□ 기술해설 □

월드 와이드 웹 보안 기술 및 동향

한국전자통신연구원 박정수·강신각·박성열

1. 서 론

웹은 일반적으로 분산되어 있는 하이퍼미디어 정보를 검색하기 위한 시스템이라 할 수 있다. 여기서 하이퍼미디어는 하이퍼텍스트와 멀티미디어의 개념이 통합된 것으로, 웹을 이용하면 세계 각지에 분산되어 있는 텍스트, 그래픽, 영상, 그리고 사운드 등으로 구성되는 정보를 동적으로 검색할 수 있게 된다. 이와 같이 초창기의 웹은 공개적으로 게시된 정보를 검색하는데 주로 이용되었으며, 보안은 고려되지 않았다. 그러나 점차적으로 웹의 편리함과 효용성이 알려지면서 전자메일, 그룹웨어 응용, 전자상거래 등 광범위한 분야로 이용이 확대되고 있다. 특히 인터넷상의 전자상거래는 시장 잠재력이 무한한 분야로써 여러 회사에서 관심을 가지고 적극적으로 사업화에 나서고 있으며, 현재 인터넷 상에는 많은 쇼핑몰이 출현하고 있다.

이와 같이 웹을 이용한 다양한 응용의 개발로 인해 보안성 문제가 제기되기 시작하였다. 본 고에서는 웹 보안 요구 사항, 간단한 웹 보안 기법, 암호 기술을 이용한 보안 기법을 소개한다. 또한 IETF(Internet Engineering Task Force)나 W3C(World Wide Web Consortium)와 같은 웹 관련 그룹들과 각 업체들에서 추진되고 있는 웹 보안 기술의 연구 개발 동향을 살펴본다.

2. 웹의 보안 취약성과 보안 요구 사항

2.1 웹 클라이언트 시스템 보안 취약성

웹 클라이언트에서 일어날 수 있는 위협의 한 형태로는 사용자에게 그래픽 인터페이스를 제공해 주는 브라우저와 함께 사용되는 외부 표시기(External Viewer)에 존재할 수 있는 보안 구멍(Security Hole)을 찾아내 브라우저 및 사용자 컴퓨터에 비인가된 접근을 시도할 수도 있다. 특히 인터넷에서 개발되어 공개되는 외부 표시기 프로그램에 누군가가 악의적으로 보안 구멍을 만들어 배포한다면, 이 공개 프로그램을 사용하는 사용자 컴퓨터는 그대로 보안 위협에 노출되게 된다. 이러한 위협을 막기 위해서는 사용되는 각종 프로그램에 보안 구멍이 존재하지 않는 지를 주의깊게 살펴보아야 하며, 이는 CERT 등과 같이 각종 보안 위협에 대한 정보 및 대응 방안을 제공해 주는 관련 게시판이나 뉴스 그룹으로 부터 도움을 받을 수 있다.

또 다른 위협의 형태로는 불법적인 서버에 의해 클라이언트가 공격받을 수 있다. 약간의 전문 지식만 있으면 어떤 사용자도 손쉽게 웹 서버를 설치할 수 있기 때문에, 악의를 가지고 서버를 설치하여 이 서버에 접속을 시도하는 클라이언트 정보를 빼내거나 클라이언트 시스템을 손상시킬 수도 있다.

이러한 위협에 대한 보호 방안으로는 Java와 같이 클라이언트에서 실행되는 프로그램의 안전성을 보장해 줄 수 있는 새로운 언어를 이용하는 방안과, 클라이언트에 대한 접근을 제한할 수 있도록 방화벽(Firewall) 시스템이나 프락시(Proxy)를 설치하는 방안이 있다. 그러나 방화벽 시스템을 사용하는 경우에도 트로이 목마를 포함하는 웹 문서에 대해서는 보호할

수 없다.

2.2 웹 서버 시스템 보안 취약성

서버에서의 가장 큰 보안 취약성은 CGI (Common Gateway Interface) 프로그램에 있다. CGI는 URL에 의해 지정된 서버 측의 프로그램을 실행해 클라이언트 측에 자료를 전송하거나 서버 측의 자료를 전송받는 등의 작업을 위해 만들어진 인터페이스이며, 현재 많은 CGI 응용 프로그램이 개발되어 있다. 사용자는 서버 측의 특정 디렉토리를 지정하여 특정 프로그램을 실행할 수 있으므로 보안 측면에서 볼 때 이것은 큰 취약성을 제공할 수 있다. 따라서 CGI 프로그램을 사용할 때에는 몇 가지 주의 사항이 요구되는데 먼저, CGI 프로그램이 들어갈 디렉토리를 특정 디렉토리로 제한하고 서버 셋업시 CGI 프로그램이 실행될 수 있는 디렉토리를 명확히 지정하는 것이 필요하다. 또 다른 방안으로는 확인되고 검증된 CGI 프로그램만을 사용하도록 제한할 필요가 있다.

이밖에 서버 프로그램(httpd)을 실행시킬 때 루트 권한으로 실행시키지 않아야 하며, 서버의 실행 디렉토리도 제한된 파일 시스템으로 지정하는 것이 안전하다. 또한 가능하면 HTTP 프로토콜 요소 중 POST 방식의 사용을 제한하는 것이 좋다.

2.3 웹 응용 보안 요구 사항

웹은 보안을 별로 염두에 두지 않고 설계되었기 때문에 보안을 요구하는 민감한 분야에서는 사용하기가 적합치 않은 것이 사실이다. 단순한 정보 검색만이 아니라 신용카드 정보와 같은 타인에게 노출되어서는 안될 중요한 정보를 전송하는 민감한 응용에 웹을 이용하고자 할 때 요구되는 보안 요구 사항을 응용 분야에 따라 살펴보면 다음과 같다.

● 폐쇄 집단의 구성원간에 정보를 공유하기 위한 응용 : 특정 그룹 구성원 사이에서만 민감한 정보를 공유하고자 하는 형태로, 서버의 정보에 접근하는 클라이언트를 제어하기 위해 클라이언트에 대한 인증서비스가 요구된다.

● 안전한 채널을 통한 비밀 정보의 교환 응용 : 구매 주문서나 공문서 같은 중요한 정보를 발행하고자 할 때, 클라이언트와 서버는 상호 인증 서비스를 제공해야 하며, 교환되는 메시지 또는 문서 자체에 대한 인증도 요구된다.

● 전자 지불 응용 : 웹을 이용하여 상품, 재화 또는 비밀정보 등을 상거래하기 위해, 판매자의 정당성 인증과 구매자의 안전한 지불 기능을 요구한다. 이때 판매자와 구매자를 위한 인증 서비스는 대체적으로 제삼자에 의해 이루어진다.

● 기밀성 서비스 응용 : 웹을 이용하여 교환되는 정보 자체가 타인에 노출되지 않아야 하는 통신 비밀 보장 서비스가 요구된다.

이러한 보안 요구 사항들을 정리해 보면 안전한 웹 응용 서비스를 제공하기 위해서는 웹 클라이언트 인증, 웹 서버 인증, 웹 서버상의 문서 정보에 대한 접근제어, 서버와 클라이언트 사이에 일어나는 트랜잭션 데이터의 인증, 무결성, 그리고 기밀성 서비스가 요구된다.

3. 간단한 웹 보안 기법

대부분의 브라우저 사용자들은 신원을 밝히지 않은 상태로 서버에 접근하고, 서버의 신원도 확인할 길이 없어 브라우저 사용자들은 불법적인 공격자에 의해 원하던 홈페이지와는 다른 서버의 홈페이지가 전송되어도 이를 알 수가 없다. 이와 같은 웹의 익명성은 서버 측의 접근 제어 서비스를 구현하기 어렵게 하고, 메시지는 평문의 형태로 전송되기 때문에 기밀성도 기대할 수 없는 실정이다. 현재 일반적으로 널리 이용되고 있는 간단한 웹 보안 기법으로는 다음과 같은 방식들이 있다.

3.1 기본 인증(Basic Authentication)

이 인증 기법은 HTTP(HyperText Transport Protocol) 1.0 규격 이상에서 정의되고 있으며, 대부분의 브라우저와 서버에서 구현되어 있다. 인증 절차를 살펴보면, 먼저 사용자 ID와 대응되는 패스워드 정보는 이전의 트랜잭션을 통해 안전하게 교환되어야 하며, 서버는 교환된 정보를 암호화된 상태로 보관하게 된다. 그 후에 접속을 시도하는 사용자의 전송된 패스워드를 암호화하여 저장된 값과 일치여부를

확인하여 접속을 허용하게 된다. 이 경우 단순하다는 장점은 있으나 사용자 패스워드가 그대로 망에 노출된 채 서버로 전송되므로 재연 공격(Replay Attack)에 취약하고, 서버는 사용자 ID와 패스워드 정보를 관리해야 하는 부담이 있다.

3.2 망 주소를 이용한 접근 제어

이 기법은 IP(Internet Protocol) 필터링이라고 불리며, 클라이언트 시스템마다 부여되어 있는 고유의 망 주소 정보를 이용하여 서버로의 접근을 제어하는 것이다. 특히, 망 주소의 구조적 특성을 이용하여 특정 도메인에 속하는 클라이언트 집합에 대해서도 손쉽게 접근 제어가 가능하다. 또한 사용자 ID와 패스워드를 도용하여 접속을 시도하는 위협을 어느 정도 차단 가능하므로 현재 널리 사용되고 있다.

기본 인증 기법처럼 사용자 ID와 패스워드가 노출되지 않으므로 안전하지만, 대개의 공격자는 자신의 IP 주소를 변조할 수 있기 때문에 가장 공격(Masquerade Attack)에는 취약하다. 또한 컴퓨터 단위로 접근 제어를 제공하기 때문에 사용자별 접근 제어는 기대할 수가 없다. 그래서 기본 인증 기법과 망 주소를 이용한 기법을 결합한 형태가 주로 이용되고 있다.

3.3 메시지 다이제스트 인증 (Message Digest Authentication)

전송할 데이터에 일방향 특성을 갖는 메시지 다이제스트 함수를 적용하여 서버에 전송하는 방법이며, 사용자 ID와 패스워드가 망상에 그대로 노출되는 기본 인증 기법의 단점을 보완하고 있다. 즉, 클라이언트 사용자 ID 및 패스워드 정보를 MD5와 같은 일방향 함수로 다이제스트하여 전송하면, 서버는 저장되어 있는 사용자 정보와 비교하여 인증하게 된다. 이때 재연 공격을 막기 위해 시간 정보를 함께 전송하는 것이 일반적이다.

현재 이 기법은 HTTP 1.1 규격 이상에서 정의되고 있으며, W3C의 Jigsaw 등에서 구현되고 있다. 일반적인 메시지 다이제스트 인증 모델은 그림 1과 같다.

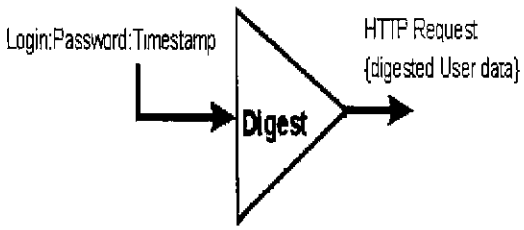


그림 1 메시지 다이제스트 인증 모델

4. 암호 기술을 적용한 웹 보안 기법

HTTP는 특정 정보로의 접근 프로토콜(Access Protocol)과 메시지 교환을 위한 구문 제공이라는 두 가지 특성을 가지고 있다. 접근 프로토콜 측면에서는 채널 보호가 요구되며, 구문 측면에서는 메시지 보호가 필요하다. 일반적으로 웹 보안 기술은 이와 같은 HTTP의 어느 특성에 중점을 두고 암호 기술을 적용하느냐에 따라 그림 2와 같이 세 가지로 분류할 수 있다.

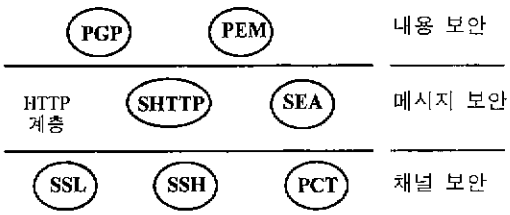


그림 2 계층별 보안 기법

4.1 채널기반 보안(Channel-based Security)방식

4.1.1 SSL(Secure Sockets Layer) Protocol

SSL은 넷스케이프사에서 개발된 프로토콜로 특정 웹 응용을 위한 보안 프로토콜이 아닌 일반적인 인터넷 보안 프로토콜로 사용될 수 있다. 그림 3에 표시된 바와 같이 웹 응용과 TCP/IP 통신 프로토콜 계층 사이에 존재하는

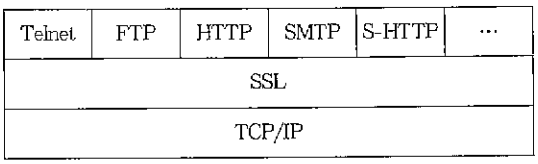


그림 3 SSL의 계층 모델

프로토콜이기 때문에 웹을 위한 HTTP 뿐만 아니라 Telnet, FTP(File Transfer Protocol) 등 다른 인터넷 응용들에도 적용될 수 있다. 현재 버전 3.0까지 나와 있다.

SSL은 인터넷 응용들간에 신뢰할 수 있는 채널을 통해 비밀보장 서비스 제공을 목표로 하며, 개념적으로 레코드 프로토콜(Record Protocol)과 핸드쉐이크 프로토콜(Handshake Protocol) 계층으로 구분된다. TCP 상위에 존재하는 레코드 프로토콜은 여러 가지 상위 계층의 프로토콜들을 캡슐화하기 위해 사용된다. 이런 캡슐화되는 응용 중의 하나가 핸드쉐이크 프로토콜이며, 서버와 클라이언트 각각에 대한 인증을 제공하고 암호 알고리즘과 암호 키들을 협상하기 위해 사용된다. 이와 같은 SSL 프로토콜에 의해 제공되는 보안 서비스는 다음과 같다.

- 두 통신 응용간의 비밀보장 서비스
- 클라이언트와 서버 인증 서비스
- 메시지 무결성 서비스
- 협상 서비스

통신 절차를 살펴보면 먼저 통신하고자 하는 응용 실체 사이에 공개키 암호화 기술을 이용한 소켓 루틴들을 사용하여 안전한 통신채널을 설정하고, 그후에 안전한 통신 채널을 통하여 응용 실체간에 정보를 교환할 수 있도록 하는 것이다. 이러한 SSL의 개념은 그림 4를 보면

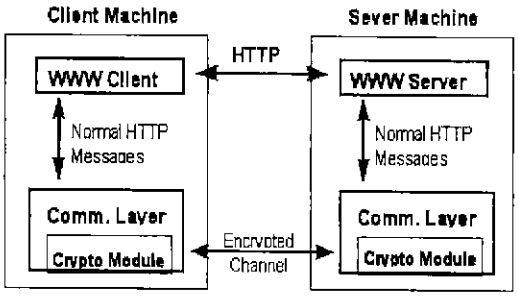


그림 4 SSL의 동작 모델

알 수 있듯이 웹 클라이언트와 서버 사이에는 정규의 HTTP 프로토콜에 의한 접속이 이루어지며, 이 HTTP 메시지는 통신망을 경유하여 전달될 때 하위 SSL 계층의 암호화 통신에 의해 보호되게 된다.

4.1.2 PCT(Private Communication Technology)

PCT 프로토콜은 두 통신 응용간에 비밀보장과 적어도 한 쪽 통신 실체(주로 서버)에 대한 인증 서비스를 제공하기 위해 설계되었다. 또한 HTTP, FTP, TELNET 등과 같은 응용 프로토콜과 독립적이고 이런 응용 프로토콜들은 상위에 놓여진다는 측면에서 SSL과 유사하다. 그러나 PCT는 SSL의 여러 가지 약점들을 수정하고 개선했으며 새로운 버전을 발표하면서 SSL과는 다른 새로운 특성들을 추가하였다.

수행 절차를 살펴보면, 먼저 핸드쉐이크 메시지를 전송하여 PCT 프로토콜 접속을 설정하며, 세션키를 협상하고 비대칭 공개키들(이전에 공유된 개인 패스워드)에 기반을 둔 인증 과정을 수행한다. 이 과정을 핸드쉐이크 단계라고 한다. 그후에 응용 데이터 메시지는 암호화와 무결성 서비스를 제공받으며 전송되게 된다.

4.2 내용기반 보안(Content-based Security) 방식

PGP 또는 PEM(Privacy Enhanced Mail)과 같은 외부 응용을 이용하여 트랜잭션 데이터를 암호화한 후 이 암호화된 문서를 HTTP를 통해 전송함으로써 데이터의 안전성을 보장하는 방식이다. 이 기술은 보통 MIME 표시기로 구현되며 성공적으로 개발될 수 있을 것으로 보인다. 현재 전자메일에서 암호화 및 전자서명을 위해 많이 쓰이고 있는 PGP와 모자익 웹의 CCI(Common Client Interface) 기능을 이용한 연구가 진행되고 있다. 물론 PEM과 Netscape Client API 또는 Plug-In 기술을 이용한 동일한 접근도 가능할 것으로 보인다.

이 방식의 기본 개념은 그림 5에서도 알 수

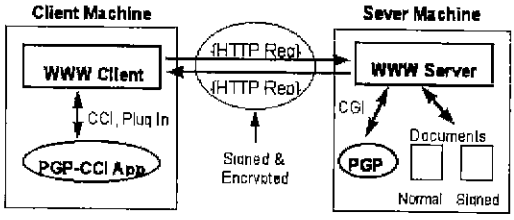


그림 5 PGP-Web의 동작 모델

있듯이 웹 보안을 위해 요구되는 암호화, 전자 서명 및 검증 그리고 키 관리 등의 기능을 전자메일 보안 도구로써 개발되어 널리 사용되고 있는 PGP를 이용해서 처리하고자 하는 것이다. 이를 위해서는 HTTP 확장, 새로운 HTML 앵커 속성의 정의, 그리고 CCI 기능의 확장 등이 추가되어야 한다. 그림 5는 PGP-Web의 동작 모델을 나타낸다.

4.3 메시지 기반 보안(Message-Based Security) 방식

4.3.1 S-HTTP(Secure HTTP)

1994년에 EIT의 Schiffman과 Rescorla는 HTTP에 보안 기능을 추가하는 응용 프로토콜인 S-HTTP를 발표하였다. S-HTTP는 기본적으로 클라이언트/서버 모델을 바탕으로 트랜잭션 단위로 통신을 하게 되며 종단간에 보안 서비스를 제공하도록 설계되었고, 트랜잭션 기밀성(Confidentiality), 메시지 무결성(Integrity), 발신자 인증(Authentication)과 발신 부인 봉쇄(Non-repudiability of Origin) 서비스를 제공한다. 또한 다양한 암호화 알고리즘과 동작모드를 제공하기 위한 협상 메커니즘을 지원한다.

HTTP 메시지는 요구되는 보안 기능 정도에 따라 암호화와 서명 메커니즘이 적용되고, PKCS-7이나 MOSS 형식에 따라 캡슐화되어 S-HTTP 메시지가 구성된다. 그리고 이 S-HTTP 메시지는 메시지의 형식과 부호화 방식 등을 표시해 주는 S-HTTP 헤더 정보와 함께 전달되게 된다. 그림 6에서도 볼 수 있듯이 앞 절에서 다룬 SSL과 S-HTTP의 중요한 차이점은 HTTP 메시지가 암호화 및 서명되어 보안 기능을 지원하지 않는 기존 TCP/IP 망을 통해 전송된다는 것이다.

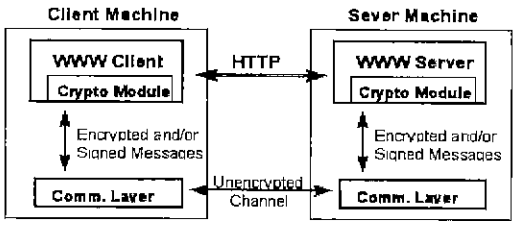


그림 6 S-HTTP의 동작 모델

4.3.2 PEP/SEA(Protocol Extension Protocol/Security Extension Architecture)

HTTP 메시지는 RFC 822 형식의 헤더 필드를 첨가함으로 확장될 수 있다. 그러나, 단지 확장만으로는 HTTP 에이전트에게 헤더의 분할, 헤더의 처리 방법, 동작 절차 등에 대해 공지할 수 없다. 게다가 다중 확장을 적용한다면 헤더 필드의 이름들이 충돌하게 될 것이다. 이런 요구 사항에 따라 개발된 PEP는 연관된 헤더 라인들을 명시하고 각각에 대한 지침을 제공한다. 또한 공통으로 사용될 프로토콜 확장에 관한 정보 집합을 협상할 수 있게 된다. 그러므로 PEP를 통해 HTTP 에이전트는 알려지지 않은 형태로 확장된 프로토콜들과도 상호 운용될 수 있다. 현재 위에서 기술한 개념의 타당성을 검토하기 위해 W3C에서는 참조 라이브러리를 이용해서 PEP를 구현하고 있다.

이와 같은 프로토콜 확장을 사용해서 HTTP/1.x 메시지를 안전하게 전송하기 위한 구조를 정의한 것이 SEA이며, 이 문서는 HTTP와 안전한 결합을 위한 요구 사항과 서명, 암호화, 키 교환 기능을 기술하고 있다. SEA는 S-HTTP 모델을 채택하여 PEP 위에서 그 기능을 모듈 구조로 구현하려는 설계 원칙 때문에 기능면에서 S-HTTP와는 큰 차이는 없지만, S-HTTP에 비해 아직은 규격이 안정적이지 못하다. 그러나, S-HTTP는 완전한 새로운 프로토콜인데 반해 PEP/SEA는 HTTP를 확장하는 형태이므로 역호환성(Backward compatability)을 제공한다. 또한 추후에 다른 기능을 첨가하고자 할 때 더 용이하다.

5. 주요 연구 동향

보안 관련 연구는 여러 단체를 통해 여러 분야에서 연구가 진행되고 있다. 특히 웹 보안 관련 연구는 다양한 응용 분야에 따라 IETF 보안 그룹들, W3C, 그리고 각 업체 등에서 추진되고 있다. 이들 중에서 가장 활발하게 활동하고 있는 주요 단체들의 연구 동향을 소개한다.

5.1 IETE보안 그룹 동향

보안 관련 9개 WG 중에서 TLS(Transport

Layer Security)와 WTS(Web Transaction Security) WG은 웹 보안과 관련이 깊은 작업반이다. WTS WG에서는 앞서 설명한 S-HTTP 규격 개발 작업을 추진하여 S-HTTP 1.2를 개발하였고 RFC 문서로 채택되기 위해 IESG(Internet Engineering Steering Group)에 제출된 상태이다. TLS WG는 수송 계층 위에서 인터넷 호스트간에 안전하고 인증된 채널을 제공하는 방법을 제시하는 것을 목표로 하고 있다. 1996년 12월 산호세에서 개최된 37차 IETF 회의에서 활발하게 논의된 TLS WG와 보안 관련 BOF 모임들에 대해서 살펴보면 최근의 IETF에서의 웹 보안 관련 연구 동향을 파악할 수 있으므로 이를 간략하게 소개한다.

먼저 1996년 12월 IETF TLS WG 회의에서는 넷스케이프사의 SSL 버전 3.0을 TLS 1.0으로 전환하여 발전시키고 다음 총회 이전에 PS(Proposed Standard)로 추진하기로 결정했다. 또한 TLS로 전환하기 위해서 요구되는 SSL의 수정 및 기능 첨가에 관한 논의도 이루어졌다.

또한 이번 회의에서는 SPKI(Simple Public Key Infrastructure), SMIME(Secure MIME)과 PGPMIME(MIME Security with PGP) BOF가 개최되었다. SPKI BOF는 PKIX WG의 활동이 지지부진한 이유를 진단하고, PKIX WG에서 연구되고 있는 공개키 관련 표준이 복잡하므로 단순하고 사용하기 쉬운 새로운 공개키 인증서, 관련 서명 양식, 키 분배 프로토콜 등의 개발을 목표로 하고 있다. 이 때 X.509나 ASN.1은 배제하고 있다. SMIME BOF는 RSADSI사의 PKCS에 기반한 S/MIME의 표준화를 목표로 하고 있으며, 이를 통해 구현 개발자간에 호환성을 제공함으로써 S/MIME을 널리 보급하는 활동을 하고자 하고 있다. PGPMIME BOF는 RFC 2015를 기반으로 널리 보급되어 있는 PGP에 대한 현실을 인정하고 표준화 노력을 통해 PGP를 사용하는 MIME 소프트웨어들의 호환성을 추구하고 있다.

5.2 W3C 보안 그룹 동향

W3C의 보안 그룹들은 웹 트랜잭션 보안, 전자 상거래, 시스템 보안 등을 연구하고 있다. 이 그룹은 IETF의 WTS WG와 보안 그룹에는 속하지 않지만 HTTP WG와 동일을 목표를 가지고 연구하고 있다. 앞 절에서 언급한 PEP, SEA 등은 이 그룹의 결과물이다. PEP는 계속적인 연구가 진행되고 있지만 SEA는 더 이상 진전을 보이고 있지 않다. 현재 W3C는 전자 상거래에 관련된 활동에 더욱 힘쓰고 있으며, 1994년 4월에 조직된 인터넷 상거래와 관련된 업체들의 연합체인 CommerceNet과 함께 JEPI(Joint Electronic Payment Initiative) 프로젝트를 수행하고 있다. 이 프로젝트의 목표는 새로운 지불 프로토콜을 개발하고자 하는 것이 아니라 기존의 다양한 지불 프로토콜을 선택하고 협상할 수 있는 방법을 제시하는 것이다. 일단계 목표는 지불 프로토콜들을 자동 선택할 수 있는 PEP를 사용한 UPP(Universal Payment Preamble)의 개발에 있다.

5.3 업체 동향

웹 보안 관련 업체들과 조직들에 대해서 살펴보면, 지불 프로토콜과 같은 인터넷 상거래에 관련된 CyberCash Inc., Digicash Co., First Virtual 등이 있으며, 웹 브라우저 개발에 힘을 쏟고 있는 마이크로소프트사, 넷스케이프사 등이 있으며, 웹 관련 알고리즘이나 메커니즘을 연구하는 RSA Data Security Inc., Terisa 시스템 등이 있다.

이들 중에서 마이크로소프트사는 자사의 웹 브라우저인 인터넷 익스플로러에 PCT 및 SSL을 기본적으로 지원하고 있으며, 운영체제인 Win95와 인터넷 검색을 위한 인터넷 익스플로러를 통합시키는 작업을 진행중이다. 넷스케이프사는 자체 개발된 SSL 메커니즘을 통해 브라우저의 보안 기능 향상에 노력을 기울이고 있다.

Terisa 시스템에서는 넷스케이프 브라우저에 S-HTTP를 Plug-In 형태로 접목한 "Secure Web"이라는 제품을 개발하여 상용으로 판매하고 있다. 사용되는 예를 보고자 하면 http://www.terisa.com : 80/products/swd/index.html 홈페이지를 방문해 보시기 바란다. 이와 관련하여 NCSA에서는 S-HTTP 1.1 규격을 지원하는 Secure Mosaic과 Secure httpd가

있다.

6. 결 론

본 고에서는 최근 웹으로 대표되는 인터넷 서비스가 점차 상업적인 목적으로 발전해 가면서 요구되고 있는 인증, 접근 제어와 기밀성 서비스와 같은 보안 요구 사항들을 지원하기 위한 다양한 웹 보안 프로토콜들의 기본 개념과 연구 동향에 대해 기술하였다. 제시된 여러 방식중 어느 방식이 앞으로 웹의 표준 보안 프로토콜로 사용될 지는 아직 미지수이며, 인터넷의 특성상 반드시 우위의 기술력을 가진 응용들이 살아남은 것은 아니므로 넷스케이프와 마이크로소프트사의 브라우저와 주요 웹 서버가 어떤 방식을 지원할 것인지가 무엇보다도 중요한 변수일 것이다. 앞으로의 발전 방향을 살펴보면, 시스템 운영체제와 웹 검색 기능이 통합되어 사용자는 자신의 하드디스크에 있는 정보를 검색하는 것처럼 보이게 될 것이다. 즉, 검색하기 위해 브라우저와 같은 것을 다시 띄울 필요가 없게 된다는 것이다.

웹 보안 관련 국내 현황을 살펴보면 현재 대부분의 웹 시스템 및 도구를 외국제품에 의존하고 있는 상황이다. 그러나 보안의 특수성에 비추어 볼 때 외국의 보안제품 및 기술을 그대로 국내에 적용하여 사용하기에는 여러 가지 문제가 있다. 특히 미국은 수출에 있어 특별한 암호 정책을 고수하고 있기 때문에, 적어도 보안 알고리즘은 국내 사정에 맞는 방식을 개발하고 이를 지원하는 제품을 자체적으로 구현, 사용할 수 있도록 연구 개발에 힘을 쏟아야 할 것이다.

참고문헌

[1] http : / / www.osf.org / www / dceweb / slides/Ogmc/sld008.htm, "The Secure Web".

[2] http : / / www.cs.unc.edu / Courses / wwwc/public/hanes/security.html, Security Issues in WWW.

[3] http : / / www.microsoft.com / intdev / security/securit.html, Microsoft Internet Security Framework.

[4] A. Cain, "Security, Authentication, and Privacy on the Web," Fourth International WWW Conference, 1995.

[5] R. Fielding, J. Gettys, J. Mogul, H. Frystyk and T. Berners-Lee, Hypertext Transfer Protocol-HTTP/1.1, draft-ietf-http-v11-spec-07.txt, 1996.

[6] A. Freier, P. Karlton, and P. Kocher, The SSL Protocol Version 3.0, 1996.

[7] D. Simon, Microsoft Corporations PCT Protocol, draft-benaloh-pct-01.txt, 1996.

[8] http : //www.cs.hut.fi/ssh/, SSH(Secure Shell) Remote Login Program, SSH Communications Security Ltd.

[9] J. Weeks, etc, CCI-Based Web Security : A Design Using PGP, WWW Journal 95, 1995.

[10] E. Rescorla and A. Schiffman, The Secure HyperText Transfer Protocol, draft-ietf-wts-shttp-03.txt, 1996.

[11] E. Rescorla and A. Schiffman, Security Extension for HTML, draft-ietf-wts-shtml-02.txt, 1996.

[12] R. Khare, "PEP : an Extension Mechanism for HTTP," W3C Working Draft 31(http : //www.w3.org/pub/WWW/TR/WD-http-pep.html), 1997.1.

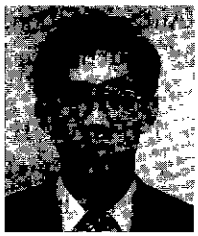
[13] R. Khare, SEA : A Security Extension Architecture for HTTP/1.x, WD-http-sea-960108, 1996.

[14] http : / / www.osf.org / www / decweb, OSF DCE Web Technology.

[15] http : / / snapple.ncsa.uiuc.edu / adam / khttp/intro.html, Kerberizing the Web.

[16] 장혁수외 4명, "제37회 IETF 회의 참가 보고," 개방형컴퓨터통신연구회 개방시스템지 제10권 제6호, 1996년 12월.

[17] A. Medvinsky and M. Hur, "Support for Kerberos in TLS," 37th IETF Meeting, 1996. 12.



박 정 수

1992 경북대학교 전자공학과 학사
1994 경북대학교 전자공학과 석사
1994～현재 한국전자통신연구원 멀티미디어표준연구실 연구원
관심분야 : 인터넷 보안, 멀티미디어 보안

강 신 각

1984 충남대학교 전자공학과 학사
1984～현재 한국전자통신연구원 멀티미디어표준연구실 선임연구원
1987 충남대학교 전자공학과 석사
관심분야 : 통신망 보안, 멀티미디어 통신

박 성 열

1973～1978 한국과학기술원 연구원
1982 Univ. of Florida 산업공학과 석사
1984 연세대학교 전자계산학과 석사
1987 Auburn Univ. 산업공학과 박사
1987～현재 한국전자통신연구원 정보기술개발단 단장
관심분야 : 분산처리, 정보보호, 인터넷 응용

● 제24회 임시총회 및 춘계학술발표회 ●

- 일 자 : 1997년 4월 25(금)～26일(토)
- 장 소 : 한림대학교
- 문 의 처 : 한국정보과학회 사무국
  T. 02-588-9246, F. 02-521-1352