공개키를 이용한 IPSec 프로토콜 세션키의 복구

Session Key Recovery of IPSec using PKI

이윤정
제주대학교

Rhee Yoon-Jung
Cheju National University

요약

네트워크에 연결된 시스템들은 TCP/IP의 인터넷 IP 계층에서 키 복구를 도입하여 사용하고 있다. 키 복구 연구는 많은 논란에도 불구하고 연구가 확대되고 있는 주제로서, 키 관리의 형태로 법인차원에서 필요하게 되었다. IPSec은 인터넷의 네트워크 계층에서 IP 메시지에 대하여, 암호화 서비스와 인증 서비스를 제공하는 보안 프로토콜이다. 본 논문은 IETF의 인터넷 표준 구조와 호환되게 키 복구 정보를 포함하는 데이터를 전송하는 방법을 제안하고 있다.

Abstract

The basic observation of the present paper is that cryptographic solutions that have been proposed so far completely ignore the communication context. IPSec is a security protocol suite that provides encryption and authentication services for IP messages at the network layer of the Internet. We propose example to provide key recovery capability by adding key recovery information to an IP datagram. It is possible to take advantage of the commuication environment in order to design key recovery protocols that are better suited and more efficient.

I. 서 론

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

IETF(Internet Engineering Task Force)는 IP계층의 보안을 위하여 IKE(Internet Key Exchange), ISAKMP(Internet Security Association and Key Management Protocol), Oakley와 IPSec 등을 표준화하였다. 이 두 프로토콜 각각은 두 단계로 보안 프로토콜을 이분화 한다. 첫 번째 단계에서는 통신 주체들이 여러 가지 보안 파라미터들 (SA: Security Association)과 세션키를 협상한다. 두 번째 단계에서는 첫 번째 단계에서 협상되었던 SA의 여러 알고리즘을 실행하여 기밀성과 무결성 상대방 인증이 적용된 IP 패킷을 만들어 전송한다.

본 논문은 IETF 프로토콜 표준 구조와 호환되는 수단으로서 키 복구 정보를 담고 있는 바이트를 전송하는 방법을 제안하고 있다. 제안한 방법은 연결 지향적이며 다른 제안들보다 안전한 키 복구 프로토콜을 설계하고 있다.

II. 관련 연구

본 연구에서 IETF 표준과 호환되는 키 복구 프로토콜을 제안하기 위하여 RHP (Royal Holloway Protocol)과 KRA(Key Recovery Alliance)를 살펴본다[1,2]. 이 두 가지 연구는 모두 캡슐과 메커니즘에 기초하고 있다. KEA (Key Escrow Agent)가 키를 복구할 수 있도록 하기 위한 키 복구에 필요한 추가적인 데이터는 키 복구 필드(KRF: Key Recovery Field)를 포함하고 있다.

RHP 구조는 하나의 교환메시지를 갖는 비-상호작용 메커니즘에 기초하며, Diffie-Hellman 이론을 사용한다. RHP 시스템은 송신된 메시지를 사용자의 개인 수신 키를 사용하여 복호화한다. 각 사용자는 사용자 A에 대한 TTP_A로 대표되는 TTP에 등록된다.

RHA 프로토콜 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 한번 이상 여러 번 보낼 필요가 있다. 그러나 이 시스템의 장점은 보안

이 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]

KRA (Key Recovery Alliance) 시스템은 TTP(Trusted Third Party)의 공개키로 세션 키를 암호화하는 방법을 제안하고 있다. KRH(Key Recovery Header)는 네트워크를 통해 KRF를 전송 시키는 방법을 제안하기 위하여 설계되었는데, 이는 키 복구를 시도하는 개체에 의하여 도청 될 수 있다. KRH는 ESP SA에 관한 키 생성 정보를 운반한다. 따라서 KRH는 ESP SA [2]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)나 IBM SKR (Secure Key recovery)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.

선행자와 응답자가 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[3,4].

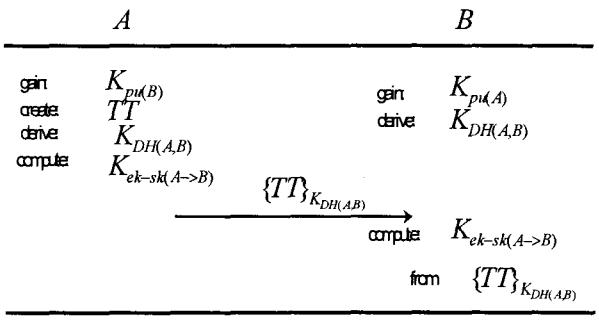
III. 제안된 키 복구 메커니즘

1. KRF의 보안협상 (SA: Security Association)

RHP의 주요 문제점은 비-연결성에 있다. 따라서 이는 연결지향이며 상호 운용성을 허용하는 IPSec이나 ISAKMP와는 부합되지 않는 점이다. KRA의 방법은 RHP보다 더 나은 해결 방법이다. 그러나 아직도 모든 통신에 대한 고정 키가 세션 키의 보안에 의존하고 있으며, 더 나아가 IPSec 프로토콜은 아직 네트워크의 효율성 면에서 최적화되어 있지 않다는 점이 문제점을 안고 있다.

본 논문에서의 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 와 같은 Diffie-Hellman 키 교환 방법을 사용하게 된다. 첫 번째 단계 후에, KRF는 데이터와 함께 보내진다.

ISAKMP에서는 키 복구에 대한 보안 협상(SA)이 일어난다. 유동성을 증가시키기 위해, RHP 메커니즘의 2단계를 수정하였다. [그림 1]은 본 논문에서 제안하고 있는 프로토콜이다.



▶▶ 그림 1. 제안한 프로토콜

A, B : 통신 상대방

TTP_A, TTP_B: A의 TTP, B의 TTP

p : TTP_A와 TTP_B 사이에 공유되는 소수

g : TTP_A와 TTP_B 간에 공유되는 요소

TT : 타임스탬프

$K_{pr(A)}$: A의 개인 키 (TTP_A가 위탁관리 함)

$K_{pu(A)}$: A의 공개 키 ($g^x \bmod p$)

$K_{DH(A,B)}$: A와 B사이에 Diffie-Hellman 공유 키

$K_{ek-sk(A->B)}$: 세션 키에 대한 암호화 키

($=f(g^{xy} \bmod p, TT)$, f는 일방향 함수)

프로토콜의 동작은 다음과 같다.

1. A: $K_{pu(B)}$를 얻고, TT 를 생성하며, $K_{DH(A,B)}$를 유도하고, $K_{ek-sk(A->B)}$를 계산해낸다.

   B: $K_{pu(A)}$를 얻는다. $K_{DH(A,B)}$를 유도한다.

2. A: B에게 $\{TT\}_{K_{DH(A,B)}}$를 전송시킨다.

3. B: 전송을 받은 뒤에, $\{TT\}_{K_{DH(A,B)}}$로부터 $K_{ek-sk(A->B)}$를

계산해낸다.

본 논문에서는, 필요한 키의 수를 감소시켜 RHP를 단순화하였다. 두 번째 단계에서는 타임스탬프와 일-방향 함수를 사용하여 매번 다른 키를 생성하여 세션 키 $K_{ek-sk(A->B)}$ 의 암호화 키에 대하여 최신성을 향상시켰고, TTP에 대한 세션 키의 암호화 키에 대한 TTP들의 의존도를 감소시키고 있다. 결과적으로, RHP에서 TTP에 전적으로 의존해서 만들어지는 개인키에 대한 위탁으로부터 받을 수 있는 영향력을 줄일 수 있기 때문에 RHP 보다 견고하다고 할 수 있다.

2. KRF 데이터 전송

IPSec 세션이 계속되는 동안, KRF는 KRA와 같은 방식으로 암호화된 메시지와 함께 전송된다. 다음은 본 논문에서 제안하는 KRH 형식이다. KRH는 ESP 보안 협상을 위한 키 복구 정보를 담게 된다. 제안하고 있는 KRH의 형식은 [그림 2]와 같다.

Next Header	Length	Reserved
Security Parameter Index (SPI)		
Encrypted Time Stamp		KRF Length
Key Recovery Field (KRF), variable length		
Validation Field type		Validation Field Length
Validation Field Value, variable length		

▶▶ 그림 2. 제안된 KRH 형식

Next Header

8bit 크기이며, KRH 뒤에 오며 데이터의 다음 부분을 알려준다. 이 부분의 값은 IANA(Internet Assigned Numbers Authority)에서 정한 IP 프로토콜의 집합이다.

Length

8 bit 크기이며, KRF의 32bit 워드 길이이다. 최소값은 0 워드이고, 이는 키 복구 메커니즘이 사용되지 않을 때 쓰인다.

Security Parameters Index (SPI)

해당 데이터그램을 위한 보안 협상을 나타내기 위한 32-bit 의사-난수 값. SPI 값 0은 보안 협상이 존재하지 않음을 위해 예약된 숫자이다.

Encrypted Time stamp

ISAKMP의 2 단계에서 발생되는 $\{TT\}_{K_{DH(A,B)}}$ 값. 이것은 KRF가 전송될 때 필요하다. 왜냐하면, TTP에 위탁되지 않기 때문에, 해당 TTP가 KRF를 복구할 때 요구된다.

Key Recovery Field Length

KRF의 길이를 나타내는 32-bit 워드 숫자.

Key Recovery Field

키 복구 데이터. 이것은 ISAKMP의 암호화 키 ($K_{ek-sk(A->B)}$)로 암호화 된 현재의 IPSec 세션에 대한 세션 키를 포함하고 있다.

Validation Field Type

검증 부분을 발생시킬 때 사용된 기술을 나타낸다.

Validation Field Length

검증 부분 값에 대한 32-bit 워드 크기. 검증 부분 길이는 Validation Field Type으로 구성되어야 한다.

Validation Field Value

이 부분의 값은 전체 KRH에 대하여 계산된다.

TTP들은 사용자의 개인키를 위탁관리하며 KRH로부터 전송되어 온 타임스탬프를 얻을 수 있다. 따라서 TTP들은 Diffe-Hellman 알고리즘을 이용하여 사용자와 같은 키를 복구해 낼 수 있다. 만일 동일한 비밀키를 가질 수 있다고 하더라도, KRF가 전송되어야 하는데, 이유는 세션키는 위탁관리되지 않기 때문이다. 따라서 KRF는 여러 번 전송된다. 본 논문에서는 KRF를 IP 패킷을 일부분인 IPSec 안에서 KRF를 전송하고 있다. 또한 KRF는 특정 사용자에 의존하기 때문에 사용자의 정책에 따라 단 방향으로 KRF를 전송하는 것도 가능하다. 사용자는 TTP의 공개키와 함께 암호화된 세션키를 보낼지에 대한 여부를 선택할 수 있다. 이는 RHP 와 비교했을 때 더 진보된 특징이다. 외냐하면 RHP 스킴에서는 양쪽 TTP가 상대방 TTP와의 통신 없이도 모든 메시지를 복호화 할 수 있기 때문에 안전성 면에서 문제를 안고 있기 때문이다.

3. 프로토콜 비교 평가

본 논문에서 제안하고 있는 방법은 IETF와 호환될 수 있도록 수정한 RHP과 KRA 두 가지를 다 채용하고 있기 때문

에 두 시스템의 장점을 조합하고 있다.

본 논문에서 제안하고 있는 스킴은 위탁 메커니즘에 기반하고 있다. 본 논문은 RHP의 상호 호환성을 유지하면서도 RHP 와 비교하여 좀더 견고한 구조를 가지며 IETF의 인터넷 프로토콜 안에 포함시켜 운용할 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, A 는 양쪽 TTP에 대한 상호 인증을 보낸다. 이는, RHP에서 TTP_B 와의 연결이 없이도 B 가 TTP_A 에 의하여 서명 된 A 의 인증을 증명할 수 있게 해준다. 이 방법에서 A 는 초기화 단계에서 해당 TTP에 대한 상호 인증을 할 수 있게 된다. 이것은 첫 번째 단계를 개선한 것이다.

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 허용되는 대역폭 범위 내에서 여러 번 전송된다. 본 연구는 IP 패킷의 한 부분으로써 IPSec 패킷 안에서 KRF를 보내게 된다. 또한, 분배된 Diffe-Hellman 키 대신에 양쪽 사용자들의 공개키로 암호화된 세션 키를 보낼 수 있도록 변형될 수도 있다. 그러므로 해당 KRF는 특정 사용자에 의존하게 된다. 이것은 사용자의 정책에 따라서 단 방향으로 KRF를 보내게 한다. 사용자 A는 자신의 TTP 공개키로 암호화 된 세션 키를 보낼지 여부를 선택할 수 있고 B 또한 같은 방법을 사용하게 된다.

IV. 결 론

본 논문에서는 첫째, 인터넷 프로토콜들에RHP의 상호 운용성을 유지하면서도, 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. 셋째, ISAKMP에서는 키 복구 정보 협상을, IPSec에서는 KRF의 키 복구 정보를 전송 시킬 수 있게 함으로서 IETF 프로토콜인 IPSec과 호환될 수 있으면서도 효율적인 키 복구가 가능하도록 설계되었다.

▌참 고 문 헌▐

[1] K. Rantos and C. Mitchell, "Key recovery in ASPeCT Authentication and Initialization of Payment protocol", Proc. Of ACTS Mobile Summit, Sorrento, Italy, June, 1999.

[2] T. Markham and C. Williams, "Key Recovery Header for IPSEC", Computers & Security, 19, 2000, Elsevier Science.

[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] 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.