VxWorks 기반의 IPv6 IKE 시스템 구현

Implementation of IPv6 IKE System on VxWorks

*강성민, 이재황, 김선우, 김영근
Kang Seong-Min, Lee Jae-Hwang, Kim Sun-Woo, Kim Young-Keun

Abstract - This paper proposes design and implementation for IKE system that is available to IP security communication on IPv6 network. IPsec is a standard for security on network or processing layer of network communication. IPsec consists of step to negotiate security policy and step to negotiate and provide security key material for peer-to-peer security. We use the ISAKMP for negotiating security policy. And we use the IKE for negotiating and providing the key material. The system is based on VxWorks and is tested with Racoon that is a IKE daemon on FreeBSD. In this paper, we propose an implementaion method for mobile host providing network communication with IP security.

Key Words : VxWorks, IPv6, IPsec, ISAKMP, IKE, SA

1. 서론

최근 IP 기반의 인터넷이 정보화 사회에서 정보통신 인프라로 자리매김하고 있으며 유무선 네트워크의 통합 및 Convergence로 인해 미래의 망은 점차 All IP망으로 통합 발전될 것으로 예상되고 있다. 이에 따라 현재 IPv4 주소의 부족, 보안 및 이동성 지원의강화, QoS 보장 등의 문제점들이 대두되었으며, 그 해결 방안으로 새로운 형태의 주소 체계를 가지는 IPv6가 등장하였다. IPv6는 IPv4의 새로운 버전으로 IETF에서 1991년에 시작되어 1996년에 기본 규격의 표준화가 완결되었다. 현재 실제 여러 분야에서 IPv6 관련한 구현 및 표준화를 진행 중이고 6Bone을 비롯한 여러 국가에서 테스트 망을 구축하고 있다.

한편 네트워크를 통한 정보의 유출 및 삭제, 수정 등의 불법적인 사고는 사생활 침해뿐만 아니라 막대한 경제적 손실을 야기할 우려가 있어 정보보호의 중요성에 대한 관심은 점차 높아지고 있다. 이러한 중요성은 이미 IETF에서도 인식되었고, 1993년부터는 IPsec WG을 통하여 인터넷 정보보호에 관한 기본 구조 연구를 시작하였다. IPsec WG은 IPsec 아키텍처를 기술한 RFC2401을 비롯한 29개의 RFC에서 [1] AH와 [2]ESP의 두 가지 확장헤더와 IKE를 정의하였다.

본 논문에서는 IPv6 망에서 IKE를 적용하여 IPsec 통신이 가능한 시스템을 구현한 결과를 소개하고자 한다. 사용한 시스템은 VxWorks OS 기반의 모바일 단말로 무선 랜을 이용하여 통신을 수행한다. 본론에서는 구현한 IPsec 기술의 간단한 개요, 시스템의 S/W 및 H/W 구성, 구현한 시스템의 동작 결과, FreeBSD 시스템과의 호환성 테스트 결과에 대해 설명한다.

저자 소개
* 正 會 員 : 三星電子 디지털미디어연구소

2. IPsec

IPsec은 IP 계층 또는 그 상위 계층 프로토콜을 보호하고자 설계된 프로토콜로 데이터의 기밀성, 근원인증, 무결성, 제3자에 의한 재전송 공격 방지등의 서비스를 제공한다.

그림 1은 IPsec 적용에 따른 인터넷 통신 보안 방법을 나타낸다. IPsec은 IP 단에서, IKE는 어플리케이션 단에서 이루어지며 ISAKMP [3]SA에 의해 결정된 보안 정책을 IP 패킷에 적용한다. IPsec은 전체 IP 패킷에 보안서비스를 제공하는 터널 모드와 상위계층 데이터에 보안서비스를 제공하는 트랜스포트 모드의 두 가지 운용모드를 가지는데, 본 논문에서는 트랜스포트 모드를 수행하도록 설계하였다.

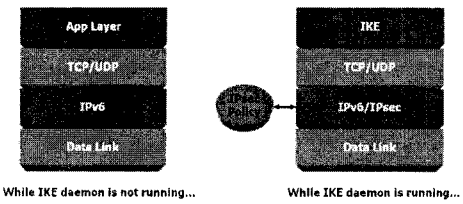

그림 1 IPsec에 따른 인터넷 통신 보안 방법

2.1 ISAKMP

ISAKMP는 양 단간 비대칭 키 관리 및 일대일 통신을 위한 형식을 규정한다. 비대칭이란 양단이 서로 다른 역할을 가지는 것을 의미하는 것으로, Initiator라 불리는 하나는 첫 번째 메시지를 보냄으로써 ISAKMP 메시지들의 교환을 시작하는 역할을, Responder라 불리는 다른 하나는 Initiator로부터 온 메시지에 응답하는 역할을 가진다.

ISAKMP의 키 관리는 키 교환 과정을 포함한다. 키 교환은 양단 사이에서 비밀 키를 생성하기 위해 교환되는 정보와 관계가 있는데, ISAKMP는 아래 과정을 수행하기 위한 키 교환 프로토콜로 IKE를 이용한다.

- 공유된 비밀 키 집합을 생성하는 과정
- 상대방에 대해 인증하는 과정
- 4)PFS를 보장하는 과정

2.2 IKE

IKE는 키 교환 프로토콜로 공유된 키 정보의 효율적인 재생 및 생성을 위하여 2-Phase 접근 개념을 사용한다.

Phase 1은 Phase 2 통신을 위하여 안전한 통신 채널을 설정하는데 목적이 있으며, Main mode와 Aggressive mode의 세부모드를 가진다. Main mode는 6 단계의 정보 교환으로 이루어지며, 서로의 신원을 확인한 후에 암호화된 식별자를 교환하기 때문에 보다 안전한 방법이다. Aggressive mode는 안전한 SA가 성립되기 전에 서로의 식별자를 교환하기 때문에 신원보호가 되지 않지만, 3 단계의 정보 교환으로 이루어지기 때문에 빠른 속도로 키 교환을 수행할 수 있다는 장점을 가진다.

Main mode나 Aggressive mode를 수행하여 SA가 성립되고 공유된 비밀 키 집합을 가지면, IKE 시스템은 실제 IP 데이터 통신을 위한 안전한 통신 채널을 설정하는 과정인 Phase 2를 수행한다. 이는 3단계의 정보 교환인 Quick mode를 통해 이루어지며, Phase 1에서 생성된 공유 비밀 키와 SA를 이용하여 암호화된다. IKE는 양 단이 공유한 키의 재생이나 서로 다른 어플리케이션의 키 생성을 위해서 Phase 2 과정만을 반복함으로써 효율성을 증진시킨다.

2.3 Diffie-HellmanAlgorithm

IKE 과정 수행에 있어 공유된 비밀 키를 생성하는 방법으로 수학적으로 증명된 여러 알고리즘이 존재한다. 구현된 시스템은 Diffie-Hellman(이후 D-H) 프로토콜을 사용하였다. D-H 키 합의 프로토콜은 1976년 Diffie와 Hellman에 의해 개발된 프로토콜로 두 사용자가 사전에 어떠한 비밀교환 없이 안전하지 않은 매체상에서 비밀 키를 공유하도록 한다.

프로토콜은 두 시스템 파라미터 p와 g를 갖는데, 파라미터 p는 소수이고 파라미터 g는 p보다 작은 정수이다. 양 단이 공통된 비밀 키를 협의 하는 과정은 그림 2과 같다. A는 랜덤한 비밀 키 a를 생성하고 B는 랜덤한 비밀 키 b를 생성한다. 그리고 파라미터 p, g 그리고 비밀 키들을 이용해서 그들의 공개 키들을 만든다. A의 공개 키는 g^a mod p이고 B의 공개 키는 g^b mod p이다. 그리고 서로의 공개 키를 교환한다. A는 kab = $(g^b \bmod p)^a \bmod p$를 계산하고, B는 kba = kab = $(g^a \bmod p)^b \bmod p$를 계산한다. 그림 2와 같이, 계산 결과 kab = kba이므로 A와 B는 공유 비밀 키를 가진다. A와 B는 이렇게 공유된 비밀 키를 이용하여 암호화 키와 인증 키를 생성하게 되고, 그 결과 A와 B는 직접적인 키 교환과정 없이 안전한 비밀 키를 가지게 된다.

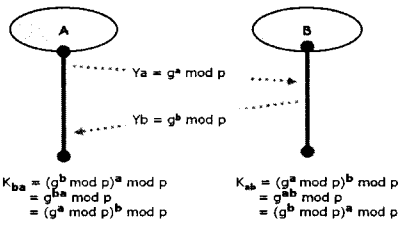

그림 2 Diffie-Hellman Algorithm

3. 시스템의 S/W 및 H/W 구성

3.1 S/W구성

3.1.1 S/W구성

구현한 IKE 시스템의 S/W 구성은 그림 3과 같다. IPsec 통신 시 IPv6 Socket을 이용하도록 xBSD OS에 구현된 Kame IPv6 Stack을 VxWorks OS에 맞도록 포팅하였다. 실제 통신 채널에 IPsec 적용 여부를 선택하는 사용자 인터페이스는 VxWorks에서 제공하는 WindML 이라는 GUI를 이용하여 구현하였다.

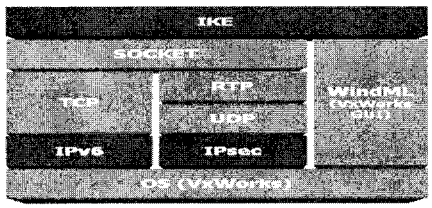

그림 3 IPv6 IKE 시스템 S/W 구성도

3.1.2 VxWorks의 개요

Vxworks는 Windriver사에서 개발한 상용 Emedded RTOS로, Fast Multitasking/Interrupt 와 Preemptive and Round-Robin Scheduling, 다양한 CPU(x86, MIPS, ARM 등) 및 Device Driver/BSP를 지원하며 POSIX와의 호환성을 지닌다. 아울러 개발 환경 및 Debugging Tool은 Tornado 라는 GUI 통합환경으로 구성되어 있으며 다양한 기술지원이 가능하다.

본 논문에서는 다음 장에서 설명할 H/W 시스템에 Vxworks를 포팅한 후에 IPsec 통신이 가능한 IKE 시스템을 구현하였다.

3.2 H/W구성

IKE 시스템이 구현된 H/W 시스템은 현재 NEXIO라는 이름으로 WINCE 4.2가 내장되어 시장에 출시된 제품이다. IntelStrongARM 계열의 PXA255를 CPU로 사용하고 무선랜 모듈(802.11b)를 내장하고 있는 것이 특징이다. 구현된 IKE 시스템은 내장된 무선랜 모듈을 이용하여 IPsec 통신을 수행한다.

4. 구현한 IPv6 IKE 시스템 동작

IPsec 통신을 위한 양 단은 각각 ISAKMP 메시지 통신을 시작하는 Initiator와 Initiator의 요청에 응답하는 Responder로 나뉜다. 본 논문에서 구현한 시스템은 Initiator와 Responder의 기능을 모두 포함하도록 설계되었으며, 서로의 식별자가 보호되는 Main mode와 빠른 키 교환이 가능한 Aggressive mode의 선택이 가능하다. Initiator가 Responder에게 SA를 포함하는 메시지를 보냄으로써 ISAKMP 단계는 시작된다. 그림 4와 그림 5는 Phase 1 단계의 Main mode와 Aggressive mode를, 그림 6은 Phase 2 단계의 Quick mode의 동작을 각각 나타낸다.

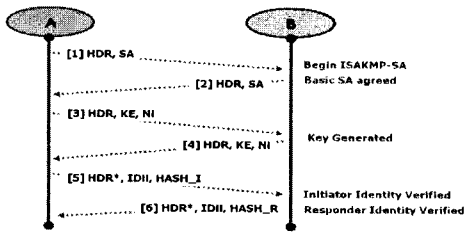

그림 4 Main mode의 동작

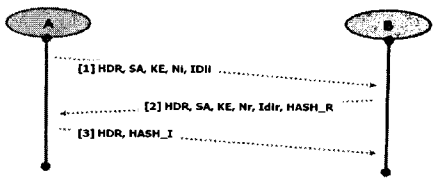

그림 5 Aggressive mode의 동작

Phase 1의 기본적인 동작을 살펴보면, Initiator가 수행 가능한 암호화 및 인증 알고리즘 등 SA를 제안하면 Responder는 그 중 수행 가능한 SA를 택하여 응답한다. 구현한 시스템은 암호화 알고리즘으로는 3DES를, 인증 알고리즘으로는 HMAC-MD5를 협의하도록 설계되었다. 또, Initiator와 Responder는 공유 비밀 키의 키 요소가 되는 자신의 공개 키를 전달한다. 이 공개 키는 D-H 알고리즘을 이용하여 계산된다. 각각의 단계 수행 시, 양 단은 SA를 이용하여 상대방의 신원을 인증한다.

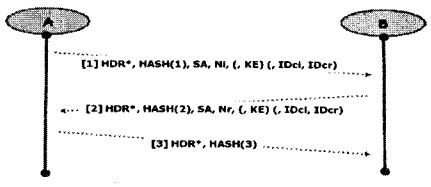

그림 6 Quick mode의 동작

Phase 2 단계의 수행 과정 또한 Phase 1단계의 기본 과정과 동일하나 통신 채널이 Phase 1 단계의 수행 결과인 SA와 공유 비밀 키를 이용하여 보호된다는 차이점을 가진다.

5. 결론

본 논문에서는 IPv6 망에서 IPsec 통신이 가능한 IKE 시스템을 구현한 결과를 소개하였다. 구현한 시스템은 IKE 과정을 수행하는데 필요한 역할인 Initiator와 Responder 의 기능을 모두 포함하고 있기 때문에 두 개의 단말을 통한 IPsec 통신 테스트가 가능하였다. 아울러 FreeBSD의 IKE 데몬인 Racoon을 이용하여, FresBSD 기반의 시스템과 구현한 VxWorks 기반의 모바일 시스템간의 IPsec 통신 수행으로 구현한 시스템의 호환성 테스트를 실시 하였다. 테스트 결과, 구현한 시스템간 IPsec 통신이나 FreeBSD의 Racoon 데몬과의 호환성 문제는 없었다. 다만, 키 요소를 생성하고 공유 비밀 키를 생성하는 과정에서 이용된 D-H 알고리즘은 상당한 수학적 계산량이 필요하기 때문에 모바일 단말이라는 H/W의 성능 문제로 약간의 시간 지연 문제를 발견하였다. 앞으로 보다 빠른 처리 시간을 가지는 IKE 시스템의 개발을 위해서는 D-H 알고리즘 관련한 키 요소 생성이나 키 계산의 최적화 과정 개발이 선행되어야 할 것이다. 또한, 본 논문에서 소개된 IKE 시스템은 VxWorks 외에 Real Time Linux나 WinCE에서도 구현 가능할 것이다.

참 고 문 헌

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

[2] D. Maughan & M. Schertler & M. Schneider & J. Turner, "Internet Security Association and Key Management" Protocol", RFC 2408. 1998

[3] D. Harkins & D. Carrel, "The Internet Key Exchange", RFC 2409. 1998

[4] H. Orman "The OAKLEY Key Determination Protocol", RFC 2412. 1998

[5] 김용진, 신명기, 박정수, 이승윤 "차세대 인터넷 IPv6" 다성출판사 2002

---

1) AH (Authentication Header) : 메시지 checksum을 이용하여 보안 서비스 제공

2) ESP (Encapsulating Security Payload) : 암호화 알고리즘을 이용하여 보안 서비스 제공

3) SA (Security Association) : IPsec의 기초적인 요소로, 동작 모드 및 암호화 알고리즘, 키의 lifetime등 AH/ESP에 대한 협상을 수행한다. 이는 단방향성 처리를 하기 때문에 양 단간 IPsec 통신을 위해서는 2개 이상의 SA가 필요하다.

4) PFS (Perfect Forword Securecy) : 하나의 키를 이용하여 이전이나 이후에 사용될 키를 유추할 수 없음을 의미한다.
- 전송되는 데이터의 암호화 과정에 사용된 키는 다른 어떤 부가적인 키의 생성에도 사용되지 않음
- 하나의 키를 유도하는데 사용된 키 요소는 더 이상 다른 어떤 키의 유도에도 사용되지 않음