SSL과 PGP를 이용한 웹 기반 메일 시스템의 설계 및 구현

신승혁°, 이기수, 장춘서
금오공과대학교 컴퓨터공학과

Design and Implemetation of the Web-based Mail System Using SSL and PGP

Seung-hyeok Shin, Ky-Soo Lee, Choon-seo Jang
Dept. of Computer Engineering, Kumoh National University of Technology

요 약

클라이언트용 메일 프로그램에 비해 웹 메일 시스템은 일반 사용자에게 인터페이스와 기능적인 면에서 편리함을 제공한다. 그러나 메일 메시지를 전송하고 관리하는 측면에서는 보안상의 취약점을 가지고 있다. 본 논문에서는 메일 메시지를 안전하게 전송하고 편리하게 관리하기 위한 웹 기반의 메일 시스템을 구현하였다. 이 시스템에서는 일반적인 메일 기능과 PGP(Pretty Good Privacy)를 이용한 메시지 암호화 기능, SSL(Secure Socket Layer) protocol을 이용하여 웹 메일 시스템과 웹 브라우저 사이의 메시지 보호 기능 등을 이용하여 클라이언트용 메일 프로그램을 이용하기 위한 설정이 필요 없이 웹 브라우저만을 가지고 안전한 메시지 전송과 관리를 할 수 있도록 하였다.

1. 서 론

클라이언트용 메일 프로그램은 메일을 전송 할 수 있는 SMTP(Simple Mail Transfer Protocol)서버와 메일을 관리 할 수 있는 POP3(Post Office Protocol)서버 또는 IMAP(Internet Message Access Protocol)서버의 설정 등 전자 메일을 이용하기 위한 기본적인 환경 설정이 필요하다. 또한 인터넷 메시지를 안전하게 전송하기 위해 인터넷상에 공신력 있는 유료 CA(Certificate Authority)에 접속하여 공개키와 비밀키를 그리고 CA에 대한 인증서를 생성, 유지, 관리하여야 하는 문제 등이 일반 사용자에게는 어려운 문제로 남는다[3,4,7,8].

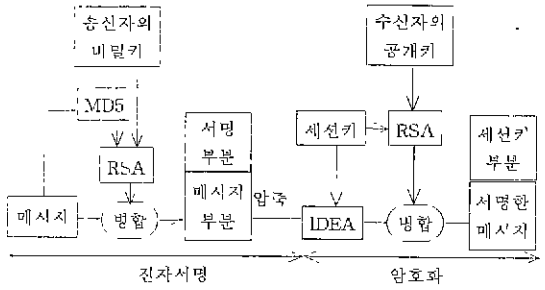
웹 기반의 메일 시스템을 이용하게 되면 메일 관련 서버의 설정 없이 사용자의 웹 브라우저만을 이용하여 메일 메시지를 쉽게 전송하고 관리 할 수 있다. 하지만 메시지의 전송 과정에서 메시지의 탈취, 변조, 위조 등 보안상의 취약점이 존재하기 때문에 메시지에 대한 암호화가 필요하게 된다[4].

본 논문에서는 인터넷 메시지를 안전하게 전송하고 편리하게 관리하기 위한 웹 기반의 메일 시스템을 구현하였다. 이를 위해 웹 기반의 메일 시스템은 PGP를 이용하여 서버에서 메일 메시지를 안전하게 암호화하여 전송하고, SSL protocol을 이용하여 웹 브라우저와 웹 기반 메일 시스템 사이의 메시지를 보호하고 인터넷상에서 자신의 메일을 안전하게 관리 할 수 있는 쉬운 사용자 인터페이스를 제공한다.

2. 기존의 연구

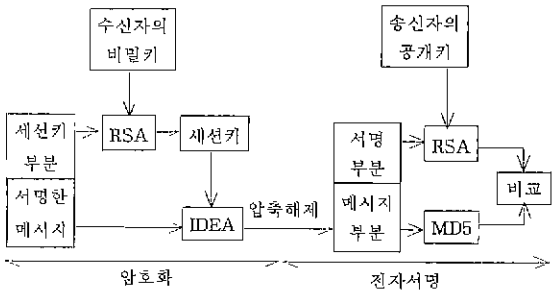
2.1 PGP (Pretty Good Privacy)

PGP는 전자 메일의 보호뿐만 아니라 일반 파일에 대한 암호화도 가능하여 개인 정보에 대한 보안을 강화한다. PGP에서 사용하는 IDEA(International Data Encryption Algorithm)는 DES(Data Encryption Standard)를 대체 하기 위한 블록 지향의 대칭키 암호 알고리즘으로 64 bit의 블록 데이터를 암호화하기 위하여 128 bit의 키를 사용하며 암호화 속도가 빠르기 때문에 메시지 자체의 암호화에 사용된다. 한편, RSA (Rivest-Shamir-Adleman)는 암호화 속도가 상대적으로 느리기 때문에 IDEA에서 쓰인 대칭키를 암호화하기 위해 쓰이는 공개키 알고리즘으로 수학적으로 계산하기 어려운 소수를 이용한 알고리즘이다. 메시지 인증을 위한 MD5(Message Digest)는 임의의 길이를 입력받아 일정한 길이로 출력하는 Hash 함수이다. 즉, 입력된 메시지를 512 bit 블록으로 나누어서 Hash함수에 입력하여 128 bit의 고정된 결과 값을 출력한다. MD5는 같은 결과 값을 갖는 입력 값을 찾는 것이 불가능하기 때문에 메시지 전송 중 변조 및 위조 여부를 판단하는 전자 서명에 사용되는 알고리즘이다[1,2].



[그림 1] 메시지 암호화

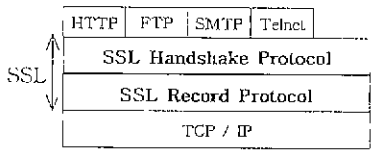
[그림 1]은 PGP에서의 메시지를 안전하게 전송하기 위한 암호화와 무결성을 증명하기 위한 전자서명 과정을 보여준다 PGP는 메시지를 MD5를 이용하여 사용하여 128 bit로 바꾼 다음 자신의 비밀키로 암호화(RSA)해서 원래의 메시지를 붙인다. 그런 후에 선택적으로 압축을 한 후 세션키를 생성하여 압축된 메시지를 암호화(IDEA)하고 세션키는 수신자의 공개키로 암호화(RSA)하여 전송을 하게 된다[1].



[그림 2] 메시지 복호화

[그림 2]는 PGP로 암호화와 전자 서명된 메시지를 복호화하는 과정을 보여준다. 인터넷을 통해 수신된 암호화된 메시지는 수신자의 비밀키로 메시지 암호화에 사용한 세션키를 복호화(RSA)를 한 후 세션키를 이용하여 메시지를 복호화(IDEA) 한 후 원래의 메시지와 서명부분으로 분리한다 그리고 메시지 전송 중의 무결성을 확인하기 위하여 메시지 부분을 MD5를 이용하여 128 bit의 결과값을 가지고 서명 부분의 메시기를 송신자의 공개키로 복호화 한 후 두 값을 비교하여 메시지를 확인한다[1].

2.2 SSL (Secure Socket Layer)



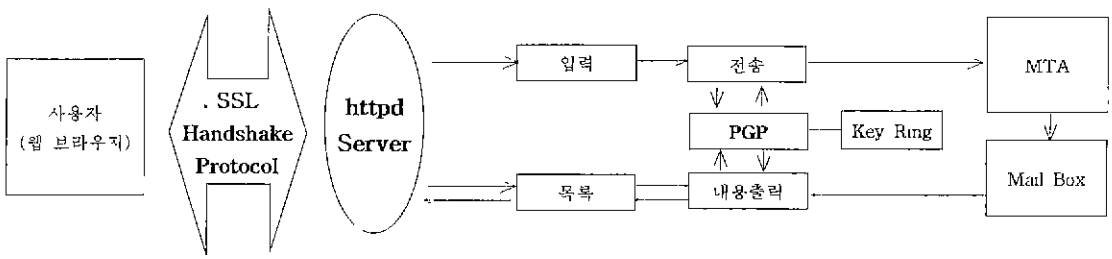
[그림 3] SSL protocol

SSL은 클라이언트와 서버 두 통신 응용 프로그램간에 정보보호를 지원하고, 서로를 인증하는 Layer 기반의 암호화 protocol이다. [그림 3]은 응용 protocol과 TCP/IP protocol 사이에 독립적으로 존재하는 SSL Layer를 나타낸다 SSL protocol은 Record protocol과 Handshake protocol로 구성되어 있으며, Record protocol은 Handshake protocol을 포함한 다양한 상위 레벨의 protocol을 캡슐화 하는데 사용된다. Handshake protocol은 세션에서 사용할 암호화 알고리즘과 세션키를 협상한다 이 결과로 양쪽은 암호화 통신에 합의하고, 암호화 통신과 인증에 필요한 값들을 준비한다. 이 단계가 지나면 SSL은 응용 protocol에서 생성해 낸 바이트 열의 암호화와 복호화만 수행하게 된다. 이는 HTTP request와 HTTP response에 포함되는 모든 정보들이 암호화된다는 것을 의미한다[5,6].

3. 시스템 구성

[그림 4]는 본 논문에서 구현한 웹 기반의 메일 시스템의 전체 구성도이다. 클라이언트의 요청을 처리해 주는 httpd 서버, 웹 브라우저와 웹 메일 시스템 사이의 안전한 메시지 전송과 상호 인증을 위한 SSL protocol, 메일을 전송하고 관리할 수 있는 메일 처리 모듈들, 전송할 메시지 보안을 위한 PGP 모듈, 전자 메일을 전송할 MTA(Message Transfer Agent)로 구성하였다

시스템 구현 환경은 Solaris 2.5.1에서 httpd서버로는



[그림 4] 시스템 전체 구성도

apache 1.3.6을 사용하였다. 암호화 통신을 위한 SSL Library는 openssl 0.9.2b를 사용하였고, PGP 2.3.6 international을 사용하였다. 웹 브라우저는 Netscape 4.5를 사용하였고, MTA는 Unix의 Sendmail을 사용하였다. CGI를 구현하기 위해 Unix C와 Perl 5.0을 사용하였다

3.1 httpd 서버

본 논문에서 사용한 httpd 서버는 SSL Library로 patch된 apache-ssl 서버로서 일반 http (port 80)가 아닌 https (port 443)로 접속을 해야한다. 접속하는 과정에서 Handshake protocol을 사용하여 웹 메일 시스템과 웹 브라우저를 인증하고, 세션에서 사용할 암호화 알고리즘과 세션키를 협상한다.

3.2 Mail 처리 모듈

메일을 처리하는 CGI 부분은 입력, 전송, 목록, 내용 출력의 4개의 모듈로 구성되어 있다. 메시지를 작성하고, 암호화 및 전자서명을 할 수 있는 부분과 상대방에게 메일 메시지를 보내는 부분, 메시지를 확인하고 관리하는 모듈로 구성된다.

특히, 전송 모듈과 내용 출력 모듈은 메시지의 암호화와 복호화의 처리를 하는 PGP 모듈과 직접적으로 통신하기 때문에 사용자는 단지 입력 모듈과 목록 모듈을 이용하여 간단하게 메시지의 암호화와 복호화 그리고 전자 서명 등을 할 수 있다.

입력 모듈은 웹 브라우저에서 메일 폼을 이용하여 직접 메시지를 작성하고, 선택적으로 파일로 된 메시지를 첨부하여 전송 모듈로 전송할 수 있다. 더구나 입력 모듈에서는 직접 작성한 메시지 부분과 파일 메시지 부분을 각각 PGP를 이용하여 메시지 암호화와 전자 서명 등을 각각 독립적으로 할 수 있다. 그런 후에 보내고자하는 메시지를 수신자의 주소와 함께 제목, 본문 등으로 구성하여 전송 모듈로 넘겨준다.

전송 모듈은 입력 모듈에서 보내온 메시지를 파라미터로 받아 분석하여 메일 헤더와 본문으로 새롭게 구성한다. 그리고 PGP가 사용된 경우 MIME(Multipurpose Internet Mail Extensions) 헤더를 새롭게 구성하고 메일 본문을 외부의 PGP 모듈을 호출하여 PGP로 암호화를 하고 이를 MTA를 이용하여 실제로 전자 메일을 전송한다.

목록 모듈은 메일 Box에서 메일의 헤더 부분만을 읽어 들여 제목과 날짜, 송신자의 목록을 만들어 주고, 수신된 메일에 PGP 사용 여부, 파일 첨부 여부 등을 나타내어 웹 브라우저로 전송한다.

내용 출력 모듈은 수신된 메일에 대해 본문과 첨부 파일을 메일 Box로부터 읽어 들인 다음 PGP 메시지 혹은 PGP의 공개키가 포함되어 있는지, 첨부된 파일에 PGP가 사용되었는지를 확인한 후 PGP 모듈을 이용하여 서버측에서 바로 메시지를 복호화 하거나 클라이언트로 메시지를 가져올 수 있게 해준다.

3.3 PGP 모듈

PGP는 메일 전송에 있어 메시지의 기밀성을 위한 암호화와 메시지의 무결성을 확인하는 전자 서명 부분으로 나누어 서로 다른 메시지를 보낼 수도 있다. 즉 메일 메시지를 암호화하여 전송 할 수 있고, 또는 전자 서명만을 이용하여 메시지를 전송 할 수 있도록 구성하였다.

PGP 모듈은 전송 모듈과 목록 모듈이 메일 메시지에 암호화, 복호화를 하는 모듈이다. 또한 입력 모듈을 통한 전송 모듈과 목록 모듈을 통한 내용 출력 모듈만이 제어할 수 있도록 구현하였다. 메시지의 암호화와 복호화, 그리고 전자서명에 사용되는 Key를 보관하는 모듈을 PGP 모듈에서 제어 할 수 있도록 하였다.

4. 결론

본 논문에서 구현한 웹 기반의 메일 시스템은 일반 사용자가 클라이언트용 메일 프로그램에서 설정해야 하는 메일 관련 서버 설정이 필요 없는 웹 메일 시스템 구조 위에 PGP를 이용한 메시지 암호화와 SSL protocol을 이용하여 웹 브라우저와 웹 메일 시스템 사이의 안전한 메시지 전송을 할 수 있도록 구현하였다. 따라서 일반 사용자들은 웹 브라우저만을 가지고 메일 관련 서버의 설정 없이 쉬운 사용자 인터페이스를 통하여 안전하게 자신의 메일을 전송하고 관리할 수 있다.

[참고문헌]

[1] Simson Garfinkel, "PGP - Pretty Good Privacy", O'Reilly & Associates, INC. 1995

[2] Bruce Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons, INC. 1996

[3] D.Brent Chapman and Elizabeth D. Zwicky . "Building Internet Firewalls", O'Reilly & Associates, INC. 1998

[4] William Stallings, "Network and Internetwork security Principles and Practice", Prentice-Hall, 1995

[5] Alan O.Freier, Philip Karlto, Paul C. Kocher, "The SSL Protocol Version 3.0", Netscape Communications Corporation 1996

[6] ITU-T Recommandation "X.509" Data Networks and Open System Communications Directory 1997

[7] Jonathan B. Postel, Simple Mail Transfer Protocol : Internet RFC 821, 1982

[8] Mike St. Johns, Authentication Server : Internet RFC 931, 1985

[9] Shishir Gundavaram, "CGI Programming on the World Wide Web", O'Reilly & Associates, INC. 1996