主題

S-HTTP와 SSL(Secure Socket Layer)에 관한 고찰

한국정보보호센터 최영철, 홍기웅

차 례

I. 서론
II. S-HTTP(Secure Hyperext Transport Protocol)
III. SSL(Secure Socket Layer)
IV. 결론

요 약

최근 인터넷을 기반으로 한 각종 전자상거래가 활성화되면서 안전한 웹 기반 프로토콜들에 대한 요구가 급증하고 있다. 인터넷 온라인 증권 트레이딩, 인터넷 온라인 뱅킹 등 많은 응용들이 고도의 보안을 필요로 하며 이를 위해 웹 보안 프로토콜들이 널리 사용되고 있다. 본 고에서는 최근 사용이 급증하고 있는 보안프로토콜인 SSL(Secure Socket Layer) 프로토콜에 대하여 분석하며, 아울러 1995년에 제안된 S-HTTP에 대하여도 함께 고찰하고자 한다.

I. 서 론

최근 전자상거래가 활성화되면서 많은 전자거래 응용들이 탄생하고 있다. 증권분야에서는 이미 인터넷을 통한 홈 트레이딩이 폭발적인 성장을 보이고 있으며, 은행분야에서는 인터넷 뱅킹 시스템들이 속속 도입되고 있는 실정이다. 이와 같이 전자상거래가 활성화되면서 사용자들은 많은 편리성을 누리고 있지만, 반대로 정보화 역기능이라는 새로운 문제점을 경험하곤 한다. 이러한 역기능에는 사용자의 개인정보 누출, 부당한 거래로 인한 손실 등과 같이 거래 회사의 부당성에 의해 발생되는 역기능도 있지만, 기술적인 문제 때문에 발생할 수 있는 다음과 같은 역기능들도 있다.

- 정보의 노출 : 인터넷상의 모든 정보는 누구에게나 노출되어 있다. 쌍방간의 전자거래시 비밀정보는 언제든지 누출될 수 있는 것이다. 이것은 인터넷상에서 신용카드 등을 기반으로 하는 기존 결제 방식의 사용을 위태롭게 만들 수 있

다.

- 정보의 위·변조 : 인터넷상의 모든 정보는 누구나가 쉽게 위·변조 할 수 있다. 이것은 올바른 정보의 전달을 어렵게 만드는 장애요소가 된다.
- 사용자 위장 : 인터넷상에서 "갑"이라고 하는 자가 실제로는 "을"일 수 있다. 거래 당사자는 상대방을 오인한 채 거래에 임할 수 도 있다.
- 거래의 부인 : 인터넷상에서 거래 당사자는 향후 자신의 행위 사실을 부인할 수 있다. 이것은 거래 후 새로운 분쟁을 발생시킬 수 있는 위험요소가 된다.

상기에서 설명된 역기능들은 암호기술을 사용함으로써 근본적으로 해결될 수 있으며, 1990년대 중반부터 상기의 문제점들을 해결할 수 있는 인터넷 보안 프로토콜들이 등장하게 되었다.

II. S-HTTP(Secure Hypertext Transport Protocol)

1995년 미국의 EIT(Enterprise Integration Technology)사는 S-HTTP (Secure-Hypertext Transport Protocol)라는 안전한 웹 보안 프로토콜을 개발하였다. S-HTTP는 기존 HTTP의 보안 문제점을 해결코자 암호화 및 전자서명(Digital Signature)의 기술적용을 통하여 HTTP를 보다 안전하게 만든 것이다.

S-HTTP는 HTTP에 추가 확장영역을 정의하여 구현하였으며 NCSA의 Mosaic에서 최초로 구현되어졌다. 그리고, 이것은 실리콘밸리에서 탄생된 커머스넷(CommerceNet)에 의해 채택되어 사용되었다. S-HTTP의 동작원리는 다음 그림 1과 같다.

아래 그림 1에서 S-HTTP는 응용 계층에서 동작하는 프로그램임을 알 수 있으며, S-HTTP를 지원하는 웹 브라우저와 웹 서버는 암호 모듈을 가지고 있음으로써 암호화/복호화 또는 전자서명 생성/검증 등의 기능을 수행할 수 있게 된다. 또한, 확장된 HTTP의 TAG를 인식할 수 있도록 S-HTTP 메시지들도 지원되어야 한다.

그러나, S-HTTP는 최근 거의 사용되지 않고 있으며, 1998년도 드래프트 버전 이후 표준화 작업이

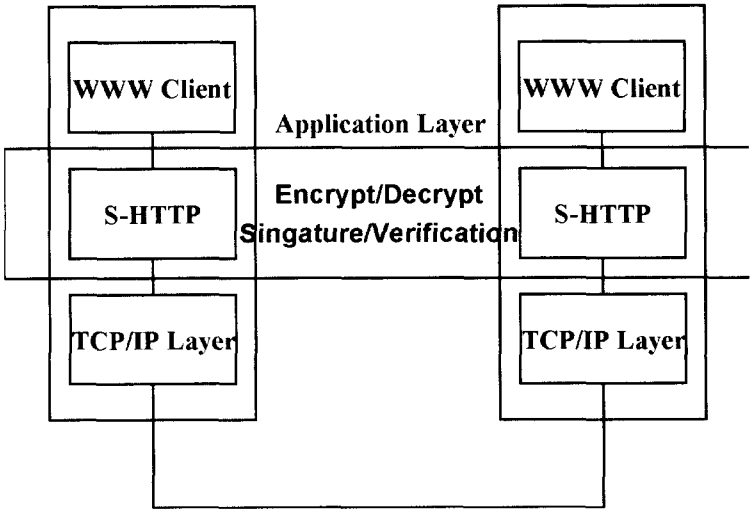


그림 1. S-HTTP의 동작 구조

미진한 상태에 있다. 최근에는 SSL(Secure Socket Layer)이 보다 폭넓게 사용되고 있으며, 본 고에서는 SSL에 대하여 보다 심도있는 분석을 하고자 한다.

III. SSL(Secure Socket Layer)

SSL은 1994년 미국의 넷스케이프사에 의해 최초로 개발되었으며, 현재 버전3.0에 이르고 있다. SSL의 특징은 HTTP, TELNET 등과 같은 응용계층과 TCP 또는 UDP와 같은 전송 계층 사이에서 클라이언트와 서버간의 안전한(Secure) 채널을 형성해 주는 역할을 수행한다는 것이다. 즉, SSL은 S-HTTP와는 달리 응용계층 아래에서 안전한 채널을 형성하기 때문에 다양한 응용 프로토콜의 보안성을 강화시킬 수 있다는 장점을 갖게 된다. 이러한 SSL의 동작구조를 살펴보면 그림 2와 같다.

가. SSL 프로토콜의 구성

SSL 프로토콜은 서버 인증(Sever Authentication), 클라이언트 인증(Client Authentication), 그리고 키 교환(Key Exchange)을 수행하는 SSL 핸드쉐이크(Handshake) 프로토콜과 이후 비밀성 보장을 위한 암호통신을 수행하는 SSL 레코드(Record) 프로토콜로 구성된다.

SSL 핸드쉐이크 프로토콜은 클라이언트와 서버간에 사용될 암호 알고리즘을 결정하고, 이에 사용될 비밀키를 교환하는 작업을 수행하며, 이 과정 중에 인증서(Certificate) 검증을 통한 서버 인증 또는 클라이언트 인증을 수행한다. 여기서 클라이언트 인증은 서버 측에서 결정할 옵션 사항이다.

그림 3은 SSL 핸드쉐이크 프로토콜의 세부 동작 과정을 나타낸 것으로서 옵션1과 옵션2는 서버가 클라이언트 인증을 세팅한 경우 추가적으로 수행되는 부분으로서 옵션1은 클라이언트 인증서 요청 정보가 되고, 옵션2는 클라이언트의 인증서가 된다.

SSL 레코드 프로토콜에서는 SSL 핸드쉐이크 프로토콜 수행중에 결정된 대칭키 방식의 암호 알고리즘을 이용하여 벌크(Bulk) 암·복호화 작업을 수행하게 된다.

나. SSL 프로토콜에서 사용되는 암호 알고리즘

SSL 프로토콜에서는 RSA 비대칭형 암호 알고

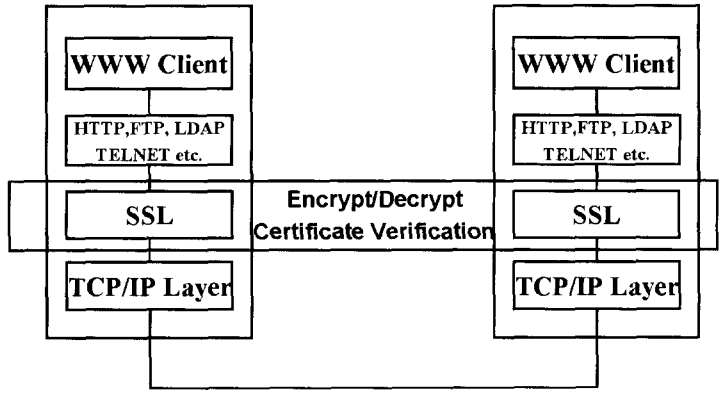


그림 2. SSL의 동작 구조

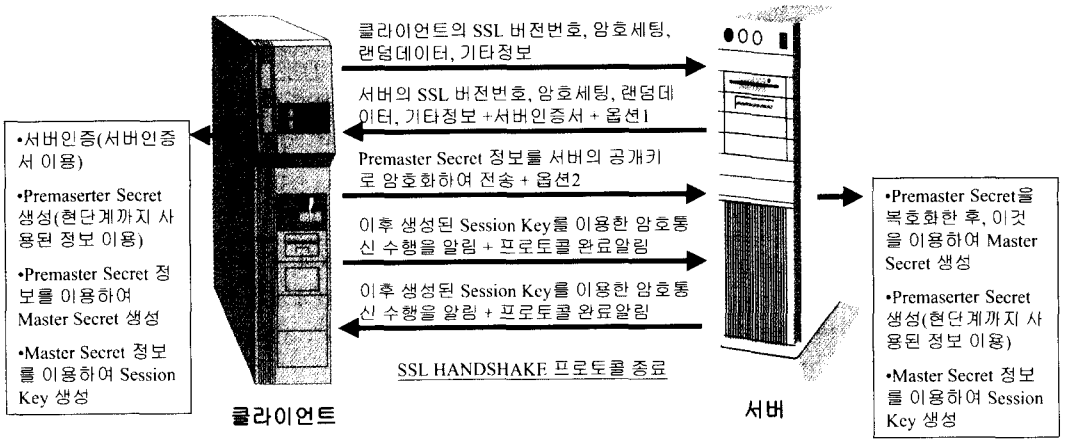


그림 3. SSL 핸드쉐이크 프로토콜의 세부 동작 과정

리즘, RC2 · RC4 · Triple-DES · SKIPJACK 대칭형 암호 알고리즘, MD5 · SHA-1 해쉬 알고리즘들이 사용된다. MD5, SHA-1 해쉬 알고리즘은 메시지 인증을 위한 MAC(Message Authentication Code)를 생성하는데 이용되거나 RSA 암호 알고리즘에서 전자서명 생성 · 검증에 사용된다.

표 1은 현재 SSL 프로토콜에서 사용되고 있는 대칭형 암호 알고리즘과 해쉬 알고리즘에 대한 현황이다.

다. SSL 프로토콜에서 사용되는 포트 번호

SSL 프로토콜상의 응용 프로토콜은 TCP/IP상의 어떤 포트를 사용해도 무방하나, 패킷 필터링 침입차단 시스템의 안전한 동작을 위해 1996년 9월경 IETF내 IANA(Internet Assigned Numbers Authority)에서는 SSL 프로토콜 기반의 응용 프로토콜 포트를 표 2와 같이 지정하였다.

키워드	포트번호	설명
https	443/tcp	SSL 기반의 http
ssmtp	465/tcp	SSL 기반의 smtp
snews	563/tcp	SSL 기반의 news
ssl-ldap	636/tcp	SSL 기반의 ldap
spop3	995/tcp	SSL 기반의 pop3

표 2. SSL 프로토콜이 적용되어 사용되는 응용 프로토콜의 포트 번호

라. SSL 프로토콜의 참조 구현

SSL 프로토콜을 실제 여러 응용에 적용하기 위해서는 SSL 프로토콜을 참조로 하여 개발된 라이브러리가 필요하게 되며, 이러한 라이브러리는 응용 프로그래머들에게 시스템상의 SSL 프로토콜 구현을 용이케 해준다.

1) SSL Ref 3.0

넷스케이프사와 컨센서스(Consensus) 개발사가 공동으로 개발한 참조 라이브러리로서 TCP/IP 환경내에 보안 제공이 필요한 응용을 개발하는 개발자들에게 편의성을 제공한다. 사용 제약 조건으로서는 미국내에서만 사용 및 판매 가능(미국외 수출 불가)하다는 것이며, 상업적 라이센스 가격이 약 $30,000(Part Number 70-01128-00) 정도가 된다. 본 라이브러리에서 제공되는 암호 체계는 표 3과 같다.

암호 비도 및 권고 내용	암호 알고리즘
o 종류 : 가장 강한 암호 o 권고 내용 - 단지 미국내에서만 사용가능 - 은행 또는 중요하고 민감한 정보를 다루는 기관에서 사용	o 168비트 Triple DES + SHA-1 메시지 인증 o 특징 : 가장 강력한 암호 o 안전성(키대상수) : 3.7×1050 o 지원 : SSL 2.0, SSL 3.0
o 종류 : 강한 암호 o 권고 내용 - 단지 미국내에서만 사용가능 - 대부분의 비즈니스나 정부 분야에서 사용가능	o 128비트 RC2/RC4 + MD5 메시지 인증 o 특징 : RC2가 RC4 보다 느림 o 안전성(키대상수) : 3.4×1038 o 지원 - RC2 : SSL 2.0 - RC4 : SSL 2.0, SSL 3.0
	o 56비트 DES + SHA-1 메시지 인증 o 특징 : SSL 2.0에서는 MD5 사용 o 안전성(키대상수) : 7.2×1016 o 지원 : SSL 2.0, SSL 3.0
o 종류 : 수출가능한 암호 o 권고 내용 - 상기 언급된 암호 강도중 가장 약한 것으로서 미국 외 수출가능 - 프랑스에서는 S/MIME은 제외하고 SSL만 허용 - 현재 안전성이 취약한 것으로 판명	o 40비트 RC2/RC4 + MD5 메시지 인증 o 특징 : RC2가 RC4 보다 느림 o 안전성(키대상수) : 1.1×1012 o 지원 : SSL 2.0, SSL 3.0
o 종류 : 가장 약한 암호 o 권고 내용 - 암호화 기능이 없는 인증 및 무결성 제공 - 기밀성 서비스를 필요로 하는부분에서는 사용 불가	o MD5 메시지 인증 o 특징 : 무결성 기능만 제공 o 지원 : SSL 3.0

※ RC4, RC2에서 40비트 암호사용시 키길이는 128비트가 되나, 단지 활성화되어 사용되는 부분이 40비트가 되는 것임

표 1. SSL에서 정의된 키교환 대상 암호 알고리즘

기 능	표 현
비보호	SSL_NULL_WITH_NULL_NULL
RSA MD5 인증 + 비암호화	SSL_RSA_WITH_NULL_MD5
RSA MD5 인증 + 수출가능한 RC4 암호화	SSL_RSA_WITH_RC4 _40_MD5
RSA SHA 인증 + DES 암호화	SSL_RSA_WITH_DES_CBC_SHA
DES 암호화와 SHA를 이용한 익명기능을 갖는 Diffie-Hellman 키교환	SSL_DH_anon_WITH_DES_CBC_SHA

표 3. SSL Ref 3.0에서 제공되는 암호체계

2) SSL Plus

SSLRef 3.0의 변형으로서 컨센서스 개발사에 의해 개발되었으며, 특징 및 사용 제약 조건으로는 SSL3.0 이후의 후속 버전인 TLS(Transport Layer Security) 프로토콜을 지원 가능토록 설계되었고, VeriSign의 인증서 요청(Certificate Request) 툴을 포함하였으며, 상업적 목적으로만 배포된다는 것이다.

3) OpenSSL

미국내에서 개발된 SSL 참조 라이브러리들이 대부분 수출 금지 품목이 되자 국제적으로 SSL 라이브러리 개발의 필요성이 대두되었으며, 1990년대 중반 호주의 Eric A. Young은 SSLeay라는 SSL 참조 라이브러리를 개발하였다. 이것은 초기 SSLeay라는 이름으로 사용되었으며, SSLeay 0.9.3 버전이후 더 많은 개발자와 수정자들의 참여 아래 OpenSSL로 이름이 바뀌었다. 특징 및 사용 제약 조건으로는 DES, RSA, RC4, IDEA, Blowfish 암호 알고리즘 지원하고 있으며, 호주에서 개발된 라이브러리이므로 미국의 암호 수출제약을 받지 않고 전 세계 국가에서 이용가능하다는 것이다. 또한, OpenSSL은 비상업적 · 상업적 이용이 모두 가능함과 동시에 라이센스에 따른 수수료는 전혀 없다.

IV. 결 론

최근 전자상거래 환경에서 웹 관련 보안 프로토콜의 적용이 크게 늘어나고 있다. S-HTTP 프로콜은 초기 시장을 형성할 수 있는 분위기를 가졌으나, 현재는 SSL 프로토콜 사용 활성화로 인하여 현재는 거의 사용되지 않고 있다.

반면에 SSL은 웹 관련 보안 프로토콜로서 그 자리를 확고히 하고 있으며, 최근에는 전자지불을 위하여 SET 및 Non-SET 지불 시스템보다 많은 사용빈도를 나타내고 있다. 현재 SSL3.0 후속 버전인 TLS 프로토콜이 개발되어 표준으로 제정되고 있는 상태이며, SSL을 지원하고 있는 많은 제품들이 이러한 TLS 프로토콜의 적용을 계획하고 있다. 이러한 SSL 프로토콜 사용의 활성화는 SSL 서버용 인증서 시장을 촉진케하는 원동력이 되었으며, 이로 인하여 많은 인증기관(Certification Authority)들이 등장하게 되었다.

향후 SSL 프로토콜은 지속적으로 사용될 것으로 예상되며, TLS의 표준 정립 이후에는 TLS가 SSL을 대치해 나아갈 것이라는 예측을 조심스럽게 할 수 있을 것이다.

기 능	표 현
RSA SHA 인증 + 비암호화	SSL_RSA_WITH_NULL_SHA
RSA MD5 또는 SHA 인증 + 수출 불가능한 RC4 암호화	SSL_RSA_WITH_RC4_128_MD5 & SSL_RSA_WITH_RC4_128_SHA
RSA SHA 인증 + Triple-DES 암호화	SSL_RSA_WITH_3DES_SHA
RC4 암호화와 SHA를 이용한 익명기능을 갖는 Diffie-Hellman 키교환	SSL_DH_anon_WITH_RC4_128_SHA
Triple-DES 암호화와 SHA를 이용한 익명기능을 갖는 Diffie-Hellman 키교환	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA

표 4. SSL PLUS에서 제공되는 암호체계

※참 고 문 헌

[1] Kipp Hickman "The SSL Protocol (version 2)", Netscape Communication Cooperation, 9 Feb. 1995

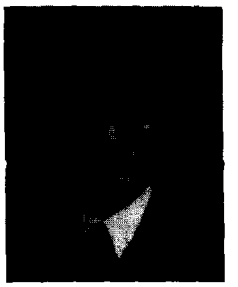
[2] Alan O. Freier, Philip Karlton, Paul C Kocher "The SSL Protocol (version 3)", Netscape Communication Cooperation, 9 Feb. 1995

[3] Jeremy Bradley, "The SSL Reference Implementation Project", University of Bristol, 2 Oct. 1995

[4] http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

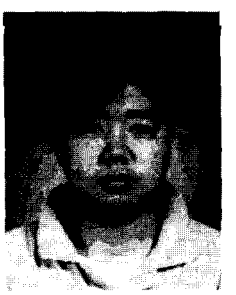
[5] http://www.consensus.com/security/ssl-talk-sec01.htm

[6] http://www.psy.uq.oz.au/~ftp/crypto/



홍 기 융

1985년 2월 전남대학교 전자계산학과 학사
1990년 2월 중앙대학교 전자계산학과 석사
1996년 2월 아주대학교 컴퓨터공학과 박사
1994년 8월 정보처리기술사
1985년 9월~1995년 10월 ETRI 선임연구원
1992년 9월~1993년 6월 Italy Alenia Spazio사 선임연구원
1995년 10월~1996년 4월 한국전산원 선임연구원
1996년 4월~1999년 현재 한국정보보호센터 인증관리팀장
※관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 평가, 정보보호표준화, 전자상거래 보안, 전자서명 인증, 공개키기반구조(PKI)



최 영 철

1996년 2월 성균관대학교 정보공학과 학사
1998년 2월 성균관대학교 전기·전자·컴퓨터공학부 석사
1998년 1월~현재 한국정보보호센터 연구원
※관심분야 : 암호학, 전자상거래 보안, 공개키기반구조