서비스 제공자의 키 획득을 위한 IPsec 프로토콜[6)]

송세화*, 이종언**, 황인용**, 이유신**, 김석중**, 최형기*
*성균관대학교 정보통신공학부
**삼성탈레스 종합연구소/SIAT
dreaminsh@ece.skku.ac.kr, jong-eon.lee@samsung.com, inyong08.hwang@samsung.com,
yous.lee@samsung.com, seokjoong.kim@samsung.com, hkchoi@ece.skku.ac.kr

A Modified IPsec Protocol for key sharing between a service provider and clients

Sehwa Song*, Jong-Eon Lee**, In-Yong Hwang**, You-Shin Lee**, Seok-Joong Kim**,
Hyoung-Kee Choi*
*School of Information and Communication Engineering, Sungkyunkwan University
**R&D Center, Samsung Thales Co., Ltd.

요 약

VoIP기반의 음성통화가 기존 PSTN망을 대체하여 빠르게 확산되고 있다. 이러한 IP기반의 음성통신은 IP 네트워크가 가진 보안 취약점을 그대로 가지고 있어 이에 대한 보완이 필요하다. IPsec은 IP망에서 보안을 제공하는 프로토콜로 데이터의 기밀성 및 무결성을 제공한다. 한편, 서비스 제공자는 적절한 과금 및 서비스 중재 및 부가 서비스 제공을 위해 통신에 사용된 암호화 키를 획득할 수 있어야 한다. 본 논문에서는 IPsec의 키 교환 프로토콜인 Internet Key Exchange v2를 수정하여 서비스 제공자와 통신하는 양 단말이 동시에 키 교환을 수행하도록 한다. 이 방식을 통하여 서비스 제공자가 키 생성에 참여함으로서 Men in the middle 공격을 효과적으로 막을 수 있고, 부가 서비스를 제공할 수 있는 발판을 마련할 수 있다.

키워드 : 네트워크 보안, VoIP, IPsec, Internet Key Exchange

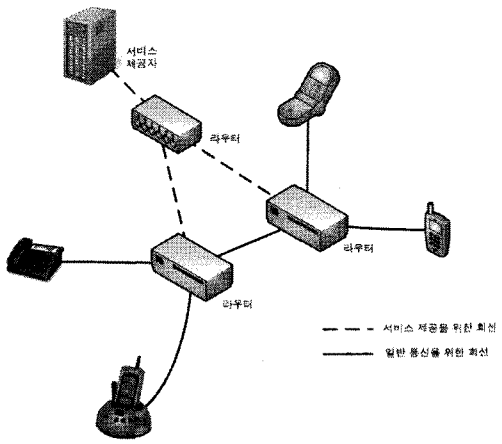
I. 서론

현재 음성통화 환경은 기존 PSTN망의 활용에서 IP망을 사용한 음성 통화로의 수요가 커지는 상황이다. 특히, Wibro 및 Long Term Evolution 등의 차세대 무선네트워크에서는 All-IP망을 목표로 하고 있기 때문에 향후, IP를 통한 무선 통화가 주류를 이룰 것이다. All-IP망은 음성과 같은 real-time service와 일반적인 data를 함께 전송할 수 있기 때문에 통신망을 효과적으로 사용할 수 있다는 장점이 이다. 하지만, 이러한 상황에서 음성과 같은 real-time 서비스에 대해서는 QoS의 유지와 보안이 큰 이슈가 될 수 있다. 특히, IP망을 통한 음성통화는 기존 IP네트워크의 보안문제점에 그대로 노출되어 보안에 대한 대비가 필요하다. IPsec은 이러한 IP망의 보안문제를 해결하기 위해 IETF에서 제안한 프로토콜이다 [1]. IPsec을 사용하여, 각 음성 데이터는 통신하는 양 단말이 Internet Key Exchange (IKE) 를 통해 합의한 알고리즘과 키를 통해 암호화되어 전달될 수 있다.

하지만, 인터넷망을 통한 통화에 대해서 서비스 제공자가 적절한 과금을 할 수 있어야 하고, 추가적으로, 통신을 수행하는 두 개체가, 서비스 제공자부터 부가 서비스를 제공받거나, 추후 법적 분쟁 발생 시 중재자로서의 역할을 요청하기 위해, IKE를 통한 암호화키의 생성에 참여해야할 필요가 있다. 예를 들어, 지적재산 보호, 산업 스파이 차단 등 다양한 목적을 위해, 미국의 경우 1994년 Communications Assistance for Law Enforcement Act (CALEA) 라는

※ "이 논문은 2008년도 삼성탈레스(주)의 재원을 지원 받아 수행된 연구임."

법안에 의해 모든 Voice over IP (VoIP) 시스템은 신뢰할 수 있는 3자가 암호화 키를 획득할 수 있도록 설계되도록 하고 있다 [2]. 그러나, 현재, IPsec을 통해서는 이와 같은 서비스를 제공할 수 없기 때문에, 별도의 프로토콜이 필요하다. 우리는 대표적인 Network Layer의 보안 프로토콜인 IPsec [1]과 IPsec의 키교환 프로토콜인 Internet key exchange v2 [3] 를 보완하여, 신뢰할 수 있는 3자와 통신하는 양 단말 간에 키 교환을 할 수 있는 보안 프로토콜인 변형된 IPsec을 제안한다. 변형된 IPsec은 통화의 암호화에 사용되는 키를 통화하는 양 노드와 서비스 제공자가 공유 하도록 한다.



〈그림 1〉 서비스 제공자의 키 획득을 위한 아키텍쳐

II. 관련 연구

IPsec은 Network Layer에서 보안을 담당하는 프로토콜로 상위 Layer에서 보안을 수행하지 않아도, IP에서 보안을 책임져 준다. 따라서 전송계층에서의 여러 프로토콜 뿐만 아니라, 응용계층에서의 여러 응용프로그램에서도 보안적용이 가능하다. IPsec은 네트워크 환경에 따라 Tunnel모드와 Transport모드로 동작이 가능하다. Tunnel모드는 주로 VPN에 사용되는데, 네트워크 단위에서 보안을 처리할 때 사용된다. 그리고 Transport모드는 각 단말이 직접 IPsec을 사용한 통신을 수행한다. 또한, 보안 요구사항에 따라 ESP프로토콜과 AH프로토콜의 사용이 가능하다. ESP프로토콜은 payload의 기밀성을 보장하며, AH프로토콜은 payload의 무결성을 보장한다. 이 두 프로토콜은 함께 사용이 가능하다.

Internet Key Exchange는 IPsec의 보안연계를 확립하기 위해 IPsec통신 전에 이루어지는 프로토콜로, IKE를 통해 IPsec에 사용할 암호화 및 무결성 프로토콜과 해당 키를 양단이 협의하게 된다. IPsec은 Phase1과 Phase2로 나뉘어 동작한다. Phase1에서는 IKE에서의 보안연계를 설정한다. 이후 IKE과정에서 상호 교환하는 데이터의 암호화 및 인증서를 통한 상호인증을 수행하며, 서로 사용가능한 암호화 및 무결성 프로토콜, 그리고 암호화 및 무결성 키를 협상한다. Phase2에서는 IPsec에서 사용할 보안연계를 설정한다. Phase2는 Phase1에서 협상된 키 및 프로토콜을 사용하여 보안이 유지된 상태에서 진행된다. 향후 실제 통신에서 IPsec이 적용될 데이터를 보호하는데 사용할 키 및 프로토콜을 협상한다.

III. 본론

용어정리

본 논문에서 사용하는 용어들은 기존 IKEv2와 〈표 1〉과 같이 동일하게 사용한다.

〈표 1〉 프로토콜에서 사용하는 용어

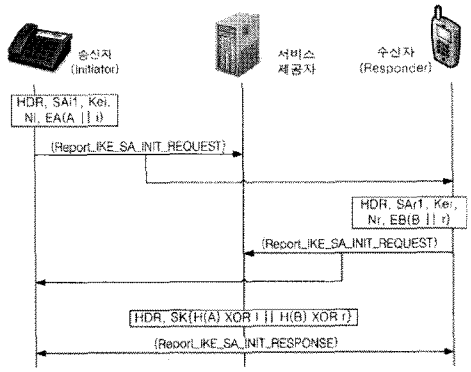
항목	내용
HDR	IKE의 header
SA	Security Association에 사용될 프로토콜 등 정보
KEi	g^i mod p
KEr	g^r mod p
Ni / Nr	Initiator와 Responder가 각기 생성한 랜덤 값
i / r	KEi / KEr의 생성에 사용된 값
A	Initiator와 서비스 제공자가 공유하는 비밀키
B	Responder와 서비스 제공자가 공유하는 비밀키
EA{..} / EB{..}	A / B로 암호화

시스템 제공자의 키 획득위한 시스템 아키텍처

본 논문에서 제안하는 프로토콜에서는 〈그림 1〉과 같이 서비스 제공자(Service Provider, SP)와 통화를 거는 노드(Initiator, I), 그리고 통화를 받는 노드(Responder, R)로 구성된 아키텍처가 사용된다. 두 노드는 같은 서비스 제공자로부터 서비스를 제공받기 때문에 위의 환경은 동일한 보안정책이 형성되어 있다고 볼 수 있다. 우리는 각 통신하는 노드와 서비스 제공자간에 공유된 키가 있는 네트워크를 가정한다. 일반적으로 VoIP통신을 위한 회선이 있고, 라우터에서는 지정된 서비스 제공자로 미러링을 하므로써, 양 노드 간에 통신은 서비스 제공자도 받을 수 있도록 한다.

시스템 제공자의 키 획득위해 수정된 IKEv2

적절한 과금을 위해 서비스 제공자는 통신하는 양 노드가 통신할 때 사용하는 암호화 키를 알아야 하며, 이를 위해 우리는 Internet Key Exchange v2를 수정하였다. 수정된 IKEv2를 통해 서비스 제공자는 양 노드의 암호화 키의 협상에 참여하게 된다.

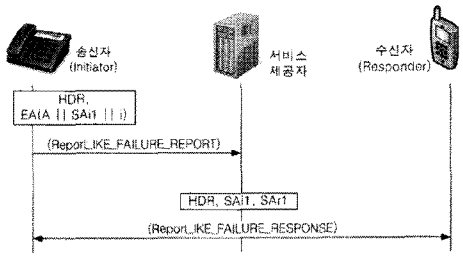


〈그림 2〉 수정된 IKEv2 Phase 1

〈그림 2〉은 과금 및 추가적인 서비스를 위해 서비스 제공자가 통신하는 양단의 암호화키를 갖도록 키 협상에 참여하는 수정된 IKEv2 Phase1 과정을 나타낸다. EA(A||i)와 EB(B||r)는 각 노드에 대한 인증을 함으로서, Man-in-the Middle 공격을 막기 위함이다. 이 방식은 Self-Encryption 방식으로 비밀키를 비밀키로 암호화함으로서 평문의 외부 노출을 최소화한다. 또한 Replay를 막기 위해 i와 r을 추가하였다. Phase1의 첫 번째와 두 번째 메시지를 통해 서비스 제공자는 Initiator와 Responder가 향후 IKE과정에서 사용할 각종 키 material을 획득할 수 있다. Phase1의 세 번째 메시지를 통해 Initiator와 Responder는 Phase1의 성공여부를 확인할 수 있다. A와 B는 Initiaotr와 Responder가 각기 서비스 제공자와 공유하고 있는 비밀값이다. H(A)는 A의 해쉬값으로, Responder가 Initiator의 비밀값을 획득하지 못하도록 한다.

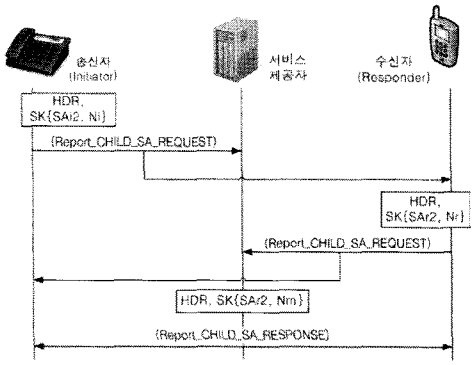
따라서, 아래와 같이 Initiator와 Responder, 그리고 서비스 제공자는 동일하게 암호화 및 무결성의 키의 생성에 사용되는 SKEYSEED를 생성할 수 있다.

$$SKEYSEED = PRF(Ni \;||\; Nr \;||\; g^{ir})$$



〈그림 3〉 Fail Report Phase

〈그림 3〉는 암호화 키의 협상이 실패할 경우, Initiator가 서비스 제공자에게 이를 알려주고, 서비스 제공자가 이를 양단에 알려주는 절차이다. 이 과정을 통해 실패한 협상에 대한 정보를 양단은 삭제하고, 다시 Phase1과정을 시작하게 된다.



〈그림 4〉 수정된 IKEv2 Phase 2

〈그림 4〉은 서비스 제공자가의 키 획득을 위해 수정된 IKEv2 phase2이다. IKEv2 Phase2는 Phase1에서 설정된 암호화 키들로 암호화되어 있고, 실질적으로 음성통신에 사용할 키를 설정하는 과정이다. Ni, Nr, Nm을 Initiator와 서비스 제공자, Responder가 공유하게 되고, 이를 통해 키 생성에 필요한 KEYMAT를 아래와 같이 생성할 수 있다.

$$KEYMAT = PRF(Ni \;||\; Nr \;||\; Nm)$$

SKEYSEED와 KEYMAT를 통해 암호화 및 무결성 키를 생성하는 방법은 RFC 4306과 동일하다.

Phase2를 통해 서비스 제공자는 Initiator와 Responder가 설정할 IPsec에 관한 보안연계의 정보를 획득하였다. 따라서, 서비스 제공자는 IPsec의 보호를 받는 음성통신의 형성을 할 수 있다.

〈표 2〉 추가된 메시지 타입 및 값

Exchange Type	Value
Report_IKE_SA_INIT_REQUEST	240
Report_IKE_SA_INIT_RESPONSE	241
Report_CHILD_SA_REQUEST	242
Report_CHILD_SA_RESPONSE	243
Report_IKE_FAILURE_REPORT	244
Report_IKE_FAILURE_RESPONSE	245

우리는 기존 IPsec과의 호환성을 위해 IKEv2 HDR의 Exchange Type을 〈표 2〉와 같이 6개의 메시지에 대하여 별도로 정의하였다. 현재 IKEv2에서는 exchange type의 240~255번을 개인적 용도로 사용할 수 있도록 제공하고 있으며, 이를 활용하면, 기존 IKEv2에 영향을 줄이면서 새로운 기능을 추가할 수 있다. 따라서, 추가적인 메시지에 대한 부분만 S/W적으로 구현하면 동작할 수 있도록 하였다.

IV. 보안분석

과금 및 부가서비스 제공을 위해 통신하는 양 노드만 가지고 있던 키를 서비스 제공자도 보유함에 따라 키 유출에 대한 위협이 존재할 수 있다. 또한, 기존의 IKEv2에서는 IKE_SA_INIT_request와 IKE_SA_INIT_response메시지는 인증없이 이루어지기 때문에 man-in-the-middle위협이 존재한다. 그러나, 본 논문에서 제안하는 방법은 양 노드와 서비스 제공자간에 보유하는 비밀 키로 인증을 수행하므로 이와 같은 위협을 제거하였다. Self-Encryption방식을 사용한 인증은 간편하면서도, 비밀키를 보유함을 보여줄 수 있다. 또한, 양 단이 키 생성을 위해 생성한 i와 r을 함께 암호화 하여 Replay공격을 방지한다.

V. 결론

VoIP기반의 통신이 활성화됨에 따라 보안이 보다 중요한 요소가 되고 있다. IP기반 네트워크에서 보안을 수행할 수 있는 IPsec을 사용하면, 효과적으로 단대단 보안을 보장받을 수 있다. 그러나, 과금 및 부가서비스의 제공을 위해 서비스 제공자가 양 노드의 통화를 암호화하는 키가 필요한 경우가 생긴다. 이러한 요구를 만족시키기 위해서는 기존 IPsec 네트워크의 변형이 필요하다. 통신하는 양 노드만이 데이터를 암호화하는 키를 보유하고 있기 때문이다.

우리는 본 논문을 통해 기존의 IKEv2를 수정하여, 서비스 제공자가 키 생성과정에 참여하는 새로운 프로토콜을 제안하였다. 메시지 타입을 추가함으로써, 기존 IKEv2의 동작을 방해하지 않고 수행할 수 있도록 하였다. 또한, 기존에 정의된 키 생성과정을 그대로 적용시키도록 설계하여, 프로토콜의 변화를 최소한으로 하도록 하였다. 특히, 동일한 보안정책이 유지되는 네트워크의 특성을 사용하여, 기존 IKEv2의 문제가 되는 Man-in-the-Middle 공격에 대해서도 보다 강한 저항성을 가지도록 설계하였다.

참고문헌

[1] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[2] CALEA, http://www.askcalea.net/

[3] C. Kaufman, The Internet Key Exchange v2 (IKEv2), RFC 4306, IETF, Dec. 2005.