PGP 방식을 이용한 전자우편 보안

박동욱[o†] 박재희[†] 김일민[††]

† 계명대학교 컴퓨터 공학과
†† 한성대학교 컴퓨터 공학과
{dwpark, jpark}@kmucc.keimyung.ac.kr
ikim@hansung.ac.kr

A Secure E-Mail System Using the PGP

Dong-Uk Park[o†] Jae-Hee Park[†] Il-Min Kim[††]

† Dept. of Computer Science, Keimyung University
†† Dept. of Computer Science, Hansung University

요 약

일반 전자우편은 그 내용이 개방된 채로 이동하고 있어 중간에서 탈취, 변조될 가능성이 있으며, 중요한 내용들이 제 3자에게 노출되어 많은 피해자를 발생시키고 있다. 웹과 전자우편의 보안에 대한 연구는 이미 많은 부분에서 이루어져 왔으나 이러한 보안기술을 사용함에 있어 기존의 방식에서는 몇 가지 문제점이 발견되고 있다. 본 논문에서는 웹 기반 전자우편 환경에, 현재까지도 뛰어난 보안성을 가진 것으로 알려져 있는 PGP 기술을 접목해서 안전하고 편리하며, 이동성이 많은 사용자 환경에 적합한 웹 기반 전자우편 보안 시스템을 구현하였고, Java 언어를 이용한 애플릿-서블릿간 통신 방식을 사용하여 기존의 방식에서 발견되는 클라이언트-서버간 통신시의 보안 취약 문제점을 해결하였다.

1. 서론

인터넷은 세계 최대의 통신 네트워크로서 최근 그 사용이 급격히 증가하고 있다. 특히 월드 와이드 웹(WWW)은 그 사용상의 편리함과 무한한 정보의 제공으로 인하여 더욱 많은 사람들이 인터넷이라는 가상공간을 이용하는데 일조를 하고 있다[1]. 웹 메일 방식은 이동성이 많은 사용자들의 환경에 매우 적합하고 사용상 까다로운 환경설정이 필요 없어서 전자우편의 대중화에 큰 기여를 하고 있다. 그러나 대부분의 전자우편들은 봉투에 넣어져서 밀봉되는 일반 편지와는 달리 내용이 그대로 개방된 채로 네트워크 경로를 따라 여러 게이트웨이를 거쳐 최종 목적지까지 이동하고 있다[2]. 이 과정에서 전자우편이 탈취, 변조되고 있으며 알아서는 안될 중요한 내용들이 제 3자에게 노출되어 많은 피해자들을 발생시키고 있다. 이에 전자우편 보안에 대한 필요성이 점차 제기되기 시작하였고, 앞으로 전자우편 환경이 더욱 보편화되고 일반화됨에 따라 전자우편 보안을 더욱더 절실히 필요로 하게 될 것이다[2][5]

2. 관련연구

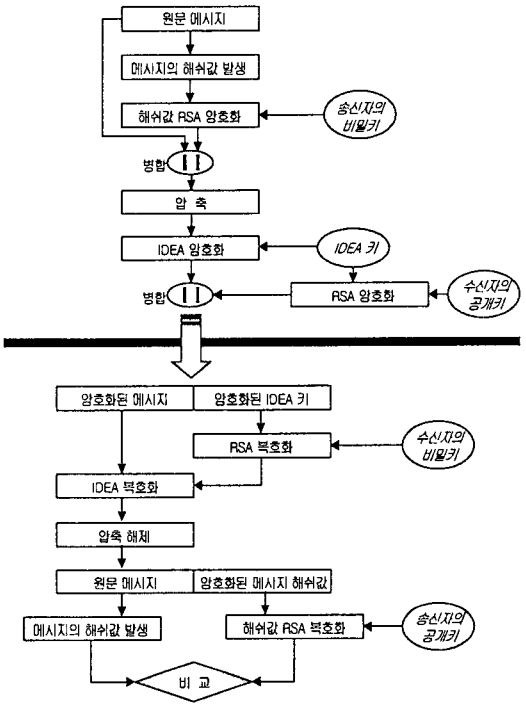
웹과 전자우편의 보안에 대한 연구는 이미 많은 부분에서 이루어져왔는데, 그 중에 웹의 보안기술로서 SSL (Secure Socket Layer), S-HTTP(Secure Hyper Text Transfer Protocol)가 대표적인 기술로 제안되었으며, 전자우편의 보안기술로서 PGP(Pretty Good Privacy), PEM(Privacy Enhanced Mail)이 가장 대표적인 보안기술로 제안되어 현재 사용되고 있다[1][2][3]. SSL은 웹 상의 안전한 데이터 송수신을 위해 Netscape사에서 제안한 프로토콜로써 HTTP, TELNET, FTP 등과 같은 응용 프로토콜 계층과 TCP 전송 프로토콜 계층 사이에서 작동된다[1]. 그러나 SSL의 경우에는 첫째, 사용자의 인증을 위한 전자서명만을 제공하고 메시지에 대한 전자서명을 지원해주지 않는 문제점이 있고, 둘째 미국의 암호기술 수출정책에 따라 자국 이외에서는 암호화에 사용하는 키를 40-bit의 크기로 제한을 두어 암호화에 대한 신뢰도가 상대적으로 떨어지는 단점이 있다[4]. S-HTTP는 1994년 EIT(Enterprise Integration Technologies)에서 기존의 WWW 기반 프로토콜인 HTTP상에 암호화 모듈을 첨가함으로써 데이터의 기밀성과 무결성을 보장받을 수 있도록 제안한 프로토콜이다[2]. PGP는 Phil Zimmermann에 의해 개발되었으며 구현이 쉽고 역시 높은 보안성을 갖고 있어 현재 전자우편의 보안 도구로 많이 사용되고 있다. 하지만 PGP는 사용법이 복잡하고 까다롭기 때문에 일반 사용자들에게는 다소 어렵고, 내용의 보안을 위한 암호화/복호화 과정이 PGP가 설치된 서버상에서만 이루어지기 때문에 서버와 서버간의 전자 우편 전송에 사용시 보안에 큰 문제점을 야기시킬 수 있다.

3. PGP의 동작원리

Phil Zimmermann이 제작하여 1991년 처음 발표한 PGP는 전자우편과 파일의 암호화 저장에 적용될 수 있는 기밀성과 인증 서비스를 제공한다. PGP는 여러 차례 수정을 거쳐, 지금은 전자우편의 보안 도구로 폭넓게 이용되고 있다. PGP가 활성화된 요소로는 다음과 같다.

- o 전세계적으로 다양한 기종에서 동작한다.
- o 소스가 공개되어 있다.
- o 싼 가격의 상용제품과 공개용 버전이 존재한다.
- o 공개적인 검토 작업을 거쳤다.

PGP는 전송하고자 하는 내용에 대하여 암호 알고리즘을 이용하여 암호화함으로서 전자우편을 엽서가 아닌 밀봉된 봉투에 넣어서 보내는 개념이다. PGP가 동작하는 전체적인 과정을 정리하면 [그림 3-1]과 같다.



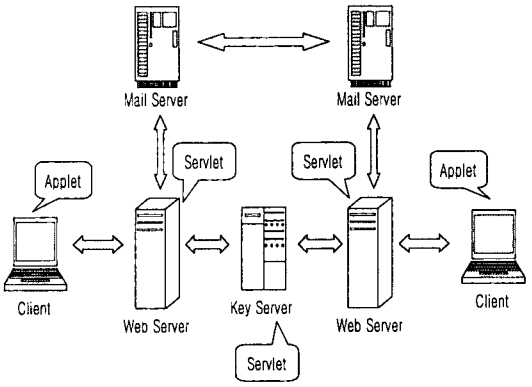
[그림 3-1] PGP 전체 동작 과정

4. 시스템 설계와 구현

보안성이 우수한 PGP 기술을 웹 기반 전자우편 송수신 방식에 적용하고, Java 애플릿으로 구현하여 보안성이 취약한 부분인 클라이언트-서버간의 통신에 있어서도 서버-서버간 통신과 동일한 보안성을 부여함으로써 보안성이 강화된 웹 기반 전자우편 보안 시스템을 구현하였다.

4.1 시스템 구성

구현한 웹 기반 전자우편 보안시스템의 구성도는 [그림 4-1]과 같다.



[그림 4-1] 전체 시스템 구성도

클라이언트(Client)는 Internet Explorer 5.0 혹은 Netscape 4.71 이상을 지원하는 웹 브라우저를 탑재한 PC로서 전자우편 사용자를 웹 서버(Web Server)에 연결시킨다. 웹 서버에는 암호 메일 송수신에 필요한 실질적인 코드들을 모두 적재하고 있어서 클라이언트가 해당 웹 페이지를 로딩할 경우 자동으로 클라이언트 측에 해당 애플릿 코드를 전송하고 SMTP와 POP3를 지원하는 메일 서버를 통해 암호화된 전자우편을 송수신한다.

키 서버에는 크게 두 가지 기능을 수행하는 서블릿이 존재하여 동작하는데, 첫 번째는 클라이언트에서 새로이 생성된 키 쌍(공개키, 비밀키)을 웹 서버를 통해 넘겨받아 이를 파일로 기록·보관하는 역할을 담당하고, 두 번째는 클라이언트로부터 요청 받은 키 쌍을 웹 서버를 통해 해당 클라이언트로 보내주는 역할을 담당한다. 비밀키는 IDEA 암호 방식으로 암호화된 상태로 각 사용자의 User ID로 명명된 디렉토리에 각기 보관되어 있어 만약 이 비밀키가 제 3자에게 유출이 된다 하더라도 passphrase를 알고 있는 사용자 외에는 사용이 불가능하다. 또한 공개키는 하나의 파일로 일괄적으로 기록되어 유지되도록 하여 새로운 공개키가 추가될 때마다 공개키 파일에 추가, 갱신되도록 하였다. 웹 서버를 통해 정당한 사용자의 키 요청이 들어오면 키 서버는 역시 웹 서버를 통해 요청한 사용자의 클라이언트(애플릿)로 해당 키 쌍을 보내주게 된다. 이는 키 서버에서 동작하는 서블릿과 웹 서버의 서블릿, 클라이언트에서 동작하는 애플릿이 서로 통신함으로써 이루어진다.

4.2 시스템의 설계

4.2.1 키의 생성 및 사용

전자우편을 암호화하기 위해 사용하는 PGP는 두 개의 암호화 알고리즘을 사용한다. 두 개의 암호화 알고리즘은 메시지 원문을 암호화하는데 사용되는 IDEA 알고리즘과 IDEA 알고리즘에서 사용되는 키를 암호화하는데 사용되는 RSA 알고리즘이다.

키 생성 부분은 모든 과정이 클라이언트의 애플릿에서 이루어진다. 128-bit IDEA 키는 사용자로부터 입력되는 *passphrase*로부터 MD5 해쉬함수를 통해 만들어지고, RSA 키 쌍인 비밀키와 공개키는 Java의 securerandom 클래스에서 지원하는 random 수를 이용해 생성되어 키 서버에 저장된다. 그 중에 공개키는 공개키를 모아두는 파일에 저장되고 비밀키는 IDEA 암호 방식으로 암호화된 후 비밀키 파일에 저장된다.

키 생성시에 사용자는 생성할 키의 크기로 512-bit, 768-bit, 1024-bit 중에서 하나를 선택하도록 하였고, 자바에서 지원하는 자료구조의 가장 큰 정수 구조가 64-bit 크기의 long형이므로 사용자가 선택한 크기만큼의 정수를 연산에 사용하기 위해서 BigInteger 클래스를 사용하였다.

4.2.2 전자서명과 압축

메시지의 무결성을 보장하기 위한 인증과 송신 부인방지를 위한 전자서명 기능을 가지기 위해서는 RSA 암호 알고리즘과 MD5 해쉬함수를 사용한다. 송신측에서는 메시지의 해쉬값을 송신자의 비밀키로 암호화하고, 수신측에서는 그것을 송신자의 공개키로 다시 복호하여 같이 받은 원문 메시지의 해쉬값과 비교함으로써 메시지가 중간에 변조되었는지의 여부를 확인할 수 있고 송신자가 보낸 것이 확실한지의 여부 또한 확인할 수 있다.

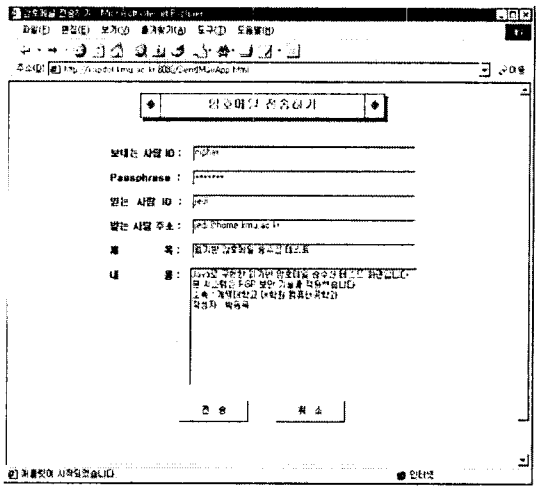
메시지 압축은 원문 메시지를 암호화하기 전에 수행된다. 압축을 함으로서 얻는 이점은 두 가지가 있다. 첫 번째로는 메시지를 압축함으로써 전체 메시지의 크기를 줄여 암·복호화 하는데 수행되는 시간과 전송하는데 걸리는 시간을 줄일 수 있다는 점이고, 두 번째로는 암호화 작업의 결과물에 대한 비도를 높일 수 있다는 점이다[2]. 본 시스템에서는 GZIP 압축 형식을 사용함으로서 전체적으로 메시지의 크기를 50% 가량 줄이는 결과를 가져왔다.

5. 전자우편 보안 시스템의 구현결과

개발된 웹 기반 전자우편 보안 시스템은 Intel Pentium MMX 166MHz, 128M 메모리의 PC 상에서 Microsoft Internet Explorer v5.5의 웹 브라우저를 사용해 실험되어졌다. 암호 메일을 송수신 하기 위해서는 먼저 새로운 사용자에 대한 키를 생성해 키 서버에 등록하는 작업을 거쳐야 한다.

사용자가 비밀키로 사용될 키의 크기를 결정하고 등록할 사용자 ID와 passphrase를 입력한 후 "생성하기" 버튼을 누르면 키는 자동으로 생성되어 키 서버로 전송되어지고 보관된다. 사용자 ID는 각 개인의 키를 식별할 목적으로 사용되므로 유일해야 하며, passphrase는 추후 이 키를 사용하고자 할 때 키에 대한 사용자의 진위 여부를 결정할 중요한 단서이므로 제 3자에게 누출되지 않도록 한다. passphrase의 입력에는 이론상으로는 그 길이에 제한이 없으므로 제 3자가 특정 사용자에 대한 passphrase를 추측하기란 실제로는 거의 불가능하다.

[그림 5-1]은 앞에서 생성된 키를 사용하여 메일 주소가 "jedi@home.kmu.ac.kr" 이라는 사용자에게 암호 메시지를 전송하는 화면을 보인 것이다.



[그림 5-1] 암호 메시지 전송 화면

6. 결론

본 논문에서는 웹 기반 환경에 전자우편 보안 서비스와 통합한 방식으로 운영되는 하나의 시스템을 구현하였다. 전자우편 내용의 기밀성과 무결성을 보장하기 위한 방법으로는 현재 전자우편 보안 분야에서 가장 활발히 사용되고 있는 PGP 기술을 차택하여 높은 보안성을 유지하였고, 웹 기반 전자우편 서비스 방식을 채택하기 위하여 기존의 WWW 보안 방법과는 다른 형태로 HTTP 암호 프로토콜을 제안하였다. 제안된 시스템으로 전자우편 송수신을 할 경우 기존의 기술들에서 나타나는 단점인 클라이언트-서버간의 보안 취약성과 외부 프로그램의 설치에 따른 번거로움, 범용적인 HTTP 전송 프로토콜과의 비호환성을 모두 해결할 수 있었다. 또한 Java 언어로 구현되었기 때문에 어떤 기종에서도 원만히 수행될 수 있는 높은 이식성을 갖고 있다.

7. 참고 문헌

[1] 강신각, 박정수. "월드 와이드 웹(WWW) 보안기술". 정보처리 제7권 제2호, pp.41-47, 2000. 3.

[2] 박창섭. 『암호이론과 보안』. 대영사, pp.272-286, 1999.

[3] 송상헌, 박정수, 강신각, 김재명, 안은미, 류재철. "웹 보안을 위한 사용자 인증과 암호화 통신 구현.". 제7회 통신정보합동학술회의 발표논문, 1997.

[4]이은성, 박현동, 류재철. "안전한 WWW통신을 위한 NetCrypt 설계." 『한국통신정보보호학회 종합학술발표회논문집』 (1998):191-200.

[5]장윤희,박선종. 『인터넷 보안 가이드』 위저드, 1998.

[6]한국전자통신연구원. 『암호학의기초』 경문사, 1999.