PKI 기반 IPSec에서의 키 복구에 관한 연구

이윤정, 김정범, 김태윤

고려대학교 컴퓨터학과

{genuine, qston, tykim}@netlab.korea.ac.kr

요약.

IPSec은 인터넷의 네트워크 계층에서 IP 메시지에 대하여, 암호화 서비스와 인증 서비스를 제공하는 보안 프로토콜이다. 키 복구 연구는 많은 논란에도 불구하고 연구가 확되되고 있는 주제이다. 키 복구는 회사차원에서 키 관리의 형태로 필요하게 되었다. 고정 시스템들은 인터넷의 IP 계층에 키 복구를 채용하고 있다. 본 논문은 IPSec 구조와 호환되는 수단으로서 키 복구 정보를 담고 있는 바이트를 전송하는 방법을 제안하고 있다.

1. 서론

IPSec은 인터넷의 네트워크 계층에서 IP 메시지에 대하여 암호화 서비스와 인증 서비스를 제공하는 보안 프로토콜이다 [5,6,7,8]. IPSec의 중요한 두 가지 프로토콜로는, 인증과 무결성 보호 기능을 제공하는 AH(Authentication Header) [7]와, IP의 데이터부분에 대한 선택적인 인증과 암호화 기능을 제공하는 ESP(Encapsulating Security Payload) [8]가 있다.

키 복구는 많은 논란에도 불구하고 연구가 확되되고 있는 주제이다. 서명키 관리와 안전한 암호화를 위해서는 대규모 공개키 구조가 요구된다. 그러나, 위탁 메커니즘이 현재의 규제를 실행하기 위해 개발될 필요가 있기 때문에 암호의 완전한 자유스러운 사용은 정부기관과 법인기관에게는 완전히 받아들여지지는 못한다. 이 문제의 기술적인 어려움 때문에, 다소 만족스럽지 못한 많은 방법들이 발표되었다. 이들 중 일부는 위조 방지 하드웨어에 기반하고 있으며, 다른 것들은 신뢰할 수 있는 제 3기관(TTP)을 사용하고 있다. 더 나아가, 이들 대부분은 통신 크기뿐 아니라 여러 기관들에 의해 교환되는 메시지의 수가 절대적으로 많다.

이런 이유들로, 유명한 전문가들에 의해 작성된 기술 보고서는 연구자들의 광범위한 의견을 피력하고 있는데, 키 복구 시스템의 대규모 채용은 아직 암호의 경쟁력을 넘어서는 것이란 의견이다. 그럼에도 불구하고, 키 복구는 회사차원에서 키 관리의 형태로 필요하게 되었다. 현재의 연구 논문들의 기본적인 관점은 지금까지 제안되어온 암호학적 해결책이 완전히 통신 문맥들을 무시하고 있다는 것이다. 고정 시스템들은 인터넷의 IP 계층에 키 복구를 채용하고 있다.

본 논문은 IPSec 구조와 호환되는 수단으로서 키 복구 정보를 담고 있는 바이트를 전송하는 방법을 제안하고 있다. 제안한 방법은 연결지향적이며 다른 제안들보다 안전한 키 복구 프로토콜을 설계하고 있다.

2. 관련 연구

2.1 키 복구 배경

1993년 4월에, 미국 정부가 제안한 CLIPPER 프로젝트라고 알려진 EES (Escrow Encryption Standard)로부터 키 복구의 역사는 시작되었다. 이후, 많은 키 복구 스킴이 제안되었다

사용자의 프라이버시를 보호하기 위하여 데이터의 기밀성이 유지되어야 하기 때문에, 키 복구의 필요성에 의문이 제기되지만, 다음과 같이 키 복구가 필요한 경우가 존재한다:

- 복구 키를 잃어버리거나, 키를 제공할 수 있는 사용자가 존재하지 않을 때.
- 회사가 통신 당사자들 모르게 그들의 암호화된 트래픽을 감시하기 위해; 예를 들어 고용인들이 회사 정책을 위반하는지의 여부를 검사하기 위해.
- 심각한 범죄나 국가적인 보안의 이유로 국가 정부가 도청한

데이터를 복구하기를 원할 때.

2.2 RHP

RHP (Royal Holloway Protocol) [1] 구조는 하나의 교환 메시지를 갖는 비-상호작용 메커니즘에 기초하며, Diffie-Hellman 이론을 사용한다. RHP 시스템은 송신된 메시지를 사용자의 개인 수신 키를 사용하여 복호화 한다. 각 사용자는 사용자 A 에 대한 TTP_A 로 대표되는 TTP에 등록된다. 다음은 RHP에서 사용되는 메커니즘이다.

1. A 는 $K_{pu-r(B)}$,$(= g^b \bmod p)$를 얻는다. TTP_A 는 B 의 이름과 $K(TTP_A, TTP_B)$ 로부터 $K_{pr-r(B)}$,$(= b)$를 계산해 낼 수 있다.
2. A 는 $K_{pr-s(A)}$ 로부터 공용 키 $(g^b \bmod p)^x \bmod p = g^{ab} \bmod p$ 를 유도해 낸다: 이는 세션 키가 되거나, 세션 키에 대한 암호화 키가 된다.
3. A 는 TTP_A and $K_{pu-r(B)}$ 에 의해 서명 된 $K_{pu-s(A)}$ 를 전송한다. 이 정보는 KRF로서 그리고 B 에게 분배되는 공용 키의 수단으로서 역할을 하게 된다.
4. B 는 수신 받은 후, A 의 공개 송신 키와 $K_{pr-r(B)}$ 로부터 $K_{pu-s(A)}$ 를 검증한다.

그러나, 단점으로는 키 협상과 키 복구가 혼합되어 있다는 것이다. 이것은 그 프로토콜이 단지 한 단계만으로 이루어졌기 때문에, ISAKMP의 보안 프로토콜들 안에서 이 방법들을 통합하기 어렵게 한다. KRF가 단지 한번만 전송된다는 것도 또 다른 단점이다. 사실, 이점은 한 세션이 길어질 수 있고 KEA가 시작을 놓칠 수 있기 때문에, 결정적인 단점이 될 수 있다. 우리는 이 어려움을 장기적인 세션에서의 문제점으로 인식한다. 이 때문에 KRF를 한번이상 여러 번 보낼 필요가 있다. 그러나, 이 시스템의 장점은 보안이 TTP가 아닌 두 통신 상대에 의존하기 때문에 공용키로 세션 키를 암호화한다는 것이다. 그러나, 개인 수신키가 TTP에 달려있기 때문에, 이 장점도 사라지게 된다. 따라서, 해결 방법은 캡슐화와 위탁 메커니즘간의 결합이라고 할 수 있다. 개인 송신키는 위탁되고, 개인 수신키는 양쪽 TTP들에 의해 재생산될 수 있기 때문이다.

2.3 KRA

The KRA (Key Recovery Alliance) 시스템은 TTPs(Trusted Third Party)의 공개키로 세션 키를 암호화하는 방법을 제안하고 이다. KRH(Key Recovery Header)는 네트워크를 통해 KRF를 전송 시키는 방법을 제안하기 위하여 설계되었는데, 이는 키 복구를 시도하는 개체에 의하여 도청될 수 있다. KRH는 ESP SA에 관한 키 생성 정보를 운반한다. 따라서, KRH는 ESP SA [9]와 함께 사용된다. ISAKMP에서는, KRH는 다른 IPSec 프로토콜(예를 들어, AH와 ESP)들과는 다른 방법으로 협상될 수 있다.

이 기술을 이용하는 TIS CKE (Commercial Key Escrow) [3]나 IBM SKR (Secure Key recovery) [2]와 같은 다양한 이론들이 제안되어 왔다. 이 시스템은 간단하며, 암호학적 암호화 이론에 따라 다양한 변형이 가능하다. 이 제안은 키 복구 정보와 키 교환으로 나누어진다. 시스템 모듈은 IETF 권고사항과 호환된다. 그러나, KRF는 많은 TTP 공개 키 기반아래 동일하게 암호화된 키를 포함하고 있다. 따라서, KRF는 브로드캐스트 메시지 공격에 대항하는 적절한 방법을 찾아야 한다. KRA 방법은 IPSec의 IP 패킷 각각에 KRF를 보낼 필요가 없다.

initiator와 responder가 보내는 KRF의 주기는 독자적으로 설정된다. 그러나, KRF의 크기가 크기 때문에 KRF는 IP 헤더에 포함될 수 없다. 따라서, 이것은 IP 패킷 데이터의 일부분인 IPSec 헤더 안에서 전송될 수 있지만, 이는 대역폭을 저하시키게 된다. 두 번째 단점은 TTP 공개 키에 의하여 세션 키가 암호화된다는 것이다. 결국, 이 방법은 이 키가 노출된다면, 시스템이 붕괴되기 때문에 안전하지 않다.

3. IPSec을 위해 제안된 키 복구

RHP의 주요 문제점은 비-연결성에 있다. 따라서, 이는 연결지향이며 상호 운용성을 허락하는 IPSec이나 ISAKMP와는 잘 맞지 않는다. KRA의 제안은 RHP보다 더 나은 해결 방법이다. 그러나, 아직도 모든 통신에 대한 고정 키가 세션 키의 보안에 달려있고, 더 나아가 IPSec 프로토콜은 아직 네트워크의 효율면에서는 최적화되어 있지 않다.

본 논문의 해결방안은 시스템과 네트워크의 보안과, 상호 인증에 대한 상호 운용성을 높이기 위하여, IETF 프로토콜을 기반으로 한다. IETF(ISAKMP, IPSec)에 수정된 RHP을 결합할 수 있는데, Oakley [4]와 같은 Diffie-Hellman 키 교환 방법을 사용하게 된다. 첫번째 단계 후에, KRF는 데이터와 함께 보내진다.

ISAKMP에서는 키 복구에 대한 보안 협상(SA)이 일어난다. 유동성을 증가시키기 위해, RHP 메커니즘의 2단계를 수정하였다.

1. A는 $K_{pu-r(B)}$,$(=g^b \bmod p)$를 얻는다.
2. A는 공용키 $(g^b \bmod p)^{x^*} \bmod p = g^{bx^*} \bmod p$를 유도해낸다.; 이는 세션 키에 대한 암호화 키가 된다.
3. A는 TTP_A and $K_{pu-r(B)}$에 의해 서명 된 $K_{pu-s(A)}$를 전송한다.
4. B는 수신 받은 후, A의 공개 송신 키와 $K_{pr-r(B)}$로부터 $K_{pu-s(A)}$를 검증한다.

2번째 단계에서, x^*는 임시의 비밀이 될 수 있으며, 다음과 같이 계산된다:

$$x^* = f(x, TT).$$

여기서 f는 일-방향 함수이며, TT는 타임스탬프 이다. 결론적으로, 이는 TTP에 의존하는 개인 수신 키를 위탁함으로써 발생하는 영향을 줄여줄 수 있기 때문에, 좀더 안전하다고 할 수 있다.

사용자는 Diffe-Hellman을 실행시켜 키를 복구할 수 있으며, 사용자들의 개인 전송 키를 위탁하고 있는 TTP들도 키를 복구 할 수 있다. 세션이 시작될 때, A는 양쪽 TTP에 대한 상호 인증을 보낸다. 이는, RHP에서 TTP_B와의 연결이 없이도 B가 TTP_A에 의하여 서명 된 A의 인증을 증명할 수 있게 해준다. 이 방법에서 A는 초기화 단계에서 해당 TTP에 대한 상호 인증을 할 수 있게 된다. 이것은 첫 번째 단계를 개선한 것이다.

그 IPSec 세션이 유지되는 동안, 암호화된 메시지와 함께 KRF를 보내게 된다. 비록, 같은 비밀 키가 유지되지만, 세션 키가 위탁되지 않기 때문에, KRF는 반드시 보내져야 한다. 그러므로, KRF는 허락된 대역폭 저하의 범위 내에서 여러 번 보내지게 된다. 우리들은 IP 패킷의 한 부분으로써 IPSec 패킷 안에서 KRF를 보내게 된다. 결국, 변형은 분배된 Diffe-Hellman 키 대신에 양쪽 사용자들의 공개키로 암호화된 세션 키를 보낼 수 있다. 그래서, 해당 KRF는 특정사용자에 의존하게 된다. 이것은 사용자의 정책에 따라서 단 방향으로 KRF를 보내게 한다. 사용자 A는 자신의 TTP 공개키로 암화화 된 세션 키를 보낼지 여부를 선택할 수 있고 B 또한 같은 방법을 사용하게 된다. 이것은 RHP에서 양쪽 TTP가 상대방과 통신 없이 메시지들을 모두 복호화 할 수 있기 때문에 RHP에 비해 흥미로운 특징이다.

4. 결론

본 논문에서는 RHP와 KRA 시스템의 이점들을 결합시키는 두 해결책의 결합하는 방법이다.이 이론은 위탁 메커니즘에 바탕을 두고 있다. 우선, 본 논문은 인터넷 프로토콜들에 RHP의 상호 운용성을 유지하며, RHP보다 안전성을 향상시키고, 인터넷 프로토콜 내에 포함되도록 하고 있다. 둘째로, KRA 방법이 사용되지만, 본 논문에서는 좀더 좋은 안전성을 얻기 위하여, 사용자들 TTP의 공개키가 아니라, 통신하는 두 사용자 사이의 Diffie-Hellman 키 교환으로 분배된 공용 키를 갖는 세션 키나 사용자의 공개키로 암호화한다.

참조

1. N. Jefferies, C. Mitchell, and M. Walker, "A Proposed Architecture for Trusted Third Party Services", in Cryptography: Policy and Algorithms, Proceedings: International Conference BrisAne, Lecture Notes In Computer Science, LNCS 1029, Springer-Verlag, 1995.
2. R. Gennaro, P. Karger, S. Matyas, M. Peyravian, A. Roginsky, D. Safford, M. Zollett, and N. Zunic. "Two-Phase Cryptography Key Recovery System." In computers & Security, Pages 481-506. Elsevier Sciences Ltd, 1997.
3. D. M. Balenson, C. M. Ellison, S.B. Lipner and S. T. Walker, "A new Approach to Software Key Encryption", Trusted Information Systems.
4. The Oakley Key Determination Protocol (RFC 2412)
5. Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
6. The Internet Key Exchange (IKE) (RFC 2409)
7. IP Authentication Header (AH) (RFC 2402)
8. IP Encapsulating Security Payload (ESP) (RFC 2406)
9. T. Markham and C. Williams, Key Recovery Header for IPSEC, Computers & Security, 19, 2000.