IPv6용 하드웨어 IPsec을 위한 키 교환 시스템의 설계 및 구현

박동익° 류준우 공인엽 이정태

°부산대학교 컴퓨터공학과

(dipark°, jwryu, leafgirl, jtlee)@pusan.ac.kr

Design and Implementation of Key Exchange System for IPv6 Hardware IPsec

Dong-Ik Park° June-Woo Ryu In-Yeup Kong Jung-Tae Lee

Department of Computer Engineering, Pusan National University

요 약

운영체제가 지원되지 않는 소규모 기기에서 IPv6의 보안기능을 고성능으로 제공하기 위해 본 연구실에서는 IPv6용 IPsec 프로토콜과 암호화 알고리즘을 하드웨어로 구현하였다. 이러한 IPv6용 하드웨어 IPsec을 기반으로 한 보안 서비스를 제공하기 위해서는 안전한 키의 교환과 인증이 중요하다. 이를 위하여 본 논문에서는 IPv6용 하드웨어 IPsec을 위한 키 교환 시스템으로서 IKE Module을 설계하여 드라이버 프로그램으로 구현하였다. 그리고 구현된 IKE Module을 IPv6용 하드웨어 IPsec의 드라이버로 탑재하여 기존의 소프트웨어 IKE Module과의 테스트를 통하여 기능을 검증하였다.

1. 서 론

무선 인터넷과 전자상거래 등의 활성화에 따른 보안 기능의 요구에 따라 IPv6에서는 IP 계층에서의 보안 서비스를 제공하기 위하여 IPsec 프로토콜을 기본 요구사항으로 채택하였다[1].

그러나 기존의 IPsec 프로토콜은 운영체제에 의존적인 소프트웨어로 구현되어 있기 때문에 운영체제가 없는 소규모 단말에서는 사용될 수 없으며 성능 면에서도 한계가 있다. 이러한 문제를 해결하기 위해 본 연구실에서는 IPv6용 IPsec을 하드웨어로 구현하였다.

기 구현된 IPv6용 하드웨어 IPsec이 AH, ESP 확장헤더를 통한 신뢰성 있는 보안 서비스를 제공하기 위해서는 양단간의 상호 인증과 안전한 키의 교환이 선행되어야 한다.

이에 본 논문에서는 IKE를 기반으로 하여 IPv6용 하드웨어 IPsec을 위한 키 교환 시스템을 드라이버 프로그램으로 설계하고 구현하였다. 구현된IKE 드라이버는 IPv6용 하드웨어 IPsec과 연동하여 기존 소프트웨어 Module과의 테스트를 수행함으로써 기능과 호환성을 검증하였다[2],[3].

2. IPsec의 키 교환 시스템

2.1 IPsec

IPv6에서의 보안기능은 IPsec의 AH (Authentication Header)와 ESP (Encapsulating Security Payload) 확장헤더를 기반으로 한다. AH 프로토콜은 IP 데이터그램에 대해 무결성(Integrity), 인증(Data Origin Authentication), 재전송 공격(Replay Attack) 방지 등과 같은 보안 서비스를 제공하기 위해 사용되며 MD5, SHA-1 등의 알고리즘을 사용한다. ESP 프로토콜은 IP 데이터그램에 3DES, AES 등의 알고리즘을 적용하여 기밀성(Confidentiality), 무결성(Integrity), 인증(Data Origin Authentication), 재전송 공격(Replay Attack) 방지 등과 같은 보안 서비스를 제공하기 위해 사용된다.

2.2 IKE

IPsec을 통한 보안 기능에 있어서 양단간의 신뢰성 있는 암호화 키의 교환이 중요하며, 이를 위한 키 교환 시스템으로서 IKE가 사용된다. IKE는 두 종단간의 상호 인증을 제공하며 AH와 ESP를 위한 키를 생성하고 관리한다. 이러한 IKE는 헤더, 페이로드 형식 및 교환 유형을 정의하는 프레임웍인 ISAKMP에 기반한 Main, Aggressive, Quick, New Group의 4가지 모드로 정의된다.

IKE의 동작은 키 교환을 위한 안전한 채널을 생성하는 Phase-1과 IPsec을 위한 암호키를 교환하는 Phase-2의 두 단계로 이루어진다.

Phase-1에서는 안전한 채널을 형성하기 위한 SA(Security Association)를 협상하고, 세션 키를 교환한다. Main Mode는 6단계 과정으로서 ID(키 교환을 위해 사용되는 값)를 안전하게 유지하는 것을 특징으로 하며, Aggressive Mode는 3단계 과정으로서 ID정보의 유지를 보장하지 않는다.

Phase-2는 IPsec를 위한 SA를 협상하고 암호키를 교환하는 단계이다. Phase-2의 모든 패킷은 Phase-1의 설정내용에 의해 보호되며 Quick Mode(3단계) 또는 New Group Mode(2단계)로 이루어진다.

그림 1은 Pre-Shared Key와 Main Mode를 사용한

Phase-1의 예를 보여준다.

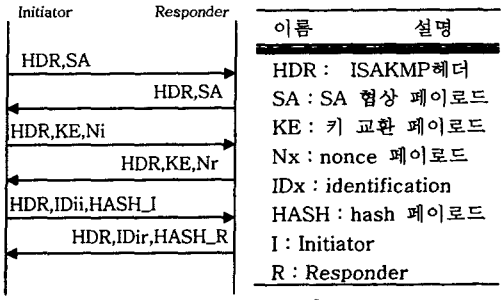

그림 1. IKE Phase - 1의 Main Mode

3. IKE 기반 키 교환 시스템의 설계

IPv6용 하드웨어 IPsec Module은 그림 2에서 보는 바와 같이 IPsec Core, 암호화 알고리즘, IKE로 구성되며, IPsec Core는 연구실에서 기 구현된 TCP/IPv6 기본 Module을 기반으로 IPsec의 AH, ESP 확장헤더 처리기능을 추가로 구현한 것을 이용하였다[4],[5],[6]. IKE 드라이버는 암호화/복호화에 사용될 알고리즘 선택과 암호화 키 생성 등을 담당하며, 드라이버 프로그램으로 구현되어 있다. Crypto Algorithm Module은 AH를 위한 MD5 및 SHA-1과 ESP 확장헤더에 필요한 3DES 및 AES 암호화 알고리즘을 하드웨어로 구현한 것이다.

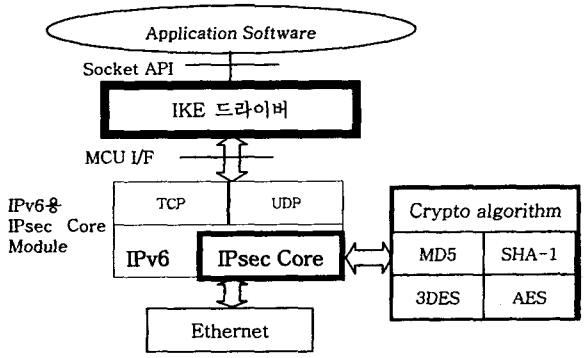

그림 2. IPv6용 하드웨어 IPsec Module의 전체 구성

3.2 IKE 드라이버

IKE는 MCU에 의해 수행될 드라이버 프로그램의 일부분으로 구현하였고, IKE의 실행 결과로 얻어진 여러 정보와 암호화 키 정보는 IPsec Core로 전달되어 IP 패킷을 암호화/복호화할 때 사용된다. IKE 드라이버의 동작은 그림 3에서 보는 바와 같이 8단계를 거쳐서 이루어진다.

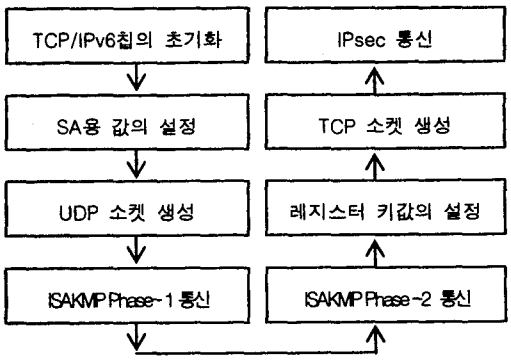

그림 3. IKE의 동작 흐름도

이를 구현하기 위하여 IKE Module은 그림 4와 같이 Interface module, Application module, Network module, Crytpography and math module로 나누어 IKE를 설계하였다.

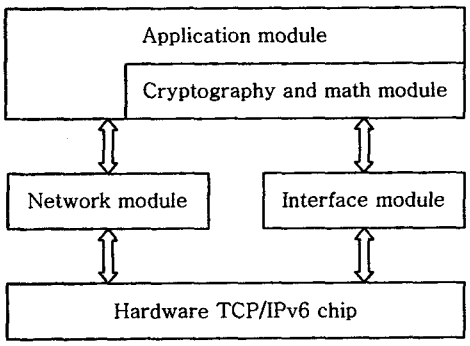

그림 4. IKE의 Module 구성도

각 Module의 기능을 간략히 기술하면 다음과 같다.

3.2.1 Interface module

IPsec 코어 Module과 통신하기 위한 Module로써 AH/ESP 여부, 암호화 알고리즘의 종류, 키, 키의 크기, IV(Initialization Vector), SPI(Security Parameter Index), SN(Sequence Number)를 IPsec Core Module로 넘겨준다. 해당 레지스터에 값을 저장함으로써 키 값을 전달하며 다음의 표 1은 IKE와 IPsec Module간의 Interface를 보여주고 있다.

표 1. IKE와 IPsec간의 Interface

Interface	설명
IPsec_comm	AH와 ESP를 구분
AH_algorithm	AH의 알고리즘 선택(MD5와 SHA-1)
ESP_algorithm	ESP의 알고리즘 선택(AES와 3DES)
IPsec_Key	키의 크기(128,160,192,256비트의 키)
IPsec_IV	암호화용 Initialization Vector
IPsec_SPI	IPsec SA를 구분하는 값
IPsec_SeqNum	재생방지를 위한 Sequence Number

3.2.2 Application module

하드웨어 TCP/IPv6칩이 초기화 되면 키 교환을 위한 Cryptography and math module을 구동시킨다. SA의 설립 후에 생성된 정보는 IPsec Core의 해당 레지스터에 저장되며 호스트의 응용 프로그램과 IPsec 기반으로 통신을 하는 Module이다.

3.2.3 Network module

이 Module은 전반적인 통신부분을 담당하는 Module로서 키 교환에 앞서 통신 소켓을 제어하고, UDP(500번 포트)를 사용하여, 상대편 호스트와 통신하도록 한다.

3.2.4 Cryptography and math module

이 Module의 주요 기능은 Diffie-Hellman을 위한 초기화와 ISAKMP 패킷에 대한 처리이다. 이를 위하여 ISAKMP/OAKLEY 프로토콜을 이용해서 네트워크 Module을 통하여 ISAKMP 패킷을 전송한다.

4. 동작 테스트

IKE 드라이버를 테스트 하기 위한 시험망은 부산대학교내의 IPv6 시험망의 일부를 사용하였으며 세부 구성은 다음과 같다[7].

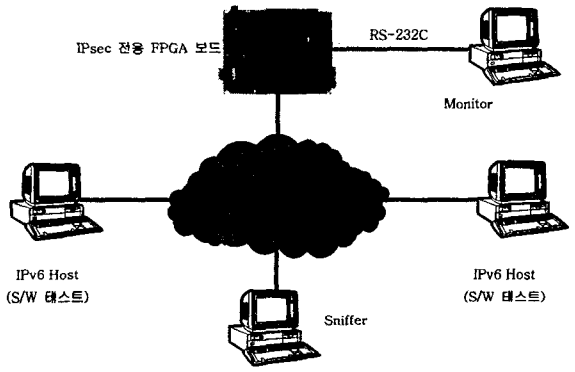

그림 5. IKE 드라이버 테스트를 위한 시험망

FreeBSD 기반의 IPv6 Host와 패킷 캡쳐를 위한 스니퍼 및 IPsec 전용 FPGA보드로 구성되는데, IPv6 Host는 kame 스택으로 IPv6 패치를 한 것이다. 기능 테스트에 있어서는 본 연구실에서 기 구현된 MD5, SHA-1, 3DES, AES 암호화 모듈과 Pre-shared Key를 사용하였다.

아래의 그림은 Main Mode에서 ISAKMP 패킷의 내용을 나타내고 있으며, IKE를 통해 교환된 레지스터 값을 보여주고 있다.

```
[IPv6 Frame]
IPv6: Version = 6
IPv6: Next header = 0x11, IP: Protocol = 17, UDP
IPv6: Source addr =
 3ffe:2e01:0024:0000:0290:27ff:fe3c:a7cc
IPv6: Destin addr =
 3ffe:2e01:0024:0000:0250:bfff:fe49:55be
[UDP Frame]
UDP: Source port = 500, isakmp
UDP: Destination port = 500, isakmp
```

(a) ISAKMP Packet

```
ah mode=transport spi=32986229(0x01f75475)
    A: hmac-sha1
 0e4d2241 95d955a5 051be659 5a394152 fe65ff67
    seq=0x0000000d replay=4
```

(b) HMAC-SHA-1용 160 bit Key

그림 6. IKE 테스트 후 결과

5. 결론 및 향후 과제

인터넷을 통한 안전한 통신을 위하여 IPv6에서는 IP계층에서 보안 서비스를 제공하는 IPsec의 사용이 필수적인 요소이다. 그러나, 기존의 IPsec 프로토콜은 운영체제가 없는 시스템에서 사용할 수 없고 소프트웨어이므로 성능에도 한계가 있다. 이에 대한 해결책으로서 하드웨어로 IPsec 프로토콜이 구현되었고, 본 논문에서는 하드웨어 IPsec Module을 위한 키 교환 시스템(IKE)을 설계 및 구현하였다. 이로써 IPv6용 하드웨어 IPsec Module은 기본적인 보안기능과 더불어 신뢰성 있는 키 교환 기능을 제공할 수 있다. 구현된 키 교환 시스템은 IPv6용 IPsec 하드웨어 칩과 연동하여 동작되며 기존 소프트웨어 Module과 호환된다. 향후 과제로는 Mobile IPv6에서의 키 관리를 위해 키 교환 시스템의 경량화와 차세대 IKE의 적용부분을 연구하는 것이다.

5. 참고 문헌

[1] S. Deering and B. Hinden, "Internet Protocol, Version 6 (IPv6) specification", IETF RFC 2460, December 1998
[2] D. Harkins and D. Carrel, "The Internet Key Exchange(IKE)", IETF RFC 2409, November 1998
[3] Niklas Hallqvist and Angelos D. Keromytis, "Implementing Internet Key Exchange(IKE)", 2000 USENIX Annual technical Conference, June 2000
[4] 이정태 외 9명, "USB 카메라용 인터넷어댑터 설계 결과보고서", ㈜Wiznet, December 2001
[5] 김경태 외 2명, "IPv6용 IPsec 프로토콜의 하드웨어 설계 및 구현", 정보과학회 추계 학술대회 제출, 2002
[6] 김지욱 외 1명, "IPv6용 HMAC-SHA-1 하드웨어 Module의 설계 및 구현", 정보과학회 추계 학술대회 제출, 2002
[7] ETRI, "IPv6 포럼 코리아 기술문서, IPv6 라우터 및 호스트 설치 및 설정 방법(FreeBSD4.2) (TM2001-003)", March 2001.