VPN을 위한 IPSec의 구현 동향

고 은 주* 손 승 일**

◈ 목 차 ◈

1. 서 론

최근 인터넷의 급속한 확산과 함께 특정 그룹을 위한 인터넷상의 망 구축이 활발히 진행되면서, 인터넷상의 데이터 정보는 누구나 공유할 수 있으므로 보안 문제 해결이 필수적이다. 따라서, 인터넷상의 보안문제가 점점 중요하게 대두되고 IP계층에서의 보안이 요구되면서, IP의 취약점으로는 네트워크 상의 신뢰하는 호스트로 가장하는 행위인 Spoofing, 다른 두 상대방의 통신 내용을 불법적으로 도청하는 행위인 Sniffing, 성립된 통신 세션을 공격하여 통신 상대인 것처럼 가장하는 행위인 Session hijacking이 있다. 이를 보완하기 위해 IETF에서는 IPSec이라는 IP계층에서의 보안 프로토콜을 만들게 되었다[1].

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 게이트웨이간에 1개 또는 그 이상의 경로(path)들을 보호하기 위해서 사용될 수 있고, 이들간의 트래픽에 대한 보안을 제공하기 위해서 AH(Authentication Header)와 ESP(Encapsulation Security payload) 프로토콜을 가지며, IPSec의 AH와 ESP는 정보의 보호 서비스로 인증, 무결성, 그리고 기밀성, 재전송 공격서비스를 제공한다[12,13,14,15]. 또한, IPSec은 두 가지 모드를 이용하는데, 하나는 트랜스포트 모드(transport mode)와 또 하나는 터널 모드(tunnel mode)이다. 트랜스포트 모드는 IP Payload의 부분만을 암호화하여 사용하고, 터널 모드는 IP Header를 포함하여 전체를 암호화하여 사용한다. 따라서, IPSec은 호스트와 호스트 사이의 보안을 수행하는 AH(Authentication Header)와 ESP(Encapsulating Security Payload)로 구성되어 있다. AH는 UDP로 전송되는 비연결 무결성을 지원하며, 데이터 부분을 인증 정보로 사용하며, 선택적인 보호 응답 서비스를 제공한다. ESP는 데이터의 기밀성, 제한된 트래픽 흐름 기밀성, 비연결 무결성, 데이터 지향 인증, 선택적인 보호 응답 서비스를 제공한다. 또한 AH, ESP 프로토콜 모두 접근 제어를 지원하여, 암호화키의 분산 방식을 지원하며, 트래픽 흐름 관리를 수행하게 된다. 이 프로토콜 부분은 독립적으로 작동되지 않고, 다른 구성 요소들을 필요로 하며 서로 연관되어 작동되며, IPSec의 암호화 모드를 선택적으로 사용하기 위해서는 네트워크 환경의 분석 및 암호화 모드 선택을 위한 기준 및 근거를 제시하여 적합한 IPSec의 암호화 모드를 사용하는 네트워크 모델을 제시한다.

본 논문에서는 먼저 VPN에 대해 소개하고, IPsec의 기본적인 동작원리와 구성 요소에 대해 다루고자 한다.

* 대전대학교 컴퓨터공학과 박사과정
** 한신대학교 정보통신학과 조교수

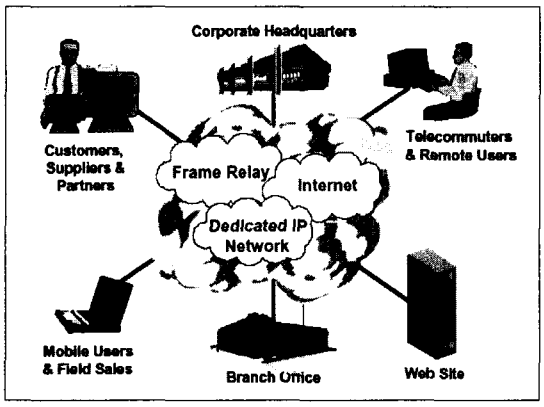
2. VPN의 정의 및 구조

2.1 VPN의 정의

정보통신망의 발달로 생활권이 컴퓨터 네트워킹으로 이루어지면서 특히 경제생활의 많은 부분은 전자상거래, EDI라고 불리는 새로운 영역을 바탕으로 세워지고 있다. 이러한 변화로 인하여 송장, 재정관련 정보, 연구개발기술 같은 중요한 정보가 인터넷상으로 흐르게 되었지만, 인터넷이 노출되어 있는 네트워크라는 취약점으로 전자상거래, EDI 등이 실제로 확산되기가 어려웠다. 인터넷으로 흐르는 정보를 보호하기 위한 방법들이 연구되었고, 그 중 해결책으로 제시된 것이 VPN(Virtual Private Network)이다[8]. 따라서, 인터넷같이 보호서비스를 제공하지 않은 채널사이로 데이터를 전송할 경우 데이터의 비밀성을 보장하기 위해서는 암호기술을 사용하여야 한다. 전송데이터의 비밀성을 보장하기 위한 방법으로 메시지 전체(IP 헤더와 데이터)를 암호화하기도 하고 또 다른 방법에서는 데이터의 일부분만을 암호화하여 전송한다.

VPN은 그림 1과 같이 한 네트워크의 자원과 구성을 다른 네트워크와 연결하는 기법이다. 연결을 할 때에는 사설 망의 연결에서처럼 똑같은 보안과 형태가 인터넷이나 다른 공공 망에서도 보장된다.

VPN은 로컬 네트워크에 위치한 회사의 보안을 필요로 하는 자원에 대하여 무결성과 보안성을 가지고 외부에 존재하는 사용자의 접근과 연결을 허용할 수 있다. 이러한 보장은 회사와 지점간의 고비용의 전용선의 임대나 전화접속에 따르는 불규칙한 비용의 불안감을 감소시킬 수 있다. 이러한 장점으로 VPN은 지역적으로 멀리 떨어져 있는 지점간의 연결에 이용 되어왔다. 이러한 연결에는 Internet Service Provider(ISP)의 회선을 임대하여 사용하는 방법과 전화 접속을 이용하는 방법이 있다. 또한, 기업은 사설 망을 구축하는 것보다 저렴한 비용으로 인트라넷이나 엑스트라넷을 구축할 수 있게 되었다. 그리고, 인터넷을 기반으로 하는 VPN을 구축함으로써 보다 유동성 있는 네트워크를 구축할 수 있다.



(그림 1) 기업 네트워크 구성도

VPN의 연결 구성요소로는 VPN 서버, VPN 클라이언트, 터널 그리고 VPN의 연결이 있다. 우선 VPN의 서버는 VPN 클라이언트가 VPN 연결을 통하여 접속하는 것이다. VPN 클라이언트는 VPN 서버와 연결을 시도하는 컴퓨터로서 직접 VPN 서버에 연결하는 것과 라우터를 통하여 VPN 서버에 연결하는 방법이 있다.

터널은 인크립션된 데이터를 연결시키기 위한 통로이다. VPN 연결은 인트립션된 데이터의 전달을 가능하게 해주는 것이다.

2.2 VPN의 기본 요소

VPN을 위한 연결을 위해서는 다음과 같은 요소를 필요로 한다.

- Encapsulation
- Authentication
- Data encryption
- Address and name server allocation

Encapsulation 은 데이터와 그에 동반하는 머리부분의 정보를 캡슐화하는 VPN의 기술로 PPTP와 L2TP를 예로 둘 수 있다. PPTP는 마이크로소프트사와 어센드사가 개발한 것으로 NT4.0 서버에 탑재되어 있다[6]. PPTP는 1996년에 발표되어 널리 쓰여지고 있고 앞으로도 계속적으로 보급될 것이지만 터널링에 대한 인증이 없다는 것이 단점이며, PPTP는 PPP를 기반으로 하여 PPP가 제공하는 다중 프로토콜 지원(IPX, NetBEUIetc), 사용자 인증, 데이터 패킷 압축 등의 기능에, TCP/IP

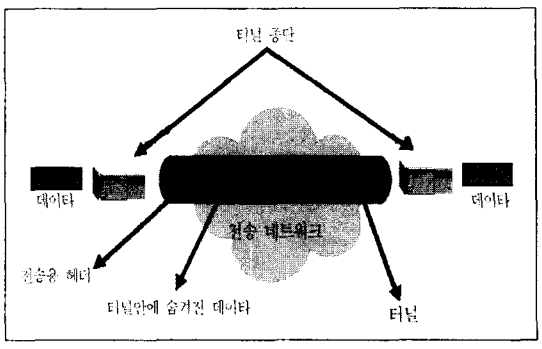
의 패킷 라우팅 기능을 수용하였다. PPTP는 PPTP 클라이언트가 생성한 IP, IPX, NetBEUI, SNA 등 PPP가 지원하는 다양한 네트워크 계층의 데이터그램을 포함하고 있는 PPP 패킷을 암호화하고 GRE(Generic Routing Header)v2를 사용하여 캡슐화(Encapsulation)한 후 IP 패킷형태로 인터넷망을 통해 PPTP 서버로 전송한다.

이에 대하여 단점을 보완하여 나온 방법이 L2TP이다. L2TP는 시스코사의 L2F와 PPTP의 결합된 기술이다. 향상된 점으로는 터널 링이 지원되는 모든 장비(IP, Frame Relay Permanent Virtual Circuits, X.25, VCs, ATM)에서 가능하고 또한 L2TP는 헤더압축이 가능하여 6바이트의 PPTP보다 작은 4바이트를 가질 수 있으며, 주로 원격 다이얼 업 사용자(Remote Dial-up User)가 공중망을 통해서 터널링을 통하여 사설 망에 연결될 수 있는 기능을 제공한다. 그러나 무엇보다도 L2TP의 장점은 터널 링에 대한 인증을 한다는 것이다. 아울러 IPSec을 이용한 강화된 보안을 구현할 수 있다. 인증(Authentication)은 사용자에 대한 인증과 데이터에 대한 인증으로 나눌 수 있다. 사용자에 대한 인증은 사용권한이 있는 사용자가 서버에 올바르게 접근한 것에 대한 것이다. 데이터에 대한 인증은 데이터의 무결성도 같이 하는데 이것은 데이터의 허가 없는 조작을 방지하는 것이다. 암호화(Encryption)에는 데이터, 혹은 데이터와 주소에 대한 정보를 포함하는 IP까지를 암호화하는 방법이 있다. 데이터만을 암호화하는 방법으로는 트랜스포트 모드를 이용하는 방법이 있고 IP 주소를 포함하여 암호화하는 방법으로는 터널 링 모드 방법이 있다. 이 방법의 차이점은 새로운 IP 주소의 유무에 따른다. 주소와 이름서버는 우선적으로 각자의 IP 주소를 가져야 한다. 그리고 VPN 서버에 연결된 클라이언트가 내부 네트워크에 연결되어 접근을 하려면 DNS 서버와 WINS 서버가 구성되어야 한다. DNS 서버는 인터넷 도메인 주소를 IP 주소로 풀이를 해주는 역할을 한다. 이것은 사설 IP 주소를 사용하는 로컬 네트워크의 주소를 풀이하여 통신이 가능하게 해준다.

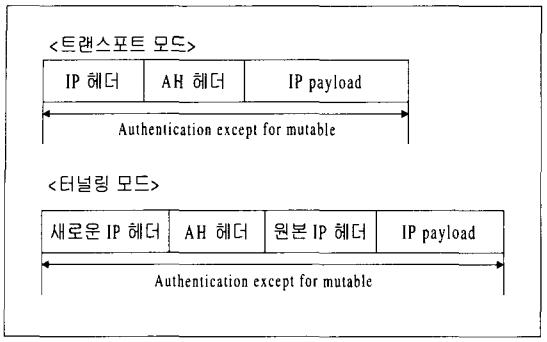
3. IPSec(IP Security protocol)

인터넷에서 보안을 유지하기 위한 한 가지 방안으로 암호 방식이 적용되고 있다. 암호 방식에는 크게 비밀 키 방식(Secret key cryptography)과 공개키 암호방식(Public key cryptograhy), 이 두 가지를 혼합한 복합 암호방식(Hybrid schemes)이 있다. 이러한 암호 방식을 이용해 TCP/IP 또는 TCP상위 레벨에서 적용을 함으써(SSL 등) 인터넷에서의 보안을 유지하려 하고 있다. 이러한 보안 유지 방법 중에서 최근에 진행되고 있는 것이 IPSec(IP Security)이다[2,3]. 지금까지 나온 네트웍에서의 보안을 보면 TCP레벨 위에서의 보안이 이루어지도록 되어 있었다. 예로 SSL은 TCP위에서 작동을 하게 된다. 그러나, IPSec은 IP에서 동작하기에 host와 host간 또는 host와 보안 gateway간 또는 보안 gateway와 보안 gateway사이에서 보안을 적용할 수 있다. VPN에서 본다면, VPN에서 PPTP나 L2TP는 링크 레벨에서 당사자간 터널링을 해주나 보안에는 문제가 있다. 그래서 연구 진행방향이 IPSec을 터널링을 위한 프로토콜로 씀으로서 터널링과 보안을 적용한 기본 구성도를 그림 2에서 보여주고 있다.

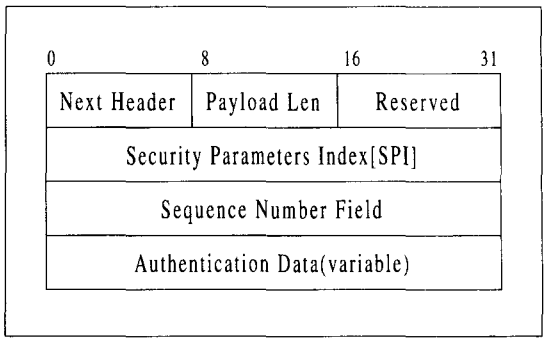
IPSec의 기본 개념은 IP Layer에서 보안 서비스를 제공해 주며, 보안 서비스라 하면, 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 재전송공격방지(replay attack)에 대한 보호 등을 말한다. 이러한 서비스를 IP 계층에서 해주게 되며, 기본 구조로는 IP 패킷에 2개의 서로 다른 확장 헤더를 포함하고, 인증을 위한 AH헤더와 암호화를 위한 ESP 헤더이다. 그리고, IPv6에서 IPSec이 진행되고 있지만, IPv4에서도 보안에 대한 요구가 있기에 IPSec이 IPv6와 IPv4에서 양립할 수 있도록 진행 중에 있으며, IPSec헤더는 IPv4에서는 optional이고 IPv6에서는 원래 형태(mandatory)가 있게 된다[5,7,9].



(그림 2) VPN 터널링 구성도



(그림 3) AH 트랜스포트/터널 모드



(그림 4) AH 헤더 형식

3.1 AH(Authentication Header)

AH는 IPSec이 지원하는 두 가지 보안 서비스 중에 하나로 IP 패킷에 대한 비연결형 무결성과 IP Datagram들을 위한 데이터 근원 인증(data origin authentication)을 제공하기 위해 사용되며 재전송 공격에 대해 보호하기 위해서 사용된다. 선택 가능한 옵션으로서 제공되는 재전송 공격 방지 서비스는 SA가 설정 될 때 수신측에 의해 선택될 수 있고, 상위 계층 데이터뿐만 아니라 IP 헤더의 가능한 모든 영역에 대해서 인증을 제공한다. AH는 인증과 무결성을 위한 알고리즘으로 MD5 또는 HMAC-MD5 또는 HMAC-SHA-1을 이용한다. 그리고 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. 또한, 보안 서비스들은 통신하는 호스트들의 쌍이나, 보안 게이트웨이들의 쌍 또는 호스와 게이트웨이간에 제공될 수 있다. AH는 두 가지 모드를 제공하는데 첫째가 트랜스포트 모드이고 두 번째가 터널 모드이다. 트랜스포트 모드는 오직 호스트 구현에서만 적용되며, 선택된 IP헤더 필드들에 추가하여 상위 계층 프로토콜에 대한 보호를 제공한다. 그리고 IP 헤더의 일부, AH자체, 그리고 IP 페이로드 부분에 대한 인증을 하며, 호스트에서의 구현에 적용 가능하다. 터널 모드는 호스트들이나 보안 게이트웨이들에 사용되며, AH가 보안 게이트웨이에 구현될 때는 (전송 트래픽을 보호하기 위해) 터널 모드가 반드시 사용된다. 그리고, 원본 소스 IP 패킷에 추가로 앞에 새로운 IP 헤더를 붙여서 터널링을 적용하게 된다. 터널 모드를 이용함으로서 소스 IP 패킷 전체에 대해 인증을 할 수 있게 된다. 소스 IP 패킷 전체와 새로운 IP 헤더의 일부, AH자체에 대한 인증을 한다.

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

그림 3은 트랜스포트 모드와 터널링 모드의 AH헤더 형식을 보여준다.

그림 4는 AH헤더 형식을 보여준다. Next header는 바로 다음에 따라 오는 헤더의 종류를 나타내고, Length는 인증 데이터 필드의 길이를 나타내고, Reserved는 아직 사용 안된 부분이고, SPI는 보안 연관을 식별하고, Sequence number는 재전송 공격 방지를 위한 번호이고, Authentication Data는 인증 알고리즘에 의한 계산된 값이 들어가게 된다.

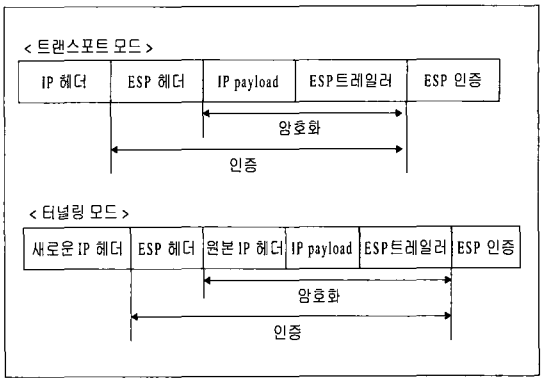
3.2 ESP(Encapsulation Security Payload)

ESP는 IPSec의 두 가지 보안 서비스 중의 나머지 하나로 IP 패킷을 위한 IPv4와 IPv6에서 여러 가지 보안 서비스를 한다. ESP는 단독으로 적용될 수 있고, IP Authentication Header(AH)와 함께 쓰일 수도 있으며, 조합된 형태로 사용될 수도 있다. 예를 들어서, 터널 모드의 사용 시에 조합된 형태가 사용될 수 있다. 그리고 통신하고 있는 호스트들 간이나, 통신 중인 보

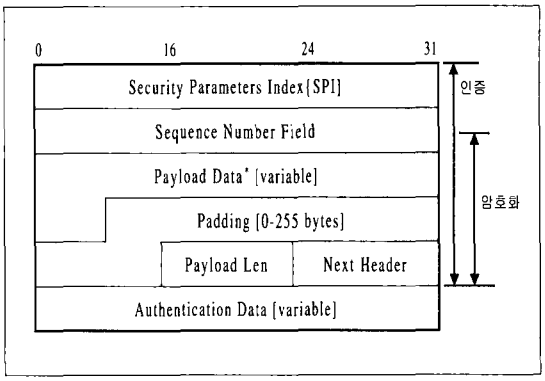
안 게이트웨이끼리, 또는 통신하고 있는 보안 게이트웨이와 호스트간에 제공되며, ESP는 AH에서 제공하는 보안서비스들 뿐만 아니라 비밀성(암호화) 서비스를 제공한다. ESP와 AH가 제공하는 서비스들간의 가장 중요한 차이점은 적용 범위에 있다. 터널 모드 ESP에 의해서 캡슐화 되는 경우가 아니라면, ESP는 어떠한 IP 헤더 필드들도 보호하지 못한다.

ESP는 비밀성(confidentiality), 데이터 근원 인증(data origin authentication), 비연결형 무결성(connectionless integrity), 재전송공격방지 서비스(anti-replay service(부분적인 순서적 무결성(partial sequence integrity))), 그리고 제한적인 트래픽 플로우 비밀성(limited traffic flow confidentiality)을 제공한다. 데이터 근원 인증과 비연결형 무결성은 결합된 서비스이고, 기밀성과 연계되어 옵션으로 제공되며, 재전송공격방지서비스는 데이터 근원 인증 서비스가 선택되는 경우에만 제공되며, 트래픽 흐름의 기밀성은 터널 모드에서 제공될 수 있으며, 트래픽 집단이 실제의 출처-목적지 패턴들을 감출 수 있는 보안 게이트웨이에서 구현된다. ESP는 기밀성과 무결성을 위한 알고리즘으로 DES-CBC 또는 MD5, HMAC-MD5, HMAC-SHA-1을 이용한다. 그리고, 제공되는 서비스 집합은 구현의 배치와 SA의 설정시에 결정되는 옵션들과 관련이 있다. ESP는 두 가지 모드를 제공하는데 첫째가 트랜스포트 모드이고 두 번째가 터널링 모드이다. 트랜스포트 모드는 오직 호스트 구현에서만 적용 가능하며, 상위 계층 프로토콜에 대해서만 보호를 제공하며, IP헤더에 대해서는 보호를 제공하지 않는다. 그리고, IP 패킷의 페이로드와 ESP 트레일러에 대한 암호화와, ESP 헤더, IP 페이로드와 ESP 트레일러에 대한 인증을 하고, 호스트에서의 구현에 적용 가능하다. 터널링 모드는 호스트들이나 보안 게이트웨이들에서 구현할 때 적용하는 모드로서, ESP가 보안 게이트웨이에서 구현될 때는 (가입자의 트래픽 전송을 보호하기 위해) 반드시 터널 모드를 사용하며, 원본 IP 패킷에 추가로 앞에 새로운 IP 헤더를 붙여서 터널링을 적용하게 된다. 원본 IP 패킷 전체에 대한 암호화와 ESP 트레일러에 대한 암호화를 하고, ESP 헤더, 원본 IP 패킷, ESP 트레일러에 대한 인증을 한다.

그림 5는 트랜스포트 모드와 터널링 모드의 ESP 헤더형식을 보여준다.



(그림 5) ESP 트랜스포트/터널 모드



(그림 6) ESP 헤더 형식

그림 6은 ESP헤더 형식을 보여준다. 각 필드의 역할은 다음과 같다. SPI는 보안 연관을 식별하고, Sequence Number는 재전송방지를 위한 번호이고, Payload Data 부분에 보안 연관의 의해 암호화된 데이터가 들어간다. 암호화될 대상으로는 트랜스포트 모드일 경우에는 TCP 헤더부터 실제 데이터까지가 되고, 터널 모드일 경우에는 원래 IP 데이터그램 전체가 된다. 길이를 맞추기 위해 Padding과 이 길이를 나타내는 Pad Length, 바로 다음에 오는 헤더를 나타내는 Next Header를 그림 5에서는 ESP 트레일러로 기록했다. 마지막으로 인증 데이터는 SPI부터 Next Header까지를 인증 알고리즘을 통한 결과 값이 들어가게 된다. 그리고 그림 5에서 보듯이 ESP 헤더의 바로 앞에 오는 프로토콜 헤더(IPv4, IPv6, 또는 확장헤더)는 그 프로토콜 필드(Protocol field) (IPv6, Extension의 경우)에 값 50을 포함하고 있어야 한다.

3.3 키 관리

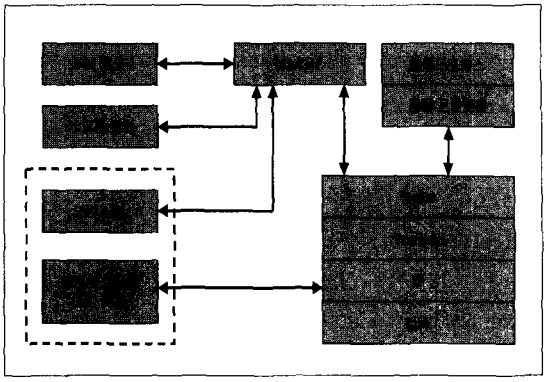
키 관리(Key Management)로 현재 IKE (Internet Key Exchange), ISAKMP (Internet Security Association and Key Management Protocol)와 같은 표준안이 있으며, 키는 사용자가 직접 입력하는 manual 방식과 사용자가 아닌 서버에 의해 자동으로 해주는 automatic 방식이 있다.

인터넷 환경에서 SA(Security Association)와 암호화 키들을 설정하는데 필요한 보안 개념을 이용한 프로토콜을 기술한다. SA들과 그들의 어트리뷰트들을 교섭하고, 설정하고, 수정하고, 삭제하는 SA 프로토콜은 수많은 보안 기법들과 각 기법들에 대한 많은 옵션들이 존재하고, 나날이 발전되는 인터넷에서 필요로 되고 있다. 키 관리 프로토콜은 인터넷상에서 공개키(Public Key)와 비밀키(Private Key)의 생성에 필요한 요구사항들을 처리할 수 있도록 충분히 강해야 한다. ISAKMP는 통신하는 사용자들을 인증하는 과정, SA의 생성과 관리, 키 생성 기법 등을 정의한다. 이러한 모든 것들은 인터넷 환경에서 안전한 통신을 설정하고 유지하기 위해 필요한 것들이다.

ISAKMP는 인터넷상에서 국가, 기업, 개인 통신을 위해 요구되는 보안을 설정하기 위해서 인증, 키 관리, 보안 협정 등과 같은 보안의 개념들을 조합하고 있다. ISAKMP는 SA을 설정하고, 교섭하고, 수정하고, 삭제하기 위한 과정들과 패킷 포맷들을 정의한다. SA들은 IP 계층 서비스, 전송 및 응용 계층 서비스, 교섭 흐름상의 자기 보호와 같은 다양한 네트워크 보안 서비스들의 실행에 필요한 모든 정보를 가지고 있다. ISAKMP는 키 생성과 인증 데이터를 교환하기 위한 payload를 정의한다. 이러한 포맷들은 키 생성 기법, 암호화 알고리즘과 인증 기법은 독립적으로 키와 인증 데이터를 전송하는 일관성 있는 구조를 제공한다[6].

그림 7은 ISAKMP의 구조를 보여주고 있다.

ISAKMP는 키 교환 프로토콜과는 구별되는데, 이는 키 관리에 대한 세부사항들과 키 교환에 대한 세부사항들이 확실히 분리되도록 하기 위해서이다. 많은 다양한 키 교환 프로토콜이 있는데, 이들 각각은 보안의 특성들이 다 다르다. 그러나, 공통의 구조는 SA 속성의 포맷이 같도록 요구된다. ISAKMP는 이 공통의 구조로 유지된다.



(그림 7) ISAKMP 구조

기능을 3부분으로 분리하게 되면 비도와 완전한 ISAKMP 구현을 위한 보안 분석을 더하게 된다. 그러나 이렇게 분리하는 것은 서로 다른 보안 요구사항들을 가지는 시스템들 사이의 상호 운영에 있어서는 그리 좋은 것은 아니다. 그래서, 이러한 보안 분석은 단순화되어야 한다. ISAKMP는 네트워크 스택의 모든 층에서 보안 프로토콜에 대한 SA들의 교섭을 지원하도록 되어 있다. SA의 관리를 집중화함으로써, ISAKMP는 각 보안 프로토콜 내에서의 중복된 기능의 양을 감소한다. ISAKMP는 또한 한번에 전 스택 서비스들을 협상함으로써 연결 설정 시간을 감소할 수 있다. ISAKMP는 교섭의 2단계를 제공한다. 첫 번째 단계에서는 2개의 엔티티들이 그들 사이의 교섭 흐름을 보호하는 방법으로 ISAKMP SA를 설정하는 것에 동의한다. 그리고 나면 이 ISAKMP SA는 요구되는 SA 프로토콜에 대한 교섭을 보호하기 위해 사용된다. 2개의 엔티티들은(eg. ISAKMP 서버들) 다중 ISAKMP SA들을 교섭할 수 있다. 교섭의 두번째 단계는 다른 보안 프로토콜들에 대한 보안 협정을 설정하기 위해 사용된다. 이 두번째 단계는 많은 보안 협정들을 설정하기 위해 사용될 수 있다. 이 단계 동안에 ISAKMP에 의해 설정된 보안 협정들은 많은 메시지/데이터 교환들을 보호하기 위해서 보안 프로토콜에 의해 사용될 수 있다. 2단계 접근은 대부분의 단순한 시나리오들을 위해서 높은 개시 비용을 가지지만, 이것이 대부분의 경우에 장점을 제공하는 몇 가지 이유들이 있다. 첫째로, 엔티티들은(ISAKMP서버들)은 몇 번의 두 번째 단계의 교섭을 거친 첫 번째 단계의 비용을 상환할 수 있다. 이것은 각 통신을 시작하지 않고

서도, 사용자들 사이에 다중 SA가 설정되도록 해준다. 둘째로, 첫 번째 단계동안에 교섭된 보안 서비스들이 두 번째 단계를 위한 보안 특성을 제공한다. 예를 들어, 교섭의 첫 번째 단계 후에 ISAKMP SA에 의해 제공된 암호화는 잠재적으로 좀더 간단한 두번째 단계의 교환의 사용을 허용함으로서, 엔티티의 보호를 제공할 수 있다. 반면에, 만약 첫 번째 단계 동안에 설정된 채널이 엔티티를 보호하는데 충분하지 않다면 두 번째 단계에서 충분한 보안 기법들을 협상해야 한다. 셋째로, ISAKMP SA가 있음으로 해서 ISAKMP 관리 작업의 비용은 꽤나 감소된다. ISAKMP SA가 사용자에게 주는 "신뢰할만한 경로" 없이도, 엔티티들은 SA의 각 에러의 알림이나 삭제를 위한 완벽한 재인증을 거칠 수 있을 것이다. 각 단계동안의 교섭은 ISAKMP 정의된 교환들이나 DOI내에서의 키 교환을 위해 정의된 교환들을 사용해서 수행된다. 보안 서비스들은 각 교섭단계에서 다르게 적용될 수도 있다. 예를 들어, 서로 다른 각각의 객체들은 서로 다른 교섭 단계동안에 인증된다. 첫 번째 단계동안에, 인증 되는 객체들은 ISAKMP 서버/호스트들이 될 수도 있다. 반면에, 두 번째 단계 동안에는, 사용자들이나 어플리케이션 레벨 프로그램들이 인증될 수 있다.

4. 결 론

본 고에서는 오늘날 인터넷의 활성화에 따른 다양한 보안상의 취약점을 해결하기 위해 새롭게 대두되고 있는 IPsec에 대해 살펴보았다. 향후에 인터넷에 대한 보안 문제는 중요한 관심 사항이 될 것으로 예측되고 있으며, 인터넷망을 활용한 데이터 전송시 기밀정보 유출 및 해킹차단을 위한 네트웍 보안 강화와 안전하고도 효과적인 네트웍 보안을 구현할 수 있는 다양한 기술들이 제안될 것으로 사료된다.

참 고 문 헌

[1] http://www.krnet.or.kr/krnet99/G/G1_1/index.htm.

[2] Compiled by Pete Loshin, 『Big Book of IPSec RFCs internet Security Architecture』, Morgan Kaufmann.

[3] Naganand Doraswamy, 『IPSEC The New Security Standard for the Internet, Intranets, and Virtual Private Networks』, Prentice Hall PTR.

[4] http://dirac.uos.ac.kr/lectures/comp/secure/chap25sec199.html.

[5] http://gong.snu.ac.kr/~kmscom/ipsec.html.

[6] http://penguin.andamiro.co.kr/doc/howto/en/html/VPN-Masquerade-HOWTO-6.html.

[7] http://landau.konkuk.ac.kr/doc/packages/freeswan/links.ipsec.html.

[8] http://www.nwfusion.com/power01/vpnlie/.

[9] http://www.openbsd.or.kr/faq/faq13.html.

[10] "http://www.ipsec.com/", SSH IPSec : VPN에서 IPSec을 쓰는 이유.

[11] 이만영외 5명, "전자상거래 보안 기술", 생능출판사.

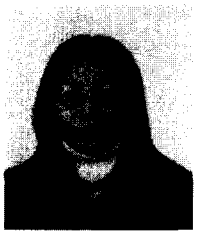
[12] 박창섭, "암호이론과 보안", 대영사.

[13] 김태현, "인터넷 보안과 해킹 화이트 페이퍼", 청암미디어.

[14] http://his.etri.re.kr/share/vpn.html.

[15] http://cnscenter.future.co.kr/ietf/vpn.html : VPN 관련 표준 문서.

◐ 저 자 소 개 ◑



고 은 주

2000년~2002년 호남대학교 컴퓨터공학과(석사)
2002년~현재 : 대전대학교 컴퓨터공학과(박사)

손 승 일

1985년~1989년 연세대학교 전자공학과(공학사)
1989년~1991년 연세대학교 전자공학과(공학석사)
1992년~1998년 연세대학교 전자공학과(공학박사)
1998년~2002년 호남대학교 컴퓨터공학과 조교수
2002년~현재 : 한신대학교 정보통신학과 조교수
주관심 분야 : ATM 통신 및 보안, ASIC 설계, 컴퓨터구조