SecWeb : S-HTTP 기반의 안전한 웹 시스템 개발

조 은 경† · 박 정 수†† · 강 신 각†† · 박 성 열†††

요 약

다양한 연구분야에서 웹을 대부분 응용의 프레임워크 또는 GUI로 사용하려는 거역할 수 없는 흐름에 발 맞추어 국내에서도 전자상거래와 관련한 법규가 가시화될 전망으로 웹을 이용한 상거래 움직임 또한 더욱 활발 할 것으로 보인다. 이와 같이 다양해지는 웹 응용을 위해서는 지금까지의 웹 보안 기술로 부인봉쇄와 같은 보안 서비스를 제공하지 못하고 있다. 본 논문에서는 최근 다양해지는 웹 보안 요구 사항을 만족시키는 웹 프로토콜로 IETF에 의해 제안된 S-HTTP(Secure HTTP, Secure HyperText Transfer Protocol)를 기반으로 하는 안전한 웹 시스템인 SecWeb의 개발을 위한 시스템 모델,구현 환경 및 개발된 시스템 그리고 적용 가능한 시나리오를 기술하였다. 개발된 SecWeb의 대표적인 응용분야로는 전자서명에 의한 부인봉쇄서비스가 중요하게 요구되는 분야들을 생각할 수 있다.

The Development of a Secure Web System based on S-HTTP : SecWeb

Eun-Kyung Cho† · Jung-Soo Park†† · Shin-Gak Kang†† · Sung-Yul Park†††

ABSTRACT

Recently, web is being proposed as a framework or graphical user interface in the various research fields. Together with this main stream, the regulation of EC (Electronic Commerce) will be prepared within nation wide and also it is expected that the usage of web in the field of EC will be prevailing. However, Until yet there is no way to provide non-repudiation security service. In this paper, we first describe the security requirements for secure web business, summarize the related work, then describe the system model, implementation environment, development of SecWeb, secure web system based on Secure HyperText Transfer Protocol (S-HTTP) which is proposed by IETF and some scenarios. SecWeb is best fit in the field of some applications which non-repudiation service by digital signature is significantly required.

1 서 론

지금까지 웹에서의 보안을 위해 사용되어온 방법으로는 기본 인증/IP 필터링/메시지 다이제스트 인증에 의한 접근제어와 같은 방법이 이용되었다. 이와 같은 기술들은 간단하나 점점 복잡, 다양해지는 웹 응용에서의 보안 요구사항 들을 근본적으로 해결할 수 없는 방법으로 기본적인 클라이언트 인증 서비스가 제공되고 있을 뿐이다. 이와 같은 웹 보안 기술에 대해 간단히 살펴보면 먼저, 사용자 ID(Identification)와 대응되는 패스워드 쌍을 'uuencode'로 변환하여 서버로 전송하는 기본 인증(Basic Authentication)은 단순하지만

† 정 회 원 : 대덕대학 전산교육팀 교수
†† 정 회 원 : 한국전자통신연구원 표준연구센터
††† 종신회원 : 한국전자통신연구원 슈퍼컴퓨터센터 센터장
논문접수 : 1997년 10월 28일, 심사완료 : 1998년 10월 13일

사용자 ID와 패스워드가 네트워크에 평문으로 흐르는 단점이 있다. 이를 해결하는 방법으로 사용자 정보에 일방향 특성을 갖는 메시지 다이제스트 함수를 적용한 값을 서버에 전송하는 메시지 다이제스트 인증 방법에 의해 사용자 ID와 패스워드가 네트워크상에 그대로 노출되는 기본 인증 기법의 단점을 보완하고 있다. IP(Internet Protocol) 필터링이라고도 불리는 네트워크 주소를 이용한 접근 제어 기법은 클라이언트 시스템마다 부여되어 있는 고유의 네트워크 주소 정보를 이용하여 서버에의 접속을 제어하는 것이다. 이 기법은 기본 인증 기법처럼 사용자 ID와 패스워드가 노출되지 않으므로 안전하지만, 대개의 공격자는 자신의 IP 주소를 변조할 수 있기 때문에 가장 공격(Masquerade attack)에는 취약하다.

살펴본 바와 같이 웹은 처음부터 보안을 별로 염두에 두지 않았기 때문에 다른 대부분의 인터넷 도구들과 마찬가지로 보안을 요구하는 민감한 분야에서는 사용하기가 적합지 않다. 그러나 최근 웹은 단순한 정보 검색만이 아닌 신용카드 정보와 같이 타인에게 노출되어서는 안될 중요한 정보의 전송 등 다양한 용도로 사용하고자 하는 욕구로 다음과 같이 다양한 응용에 따른 보안 서비스가 요구된다.

- 폐쇄 집단 구성원간의 정보 공유 : 특정 집단 구성원 사이에서 중요한 정보를 공유하고자 하는 형태로 서버에 접근하는 클라이언트를 제어하기 위해 클라이언트 인증 서비스가 요구되며 특정 정보로의 접근을 제한할 수 있다.
- 중요 정보를 안전한 방법으로 교환/발행하기 위한 응용 : 구매 주문서를 제출하거나 공문서 같은 중요한 정보를 발행할 때 클라이언트/서버 정보의 출처가 진짜인지와 데이터가 중간에 변경되지 않았음을 증명하는 부인봉쇄 서비스가 요구된다. 또한 이것은 클라이언트와 서버에 대한 상호 인증 서비스를 요구하며 교환되는 메시지 또는 문서 자체에 대한 인증도 요구된다.
- 전자 지불 응용 : 웹을 이용한 전자 상거래 응용은 트랜잭션에 포함된 당사자 특히 판매자의 정당성을 입증하기 위해 인증을 포함할 수 있으며, 구매사의 지불 자체에 대해 제삼자에 의한 검증이 필수적으로 요구된다.
- 기밀성 서비스 응용 : 웹을 이용하여 교환되는 정보 자체가 타인에 노출되거나 변경되지 않기를 바라는 기밀성 서비스가 요구된다.

이러한 다양한 웹 응용에 따른 요구 사항들을 요약하면 클라이언트 인증, 서버 인증, 서버상의 문서에 대한 접근 제어, 서버와 클라이언트 사이에 일어나는 트랜잭션 데이터 인증, 부인봉쇄, 그리고 기밀성 서비스가 요구된다. 이와 같은 보안 서비스 요구사항을 제공하기 위한 S-HTTP기반의 웹 보안시스템인 SecWeb 은 전자서명, 암호 및 인증을 이용하여 기밀성, 무결성, 부인봉쇄, 메시지 및 사용자 인증 서비스를 제공하는 웹 시스템으로, 본 논문에서는 SecWeb의 시스템 모델 및 설계, 개발환경, 개발된 시스템 및 적용 시나리오 등을 기술하였다.

제 2장에서는 관련 연구를 요약하여 기술하였으며, 3장에서 SecWeb시스템의 기반이 되는 S-HTTP에 대한 개괄적인 설명을 하였으며, 4장에서는 SecWeb시스템의 시스템 모델 등 시스템 설계에 대해 기술하였고, 5장에서는 시스템을 개발하는데 이용된 주요기술을 기술하였다. 그리고 6장에서는 개발된 SecWeb 및 적용시나리오에 대하여 기술하였으며, 마지막으로7장에서는 향후 방향 및 S-HTTP 및 SSL(Secure Socket Layer) 기반의 웹 시스템에 대한 간단한 비교로 결론을 맺었다.

2. 관련 연구

일반적으로 웹 보안 기술은 HTTP에 암호 기술을 어떻게 적용하느냐에 따라 크게 3가지 방향으로 연구[3]가 진행되고 있다. HTTP 응용계층에서 적용하는 내용보안, HTTP계층에서 적용하는 메시지 보안, 그리고 HTTP 하위 계층에서 HTTP와는 무관하게 보안서비스를 제공하고자 하는 채널보안이 이에 해당한다.

- 채널 보안(Channel Security)

FTP, HTTP등과 같은 응용아래에서 응용과 무관하게 채널의 보안을 제공한다. 대표적으로 넷스케이프의 SSL이 이에 해당한다. 유사한 목적을 제공하는 것으로는 IPsec와 GSSAPI(Generic Security Service API)가 HTTP에 대한 사전동작으로 작동한다. 이들은 링크레벨의 접근으로 메시지 보안의 장점인 스트림에서 완벽하고 안전한 분석으로써 메시지를 추출하는 능력을 제공하기가 어렵다.

- 메시지 보안 (Message Security)

HTTP의 병행하는 방법(parallel mechanism)으로, 상규의 HTTP/1.x 메시지에 대해 외부의 가려개(En-

veloping) 계층을 생성하기 위해 HTTP와 HTML에 보안기능을 추가한다. IETF에서 제안한 S-HTTP와 W3C(World Wide Web Conference)가 S-HTTP의 논리적 보안모델을 HTTP/1.x 개발로 유도하려는 SEA (Security Extension Architecture)가 이에 속한다.

● 내용 보안(Content Security)

HTTP와 PGP(Pretty Good Privacy), PEM(Privacy Enhanced Mail) 등과 같이 기존에 개발되어 있는 암호 시스템과 연계시키는 방식으로, PGP로 암호된 문서와 같이 응용에서 외부적으로 보호된 데이터를 HTTP를 통해 전송하는 방법이다.

이와 같은 세가지 방법에 대한 비교를 <표 1>에 정리하였다. 채널보안의 장점으로는 즉시 확산가능하며, 널리 적용이 가능하다는 것이며, 단점으로는 메시지를 구분할 수 없고 보안정책을 향상시킬 수 없다. 메시지 보안의 장점으로는 모든 HTTP 속성이 보호되며 각 자원에 적절한 정책을 수용할 수 있으며 보호된 메시지를 분리 가능하며 보안과 관련한 알고리즘등의 협상이 가능하다는 것이다. 그러나 단점으로는 기존의 HTTP와 하나로 이루어진 구현물 형태(Monolithic Implementation)로 구현이 되어야 하기에 어렵다는 것이다. 그리고 내용보안의 장점은 즉시 확산가능하지만 응용계층보안을 대체할 수는 없다. <표 1>과 같은 여러가지 접근 방식중 본 논문에서는 메시지 보안방식에 속하는 Secure HTTP(S-HTTP)를 기초로 하는 웹 보안시스템인 SecWeb의 개발에 대해 기술하고자 한다. 앞서 언급하였듯이 메시지 보안 방식은 채널보안 방식에 비해 HTTP 메시지 단위로 구분하여 보호를 할 수 있고 보안 정책도 적용 할 수 있어 채널보안과 같은 all or nothing 정책이 아닌 사용자의 필요에 따라 보안 서비스를 적용할 수 있는 장점이 있다. 동일한 접근 방식을 이용한 웹 보안시스템은 국제적으로는 EIT가 RSA Data Security와 NCSA등의 협조아래 Secure Mosaic/httpd를 개발하여 CommerceNet 콘소시엄내에 발표하였고 이의 상용버전을 EIT와 RSA Data Security의 합작 회사인 Terisa systems[24]이 제공하고 있다. 그럼에도 불구하고 보안 제품에 대한 미국 등의 수출 억제 정책으로 비도가 높은 보안 제품을 국내에서 사용하기가 곤란하다는 점과 미국 등의 수출 억제 정책이 폐지된다 하더라도 수입되는 제품에 보안 홀의 가능성 및 국내에서 개발하고 있는 전자 서명 표준 등의 암호모듈을 수용할 수 있는 하부구조를 제공하고자 하는데 그 의의가 있다.

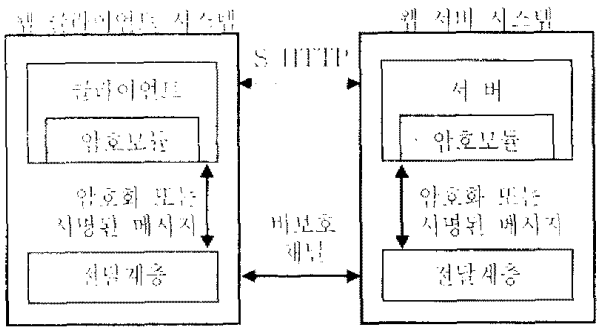
3. 웹 보안 프로토콜 S-HTTP

IETF WTS(Web Transaction Security) 작업반에서 표준화하고 있는 웹 보안 프로토콜인 S-HTTP의 동작 모델은 (그림 1)과 같다. S-HTTP는 HTTP와 함께 사용할 수 있도록 설계된 안전한 메시지 기반 통신 프로토콜이며, HTTP 응용에 쉽게 통합될 수 있는 이 프로토콜은 클라이언트와 서버 자체에 암호 모듈이 포함되어 있기에 트랜잭션 채널이 보호될 필요가 없다.

기본적으로 트랜잭션의 기밀성, 무결성, 인증, 부인봉쇄, 접근 제어 서비스를 제공하며, 이러한 보안 서비스를 제공하기 위해 요구되는 키 관리 메카니즘, 보안정책, 암호 알고리즘 등의 협상 기능이 다양하다. <표 2>는 보안 관련 협상 매개변수 및 가능한 값들을 보

〈표 1〉 웹 보안 접근방식 비교
〈Table 1〉 Some Comparisons of WWW Security Approach

방식 / 항목	채널 보안	메시지 보안	내용 보안
접근 방법	네트워크 연결을 보호	HTTP 메시지 단위로 보호	문서, 데이타 베이스등을 보호
HTTP와의 관계	HTTP를 단순한 응용으로 사용	HTTP를 Security를 인식하는 프로토콜과 구문으로 향상	HTTP는 단순한 전송수단으로 사용
보안서비스	기밀성, 무결성, 메시지 및 사용자 인증 서비스	기밀성, 무결성, 부인봉쇄, 메시지 및 사용자 인증 서비스	응용에 의존함
예	SSL, PCT(Privacy Communication Technology)	S-HTTP	PGP(Pretty Good Privacy), PEM(Privacy Enhanced Mail)



(그림 1) S-HTTP의 동작 모델
(Fig. 1) Working Model of S-HTTP

〈표 2〉 S-HTTP의 보안관련 협상 매개변수
〈Table 2〉 Security Negotiation Parameters of S-HTTP

대칭키 헤더 알고리즘	DES-ECB, DES-EDE-ECB, DES-EDE3-ECB, DESX-ECB, IDEA-ECB, RC2-ECB, CDMF-ECB
대칭키 내용 알고리즘	DES-CBC, DES-EDE-CBC, DES-EDE3-CBC, DESX-CBC, IDEA-CBC, RC2-CBC, CDMF-CBC
서명 알고리즘	RSA, NIST-DSS
키교환 알고리즘	RSA, Outband, Inband
메시지 다이제스트 알고리즘	RSA-MD2, RSA-MD5
Message Authentication Code 알고리즘	RSA-MD2, RSA-MD5, NIST-SHS, RSA-MD2-HMAC, RSA-MD5-HMAC, NIST-SHS-HMAC
인증서	X.509, X.509v3
프라이버시 도메인	MOSS, PKCS-7

앞서 언급한 바가 있는 S-HTTP가 제공하는 보안 서비스를 간단히 살펴보면 다음과 같다.

● 기밀성 서비스

메시지 암호화에 사용된 키를 공유하는 방식에 따라 두 가지 방식이 있다. 클라이언트와 서버가 서로 상대방의 공개 키를 알고 있는 경우 대칭 암호시스템에 사용된 비밀키를 PKCS-7의 EnvelopedData 타입에 의해 상대방의 공개키로 암호하여 전송 및 공유할 수 있다. 이 경우 클라이언트의 전자 서명을 포함시키고자 하는 경우에는 SignedAndEnvelopedData 타입을 이용하여 발신자 인증서비스 등도 함께 제공되기도 한다. 또한 패스나 전화 등과 같이 외부적인 방법에 의해 공유된 비밀키로 메시지 암호화에 사용된 세션 키를 공유한다. 이 경우에는 EncryptedData 타입이나 SignedData 타입으로 서명 후 암호화하여 제공된다.

● 발신자 인증 서비스

클라이언트의 디지털 서명을 위한 개인키는 특정 클라이언트만이 가질 수 있으므로 서버는 디지털 서명 값을 통해 발신자 인증을 할 수 있다. 또한 전송되는 메시지에 대한 디지털 서명 값을 구하므로 메시지 인증도 함께 제공하게 된다. 그러나, 이 서비스만 제공되면 재연 공격에 취약하기 때문에 암호화와 함께 사용하거나 S-HTTP의 Nonce 헤더를 함께 사용하는 것이 바람직하다. 그리고 MAC-Info 헤더의 해쉬 키 값으로 패스워드를 사용하므로써 기존의 메시지 다이제스트 인증과 동일한 인증서비스를 제공할 수 있다.

● 메시지 인증 및 무결성 서비스

디지털 서명을 이용하는 방법 외에도 S-HTTP헤더 중의 하나인 MAC-Info 헤더를 이용하여 메시지 인증과 함께 무결성 서비스가 제공된다.이 방식은 옵션 헤더와 내용 영역에 대한 해쉬값을 계산해서 S-HTTP의 헤더를 통해 전송한다. 이때 옵션 헤더와 내용 영역 값 외에도 이전에 교환된 키 값과 시간정보 등을 포함해서 함께 해쉬 값을 계산하므로 재연 공격이 방지된다.

● 부인봉쇄 서비스

디지털 서명에 의해 제공되며 특정 개인키를 가지고 있는 클라이언트는 하나뿐이라는 것에 기초를 두고 있다. 또한 이 서비스만으로는 재연 공격에 취약하므로 다른 보안 서비스들과 함께 사용되는 것이 바람직하다.

● 접근제어 서비스

발신자 인증을 이용하여 인가된 클라이언트들에게만 접근을 허용하는 서비스를 할 수 있다. 그러나, 이 서비스는 S-HTTP 자체보다는 서버의 특성에 의존된다.

● 재연방지 서비스

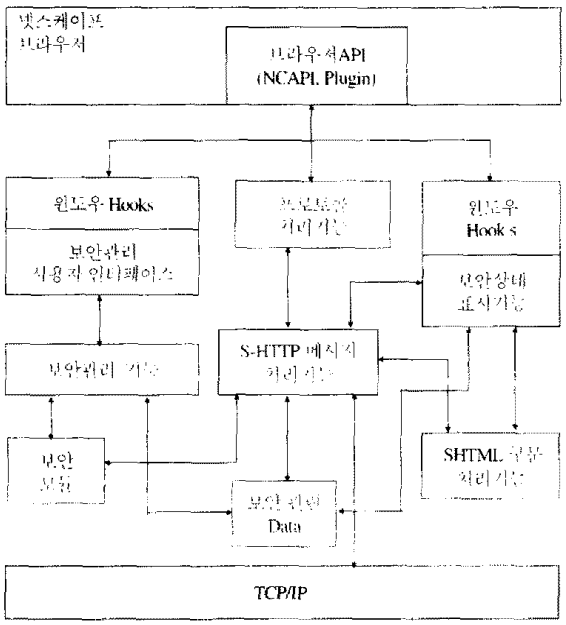
두 통신 대상간에 전송의 일회성을 보장하기 위한 Challenge-response 메카니즘이 S-HTTP 헤더 또는 HTML의 앵커속성으로 NONCE와 NONCE-Echo에

의해 제공된다.

위와 같은 보안서비스를 제공하는 S-HTTP의 사용자 또는 관리자 입장에서의 특징으로는 먼저 URL로 shttp를 사용한다는 것이다. 즉 "http://security.etri.re.kr" 대신 "shttp://security.etri.re.kr"을 사용하게 된다. 또한 HTTP에 "Secure" 메소드를 추가하므로써 S-HTTP 메시지를 HTTP 메시지와 구분하여 특별한 처리를 하도록 하였다. 그리고 HTTP 헤더로 암호관련 협상매개변수[3] 들을 추가 하였다. 또한 S-HTTP와 함께 사용될 HTML은 새로운 앵커 속성으로 서버를 유일하게 식별할 수 있도록 하는DN(Distinguished Name), 재연공격을 막기위한 NONCE, 암호학적 선택사항을 기술하기 위해 CRYPTOPTS이 추가 되었다. 또한 인증서를 표현하기 위해 CERTS 요소 및 앵커에서 이름에 참조될 수 있도록 CRYPTOPTS 요소가 추가되었다.

4. SecWeb 시스템 모델

4.1 S/W 구조



(그림 2) 클라이언트 시스템 S/W 구조
(Fig. 2) S/W Architecture of Client System

클라이언트 시스템의 S/W 구조는 (그림 2)와 같다. 넷스케이프 브라우저에서 shttp URL에 대한 클릭은 프로토콜 처리기능에 의해 shttp URL을 인식하며, 해당 URL이 사용자에 의한 첫번째 클릭인지에 따라 선택적으로 SHTML구문처리기능에서 처리한 데이타를 이용하여 S-HTTP 처리기능에서는 해당 URL에 대한 적절한 S-HTTP request 메시지를 생성하여 서버로 송신한다. 보안모듈을 이용하여 S-HTTP request를 생성하며 이 과정에서 사용자가 선택한 보안관련 협상정보 들을 보안관련 데이타로부터 검색하여 이용하거나 변경시 저장하게 된다. 서버로부터 수신된 S-HTTP response는 S-HTTP메시지 처리기능에서 보안모듈 및 보안관련 데이타를 이용하여 S-HTTP response를 해석하여 프로토콜 처리기능 통해 브라우저에 디스플레이 한다. S-HTTP메시지 처리기능에서 S-HTTP response에 대한 복호 및 검증 등 암호학적인 동작을 수행하는 과정의 상태에 대한 표시를 보안상태 표시기능을 이용하여 수행하게 된다.

서버 시스템은 사용자 및 브라우저 인터페이스 그리고 SHTML 구문처리기능을 제외한 나머지 기능 외에 시스템 관리기능으로 구성되어 있다. (그림 2)의 S/W 구조에 대해 간략히 설명하면 다음과 같다.

(1) 보안관리 사용자 인터페이스

오프라인으로 클라이언트가 전자 서명에 사용하게 될 공개키/개인키(Private Key)의 생성/삭제/선택등의 관리와 공유키의 관리, 패스워드의 생성 및 변경, 문서 소유자의 공개키에 대한 인증서를 검증할 수 있도록 인증서를 관리한다. 이외에도 보안과 관련한 협상 매개변수[3]를 보안에 관해 지식이 많지 않은 사용자가 기본값으로 선택할 수 있도록 하였다. 또한 통신 중에는 이와 같이 요구되는 사항에 대해서는 지시에 따라 수행하면 된다.

(2) 보안 상태 표시 기능

보안 상태 표시기능에는 클라이언트가 URL을 풀기(dereference)전 즉 문서를 검색하기 전에 클라이언트에게 요구되는 처리 - 암호, 서명, 인증 및 이들의 조합 에 대한 요구사항을 미리 볼 수 있는 문서처리 요구 표시기능과 서버로 부터 문서를 검색하는 과정의 진행 상태를 표시하는 문서처리 상태 표시기능이 있다. 또한 서버로 부터 검색된 문서가 암호화, 서명, 암호화와 서명, 평문인지를 사용자에게 알려주는 문서상태 표시를 제공한다.

(3) 프로토콜 처리기능

HTTP URL이 아닌 S-HTTP URL을 인식 할 수 있도록 하는 프로토콜 식별자 인식기능을 제공한다.

(4) S-HTTP 메시지 처리 기능

S-HTTP 헤더에 대한 처리기능, 확장된 HTTP 메시지 처리 기능과 S-HTTP 내용에 대한 처리기능으로 구성되어 있다. S-HTTP 헤더에 대한 처리기능에서는 S-HTTP 헤더의 생성 및 인식을 통해 S-HTTP내용에 대한 적절한 처리를 수행할 수 있도록 한다. Content-Privacy-Domain, rearranged-Key-Info, Content-Type, Mac-Info헤더가 이에 해당한다. 확장된 HTTP 메시지 처리 기능에서는 클라이언트/서버간에 송수신하는 실제 내용에 대한 보안수준 협상을 위해 확장 헤더를 적절히 이용하여 확장된 HTTP 메시지를 생성한다. HTTP 헤더외에 보안 서비스를 제공하기 위해 추가된 헤더[3, 6]들을 확장 헤더라 한다. S-HTTP 내용에 대한 처리기능으로는 'Content-Privacy-Domain' 또는 'Prearranged-Key-Info'값을 적절히 이용하여 내용에 대한 부호화/복호화를 수행한다.

(5) SHTML 구문 처리 기능

보안을 위해 확장된 HTML구문[5]에 대한 인식 및 각각에 대한 적절한 처리를 수행한다. 확장된 HTML 구문으로는 서버를 유일하게 식별할 수 있도록 하는DN (Distinguished Name), 재연공격을 막기위한 NONCE, 암호학적 선택사항을 기술하기 위해 CRYPTOPTS이 추가 되었다. 또한 인증서를 표현하기 위해 CERTS 요소 및 앵커에서 이름에 참조될 수 있도록 CRYPTOPTS 요소가 있다.

(6) 보안 관리기능 및 보안 모듈

보안모듈을 이용하여 인증 기능, 서명 기능, 대칭키 암호 기능, 대칭키(비밀 키) 관리 기능, 공개키 및 인증서 관리 기능 보안관리기능을 제공한다. 좀더 자세한 내용은 참고문헌 2에서 기술되고 있다.

4.2 클래스 다이어그램

(그림 3)은 OMT(Object Modeling Technique) II 또는 UML(Unified Modeling Language)을 이용하여 SecWeb시스템 설계과정에 추출된 클래스 및 이들의

(그림 3) SecWeb 시스템의 Class Diagram-클라이언트
(Fig. 3) Class Diagram of SecWeb-Client

관계를 보여주는 클래스 다이어그램으로 각 클래스는 4.1에서의 기능들을 구성하는 요소이며, 각 클래스의 속성은 다이어그램에서 생략하였다. 그리고 이렇게 추출된 클래스 사이의 순열 다이어그램(Sequence diagram) 작성에 의해 설계가 이루어 졌다.

(그림 3)에서 보는 바와 같이 SHTTP request와 SHTTP response클래스는 SHTTP message클래스로부터 상속을 받아 S-HTTP 메시지를 구성 및 해석기능을 수행한다. 이 SHTTP message클래스는 SHTML 구문처리기능을 수행하는 SHTML CryptData와 SHTML Processor 클래스로 부터의 shttp URL에 대한 속성을 상속받고 있다. 보안관리 사용자 인터페이스 기능을 수행하는 SecuritySelectionWindow 클래스는 Authorization UI, CryptOption UI, KeyDB UI, Certificate Data UI클래스들의 집합으로 구성된다.

5. SecWeb 개발 환경

SecWeb 클라이언트 개발을 위한 주요기술로는 shttp URL 확장을 위해서는 NCAPI(Netscape Client API)[6]를, 이와 관련한 MIME 타입 확장 및 클라이언트 프로그램 구동을 위해서는 Plug in기술 그리고 보안관리를 위한 사용자 인터페이스 등을 위해서는 윈도우의 Hooks를 이용하였다. 주요 구현기술에 대하여 간략히 기술하면 다음과 같다.

(1) 프로토콜 확장

Netscape의 클라이언트 확장기술로 최근 주로 사용하고 있는 Plug-in 기술은 프로토콜확장 기능을 제공하고 있지 않으므로, Plug-in기술이 출현되기 전에 사용되던 NCAPI를 이용하고 있다. NCAPI는 Spyglass, Inc,에서 웹 브라우저의 기능을 확장할 사용될 수 있는 플랫폼에 독립적인 API를 정의하고 있는 Software Development Interface(SDI)[14]에 근거하고 있으며 마이크로소프트의 인터넷 익스플로러(MSIE) 또한 이를 지원[13]하고 있다.

NCAPI로는 DDE(Dynamic Data Exchange)[17]와 OLE(Object Linking & Embedding)[18] 인터페이스를 제공하고 있다. 이중 OLE인터페이스에 의해서는 서버로 부터 수신한 데이터를 넷스케이프 브라우저에 디스플레이하는 기능이 제공되지 않으므로 DDE인터페이스를 이용하여 shttp URL을 확장 하였다. DDE 인터페이스, 정확하게는 DDEML(DDE Management Library)[12]을 이용하여 shttp URL을 처리하는 프로토콜 처리기능을 개발하였다.

(2) MIME 타입 확장 및 클라이언트 프로그램의 실행

일반적으로 특정 MIME타입 확장에 의한 해당 컨텐트 뷰어를 구동시키는 기술로 Plug-in[15, 16]에 의해 많은 소프트웨어들이 개발되고 있다. 여기서는 컨텐트 뷰어가 아닌 프로토콜 처리기를 실행시키므로써 S-HTTP 프로토콜 처리기를 실행시키도록 하였다. 확장된MIME정보는 "application/x-shtml"으로 확장자는 "shtml"을 사용하도록 하였다. 다음은 플러그인 페이지를 HTML페이지에 포함시킨 HTML을 보여주고 있다.

```
<HTML>
...
<EMBED Type="application/x-shtml"PLUGINSPA-
  GE-"shtml.html"width-2 height=2>
```

(3) 사용자 인터페이스

넷스케이프에서의 보안관련 사용자 인터페이스를 위해서 윈도우가 제공하는 Hooks를 이용하였다. 즉, 넷스케이프 윈도우 및 메뉴의 핸들을 잡아서 메뉴 및 메뉴 아이템을 추가하였고 Hook기능을 설치하여 보안과 관련된 메뉴 아이템들이 선택되도록 하였다. 이는 윈도우에서 제공하는 기초적인 방법을 이용한 것으로 이런 방법 외에도 사용자의 필요에 따라 브라우저를 짜맞출 수 있는 도구를 넷스케이프 3.0이상에서는 Administration Kit[19,20]을 유료로, 그리고 MSIE의 IEAK (Internet Explorer Administration Kit)[23]는 등록을 하면 무료로 제공하고 있으므로 이를 활용하여 개발할 수도 있을 것이다.

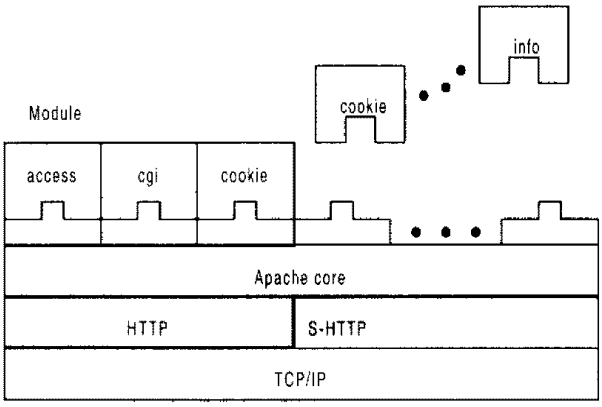
(4) 보안기능

클라이언트와 서버 공통적으로 사용하고 있는 보안 모듈은 독일 GMD에서 개발중인 SECUDE-5.1 preview release III[22]를 이용하고 있으며 이 툴킷은 다음과 같은 기능을 제공하는 보안 함수 라이브러리와 보안 API 등을 제공한다. RSA, DES, DSA, MD5, SHA 와 같은 암호 및 해쉬 함수, 인증서 관리 기능, CA(Certification Authority) 기능과 인증서 교환 기능, PEM 처리 기능, GSS(Generic Security Services) API 제공, PKCS(Public Key Cryptography Standards) 인코딩/디코딩 기능, ASN.1 인코딩/디코딩 함수, 기밀성 및 무결성 서비스에 의한 사용자 정보의 저장 기능 등

을 제공하고 있다.

(5) 서버

SecWeb 서버는 Apache 서버 1.2 Release에 S-HTTP 프로토콜 버전 및 보안 기능을 추가하였다. Apache 인터페이스에서는S HTTP 프로토콜 버전을 Apache 서버에 확장을 위한 인터페이스 외에도 Request 메시지의 암호상태 및 클라이언트에 의해 사용된 서명자 등을 수용할 수 있도록 CGI 환경변수를 확장 한다. 그리고 키 및 인증서 데이타에 대한 접근제어등을 수행하는 서버관리기능을 수행한다. 확장된 HTTP 메시지 처리 기능은 클라이언트 시스템의 경우 S-HTTP 메시지 처리기능에 포함되어 있던 기능이 서버의 경우 Apache와의 인터페이스를 위해 분리되었으며 기능상으로는 동일하다.



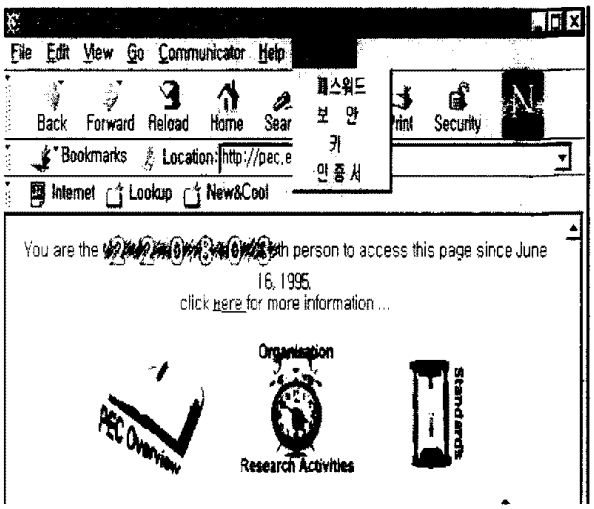
(그림 3-4) Apache서버에서 프로토콜 확장

6. 구현 및 적용

6.1 구현

(1) 사용자 환경설정 기능

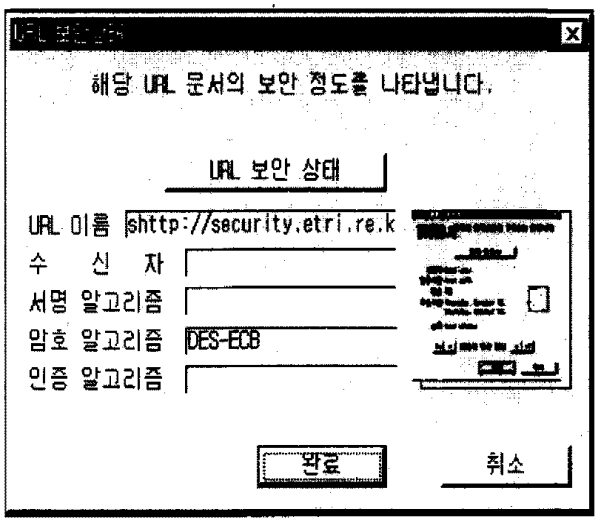
안전한 웹 시스템으로부터 문서를 검색하기 전 또는 문서를 검색하는 과정에서 암호, 전자 서명, 인증등과 관련한 알고리즘등을 사용자가 선택할 수 있다(그림 4). 문서를 검색하기 전에는 넷스케이프 메뉴의 "보안관리" 메뉴의 패스워드/보안/키/인증서 메뉴 아이템에서 사용자가 원하는 옵션을 선택, 관리할 수 있다. 패스워드는 보안과 관련된 데이터를 안전하게 저장, 관리하기 위해 사용되며, 보안에서는 암호, 전자서명, 인증 트랜잭션에서 사용될 암호, 서명, 해쉬 등의 알고리즘을 선택할 수 있다. 키에서는 암호, 전자서명 트랜잭션에 사용될 비밀키 및 공개키의 생성 및 관리를 수행한다. 그리고 인증서에서는 사용자 본인은 물론 웹 서버 및 인증기관의 인증서를 관리하므로써 공개 키에 의한 전자서명 트랜잭션을 가능케 한다.



(그림 4) 보안관리 화면
(Fig. 4) Security Management Scene

(2) Link Security Status 보기 기능

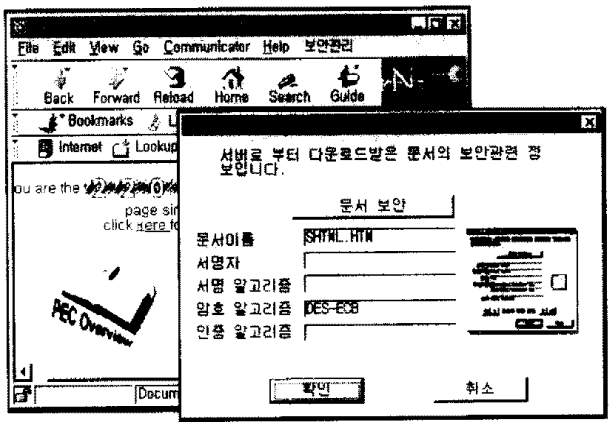
사용자는 shttp URL을 클릭하므로써 shttp 프로토콜에 의해 안전하게 문서를 수신함은 물론, 클릭을 하지 않은 상태에서 수신하게 될 문서의 보안상태 즉 이 문서를 수신하기 위해 클라이언트에 요구되는 보안사항을 CTRL과 함께 클릭을 하므로써 (그림 5)와 같이 미리 알 수 있다.



(그림 5) URL 보안상태 화면
(Fig. 5) URL Security Status Scene

(3) 문서 검색기능

서버로 부터 shttp 프로토콜에 의한 문서를 수신 중에 사용자는 넷스케이프 로고 옆의 보안처리 로고, (그림 6)에서 보는 바와 같이 문서가 복호 또는 서명 검증 등이 수행되고 있음을 알 수 있으며, 문서가 완료된 뒤에는 수신된 문서가 어떤 종류의 보안에 의해 안전하게 수신되었는지를 보여 준다. 또한 이 로고를 클릭하면 (그림 6)의 우측 화면과 같이 수신한 문서의 보안 정보를 좀더 상세히 알 수 있다.



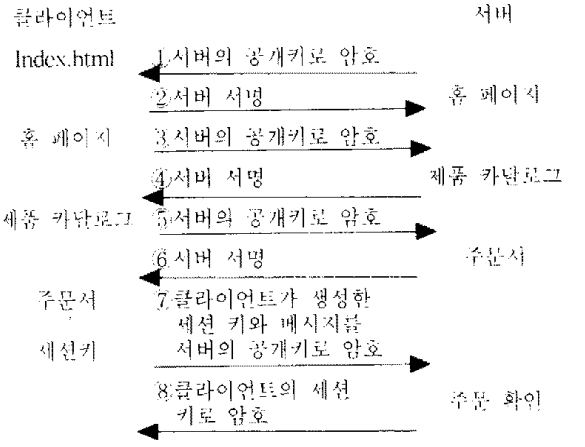
(그림 6) 문서검색 및 보안상태 화면
(Fig. 6) Document Retrieval & security Status Scene

6.2 시나리오

SecWeb을 이용한 기본적인 트랜잭션으로는 클라이언트의 전자 서명 없이 암호화, 클라이언트의 전자 서명과 함께 암호화, 전자 서명에 기초한 인증, 패스워드에 기초한 인증, 트랜잭션과 무관한 방법에 의한 키 교환, 트랜잭션중의 키 교환 등으로 또한 이들을 적절히 조합하여 안전한 웹 시스템 응용을 개발할 수 있다. 다음에서는 홈 쇼핑 시나리오에 적용한 시나리오를 좀더 구체적으로 들었다. 첫번째는 일반적인 상품 구매 시나리오로 모든 사람을 대상으로 하는 경우이며, 두 번째는 회원에 대한 우대행사로 가격 인하 등을 제공하기 위해 회원 인증을 전자 서명에 의해 수행하는 경우에 대한 시나리오를 보여주고 있다.

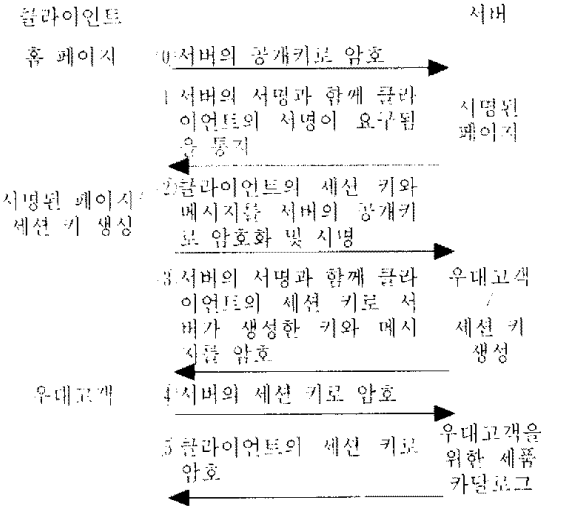
(1) 상품 구매 시나리오

이 시나리오는 서버가 신뢰할 수 있는 서버임과 주문서 등의 페이지가 수정되지 않았음을 알려주는 무결성 서비스를 제공하고자 하는 경우에 적용할 수 있다. 클라이언트는 공개키/개인키 쌍이 없는 경우 서버의 공개키로 암호화를 수행한다. 이 경우 클라이언트는 서버의 공개 키를 미리 보유하고 있거나 없는 경우는 서버로 부터 공개 키를 다운로드 받을 수 있다. 서버는 클라이언트에게 홈페이지, 제품 카달로그 또는 주문서 등이 변경되지 않았음을 서버의 개인 키에 의해 서명을 하므로써 제공할 수 있다. 다음은 이와 같은 트랜잭션을 Request/Response별로 간략한 해석과 함께 설명하고 있다.



(2) 우대 고객을 위한 구매 시나리오

우대고객의 경우 일반 고객과는 달리 부가적인 서비스, 즉 가격 할인 등을 제공하고자 하는 경우에 우대고객 임을 확인하는 인증과정이 요구되는데 이를 클라이언트의 서명을 통하여 가능함을 보여주고 있다. 이때 클라이언트와 서버 모두 상대방의 서명을 검증할 수 있다. 인증 후에는 클라이언트와 서버는 각각 사용하게 될 세션 키를 공유하여 이를 이용하여 데이터의 기밀성을 또한 제공한다.



7. 결론 및 향후계획

웹 보안프로토콜인 S-HTTP를 기반으로 하고 있는 안전한 웹 시스템인 SecWeb은 국내에서 처음으로 개발되었으며 차별되는 대표적인 적용분야는 전자 서명이 요구되는 응용으로 본 논문에서는 시스템 모델, 관련 주요 구현기술 및 개발된 시스템에 대하여 기술하였다. '97년 10월 현재 시험 중으로 완료 후 신용카드 기반의 전자지불 형태로 비디오와 CD를 취급하는 홈쇼핑몰 "장터로 가는 길[R]"에 적용할 계획이다.

지금까지는 웹 보안에 대한 인식 부족으로 거의 넷스케이프에서 브라우저와 함께 제공되는 SSL기반의 보안시스템이 대부분 이용되어 왔기에 SSL기반의 웹 시스템과 보안측면에서 간단히 비교[5]하면 다음과 같다.

S-HTTP는 메시지의 서명에 의해 부인봉쇄 서비스를 제공하므로 영수증 등으로 활용할 수 있다. 반면에 SSL은 부인봉쇄 서비스를 제공하지 않는다.

- S-HTTP는 보안관련 매개변수 놀을 다양한 범위로 디스플레이 및 제어가 가능하다. 근본적으로 사용자가 보안 옵션을 명시적으로 처리할 수 있다.
- 암호동작이 좀더 간단하며 메시지에 대한 서명기능을 제공하지 않기 때문에 성능면에서 SSL이 약간 나은 것으로 알려지고 있다.
- SSL은 웹이나 HTTP에 한정되지 않고 다른 네트워크 응용을 매우 쉽게 지원할 수 있다.
- SSL이 좀더 간단한 메카니즘으로 브라우저 사용자와 서버 관리자에 의해 좀더 쉽게 사용될 수 있다. 즉 S-HTTP의 앵커 속성 등을 정확히 기술하는 것은 SSL처럼 단순히 "http"를 "https"로 변경하는 것보다는 어려울 수 있다.

위와 같은 비교로도 단순히 어떤 방법에 기초한 웹 시스템이 좋다고 단정짓기는 어렵기에 기밀성 서비스가 강조될 때는 SSL을, 부인봉쇄 서비스가 요구될 때는 S-HTTP를, 문서에 대한 보안서비스가 사전에 적용될 때는 S-HTTP, 그리고 상호 운용성을 극대화 시키고자 할 때는 SSL을 권장하고 있으므로 정보 제공자 또는 웹 응용 서비스 제공자가 적절히 선택하여 사용하는 것이 바람직하다.

참 고 문 헌

[1] 박정수외 1인, "윈도와이드 웹보안기술 및 동향", 정보과학회 학회지, 제15권, 제4호, pp.37-44, 1997년 4월호.

[2] 조은경외 2인, "안전한 World Wide Web 시스템 개발", 1996년도 추계종합학술대회 논문집(A), 제19권, 제2호, pp.78-81, 대한전자공학회, 1996년11.

[3] 박정수외 3인, "인터넷 웹 보안 프로토콜 기능분석", 정보보호학회 학회지, 제8권, 제4호, 1996년 12월호.

[4] 박정수외 2인, "S-HTTP 기반 안전한 World Wide Web시스템 설계", JCCI' 97, pp.1407-1410, 1997.

[5] Adam Cain, "Web Security," NCSA, 5th International WWW Conference Tutorial Notes, pp.1-31, 1996.

[6] E.Rescorla, etc."The Secure HyperText Transfer Protocol," Internet-Draft <draft-ietf-wts-S-HTTP-04.txt>, 1997. 3.

[7] William T. Wong, "Secure NCSA Mosaic Reference Manual," EIT, 1995. 2.

[8] iam T. Wong, "Secure NCSA httpd Reference Manual," EIT, 1995. 2.

[9] E.Rescorla, etc. "Security Extension for HTML," Internet-Draft <draft-ietf-wts-shtml-03.txt>, 1997. 3.

[10] http://www.eit.com/creations/s-http, EIT, "Secure HTTP".

[11] http://hoohoo.ncsa.uiuc.edu/beta-1.6, NCSA, "NCSA HTTPd 1.6 Beta 1," 1996. 8.

[12] Jeffery D. Clark, Windows Programmer's Guide To OLE/DDE, SAMS, 1992.

[13] http://www.microsoft.com/ie/press/techinfo-f.htm?/ie/press/win31/30win31wp.htm, Microsoft Internet Explorer 3.0 for Windows 3.1 Technical White Paper.

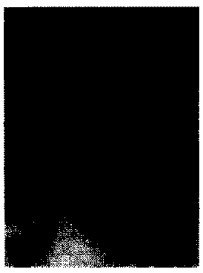
[14] http://www.spyglass.com/products/smosaic/sdi/sdi_spec.html, Software Development Interface, Spyglass, Inc., 1996. 8.

[15] http://developer.netscape.com/library/documentation/communicator/plugin/index.htm, Plug-in Guide 4.0, 1997. 6.

[16] http://home.netscape.com/eng/mozilla/3.0/handbook/plugins/index.html, The Plug-in Developer's Guide, 1996.

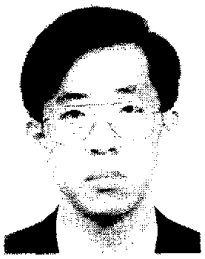
[17] http://developer.netscape.com/library/documentation/

communicator/DDE/index.htm, Netscape's DDE Implementation, 1997. 10.
[18] http://developer.netscape.com/library/documentation/communicator/OLE/index.htm, OLE Automation in Navagitor, 1997. 5.
[19] http://search.netscape.com/comprod/products/navigator/version_3.0/management/admin/index.html, Netscape Administration Kit,
[20] http://search.netscape.com/eng/mozilla/4.0/relnotes/pro-4.0b4.html, NETSCAPE COMMUNICATOR PROFESSIONAL EDITION Preview Release 4, 1997. 8.
[21] MicroSoft, Visual C++ Books Online 4.0
[22] http://www.darmstadt.gmd.de/secude/, SECUDE-5.1 preview release III, 1997. 10.
[23] http://www.microsoft.com/ie/ieak, Internet Explorer Administration Kit, 1997. 10.
[24] http://www.terisa.com/products, About our Products, 1997. 11.



조 은 경

e-mail : ekcho@mail.ddc.ac.kr
1984년 충남대학교 계산통계학과 졸업(학사)
1988년 충남대학교 대학원 전산학과 졸업(석사)
1998년 충남대학교 대학원 전산학과 박사과정 수료
1985년~1998년 한국전자통신연구원 멀티미디어표준연구실 선임연구원
1998년~현재 대덕대학 전산교육팀 조교수
관심분야 : 통신망 보안, 보안 응용 등



박 정 수

e-mail : jspark@etri.re.kr
1992년 경북대학교 전자공학과(학사)
1994년 경북대학교 전자공학과(석사)
1994년~현재 한국전자통신연구원 표준연구센터 연동표준연구팀 연구원
관심분야 : 인터넷 보안, 멀티미디어 보안

강 신 각

e-mail : sgkang@etri.re.kr
1984년 충남대학교 전자공학과(학사)
1987년 충남대학교 전자공학과(석사)
1984년~현재 한국전자통신연구원 표준연구센터 표준기획연구팀 책임연구원
관심분야 : 통신망 보안, 멀티미디어 통신

박 성 열

e-mail : sypark@etri.re.kr
1977년 연세대학교 전자계산학과(석사)
1982년 Univ. of Florida 산업공학과(석사)
1987년 Auburn Univ. 산업공학과(박사)
1973년~1978년 한국과학기술원 연구원
1987년~현재 한국전자통신연구원 슈퍼컴퓨터센터 센터장
관심분야 : 분산처리, 정보보호, 인터넷 응용