대학 전산망에서의 IPSec 키 관리 시스템

김건웅[0], 윤성중
목포해양대학교 해양전자 · 통신공학부
kgu@mmu.ac.kr

The IPSec Key Management System in Campus Networks

Geonung Kim[0], Seong-jung Yoon

Division of Communication & Electronic Engineering, Mokpo National Maritime University

요 약

대학 전산망은 다양한 종류의 하드웨어와 소프트웨어로 이루어진 대표적인 이질망이며, 다양한 성향을 갖는 사용자들이 공존하는 환경이므로 망 계층 보안 서비스의 도입이 필연적이다. 본 논문에서는 대학 전산망에서 IPSec을 도입하는데 필수적인 IPSec 키 관리 시스템을 제시한다. 제안된 IPSec 키 관리 시스템은 IPSec과 PKIX가 결합된 형태로 구성되며, 각 호스트는 부팅 과정에서 IP 주소를 결정 한 후, 망 계층 서버에 자신의 IP 주소와 공개키를 등록하여 망 계층 보안 서비스를 제공하도록 한다. 또한 망 계층 인증 서버는 웹 인터페이스를 통해 망 관리자가 전체 구성원의 키를 관리하는 인터페이스를 제공한다.

1. 서 론[1)]

인터넷 망을 통한 정보 교류가 증가함에 따라 인터넷 보안의 중요성도 날로 커지고 있다. 현재 인터넷 망 프로토콜인 IPv4에서 보안을 제공하기 위해 시작된 IPSec에 대한 연구는 차세대 망 프로토콜인 IPv6에 이르러 기본 프로토콜로 포함되기에 이르렀다. 따라서 IPv6가 도입되면 현재 트랜스포트 계층이나 응용 계층에서 개별적으로 제공되던 보안 서비스가 망 계층에서 제공되므로, 보다 신뢰할 수 있는 망 환경 구축이 가능할 것이다.

대학 전산망은 본부 시스템을 구성하는 서버들과 교직원들의 개인용 컴퓨터, 실습실의 컴퓨터, 그리고 학생들의 개인용 컴퓨터 또는 노트북들로 구성된, 이질적인 망이다. 특히 사용자들의 구성이 다양하여, 일반 회사의 구성원과 같은 사용 형태를 나타내는 그룹도 존재하지만, '스크립트 키드(script kiddies)'나 '크랙커(cracker)', '해커(hacker)' 등 보안에 위협을 주는 사용자들도 공존한다. 그 결과 인터넷 공격의 진원지가 되거나 중간경유지 역할을 하는 경우가 빈번히 일어나고 있다. 따라서 이러한 보안 위협을 근본적으로 방지할 수 있는 IPSec 또는 IPv6와 같은 망 계층의 보안 서비스 도입은 필연적이다. 본 논문에서는 대학 전산망에서 IPSec 도입을 위해서 필수적인 IPSec 키 관리 시스템 도입 방안에 대해 강구한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 인터넷 보안 구조 전반을 검토하고, 다음 3장에서는 공개키 암호화를 이용한 인증 방법과 이를 지원하기 위한 공개키 기반 키 관리 시스템의 역할, 제안된 키 관리 시스템의 도입으로 인한 호스트의 망 구성 설정의 변화를 검토한다. 4장에서는 망 계층 보안 서비스를 제공하기 위한 시스템 구현 방안을 모색하고 5장에서 결론을 맺는다.

2. 인터넷 보안 구조

본 논문은 한국과학재단 목적기초연구(R05-2002-000-01055-0)의 중간 결과물입니다.

인터넷 보안 구조는 4가지 요소들로 구성되어 있는데, 그것들은 보안 프로토콜, 보안 연관, 키 관리 프로토콜, 그리고 인증이나 암호화에 쓰이는 다양한 알고리즘들이다.[1][2]

보안 프로토콜에는 AH(Authentication Header)와 ESP (Encapsulating Security Payload)가 있다. 여기서 AH는 비연결형 무결성(connectionless integrity), 자료 출발지 인증(data origin authentication)을 제공하며, 부수적으로 재전송 방지(anti-replay) 서비스를 제공할 수 있다. ESP는 기밀성(confidentiality)과 제한된 트래픽 흐름 기밀성(traffic flow confidentiality)을 제공하며, 비연결형 무결성, 출발지 인증, 재전송 방지 서비스도 제공할 수 있다. 이러한 두가지 프로토콜은 각각 적용될 수도 있고 동시에 적용될 수도 있다. 또한 각 프로토콜은 트랜스포트 모드(transport mode)와 터널 모드(tunnel mode)로 동작할 수 있다[3][4].

보안 연관(SA: Security Association)은 논리적 연결로서 AH나 ESP 서비스는 이를 이용하며, 뒤에서 언급할 키 관리 프로토콜들의 주 역할은 이러한 SA를 생성하고 유지하는 역할을 담당한다. 이러한 SA는 SPI(Security Parameter Index), IP 목적지 주소, 보안 프로토콜 식별자(AH 또는 ESP)로 구별되며, 서비스별로, 방향별로 하나씩 생성되어야 한다. 따라서 하나의 양방향 연결에서 AH와 ESP 서비스를 동시에 이용하고자 한다면 4개의 SA가 필요하다.

이러한 보안 연관에 관련된 데이터베이스로 SPD와 SAD가 있는데, SPD는 각 IP 데이터그램이 어떤 방식으로 다루어져야 하는지에 대한 정보를 담고 있다. IPSec 수신자측은 이를 바탕으로 데이터그램을 폐기, IPSec을 적용하지 않고 통과, 또는 IPSec을 적용한다. 각 SA는 SAD에 하나의 엔트리(entry)로 저장되는데, 여기에는 IPSec 처리에 관련된 순서 번호나 각 프로토콜에서 이용하는 알고리즘이나 키에 대한 정보를 담고 있다.

IPSec에서는 SA의 수동 설정과 자동 설정을 모두 규정하고 있는데, 보안 프로토콜과 독립적으로 운영되도록 되어있다. 수동 설정은 관리자가 직접 각 시스템의 키를 설정하는 방법으로 소규모의 고정된 망 환

경에서 운영이 가능하다. 자동 설정은 IKE[5]를 비롯한 키 관리 프로토콜을 이용하여 사용자별, 세션별로 키를 생성하고, 유지하며, 폐기하는 것으로서 현재 IKEv2[6]와 JFK[7] 등이 활발히 논의 중이다. SA의 세밀성(granularity)은 이러한 자동 설정이 지원되는가에 대해 종속적인데, 미세한 SA를 지원하기 위해선 자동 설정이 필수적이며, 또한 규모가 큰 유동 망에서 보안 구조를 적용하고자 할 때에도 필수적이다.

마지막으로 인증이나 암호화에 쓰이는 다양한 알고리즘들인데, 인터넷 보안 구조에서는 이들에 대한 특별한 제약이 없이 모두를 수용할 수 있는 구조로 되어 있으며 상호 호환을 위해 최소한의 알고리즘을 반드시 포함하도록 규정하고 있다.

3. 공개키 암호화를 이용한 키 관리 시스템

비대칭형 알고리즘에서는 공개키 또는 개인키로 전달정보를 암호화함으로써 보안이 가능한데, 문제는 교환하는 상대방이 적법한 사람 본인이 맞는가 하는 인증 문제이다. 이를 해결하기 위한 방안이 전자인증서(digital certificate)와 이를 발급하는 인증기관(CA: Certificate Authority)의 도입인데, 대표적인 표준이 X.509 PKI(Public Key Infrastructure)이다. X.509는 1988년 발표된 이후, 보완과 추가를 통하여 1996년 v3까지 발표되었는데, IETF의 pkix 그룹에서는 X.509를 기반으로 하는 전자인증서의 구성과 전자인증서의 발급/보관/폐기, 전자인증 기관의 구성 등을 정의하는 작업을 하고 있다[8].

IKE에서는 2단계에 걸쳐 SA를 설정하는데, 첫 단계에서는 IKE 자체의 SA를 설정하고, 두 번째 단계에서 IPSec SA를 설정한다. 첫 단계에서는 IPSec SA 설정시 필요한 암호화 매개변수를 합의하고 공유 비밀키를 생성한다. 이때 쌍방간의 인증 방법으로 ①전자서명, ②공개키 암호화, ③수정된 공개키 암호화, ④미리 공유된 비밀키 등을 활용할 수 있다. 이들 중 가장 보안이 강화된 방법이 공개키 암호화 방법을 이용하는 ②와 ③이다. 다음 그림 1은 ②의 1단계의 메인 모드(main mode)를 보여주고 있다. ③은 이러한 공개키 기반 암호화/복호화를 반으로 줄인 방법이다[5].

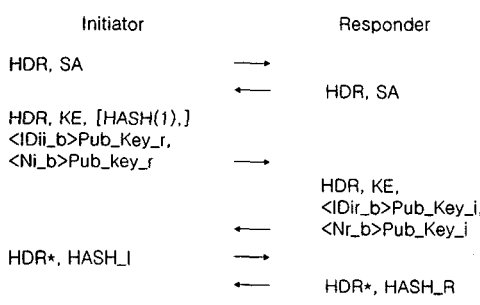

그림 1. 공개키 암호화를 이용한 메인 모드

그림 1에서 보이는 바와 같이 6개의 메시지를 통해 인증을 수행하고, IKE SA를 설정한다. 여기서 세 번째 메시지와 네 번째 메시지에서 각각 상대방의 공개키를 이용하여 신원(IDii, IDir)과 nonce(Ni, Nr)을 암호화하여 전송하고, 그것을 자신의 비밀키로 복호화 하여 다음 처리를 함으로써 인증이 이루어진다. 결국 이를 이용하기 위해서는 각자 신뢰할 수 있는 제3자를 통해 상대방의 공개키를 알아내야 한다.

일반적인 공개키 기반 구조의 구성 요소는 ①인증서(Certificates), ②인증서 상태 확인 방법(Certificate Status Mechanism), ③인증기관(CA: Certificate Authority), ④등록기관(RA: Registration Authority), ⑤데이터 복구 에이전트(Data Recovery Agent), ⑥인증서와 CRL(Certificate Revocation List) 저장소, ⑦인증 정책(CP: Certification Policy)과 인증 적용 지침(Certification Practice Statement)이다[9]. 공개키 기반 키 관리 시스템의 구성도 일반적인 공개키 기반 구조의 요소들을 그대로 이용할 수 있는데, 다만 실제로 인증되어야 하는 대상이, 일반적인 사용자가 아닌, 호스트인 관계로 호스트가 스스로 키를 생성하고, 공개키를 등록하는 방법이 제공되어야 한다.

일반적인 호스트의 망 구성 설정은 하드웨어 주소와 IP 주소간의 매핑, IP 주소와 호스트 이름간의 매핑으로 나누어 이루어진다. 하드웨어 주소와 IP주소간의 매핑은 호스트 내의 설정 파일을 이용할 수도 있고, DHCP나 RARP 등의 프로토콜을 이용할 수 있다. IP 주소와 호스트 이름간의 매핑은 DNS(Domain Name Service)를 이용한다. IPSec을 도입하고자 하면, 앞서 언급한 두 가지 매핑 이외에도 IP 주소와 그것의 인증 정보간 매핑이 필요하다. 이러한 매핑을 담당하는 것이 공개키 기반 키 관리 시스템이다.

호스트가 부팅되면 자신의 IP 주소를 설정한 후, 그림2에서 보이는 기능을 수행하여야 한다. 이때 CA 관련 정보는 구성 파일을 이용하거나, DHCP를 통해 전달받을 수 있다. 또한 호스트가 종료하는 경우, 자신이 등록했던 공개키를 삭제하는 기능이 필요하다. 반대로, 망 계층 인증서버는 등록된 공개키의 생명주기가 끝나면 자동 삭제하는 기능이 필요하다.

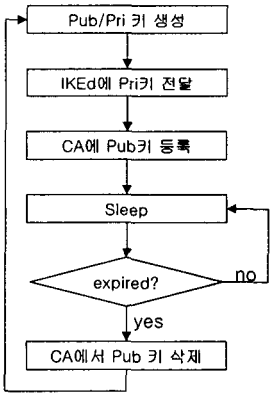

그림 2. 인증 정보 관리 동작

그림 3은 PKI를 기반으로 하는 망 계층 인증 서버와 IKEd와의 동작을 보이고 있다. 그림에서는 IKEd의 일부에서 CA와 동작하는 것으로 표현하였지만, IKEd와 이런 인증을 담당하는 기능간의 인터페이스가 정의되면 분리되어 수행할 수도 있다. 또한 망 관리자가 Web 서비스를 기반으로 구성원들의 인증 정보를 검색하고 관리할 수 있는 일련의 작업을 수행할 수 있는 인터페이스를 제공할 수 있다.

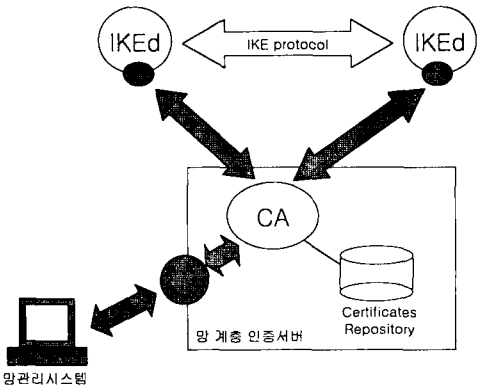

그림 3. PKI 기반 키 관리 시스템

4. 구현 방안

현재 대부분의 운영체제에서 IPSec을 구현하는 작업이 진행 중이다[10][11][12][13][14][15][16][17][18]. 현재 Linux에서 IPSec 서비스를 제공하는 대표적인 구현이 FreeS/WAN[10]인데, 여기에서는 IPSec의 AH, ESP를 지원하며, IKE도 일부 지원하고 있다. 그러나 이 프로젝트의 주목적이 IPSec을 이용한 가상사설망(VPN)의 지원이어서, 제한된 호스트들간의 연결 또는 호스트와 망 사이의 IPSec 게이트웨이(gateway) 기능 지원에 초점이 맞추어져 있고, 현재는 구성 파일에서 상대방의 공개키들을 저장하고 있는 형태로 지원되고 있다. 또한 독립된 프로젝트로 FreeS/WAN에서 X.509 인증서를 이용하도록 패치 형태로 개선하는 작업이 진행 중이다[11].

Solaris 9에서는 IPv4의 SA의 경우 IKE를 통한 자동 설정도 지원하고 있으며, IPv6의 SA에 IKE를 지원하는 구현 작업이 진행 중이다[12]. MS/Windows에서는 Windows NT 4.0 이후 버전과 Windows 2000에서 별도의 패키지 형태로 IPv6를 지원하고 있으며[13], Windows XP에서는 실험적 지원 형태로 운영체제에 포함되어 있다[14]. 그러나 다른 운영체제에 비해 상대적으로 진행이 느린 편이다.

다양한 운영체제가 존재하는 대학전산망에서 망 계층의 보안 서비스를 지원하기 위해서는 구성 요소들의 운영체제에서 IPSec을 지원하는 것이 선결되어야 하는데, UNIX 계열의 경우, 운영체제의 업그레이드나 해당 패키지의 설치로 지원이 가능하다. 그러나 대부분의 일반 사용자가 이용하고 있는 MS/Windows 계열의 경우, 아직 구현이 제대로 진행되지 않은 관계로 도입하는데 시간이 요구된다. 이러한 IPSec 부분은 시스템 전체 성능을 좌우하는 기능이므로 독립된 응용 프로그램이 아닌 운영체제 내부에서 제공하는 것이 바람직하다.

망 계층 인증 서버의 경우 디렉토리 서버나 LDAP 서버를 이용하여 저장소를 구축하고, PKI 인증서를 이용하여 인증 정보를 교환하며, 현재 진행중인 pkix 작업 그룹의 연구결과를 수용하여 구현이 가능하다. 앞으로 Linux 운영체제에서 LDAP 서버를 이용하여 망 계층 인증 서버를 구현할 예정이다[19].

5. 결론

대학 전상망과 같은 다양한 구성원과 다양한 응용이 존재하는 이질망에서는 망 계층의 보안 서비스 도입은 필수적이며, 이를 위해선 IPSec 이외에도 이러한 호스트들을 인증할 수 있는 방안이 필요하다. 본 논문에서 논의한 IPSec과 PKI의 결합은 이러한 문제들을 해결할 수 있는 가장 좋은 방안으로 보여지며, 앞으로 실제 구현과 도입을 통해 대학 전산망의 보안성을 높일 계획이다.

현재, 각 운영체제의 작업 결과를 도입하여 대학망에서 망 계층의 보안 서비스를 제공하는 작업을 진행 중인데, 가장 큰 걸림돌은 대학망을 구성하는 대부분의 호스트들이 MS/Windows를 기반으로 하고 있고, 이 운영체제가 IPv6 또는 IPSec에 대한 지원이 상대적으로 빈약하다는 점이다. 따라서 우선은 SSL과 같은, 응용 계층에서의 보안 서비스를 이용하고, 단계적으로 가능한 서버 시스템부터 망 계층 보안 서비스를 도입하는 방향으로 진행할 예정이다.

참고문헌

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

[2] A. Krywaniuk, "Security Properties of the IPSec Protocol Suite", draft-ietf-ipsec-properties-02, June 2002

[3] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, Nov. 1998

[4] S. Kent, R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, Nov. 1998

[5] D. Harkins, D. Carrel, "The Internet Key Exchange", RFC 2409, Nov. 1998

[6] D. Harkins, C. Kaufman, S. Kent, T. Kivinen, R. Perlman, "Proposal for the IKEv2 Protocol", draft-ietf-ipsec-ikev2-02, April 2002

[7] W. Aiello, S.M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A.D. Keromytis, O. Reingold, "Just Fast Keying", draft-ietf-ipsec-jfk-04, April 2002

[8] http://www.ietf.org/html.charters/pkix-charter.html

[9] A. nash, W. Duane, C. Joseph, D. Brink, "PKI Implementing and Managing E-Security", McGraw-Hill, 2001

[10] http://www.freeswan.org

[11] http://www.strongsec.com/freeswan

[12] http://www.sun.com/solaris

[13]http://www.microsoft.com/windows2000/techinfo/planning/security/ipsec.asp

[14]http://www.microsoft.com/windowsxp/pro/techinfo/administration/ipv6/default.asp

[15] http://www.software.hp.com

[16] http://www.bieringer.de/linux/IPv6

[17] http://www.tahi.org/inop/inop.html

[18] http://www.kame.net/

[19] http://www.openldap.org