공개 키를 기반으로 하는 무선망에서의 암호화 키 분배 방법

안수현[0] 한규호 안순신
고려대학교 전자공학과
(ashddd[0], garget, sunshin)@dsys.korea.ac.kr

Internet Key Exchange based on PKI in wireless environment

Soo-Hyun Ahn[0] Kyu-Ho Han Sun-Shin Ahn
Dept. of Electronic Eng., Korea University

요 약

최근 보안에 관한 관심이 높아지면서 IPSec을 이용한 VPN system이 널리 이용되고 있다. IPSec에서 암호화에 사용되는 키를 생성하는 IKE는 IPSec의 핵심 프로토콜이지만 다소 복잡하고 메시지 교환도 많아 패킷의 손실이 큰 무선망 에는 적합하지 않다. 무선망에서 좀 더 효율적으로 동작하기 위한 인터넷 키 교환 방법 및 공개키 기반구조를 제시 하였다.

1. 서 론

최근 인터넷 상의 보안의 중요성이 부각되면서 VPN에 대한 관심이 높아 지고 있으며, 특히 인터넷 프로토콜의 보안 정책인 IPSec을 이용한 VPN에 많은 관심이 집중되고 있다. IPSec은 터널링(tunneling)을 사용하여 VPN을 인터넷 상에서 패킷을 안전하게 목적지로 전달 할 수 있으며 인증과 암호화를 통하여 높은 수준의 보안을 보장 할 수 있다. 또한, IPSec은 특정한 암호화 및 인증 알고리즘(algorithm)에 국한되지 않고 현재까지 개발된 거의 모든 암호화 및 인증 알고리즘(algorithm)을 사용하여 보안을 유지 할 수 있는 장점이 있다. IPSec이 암호화 및 인증 과정에 필요한 키(key)는 IKE(Internet Key Exchange)라는 프로토콜이 생성하며 IKE는 미리 알고 있는 공개키(public key)와 프로토콜이 발생하는 난수 등을 이용하여 키를 생성하며 상대편과의 협상(negotiation)을 통하여 암호화 및 복조화에 쓰이는 알고리즘을 결정한다.

IPSec을 이용하여 보안을 유지하는 핵심은 암호화 및 인증에 필요한 키를 생성하고 관리 하는데 있다. 이러한 점에서 IKE는 IPSec VPN system을 구성하는데 핵심이 되는 프로토콜이라고 할 수 있으나 다소 복잡하고 상호간의 통신이 여러 번 이루어 져야 하는 단점이 있다. 최근 관심이 집중되고 있는 무선 인터넷 환경에서는 패킷의 손실이 유선망 보다 크고 보안이 취약하므로 이러한 복잡한 과정이 프로토콜 자체가 가지고 있는 다양한 기능에도 불구하고 큰 단점이 될 수가 있다. 이 논문에서는 무선 인터넷의 특수성, 즉 높은 전송 실패율과 단말기의 하드웨어적인 제약 등을 고려하여 기존의 키 교환 프로토콜을 수정한 프로토콜과 공개키 기반구조를 이용한 키 분배 방법을 제안한다.

2. 관련연구

2.1 인터넷 키 교환(Internet Key Exchange)

IPSec이 안전한 터널을 통한 통신을 수행하기 위해서는 사용할 보안 알고리즘이 협의 되어야 하며 알고리즘에 사용될 키가 생성되어야 한다. 이러한 두 가지 역할을 담당한 것이 IKE, 즉 Internet Key Exchange이다.

IKE는 두 프로토콜의 합성으로 ISAKMP/Oakley로 불렸으며, ISAKMP(Internet Security Association Key Management Protocol)는 암호화 키의 생성과 SA의 협의에 필요한 framework를 제공하며 Oakley는 ISAKMP에서 정의하지 않는 보안 메커니즘을 정의하고 있다. IKE는 두개의 phase로 구성이 되며, 그 각각은 ISAKMP의 framework에 정의되어 있고, Oakley가 각 phase의 mode를 정의하고 있다.

Phase1은 ISAKMP SA을 성립하는 절차이다. 이때, 어떠한 안전한 채널도 없다고 가정하여 ISAKMP 메시지들을 보호하기 위하여 SA를 성립한다. Phase1에는 두 가지 모드, 즉 main mode와 aggressive mode가 쓰일 수 있다. Main mode는 SA를 성립하려고 하는 상대의

identity를 보호할 수 있는 장점이 있으며, 그와 반대로 aggressive mode는 메시지 교환 횟수가 적은 장점이 있다.

Phase2는 IPSec이 제공하는 여러 가지 서비스에 필요한 SA를 성립하기 위하여 필요한 절차이다. 이 때 ISAKMP 메시지들은 Phase1에서 만들어진 ISAKMP SA에 의하여 보호 받게 된다. Phase2에서는 여러 가지 서비스에 대한 SA를 협의 하기 위하여 quick mode를 사용한다. Informational mode는 실패 등으로 생기는 비정상적인 조건등에 대한 정보를 상대편에게 전달할 때 쓰인다.

2.2 공개키 기반 구조(Public Key Infrastructure)

공개키를 사용하는 알고리즘은 암호화 및 전자 서명과 키 분배 등의 보안 작용을 제공한다. RSA로 대표되는 공개키 보안기술의 가장 큰 문제점은 공증 기관으로부터 얻은 키의 신뢰성을 확신 할 수 없다는 데 있다. 이러한 문제점을 해결하기 위한, 믿을 만한 권위를 가진 기관이 존재하는 인터넷 상의 보안 환경을 공개키 기반 구조, 즉 PKI(public key infrastructure)가 제공한다. 즉,공개키의 생성, 발급 분배 및 관리를 체계적으로 수행하는 인터넷의 기반 구조를 공개키 기반 구조 라고 말한다. PKI에서는 CA(Certificate Authority) 라고 불리는 인증기관이 계층적으로 구성되어 공개키를 사용하고자 하는 사용자들에게 인증서를 발급하여 공개키의 유효성을 보장할 수 있다. 대표적인 응용 분야로 전자 서명과 IPSec이 있다.

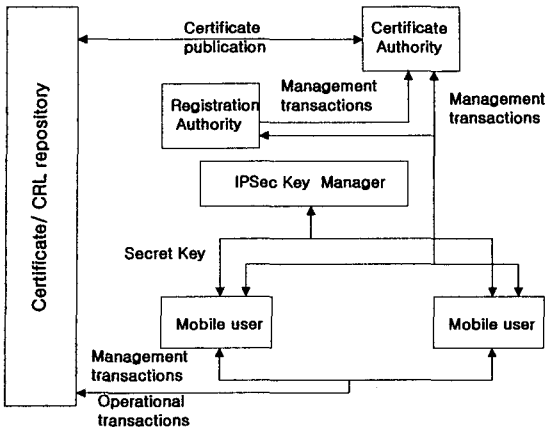
3. 무선 환경에 적합한 키 교환 프로토콜

3.1개선된 공개키 기반구조

무선 환경에 적합한 키 분배 프로토콜을 만들기 위하여 기존의 공개키 기반구조(PKI)를 수정한다. 여기서는 IPSec에 쓰일 암호화 키를 생성하기 위한 키교환 프로토콜을 전혀 사용하지 않고 공개키 기반 구조가 IPSec의 통신 사용자에게 키를 분배한다.

기존의 공개키 기반구조와 마찬가지로 여기서는 Certificate Authority(CA)가 공개키에 대한 인증서를 발급하고 Registration Authority(RA)는 키의 주인을 CA에 등록하는 역할을 한다.

여기에 새로운 구성원인 IPSec Key Manager가 사용자들에게 IPSec에 쓰일 대칭키를 분배한다. 즉, 패킷을 보내려고 하는 무선 사용자가 공개키 기반구조의 IPSec Key Manager에게 키의 분배를 요청하면 IPSec Key Manager는 MD5 혹은 SHA-1과 같은 해쉬 알고리즘으로 키를 요청한 노드의 공개키와 난수 등을 이용해 키를 발생시킨다.



<그림1> 무선망 키 교환은 위한 PKI 구성

여기서 발생된 키는 IPSec Key Manager가 통신의 양 당사자에게 보낸다. 이 때, 키를 보내는 패킷의 내용은 RSA와 같은 공개키 알고리즘을 사용하여 각각의 공개키로 암호화 하고 전자서명을 하여 보내어 진다. 키를 받은 사용자는 자신의 공개키/비밀키의 쌍을 이용하여 IPSec 통신에 이용할 대칭키를 복구 해 내고 전자서명에 의한 인증절차를 거치게 된다.

그림1은 무선망의 키 분배를 위하여 IPSec Key Manager가 추가되고 기능이 추가된 공개키 기반구조의 구성도이다.

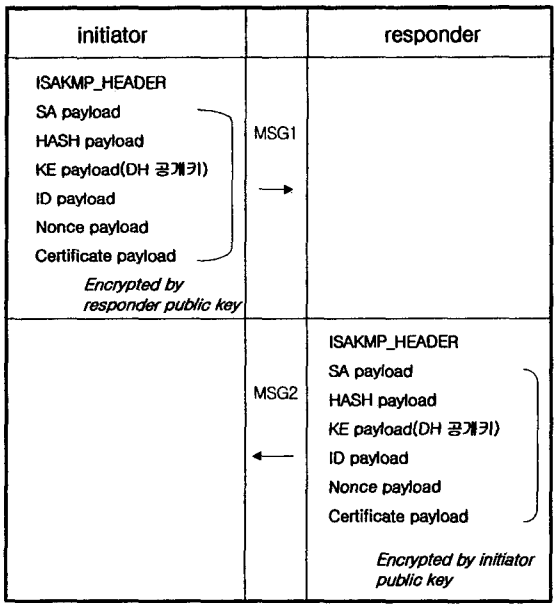
이러한 방법을 쓰게 되면 무엇보다도 키를 분배하는 절차가 매우 단순화 되는 장점이 있다. 그러나, 기존의 공개키 기반 구조에 새로운 구성원을 포함 시키고 새로운 기능을 추가시키는 등 많은 변화가 불가피하게 되는 단점이 있다. 또한 이러한 점 때문에 기존의 유선망과의 연동이 어렵다고 볼 수 있다.

3.2 키 교환 프로토콜의 개선

두번째 방법으로 기존의 키 교환 프로코콜(IKE)를 개선하여 무선망에 적용하는 방법을 생각 해 볼수가 있다. 모두 세가지 측면에서 개선의 여지가 있으며 첫째로, 다중 SA(multiple SA)의 방법을 사용하기 위하여 phase1과 phase2로 나누어져 있는 IKE의 키 교환 절차를 하나의 phase만 사용하도록 한다. 다중 SA는 여러 가지 다른 목적을 가진 여러 가지 응용 분야에 따라 서로 다른 SA에 의 하여 보호를 받을 수 있도록 하는 장점이 있기는 하지만, 무선망의 경우 사용자의 네트워크 응용 범위가 유선망 사용자에 비해 한정되어 있고 통신

시간이 짧기 때문에 다중 SA의 사용이 적합하지 않다. 반면 두개의 phase로 계층구조를 이루는 경우 더욱 강력한 보안을 제공하므로 이를 공개키 기반 구조를 더욱 적극적으로 사용하여 보완한다.

공개키 기반 구조로 부터 얻은 공개키를 이용하여 암호화 및 전자서명등에 의한 방법으로 인터넷 키 교환에 쓰이는 메시지를 보호한다. 즉, 두 단계로 나뉘어진 계층적인 보안 phase를 공개키 기반구조를 바탕으로 하는 보안 정책으로 대체한다. 참고로 현재의 IPSec에서는 공개키 알고리즘에 의한 터널링을 지양하고 있는데 이것은 공개키 알고리즘은 강력한 보안을 제공하는 반면에 굉장히 많은 시간과 리소스를 차지하므로 모든 데이터 패킷에 적용하기에는 적합하지 않기 때문이다.



<그림2> 무선망 ISAKMP 메시지 포맷

둘째로 메시지의 교환 횟수를 대폭 줄인다. 이로 인하여 SA를 만들기 위하여 각 노드가 받게 되는 오버헤드가 많이 줄어 들게 되고, 오류의 가능성이 줄어들게 된다. 기본적으로 메시지 포맷은 하나의 phase, 즉 phase1의 aggressive mode을 기본으로 하여 전자 서명을 하게 되는 payload(Certificate Payload)가 추가되며, 각 메시지는 ISAKMP 헤더를 제외한 나머지 부분이 모두 상대방의 공개키로 암호화 된다.

셋째로 기존의 유선망에서 쓰이는 IKE 와의 연동을 가능하게 한다.

즉, 기존의 유선망에서 쓰이는 방식과 통합하여 쓸 수 있도록 한다. 먼저 무선망의 노드가 유선망의 노드에 대하여 키교환 프로토콜을 시작할 때 ISAKMP 헤더의 Exchange Type 필드에 무선망에서 쓰이는 mode임을 명시하여 메시지를 보낸다. 반대로 유선망의 노드가 기존의 main mode나 aggressive mode의 메시지를 무선망 노드에 보낸다면 이를 받은 무선망 메시지는 Informational Exchange를 통하여 오류가 발생되었음을 알리고, SA를 생성하는 협상을 다시 시작할 것을 알린다.

4 결론 및 향후 과제

이 논문에서는 무선망에서 좀더 빠르고 효율적으로 보안 정책에 쓰일 수 있는 키를 분배하고 교환하는 방법을 제시하였다. 위에서도 말하였듯이 현재 터널링에 쓰이고 있는 대칭키 알고리즘은 비교적 보안에 취약하기 때문에 되도록 자주 효율적으로 키를 갱신할 수 있는 방법을 연구하는 것이 중요하다.

또, 좀 더 강력한 보안을 제공할 수 있는 공개키 알고리즘과 이러한 공개키를 신뢰할 수 있는 방법으로 제공할 수 있는 공개키 기반 구조를 VPN에 보다 적극적이고 효율적으로 사용할 수 있는 방법을 연구해야 할 것이다. 무선망 뿐만 아니고 유선망에서도 좀 더 효율적이고 단순하면서도 강력한 기능을 갖춘 키 교환 프로토콜의 지속적인 연구가 이루어 져야 할 것이다.

5. 참고 문헌

[1]D.Harkins, D.Carrel. " The Internet Key Exchange" ,RFC 2409

[2]S.Kent, R.Atkinson, " Security Architecture for the Internet Protocol" , RFC2401

[3]Perlman, R. and Kaufman, C " Key Exchange in IPSec:Analysis of IKE" , IEEE Internet Computin 11/12 2000

[4]Radia Perlman, " Analysis of IPSec Key Exchange Standard" . IEEE 2001