인터넷에서 정보보호 프로토콜 분석

김 상 춘* · 권 기 현*

요 약

인터넷이 발전해감에 따라 사이버 세계라고 하는 또 다른 세상이 창출되었다. 그러나 정보보호의 취약성 때문에 인터넷 서비스를 이용하는 사용자들의 안전성이 보장되지 않는다. 이처럼 불법 침입자들로부터 선의의 이용자를 보호하기 위해한 대응책을 숙지해야 할 것이다. 인터넷 기술의 발달에 따라 인터넷을 통하여 일반 사용자들도 이러한 정보들에 손쉽게 접근할 수 있게 됨으로 인해 인터넷에 대한 정보보호 문제는 더욱더 중요한 과제로 부각되고 있다. 이 논문에서는 인터넷 환경에서 정보보호 문제를 해결하기 위해 개발된 정보보호 프로토콜에 대하여 분석하는데 그 목적이 있다.

An Analysis of Security Protocol in Internet

Sang Choon Kim* · Ki Hyeon Kwon*

ABSTRACT

The development of Internet has created a new world called the Cyber world. However, because of the weakness in the security service, Internet service users still reluctant to use Internet to accomplish high value business transactions. To overcome this situation we must develop various security services so that the Internet service users can use any services freely. As the development of Internet, the corresponding technologies are available for the general public and this makes the security services more important than ever before. In this paper, we analyze the security protocols that are supposed to solve the Internet security problems.

* 삼척대학교 정보통신공학과

1. 서 론

수백만 대의 컴퓨터가 상호 연결되어 전 세계적으로 수천만의 네티즌들이 사용하고 있는, 현존하는 세계 최대의 정보 통신망인 인터넷은 그 규모에 걸맞게 "정보의 바다"라고 한다. 이처럼 거대한 인터넷은 아직도 그 성장이 멈추지 않고 있으며, 21세기 정보화 사회에 있어서 정보와 통신이 결합되어 움직이는 명실상부한 "정보화 사회의 기반 구조"가 될 것이 확실하다.

그러나 이러한 정보화 사회는 긍정적인 측면과 부정적인 측면이 함께 공존하고 있음은 주지의 사실이며, 특히 부정적인 측면은 개인 생활의 파멸을 초래할 수도 있을 뿐만 아니라, 국가적인 안보의 위협까지 초래할 수 있다. 이는 21세기 정보화 사회가 모든 정보들이 집중화 되고 이를 광범위한 측면에서 이용함으로 인해, 이들 정보에 손쉽게 접근할 수 있는 소수의 권력층들이 이들 정보들을 거의 무한정으로 축적, 처리하며 유통 시킬 수가 있는 반면에 각 개인은 자기 자신의 정보가 어디에 어떻게 사용되고 있는 지도 모른 채 그 위험에 그대로 노출되고 있는 것이다.

우리나라의 경우 초고속 정보통신망이 인터넷과 연동될 것이며, 또한 국가 기간 전산망도 인터넷을 통하여 접속이 가능하게 될 것이다. World Wide Web 기술의 발달에 따라 인터넷을 통하여 일반 사용자들도 이러한 정보들에 손쉽게 접근할 수 있게 됨으로 인해 인터넷에 대한 정보보호 문제는 더욱더 중요한 과제로 부각되고 있다[1].

<table>
<tr><td colspan="2">SEP</td><td colspan="2">PGP</td><td>S-MIME</td><td rowspan="2">Application Layer Security</td></tr>
<tr><td>SMTP</td><td>FTP</td><td>S-HTTP</td><td>SEA</td><td></td></tr>
<tr><td colspan="3">SSL</td><td colspan="2">TLS</td><td rowspan="2">Transport Layer Security</td></tr>
<tr><td colspan="5">Transport Layer</td></tr>
<tr><td colspan="5">IP Layer(IPSec, IPv6)</td><td rowspan="2">Network Layer Security</td></tr>
<tr><td colspan="5">Link Layer</td></tr>
</table>

현재 인터넷상에서 정보보호를 위해 각 계층에서 제공되는 프로토콜은 위의 그림과 같다. 이들 프로토콜에 대하여 분석한다.

1.1 Applications Layer

1.1.1 S/MINE

인터넷의 멀티미디어 전자우편 프로토콜인 MIME(Multipurpose Internet Mail Extensions) 기능에 정보보호 기능을 추가한 프로토콜로서 전자서명(Signed), 데이터 암호(Enveloped), 전자서명과 데이터 암호화(Signed And Enveloped) 등의 정보보호 기능을 지원한다.

MIME는 SMTP(Simple Mail Transfer Protocol) 기능에 더하여 기존의 메일에 다양한 형태의 데이터도 처리할 수 있는 프로토콜이다.

MOSS는 MIME에 PEM에서 이용된 정보보호 기능을 부가한 것이다.

S-MIME은 RSA사에서 발표한 PKCS에 기반을 둔 강력한 암호 기능과 유연성 있는 확장 능력을 갖고 있는 대표적인 MIME 프로토콜이다.

S-MIME의 입력 데이터는 MIME 메시지로서 MIME 메시지 전체에 대하여 전자서명 및 암호화 처리를 한다. 따라서 인터넷으로부터 수신된 S-MINE 메시지 처리 결과는 MIME 메시지가 된다. 가장 강력한 정보보호 기능을 제공하는 형식으로 전자서명과 데이터 암호화는 전자서명과 암호화에 필요한 모든 데이터를 동시에 필요로 한다. 전자서명 방식에서 계산된 Message Digest는 송신자의 비밀 키에 의해 암호화되고 그 결과는 다시 메시지 암호화에 사용된 대칭 키로서 다시 암호화 된다.

- 장 점
  - 사양이 풍부하다.
  - 지원이 광범위하다.
  - 구현 제품간 상호 운영성이 보장된다.

- 멀티미디어 데이터를 지원한다.
- 키 관리가 간편하다.

● 단 점
- 암호학적으로 취약하다.
- 상용 제품이 전무하다.

1.1.2 PGP(Pretty Good Privacy)

전자우편과 파일 저장 응용에 사용할 수 있는 기밀성, 인증, 무결성, 부인방지 등의 서비스를 제공한다.

PGP는 RSA, MD5, IDEA와 같은 가장 사용하기 좋은 암호학적 알고리즘들을 선택하여 이용하고 인터넷, 전자게시판 등의 사용 네트워크를 통하여 무료로 소스 코드를 공개하였다. 또한 DOS/Windows, UNIX, Macintosh 등의 다양한 환경에서 무료로 사용 가능하다.

● 특 징
- RSA, IDEA, MD5가 사용되고 있으며, 압축과 전자우편의 호환성을 위하여 Radix-64 변환이 포함되어 있다.
- 최대 메시지 크기의 제한을 수용하기 위하여 단편화와 재조립을 수행하는 기능이 있다.
- PEM에 비해 정보보호성은 조금 취약하나 구현이 쉽고 키 인증 등의 권한이 한 곳에 집중되지 않고 사용자 스스로가 가진다.

● 동 작
- 인증 → 기밀성 → 압축 → 전자우편 → 호환성 및 세그멘테이션 등의 서비스로 구성

● 장 점
- 암호학적으로 강력하다.
- 상용 제품이 있다.
- 구현 제품간 상호 운영성이 보장된다.

● 단 점
- 멀티미디어 데이터 지원에 한계가 있 다.
- 사용과 관리에 어려움이 있다.

● 평문 생성시 고려 사항
- 평문을 UNIX에서 편집기로 생성할 경우 /tmp 디렉토리 노출
- UNIX Host 콘솔이외에서 작업할 경우 패킷 스니핑 공격에 노출
- 암호문을 만든 후 평문 파일을 지우더라도 파일의 내용에 대한 흔적이 남게 되며, 그 흔적을 지우는 유틸리티 사용이 요구됨.
- 수신자 측에서도 위의 3가지 위협이 동일하게 적용된다.

● PGP의 문제점

FAQ를 보면 최신 인터내셔널 버전인 2.6.3i는 PGP2.x 버전들과 모두 호환된다고 한다. 하지만 PGP2.3a 버전과 이전 프로그램이서 읽을 수 있는 메시지를 만들려면 Config.txt 파일에서 legal_kludge = off에 붙어있는 코멘트를 제거해야 한다는 불편이 있다.

하나의 프로그램에서 호환 문제를 논하는 데는 역시 이전 버전과의 호환 여부가 가장 큰 쟁점인데, 이점에 대해서는 그리 편리하지만은 않다고 할 수 있다. 그나마 다행인 것은 현재 국내에서는 PGP를 사용하는 기업이나 단체가 없다는 것이며, 지금부터 사용하는 버전에는 시스템 사이의 호환성에 아무런 문제가 없을 것이라는 것이다. PGP가 강력한 암호화 능력을 가지면서 메시지 인증, 사용자 인증, 부인봉쇄 들을 지원해주고 있지만 당장 E-Mail을 사용할 때 PGP를 함께 쓰려면 불편하다. 그 이유는 모든 동작들이 커맨드 라인에서 사용자의 타이핑으로 이뤄지기 때문이다. 미국과 캐나다에서 판매되고 있는 상업용 버전에는 GUI(Graphic User Interface)를 장착, 간단한 동작으로 PGP를 사용할 수 있도록

했다.

또 다른 단점으로 생각할 수 있는 것은 암호화 모듈이 클라이언트의 브라우저나 서버 자체에 포함되어 있지 않고 외부 프로그램으로 존재하기 때문에 프로그램들 사이의 통신 횟수가 다른 프로토콜보다 늘어나고, 이에 따라 속도 면에서는 취약점을 보이고 있다. 그리고 CCI 라이브러리는 NCSA에 의해 만들어진 관계로 현재 모자익만을 지원하고 있다. 하지만 대다수의 클라이언트 사용자들이 윈도우에서 수행되는 넷스케이프를 사용하고 있는 상황에서 이들을 지원하지 못한다는 사실이 아쉬움으로 남는다.

1.1.3 SET(Secure Electronic Transaction)[2, 3]

비자/마스터 카드사가 공동으로 개발한 신용카드 결제용 전문 및 정보보호 프로토콜로써 전자상거래 고객, 판매자, 지급 결제, 중계기관간 상호인증, 거래 정보의 기밀성 및 무결성을 최대한 보장하도록 설계되어 있다. 또한 전자상거래에서 필요한 지급 결제관련 처리절차에 대한 안전한 표준 제정을 목적으로 하고 있으며, 전자상거래 처리 절차 중 고객의 주문, 결제 요청/응답, 판매자 거래 금융기관에 지급요청 및 승인 처리 등 지급과 관련된 처리 절차를 규정하고 있다.

- 구성 요소
  - 카드를 소지하고 이를 사용하는 카드 소지자(Card Holder)
  - 공개망을 통해 물건과 서비스를 파는 가맹점(Merchant)
  - 카드 소지자의 은행인 발행인(Issuer)
  - 가맹점의 은행인 매입자(Acquirer)
  - 매입사와 발행인간의 중간 매개체인 지블게이트웨이(Payment Gateway)

- 기본 요구사항
  - 정보 기밀성(Confidentiality of Information)
  - 데이터의 무결성(Integrity of Data)
  - 카드 소지자의 계좌 인증(Cardholder Account Authentication)
  - 가맹점 인증(Merchant Authentication)
  - 상호 동작성(Interoperability)

- 문제점
  - 각자의 공개 키에 대한 권위 있는 공공기관(CA)에 의한 키 등록 및 인증
  - 고객 등의 비밀 키 보관 방법 문제로서 RSA는 키 사이즈가 128비트에 이르는 핵사 값으로서 노트에 적어 두거나 PC 등의 하드 디스크에 보관하기에는 너무도 위험하기 때문에 이에 대한 보완책 마련이 시급하다.

1.1.4 SEA(Secure Extension Architecture)

W3C(World Wide Web Consortium)에서 최근에 개발하고 있는 웹 정보보호 프로토콜로서 SSL/S-HTTP의 두 프로토콜이 약점이 있다고 판단하여 HTTP 프로토콜과 더 밀접하게 관계를 가지는 새로운 프로토콜을 제안하였다.

SEA[4]는 S-HTTP의 기능을 수용하면서 구현은 W3C에서 최근 제안한 PEP(Protocol Extension Protocol)을 이용하는 형태를 띄고 있다.

(1) 구 조

- 중심 클래스 : 전자서명, 암호화 및 키 교환 메커니즘으로 구성되어 있다.
  전자서명은 HTTP 프로토콜로 주고 받는 메 시지(body)에 대하여 전자서명을 한 후, 이를 HTTP 헤더에 추가하여 주고 받는 메커니즘이다.
  - 기존 시스템을 쉽게 추가할 수 있다.
  - 다른 정보보호 메커니즘으로부터 전자서

명을 분리시킬 수 있다.
  - 과거버전의 HTTP와도 호환성을 유지할 수 있다. 즉 서명된 문서를 이전 버전의 브라우저가 볼 수 있다.
- 암호화 클래스 : HTTP 메시지는 키 교환으로 얻어진 세션 키를 이용하여 암호화한다. 키 교환 메커니즘은 HTTP 메시지를 암호화 하기 위한 키를 서로 생성해 주고 받는 메커니즘으로 RSA 또는 Diffie-Hellman 방식을 사용하여 세션 키를 주고 받는다.

(2) 특 징

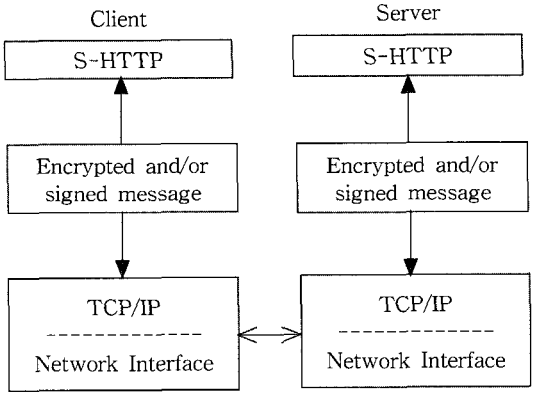
- SSL은 트랜스포트층의 정보보호 프로토콜이고, S-HTTP는 HTTP와는 비슷한 구조이지만 별도의 새로운 프로토콜이어서 기존의 HTTP와의 호환성의 문제 등을 W3C에서는 문제시하고 있다.
- S-HTTP의 기능을 수용하면서 구현은 W3C에서 최근에 제안한 PEP을 이용하는 형태이다. PEP는 HTTP 프로토콜을 사용자 레벨에서 정의해서 확장할 수 있는 "프로토콜 확장 플랫폼" 프로토콜이다.
- 전자서명을 통해 기존 시스템에 쉽게 추가할 수 있고, 다른 정보보호 메카니즘으로부터 전자서명을 분리시킬 수 있다.
- 이전 버전의 HTTP와도 호환성을 유지할 수 있다.

1.1.5 S-HTTP(Secure Hyper Text Transfer Protocol)

S-HTTP[5]는 1994년 EIT(Enterprise Integration Technologies), NTSA, RSA에서 Web의 상업적 이용에 대비하여 HTTP 서버와 클라이언트 사이의 안전한 통신 메커니즘을 제공하기 위하여 설계되었다. 즉 S-HTTP는 HTTP에 붙여서 사용하기 위해 고안된 통신 프로토콜이며 HTTP 메시지 모델과 함께 존재하고, 쉽게 HTTP 응용에 결합되도록 고안되었다. S-HTTP는 헤더를 통해 각 거래마다 상대방들 사이에 옵션을 협상하고 이 협상을 통한 다중 직교 동작 모드, 키 관리 메커니즘, 신뢰 모델, 암호 알고리즘, 캡슐화 형식을 지원하는 융통성 있는 프로토콜을 제공한다. 이들은 모두 공개 키 기반 구조를 가지며 X.509와 X.509v3를 사용하고 있다.

(1) 구 조

S-HHTP는 프로토콜 헤더를 통해 협상하고, 협상을 통한 암호 그리고/또는 서명한 문서를 일반 채널을 통해 상대방에게 전달한다.



(2) 특 징

- 응용계층에서 적용되며, 트랜잭션의 기밀성, 서버 인증, 무결성, 발신 부인봉쇄, 접근제어 등을 지원한다.
- 다양한 암호화 알고리즘을 사용한다.
  - 캡슐화 형태 : PKCS-7, PEM/PGP
  - 전자서명 알고리즘 : RSA/DSA
  - 암호화 키 교환 알고리즘 : RSA, In-band, Out-band, Kerberos, D-H
  - 메시지 다이제스트 알고리즘 : MD2, MD5, SHA

- 정보보호 모드 : 서명, 암호화, 키 기반 MAC
- 공개키 인증 형식 : X.509, PKCS-6

● 구현 및 표준화 뒷 받침이 미흡하다.

1.1.6 FTP(File Transfer Protocol)

인터넷에서 파일 전송을 위한 표준으로 정착된 프로토콜로서 데이터 채널과 컨트롤 채널이라는 두개의 가상 연결을 통해서 서로 데이터와 제어 정보를 주고 받는다.

컨트롤 채널은 클라이언트에서 서버 포트 21번호를 접속했을 경우에 연결이 이루어진다.

데이터 채널은 특별한 방식으로 그 연결이 설정되는데 우선 클라이언트가 PORT 명령을 통해서 서버에 자신의 데이터 채널 포트 번호를 보내면 서버의 20번 포트에서 PORT 명령에 나타난 포트로 연결을 설정한다.

● FTP의 정의

FTP는 파일을 한 시스템으로부터 다른 시스템으로 전송하는 프로그램이다. FTP는 사용자 인증(authentication), 데이터 변환, 디렉토리 리스팅 등의 다양한 기능과 옵션을 제공 한다. 대화형 사용자의 전형적인 절차는 자기 시스템에서 FTP를 클라이언트를 호출하고, 이어 이 클라이언트 프로세스는 TCP를 이용하여 원격 시스템의 FTP 서버 프로세스와 연결을 설정한다.

1.1.7 SMTP(Simple Mail Transfer Protocol)

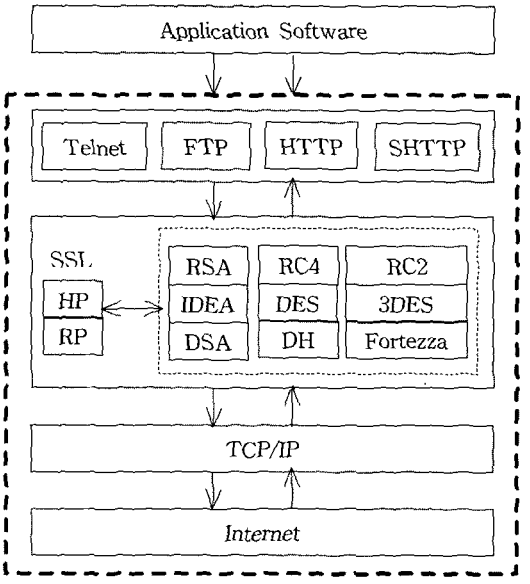
인터넷에서 전자메일을 전송하는데 사용되는 프로토콜로서 내부의 메일 허브와 외부의 메일 허브를 두는 구조로 되어 있다. 내부 사용자들은 내부 메일 허브를 메일 서버로 사용한다. SMTP는 전자우편 교환 서버에서 사용되는 통신 규약으로 두 컴퓨터가 어떻게 상호 접속하는 지와 전자우편을 전송하기 위해 사용하는 제어 명령을 규정하고 있다. RFC 821에서 정의하고 있다.

2. Transport Layer(6)

2.1 SSL(Secure Socket Layer)

SSL은 1993년 Netscape Communications사에서 응용 프로토콜들(HTTP, Telnet, SHTTP, FTP 등)과 전송 프로토콜(예, TCP/IP)사이에 정보보호를 제공하기 위하여 개발되었으며, 메시지 길이, 종류, 내용 필드 등을 다루고 있다. 또한 메시지를 블록 단위로 분할하고 선택적으로 압축하며 이에 대한 MAC(Message Authentication Code)를 계산하고, 이를 암호화한 후 그 결과를 상대방에게 전송한다. 수신된 데이터는 복호화, MAC 검증, 압축 풀기, 역 분할의 과정을 거쳐 상위 개체로 전달된다.

2.1.1 구 조



● HP(Handshake Protocol) : 상호 인증 및 데이터를 전송하기 전에 암호 알고리즘과 키

의 협상을 하는 프로토콜
- RP(Record Protocol) : 여러 가지 상위 프로 토콜의 Encapsulation을 위해 사용된다.

2.1.2 특 징

- 웹이나 HTTP 등에 제한되지 않고, 응용 프로토콜에 독립적인 계층 구조 프로토콜이며, TCP/IP와 응용 프로토콜 사이에 존재하는 소켓 계층 역할을 수행한다.
- 인증을 위하여 X.509 인증서 시스템을 이용하고, 공개키로서 RSA, 대칭 암호화를 위하여 RC4-128, RC2-128, DES, Triple DES, IDEA 중에 하나를 이용한다.
- 인터넷 제반 응용 서비스의 암호화를 지원한다.
- 인터넷상에서 상업적 기밀 통신을 위해 제안 되었다.
- 데이터의 기밀성, 인증성, 무결성, 부인 봉쇄 등의 정보보호 서비스를 통해 도청과 위조로부터 안전하게 데이터를 전송하는 안전한 통신 메커니즘이다.
- 응용별 선택적 암호화가 불가능하다.
- 오버헤드 발생한다.
- 데이터 전송속도 느려진다.

2.1.3 참고자료

- SSL 3.0 Specification
  http://home.netscape.com/eng/ssl3/3-SPEC.HTM
- SSL 3.0 Implementation Assistance
  http://home.netscape.com/eng/ssl3/traces/index.html
- Introducing SSL and Certificates using SSLeay
  http://www.camb.opengroup.org/RI/www/prism/wwwj/
- SSLeay and SSLapps FAQ
  http://psych.psy.uq.oz.au/~ftp/Crypto/
- SSL Challenge
  http://www.rain.org/~hal/sslchallong.thml
- Apache-SSL
  http://www.apache-ssl.org

2.2 TLS(Transport Layer Security)

1996년 IETF에서 추진하고 있다.

- SSL 3.0을 기반으로 한 업그레이드 프로토콜(TLS1.0)
- HMAC(Message Authentication Code)사용한 강화된 인증 기능
- 연구 및 구현이 초기 단계

3. Network Layer Security

3.1 IPSec(IP Layer Security Protocol; ISAKMP)

IPSec은 인터넷의 IP 계층을 보호하기 위한 정보보호 프로토콜이다.

서로 다른 업체의 제품간에 상호 운용성을 보장, 인터넷에서 사설 통신을 하기 위한 암호 터널을 쉽게 구축할 수 있도록 TCP/IP 패킷을 인터넷으로 보내기 전에 암호화 하는 방법을 규정한다. 마이크로소프트사가 주창하는 PPTP(Point-to-Point Tunneling Protocol)와 양대 산맥을 이루고 있는 표준 정보보호 프로토콜로서 체크 포인트, 랩터 시스템, 트로스티디 인포메이션 등 화이어월 업체들이 VPN 정보보호를 위해 각양각색의 자사 고유 방식을 표준화 해 상호 연동하는데 그 목적을 두고 있다. 한편 마이크로소프트사가 주관하고 있는 PPTP는 어센드, 3COM, U.S. 로보틱스, ECI 테레마틱 등의 리모트 액세스 업체들과 공동 개발된 것이다. 이 안은 1996년 3월에 발표되었으며 1996년 6월에 IETF에 상정됐다.

FC가 인증한프로토콜(RFCs 1825~1829)로서, IETF가 TCP/IP 프로토콜 스위치에 표준 기반의 인증 및 암호화를 추가하기 위하여 설계한 것으로 두 가지 형태의 키 관리를 규정한다. IPSec은 IPv6에 필수 요소이다.

3.1.1 구 조

- Key management : 세션을 위한 SA(Security Association)을 확증한다.
  - IKE(Internet Key Exchange)
  - SKIP(Simple Key Exchange Internet Protocol) 썬 마이크로 시스템에서 개발
- SA : 인증 및 기밀성을 제공한다.
- IP datagram
  - Authentication Header(AH) : 트래픽을 암호화하는 것이 아니라 인증하는 방법을 규정하며, 각 패킷과 데이터의 무결성을 보장 한다.
  - Encapsulating Security Protocol(ESP) : 전체 패킷을 암호화하고 전송하기 위하여 보다 큰 패킷을 내부에 배치하는 절차인 터널링 방법을 규정하며, 3중 DES(112비트)나 DES(56비트)를 보장한다.

3.1.2 특 징

- 인증, 무결성, 접근제어, 부인봉쇄 서비스를 지원한다.
- IP 정보보호계층 메커니즘은 캡슐화 메커니즘과 키관리 메커니즘으로 조합하여 실현된다. 키 관리는 공개키 암호 기술을 사용하고 공 개키 기반 메커니즘을 지원한다.
- 오버 헤드가 발생하지만 암호화는 트래픽이 동을 위해 더 안전한 방법이다.
- 공중망을 통해서도 전용회선 못지 않은 안전한 데이터 전송로를 확보할 수 있게 되므로 회선 비용의 부담을 덜 수 있다.
- TCP/IP의 계층 구조 중 IP Layer에서 운용되 기 때문에 사용자들이 전자서명과 같은 전자 상거래에서 직접적으로 필요한 정보를 얻을 수 없다는 단점이 있다.

3.2 IPv6

IETF에서 제정한 차세대 IP 규격, 차세대 인터넷 프로토콜로 불리 우는 IPv6는 현재의 IPv4와 라우터 프로토콜을 업그레이드시킨 버전으로 주소 구조를 32비트에서 128비트로 확장하여 인터넷 주소 부족 현상을 제거할 것으로 보인다.

IPv6는 향상된 기능의 IP 어드레싱, 사용의 편리성, 최신 인터넷 기술, 보안 기능 모두를 지원한다. IPv6 어드레스 공간의 일부는 IPv4 어드레스를 위해 남겨져 있어 IPv6로 이전할 경우를 대비한 유연성을 제공할 뿐만 아니라 노벨의 IPX나 OSI의 NSAP 같은 다른 포로토콜 슈트도 지원하고 있다.

IPv6의 주소 헤더는 향후의 확장을 위해 예비 공간을 확보하고 있으며, 저비용 대역폭을 보장하기 위하여 지능적이고 효과적으로 트래픽 흐름을 제어할 수 있도록 설계하였다. 또한 플러그 and 플레이 설계를 통해 주소를 새로 입력할 필요 없이 호스트가 자동으로 글로벌 네트워크에 접속하는데 필요한 정보를 획득하게 하는 자동 구성 기능을 가지고 있다.

IPv6로 업그래이드된 호스트는 IPv4와 IPv6 모두에서 통신할 수 있으며, 각 프로토콜에 대해 두 개의 어드레스를 가질 수 있다. 즉 개별적인 PC, 기업내의 네트워크, IPv6 호스트들의 IP 터널링을 통해 IPv4 네트워크와 라우터 상에서 다른 IPv6 호스트들과 통신할 수 있다.

IPv6를 사용하기 위해서는 IPv4와 IPv6 어드레스를 지원하는 IPv6DNS 서버를 이용해야 한다.

RFC-791에서 규정하고 있는 IPv4를 발전시킨 새로운 인터넷 프로토콜로서, IPv6에서는 선택적인 인터넷 계층의 정보가 패킷 내 상위 계층 헤더와 IPv6 헤더 사이에 위치하며, IPv6 헤

더와는 분리된 헤더로써 인코딩 된다. IPv6 패킷은 0, 1, 그 이상의 확장 헤더를 포함할 수 있으며 각각의 확장 헤더는 그 이전 헤더의 Next Header 필드에 의해 구분된다.

3.2.1 구 조

IPv6의 IP Header의 구조는 다음과 같다.

vers	priority	flow label
Payload Length	next header	hop limit
source IP Address		
destination IP Address		
nxt header	hdr header	
Extension Header		
TCP header and Data		

3.2.2 특 징

- 확장된 주소 능력(Expanded Addressing Capabilities) : IP 주소크기를 IPv4의 32비트에서 128비트로 확장하여 더 많은 단계의 주소 계층화와 노드의 주소화 및 더욱 간단해진 주소 자동 설정을 지원한다.
- 개선된 선택 사항과 확장의 지원(Improved Support for Extensions and Options) ; IP 헤더 선택 사항을 효율적인 forwarding을 가능 하게 하고, 선택 사항 길이에 대한 제한을 완화하고, 새로운 선택 사항을 쉽게 추가할 수 있도록 융통성 있는 구조로 만들었다.
- 단순화된 헤더 형식(Header Format Simplifications) : 헤더의 대역폭 비용을 절감하고 패킷 처리시 공통적인 부분의 처리 비용을 절감하기 위하여 IPv4 일부 헤더를 삭제하거나 선택 영역으로 변경하였다.
- 흐름 표시 기능(Flow labeling Capability) : 실시간 서비스나 혹은 Non-Default 서비스 품질과 같이 송신자가 특별한 처리를 요구하 는 트래픽 처리에 속하는 패킷에는 특정한 표시를 하는 기능을 추가 하였다.
- 인증과 프라이버시 기능(Authentication and Privacy Capabilities) : 인증, 데이터 무결성과 선택적인 데이터 기밀성을 지원하도록 확장 하였다.
- 효과적인 실시간 형의 멀티미디어 통신에 적합하다.
- 확장성, 유연성, 대역폭 이용의 편리성이 우수하다.

4. 프로토콜 비교 분석

4.1 SSL과 S-HTTP의 비교

아래 <표>는 SSL과 S-HTTP의 비교 표이다.

구 분	SSL	S-HTTP
정보보호 계층	응용 계층의 암호화 방식이기 때문에 HTTP, NNTP, FTP 등에도 사용할 수 있다.	HTTP에 정보보호적 기반을 둔 메시지를 첨부하는 형태
인증 기법	Keyed MAC, Hash(SHA, MD5)	Hash(SHS, MD2, MD5)
암호화 기법	DES, RC4	DES, RC2, RC4, IDEA
구 조	응용 계층을 그대로 사용하고 이와 접목하여 새로운 계층을 갖는 형식을 취한다.	기존의 HTTP 프로토콜에 정보보호 메카니즘을 덧붙인 형식을 취하고 있다.
키 분배 방식	핸드 쉐이크를 통해 RSA, Diffie-Hellman, Fortezza 방식으로 키 분배	일반적으로 RSA 방식을 사용하고, 어느 한쪽이 공개키가 없는 경우 Inband, Kerberos, Outband 방식으로 키 분배
암호화 및 인증 단위	서비스	메세지

4.2 SSL과 SET의 비교

아래 <표>는 SSL과 SET의 비교 표이다.

구 분	SSL	SET
목 적	일반 상거래에서 신용카드가 사용되는 과정을 그대로 전자상거래 개념으로 전환한 것	브라우저와 서버간에 안전한 통신을 보장하는 것
비 용	저비용	고비용
사 용 편리성	아주 쉬움	다소 어려움
금융기관간의 온라인 결 재	제공 안함	제공함
안전성	낮음(상점에 카드번호노출)	높음(금융기관만이 카드번호확인)
조 작 가능성	상점 단독 가능	다자간의 협력 필요

4.3 S/MIME과 PGP, PEM, MOSS와의 비교

이들 모두는 전자우편의 정보보호 기법의 일종이다. 모두다 authentication과 privacy를 보장한다. PGP, PEM, MOSS는 각각이 서로 매우 상이하다. 그러므로 이들을 S/MIME과 각각 비교해야 할 것 같다. PGP는 사양(specification)이면서 응용 프로그램(application)이라고 봐야 할 것 같다. PGP는 사용자들이 서로 키를 교환하고 서로 인증(trust)을 확립하는 체계이다. 이런 "web of trust" 구조는 비공식적이기 때문에 작은 그룹에는 적용하기 쉽다. 그러나 많은 수의 사람들이 포함된 그룹에서는 관리하기가 쉽지 않게 된다. 그러나 S/MIME은 PGP보다는 적응성이 좋고 좀더 보안성이 좋다. S/MIME은 작은 그룹의 사용자들 간의 신뢰 구조를 쉽게 구축할 수 있을 뿐 아니라 큰 그룹을 구성하는 데도 쉽게 적응하는 구조를 가지고 있다. S/MIME은 많은 전자우편 응용프로그램에 접목될 수 있고 그렇게 하는 것이 쉽다. PEM은 IETF RFC 1421-1424까지 정의되어 있다. PEM은 초기의 전자메일 정보보호 표준이다. PEM은 주로 메시지 포멧과 인증구조를 정의한 것이다. PEM메시지는 7bit 텍스트 메시지를 기반으로 되어있는데 반해 S/MIME은 MIME binary attachment로 동작하도록 설계되었다. 인증 구조를 구성하는 것도 flexible하게 되어있고, 작은 워킹 그룹들의 구조를 만드는데 매우 쉽게 되어 있으면서도 인증그룹의 규모에 적합한 대안을 가지고 있다. MOSS는 PEM의 제약을 극복하기위해 만들어진 것으로서 MIME 메시지로만 표현하고 나머지 사양은 자유롭게 사용하도록 한 것이다. 그러나 MOSS는 많은 구현 option을 가지고 있어서 두 사람의 MOSS 메일 프로그램을 구현하는 사람이 상호 호환되는 프로그램을 만들기가 매우 어렵게 되어있다. MOSS는 사양(Specification) 이라기 보다는 어떤 구조(Framework)정도를 정의했다고 보는 것이 더 좋겠다. 그러나 S/MIME은 상호호완성에 역점을 두고 전자우편에 촛점을 두고 만들어진 것이다.

5. 결 론

국내의 대부분의 전자 쇼핑몰들이 SSL 기능을 갖는 웹 서버를 구축, 운영하고 있으며 향 후 지속적인 성장과 발전이 예상된다.

정보보호 프로토콜은 주로 웹 기반이므로 웹 서버 및 웹 브라우저를 판매하는 기업체들에 의해 별도의 수수료 없이 웹 관련 프로그램을 탑재하여 판매되는 형태를 취하고 있다. SSL의 경우에는 Apache-SSL 웹 서버와 같이 무료로 설치할 수 있는 프로그램이 존재하고 있다. 그러나, SSL를 설치할 경우 서버의 인증서가 필요하기 때문에 현재 대부분의 국내전자 쇼핑몰들이 외국의 인증기관으로부터 인증서 발급 서비스를

이용하고 있다. 미국의 Verisign사의 경우 SSL 서버용 인증서 수수료가 1년에 349$이다.

정보보호 프로토콜 분야는 인터넷의 TCP/IP를 기반으로 한 고도의 웹 기반기술을 요구하기 때문에 국내에서 개발하기 어려운 실정이므로 국내 기업체나 연구기관의 참여도가 거의 없는 실정이다. 그러나 정보보호 프로토콜 내에 필요한 암호 알고리즘 등에 국산 암호 알고리즘 시도는 필요하다. 또한 전송계층이나 세션계층이 아닌 응용계층의 특화된 프로토콜을 개발한다면 경쟁력이 있을 것으로 예상된다. 아직은 환경이 조성되어있지 않지만 IPv6 프로토콜은 외국에서도 활발한 연구가 진행되지 못하는 상황이므로 국내에서 연구 개발을 조기에 시작함으로써 선진국과 동등한 기술력을 확보할 수 있다고 판단된다.

인터넷은 전세계를 하나로 묶는 정보화 사회의 기반이 되는 정보 통신망으로 성장하고 있다. 현재는 일반 사용자들도 쉽게 WWW 기술을 이용하여 인터넷으로 접속할 수 있으며, 이를 이용한 많은 상용 서비스들이 시작되고 있는 시점이다.

우리나라의 경우 초고속 정보통신망이 인터넷과 연동될 것이며, 또한 국가 기간 전산망도 인터넷을 통하여 접속이 가능하게 될 것이다. 이러한 여건 속에서 인터넷에서의 정보보호 대책은 그 중요성이 매우 높다 할 것이다. 우선 PGP는 현재 인터넷에서 가장 많이 사용되고 있는 전자 우편 정보보호 도구로써 문서의 기밀성을 보장해 주면서 불법적 변경 여부와 송신자의 신원 확인, 그리고 송신자가 문서를 보낸 사실을 부인하지 못하게 하는 기능들을 제공하고 있기 때문에 전자우편 사용에 있어서 중요한 역할을 수행하고 있다. 그러나 국내에서는 아직 초기 단계이나 차츰 사용자가 증가하고 있는 추세이다. 앞으로 일반 사용자들이 암호화/복호화의 복잡한 구조를 모르더라도 손쉽게 사용할 수 있도록 GUI(Graphic User Interface)의 구현과 한글화가 이루어지면 그 사용이 급격히 증가하리라고 예상되고 있다.

IP security는 사용자들에게 정보보호 위험을 줄이고 더 나은 정보보호를 제공하기 위해 다른 환경과 응용들과 결합될 수 있다.

인터넷이 범위를 확장함에 따라 강력하고 믿을 수 있는 암호화기법이 요구된다.

참 고 문 헌

[1] http://queen.sungshin.co.kr.
[2] http://ssmart.co.kr.
[3] http://metaland.com.
[4] http://infor.kisc.net.
[5] http://msi.21cfl.com.
[6] http://poem.cheju.ac.kr.
[7] Internet-Draft
- Internet Security Association and Key Management Protocol
- Simple Key Management For Internet Protocols(SKIP)
- IP Encapsulating Security Protocol (ESP)
- Security Architecture for the Internet Protocol
- Certificate Discovery Protocol
- The Internet IP Security Domain of Interpretation for ISAKMP

[8] RFC
- RFC 1825 : Security Architecture for the Internet Protocol
- RFC 1826 : IP Authentication Header
- RFC 1827 : IP Encapsulating Security Payload(ESP)
- RFC 1828 : IP Authentication using Keyed MD5
- RFC 1829 : The ESP DES-CBC Transform
- RFC 1421 : Privacy Enhancement for Internet Electronic Mail : Part I : Message Encryption and Authentication Procedures
- RFC 1422 : Privacy Enhancement for Internet Electronic Mail : Part II : Certificate-Based Key Management
- RFC 1423 : Privacy Enhancement for Internet Electronic Mail : Part III : Algorithms, modes, and Indentifiers

김 상 춘

1986년 한밭대 전자계산학과 (공학사)
1989년 청주대 전자계산학과 (공학석사)
1999년 충북대 전자계산학과 (이학박사)
1983년~2001년 한국전자통신연구원 정보보호기술 연구본부(선임기술원)
2001년~현재 삼척대학교 정보통신공학과 조교수

권 기 현

1993년 강원대 전자계산학과 (이학사)
1995년 강원대 전자계산학과 (이학석사)
2000년 강원대 컴퓨터과학과 (이학박사)
1998년~2002년 동원대학 인터넷 정보과 조교수
2002년~현재 삼척대학교 정보통신공학과 전임강사
관심분야 : 분산 소프트웨어, 임베디드 소프트웨어, 데이터마이닝, 정보보안