通信情報保護學會誌
第 8 卷 第 2 號, 1998. 6

네트워크 보안 기술 동향

권 현 조*, 김 학 범*, 홍 기 웅*

요 약

본 고에서는 광범위한 분산 망 환경에서 그 중요성이 점차 중요하게 부각되는 네트워크 보안에 대한 최신 기술 동향을 소개한다. 네트워크 보안은 개별적인 정보보호 서비스에 필요한 다양한 기술들이 복합적으로 구성되어 개발된다. 통신 프로토콜의 기본인 OSI 참조 모델에서의 보호 프로토콜, 현재 가장 많이 사용되어지고 있고 개발이 활발히 이루어지고 있는 응용인 전자 우편 보안 프로토콜, 그리고 인터넷 망의 데이터 흐름을 보호하고자 하는 VPN과 가장 관심이 많은 스위칭 기술인 ATM에서의 보안 고려사항 등을 고찰해 본다

1. 서 론

정보통신망에 제공되는 기본적인 정보보호 서비스로는 인증, 접근통제, 비밀보장, 무결성, 부인방지 등이 있고 이를 위한 보호메커니즘으로 암호화, 인증, 데이터 무결성, 트래픽패딩, 경로제어 등이 있는데 이러한 기술을 복합적으로 적용한 네트워크 보호프로토콜들이 개발되고 있다.

본 고에서는 현재 개발되어 상용화되거나 프로젝트의 일환으로 실용연구중인 보호프로토콜을 소개하며 이러한 보호프로토콜을 적용한 네트워크 보안 제품 중에서 TCSEC의 네트워크 해설 기준인 미국의 TNI(Trusted Network Interpretation of TCSEC)[1], 유럽의 ITSEC으로 평가된 제품목록을 수록하였다. 마지막으로 초고속통신망을 실현할 수 있는 ATM에 비밀성을 제공하려고 연구되는 기술과 VPN(Virtual Private Network) 기술을 소개하고 마지막으로 IPv6과 SSL(Secure Socket Layer)을 비교 분석하였다.

*한국정보보호센터

2. 정보통신망 보호프로토콜

2.1 OSI 참조모델과 보호프로토콜

정보통신망 보호를 위하여 OSI 참조모델에 따라 많은 보호프로토콜들이 개발되어 표준화되었는데 [표 1]에 나타내고 있다.

SILS(Standard for Interoperable Local area network Security) 표준안은 SILS 모델, 안전한 데이터 교환, 키관리(Key management) 프로토콜, 시스템 보안 및 관리 프로토콜의 4분

야로 구성되며 데이터 발신처 인증, 비밀보장, 비접속 무결성과 접근통제 서비스를 제공한다[2].

표 1. OSI 참조 모델에 따른 보안 프로토콜

OSI 계층	OSI 계층	OSI 계층
7계층	응용 계층 보안프로토콜 (Application layer security protocol)	S/MIME, SET, OTP, PEM, MOSS
6계층	표현 계층 보안프로토콜 (Presentation layer security protocol)	보안서비스를 제공
5계층	세션 계층(Session protocol)	보안서비스를 제공하지 않음
4계층	전송 계층 보안프로토콜 (Transport layer security protocol)	SP4(SDNS 프로젝트), SSL(Secure Socket Layer)
3계층	네트워크 계층 보안프로토콜 (Network layer security protocol)	SP3(SDNS 프로젝트), IPv6, IPSec
2계층	데이터링크 계층 보안프로토콜 (Datalink layer security protocol)	SILS(Standard for Interoperable Local area network Security) - SDE(secure data exchange), SDNS(Secure Data Network System)
1계층	물리 계층 보안 (Physical layer security)	전송되는 비트를 모두 암호화 (ISO 9160)

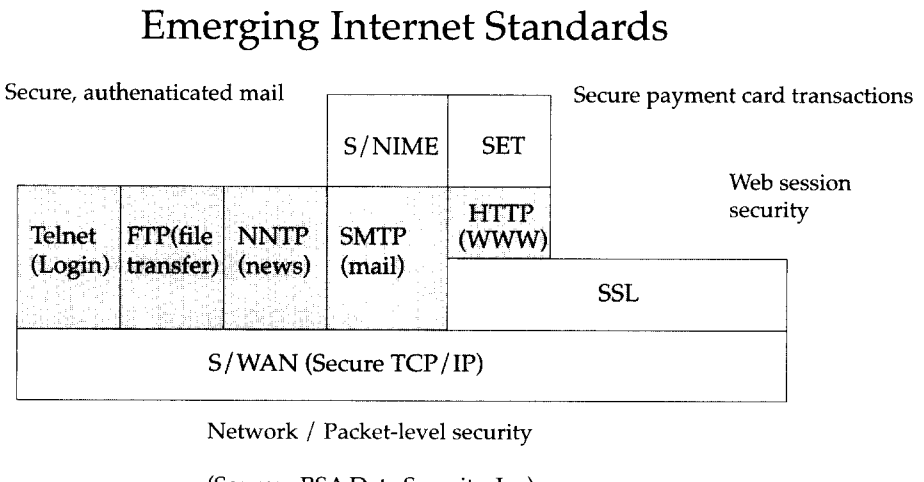

그림 1. 보안프로토콜의 계층관계

2.2 전자우편보안

인터넷이 우리생활과 밀접한 관계를 갖기 시작하면서 가장 큰 변화를 가져온 것중에 하나가 편지이다. 편지는 기본적으로 전달하는데 걸리는 시간을 고려하여야 하는 통신수단이었다. 하지만 통신기술의 발달로 인하여 인터넷이 전자우편이라는 서비스를 제공하게 되면서 이제 편지는 가장 빠른 전송수단으로 자리잡게 되었고 현재 인터넷을 사용하는 많은 이용자들에게 전자우편서비스는 보편화되었다. 통신망 보호기술이 발전하면서 전자우편에 대한 보안문제도 부각되었다. 보안관련 연구기관이나 업체들이 전자우편 보안기술을 연구하기 시작하였는데 이러한 보안기술을 적용한 전자우편 보안프로토콜로 대표적인 것은 X.400(1988), PGP, PEM 및 S/MIME 등이 있다.

2.2.1 X.400

X.400(ISO 10021-1)은 1984년 CCITT (International Telegraph and Telephone Consultative Committee, ITU-T의 전신)에 의해 발표되었고 인증, 메시지 무결성, 메시지 암호화 등 보안기능을 추가하여 1988년에 개정되었다. 새로운 X.400(1988)은 1993년 연구소에서 사용할 목적으로 런던대학과 Gesellschaft(독일)에서 각각 OSISEC와 SECUDE 프로젝트로 구현하였다. 또한 유럽에서는 시범적으로 PASSWORD 프로젝트에서 X.400을 적용하였고 미국에서는 DMS(Defense Messaging System) 개발과정에서 Secure X.400을 구현하였다. X.400은 MHS 보안을 위하여 안전한 접근관리와 안전한 메시지 처리 요구사항을 기술하고 있다[3]. 다음 (그림 2)는 X.400에서 보안기능이 실현되는 사항을 시나리오화 한 것이다[4].

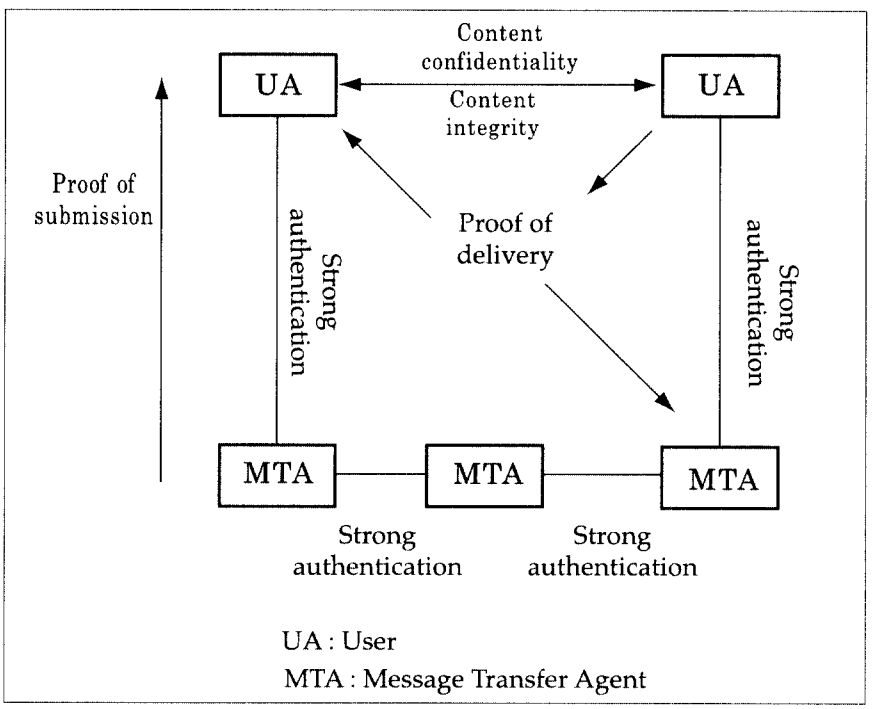

그림 2. X.400 보안 시나리오

2.2.2 PGP(Pretty Good Privacy)

PGP는 Boulder에서 컴퓨터 과학자로 일하던 필립 짐머만에 의해서 1991년에 개발되었다. PGP는 비상업용으로 개발되었으며 현재 저가의 상용제품과 공개용 버전이 나와있는데 국제용으로 PGP2.6.3i버전까지 나와있지만 이 버전은 신뢰성을 보장하지 못하고 있는 실정이다. 공개용 버전은 MIT 대학에서 비상업용을 전제로 개발된 것이며 공식적으로는 공개버전과 상업용 버전 모두 미국과 캐나다에서만 사용할 수 있고 UNIX버전만 국제용으로 다른 나라에서 사용할 수 있다[5]. PGP가 널리 사용되는 이유는 DOS, WINDOWS, UNIX, MAC 등 여러 기종에서 사용가능하고 PGP에서 사용되고 있는 알고리즘은 보안성이 높은 것들이며 넓은 활용분야를 가지고 있기 때문이다. PGP에서 사용되고 있는 알고리즘은 [표 2]와 같으며, 암호문의 구조는 (그림 3)과 같다.

표 2. PGP에서 사용되는 알고리즘

기 능	알고리즘
메시지의 암호화	IDEA, RSA
전자서명	RSA, MD5
압축	ZIP
전자우편 호환	Radix 64 conversion

2.2.3 PEM(Privacy Enhanced Mail)

PEM은 IETF가 개발한 전자우편 보안의 인터넷 표준인데 기존의 RFC 822에 비밀성, 송신자 인증, 내용무결성, 송신자 부인방지와 같은 보안서비스를 추가한 것이다. IETF는 PEM과 관련하여 Privacy Enhancement for

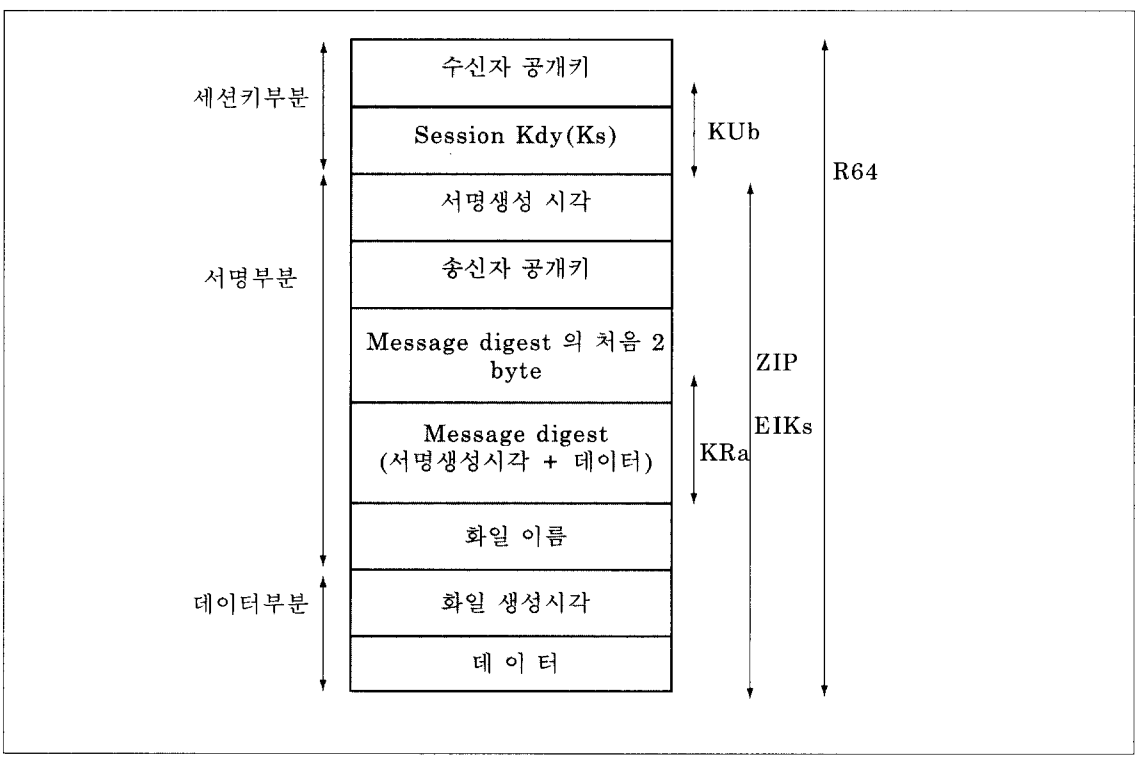

그림 3. PGP 암호문 구조

Internet Electronic Mail를 다음과 같이 네 부분으로 정의하고 있다.

- RFC 1421(Part Ⅰ) : Message Encryption and Authentication Procedures
- RFC 1422(Part Ⅱ) : Certificate-Based Key Management
- RFC 1423(Part Ⅲ) : Algorithms, Modes, and Identifiers
- RFC 1424(Part Ⅳ) : Key Certification and Related Services

PEM은 공개키 구조에서 RSA알고리즘을 사용하고 있고 PEM 키관리는 X.509 인증서(Certificates)와 인증구조(certification infrastructures)를 기반으로 이루어진다. 이 인증서로 메시지 송신자에게는 수신자의 공개키를 제공하고 수신자에게는 송신자의 공개키를 제공할 수 있도록 한다. 인증서는 PEM 메시지 헤더필드에 저장되어 전송되거나 더 일반적인 방법으로 디렉토리에 인증서를 저장하고 접근권한이 있는 사용자에게만 접근을 허용하여 공개키를 볼 수 있도록 한다. 다음 [표 3]은 PEM과 PGP를 비교한 것이다.

표 3. PEM과 PGP 비교[6]

구분	PEM	PGP
개발자	IETF	Phil Zimmermann
키인증방식	중앙 집중화된 키인증	분산화된 키인증
특 징	•인터넷 표준(안) •익명성이 제공되지 않음 •구현이 어려움 •보안성이 높음 •제한적사용(군사용, 금융계)	•응용프로그램 •익명성 제공 •구현의 용이성 •PEM에 비해 보안성이 낮음 •실세계 사용중심(널리 이용됨)

보안기능이 전자우편에 추가되면서 여러 가지 프로토콜이 개발되어 표준화가 추진되고 있는데 기존의 전자우편 프로토콜을 확장한 개념으로 PEM-MIME, MOSS(MIME Object Security Standard), S/MIME 등이 있다. MIME(Multi-purpose Internet Mail Extensions)은 원래 SMTP mail에 멀티미디어 데이터를 처리하도록 전자우편을 확장한 것인데 RFC 1341, 1342로 표준화되었다. 1994년 초반에 PEM과 MIME을 통합하기 위한 제안이 있었는데 그 하나는 1993년 제안된 "MIME-PEM Interaction"[7]이고 다른 하나는 "An Alternative PEM MIME Integration"에서 Schiller, J 가 제안한 것이다. 이 두가지 제안이 서로 다른 방향을 제시하였는데 "MIME-PEM Interaction"에서는 PEM에서 제공되는 각각의 기능을 MIME내에서 구현하는 방법으로 PEM-MIME에 접근하였고 "An Alternative PEM MIME Integration"[8]에서는 PEM, MIME을 근본적으로 변화시키지 않고 두 개 프로토콜을 합하는 방식으로 접근하였다.

2.3 네트워크 보안제품 평가

[표 4][표 5] 미국의 TNI와 유럽의 ITSEC으로 평가된 네트워크 보안제품 목록이다.

표 4. 미국의 네트워크 보안제품 평가목록

제 품 명	등급	업 체 명	날 짜
MLS LAN	A1	Boeing Company	'94.8.15
Gemini Trusted NetworkProcessor	A1	Gemini Computers, Inc.	'94.9.6
VSLAN 5.0	B2	Verdix Corporation	'90.8.22
VSLAN/VLSANE 5.1	B2	General Kinetics Inc.	'94.1.11
VSLAN/VLSANE 6.0	B2	General Kinetics Inc.	'95.7.20
Trusted UNICOS 8.0	B1	Cray Research, Inc	'95.3.9
CX/SX with LAN/SX 6.1.1	B1	Harris Computer System Corporation	'93.9.15
CX/SX with LAN/SX 6.2.1	B1	Harris Computer System Corporation	'93.9.18
NetWare 4 Network System Architecture & Design	C2	Novell, Incorporated	'97.10.7
NetWare 4.11	C2	Novell, Incorporated	'97.10.7
Cordant Assure EC 4.11	C2	Novell, Incorporated	'97.10.7

표 5. 영국의 네트워크 보안제품 평가목록

제 품 명	등급	업 체 명	날 짜
Gauntlet Internet Firewall	E3	Trusted Information System(UK) Ltd	'97.8
VINES	E2	Banyan Systems Incorporated	'97.4
CyberGuard Firewall	E3	CyberGuard Europe Ltd	'97.3

2.4 네트워크 보안기술 동향

2.4.1 초고속정보통신망을 위한 ATM 보안기술

세계각국의 네트워크 개발자들은 더 빠른 통신속도, 더 높은 신뢰성의 요구를 충족시키기 위하여 정보통신망을 점점 발전시켜 왔다. 최근 부각되고 있는 B-ISDN(광대역종합정보통신망)에 적용될 수 있는 스위칭기술로 최근 세계적으로 관심을 끌고 있는 기술이 ATM(Asynchronous Transfer Mode)이다.

ATM은 기본적으로 기존의 프로토콜 트래픽 단위인 패킷이 아닌 셀(cell)이라는 새로운 단위로 통신을 하며, ATM 프로토콜 참조모델은 ITU-T에 의해 개발된 표준안에 기초하고 있다.

보안개념 인식에 대한 증가로 네트워크 개발에 있어서 가장 중요한 요소로 보안서비스의 제공여부를 고려하여야 하는데 ATM 구조는 (그림 4)에서와 같이 OSI 참조모델과는 다르기 때문에 OSI 참조모델을 기본으로 개발되었던 보호서비스를 ATM망에 그대로 적용시킬 수가 없다. 따라서 ATM망에 적합한 보호기술을 개발하여야 하는데 이를 위하여

ATM포럼에서는 1995년 6월에 Security Ad Hoc을 설립하였고 1995년 12월에 보안작업그룹(Security Working Group)으로 개편하여 독립시켰고 현재는 이 단체를 통해 ATM 보안 규격 개발작업을 수행하고 있다.

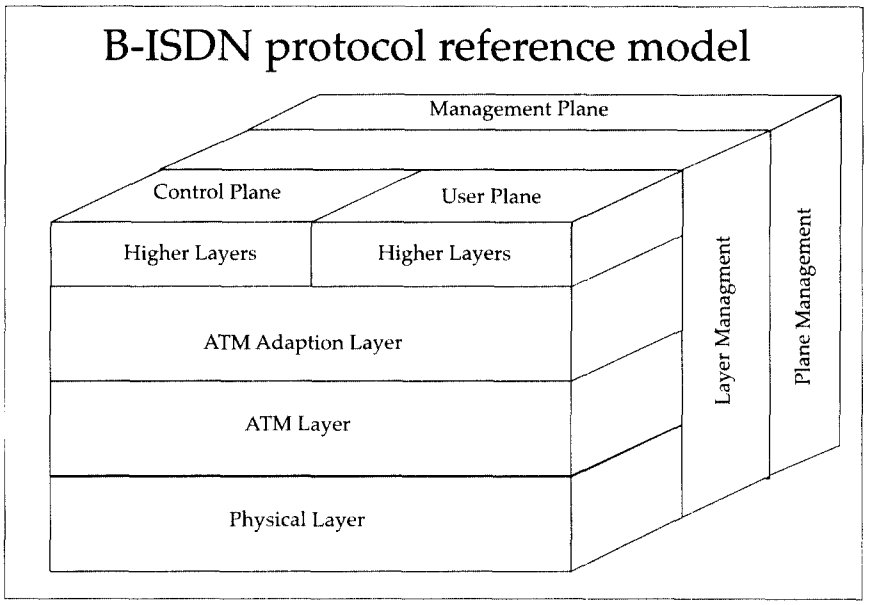

그림 4. ATM 구조

ATM망을 위한 보안구조로 제안된 3가지 방법을 [표 6]으로 나타내었다. 표에서 설명되는 바와 같이 ATM망에 보안기능을 추가하기 위한 연구가 다각적으로 이루어지고 있는데 보안기능을 구현하는 계층에 따른 장단점을 분석하여 보안기능을 구현하는데 가장 적합한 계층을 알아내기 위한 연구가 국내에서도 활발히 진행되고 있다.

2.4.2 VPN 기술개발

1) VPN의 데이터 전송모드

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 네트워크망이라는 취약점으로 전자상거래, EDI등이 실제로 확산되기가 어려웠다. 인터넷으로 흐르는 정보를 보호하기 위한 방법들이 연구되었고 그 중 해결책으로 제시된 것이 VPN(Virtual Private Network)이다.

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 또다른 방법에서는 데이터의 일부분만을 암호화하여 전송한다.

표 6. ATM 보안구조

제안자	특 징	단 점
Stevenson[9,10]	•링크레벨 •key agility기능을 하드웨어로 구현 •동기 셀사용(손실된 셀을 단일한 암호체인으로 한정) • ATM LAN과 ATM WAN사이에 보안게이트웨이로 적합 • 전송되는 모든 데이터의 암호화로 인한 트래픽 비밀성 제공	• 동일 스위치에 연결된 종단 시스템간의 공격이 가능 • 물리계층에서 데이터를 암호화하므로 부하가 생김 • 라우팅을 위해 스위칭노드에서 복호화하여야 하는데 이과정에서 메시지 무결성이 보장 안됨
Deng[9,11]	• 통제영역과 사용자 영역으로 구분 •보안관련기능 제공 - 통제영역 • DPL(Data Protection Layer) - 사용자 영역 - AAL계층의 SAR부분에 위치	• AAL TYPE 1, 2, 3/4, 5의 각 형태별로 구현이 필요함 • 동기 클럭을 유지 - Timestamp 사용
Chuang[9,12]	•ATM계층 • AAL5의 PDU토큰 이용하여 다음 블럭의 데이터를 암/복호화	• 동기화를 하는 계층과 암호화하는 계층을 분리 • 하위계층이 상위계층의 PDU 구조를 이해하여야 함

VPN을 통해 데이터를 전송할 경우 네가지 전송모드가 존재하는데 이를 [표 7]과 (그림 5)로 나타내었다.

2) Worldwide VPN

각국의 암호정책에 따라 VPN에 적용할 수 있는 암호비도에 제약이 가해진다. 따라서

표 7. VPN의 전송모드

전송 모드	특 징
In Place Transmission Mode	• 암호화 : 데이터 • IP 헤더
Transport Mode	• 암호화 : 데이터 • IP 헤더 + IPSec 헤더 • VPN 노드간에 데이터 비밀성 보장
Encrypted Tunnel Mode	• 암호화 : IP 헤더 + 데이터 • New IP 헤더 + IPSec 헤더
Non-Encrypted Tunnel Mode	• 전송데이터를 암호화하지 않음 • New IP 헤더

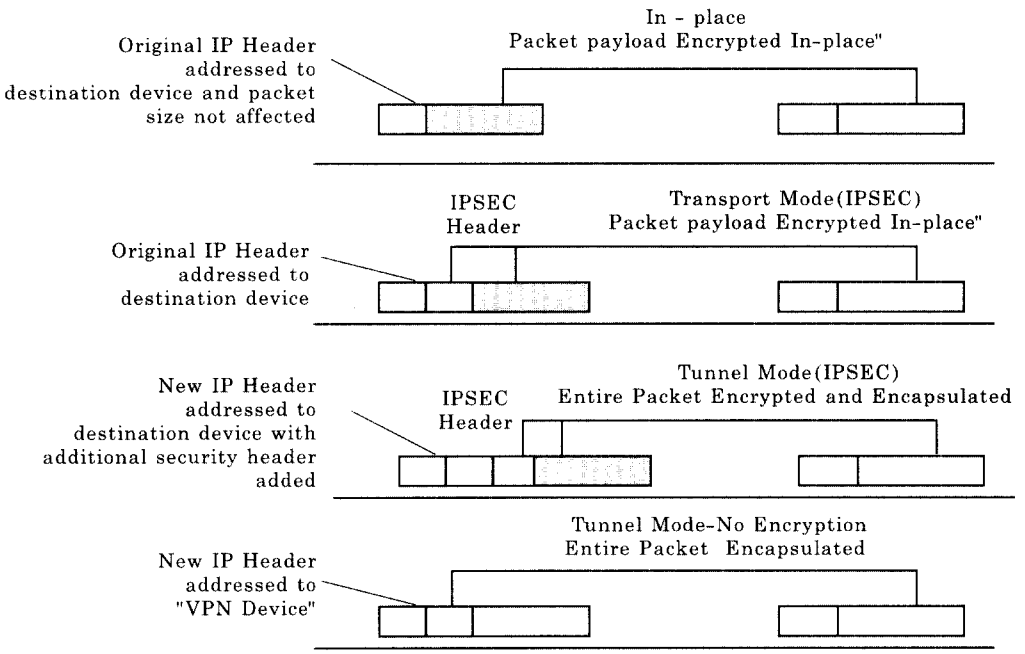

그림 5. 암호화 및 비암호화 전송 모드

VPN을 전세계에 걸쳐 구성하는데는 암호비도 차이로 인한 문제가 발생하게 된다. 예를 들어 (그림 6)에서와 같이 샌프란시스코, 뉴욕 및 런던을 거치는 통신은 VPN을 통해 56비트 암호기술을 사용하지만 런던에서 홍콩을 거쳐 샌프란시스코로 이어지는 통신은 40비트의 암호기술을 사용하여야 한다. 만약 VPN이 다중 암호기술을 지원할 수 없다면 비도가 약한 암호알고리즘 사용으로 인해 데이터의 비밀성이 더 쉽게 깨질 수 있는 악영향이 발생하게 된다. 이러한 문제를 해결하기 위해서 VPN은 암호, 인증, 접근통제에 관한 다양한 기술을 다룰 수 있어야 하므로 이를 개선하려는 노력이 진행되어오고 있다.

VPN의 주목할만한 발달로 VPN내에 적용되는 특정서비스나, 응용프로그램에 대해 암호기능을 선택적으로 사용할 수 있게 하였다. 예들 들면, 협력사들이 제품에 관한 일반정보를 전송하기 위한 데이터는 암호화할 필요가 없지만 제품개발에 관련한 중요정보를 전송할 경우에는 데이터의 암호화기능을 필요로 하게 된다. 이처럼 VPN을 이용하여 네트워크를 구성하더라도 전송되는 데이터를 항상 암호화할 필요는 없기 때문에 암호기능을 선택적으로 사용할 수 있도록 유연성을 두고 있다. 접근통제기능과 암호기능(선택)을 결합한다면 사용자는 암호화된 특정세션을 설정하여 VPN 응용계층으로 직접 연결할 수 있다. 이로써 네트워크 보안과 더불어 전송되는 데이터의 안전성까지 보장받을 수 있다[13].

3) 표준 VPN을 위한 노력 - IETF IPSec

인터넷보안을 다루는 IETF의 IPSec working group은 VPN 통신에 관련되는 보안기능을 고려하여 IP 패킷을 전체적으로 정의하고 있는데 다음 두가지가 패킷에 포함되는 보안관련 필드이다. (그림 7)은 IPSec이 정의

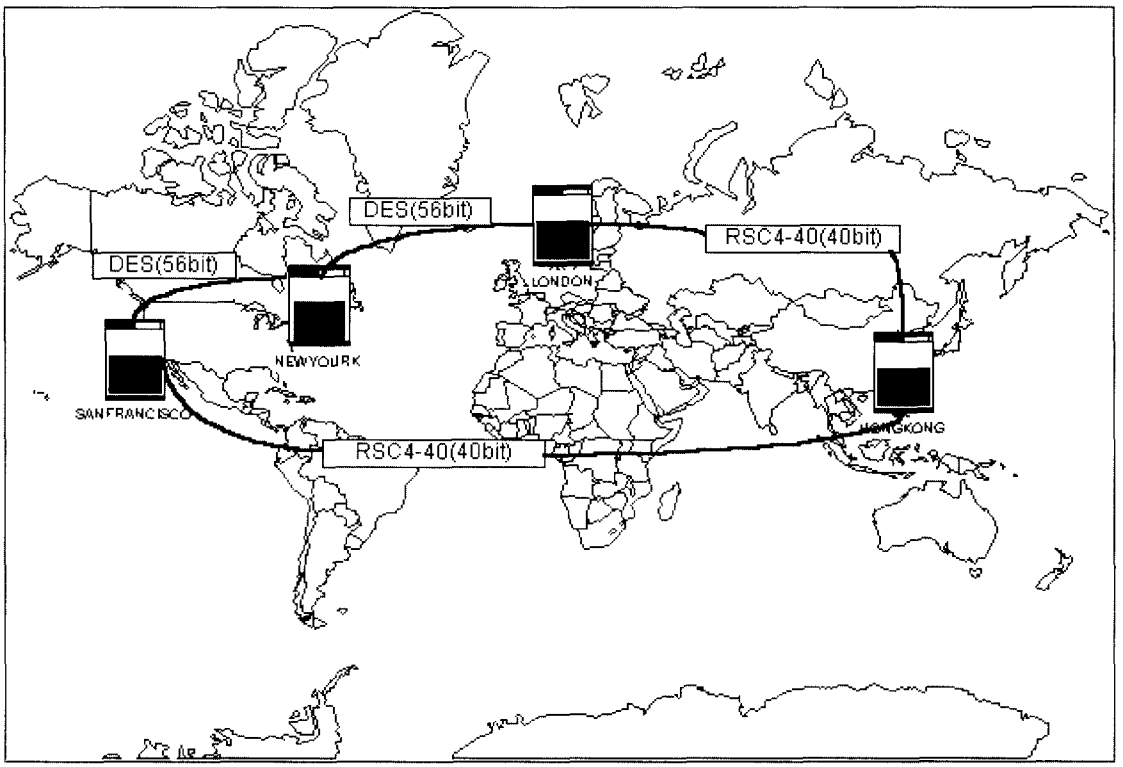

그림 6. Worldwide VPN 적용 예

한 인증헤더 패킷구조를 나타내고 있으며 [표 8]에서는 보안관련 필드인 AH와 ESP의 차이점을 보였다.

- AH(Authentication Header) : 전체 IP 데이터그램에 대한 비접속 무결성과 데이터 인증

표 8. AH 무결성과 ESP 무결성의 차이점

AH	ESP
데이터 무결성 제공	데이터 무결성 및 암호 제공
패킷 전체를 인증	IP 헤더는 인증하지 않음
AH 필드내에 메시지 다이제스트 포함	AH 패킷 마지막 부분에 메시지 다이제스트를 추가 삽입

- ESP(Encapsulation Security Payload) : 사용자가 적용하는 암호알고리즘을 허용하는 IP 데이터그램으로 인증과 암호제공

IP 계층 서비스(헤더인증 및 payload encapsulation), 전송/응용계층 서비스 및 세션결정 트래픽의 자체보호 등 다양한 네트워크 보안서비스를 제공하는데 필요한 모든 정

보를 SA(Security Association)가 가지고 있으므로 데이터를 전송하기 전에 VPN 노드간(게이트웨이 또는 클라이언트)에 SA(Security Association)를 결정하여야 한다. 이들 형식은 독립적인 전송키와 인증데이터에 대한 일관된 구조를 제공하는데 이러한 구조는 암호기능을 위해 사용되는 메커니즘(암호알고리즘, 인증메커니즘, 키생성)에 독립적이어야 한다. 따라서 IPSec working group은 SA와 패킷구조를 표준화하여 데이터 전송레벨에서 상호연동할 수 있는 VPN을 활용하도록 노력하고 있다.

IP 보안표준은 아니지만 IPSec 표준과 비교될만한 VPN 기술들은 OSI 참조모델의 계층2에서 터널링 프로토콜(tunneling protocol)을 제공하는데 [표 9]에서 이들 프로토콜의 특징을 요약했다.

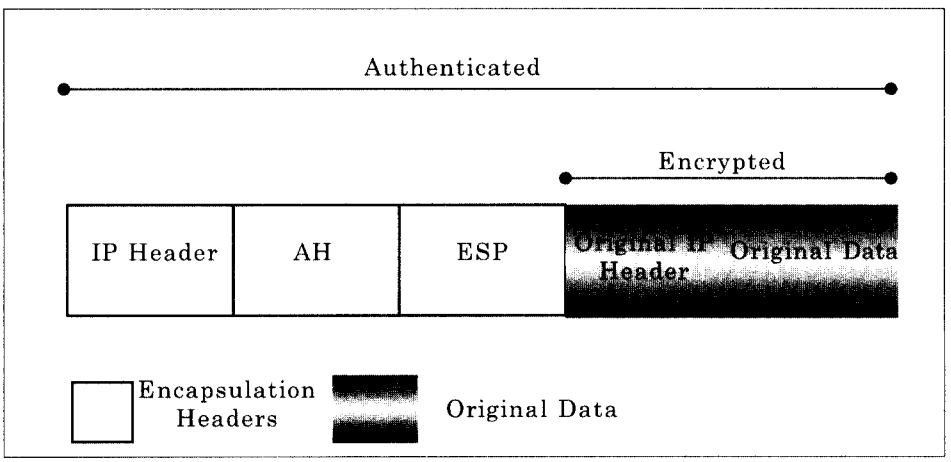

그림 7. IPSec AH 패킷 구조

표 9. VPN에 적용되는 프로토콜

터널링 프로토콜	특 징
PPTP(Point to Point Tunneling Protocol)	• PPP의 확장 • IP패킷에서 IP, IPX 또는 NetBEUI를 캡슐화 • ISP(Internet Service Provider) 장비를 이용 • end-to-end, server-to-server • 독자적인 암호메커니즘 제공(선택사양)
L2F (Layer 2 Forwarding)	• tunnel higher level protocols into a link layer protocol • remote dial • L2F 트래픽은 암호화되지 않음
L2PT (Layer 2 Tunneling Protocol)	• 다양한 네트워크(예, IP, SONET, ATM)를 하부구조로 하는 PPP 트래픽을 전송하는 프로토콜 • POP(Point of Presence)를 위한 다중 프로토콜 dial-up 서비스 제공 • 기본적으로 암호메커니즘을 제공하지 않음 • 현재 데이터의 비밀성을 제공하기 위해 IPSec 프로토콜에 L2PT를 적용시키려는 초안을 마련

Socksv5	proxy based VPN IETF 프로토콜 상호연동성이 없음

2.4.3 차세대 인터넷 프로토콜

1) IPv6(IPng)

IPv6의 특징은 크게 세가지로 구분된다. 첫번째 IPv6의 가장 큰 특징은 기존에 IPv4가 가지고 있던 제약사항을 수정하여 128비트의 주소체계로 인터넷상에서 광범위한 주소공간을 제공하는 것이다. 이러한 숫자는 매 초마다 10억대의 컴퓨터를 인터넷에 연결할 수 있다. IPv4는 등급별 주소체계(A, B, C, D)를 가지고 있어서 주소공간의 낭비를 초래하였는데 IPv6은 이를 개선하여 사용자에게 적합한 유형을 정의하여 유연성 있는 주소체계를 제공하고 있다. 이런 유형으로 인터넷 개인 사용자를 위한 유니캐스트(unicast), LAN을 사용하는 기업형 사용자를 위한 애니캐스트(anycast), ISP와 같은 서비스 사업자를 위한 멀티캐스트(multicast)가 있다. 두 번째 특징으로 멀티미디어 데이터를 실시간 처리가 가능하도록 각기 다른 대역폭에서 비디오 데이터를 무리 없이 처리할 수 있도록 대역폭을 확보하는 기능을 지원한다. 마지막으로 IPv6을 지원하는 패킷형식 중 인증헤더(AH)와 Encapsulating Security 헤더에서 보안관련(SA) 필드를 정의하므로써 기존에 IP 프로토콜이 가지고 있던 보안문제를 해결하였다. IPv6은 비밀성을 제공하기 위하여 두가지 모드를 제공하고 있는데 다음과 같다.

- Tunnel mode ESP : IP헤더를 포함한 IP 데이터그램을 암호화하여 새로운 IP 데이터그램을 생성한다. 라우팅을 위해 추가되는 중요정보는 암호화되지 않은 채로 IP헤더와 ESP사이에 저장된다.
- Transport mode ESP : payload 필드만을 암호화한다. IP헤더와 IP선택 필드는 암호화되지 않으며 패킷을 라우팅하는데 사용된다.

Tunnel mode는 LAN에 사용되어 암호화되지 않은 트래픽을 흘려보내면 IPv6의 게이트웨이는 IP패킷을 암호화한다. 이로써 패킷내용에 관한 정보를 얻으려고 하거나 IP트래픽을 분석하려고 하는 불건전한 의도를 가진 자가 이 패킷의 발신지와 목적지 주소를 알아낼 수 없도록 한다. IPv6에서 키교환 프로토콜로 제안되고 있는 IKMP(Internet Key Management Protocol)이 있지만 실제로 네트워크의 방대함으로 인해 키교환을 위한 프로토콜을 개발하는 것이 쉽지 않다. IKMP도 네트워크계층을 기반으로 하는 것이 아니라 응용계층 프로토콜에서 이루어지는 것으로 하위계층의 보안프로토콜에 독립적으로 적용될 것이다. IKMP는 Kerberos를 이용한 KDC(Key Distribution Center)가 공개키를 제공하도록 되어 있다. 1997년 3월에 IKMP를 표준초안으로 IESG에 제출하였다[14].

2) IPv6과 SSL 비교 분석

일반적으로 SSL보다 IPv6 프로토콜의 인증과 비밀성 기능이 더 뛰어나다. SSL은 전송계층이므로 단지 포트번호를 사용하여 프로토콜에서 인증과 비밀성만을 제공하지만 IPv6은 네트워크계층에 자리잡고 있어 상위계층의 모든 패킷에 대해 인증과 비밀성을 제공할 수

있다. 그러나 Netscape사가 SSLRef를 개발하여 SSL을 실제로 구현한 사례가 있으나 IPv6은 현재로서는 여러 연구기관들이 프로젝트로만 구현을 하고 있는 실정이다. IPv6 구현에 가장 큰 문제점으로 부각되고 있는 것이 키교환 메커니즘이다.

인터넷 망이 워낙 방대하므로 네트워크 계층에서 키교환을 구현하는 것이 쉽지 않아서 실제로는 응용계층에서 개발되고 있다. 다음 [표 10]은 IPv6과 SSL을 비교한 것이다.

표 10. IPv6과 SSL 의 비교분석

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

5. 결 론

정보통신망을 기반으로 하는 생활권의 변화를 받아들이기 위해 국가차원에서든 개인차원에서든 다방면으로 노력하는 가운데, 네트워크 개발자들은 이런 변화에 발맞춰 네트워크의 사용 용도를 다각화하기 위해 광범위한 분야에서 연구·개발을 진행하고 있다.

네트워크 분야에서도 최근 가장 크게 요구되어지는 부분은 네트워크 보안이다. 네트워크 보안은 단순히 한 응용에 대한 보안 기술만이 아닌 다양한 기술의 복합으로 이루어지고 있다. 이미 미국에서는 정보보호에 대한 인식을 토대로 '80년대 TCSEC을 개발하였고 이를 기반으로한 TNI를 개발하여 네트워크 보안제품 평가를 시행해오고 있으며 유럽에서도 ITSEC의 평가기준을 마련하여 네트워크 보안제품을 평가해오고 있다. 국내에서도 침입차단(Firewall)시스템 평가기준[15]을 개발하여 현재 평가가 진행 중에 있다.

이와 같이 보안에 대한 인식의 확대로 네트워크 분야에서도 정보보호기술 서비스를 적용하여 전자상거래, CALS, EDI 등의 구현을 실현가능하게 하고 있다. 인터넷에서 가장 많이 사용되어지고 시급하게 요구되는 전자우편 보안 프로토콜은 전 세계적으로 매우 활발하게 개발 및 표준이 이루어지고 있다. 또한 인터넷상에서 노출되는 정보의 보호가 필수 사항인 전자상거래나 EDI 등의 서비스 저변 확대를 위해 생긴 VPN(Virtual Private Network)은 다양한 연구팀에서 연구, 개발되는 프로토콜이다. 이처럼 다양한 네트워크 보안기술의 발달과 노력은 차세대 인터넷 프로토콜에도 영향을 미쳐 보안기능을 추가한 IPv6에 관한 개발이 활발해지고 있으며 최근 전자상거래를 위한 보안프로토콜로 SSL이 많은 관심을 불러일으키고 있다.

이제는 새로운 네트워크 기술 개발에 보안을 고려하지 않을 수 없게 되었다. 선진국에서 진행되고 있는 네트워크 보안에 대한 최근 기술 동향을 분석하고 참조하여 현재 국내 기술 개발에 대한 방향성을 제시할 뿐만아니라 보안기술과 이들이 적용되는 분야를 일반인들이 이해할 수 있도록 간결하면서도 정확한 정보를 전달하고자 하는 노력도 함께 기울여야 하겠다.

참 고 문 헌

[1] National Computer Security Center, *Trusted Network Interpretation of The TCSEC*, NCSC-TG-005, Jul., 1987.

[2] 김학범, 이철원, 홍기웅, 심주걸, "국내외 정보보호관련 표준화 동향" 정보과학회지 제 15권, 제6호, pp. 30 ~ 39, 1997. 6.

[3] 조인준, 김학범, 홍기웅, 김동규, "캐스케이드 취약성 방지를 위한 MHS 접근통제 정책 설계 한국통신정보보호학회 논문지 제7권, 제3호, pp. 117 ~ 128, 1997. 9.

[4] Daniel J. Blum, "The E-Mail Frontier" pp 237, 1994.

[5] http://esperosun.chungnam.ac.kr

[6] http://md.sicc.co.kr/academy/solutions/misc

[7] Crocker,S., N.Freed, and J.Galvin, "MIME-PEM Interaction" Internet Draft〈draft-itef-pem-mime-03.txt〉, 1993.

[8] Schiller, J., "An Alternative PEM MIME Integration" Internet Draft〈draft-itef-pem-mime-ALTERNATIVE-00.txt, .ps〉, 1993.

[9] 신효영, 유황빈, "ATM 방식의 고속 통신망에서 비밀성 보장을 위한 구조와 암호 알고리즘에 관한 연구" 한국통신학회 논문지 제23권 제1호, 1998.

[10] Daniel Stevenson, Nathan Hillery, and Greg Byrd, "Secure communication in ATM Networks", Communication of the ACM, Vol.38, No.2, pp 46-52, February 1995.

[11] Robert H. Deng, Li Gong, Aurel A. Lazar, "Securing Data Transfer In

Asynchronous Transfer Mode Networks", IEEE GLOBECOM'95, 1995.

[12] Shaw-Cheng Chuang, "Securing ATM Networks", 3rd ACM Conference on Computer and Communication Security, pp 19-30, March, 1996.

[13] Checkpoint Software Technology Ltd, *Virtual Private Network Security Components, March 23, 1998.*

[14] Reto E. Haeni, The George Washington Univ. Cyberspace Policy Institute, "IPv6 security in comparison to SSL" January, 1997.

[15] C. W. Lee, K. Y. Hong, H. B. Kim, J. G. Sim, "Development of Security Evaluation Criteria for Firewall in Korea", 10th Annual Canadian Information Technology Security Symposium, Ottawa Congress Center, Ottawa, Canada, pp. 107 ~ 121, 1 - 5, June, 1998.

□ 著者紹介

권 현 조

1997년 2월 성균관대학교 정보공학과(학사)
1998년 3월 - 현재 성균관대학교 정보통신대학원 재학중
1997년 1월 - 1997년 7월 (주)나라계전 연구소, 연구원
1997년 7월 - 현재 한국정보보호센터 연구원

※ 주관심분야 : 정보보호시스템 평가체계, 네트워크 보안, 전자서명

김 학 범

1988년 2월 경기대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산학과(석사)
1996년 3월 - 현재 아주대학교 대학원 컴퓨터공학과 박사과정 재학중
1991년 10월 - 1996년 6월 한국전산원 주임연구원
1996년 7월 - 현재 한국정보보호센터 선임연구원

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호 표준화

홍 기 웅

1985년 2월 전남대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산과(석사)
1994년 4월 정보처리기술사
1996년 2월 아주대학교 컴퓨터공학과(박사)
1985년 9월 - 1995년 10월 한국전자통신연구소 선임연구원
1992년 - 1993년 이태리, Alenia Spazio사 Senior Researcher
1995년 10월 - 1996년 4월 한국전산원 선임연구원
1996년 4월 - 현재 한국정보보호센터 책임연구원, 평가체계팀장/기술표준팀장

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보시스템 위험분석 · 평가, 정보보호 표준화