특 집

인터넷 보안 기술

인 소 란
(주)니츠

I. 개 요

다양한 정보통신서비스 분야의 급격한 발달로 인해, 모든 일상 생활에서 원하는 정보들을 시간적, 공간적 구애 받지 않고 연결시켜주는 인터넷의 국내 이용자의 수는 연평균 약 51%씩 증가하여 2002년 1,900만 명에 달할 것으로 예상되고 있다. 네트워크의 변화와 사용자 수의 급증, 다양한 정보통신서비스 환경에서 기본 프로토콜로 사용되던 인터넷 프로토콜(IP)는 사용자의 양적인 증가 속도에 따른 요구를 IP 프로토콜내의 주소 공간이 역부족하고, 경로 설정의 어려움, 보안 기능의 부족, 다양한 멀티미디어 서비스 제공상의 용량 부족, 대역폭의 제한 등의 약점으로 인해 위험수위를 넘어서고 있다. IETF에서는 앞에서 언급한 문제점들을 해결할 수 있는 차세대 인터넷 프로토콜인 IPv6를 제안하였고, 아직 국내는 IPv6가 도입 단계이나 일본, 캐나다 등에서는 이미 선도 시험망을 구축하여, 기반으로 정보통신 제품들을 연구개발하고 있다.

최근 인터넷이 폭발적인 증가로 해킹/크래킹 문제를 해결하기 위한 보안 대책의 중요성이 부각되고 있고, 서비스를 제공하는 자와 받는 자의 측면에서 보안요구가 가장 하위의 IP에 요구되고 있다. 인터넷상에서 기본 프로토콜인 IP에서 보안 서비스를 제공할 수 있도록 IETF에서 IPsec 표준과 이에 관련된 다른 표준들을 제안하였다. 이들 표준은 크게 인증 프로토콜, 암호화 프로토콜, 보안설정에 관련된 프로토콜, 보안 설정과 보안정책 관리에 관련된 데이터베이스, 암호및 인증용 암호 알고리즘 등으로 구성되어 있다. 〈표 1〉에서 보듯이 통신망 장비 개발업체에서 이와 유사하게 PPTP, L2TP 등 통신 프로토콜들을

〈표 1〉 IPsec, PPTP, L2TP 비교

비교항목		IPsec	PPTP	L2TP
구조		Host-to-Host	Client-server	Client-server
OSI Layer		Layer 3	Layer 2	Layer 2
지원 프로토콜		IP	IP, IPX, Appletalk	IP, IPX, Appletalk
사용자 인증	사용자 인증	없음(PAP, CHAP, Kerberos, Token ID 등)		
	패킷 인증	AH Header	표준에 포함안됨, 제공안함	IPsec 참조안함
	패킷 암호화	ESP Header	벤더의존적 구현	IPsec 참조안함
	키 관리	ISAKMP/Oakley, SKIP	표준에 포함안됨, 제공안함	IPsec 참조안함
	Tunneling 서비스	공중망, multipoint tunneling VPN 동시접속 지원	단순한 end-to-end tunneling, 인터넷 동시접속 지원 못함	단순한 end-to-end tunneling, 인터넷 동시접속 지원 못함

사용하고 있으나, 이들은 보안에 관련된 기능이 전무한 상태이다.[1]

II. IP 보안[2,3,4]

〈그림 1〉은 IETF에서 제안한 IP 레벨에서 보안의 참조 모델을 보여주고 있다.

IP 레벨에서 요구되는 보안 기능은 크게 무결성, 인증, 비밀성, 접근통제 등이 있다. 이들을 지원하기 위해 관련된 요소기술들은 〈그림 2〉에서 보여주고 있다. IETF에서는 이들을 기존의 인터넷 망 프로토콜인 IPv4와 차세대 인터넷 프로토콜인 IPv6에서는 각각 선택적인 기능과 필수적인 기능으로 사용되도록 6가지의 IP 보안 서비스를 제안하였다.

1. IP 보안 서비스[2,3]

IP 레벨에서 제공되는 보안 서비스는 비연결형 무결성(Connectionless Integrity), 부분적인 일련번호 무결성(Partial Sequence Integrity), 데이터 근원 인증(Data Origin Authentication), 비밀성(Confidentiality), 제한적인 트래픽 플로우 비밀성(Limited Traffic Flow Confidentiality), 그리고 접근 통제(Access Control) 등 크게 6가지로 분류된다.

보안 서비스들은 통신하는 호스트들의 쌍이나, 게이트웨이들의 쌍 또는 호스트와 게이트웨이 간에 제공될 수 있다.

a. 비연결형 무결성(Connectionless Integrity)

트래픽을 구성하는 각 IP 데이터그램의 변조를 알 수 있게 하는 서비스로서, 일련의 데이터그램의 순서와는 관계없는 것으로 부분적인 순서 무결성(partial sequence integrity)과는 대조적인 것이다. 데이터그램의 전부분 뿐만 아니라 공유 되어 있는 키의 정보가 같이 영향을 미치는 인증 값이 부가되기 때문에 중간에 제3자가 메시지 값을 변조하게 되면 키를 알지 못하는 경우 제대로 된 인증 값이나 암호화 된 메시지를 생성하기 어렵게 된다.

b. 부분적인 일련번호 무결성(Partial Sequence Integrity)

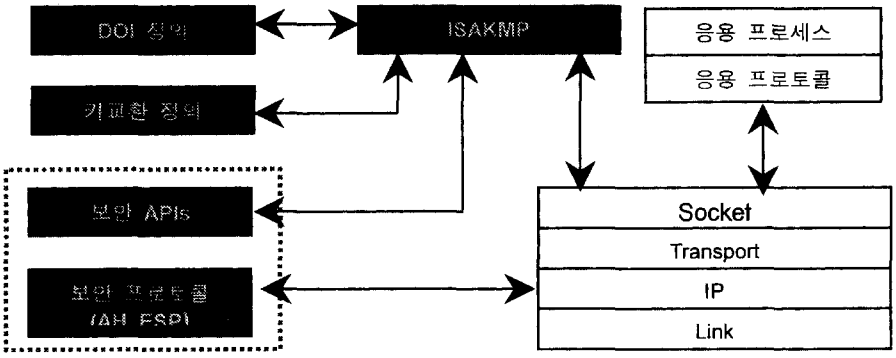
IP 트래픽의 순서를 조사함으로써 재연공격(replay-attack)을 방지하는 데에 사용될 수 있다. 각 AH나 ESP 헤더에는 그 데이터그램만의 일련 번호가 들어가 있다. 이 일련번호를 체크함으로써 데이터그램의 재전송여부를 알아낼 수 있다. 송신자 측에서는 SA가 초기화 되면 이 일련 번호를 계속적으로 증가 시켜가면서 데이터그램을 보내게 된다. 일련번호도 포함해서 그 데이터그램의 모든 부분이 다 인증 값에 영향을 미치게 때문에 어느 한 부분이라도 변조한 경우 키를 모르고서는 변조 사실을 숨기기가 어렵게 된다.

c. 데이터 근원 인증(Data Origin Authentication)

데이터를 보낸 자가 누구인지 알 수 있게 하는 보안 서비스이다. 송신자 A가 있고 수신자 B가 있는데 중간에 C라는 공격자가 들어와서 자기가 A인 것처럼 속이려 하더라도 그 데이터가 어디에서 왔는지를 알 수 있게 된다. 통신하고자 하는 당사자끼리 공유한 키를 다른 제3자가 알지 못한다는 전제가 있기 때문에 지금 받은 데이터의 인증 값을 제대로 생성한 사람은 바로 사전에 나와 키를 공유한 사람이라는 것을 알 수가 있는 것이다. 메시지의 근원을 확인할 수가 있다.

d. 비밀성(Confidentiality)

비밀성은 네트워크를 통과하는 트래픽의 내용을 제3자가 보더라도 알 수 없게 만들어 주는 서비스이다. 사전에 공유한 키를 사용하여 데이터그램을 암호화함으로써 가능하다. IPsec에서는 속도적인 문제가 매우 중요하기 때문에 암호화를 하기 위해서는 대칭키 암호시스템을 사용한다. 대칭키 암호시스템



〈그림 1〉 인터넷 보안의 참조 모델

에서는 정보를 주고 받고자 하는 양자간에 똑같은 키를 공유하고 있어야 할 필요가 있다. 키의 안전한 관리 메커니즘으로 ISAKMP와 같은 키 관리 프로토콜을 사용한다.

e. 제한적인 트래픽 플로우 비밀성(Limited Traffic Flow Confidentiality)

호스트간의 트래픽의 흐름을 숨길 수 있는 서비스이다. 게이트웨이에서 터널 모드의 IPsec을 이용하여 트래픽을 전달해주는 경우에 가능한 서비스로서 구체적으로 어떤 호스트로 가는지에 대한 정보가 은닉되게 된다. 트랜스포트 모드의 IPsec인 경우에는 호스트와 호스트간의 모든 트래픽의 흐름이 노출되게 되므로 이 서비스가 제공되지 않는다.

f. 접근 통제(Access Control)

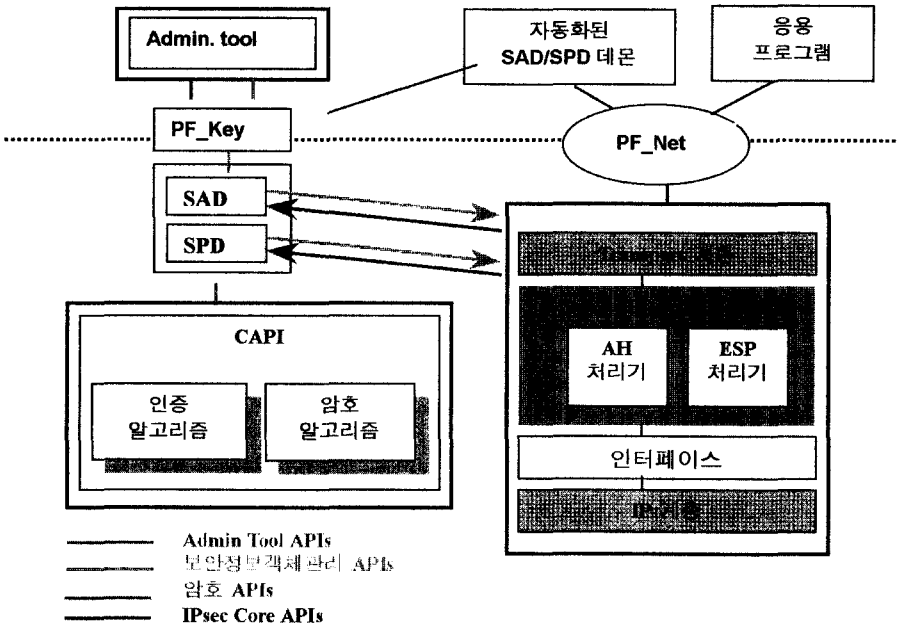
사전 공유 정보를 알지 못하는 사용자의 접근을 제어할 수 있는 서비스로서, IPsec을 사용하는 경우 안전한 통신을 하기 위해서는 노드간의 사전에 협상되고, 이때 설정되는 여러 정보들과 여러 조건들이 적합해야 상대방의 트래픽이 받아들여지게 된다. VPN같은 경우 멀리 있는 사내 사용자의 접근을 위해서 IPsec을 이용할 수 있다. 이런 경우 적법하지 않은 사용자는 미리 설정된 정보, 특히 키에 대한 정보를 알지 못하므로 VPN으로 들어갈 수가 없게 된다.

2. IPsec[1]

IPsec은 네트워크 계층에 보안 서비스를 제공해주는 메커니즘을 말한다. IPsec은 암호화와 인증이라는 강력한 암호학적 보안 서비스를 IP 패킷단위로 제공해 주고, 강력하고 새로운 암호 기술에 기반하고 있으며 현재 상용되고 있는 인터넷 프로토콜 표준인 IPv4 표준과 차세대 인터넷 프로토콜로 사용될 IPv6에 모두 보안 서비스를 제공할 수 있도록 설계되었다. IP 보안 서비스들은 IP 계층(IP layer)에서 제공되기 때문에 IP 계층 뿐만 아니라 IP 계층부터 그 위의 응용 계층까지의 보안 서비스를 제공한다. 따라서 어떤 사용자가 자신이 일상적으로 IP를 사용하고 있는 곳에서 IPsec 프로토콜을 사용한다면 그 사용자는 자신이 사용하고 있는 네트워크의 모든 응용들에 대한 보안 서비스를 제공 받게 되는 것이다.

1) 주요 기능

IPsec은 시스템이 요청하는 보안 프로토콜을 선택하고, 서비스에 사용하기 위한 알고리즘을 결정하고, 요청되는 서비스를 제공하기 위해 요구되는 암호학적 키(cryptographic key)들을 사용하여 IP 계층에서의 보안 서비스를 제공한다. IPsec은 서비스를 받을 양측의 호스트들 간이나 양측의 보안 게이트웨이들 간, 또는 호스트와 보안 게이트웨이 간에 1개 또는 그 이상의 경로(path)들을 보호하기 위해서 사용될 수 있고, 이들간의 트래픽에 대한 보안을 제공하기 위해서



〈그림 2〉 인터넷 보안 기술 요소기술 구성도

AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 2가지 프로토콜들을 사용한다. IPv4와 IPv6에서 원하는 보안 서비스들을 제공하기 위해서 이들 보안 프로토콜들은 서비스의 용도에 따라서 하나씩 사용될 수도 있고 조합으로 사용될 수 있다. AH와 ESP 프로토콜들은 두 가지의 모드로 사용될 수 있다. 하나는 트랜스포트 모드(transport mode)로서 상위 계층 프로토콜들에 대한 보호를 제공하고, 다른 하나는 터널 모드(tunnel mode)로서 터널화 된 IP 패킷(tunneled IP packet)들에 적용되는 프로토콜이다.

2) 구현 방법

호스트 내에 또는 보안 게이트웨이(라우터와 침입 차단 시스템(방화벽)이 결합된 것) 내에 IPsec이 구현될 수 있는 방법은 다음과 같이 몇 가지 방법이 있다.

a. 원래의 IP 구현 내에 IPsec을 결합시키는 것:

IP 소스 코드에 접근하는 것이 필요하다. 호스트나 보안 게이트웨이에 적용 가능하다.

b. "Bump-in-the-Stack"(BITS) 구현

IPsec이 원래의 IP와 지역적인 네트워크 드라이버(local network driver)들 사이에 존재하는 IP 프로토콜 스택 구현의 하부에 구현되는 것이다. IP 스택에 대한 소스 코드 접근은 이 경우에서는 필요하지 않다. 이 접근 방법은 호스트 내에서 일반적으로 사용된다.

c. "Bump-in-the-Wire"(BITW) 구현

Outbound crypto processor의 사용은 몇몇의 상업적인 시스템이나 군에서 사용되는 네트워크 보안 시스템의 공통적인 설계 특징이다. 그러한 구현들은 호스트나 게이트웨이를 지원하기 위해 설계 될 수 있다. 일반적으로 BITW 디바이스는 IP 주소 부여가 가능하다. 단일 호스트를 지원할 때에는 BITS 구현과 매우 유사할 수가 있다. 그러나 라우터나 침입 차단 시스템을 지원할 때에는 보안 게이트웨이와 같이 동작해야만 한다.

Ⅲ. IPsec에서 사용되는 2가지 보안 프로토콜

IP레벨에서 제공되는 6가지의 보안 서비스를 제공하기 위해 사용되는 프로토콜은 인증용 AH (Authentication Header)와 암호화용 프로토콜인 ESP(Encryption Security Payload)가 있다.

1. AH 프로토콜[5]

〈그림 3〉에서 보듯이 IP Authentication Header(AH)는 비연결형 무결성과 IP Datagram들을 위한 데이터 근원 인증(data origin authentication)을 제공하기 위해 사용되며 재연 공격에 대해 보호를 하기 위해 사용된다. 선택 가능한 옵션으로서 제공되는 재연 공격 방지 서비스는 SA가 설정 될 때 수신측에 의해 선택될 수 있고, 상위 계층 데이터 뿐만 아니라 IP 헤더의 가능한 모든 영역에 대해서 인증을 제공한다. AH는 단독으로 사용될 수도 있고, IP ESP (Encapsulation Security Payload)와 결합되어 사용될 수도 있으며, 또는 터널 모드의 사용을 통해서 조합된 형태로서 사용될 수도 있다

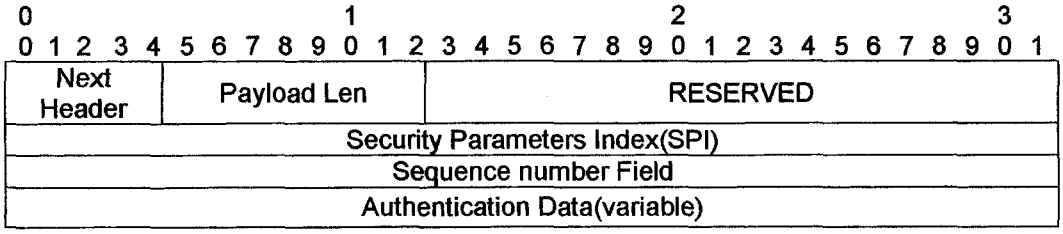
AH 헤더로 인해 IPsec 사용자는 데이터의 근원지에 대한 신원(Identity)과 데이터가 전송 도중에 변조되지 않았음을 확신할 수 있고, 서비스 거부 공격(denial of service attack) 방지를 위해서 수신자의 판단에 의한 재연공격 방지 서비스(partial sequence integrity에 의한)를 제공한다. AH는 비밀성이 요구되지 않을 경우에 사용하기 적당한 프로토콜이다.

2. ESP 프로토콜[6]

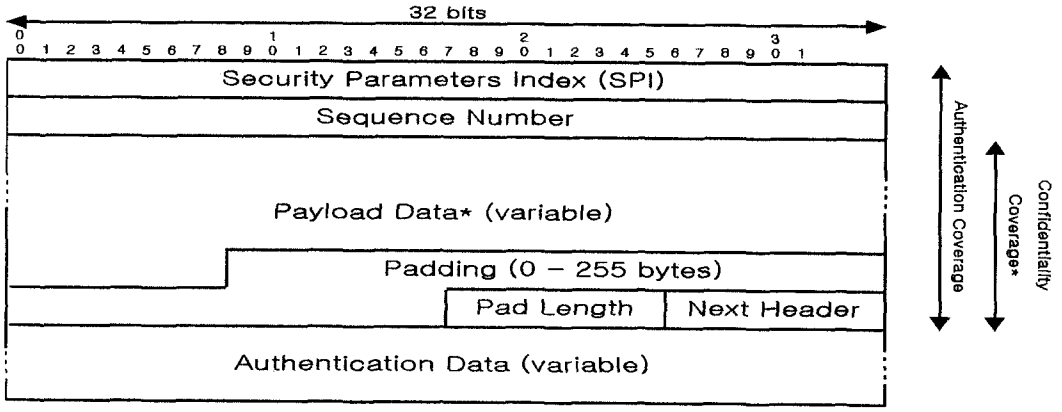
Encapsulating Security Payload(ESP) 헤더는 IPv4와 IPv6에서 여러 가지 보안 서비스를 한다. ESP는 단일하게 적용될 수도 있고, IP Authentication Header(AH)와 함께 쓰일 수도 있으며, 조합된 형태로 사용될 수도 있다. 예를 들어서, 터널 모드의 사용 시에 조합된 형태가 사용 될 수 있다. ESP는 AH에서 제공하는 보안 서비스들 뿐만 아니라 비밀성(암호화) 서비스를 제공한다. ESP와 AH가 제공하는 서비스들 간의 가장 중요한 차이점은 적용 범위에 있다. 터널 모드 ESP에 의해서 캡슐화 되는 경우가 아니라면, ESP는 어떠한 IP 헤더 필드들도 보호하지 못한다.

ESP는 비밀성(confidentiality), 데이터 근원 인증(data origin authentication), 비연결형 무결성(connectionless integrity), 재연 공격 방지 서비스(anti-replay service(부분적인 순서적 무결성(partial sequence integrity))), 그리고 제한적인 트래픽 플로우 비밀성(limited traffic flow confidentiality)을 제공한다. 제공되는 서비스 집합은 구현의 배치와 SA의 설정 시에 결정되는 옵션들과 관련이 있다.

〈그림 4〉에서 보듯이 ESP 헤더의 바로 앞에 오는 프로토콜 헤더(IPv4, IPv6, 또는 확장헤더)는 그 프로토콜 필드(Protocol field)(IPv4의 경우) 내에, 또는 Next Header 필드(IPv6, Extension의 경우)에 값 50을 포함하고 있어야 한다.



〈그림 3〉 AH Packet Format



〈그림 4〉 ESP Packet Format

Ⅳ. SA/SP

IP 보안 서비스를 제공하기 위한 core engine인 IPsec 엔진이 동작되기 위해서 보안 설정을 하고, 이에 대한 보안 관리를 담당하는 기능이 SA와 SP이다. 이들 SA와 SP가 IP 보안 서비스 제공하기 위해 IPsec Engine과 함께 수행하는 역할과 특성들을 살펴보면 다음과 같다.

1. SA(Security Association)

AH, ESP를 구현하는 IPv6와 IPv4의 모든 구현에 대한 SA 관리(security association management)가 있다. SA는 IPsec에서 기본이 되는 개념이다. AH와 ESP 모두가 SA를 사용하고 IKE의 가장 중요한 기능이 바로 SA의 설정과 관리이다.

SA는 트래픽에 보안 서비스를 제공하는 simplex "connection"이다. 보안 서비스는 AH나 ESP의 사용에 의해 SA에 제공될 수 있다. 전형적인 두 호스트들 간이나 두 보안 게이트웨이들 사이의 양방향 통신을 안전하게 하기 위해서는 2개의 SA들이 필요하다. 각 SA는 3가지의 구성요소인 SPI(Security Parameter Index), IP 목적지 주소(Destination Address), 그리고 보안 프로토콜(Security Protocol, AH나 ESP 등) 식별자(identifier)에 의해서 단일하게 식별된다. 원칙적으로 목적지 주소는 unicast 주소가 될 수도 있고 IP broadcast 주소나 multicast 그룹 주소(multicast group address)가 될 수도 있다.

SA에는 2가지 타입이 있다. 하나는 트랜스포트 모드이고 다른 하나는 터널 모드이다. 트랜스포트는 두 호스트들 간에 SA가 설정될 때 사용되는 모드이다. IPv4에서는 트랜스포트 모드에서의 보안 프로토콜 헤더가 IP 헤더와 다른 모든 옵션들의 바로 뒤에 위치하며, 다른 어떤 상위 프로토콜들보다 앞에 위치하게 된다. 터널 모드 SA는 본질적으로 IP 터널에 적용되는 SA이다. 이 경우, IPv4와 IPv6에 따라서 보안 프로토콜 헤더가 놓이는 위치가 다르다. 그리고 터널 모드는 IP 터널에 적용되는 SA이다. 양단의 어느 하나가 보안 게이트웨이라면 SA는 반드시 터널 모드여야 한다. 따라서 양쪽이 모두 보안 게이트웨이인 경우는 언제나 터널 모드SA가 되고 한쪽은 호스트이고 다른 한쪽은 보안 게이트웨이인 경우 역시 터널 모드SA가 된다.

2. SP[10]

SA는 IPsec 환경에서 보안 정책을 집행하기 위해서 사용되는 관리 구조이다. 따라서 SA 처리의 근본적인 요소는 IP 데이터그램 들에 어떤 서비스들이 제공되어야 하고 어떠한 방식으로 이루어져야 하는지를 명기하는 하부에 깔려있는

SPD가 된다.

SPD는 IPsec이 아닌 트래픽을 포함해서 모든 inbound와 outbound 트래픽에 대해서 참조되어야 하고, 이을 지원하기 위해서 SPD는 inbound 트래픽과 outbound 트래픽에 대해서 별개의 요소를 가지고 있어야 한다. 이것을 분리된 SPD들(inbound와 outbound)로 생각할 수 있다. 또한 별도의 명칭을 가진 SPD가 각 IPsec이 지원되는 인터페이스에 대하여 제공되어야 한다.

SPD는 IPsec에 의해서 보호가 제공되는 트래픽과 IPsec을 우회할 수 있도록 허용된 트래픽들을 구별할 수 있어야만 한다. 이것은 송신자에 의해서 적용되어야 하는 IPsec 보호와 수신자쪽에서 제공해야 하는 IPsec 보호에 적용되게 된다. 어떤 outbound나 inbound 데이터그램 대해서도 세 가지 처리 선택이 가능하다. 그것들은 "Discard", "Bypass IPsec", 그리고 "Apply IPsec"의 세 가지 이다. 이 중 첫 번째 선택인 Discard는 호스트를 빠져나가 보안 게이트웨이를 거치고, 응용에게로 전달되는 것들이 허용되지 않은 트래픽을 말한다. 두 번째 선택인 Bypass IPsec은 부가적인 IPsec 보호 없이 통과될 수 있도록 허용된 트래픽을 말한다. 세 번째 선택인 Apply IPsec은 IPsec 보호가 제공되는 트래픽을 말한다. 이러한 트래픽 대해서 SPD는 제공될 보안 서비스, 적용될 프로토콜들, 그리고 사용될 알고리즘 등에 대해서 명시를 해주어야 한다.

V. ISAKMP[7]

ISAKMP(Internet Security Association & Key Management Protocol)은 SA(Security Association)의 관리(설정, 협상, 변경 및 삭제)와 키 관리를 정의하는 프레임워크(framework)이다. <그림 1 참조>

IPsec에서 보안과 인증 서비스를 제공하기 위해서는 안전한 통신(secure communication)을 하기 원하는 양단 간에 사용될 암호 알고리즘, 키 등에 대한 합의가 있어야 한다. 양단 간의 트래픽에 보안 서비스를 제공하기 위하여 맺는 connection을 RFC2401 문서에서는 SA라고 정의하고 있다.

키는 우리가 일상적으로 사용하는 비밀번호와 같은 역할을 하므로 키의 교환에는 고도의 보안이 요구되기 때문이다. IPsec에서는 키 교환을 위해서 2가지 방법을 필수 사항으로 구현할 것을 요구하고 있는 데 하나는 수동 키 교환(manual key exchange)과 다른 하나는 자동 키 교환(automated key exchange)이다. 수동 키 교환은 SA를 설정하는 데 필요한 키 또는 그 밖의 사항들을 물리적인 방법(전화, 직접 전달)에 의해 양단이 합의하는 것이고 자동 키 교환이란 정의된 키 교환 프로토콜을 사용하여 SA를 설정하는 것이다. 현재는 수동 키 관리 기반의 메커니즘이 널리 사용되고 있으나 나날이 커지고 복잡해지는 네트워크의 보안 수요를 감당하기에는 어려울 것으로 보인다. 따라서 좀 더 효율적이고 체계적인 자동 키 관리 프로토콜이 요구되는데 IETF는 이 SA의 관리(설정, 협상, 변경, 삭제)와 키 교환을 정의하는 프레임워크인 ISAKMP를 제안하였다. ISAKMP에는 SA의 설정, 협상, 변경, 삭제를 위한 과정과 패킷 포맷, 그리고 키 생성과 인증된 데이터의 교환을 위한 페이로드(Payload)가 정의되어 있다.

ISAKMP를 SA의 관리에 사용함으로써 얻는 이점은 첫째, 시스템에 보안을 제공하기 위한 기능을 분리함으로써 보안 요구 사항이 다른 시스템들 간에 상호 운용성을 제공하고, 둘째, 보안 요구사항이 다른 망의 모든 사용자들 공통의 속성 집합을 정의함으로써 인증 및 암호화된 방식으로 상대방과 통신할 수 있도록 하는 토대를 마련하며, 셋째, 각 보안 프로토콜마다 중복되는 SA관리를 집중화 함으로써, 전체 네트워크 프로토콜 스택에 대한 보안 서비스를 한번에 협상하여 연결 설정 시간을 줄일 수 있고, 넷째, 특정 보안 기법과 알고리즘에 대한 독립성을 제공함으로써 더 나은 보안 기법과 알고리즘으로의 변형이 언제나 용이하다.

ISAKMP에는 키 교환의 메커니즘 자체에 대한 언급이 없고, IETF가 권고하는 키 교환 메커니즘인 OAKLEY에 정의되어 있다. OAKLEY의 키 교환 프로토콜은 Diffie-Hellman의 프로토콜에 기반을 두고 있으며, 이 Diffie-Hellman 프로토콜에 네트워크 상에서 가능한 공격들을 방지하기 위한 메커니즘을 첨가하여 설계한 일반적인 키 교환 프로토콜이다. IETF는 OAKLEY와 ISAKMP를 결합하여 IPsec에서의 키 교환과 SA협상을 위한 프로토콜인 IKE (Internet Key Exchange)프로토콜을 제안하고 있다.

VI. IKE[8,9]

IKE는 IETF IPsec DOI를 위한 AH나 ESP와 같은 다른 SA(Security Association)들이나 ISAKMP에서 사용하기 위한 인증된 keying material을 얻기 위하여 ISAKMP와 연계하여 Oakley의 일부와 SKEME의 일부를 이용하는 합성 프로토콜인 인터넷 키 교환 프로토콜(Internet Key Exchange, IKE)이다.

IKE를 구현한 프로세스는 가상 사설망을 협상하는데 사용될 수 있고, IP 주소가 이전에 알려지지 않았던 원격 사이트에 있는 원격 사용자에게 안전한 호스트나 네트워크에 대한 접속을 제공할 때에 사용될 수 있다.

ISAKMP는 인증과 키 교환을 위한 골격을 제시하지만 정의하지는 않는다. ISAKMP는 키 교환과 독립적으로 설계되었다. Oakley에서는 "Modes"라 불리는 일련의 키 교환들에 대해서 서술하고 각각이 제공하는 서비스들인 키에 대한 perfect forward secrecy(PFS), 신원 보장(identity protection), 그리고 인증(authentication)가 있다.

Security Key Exchange MEchanism (SKEME)에서는 익명성(anonymity)과 부인성(repudiability), 그리고 빠른 키 refreshment를 제공하는 용도가 다양한 키 교환을 다루고 있다.

IKE는 Oakley 프로토콜 전체를 구현하는 것이 아니고 오직 인터넷 키 교환 프로토콜의 목적에 만족시키는데 필요한 부분만을 구현하므로, Oakley 프로토콜 전체와 일치되어야 하거나 그대로 따라야 할 필요가 없으며, 또한 Oakley 프로토콜과는 독립적이다.

VII. 결 언

본 고에서는 인터넷 보안기술 중에서 가장 하부 계층인 IP 레벨에서의 보안에 대하여 기술하였다. 국내에서도 인터넷 정보가전, 홈 게이트웨이, PDA 등 IP를 기반으로 정보통신 서비스를 제공하는 망사업자, 가전업체, 단말기 업체에서 인터넷 보안 기술에 대하여 작년부터 많은 활동을 하고 있다. 이 기술은 최근 서버, 네트워크, 클라이언트급 레벨에서 다양한 보안 제품들이 연구개발되어 출시 되고 있다.

본고에서 기술한 인터넷 보안 기술은 네트워크 레벨에서의 보안으로서 인터넷 프로토콜인 IP에서 제공되는 6가지의 보안 서비스, 이를 제공하기 위한 프레임워크, 구성되는 주요 요소 기술들, 이들을 동작시키기 위해서 사용되는 데이터베이스, 키 관리 시스템 등을 중심으로 기술하였다.

그리고 인터넷 환경에서 서비스를 제공하고 받기 위하여 요구되는 각 기관별, 서버별, 네트워크별, 서비스별 보안정책을 표준화하는 보안정책시스템에 대한 연구가 이미 IETF에서 활동 중에 있고, IP 버전간의 연동기술, 그리고 인터넷 보안기술의 핵심인 인터넷 프로토콜의 보안을 통해 가장 많이 활용되는 가상 사설망(VPN, Virtual Private Network)에 대한 연구 개발과 구축이 이루워 지고 있다.

다양한 VPN 제품들을 광역망이나 대규모의 망에서 사용하고, 외국과의 연동을 위해서는 이

들에 대한 향후 연동시에 발생되는 상호호환성을 고려하여 국제표준규격을 준수하여 제품개발이 이루워져야 한다고 본다.

또한 키관리 시스템도 현재는 수동식(manual)이나 자동화(automatic) 방식으로 할 수 있는 연구와 기술 개발이 조속히 필요하다.

참 고 문 헌

〔1〕 (주)니츠, "인터넷보안기술", 동서출판사, 2000

〔2〕 (주)니츠, "IPv6 보안 소켓 개발", 정보통신부 선도기반기술개발사업, 2000

〔3〕 Sidnie Fiet, "TCP/IP : Architecture, Protocols, and Implementation With IPv6 and IP Security", Dec 1998

〔4〕 S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol (IPsec)", RFC 2401, Nov 1998.

〔5〕 S. Kent, R. Atkinson, "IP Authentication Header(AH)", RFC 2402, Nov 1998

〔6〕 S. Kent, R. Atkinson, "IP Encapsulation Security Payload(ESP)", RFC 2406, , Nov 1998.

〔7〕 D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol(ISAKMP)", RFC 2408, Nov 1998.

〔8〕 D. Harkins, D. Carrel, "The Internet Key Exchange(IKE)" RFC 2409, Nov 1998.

〔9〕 H. Orman, "The OAKLEY Key Determination Protocol", RFC 2412, Nov 1998.

〔10〕 L. A. Sanchez and M. N. Condell, "Security Policy Protocol", Internet Draft, draft-ietf-ipsec-spp-00, 1999. 7.

저 자 소 개

印 素 蘭

1954년 12월 6일생, 1978년 2월 홍익대학교 전산과 학사, 1982년 8월 홍익대학교 전산과 석사, 1991년 8월 홍익대학교 전산과 박사, 1987년 8월 정보처리기술사(전자계산기 조직응용분야) 취득, 1978년 1월~1998년 6월 : 한국전자통신연구원/책임연구원/실장, 1998년 7월~2000년 3월 : (주)니츠 연구소장, 2000년 3월~현재 : (주)니츠 부사장, 2000년 7월~현재 : (주)에이전트엑스퍼트 대표이사, 〈주관심 분야 : 프로토콜 공학, 정보보호, 소프트웨어 공학〉