수를 증가시키므로 피해야 한다.

일곱째, PFS(Perfect Forward Secrecy)에 접근해야만 한다.

JFK는 JFKi와 JFKr로 나뉘어진다. 이 둘 모두 같은 레벨의 서비스거부공격에 대한 보호를 행한다. JFKi 프로토콜은 적극적인 공격자에 대하여 개시자의 ID를 보호하고 응답자의 ID를 보호하지는 못한다. 이는 client-server scenario에 적합하다. JFKr 프로토콜은 적극적인 공격에 대하여 응답자를 보호하고, 개시자는 수동적인 공격에 대하여 보호 받는다. 이는 peer-to-peer scenario에 적합하다.



(그림 4) JFKr 프로토콜의 메시지 흐름도

(그림 4)는 JFKr 프로토콜에서 개시자와 응답자 사이에서 일어나는 메시지의 흐름을 나타낸 것이다. 여기서 Ke, Ka는 아래와 같이 정의된다.

Ke = HMAC{g^ir}(Ni, Nr, 1)

Ka = HMAC{g^ir}(Ni, Nr, 2)

다음으로 메시지별로 각 메시지의 특성과 각각의 요소들은 어떠한 역할을 하는지 살펴본다.

● 메시지 1

— 개시자는 이미 응답자가 수락하는 그룹과 생성자를 알고 있다고 가정한다.

— 개시자는 Ni, g^i를 응답자에게 보낸다.

— g^i가 같더라도 Ni에 의하여 각각 다른 병렬 세션들을 구별할 수 있다.

● 메시지 2

— 응답자는 자기 자신의 g^r, 다음 메시지에서는 어떤 암호키 알고리즘을 쓸 것인지에 대한 정보(GRPINFOr), Nr, 인증자를 개시자에게 보낸다

— 응답자의 g^r은 forward secrecy interval 동안 재사용되어질 수 있으므로, MAC 계산만이 계산량에 영향을 준다.

응답자는 개시자가 합법적인지 DOS 공격에 의한 위조된 메시지인지 알 수 없다. 즉, 아직까지 round-trip이 없었다. 따라서 이 시점에서는 응답자가 많은 계산이나 새로운 state 생성을 수행하는 것이 요구되어져서는 안된다.

— 응답자가 새로운 g^r을 많이 사용한다는 것은 계산량과 시간적인 측면에서 비효율적이므로 권고되지 않는다. 따라서, g^r의 재사용으로 인한 두 개의 연속된 세션 키들이 똑같아지는 것을 nonce(Nr)가 방지해주고 있다.

● 메시지 3

— 응답자는 인증자를 통하여 리턴되어진 데이터를 인증하며, 메시지 1과 메시지 3을 보낸 사람이 동일한 주소를 사용하는지를 확인한다.

— HKr가 바뀌기 전까지 응답자는 메시지 3과 메시지 4의 복사본을 저장하고 있는다. 만약 동일한 메시지 3이 응답자에게 도착한다면 응답자는 새로운 state를 만들지 않고 저장하고 있던 메시지 3에 대응하는 메시지 4를 재전송함으로써 DOS 공격에 대응할 수 있다.

● 메시지 4

— 응답자의 IPsec SPI와 같은 SA에 대한 정보가 포함되어 있다.

— Ke에 의하여 모두 암호화 된다

— 메시지 4과 같이 키 Ka를 사용하는 MAC에 의하여 메시지 4도 보호된다.

— 포함되어 있는 디지털 서명을 확인하고 메시지를 복호화함으로써 개시자는 응답자가 현재 세션에 참고하고 있는지를 확인할 수 있다.

JFK 프로토콜에서는 응답자는 메시지 2와 메시지 4를 보내는 대신 거부 메시지를 보낼 수 있다.

● 메시지 2에 대한 거부

— 이 메시지 거부는 응답자가 개시자가 사용한 exponential을 수락할 수 없을 때 발생한다.

— 메시지 2에는 이미 GRPINFOr 필드가 포함되어 있으므로, 명백한 거부 메시지가 필요한 것은 아니다

● 메시지 4에 대한 거부

— 개시자에 의하여 요구되어지는 서비스에 대한 인가가 부족하거나, 개시자가 요구하는 암호 알고리즘이 응답자에게 불충분한 것으로 간주될 때 발생한다.

이런 경우 응답자는 허용 가능한 암호 알고리즘을 나열해 주어야 한다.

개시자는 다시 메시지 3을 보내게 되고, 응답자는 다시 메시지 4을 수락하게 된다. 이때 응답자는 허용 가능한 메시지 3을 받을 때까지 어떠한 state도 만들지 않는다.

IV. 두 프로토콜의 비교

IKEv2와 JFK는 전혀 다른 프로토콜이지만, 새로운 키관리 프로토콜이 만족시켜야 하는 요구사항을 거의 대등하게 만족시키고 있다.

첫째, 두 프로토콜 모두 정상상태에서 4개의 메시지 교환에 의해 통신쌍방이 인증된 보안채널을 수립한다. 기존 IKE가 6개의 메시지 교환으로 이를 달성하는 것에 비해 경제적이다.

둘째, 두 프로토콜은 모두 기존 프로토콜이 갖지 못한 서비스거부공격(DOS)에 대한 대응력을 갖고있다. IKEv2 는 DOS 공격 시 2개의 메시지 교환을 추가함으로써, JFK는 메시지에 DOS 대응 기능을 항상 포함시킴으로써 이를 달성한다. DOS 공격 대응력을 높이기 위해 두 프로토콜 모두 PFS를 타협할 수 있도록 허용하였다.

셋째, 두 프로토콜은 모두 IKE에서와 같이, 개시자에 수동적 신원(identity) 보호와 응답자에 적극적 신원 보호를 도모할 수 있다.

이 두 프로토콜 사이의 수많은 차이점 중에서 가장 중요한 것들을 살펴보면 다음의 세 가지를 들 수 있다.

첫째, 암호협상 개념 면에서 두 프로토콜은 차이를 보인다. IKEv2가 IKE에서보다는 선택사항이 훨씬 줄어들긴 했지만 아직도 암호협상을 허용하는데 반해, JFK는 암호협상을 허용하지 않음으로 간결성을 강조하였다.

둘째, IKEv2는 기존 IKE의 phase I/II 분리개념을 계승하여 phase I에서 수립된 IKE SA를 후속 IPsec SA들의 수립과 관리시 제어채널로 활용할 수 있게 하는데 비해, JFK는 phase 개념을 없애 프로토콜의 간결성을 제고하였다.

셋째, 인증 방식 면에서는 두 방식 모두 인증서에 의한 인증을 기본으로 하지만, IKEv2는 공유 시크릿 사용도 지원하고, 기존 인증 시스템의 사용도 간접 지원한다.

V. 결론

앞으로 마련될 후속 IKE 프로토콜은 기존 IKE 프로토콜보다 훨씬 간결하게 마련될 것으로 보여 이 프로토콜을 채택한 제품의 상호연동성이 높아질 것으로 보인다. 기존 IKE 프로토콜의 개념에 익숙해져 있는 WG 멤버들과 IKE를 구현해 본 산업체의 다수는 새로운 프로토콜보다는 IKE 개념을 계승하는 IKEv2를 선호 할 것으로 보이며, 이에 따라 앞으로 표준화는 IKEv2를 기본문서로 하고 JFK에서 제시된 stateless cookie의 사용이 반영되는 형식으로 표준화추진이 전망된다. 기존 IKE 보다 훨씬 간단한 프로토콜로 정의될 IKEv2 프로토콜은 그만큼 상호 연동성이 제고될 뿐 아니라 구현도 쉬워질 전망이어서, 국내 VPN 업체들도 자체 개발을 일찍 서두르는 것이 바람직할 것으로 생각된다.

SA 협상은 다수의 계산량적 비효율성을 비롯해서 새로운 round-trip이 있어야만 하므로 고속 암호화의 문제에서는 그 존재를 고려해야만 한다. 현재 나와있는 두가지 IKE 후속 키관리 알고리즘에 있어서 각각은 장단점을 공유하고 있다. 결국 최종 결정된 알고리즘은 표준으로 추진될 것이므로 두 개의 프로토콜의 장점을 결합한 형태의 결론이 날 것이라 예상된다. 문제는 이 중 어느 프로토콜에 더 비중을 두느냐는 점이다.

이후 IPsec에서의 키관리 방법으로는 기존의 방식을 승계하였으며 다양한 경우에 적용이 가능한 IKEv2로 표준화가 추진될 가능성이 매우 높은 것이 사실이지만, 고속화에 있어서는 IKEv2보다 JFK가 더 가능성이 열려있다.

다양한 보안노드 들 사이의 고속 암호화 기술에 있어서 적합한 알고리즘을 선택한다면 현재 시장상황이거나 기존의 구현물등을 고려해 IKEv2를 사용하는 것이 비용과 효과 면에서 더 좋은 결과가 기대된다.

참고문헌

[1] Proposal for the IKEv2 Protocol, draft-ietf-ipsec-ikev2
[2] Just Fast Keying (JFK), draft-ietf-ipsec-jfk
[3] Comparison of IKEv2, JFK and SOI Requirement, IPsec WG 53rd IETF
[4] Features of Proposed Successors to IKE, draft-ietf-ipsec-soi-features