通信情報保護學會誌
第8卷 第2號, 1998. 6

인터넷 보안 메커니즘에 관한 연구

A Study on Internet Security Mechanism

*조 인 준, *정 회 경, **김 동 규

요 약

IPv6(일명 IPng(Internet Protocol next Generation))은 현재의 인터넷 프로토콜인 IPv4를 개량한 다음 세대의 인터넷 프로토콜이다. 새롭게 개량된 주요내용은 주소공간의 확장, 이동사용자를 위한 IP(Mobile IP)추가, VOD(Video on demand)와 같은 고속통신 QOS(Quality of Service)추가, 그리고 네트워크 계층에서 보안메커니즘 제공 등을 들 수 있다[1][2][3].

본 논문에서는 이들 중에서 네트워크 계층의 보안 메카니즘을 기존의 전송 계층의 SSL(Secure Socket Layer)보안 메커니즘과 비교 분석 하였다.

핵심어 :IPv6, SSL, IPsec, 인터넷 보안

I. 서 론

최근의 인터넷과 WWW(World Wide Web)의 폭발적인 증가는 개방형 네트워크상의 여러 응용에 보안의 필요성을 강요하고 있다. 지금까지 인터넷 응용분야에 대표적인 보안 메커니즘으로는 전자우편 부문에 PGP(Pretty Good Privacy)와 PEM(Privacy Enhancement Mail), 네트워크 관리 부문에 SNMPv2 보안(Simple Network Management V2 Security), 웹 부문에 S-HTTP(Secure-Hyper Text Transport Protocol)과 SSL(Secure Socket Layer)등을 들 수 있다.

IETF(Internet Engineering Task Force)는 TCP/IP네트워크을 대상으로 전송계층과 네트워크계층에 표준 보안메커니즘을 제공하고자 노력을 계속하고 있다[4][5].

IPv6의 IPsec(IP Security)프로토콜은 1994년 7월에 IETF의 IPsec WG(Working Group)가 RFC(Request For Comments)로 제안 중인 표준이다[4]. 이는 현재 여러 운영체제에서 시험 중에 있고 금년 중으로 표준이 확정되어 2-3년 후에 시장에 공급될 것으로 예상되고 있

* 배재대학교 컴퓨터공학과 교수
**아주대학교 컴퓨터공학과 교수

다.

SSL프로토콜은 1994년 10월에 IETF 전송계층 보안 WG가 RFC로 제안하였고 1995년2월에 범용 프로토콜설계가 이루어져 안정된 상태로 사용되고 있다[5][6]. 현재는 SSL 2.0의 여러 가지 단점(보안 및 기능상의 단점)을 개선한 SSL 3.0이 산업계표준으로 인식되고 있다.

본 논문에서는 인터넷응용에 보안기능을 제공하는 이들 두 가지 보안매커니즘을 분석하고 이들의 차이점을 정의함으로써 향후 인터넷응용 보안의 방향을 모색하였다. 이를 위해 Ⅱ장에서는 IPv6의 중요특징을 정리하고, Ⅲ장에서는 SSL의 보안메커니즘, Ⅳ장에서는 IPv6의 IPsec의 보안메커니즘, Ⅴ장에서는 SSL 3.0과 IPv6의 IPsec을 비교 분석하였고, 마지막 Ⅵ장에서는 결론으로 향후 전망을 하였다.

II. IPv6 중요 특징

이 장에서는 IETF가 제안 중인 표준 IPv6의 중요 특징을 헤더형태, 어드레싱, 라우팅, 보안서비스 순으로 간략하게 설명하고 마지막으로 IPv4에서 IPv6로의 전환방법을 논의하였다.

1. 기본헤더

IPv6의 주소영역 128비트는 IPv4의 32비트보다 4배 크지만 헤더의 크기는 단지 2배 크다. 이는 낮은 전송대역으로 패킷처리 비용을 최소화하기 위해 IPv6의 헤더항목을 줄인 결과이다. IPv6의 기본헤더 형태와 각 항목의 내용을 정리하면 다음과 같다[4].

<table>
<tr><td colspan="2">버전(4비트)</td><td>우선순위(4비트)</td><td colspan="3">흐름레벨 (24비트)</td></tr>
<tr><td colspan="3">페이로드길이 (16비트)</td><td>다음헤더(8비트)</td><td colspan="2">홉제한(8비트)</td></tr>
<tr><td colspan="5">소스주소 (128비트)</td></tr>
<tr><td colspan="5">목적지 주소 (128비트)</td></tr>
</table>

그림 1. IPv6 기본헤더

(1)버전 : IP프로토콜의 버전 번호(4비트)

(2)우선순위 :1) 혼잡 트래픽 통제용으로 7가지 패킷 전송 우선순위를 정의한다.

0 : 특징이 없는 트래픽
1 : 뉴스와 같은 후향(Background)트래픽
2 : 전자우편과 같은 데이터 전송
3 : 예약
4 : 파일전송과 같은 대용량 데이터전송
5 : 예약
6 : "Telent"과 같은 상호 동작 트래픽
7 : SNMP(Simple Network Management Protocol)와 같은 인터넷 통제 트래픽

2) 비 혼잡 트래픽 통제용 즉, 발신지에서 트래픽 지연이 허용되지 않은 응용(예, 오디오)를 위해 우선순위 값 8-15를 의한다. 가장 낮은 우선순위 8는 사용자가 대부분의 트래픽을 잃어버려도 되는 상황에 사용하고 가장 높은 우선순위 15는 사용자가 최소한의 트래픽 잃음을 허용할 경우 사용한다.

(3) 흐름레벨(24비트) : 이는 송신자 혹은 수신자의 패킷의 흐름정보를 라우터에 캐쉬하고 이를 라우터가 참조하여 패킷

의 목적지를 결정한다. 따라서 라우터의 경로설정에 필요한 계산부담을 줄이는 효과가 있다. 이는 실시간 비디오와 같은 응용에서 매우 유용하다.

(4) 패이로드 길이(16비트) : 헤더 다음의 패킷길이를 정의한다. IPv6는 각 링크가 기본적으로 576 바이트 패킷을 처리한다. 따라서 헤더 40비트를 제외한 536 바이트가 데이터 크기이다. 하지만 IPv6는 65,535바이트의 페이로드를 전송할 수 있다. 이를 위해서 단편화(Fragmentation)가 지원된다. 이때 단편화 헤더(8바이트)가 사용되고 수신측에서 이의 재조립이 이루어진다. 홉들간에 헤더가 정의한 또 다른 선택은 점보 페이로드이다. 이는 패킷이 65,535바이트보다 클 때 사용한다.

(5) 다음헤더(8비트) : IPv6 기본 헤더 다음에 어떤 헤더가 오는지를 나타낸다. 현재 "다음헤더" 항목에 정의된 헤더 값은 다음과 같다.

0 : 홉간의 옵션헤더　　4 : IP
6 : TCP　　17 : UDP
43 : 라우팅 헤더
44 : 단편화 헤더
45 : IRP(Interdomain Routing Protocol)
46 : RRP(Resource Reservation Protocol)
50 : ESP(Encapsulation Security Payload)
51 : AH(Authentication Header)
58 : ICMP(Internet Control Message Protocol)
59 : 다음헤더 없음
60 : 목적지 옵션헤더

(6) 홉(Hop)제한(8비트) : 패킷이 얼마나 멀리 갈수 있는지를 정의한다. 이는 반복(Looping)되는 라우팅 현상 방지 그리고 최적의 홉값을 선택함으로써 라우터의 부담 최소화라는 두 가지 목적을 위해 사용된다. 이는 노드 통과마다 1씩 감소시키고 홉 제한 값이 0이면 그 패킷은 자동으로 제거된다.

(7) 소스주소(128비트) : 패킷 송신자의 128비트 주소

(8) 목적지주소(128비트) : 패킷 수신자의 128비트 주소이다. 라우팅 헤더인 경우 목적지 주소는 최종 수신자 주소가 아니고 중간 노드의 주소가 된다.

2. 어드래싱

IPv6는 3가지 주소형태를 지원한다.

(1) Unicast : 단일 인터페이스를 지정한다. 패킷이 해당주소의 인터페이스에 전달된다.

(2) Anycast : 여러 노드의 인터페이스 집합을 지정한다. 따라서 패킷은 이 주소에 해당되는 인터페이스 집합 중 한 인터페이스에 전달된다.

(3) Multicast : 여러 노드의 인터페이스 집합을 지정한다. 따라서 패킷은 이 주소에 해당 되는 인터페이스 집합 모두에게 전달된다.

따라서 IPv6에는 "Broadcast"주소가 없어지고 이를 "Multicast"로 대체하였다.

증가하는 인터넷을 수용하기 위해 IPv6는 주소영역을 32비트에서 128비트로 확장하였다. 이 128비트 주소가 충분한지를 검증하기위해서 지구의 표면을 계산하여 비교한 예를 인용한다[7]. IPv6는 이론적으로 2^{128}개의 인터페이스 혹은 인터페이스 집합을 식별할 수 있다. 실제의 구현에서 이 숫자는 적정한 주소 스킴이 이용되기 때문에 더 줄어들 수 있다 이러한

스킴의 예(실제적인 주소 스킴은 아직 정의되지 않음)는 다음과 같다.

〈제공자〉〈기관〉〈네트워크〉〈인터페이스〉

따라서, 이용할 수 있는 주소영역은 2^{128}보다 상당하게 줄어들 것이다. Huitema는 IPv6의 주소를 8×10^{7} 과 2×10^{23}개 사이가 될 것으로 계산하였다. 가장 낮은 추정을 사용한다고 해도 지구의 표면적이 511,263,971,197,990 로 가정했을 경우 각 m^2당 1,563개의 주소가 배당되는 것으로 나타났다. 이는 먼 미래에도 충분한 주소영역이라고 보여진다.

3. 라우팅

IPv6의 라우팅은 주소길이가 128비트라는 것을 제외하고는 IPv4의 라우팅과 차이가 없다. 따라서 IPv4의 라우팅 알고리즘이 IPv6에 적용될 것이다. 하지만 IPv6는 다음과 같은 확장 라우팅을 지원한다.

(1) 라우팅에 정책, 성능 등을 반영할 수 있는 기능지원
(2) 이동호스트가 이동하였을 때 이동위치로 자동 라우팅하는 기능지원
(3) 새로운 주소로 라우팅 해 주는 자동 재어드래싱 기능지원

"다음헤더"에 정의된 라우팅헤더는 패킷이 전송되어야 할 한 개 이상의 중간노드 리스트에 사용된다. 이는 IPv4의 소스라우트와 매우 유사하다.

4. 보안서비스

이 절에서 IPv6의 보안서비스를 간단하게 설명한다. Ⅳ장에서 더 자세하게 논의 할 것이다. IPv6는 인증서비스와 ESP(Encapsulating Security Payload) 보안 서비스를 각각 분리하여 제공하거나 이들을 조합하는 방법으로 제공한다[Ⅳ장 5절 참조].

4.1 IPv6 인증 헤더

인증헤더[8]는 IPv6의 확장헤더 51번이다. 이는 송신자를 인증하고 전송도중에 패킷의 변경 유무를 검증하는 무결성 보안 서비스를 제공하기위한 메커니즘이다. IPv6는 다종의 인증기법과 이에 관련된 인증알고리즘을 지원한다. 이 중에서 키를 가진 MD5(Message Digest 5) 알고리즘이 인터넷에서 양립성 문제해결을 위해 제안된 표준이다. 이 표준 알고리즘이 IP스누핑 혹은 호스트 가장과 같은 여러 네트워크 공격을 방어한다. IP가 네트워크계층에 위치하기 때문에 호스트 인증(원적 인증)에 도움이 된다. 미국의 수출 제한이 이 논문의 주제에는 벗어나지만, IPv6에서는 인증과 무결성 서비스만을 제공(기밀성은 제공하지 않음)하기 때문에 수출이 가능하다.

인증헤더의 형태는 그림2)에서 보여주고 있다. 여기에서 SPI(Security Parameters Index)는 송·수신자 간의 통신 보안협상[Ⅳ장 2절 참조]을 정의한다. 그리고 SPI 다음에 오는 인증데이터는 32비트 정수로 구성된다. 만약 MD5를 사용한다면 인증데이터는 16바이트로 구성된다. 이는 MD5의 해쉬값이 128비트이기 때문이다.

4.2 IPv6 ESP(Encapsulating Security Payload) 헤더

ESP헤더[9][10]는 IPv6 확장헤더 50번이다. 이는 IPv6 데이터그램 패킷에 기밀성 서비스를 제공하기위한 메커니즘이다. 인증헤더에서 처럼 ESP헤더는 암호알고리즘에 독립적이다. 인터넷내에서 상호 운용성 보장을 위해서 DES-CBC(Data Encryption Standard-Cipher Block

다음헤더(8비트)	길이(8비트)	예 약 (16비트)
보안 매개 색인 (SPI : Security Parameters Index) :32비트		
인증데이터 (32비트 배수)		

그림 2. 인증헤더의 구조

Chaining)알고리즘이 표준처럼 사용되고 있다. ESP는 전 IP 패킷이 암호화되면 터널형 모드가 되고, 전송계층의 세그먼트만 암호화되면 전송형 모드가 된다.

그림3)은 ESP의 구조를 보여주고 있다. SPI 다음의 초기벡터는 DES-CBC암호알고리즘의 입력 매개변수 값이다. 그리고 이 벡터 다음에 암호화 페이로드가 위치한다. 그리고 패딩 항목은 전체 ESP크기를 32비트 정수배로 만들기 위해 필요한 것이다. 마지막으로 페이로드형 항목은 페이로드 데이터가 전송계층의 프로토콜 중 어느 프로토콜(예, TCP, UDP등)에 속하는지를 나타낸다.

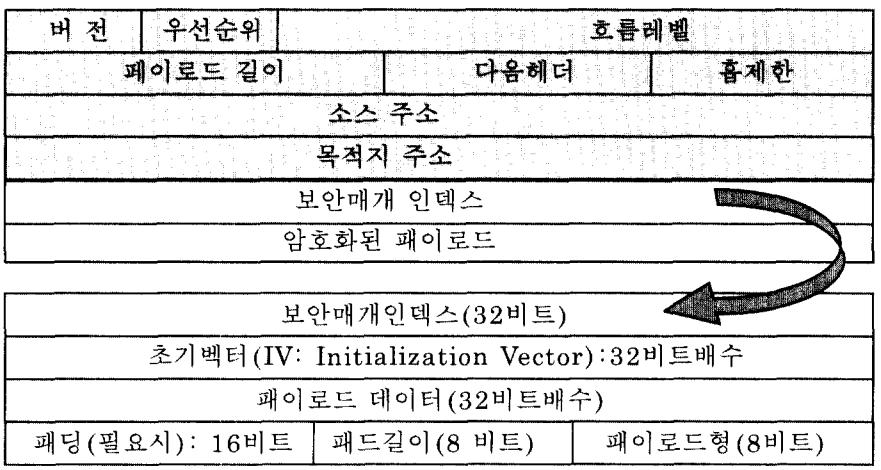

그림 3. ESP(Encapsulating security payload)의 구조

5. IPv4에서 IPv6로 전환

IPv6는 IPv6와 IPv4가 혼재 되어 설치된 호스트와 라우터에서 상호 동작할 수 있도록 설계되었다. 이는 용이한 인터넷 전환을 위한 것이다. IPv6로 전환메커니즘은 다음과 같은 특징을 갖는다.

(1) 점진적인 전환 : 호스트 혹은 라우터를 대상으로 단위별 설치를 가능하게 한다.
(2) 최소 업그레이그 종속성 : 선행조건은 DNS(Default Name Server)에만 설치하면 된다.
(3) 용이한 어드래싱 : 호스트나 라우터가

IPv4에서 IPv6로 업그레이드 될 때 기존의 주소패스가 변경될 필요가 없다. 호스트와 라우터는 기존의 주소를 계속 사용한다.

(4) 저렴한 초기비용 : 어떠한 준비 작업도 기존시스템을 IPv6로 업그레이드할 경우 필요치 않다.

이러한 전환메커니즘이 IPv6가 설치된 호스트와 라우터가 IPv4가 설치된 호스트 및 라우터간에 상호동작을 보장해 준다.

전환은 IPv4의 주소영역 제한 때문에 상당히 빠른 속도로 이루어질 것으로 보인다. 대체적으로 호스트간에 업그레이드가 이루어질 때까지 LAN에서는 IPv4가 사용될 것으로 보인다. LAN을 인터넷에 연결시켜주는 DNS와 라우터는 사용준비가 되면 곧 업그레이드해야 할 것이다. 이는 인터넷 환경에서 가장 빠르게 IPv6의 장점을 얻기 위한 가장 쉬운 방법이 될 것이다.

III. SSL 보안메커니즘

SSL은 인터넷 클라이언트/서버간의 연결지향형 보안서비스를 제공하는 프로토콜이다. 이는 기밀성, 인증 그리고 재현공격 방지 등의 보안 서비스를 제공한다[11][12].

1. 구조

그림4 는 OSI 참조모델과 SSL간의 관계를 보인 것이다. SSL은 "SSL 레코드계층"과 "SSL 핸드쉐이크계층"이란 2개의 부 계층으로 구성된다. 각 계층은 상위계층에게 서비스를 제공하고 하위계층으로부터 제공된 서비스를 사용한다. "SSL 레코드계층"은 TCP와 같은 연결지향형 전송계층 위에서 기밀성, 인증 그리고 재현공격 방지 등의 보안서비스를 제공한다.

"SSL 레코드계층" 위에 위치하는 "SSL 핸드쉐이크계층"은 두 종단간에 보안시스템을 동기화 시키고 초기화하는 키 분배 프로토콜 기능을 한다. 키 분배가 종료되면 응용정보는 "SSL 레코드계층"을 통해서 보안서비스를 받는다.

SSL2.0은 SSL 3.0에 비해 약점을 갖는다. 간략히 요약하면 인증키가 40비트이다. 그리고 블록암호 모드내에 있는 MAC(Message Authentication Code)안으로 패딩바이트를 놓게 되어 패딩 길이 항목이 비 인증상태가 된다. 이는 "적극공격자"에게 메시지의 끝으로부터 바이트 삭제를 허용한다. 기타의 약점은 [13]을 참고하길 바란다.

2. 키 분배 및 암호알고리즘 협상(핸드쉐이킹 프로토콜 계층)

핸드쉐이크 프로토콜은 크게 두 단계로 구성된다. [단계1]에서는 암호알고리즘의 선택, 마스터 키의 분배, 서버인증을 행한다. [단계2]에서는 요구된다면 클라이언트를 인증하고 핸드쉐이킹을 종료한다. 이 단계가 끝나면 서버와 클라이언트간에 데이터전송이 시작된다. 핸드쉐이킹 동안 및 그 후에 모든 메시지는 "SSL레코드 계층"에 보내진다.

핸드쉐이킹 프로토콜이 동작되는 절차를 더 상세하게 구분하면 세션ID가 사용되지 않고 클라이언트 인증이 필요 없는 경우, 세션ID가 사용되고 클라이언트 인증이 필요 없는 경우, 그리고 세션ID가 사용되고 클라이언트 인증이 필요한 경우로 나누어 설명할 수 있다.

이 중에서 첫번째 경우를 상세하게 설명하면 다음과 같다. 기타의 경우는 참고문헌[14]를 참조하기 바란다. 여기에서 사용되는 표기법으로 "C→S : XXX" 는 C(클라이언트)에서 화살표 방향으로 S(서버)에 메시지 내용 "XXX"를 전송한다는 의미이다. 메시지내의

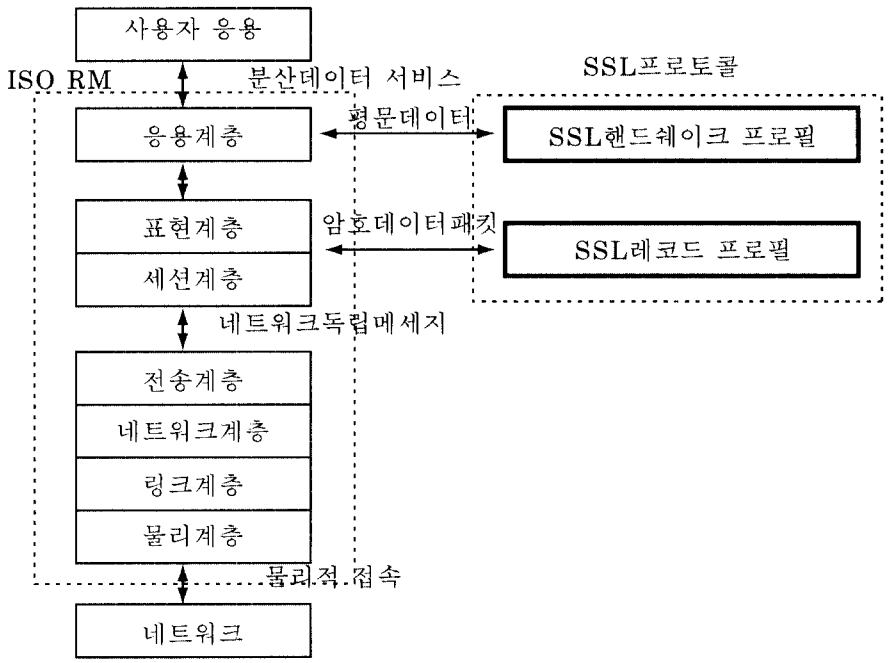

그림 4. OSI RM 과 SSL 관계도

"{yyy}z-key"는 "yyy"를 "z-key"로 암호화한다는 의미이다.

[단계1] C→ S : Challenge-data, cipher-specs

이 단계에서 클라이언트가 지원할 수 있는 암호관련 명세와 후에 서버를 인증할 수 있는 챌린지-데이터를 서버에게 보낸다.

[단계2] S→C : Connection-ID, Server-certificate, cipher-specs

이 단계에서 서버가 접속-식별자, 클라이언트와 서버 모두가 지원할 수 있는 협의된 암호관련 사항, 그리고 서버-보증서 등을 클라이언트에게 보낸다. 서버-보증서는 클라이언트가 서버의 공개 키를 얻어서 CA(Certification Authority)로부터 서버의 신원 검증을 위한 것이다.

[단계3] C→S : Cipher-kind, clear-master-key, {secret-master-key}server-public-key

이 단계에서는 [단계2]에서 보낸 암호관련 사항을 참조하여 최종 협의된 암호관련 사항들과 마스터 키를 서버에게 보낸다. 선택된 암호알고리즘이 수출수준의 등급을 갖는 것이면 총 128비트 키 중에서 서버의 공개키로 40비트만 암호화하고 88비트는 비 암호화 상태로 보낸다. 반대로 클라이언트가 전체 키를 암호알고리즘에 사용한다면 서버의 공개 키로 전체를 암호하하고 "Clear-master-key"항목은 빈 상태로 보내진다.

이 단계까지 세션 키 분배가 완료된 상태이다. 따라서 이후로 발생하는 모든 메시지는 "SSL레코드계층"에서 암호화된다. 여기에서 마스터 키는 직접 암호화 키로 사용되지 않고

2종의 세션 키를 계산하는데 사용된다. 클라이언트가 서버에게 메시지를 보낼 때 클라이언트는 암호화를 위해 "client-write-key"를 계산하여 사용하고 서버는 이의 복호화를 위해 "server-read-key"를 계산하여 사용한다. 내용적으로 이는 동일하다. 반대로 서버가 클라이언트에게 메시지를 보낼 때 서버는 암호화용으로 "server-write-key"를 계산하여 사용하고 클라이언트는 복화용 키로 "client-read-key"를 계산하여 사용한다. 이는 내용적으로 동일하다. 이들이 "client-master-key"를 사용하여 계산된 두 종의 세션 키들이다. 몇몇 암호메커니즘에서는 암호용 키로 1개 이상을 요구할 수 있다(예. 3-DES). 따라서 여러 개의 "write-key" 및 "read-key"가 실제적인 세션 키를 구성할 수 있다. 이는 실제 사용된 세션 키를 보내지지 않고 마스터 키로 이를 계산하여 사용한다.

[단계4] C→S : {connection-id}client-write-key

이 단계는 클라이언트가 핸드쉐이킹을 종료한다. 이는 원래 서버가 만든 접속 식별자로 구성되는데 이는 재현공격 방지를 위한 넌스 값으로 사용된다.

[단계5] S→C : {challenge-data}server-write-key

이 단계는 서버인증의 최종 단계이다. 이에는 클라이언트가 원래 보낸 "challenge-data"가 포함된다. 실 서버만이 [단계3] 메시지 내에 "secret-master-key" 복화용 개인 키를 가지고 있기 때문에 이 메시지의 수신 및 복호화는 서버인증의 최종 단계가 된다 이 메시지는 "sever-write-key"사용하여 암호화된다.

[단계6] S→C : {session-id}server-write-key

이 단계에서 서버가 핸드쉐이킹을 종료한다. 이에는 서버가 생성한 "session-id"가 포함된다. 이는 이 후의 핸드웨이킹에서 동일 클라이언트와 서버간에 암호알고리즘 및 키 협상을 다시 하는 것을 피하기 위해서 사용된다. 세션-id들은 접속이 종료된 후 양측에 케쉬된다. 이들은 이후의 접속에 재 사용된다. 케쉬 시간은 100초를 추천하고 있다.

3. 보안 서비스 제공(SSL 레코드계층)

이 계층에서는 기밀성, 메시지인증, 재현공격방지 등의 보안 서비스를 제공한다. 이들의 특징을 요약하면 다음과 같다.

3.1 기밀성 보안서비스

첫째, 도청방지를 위해 SSL 프로토콜은 "핸드쉐이크 프로토콜"에 의해 협의된 세션 키로 모든 응용계층 데이터를 암호화한다. 이때 표준 모드로 사용중인 다양하고 강력한 알고리즘이 로칼 응용의 보안등급에 따라 가용하다. 이때 세션 키는 연결 당 하나의 해쉬랜덤 값을 생성하여 사용한다. 이는 독립된 세션 키가 연결의 각 방향에서 사용될 수 있다. SSL은 도청자에게 알 수 있는 많은 평문을 제공하지만 이를 방지할 보다 좋은 대안은 없다. 이는 미리 알고 있는 평문공격을 방어할 수 있는 안전한 암호알고리즘이 필요함을 의미한다.

둘째, 트래픽 분석과 같은 소극적 공격(Passive Attacks)에 대한 대처이다. 트래픽공격은 보호된 세션에 흐르는 비 암호화된 패킷 항목과 비 보호된 패킷 속성들을 검사하여 기밀정보를 찾아내는데 목적이 있다. 예를 들면 비 암호화된 IP 소스 및 목적지 주소, TCP 포트번호, 혹은 네트워크 트래픽 양을 검사하여 트래픽 공격자는 누구와 통신을 하고 있고,

서비스의 형태는 무엇이고, 그리고 사업 및 개인 관계성 등 어느 정도의 정보를 찾아낼 수 있다. SSL에서는 이러한 종류의 공격은 방어하지 못한다.

셋째, 알고리즘 분석과 같은 적극공격(Active attacks)에 대한 대처이다. 이는 선택된 평문/암호문 공격에 대비하여 기본적으로 암호알고리즘이 안전해야 한다. 이는 알고리즘 자체의 안정성만으로 충분한 것이 아니다. IETF IPsec WG에 의한 최근의 연구에서 레코드계층에 "적극적공격"은 기본적인 암호문이 강력하다고 해도 시스템 기밀성이 파괴될 수 있다는 것을 보여주고 있다. 이는 SSL 3.0 레코드계층이 이러한 강력한 공격에 저항하도록 하고 있다.

3.2 메시지 인증서비스

응용데이터의 기밀성 보장과 더불어 SSL은 암호기법을 사용하여 메시지를 인증한다. 인터넷에서 IP스누핑과 TCP세션중 데이터강탈과 같은 "적극적공격"용 소프트웨어들이 상업적으로 가용한 상태이다. 더구나 통신보안 취약점들을 찾아내기 위한 재정적인 투자가 빠른 속도로 이루어지고 있다. 이에 대응하기 위해서 강력한 메시지인증을 요구하고 있다.

SSL 3.0은 개선된 MAC(Message Authentication Code)를 사용하여 응용데이터의 무결성을 보장한다. SSL 3.0에서는 단순하고 빠른 해쉬 구조체를 생성하는 HMAC (Hash based MAC)[15]을 선택하였다. 따라서 SSL 3.0은 MAC을 대상으로 직접적이고 포괄적 혹은 암호분석 공격에 매우 안전하다. 이는 SSL 2.0이 불안전한 MAC 사용에 따른 심각한 설계 문제점을 개선한것이다.

SSL 3.0 HMAC키는 최소 128비트를 가진다. HMAC의 선택은 암호분석 공격을 방지한다. 하지만 SSL 3.0은 부인봉쇄 서비스는 제공하지 않는다. 이는 특정 상위레벨 응용계층 프로토콜에서 구현해야 한다.

3.3 재현공격 방지 서비스

근본적으로 HMAC을 사용한다고 해도 공격자가 효력이 없는 패킷을 재현하는 것을 방지하지 못한다. SSL은 MAC데이터와 더불어 암시적인 순서번호를 사용하여 재현공격을 방지한다. 이러한 메커니즘은 또한 지연, 재순서, 혹은 데이터 삭제 등의 경우에 대처를 가능하게 한다. SSL에서 순서번호는 64비트이기 때문에 순서번호가 겹치는 문제는 발생치 않는다.

또한 순서 번호는 각 연결의 각 방향에서 독립적으로 유지하고 새로운 키 교환 시 재설정 되기 때문에 취약성은 없다.

IV. IPv6의 IPsec보안 메커니즘

IP계층(네트워크계층)에 보안메커니즘을 구현하면 기존의 보안 메커니즘이 적용된 응용뿐만 아니라 보안 메커니즘이 적용되지 않은 응용까지도 안전한 TCP/IP 네트워크를 사용할 수 있다. 이는 믿을 수 없는 시스템이 통신링크에 접근 방지를 위해 패킷을 암호화 하고 인증하여 이루어진다.

이를 위해 IPv6의 IPsec은 접근통제, 무결성, 메시지 원적지 인증, 재현공격 방지, 기밀성, 제한된 트래픽 기밀성 보장 등의 보안서비스 제공을 위해 제안 중인 보안 메커니즘이다[4].

1. 구조(Architecture)

상기의 보안 서비스들이 IP계층에서 이루어지기 때문에 상위 계층인 TCP, UDP, ICMP, BGP등의 전송계층 프로토콜이 이들 서비스를

사용할 수 있다. 즉, 이는 네트워크 계층 상위 모든 계층에 대해 보안서비스가 제공됨을 의미한다. 따라서 IPv6의 IPsec은 전송계층 이상의 모든 정보에 인증 및 기밀성 보안서비스를 제공한다.

이들이 제공하는 보안 서비스 형태를 보면 다음과 같다.

(1) 호스트와 호스트간 보안
(2) 호스트와 서브네트워크간 보안
(3) 서브네트워크과 서브네트워크간 보안

이들 모두는 암호화, 인증 혹은 이들의 조합으로 보안서비스를 제공한다. 즉, 호스트와 호스트간에 데이터 기밀성 서비스를 제공한다. 또한 서로 연동된 두 네트워크가 상호 작용할 경우 네트워크간에 데이터 기밀성 서비스도 제공한다. 이는 네트워크내에서 지연 및 컴퓨테이션 자원의 절약을 위해 데이터를 비 암호형태로 전송하고 서브네트워크을 떠나는 지점인 라우터에서 IP의 모든 패킷을 암호화하여 인터넷으로 전송할 수 있음을 의미한다.

이러한 관점에서 보면 IPv6의 보안메커니즘은 대부분의 네트워크 환경에 적용된다. 이는 네트워크가 적정하게 설계되고 외부세계로 명확하게 게이트웨이가 정의될 것을 요구한다.

이와 더불어 양측은 동일한 IP(V4, V6)가 지원되어야 한다.

2. SA(Security Association) 및 키 분배

먼저 SA는 IP에서 인증 및 기밀성 서비스 제공 전에 선행되어 이루어지는 송신자와 수신자간에 보안 협상이다. SA는 인터넷 목적지 주소와 SPI에 의해 유일하게 정의된다. 이는 다음과 같은 매개변수에 의해 정의된다[1].

- IP AH(Authentication Header)에 사용될 인증알고리즘 식별자와 알고리즘 형 그리고 사용되는 키.
- IP ESP(Encapsulation Security Payload)에 사용될 암호알고리즘 식별자와 알고리즘 형 그리고 사용되는 키
- 암호알고리즘의 IV(Initialization Vector) 혹은 암호 동기화 유무
- ESP변환에 사용된 인증 알고리즘 식별자와 알고리즘 형 그리고 인증 키
- 키의 유효시간 및 키 변경 시간
- 해당 SA가 유효한 시간
- SA의 소스 주소(들) : 이때 한 개 이상의 송신 시스템이 동일 SA를 공유하면 "*" (Wildcard)주소가 된다.
- 보호정보의 보안 등급

다음으로 IPv6의 키 분배메커니즘은 아직 정의되지 않는 상태이다. 따라서 키는 수작업 분배로 가정한다. 대형 네트워크에서 이는 거의 불가능한 작업이다. 따라서, IPv6 키 관리를 지원할 프로토콜과 암호화 기술이 개발중이다. 인터넷 키 관리 프로토콜(IKMP: Internet Key Management Protocol)이 응용계층 프로토콜로 지정될 것으로 보인다. 이는 하위 계층의 보안 프로토콜과는 무관할 것이다. 이는 공개 키 기반의 기술들을 지원할 것이고 Kerberos에서처럼 키 분배 센터(KDC : Key Distribution Center)를 지원할 것이다. IKMP는 트래프트 표준으로 고려하기 위해 1997년 3월 IESG(Internet Engineering Steering Group)에 제출되었다.

3. 사용된 암호알고리즘

IPv6는 암호화 알고리즘에 독립적이다. 이

는 암호알고리즘이 변경되거나 작은 키 길이 때문에 암호알고리즘이 취약할 경우 프로토콜이 더 강력한 알고리즘의 선택사용을 허용하기위한 것이다. IPv6는 인증에 키를 가진 MD5알고리즘과 128비트 해쉬값을 사용하고 암호화에 DES-CBC에 56비트 키 길이를 사용한다. IPv6는 양립성 때문에 DES-CBC 암호알고리즘을 기본으로 선택한다. 이들 암호알고리즘은 공격에 취약하다는 것이 현실적으로 알려졌다.

Weiner는 1만 달러 컴퓨터로 3.5시간마다 한 개의 키를 알아낼 수 있는 DES클래킹 컴퓨터 설계가 가능함을 보여주었다. 컴퓨터 H/W는 빠른 속도로 발전되기 때문에 상기의 알고리즘이 강력한 데이터 기밀성을 제공한다는 것은 현실적이지 못하다. 따라서, IPv6가 일반적으로 활용되는 시점에서 DES-CBC선택은 타당치 않다고 본다. 이들은 DES-CBC대신에 3-DES 사용이 좋지 않을까 생각한다. 3-DES가 더 많은 기밀성을 제공하고 미래의 공격에도 견고하게 견딜 가능성이 높기 때문이다.

4. 인증 서비스

Ⅱ장의 4절에서 인증해더의 형태를 보았다. 어떤 경우든 인증데이터는 전송 중에 변경이 가능한 부분(예, 홉제한 항목등)을 제외하고 전체 IP패킷을 대상으로 계산된다. 이때 변경가능 항목은 "0"으로 재설정하여 계산된다.

IPv6의 IPsec은 인증알고리즘으로 키를 가진 MD5를 제안하고 있다. 인증이 수행되는 과정을 보면 먼저 송신측에서 MD5 알고리즘이 송신측의 기밀 키와 IP패킷을 입력으로 받아 실행되고 이의 결과가 IP패킷에 삽입되어 전송된다. 수신측에서는 수신측의 기밀 키와 IP패킷을 입력으로 하여 송신측에서 행했던 것과 같은 동일한 계산이 이루어지고 이 결과를 수신된 결과와 비교하여 일치 여부에 따라 인증 및 무결성 유무가 검증된다.

IP의 인증 서비스는 여러 가지 방법으로 이루어 질 수 있다. 인증이 서버와 클라이언트간에 직접 이루어질 수 있다. 이때 클라이언트는 서버와 동일 혹은 다른 네트워크에 존재할 수 있다. 클라이언트와 서버가 동일한 기밀 키를 공유하면 인증은 안전하게 이루어진다. 또 다른 대안으로 원격 클라이언트가 상호 작용하는 방화벽시스템과 스스로를 인증할 수 있다. 이는 내부네트워크 전부를 접근하거나 요구된 서버가 인증기능을 갖지 못할 경우에 사용된다.

MD5는 128비트 해쉬값을 갖는다. 이는 MD5해쉬 값으로 텍스트를 발견할 수 있는 공격에 더 저항성을 높게 한 것이다.

IPv6의 IPsec은 네트워크계층에서 인증되기 때문에 여러 가지 네트워크 공격을 퇴치할 수 있다. 즉 호스트 가장공격과 IP 스누핑 공격 등을 퇴치할 수 있다. IPv6의 인증은 상위 계층 프로토콜과 더불어 최초 송신자 및 목적지 주소에 인증서비스를 제공한다.

5. 기밀성 보안 서비스

Ⅱ장 4절에서 ESP해더를 보았다. IPv6는 이를 사용하여 다음과 같은 2가지 모드의 IP 패킷 기밀성 서비스를 제공한다.

1) 전송모드 ESP(Encapsulating Security Payload) : 이 모드에서 전송계층의 세그먼트(예, TCP, UDP등의 세그먼트)만을 암호화 된다.
2) 터널모드 ESP(Encapsulating Security Payload) : 이 모드에서 IP패킷 모두가 암호화 된다.

ESP해더는 SA를 정의하는 32비트 SPI로 시작한다. 헤더의 나머지 부분은 사용될 암호

알고리즘에 종속된 매개 변수들을 가질 수도 있다(예, IV값 등). 일반적으로 헤더의 SPI 및 몇몇 매개변수를 포함한 첫 부분은 평문 형태로 전송되고 나머지 부분은 암호문 형태로 전송된다.

5.1 전송모드 기밀성 서비스

이 모드에서는 IP에게 운반된 TCP/UDP세그먼트를 대상으로 기밀성 서비스가 제공된다. 이들 세그먼트에는 응용데이터가 포함된다. 이때 ESP해더는 전송계층 헤더(TCP, UDP, ICMP등) 바로 앞에 놓인다[그림 5]. 기밀성 서비스 제공 절차는 다음과 같다.

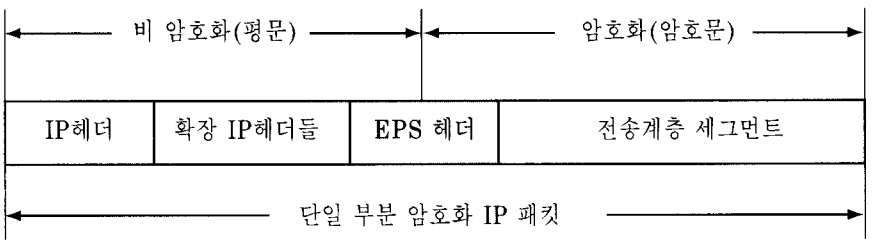

그림 5. 전송모드 IP 패킷

1) 송신측에서 ESP의 끝 부분과 전송계층 세그먼트로 구성된 데이터 블록을 암호화한다. 이 블록의 평문 부분은 전송동안 IP패킷을 형성하기 위해 암호문으로 대치된다.
2) 다음으로 이 패킷이 수신처를 향해서 발사된다. 중간 라우터는 IP헤더와 IP 확장 헤더(평문)를 검사하여 경로설정을 한다. 암호화된 부분에 대해서는 라우터가 아무런 작업을 하지 않는다.
3) 최종 목적지 수신측에서는 IP헤더와 IP 확장 헤더를 검사하여 자신에게 전송패킷임을 확인한다. 그리고 나서 ESP헤더내의 SPI의 내용을 기반으로 암호화된 전송계층 세그먼트를 복호화 한다.

이러한 방법으로 각각의 응용에 기밀성 서비스를 구현할 필요 없이 IP계층에서 일괄적으로 이를 제공할 수 있다. 이 모드의 약점은 전송된 패킷의 트래픽 분석공격에 취약하다는 점이다. 이는 IP 주소의 노출 때문이다.

5.2 터널모드 기밀성 서비스

이 모드에서는 IP가 IP 패킷 모두를 암호화하여 전송함으로써 전송모드의 단점(트래픽분석 공격)을 개선한 것이다. 이때 ESP해더는 IP패킷 바로 앞에 놓인다[그림 6].

IP해더가 최종 목적지 주소와 가능한 경로 방향 그리고 흡제한 정보를 가지기 때문에 단순히 ESP헤더에 의해 암호화된 IP패킷을 전송할 수 없다. 이는 중간 라우터가 이를 처리할 수 없기 때문이다. 따라서 트래픽 분석을 피할 수 있는 경로설정에 충분한 정보를 가진 "새로운 IP헤더"로 전 블록(ESP와 IP헤더 포함)을 인캡슐레이션 할 필요가 있다.

따라서 터널모드는 외부 네트워크 공격으로부터 안정적으로 네트워크를 보호하는 방화벽 시스템 혹은 기타의 보안 게이트웨이가 설치된 구성에 유용하다. 이 경우 암호화는 단지

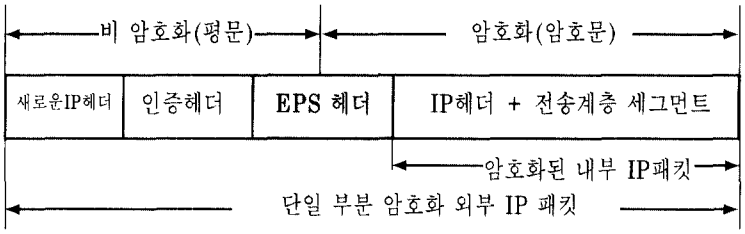

그림 6. 터널모드 IP 패킷

외부 호스트와 보안 게이트웨이 간에 혹은 두 보안 게이트웨이 간에 이루어진다. 이렇게 함으로써 내부 네트워크에 접속된 호스트들에게 암호화처리 부담을 줄이고 필요한 키 수를 줄여 키 분배 작업을 단순화할 수 있다. 이러한 방법으로 최종 목적지 트래픽 분석공격을 방지한다.

예를 들어 외부 호스트가 방화벽으로 보호된 내부네트워크내의 호스트와 통신하고자 할 겨우 터널 모드의 ESP는 다음과 같이 동작한다.

1) 송신측에서 최종 호스트의 IP주소로 내부 IP패킷을 만든다. 만들어진 이 패킷 앞에 ESP헤더가 놓이다. 그리고 나서 IP패킷과 ESP헤더 일부가 암호화된다. 다음으로 목적지가 방화벽 시스템의 IP 주소를 가지고 "새로운 IP헤더"를 만든다. 이로써 외부 IP패킷이 완성된다.
2) 1)에서 만들어진 외부 IP패킷이 목적지 방화벽 시스템에 발사된다. 중간 라우터는 새로운 IP해더와 확장 IP헤더를 검사하여 경로설정을 한다. 이때 암호화된 내부 IP패킷 에 대해서 라우터는 아무런 처리를 하지 않는다.
3) 목적지 방화벽 시스템은 "새로운 IP해더"와 확장 IP해더를 검사하여 자기에게 전송된 IP패킷임을 확인하고 ESP 헤더내의 SPI내용을 기반으로 내부 IP 패킷을 복호화 한다. 이로부터 최종 목적지 호스트 주소가 얻어진다. 이 내부 패킷이 방화벽 시스템으로부터 내부네트워크에 전송된다.
4) 내부 패킷은 내부네트워크에 접속된 라우터를 통해서 최종 목적지 호스트에 전달된다.

5-3. 병합 인증 및 기밀성 서비스

인증과 기밀성 둘 다를 병합한 서비스가 IP 패킷에서 이루어질 수 있다. 이는 "인증 전 암호화" 방법과 "암호화 전 인증"방법으로 분리된다.

1) 인증 전 암호화방법

이 방법은 사용자가 먼저 보호될 데이터에 ESP를 적용한다. 그리고 나서 인증헤더(AH)와 평문의 IP헤더를 그 앞에 첨가한다[그림7]. 이때 전송되는 전 IP패킷에 인증 알고리즘이 적용된다. 이에는 전송모드 ESP경우와 터널모드 ESP경우가 있다.

전송모드 ESP경우는 최종목적지에 운반된 전 IP페킷이 인증된다. 그리고 전송계층 세그먼트는 기밀성 메커니즘으로 보호된다.

터널모드 ESP경우는 외부 IP 목적지 주소에 운반되는 전 IP페킷을 인증한다. 인증은 목

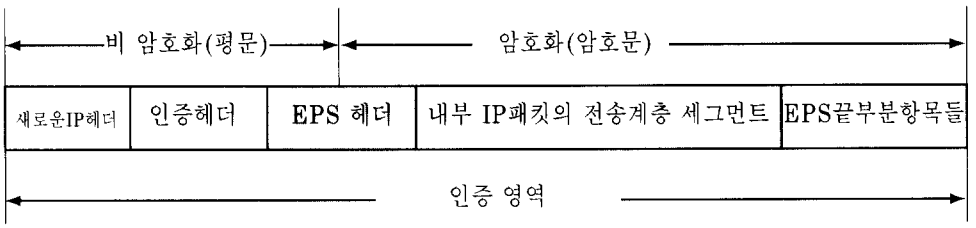

그림 7. 인증 전 암호화 방법(전송/터널모드)

적지 외부 IP주소에서 이루어진다. 전체적인 내부 IP패킷은 기밀성 메커니즘으로 보호된다.

2) 암호화 전 인증방법

이 방법은 ESP터널모드에 적합하다. 이 경우 인증헤더(AH)가 내부 IP패킷내에 놓이게 되고 이 내부 IP 패킷은 기밀성 메커니즘에 의해 보호된다.[그림8].

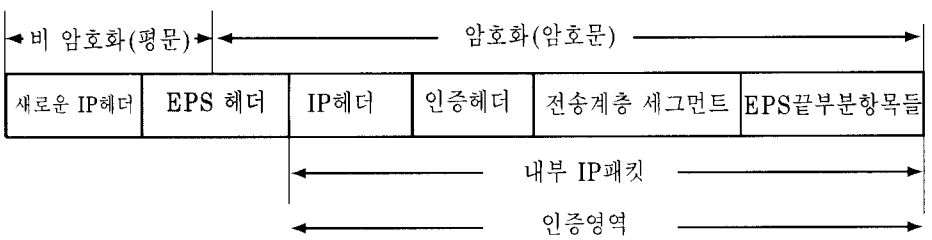

그림 8. 암호화 전 인증 방법(터널모드)

암호화 전 인증방법 사용은 다음과 같은 이유 때문에 유용하다. 첫째, 인증헤더가 ESP에 의해 암호화되기 때문에 인증헤더 변경 공격 및 전송되는 메시지의 가로채기 공격을 불가능하게 한다. 둘째, 후에 참조를 위해서 목적지와 메시지 정보를 인증헤더에 저장할 수 있다.

이는 인증정보가 비 암호화된(평문) 메시지에 적용되면 더욱 편리하다. 기타의 경우는 메시지가 인증정보의 검증을 위해서 재 암호화되어야 한다.

V. SSL과 IPv6의 IPsec의 보안 메커니즘 비교

상기에서 두 개의 보안메커니즘을 각각 검토한 내용을 정리하면 다음과 같다.

1) 첫째, SSL은 전송계층에 위치하고 IPv6는 네트워크계층에 위치하기 때문에 SSL은 현재 HTTP, NNTP, SMTP에게만 인증과 기밀성 보안서비스를 제공한다. 반면에 IPv6는 네트워크 계층에 전송되는 모든 패킷에 대해 IPv6의 모든 보안기능을 제공할 수 있다.
2) 둘째, SSL이 호스트와 호스트(대부분은 호스트와 서버)간에 보안서비스를 제공하지만 IPv6는 호스트와 호스트, 호스

트와 서브네트워크, 서브네트워크와 서브네트워크간의 인증 및 기밀성 보안서비스를 제공한다. 이는 IPv6가 LAN내의 패킷 암호화 작업에 추가적인 처리시간 부담 때문에 서브네트워크와 서브네트워크간을 기반으로 보안서비스 제공이 주류를 이룰 것으로 판단된다.

3) 셋째, IPv6에 키 교환 메커니즘은 아직 정의되지 않았다. 하지만 이는 IPv6의 보안 메커니즘이 일반적으로 사용된다면, 절대적으로 필요한 메커니즘이다. 네트워크에는 수 많은 호스트가 존재하기 때문에 수작업으로 키를 교환한다는 것은 매우 어려운 문제이다.

4) 넷째, IPv6와 SSL모두 개방되어 있고 어떤 인증 및 암호알고리즘에 종속성은 없다. 하지만 두 프로토콜 모두 표준 알고리즘으로 MD5와 DES-CBC를 사용한다. 이러한 암호체계는 상대적으로 적은 노력으로 깨질 수 있기 때문에 오늘의 표준으로서는 약한 측면이 있다. 다음 버전에는 표준암호화가 더 강화될 필요가 있다. 이는 표준 암호화는 3-DES(Triple DES)가 하나의 대안이 될 수 있다.

5) 다섯째, IPv6는 네트워크 계층에 위치하기 때문에 전 IP 패킷에 터널모드

표 1. IPv6과 SSL 의 비교분석

구 분		IPv6	SSL
구 조 (Architecture)		· 네트워크계층(3계층) · 모든 전송패킷(3계층)에 대해 보안이 가능	· 전송계층(4계층) · 제한된 프로토콜에서 인증과 비밀성 제공
사용형태		· host-to-host · host-to-subnet · subnet-to-subnet	· host-to-host
키 교환 (Key exchange)		· 네트워크 규모가 방대하므로 키 교환 메커니즘을 정의하기가 어려움 · IKMP(Internet Key Management Protocol)	· Sever 키 교환 메시지 · 클라이언트 키 교환 메시지 · secure WWW 기반
보안기술	암호문	· 암호문에 사용되는 암호알고리즘을 제한하지 않음 · DES(56 비트)	· 암호문에 사용되는 암호알고리즘을 제한하지 않음 · Fortezza(96 비트), IDEA(128 비트), RC2 (40 비트), RC4(40 비트, 128 비트), DES(56 비트), 3DES(168 비트)
	인 증 알고리즘	· Keyed MD5(128 비트) · 네트워크계층의 패킷을 인증 · 근원지와 목적지 주소에 대한 인증 제공	· MD5(128 비트) · 전송계층의 패킷을 인증
	기밀성	· Tunnel mode ESP · Transport mode ESP	· 전송 프로토콜 (HTTP, NNTP, SMTP)에 의존

ESP를 사용하여 인증과 기밀성 서비스를 제공할 수 있다. 이러한 능력은 호스트 가장과 IP스누핑과 같은 수많은 네트워크 공격을 방어할 수 있다.

6) 여섯째, 이 프로토콜 둘 다는 트래픽 분석공격을 제한적으로 방어한다. 하지만 IPv6의 경로배정 헤더가 교통량 분석 시도를 더 어렵게 할 수 있다.

이들을 구조, 사용형태, 키 교환, 적용된 보안기술 등을 중심으로 상호 비교하여 정리하면 표1과 같다.

VI. 결 언

위에서 분석한 바에 의하면 IPv6의 IPsec이 SSL 3.0보다 인증, 기밀성 그리고 트래픽 공격 방어 등의 보안서비스에 우수하다는 결론은 명확하다. 이는 IPsec이 네트워크 계층에서 그리고 SSL이 전송계층에서 동작함에 따라 얻어진 결과이다. 따라서 IPsec은 네트워크 계층 상위의 모든 정보에 대해 보안서비스를 제공할 수 있는 반면에 SSL은 정의된 포트의 응용에 대해서만 보안서비스를 제공한다.

하지만 IPv6의 IPsec은 보안서비스 제공에 기반이 되는 키 분배 메커니즘이 아직 정의되지 않고 있다. 이는 모든 계층에 키 분배 서비스를 제공해야 하기 때문에 응용계층에 구현될 것이라 예측한다.

IPv6와 SSL의 향후 전망은 IPv6가 여러 측면에서 장점이 있지만 가까운 미래까지는 현재의 상황이 계속되라 예상한다. 이는 SSL의 키 분배가 자신의 개인 키를 알지 못해도 보안서비스가 가능하기 때문에 인터넷 응용에 적합하기 때문이다. 따라서 SSL은 웹 브라우저 응용에서 계속 이용될 것으로 보인다.

IPv6의 IPsec은 현재 여러 기관에 프로토타입으로 구현되고 있다. 이는 SSL 2.0이 네트케이프 응용을 위해 구현되었을 때 취약점이 발견되어 SSL 3.0을 개선한 것과 같이 IPsec도 이를 반복할 개연성은 충분하게 있다.

IPv6의 IPsec이 인터넷에서 안전한 보안 서비스를 위한 표준이라고 생각할 수 있지만 이것이 100% 안전한 보안 서비스를 보장할 수는 없다.

〈〈 감사의 글 〉〉

본 논문은 '98학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 연구의 일부로 이에 감사를 드립니다.

참고문헌

[1] William Stallings, "IPv6 : The New Internet Protocol", IEEE Communications Magazine, July 1996

[2] D. Borman, "RFC-2147 : TCP and UDP over IPv6 Jumbograms", Network Working Group, May 1997

[3] Stephen A. Thomas, "Ipng and the TCP/IP Protocols", Wiley Computer Publishing, 1996

[4] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol , Internet Draft, draft- ietf-ipsec-arch-sec-04.txt , March 1998.

[5] David Wagner, Bruce Schneier, Analysis of the SSL 3.0 protocol, November 1996

[6] A. Freier P. Karlton P. Kocber, The SSL Protocol Version 3.0, Internet Draft, Netscape Communications Corporation, March 1996.

[7] Robert M.Hinden, IP Next Generation Overview, http://playground.sun.com/pub/ipng/INET-IPng-Paper.html,

May 14 1995

[8] S. Kent, R. Atkinson, IP Authentication Header , Internet Draft, draft-ietf-ipsec-auth-header-05.txt , March 1998.

[9] R. Atkinson, " RFC-1827 : IP Encapsulating Security Payload (ESP)", Network Working Group, August 1995

[10] S. Kent, R. Atkinson, IP Encapsulating Security Payload (ESP), Internet Draft, draft-ietf-ipsec- esp-v2-04.txt , March 1998.

[11] J Bradley and N Davies, Analysis of the SSL Protocol. Technical Report CSTR-95-021, Department of Computer Science, University of Bristol, June 1995.

[12] Adam Shostack, An Overview of SSL, May 1995 http://www.homeport.org/~adam/ssl.html

[13] J. Benaloh, B. Lampson, D. Simson, "Microsoft Corporation's PCT Protocol", October 1995, Internet draft, Work in progress.

[14] J Bradley, Master's thesis," The SSL Reference Implementation Project", Department of Computer Science, University of Bristol, October 1995.

[15] Mihir Bellare, Ran Canetti, Keying Hash Functions for Message Authentication, Crypto 96 proceedings, 1996

□ 著者紹介

조 인 준

1982년 2월 전남대학교 전자계산학과 졸업 (학사)
1985년 2월 전남대학교 전자계산학과 대학원 졸업(석사)
1997년 10월 ~ 현재 아주대학교 컴퓨터 공학과 박사과정 재학중
1990년 12월 정보처리기술사(전산 조직 응용)
1983년 9월 ~ 1994년 2월 한국전자통신연구소 선임연구원
1994년 3월 ~ 현재 배재대학교 컴퓨터 공학 교수
※ 관심분야 : 전산 조직응용 및 정보통신 Security

정 희 경

1993년 광운대학교 대학원 컴퓨터공학전공 (공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 조교수

※ 관심분야 : 하이퍼미디어/멀티미디어 문서정보처리, SGMI , XML, HyTime DSSSL

김 동 규

서울대학교 공과대학 졸업 (학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대학원 졸업 (Ph.D. 전산학 박사, 정보통신전공)
미국 Kansas 주립 전산학과 교수
1979년 3월 ~ 현재 아주대학교 컴퓨터 공학과 교수

※ 관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링 정보통신 Security , 분산처리 시스템