主題

인터넷 정보보호 IPsec 기술

한국전자통신연구원 이종태, 손승원

차 례

요 약

인터넷에서의 정보보호는 IPsec으로 대표된다. IPsec은 인터넷에서 필수적인 암호와 인증 서비스를 구조적으로 제공하면서 안전한 키교환이나 replay 공격등을 방어할 수 있는 메카니즘도 제공하고 있다. IETF IPsec과 IPsp워킹그룹에서는 패킷 기반의 비연결형 정보보호 서비스를 제공하기 위하여 두 개의 확장 헤더를 정의하였고, 헤더 처리를 위한 키교환 및 인증 프로토콜, 정보보호 정책기술, 그리고 정보보호 서비스 관리를 위한 MIB들을 정의하였다. IPsec은 다양한 플랫폼에서 구현되고 있어, 조만간 기존의 특정 어플리케이션 위주의 정보보호 기술들을 대체시킬 것으로 보인다. 이 논문에서는 인터넷 정보보호 서비스제공을 위한 프레임워크를 설정하고 각 주요 구성 요소에 대해 기술한다.

Ⅰ. 서 론

최근 인터넷 활용의 급속한 증가로 정보보호에 대한 필요성이 절실하게 인식된 반면, 컴퓨터에 대한 크래킹 및 바이러스등에 의한 피해 사례도 끊임없이 보도되고 있다. 1994년 IETF IAB에서는 이미 인터넷의 당면한 가장 중요한 과제 중의 하나가 "보안 문제"라는데 합의하였고 IPsec WG는 1993년 6월부터 작업을 시작하여 현재 IPsec 아키텍쳐를 기술한 RFC2401을 비롯한 18개의 RFC를 작성하였다. IETF Security Area에서 IPsec WG는 인터넷 정보보호에 관한 기본 구조를 연구하고 있는 그룹으로서, AH(Authentication Header)와 ESP(Encapsulation Security Payload)의 두가지 확장헤더와 IKE(Internet Key Exchange)를 정의하였다. 현재 AH, ESP와 IKE는 대부분의 플랫폼에서 프로토타입으로 구현되었고 WINDOWS 2000에서도 구현되었으나 아직 완전하다고는 볼 수 없다.

IPsec의 특징은 다음 몇 가지로 요약될 수 있다. 정보보호 서비스가 IP 계층에서 제공됨으로서 기존의 응용 소프트웨어에 대한 변경을 요하지 않아, 일반 인터넷 사용자에게는 투명한 상태로 처리된다. 응용계층 및 트랜스포트 계층의 모든 프로토콜에 공통된 정보보호 서비스를 제공할 수 있기 때문에, 한 호스트 내에서는 일관된 방식의 정보보호 서비스 설정이 가능하다. 또한 특정 알고리즘이나 인증 방식에 국한시키지 않으면서 새로운 정보보호 기술 수용이 용이한 프레임워크를 갖고 있어 국내 암호 기술 적용도 쉽게 이루어질 수 있다.

현재 IPsec이 가장 활발하게 적용되고 있는 VPN(Virtual Private Network) 산업분야에서는, IPsec을 엔터프라이즈 네트워크에 적용시 확장성 및 호환성을 해결할 수 있는 유일한 정보보호 프로토콜로 여기고 있다. 이 논문에서는 현재 인터넷이 갖고 있는 취약점 분석과 이러한 취약 요소를 극복하기 위한 인터넷 정보보호 프레임워크를 기술하고 각 주요 기능 컴포넌트에 대해 설명한다.

Ⅱ. 인터넷 취약요소

인터넷은 그 효용성에도 불구하고 정보보호 관점에서 볼 때, 근본적으로 여러 가지 문제점을 안고 있다. 최근에 자주 등장하는 분산 서비스 거부공격같은 경우도 인터넷이 갖고 있는 문제점이 드러난 한 예에 불과하다.[1] 문제점을 분석하기 전에 먼저 인터넷을 구성하고 있는 요소를 살펴보면 이는 근본적으로 호스트라고 할 수 있다. 그리고 이 호스트는 하드웨어와 소프트웨어로 이루어져 있고 호스트간의 네트워킹을 위한 링크가 존재한다. 하드웨어 부분은 전자파 방출에 따른 tempest와 같은 문제점외에는 거의 문제시 되지 않고 대부분의 인터넷 취약점은 바로 소프트웨어와 링크상에 잠재되어 있으며 표.1은 취약점을 공격하는 대표적인 크래킹기법들을 보여주고 있다.

먼저 링크상의 문제점을 살펴보면, LAN 환경에서는 shared media 방식이기 때문에 누구나 패킷 절취가 가능하게 되어 있다. 비인가자라 할지라도 PC를 LAN에 접속시키기만 하면 무작위로 전송되는 패킷 데이타를 일목요연하게 읽어낼 수가 있다. 또한 패킷 데이터의 내용을 위·변조시켜 재전송(replay)할 수도 있다. 이러한 문제는 LAN 방식을 지양하지 않고는 해결될 수 없으며 현재는 switch hub를 사용하여 라우팅을 적절히 제어하고 있기도 하다.

표 1. 인터넷에서의 주요 크래킹 기법

구 분	크래킹 기법	구 분	크래킹 기법
전자우편	Spam Mail	네트워크 응용서버 공격	namcd 공격
	Email Bomb		Imapd 공격
서비스 거부 공격	Smurf 공격		popd 공격
	ICMP 공격		identd 공격
	Syn Flooding		innd 공격
	Ping 공격	스캐너	post scan
웹서버 공격	Phf Bug 공격		mscan
	Php Bug 공격	ID 도용	
	Test-cgi 공격	백 오리피스	
		크래킹 도구	
스니퍼		바이러스	

그 다음은 소프트웨어 문제점으로서 크게 응용계층 문제점과 TCP/IP를 포함한 커널계층의 문제점으로 분류해 볼 수 있다. 소프트웨어 부분에서 공통적으로 나타나는 문제점은, 예상하지 못한 비정상 상태가 발생하였을 때 적절한 대응을 하도록 하는 코드가 구현되어 있지 않기 때문에 나타나는 경우다. 대부분의 응용 프로그램이 기능 구현에 역점을 두고 있기 때문에 복잡한 sequence flow상에서 나타날 수 있는 모든 비정상 경우를 전부 커버하지 못하고 있다. 그래서 소스 코드가 잘 알려져 있는 리눅스 경우에, 해커들은 그러한 헛점을 종종 이용하게 되어 크랙킹사고가 발생되는 것이다.

응용계층 프로그램은 주로 전송 경로상에서 패킷 절취나 도·감청이 불가능하도록 암호·인증 서비스를 구현하고 있어, 하부 커널계층의 문제점을 보완할 수 없고 SYN flooding 공격에 대해서는 무방비일 수 밖에 없다. 응용계층의 정보보호는 각 응용 프로그램이 독립적으로 운용되기 때문에, 사용자측에서 볼 경우 각 프로그램에 대한 보안 파라메터를 설정하여야 하는 불편이 따르게 마련이고 이런 과정에서 개인 비밀 정보 관리가 어려워지며 쉽게 타인에게 노출될 수 있게 된다.

커널계층의 보안은 호스트로의 influx에 대한 접근제어 및 응용계층에서의 호스트 자원 접근에 대한 제어를 달성하고자 하는데 목적이 있다. 커널 자체에 대한 크래킹은 쉽지 않지만 backdoor 문제가 대두될 수 있다. 그러나 buffer overflow와 같은 취약점은 커널계층에서 근본적인 해결을 해야 한다고 보고 있다.

인터넷의 경우 다양한 TCP/IP계층 프로토콜 및 소스 코드는 이미 일반에게 익숙한 상태에 있다. 이에 따라 full mesh 형태의 통신이 가능한 인터넷에서는 그들의 헛점을 이용한 해커들의 다양한 공격방식이 넘쳐나고 있다. TCP/IP 자체가 안고 있는 취약점중 간과할 수 없는 것은 패킷이 destination address만으로 라우팅된 다는 점이다. Origin address를 임의로 변경하여도 패킷은 목적지에 폐기되지 않고 정확히 전달된다. 이러한 IP spoofing에 의해 수신 데이터 내용과 발신지 주소간에 상관 관계가 없게 된다. 또한 중간 노드에서 가로챈 패킷의 내용을 수정한 후 동일 destination으로 재전송하는 경우에도 origin address가 같지만 수신데이타와 발신주소간에는 상관 관계가 없다. 일반 통신 구조에서 더욱 문제시 될 수 있는 것은 IP 주소와 실제 사용자간에 1:1 관계가 성립되지 않는다는 점이다. 따라서 타인의 PC를 사용하여 악의의 메일을 보내도 현재 인터넷에서는 실제 송신자를 확인할 길은 별로 없다.[2, 3]

위에서 지적한 인터넷의 취약점들을 일시에 해결할 수는 없다. 기존의 폐쇄그룹간의 통신만을 지원하는 것은 특정 서비스에 한하여 부합될 수 있지만, 네트워크 전체 혹은 모든 어플리케이션을 보호하면서 유연한 보안관리까지도 고려하게 되면 범용 정보보호기술로서 IPsec을 들 수 밖에 없다. 인터넷 계층별로 볼 때 IP 계층에 표준화된 정보보호 메카니즘을 구현시키는 것이 가장 효율적이고, 장기적으로 볼 때 비용절약 및 개방기술로서 성공할 수가 있다고 본다.

이를 토대로 IETF IPsec WG에서는 IP계층에서 정보보호 서비스 제공을 위한 AH/ESP와 IKE 프로토콜을 표준화시켰으며 다음과 같은 목적을 달성하고자 하였다.

- Access control
- Data Origin Authentication
- Connectionless integrity
- Data confidentiality
- Replay protection
- Limited traffic flow confidentiality

기본적으로 IPsec은 inbound 혹은 outbound packet 단위로 암호 및 인증서비스를 제공하여 상위 계층 보호를 목표로 하고 있다. 전송 링크상에서 발생할 수 있는 위·변조 및 replay 공격을 방지할 수 있으며 제3자에 의한 트래픽 분석 공격에 대응할 수 있도록 되어 있다.

Ⅲ. IETF의 정보보호 활동

IETF의 Security Area에서는 인터넷 정보보호 관련 프로토콜들을 표준화하는 작업을 진행중에 있으며 현재 18개의 WG그룹으로 구성되어 있다. 표 2는 각 WG그룹의 특징을 간략하게 기술하고 있다.

표 2. IETF Security Area 워킹그룹 현황

Working Group	연구 영역
openpgp	기존의 PGP를 표준화함
aft	기존의 SOCKS v5 프로토콜을 표준화함
cat	GSS-API 정의
ipsec	AH/ESP 및 IKE 프로토콜 정의
ipsp	Security policy 구조 및 분배프로토콜 정의
ipsra	원격 접속을 위한 인증 절차 정의
idwg	침입탐지시스템간 정보교환 프로토콜 정의
krb-wg	기존의 Kerberos에서 호환성 문제점 개선
otp	기존의 Bellcore S/KEY를 표준화함
pkix	X.509 기반 PKI 정의
smime	MIME 데이터에 암호/인증 서비스 적용
stime	기존의 NTP에 대한 인증서비스 적용
secsh	기존의 SSH 프로토콜을 표준화함
syslog	기존의 Syslog 메카니즘에 보안성 추가
spki	간단한 인증서 구조 및 운영절차 정의
tls	기존의 SSL v.3을 표준화함
wts	HTTP에 security를 추가한 S-HTTP 정의
xmldsig	XML을 위한 디지털 서명 정의

Security Area의 WG들중 IPsec, IPsp, IPsra, PKIX, IDWG가 인터넷에서 범용으로 적용될 새로운 표준을 정하고 있다고 볼 수 있다. 특히 IPsra는 금년에 시작되었으며 road warrior 혹은 kiosk 환경에서 원격접속을 지원하기 위한 PIC (Pre-IKE Credential)을 제안하고 있다.

그 밖의 WG그룹들은 주로 기존의 de-facto standard를 수용하거나 기존의 인터넷 서비스에 security 기능을 추가하여 발전시키는 형태의 작업을 추진하고 있으며 특정 응용에 국한되어 사용되는 경우가 대부분이다.

Ⅳ. 인터넷 정보보호 프레임워크

이 장에서는 인터넷 정보보호의 프레임워크를 기술하고자 한다. 그림 1은 기본 구조를 보이고 있다.

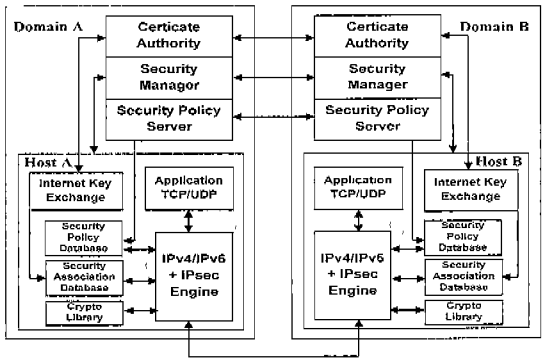

그림 1. 인터넷 정보보호 프레임워크

IPsec은 IPv4에서는 선택 기능이나 IPv6에서는 필수 기능에 속한다. 모든 inbound 혹은 outbound 패킷은 IPsec engine을 거치면서 정보보호 서비스를 받게 되는데 engine은 SPD (Security Policy Database), SAD(Security Association Database), CL(Crypto Library)을 항상 참조하게 되어 있다.[4] 특히 IKE(Internet Key Exchange)는 데이터 암호 및 인증서비스 제공의 전처리 과정으로서 키생성, 키교환과 사용자 인증을 담당하고 있다. SPS (Security Policy Server)는 각 호스트가 갖고 있는 SPD내의 정보보호 서비스 적용 규칙을 정하고, CA(Certificate Authority)는 사용자 인증에 필요한 인증서를 발급하여 IKE에서 상대측 사용자를 인증하도록 한다. SM(Security Manager)은 일련의 정보보호 서비스 제공 과정을 실시간 모니터링하면서 도메인내의 정보보호 서비스 제공 상

표 3. AH/ESP 지원 정보보호 서비스

보안서비스	AH	ESP
Access Control	○	○
Connectionless integrity	○	○
Data Origin Authentication	○	○
Proteection Against Replay	○	○
Confidentiality	×	○
Limited Traffic Flow Confidentiality	×	○

태를 파악할 수 있게 된다. 아래에서 각 구성 요소들에 대해 기술하기로 한다.

1. IPsec Engine

IPsec 엔진은 IPsec WG에서 정한 AH와 ESP 헤더를 처리한다. AH는 IP 패킷 전체에 대한 무결성 및 인증을 위해 필요한 헤더이며 ESP는 payload내의 데이터를 암호화 하는데 사용된다. 두 헤더를 사용하여 패킷 단위로 제공되는 정보보호 서비스는 표.3으로 요약된다.[5]

먼저 AH 헤더 구조는 그림 2에서 보인 것과 같이 각각 32bit의 SPI(Security Parameter Index)와 SN(Sequence Number) 그리고 가변길이의 ICV (Integrity Check Value)로 이루어져 있다. ICV는 패킷 전체에 대해 단방향 해쉬함수(MD5 혹은 SHA-1)를 이용하여 계산한 MAC(Message Authentication Code)값으로서, 키를 알고 있는 사용자만이 해쉬값을 알아낼 수 있고 수신된 패킷이 중간 경로상에 위·변조되었는지를 검사할 수 있게 한다. 그리고 SN은 replay attack을 방지하기 위하여 동일 패킷이 중복되어 수신되었는지 여부와 일정한 time window내에 도착하였는지를 검사하는데 사용된다. 마지막으로 SPI는 destination 주소와 더불어 SN과 ICV에 대한 특정 IPsec 처리 방식을 지시한다. 이러한 정보는 SAD에 저장되어 있다. 이 AH는 extension 헤더로서 사용되는 transport 모드와 outer 헤더로서 IPsec 적용전 전체 패킷을 encapsulaton하는 tunnel 모드 두가지에 적용될 수 있다.

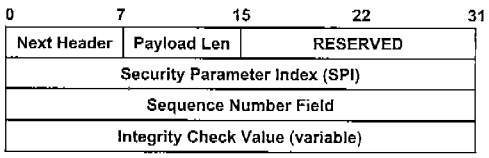

그림 2. AH 헤더 구조

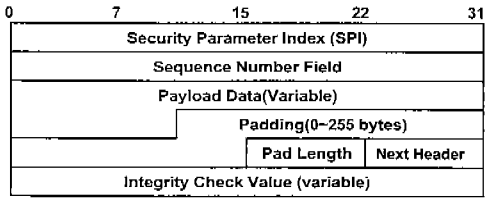

그림 3. ESP 헤더 구조

ESP 헤더 구조는 그림 3과 같고 암호화하기 위한 데이터를 payload 필드에 둔다.[6] SPI와 SN은 AH 헤더에서와 같이 동일하게 사용된다. Payload 데이터부분은, transport 모드에서는 상위계층 데이터가 되고 tunnel 모드에서는 IPsec 적용 전 패킷 전체에 해당된다. 암호 알고리즘으로서는 대칭키 블록알고리즘이 사용되며 일반적으로 padding 부분은 알고리즘이 요구하는 평문 길이를 조정하기 위해 사용된다. 구현에 필요한 필수적인 알고리즘은 DES in CBC mode(RFC1829), Null Encryption (RFC2410)으로서 현재 IETF에서 계속 확장중에 있다. ICV는 ESP 헤더, payload, ESP trailer에 대한 MAC값을 의미한다. ESP를 적용할 경우 암호와 인증이 둘 다 동시에 NULL이 되어서는 안된다.

ESP도 AH와 마찬가지로 transport 모드와 tunnel 모드에 모두 적용될 수 있으며 패킷 데이터

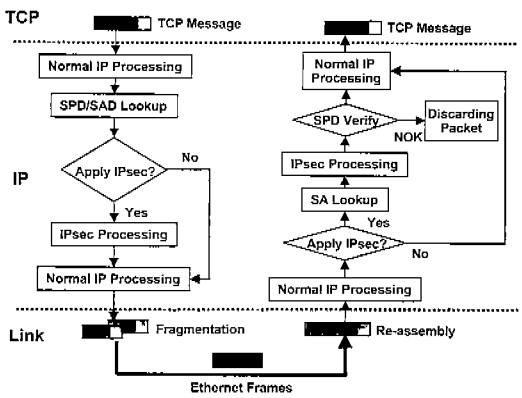

그림 4. IPsec 처리 순서도

가 제3자에게 노출되지 않도록 한다. 반면에 AH 적용시는 패킷내용이 제3자에게 노출될 수 있다. 게이트웨이간 ESP tunnel 모드가 적용될 경우 호스트 주소가 암호화되어 통신 트래픽 분석을 불가능하게 만들 수 있다.

2. SA Databse

패킷에 대한 암호 및 ICV값 계산을 위해 전처리 과정으로서 SA협상이 있다. 이러한 SA협상 과정중에는 해쉬함수나 암호알고리즘, 키값, 키수명등에 대한 협상이 송수신자간에 이루어지게 되며, 그럼으로서 정보보호 측면에서 볼 때 양자간에 SA (scurity association)가 성립되었다고 한다. IP 계층에서는 단방향 패킷 포워딩만이 존재하므로 양방향 connection을 위해서는 송신 SA와 수신 SA 두 개가 있어야 한다. 이 SA들이 SAD에 저장되고 SAD는 다음과 같은 필드를 갖을 수 있다.

- Destination IP Address
- Security Parameter Index(SPI)
- IPsec Protocol
- Name: user ID & system name
- Data Sensitivity Level
- Source IP Address
- Transport Layer Protocol
- Source and Destination Ports
- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- AH authentication algorithm & key
- ESP encryption algorithm & key
- ESP authentication algorithm & key
- Lifetime of SA
- IPsec protocol mode
- Path MTU

SAD는 {Destination IP Address, SPI, IPsec Protocol}에 의해 유일하게 select되며 IPsec engine은 AH나 ESP 프로세싱 과정중 SAD를 참조함으로서 특정 연결에 대해 일정한 방식의 정보보호 서비스를 적용시킬 수 있게 된다. SAD에서는 상위계층의 트랜스포트 계층 프로토콜이나 포트까지 지정할 수 있어 SA의 granularity를 조절할 수 있도록 하고 있다.

3. IKE

IKE는 자동화된 SA협상을 위해 ISAKMP, Oakley, SKEME의 세가지 프로토콜로부터 만들어 졌다. ISAKMP는 인증 및 키교환을 위한 프레임워크로서 phase I과 phase II 단계를 제공하고, Oakley는 키 교환 모드를 정의하며 SKEME는 키 공유 및 rekeying 기법을 제공한다. IKE는 서비스 거부 공격 및 man-in-the-middle attack을 방지하며 Perfect Forward Secrecy(PFS)를 제공하도록 설계되었다. IKE는 응용계층에 속하고 UDP port 500번을 사용한다.[7]

IP계층에서는 AH/ESP 처리 전에 SAD내에 원하는 SA가 없을 경우 IKE를 호출할 수 있도록 되어 있다. 따라서 IKE 기능은 응용 및 트랜트포트 계층과 무관하여 사용자에게는 투명하게 동작된다.

IKE는 그림.5에서와 같이 phase I 과 phase II를 거쳐 SA협상 및 생성을 한다. Phase I은

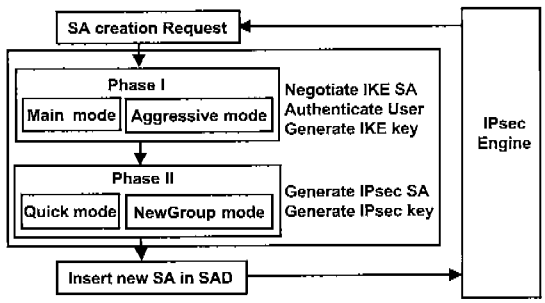

그림 5. IKE 처리 절차도

phase II 협상 트래픽을 보호하기 위한 IKE SA 협상과 사용자 인증 절차를 수행하며, Phase II에서는 Phase I에서 생성된 IKE SA로 보호받으면서 IPsec SA를 생성한다. 이러한 협상을 통해 protection suite (encryption algorithm, hash algorithm, authentication method, Diffie-Hellman group)가 결정되고 SAD에 저장되면, IPsec 엔진은 SAD를 참조하여서 IPsec 처리후 사용자 트래픽을 안전하게 전송하게 된다.

Phase 1에는 Main 모드와 Aggressive 모드의 두가지 방법이 있다. 두 모드간 차이점은, Main 모드에서는 6개 메시지가 교환되지만 Aggressive 모드에서는 3개의 메시지만 교환되어 처리 과정을 빠르게 하고 있다는 것이며 단 Aggressive 모드에서는 사용자 ID 보호는 하지 않고 있다. Phase I에서는 사용자 인증을 위해 Digital signature, public key encryption, revised mode of public key encryption, pre-shared key 의 4가지 방식이 채용되고 있다. 여기서 pre-shared key 방식을 제외하고는 공개키 인증서가 요구되는데 이는 PKI를 염두에 두고 있기 때문이다.

Phase II에서는 IPsec SA를 생성하기 위해 Quick 모드를 사용한다. New Group 모드는 Diffie-Hellman 그룹 특성을 협상하기 위해 사용되는 메시지 교환으로 IPsec SA 생성과는 무관하다. Quick 모드에서는 3개의 메시지가 사용되며 key refresh를 위해 자주 수행될 수 있다. 즉, phase I에서 생성된 IKE SA의 보호하에서 둘 이상의 Quick 모드 수행이 가능하다. 일반적으로 IKE SA는 도메인 정책에 따라 다르지만 1주일 이상 refresh 없이 사용될 수 있으나 IPsec SA는 동적으로 자주 갱신된다. 모든 메시지는 phase I에서 생성된 cookie를 사용하고 Message ID로 각 instance를 구별한다.

현재 IETF Security Area에서는 IKE의 기능 확장을 기하고 있다. 4가지 인증방식을 필드에 적용하기에는 PKI 구축이 더디고 road warrior나 kiosk 환경을 충분히 지원하지 못하고 있기 때문이다. 또한 대부분의 네트워크에서 legacy 인증방식(username/password, OTP등)을 고수하고 있어 이를 수용하기 위한 메카니즘을 제안해 놓고 있다. 그리고 Pre-shared key 인증방식도 $O(N^2)$ 크기의 키관리가 대규모 네트워크에서는 용이하지 않기 때문이다.[8]

4. SPS & SP Database

한 도메인내에서 적용되어야 할 암호 알고리즘 종류와 키크기의 설정 혹은 특정 서브도메인간 tunnel 설정등은, 도메인내의 보안관리자에 의해 임의로 설정될 수 있으며 이는 보안정책서버간의 협상 과정을 통해서 집행된다. IPsec 엔진은 outbound 패킷에 대해 IPsec 적용 여부 및 적용 방식을 결정하기 위해 SPD를 참조하도록 되어 있다. Inbound 패킷에 대해서도 적합한 정보보호 서비스가 적용되었는지를 확인하기 위해 SPD를 참조한다. SPD내의 도메인 보안정책은 SPS(Security Policy Server)로부터 다운로드받게 되는데 이에 대한 기술적 메카니즘을 제공하기 위해 그림.6에서 보인 바와 같이 SPS(Security Policy Server), PC(Policy Client), Master Files, SPS Databases, SPP(Security Policy Protocol)를 정의하고 있다.[9, 10, 11]

그림 6의 구조에서 가장 중요한 부분은 Master File로서 로컬 보안정책과 보안 도메인에 대한 특정 정보를 포함하고 있다. SPS의 데이터베이스는 로컬 보안정책과 원격 보안정책의 결합된 형태를 가진다. 보안정책서버는 클라이언트와 다른 보안정책 서버로부터 요청 메시지를 전송받았을 경우, 이를 분석한 후 요청과 접근제어 규칙을 기반으로 해당되는 보안정책 정보를 제공한다.

보안정책 기능은 호스트와 보안 게이트웨이에게

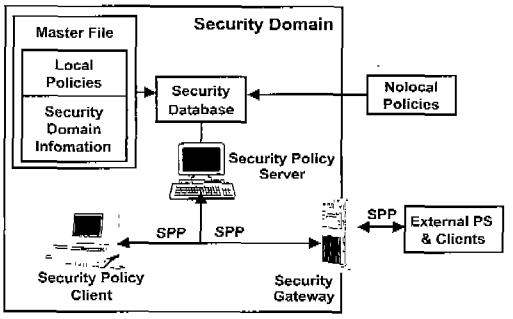

그림 6. Security Policy 모델

다중 게이트웨이를 통한 안전한 통신 채널을 설정하기 위해서 필요한 정책 정보를 제공하는 분산 시스템으로 구현된다. 또한, 호스트가 end-to-end 통신에 필요한 primary 보안 게이트웨이와 secondary 보안 게이트웨이를 검색할 수 있는 자동 메커니즘을 제공한다. 보안정책 시스템을 통해서 각 호스트는 보안 게이트웨이를 식별하고 이들 게이트웨이들이 시작 호스트 또는 목적 호스트에 대한 권한 여부를 검증할 수 있다. 반면에 정책 클라이언트는 정책 정보를 요청하고, 전송받은 결과를 알맞은 형태로 전환한다.

정책 서버와 정책 클라이언트간의 정책 정보를 교환하기 위해서 SPP(Security Policy Protocol)를 사용한다. SPP는 보안 노드간의 정책요청 및 이에 대한 응답으로 해당하는 보안 정책을 제공해 주거나 새로운 정책을 협상할 수 있는 자동화된 보안 정책 프로토콜이다.

보안 정책은 파이어월, VPN서버, 라우터등에서 적용되고 있지만 제품군에 따라 정책이나 적용방식이 매우 달라 정보보호 제품들의 통합에서 커다란 장애로 등장하고 있다.

5. SM

보안관리는 IPsec engine, IKE, SPS가 통합되어 운용되는 동안 정보보호 서비스의 제공상태나 audit 정보를 보안관리자에게 보여 주고 보안 관리자가 조정 및 제어할 수 있는 메카니즘을 제공하는 기능이다. 예로서 SA의 인증 및 암호화 알고리즘에 대한 정보와 SA의 생성, 삭제에 대한 정보를 수집하여 관리자에게 보여준다. SA에 문제가 있거나 네트워크에 문제가 발생했을 때 관리자에게 이벤트 통지를 보내 문제를 알려서 관리자가 문제를 해결할 수 있도록 한다.

보안 관리를 위해서는 관리 정보를 가지고 있는 MIB의 정의가 먼저 필요하다. IPSec을 관리하기 위해서는 IPSec SA와 IKE SA를 모니터링하는 MIB이 있어야 하고 DOI Textual Convention이 정의되어야 한다. 다음 리스트는 보안 관리의 구현에 필요한 MIB 정의를 하고 있는 IETF 드래프트 문서들이다.

- IPsec Monitoring MIB[12]
- IKE Monitoring MIB[13]
- ISAKMP DOI-indep. Monitoring MIB[14]
- IPsec DOI Textual Conventions MIB[15]

IPsec Monitoring MIB은 IPsec SA를 모니터하고 관리하는데 필요한 정보를 정의하는 MIB이다. 이 MIB은 하위 레벨 진단이나 정보의 디버깅에 사용되지 않는다. 그리고, 이 MIB은 IPsec의 일반적인 사용을 가정하고 있으며, 보안정책에 관한 정보를 정의하고 있지 않다. 이 MIB의 목적은 보안관리자로 하여금 운용 상태를 결정할 수 있도록 하고, 네트워크에서 IPsec이 차지하는 부분을 시스템 운용적인 차원에서 모니터링을 할 수 있게 한다. 부가적으로 IPsec SA의 명확한 사용을 위해 application specific MIB의 기본을 사용할 수 있다. 이 MIB은 IPsec SA의 정보에 대한 테이블, 통계자료 테이블과 트랩에 관한 테이블로 구성되어 있다. 트랩은 관리자가 잘못된 설정을 감지하고 에러와 시스템의 공격 상태를 알 수 있도록 한다. 관리 프로토콜로 SNMP를 사용하고, 관리 정보에 접근

하기 위한 프로토콜 명령은 PDU(Protocol Data Unit) 포맷으로 표현된다.

IKE Monitoring MIB은 IPsec SA를 생성하는데 필요한 IKE 프로토콜을 모니터링하는 MIB이며 IKE SA와 IPsec SA 사이의 연결관계를 제공한다. IPsec 설정, 하위 레벨 진단 및 정보의 디버깅에는 사용되지 않는다. 그리고, 이 MIB은 IKE를 사용하여 생성되는 정보들을 제외하고 IPsec의 일반적인 사용을 가정하고 있으며, 보안정책에 관한 정보를 정의하고 있지 않다.

IKE Monitoring MIB은 endpoint 테이블, IKE SA 테이블, phase 2 SA 테이블, SA bundles, uni-directional suites, Oakley group 테이블, exchange 테이블, 트랩에 관한 테이블로 구성되어 있다. IKE SA 테이블은 phase 1 SA를 모니터링하기 위한 것으로 ISAKMP DOI-indep. MIB의 ISAKMP SA 테이블을 기반으로 한다. Endpoint 테이블은 IKE SA의 협상과 관련된 endpoint를 정의하는 테이블이며, 다른 테이블들은 phase 2 SA에 대한 것이다. 이 MIB은 IKE SA에 대한 정보와 통계자료와 트랩에 관한 정보를 가지고 있다.

6. CA

IKE phase 1에서 사용자 인증을 위해서 공개키 인증서를 CA로부터 가져올 수 있어야 한다. 이러한 CA는 독립적인 시스템이 아니고 PKI라는 기반구조에 소속되어 있는 인증시스템이다. 그림 7에서는 국내 PKI 구축 방향을 보여주고 있으며 Root CA로서 전자서명 인증관리 센터와, 하위 단계인 CA 및 RA(Registeration Authority) 계층으로 구성되어 있음을 알 수 있다.

CA는 인증서 발급 및 CRL(Certificate Revocation List) 생성기능을 가지고 있다. 인증서는 사용자가 공개키를 등록시키고자 할때 발행되는 것이며, CRL은 유효기간이 지나기 전의 인증서에 대한 폐기목록을 기록한 것이다. 사용자는 인증서의 발급을 CA에 직접 의뢰할 수도 있지만, RA에 대행의뢰를 할 수 도 있다. RA는 인증서 발급시 수반되는 복잡한 절차를 사용자를 대신하여 처리하여 준다. 인증서와 CRL은 Certificate/CRL Repository에 저장되며, 사용자는 필요한 경우 이곳에서 인증서를 가져다 사용한다.

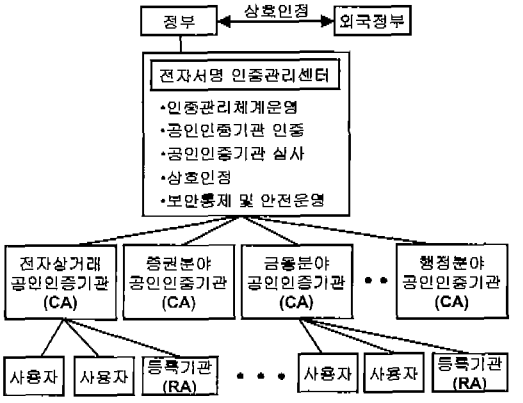

그림 7. 국내 PKI 구조

CA는 지역별 혹은 기관별로 설치될 수 있고, 각 CA간에는 상호인증을 통해 자신이 발급한 인증서가 다른 CA에서 사용될 수 있도록 하고 있다. 인증서 포맷은 ITU의 X.509를 따르고 있다. 국내에서는 1999년 2월 전자서명법이 제정됨에 따라, 1999년 7월 한국정보보호센터내에 전자서명 인증관리센터를 설립되어 최상위 인증기관 역할을 맡고 있다.

7. CL

패킷 헤더와 상위 계층 데이터에 대해 정보보호 서비스를 제공하기 위한 알고리즘에 대한 표준화는 송수신자간의 상호 협상을 위해 필요하다.[16] 표 4는 AH에서 지원되는 해쉬 알고리즘들을 보이고 있다. 값 249-255는 private use를 위해 사용될 수 있다. 각각은 특정 해쉬함수를 적용하는 방식에 대

표 4. IPsec AH transform id.

Assigned #	AH transform	related RFC
2	AH_MD5	1826, 2403
3	AH_SHA	2404
4	AH_DES	optional

한 총칭으로서 별도의 인증 방식(HMAC 혹은 KPDK등) 정의가 요구된다.

표 5는 ESP에서 지원되는 암호 알고리즘들을 보이고 있다. 값 249-255는 private use를 위해 사용될 수 있다. 국내 표준으로 채택되고 있는 SEED를 지원하기 위해서는 private use로 할당된 번호를 사용할 수 있다.

표 5. IPsec ESP transform id.

Assigned #	IESP transform	related RFC
1	ESP_DES_IV64	1827, 1829
2	ESP_DES	2403, 2405
3	ESP_3DES	2451, 2403
4	ESP_RC5	2451
5	ESP_IDEA	2451
6	ESP_CAST	2451
7	ESP_BLOWFISH	2451
8	ESP_3IDEA	reserved
9	ESP_DES_IV32	1827, 1829
10	ESP_RC4	reserved
11	ESP_NULL	2410

각 트랜스폼을 패킷에 적용하였을 경우 현재 문제시되는 것은 계산량의 증가로 패킷 처리속도가 늦어진다는 것이다. 따라서 성능 개선을 위해 암호프로세서를 사용하고 있다.

V. 결 론

Ⅳ장에서는 IPsec을 기반으로 하면서 인터넷 정보보호 프레임워크를 구성하는 주요 컴포넌트들에 대해 기술하였다. IPsec은 IKE와 더불어 지금까지 성공적인 인터넷 표준 중의 한 분야로 언급되고 있다. 이러한 사실은 대부분의 VPN 장비 제조 업체들이 기존의 L2TP, PPTP를 지양하고 IPsec을 채용하고 있음을 보아도 알 수 있다. 그러나 IKE가 VPN의 주요 기능으로서 또는 다른 응용 소프트웨어에서 널리 사용되기 위해서는 PKI의 보급이 선결되어야 한다. 최근 IETF security area에서는 IPsec의 빠른 적용을 위해서 키관리, PKI의 미성숙에 따른 문제점을 보완하기 위해 IPsra WG그룹이 만들어 졌으며 IKE의 확장을 기하고 있다. 앞으로 차세대인터넷 진입을 위해서는 이동인터넷과의 통합, 그룹키관리, AES(Advanced Encryption Standard)를 포함한 다양한 알고리즘의 수용, 성능개선등의 문제점이 해결되어야 할 것으로 보인다. 이제 IPsec은 단순히 구현 차원을 넘어서 실제 필드에서 적용되었을 때 나타나는 여러 가지 문제들이 보완되면, 조만간 IPsec 사용이 급속히 확산될 것으로 보인다.

※참고문헌

[1] 임채호, "야후등 유명 웹사이트 해킹 사고와 분산 서비스 거부공격 대책", 정보보호21c, 제2권 제3호, pp.50-54, March, 2000.

[2] Ryoichi Sasaki, "Internet and Security", IEICE 학회지 Vol.83, No.2, pp.107-111, 2000.

[3] N. Haller, R.Atkinson, "On Internet Authentication", RFC 1704, Oct., 1994.

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

[5] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, Novem-

ber, 1998.
[6] S. Kent, R. Atkinson, "IP Encapsulation Security Payload", RFC 2406, November, 1998.
[7] H. Harney, C. Muckenhirn, "The Internet Key Exchange(IKE)", RFC 2409, Nov., 1998.
[8] S. Kelly, S. Ramamoorthi, "Requirements for IPsec Remote Access Scenarios", Internet draft, Mar., 2000.
[9] M. Blaze, A. Keromytis, M. Richardson, L. Sanchez, "IPSP Requirements", Internet draft, July, 2000.
[10] M. Blaze, A. Keromytis, M. Richardson, L. Sanchez, "IPsec Policy Architecture", Internet draft, July, 2000.
[11] S. Kelly, S. Ramamoorthi, "Requirements for IPsec Remote Access Scenarios", Internet draft, Mar., 2000.
[12] L. Sanchez, M. Condell, "Security Policy Protocol", Internet draft, July, 2000.
[13] T. Jenkins, J. Shriver, "IKE Monitoring MIB", Internet draft, July, 2000.
[14] T. Jenkins, J. Shriver, "ISAKMP DOI- Independent Monitoring MIB", Internet draft, July, 2000.
[15] J. Shriver, "IPsec DOI Textal Conventions MIB", Internet draft, June, 2000.
[16] Piper D., "The Internet Security Domain of Intepretation for ISAKMP", RFC2407, Nov. 1998.

이 종 태

1984년 서울대학교 물리교육학과 졸업
1991년 Indiana University 물리학과 박사
1992년~현재 한국전자통신연구원 책임연구원
관심분야: 통신정보보호, 인터넷보안, 양자암호

손 승 원

1984년 경북대학교 전자공학과 졸업
1999년 충북대학교 컴퓨터공학과 박사
1991년~현재 한국전자통신연구원 책임연구원
관심분야: 차세대인터넷, 네트워크 보안, QoS 보장기술, 센서 네트워크