PGP 방식을 이용한 웹 기반 전자우편 보안 시스템

박 동 욱† · 박 재 희†† · 김 진 상†† · 김 일 민†††

요 약

정보화 사회가 도래하고 우편이나 통신 체계도 물리적인 공간에서 인터넷이라는 가상공간으로 점차 옮겨짐에 따라 일반인들의 전자우편에 관한 관심이 높아지고 있다. 대부분의 전자우편은 그 내용이 개방된 채로 이동하고 있어 중간에서 탈취, 변조되고 있으며, 중요한 내용들이 제3자에게 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.

키워드 : 전자우편, 보안, 암호화

A Web Based Secure E-Mail System Using the PGP Algorithm

Dong-Uk Park† · Jae-Hee Park†† · Jin-Sang Kim†† · Il-Min Kim†††

ABSTRACT

With the high-tech informatization of our society that caused the mail and communication systems to transfer from physical to cyber space of the Internet, people become more and more interested in using E-mail. Because most of E-mail messages are transferred in an open form, they are carried off and altered in the process of sending and receiving, and due to the disclosure of important messages to unauthorized persons, some serious problems are occurred. Many kinds of studies on the protection of the World Wide Web and E-mail have been carried out, but several problems are still being discovered existing protection methods. In this paper, we have developed the web-based secure E-mail system using the PGP algorithm that is well known for a reliable protection method in the web-based E-mail system. This system is anticipated to be a solution to E-mail protection so required in the client-server communication who use Applet-Servlet communication technology in Java language.

Key word : PGP, web mail, Java

1. 서 론

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]. 특히 그 중에서도 인터넷을 이용한 전자우편의 사용에 대한 관심이 점점 높아지고 있다. 이는 전자우편의 효용성이 점점 널리 알려지고 있을 뿐만 아니라, 예전에는 다소 까다로웠던 전자우편 사용 환경이 최근에는 복잡한 환경 설정이 필요 없고 단순히 웹 브라우저를 통해서 전자우편을 주고받을 수 있도록 하는 웹 메일(Web Mail)이 등장함으로서 많은 사용자들이 쉽게 전자우편을 사용할 수 있게 됨에 있다. 그래서 최근에는 많은 회사에서 무료 웹 메일 서비스를 하고 있다.

대부분의 전자우편들은 내용이 그대로 개방된 채로 네트워크 경로를 따라 여러 게이트웨이를 거쳐 최종 목적지까지 이동하고 있다[2]. 이 과정에서 전자우편이 탈취, 변조될 가능성이 있으며, 중요한 내용들이 제3자에게 노출되어 많은 피해자들을 발생시키고 있다. 앞으로 전자우편 환경이 더욱 보편화되고 일반화됨에 따라 전자우편 보안을 더욱더 절실히 필요로 하게 될 것이다[2, 7, 10, 14].

웹과 전자우편의 보안에 대한 연구는 이미 많은 부분에서 이루어져왔는데, 그 중 웹의 보안기술로서 SSL(Secure Socket Layer), S-HTTP(Secure-HyperText Transfer Pro-tocol)가 대표적인 기술로 제안되었고, 전자우편의 보안기술로서 PGP(Pretty Good Privacy), PEM(Privacy Enhanced Mail)이 가장 대표적인 보안기술로 제안되어 현재 사용되고 있다[1, 2, 4]. 그 중 현재 전자우편의 보안도구로 높

† 준 회 원 : (주)나라비전 연구원
†† 정 회 원 : 계명대학교 컴퓨터전자공학부 교수
††† 종신회원 : 한성대학교 컴퓨터공학과 교수
논문접수 : 2000년 10월 9일, 심사완료 : 2001년 2월 10일

은 보안성을 갖고 있어 PGP를 가장 많이 사용하고 있다. 그러나 PGP는 사용법이 복잡하기 때문에 웹 기반 전자우편 시스템에서는 사용하고 있지 않다. 또한 PGP를 사용하는 전자우편 시스템은 암·복호화 과정이 서버상에서만 이루어지기 때문에 서버와 클라이언트간의 보안에 문제점을 야기시킨다[16].

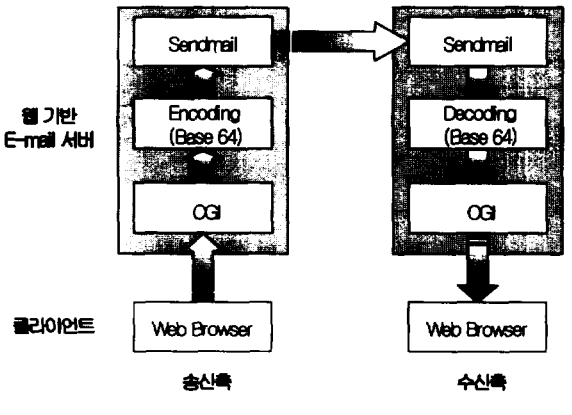
본 연구에서는 사용하기 쉽고 편리한 환경을 제공하는 웹 기반 전자우편 시스템에 PGP를 적용하여 보안성이 향상되고 Java 언어를 이용한 애플릿-서블릿간 통신 방식을 사용하여 기존 전자 우편 보안 시스템이 가지고 있는 클라이언트와 서버간의 보안문제가 해결된 웹 기반 전자우편 보안 시스템을 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 웹 기반 전자우편 보안 시스템을 구현하기 위해 적용된 PGP 보안 기술을 개략적으로 살펴보고, 3장에서는 시스템의 전체 구성도와 설계, 구현 부분을 세부적으로 살펴보며, 4장에서는 구현된 시스템을 이용하여 실제로 암호화된 메시지를 송수신하는 과정을 보이며, 5장에서는 본 시스템의 특징과 향후 활용 방안을 제시한다.

2. 관련연구

2.1 웹 기반 전자우편 시스템의 동작원리

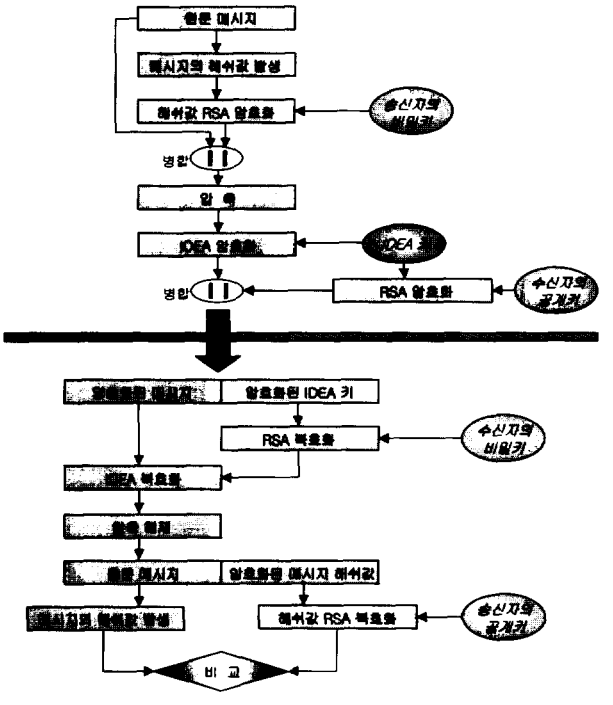
현재 많은 회사에서 일반 사용자들에게 무료로 서비스하고 있는 웹 기반 전자우편 시스템의 동작원리를 나타내면 (그림 1)과 같다. 사용자는 일반 웹 브라우저를 통해 서버에 접속한 후 보내고자 할 내용을 입력하고 POST 방식으로 서버에 전송하면 서버는 전송 받은 메시지를 CGI 프로그램에서 파싱한다. 파싱된 메시지는 연속적인 8-bit의 흐름으로 이루어져 있지만, 대개의 전자우편 시스템은 ASCII 문자만을 인식하므로 3개의 8-bit를 4개의 ASCII 문자로 변화시키는 Base64 인코딩 작업을 거친 후, sendmail 프로그램을 구동해서 목적지 서버로 전송하게 된다. 목적지 서버에 도착한 메시지는 서버에 저장되어 있다가 수신자가 웹 브라우저를 통해 서버에 접속해서 요청을 하게 되면 반대 과정을 거쳐 수신자의 브라우저에 보여지게 된다[15, 16].



(그림 1) 웹 기반 전자우편 시스템의 동작원리

2.2 PGP Algorithm

Phil Zimmermann이 1991년 처음 발표한 PGP algorithm(그림 2)는 전자우편과 파일의 암호화 저장에 적용될 수 있는 기밀성과 인증 서비스를 제공한다. PGP는 처음 발표 후 계속해서 여러 버전으로 수정, 발표되어 왔으며, 지금은 전자우편의 보안 도구로 폭 넓게 이용되고 있다. PGP는 전송하고자 하는 메시지에 대하여 암호 알고리즘을 이용하여 암호화하는 방식이다.



(그림 2) PGP 전체 동작 과정

PGP에서는 내부적으로 대칭키 암호화 방식과 공개키 암호화 방식의 두 가지를 사용한다. 대칭키 암호화방식은 암호화 할 때 사용했던 키를 암호화된 메시지와 함께 상대방에게 전달해주어야 한다. 이 방식은 메시지를 암호화하는 속도가 빠르다는 장점이 있는 반면 키를 상대방에게 전달해 주어야 하는 키 분배의 문제도 따르게 된다[2, 8]. PGP에서는 장문의 메시지를 암호화할 때는 대칭키 방식인 IDEA 방식을 이용하고 이 때 사용된 IDEA 키를 다시 공개키 방식인 RSA 방식으로 암호화하여 전송하는 방식을 취하였다[3]. 공개키 암호화 방식은 대칭키 암호화 방식의 단점인 키 분배의 문제를 해결한 방법으로 서로 다른 두 개의 키 쌍(공개키, 비밀키)을 사용하고 있다[2, 3, 8].

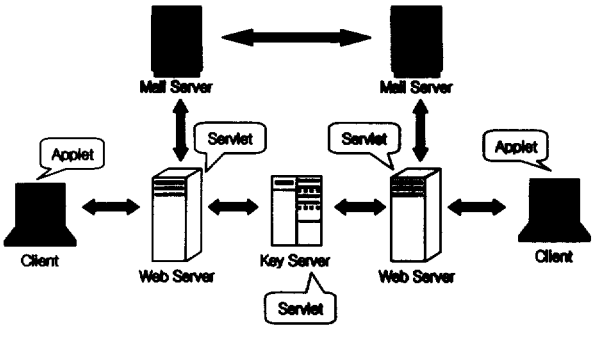
일반 PGP 메일 시스템은 PGP 프로그램이 클라이언트에 설치되거나 서버에 설치되어야 한다. PGP 프로그램을 클라

이언트에 설치하는 경우, 사용자가 장소를 옮길 때마다 다시 설치해야 하는 불편함때문에 웹 메일의 장점이 반감된다. PGP가 설치된 서버에 접속해서 사용할 경우에는 클라이언트 프로그램을 설치할 필요는 없으나, 클라이언트-서버 간 통신에 있어서 PGP가 지원하는 기밀성을 보장받을 수가 없다. 본 연구에서는 PGP 우편 시스템의 이러한 단점을 개선하고자 하였다.

3. 시스템 설계와 구현

3.1 전체 시스템의 구성

웹 기반 전자우편 보안 시스템의 구성도는 (그림 3)과 같다. 클라이언트는 Internet Explorer 5.0 혹은 Netscape 4.71 이상을 지원하는 웹 브라우저를 탑재한 PC로서 전자우편 사용자를 웹 서버에 연결시켜 준다. 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.



(그림 3) 전체 시스템 구성도

키 서버에는 크게 두 가지 기능을 수행하는 서블릿이 존재하여 동작하는데, 첫번째는 클라이언트에서 새로이 생성된 키 쌍(공개키, 비밀키)을 웹 서버를 통해 넘겨받아 이를 파일로 기록·보관하는 역할을 담당하고, 두번째는 클라이언트로부터 요청받은 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. 클라언트에서 시행되는 자바 애플릿을 사용함으로서 메일 서버와 클라이언트간의 보안을 구현하였다.

3.2 시스템 설계

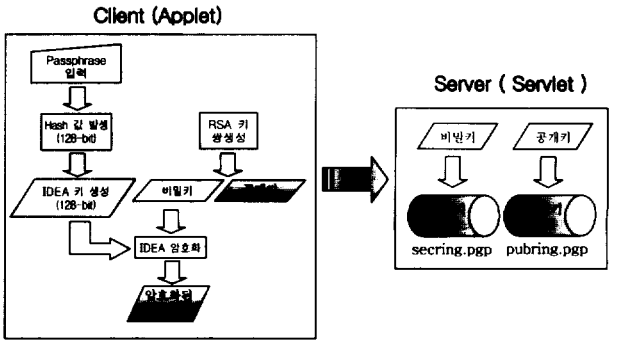
3.2.1 키의 생성 및 사용

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. 여기에서는 IDEA 알고리즘에서 필요한 IDEA 키와 RSA 알고리즘에서 필요한 RSA 키 쌍(비밀키, 공개키)의 생성과 사용에 대해 언급하였다.

키 생성 부분은 모든 과정이 클라이언트 측의 애플릿에서 이루어진다. 128-bit IDEA 키는 사용자로부터 입력되는 passphrase로부터 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.

(그림 4)는 클라이언트에서 RSA 키 쌍을 생성한 후 서버로 전송하여 파일로 기록·보관하는 과정을 나타낸 블록 다이어그램이다.



(그림 4) RSA 키 쌍 생성 과정

3.2.2 전자서명과 압축

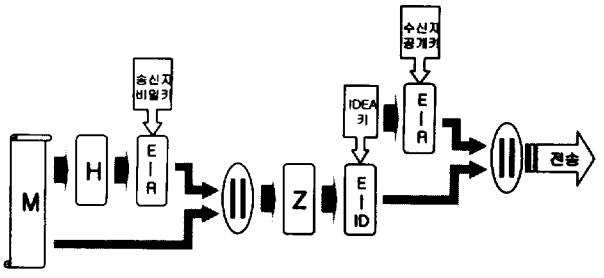
메시지의 무결성을 보장하기 위한 인증과 송신 부인방지를 위한 전자서명 기능을 가지기 위해서는 RSA 암호 알고리즘과 MD5 해쉬함수가 사용된다. RSA 암호 알고리즘은

IDEA 키를 암호화할 때와는 반대로 키를 사용한다.

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 가져올 수 있었다.

3.2.3 메시지 암호 모듈 및 복호 모듈

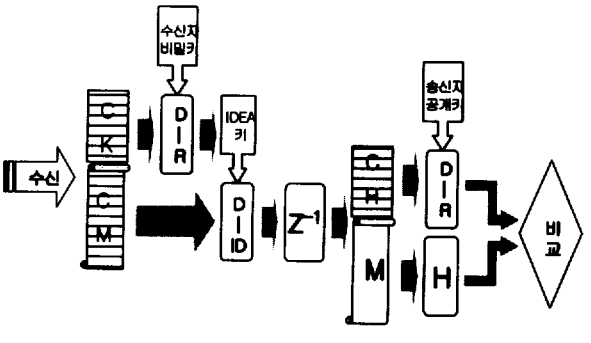
메시지 송신측 암호 모듈의 블록 다이어그램은 (그림 5)에 있다.



M : 원문 메시지
H : MD5 해쉬 함수
E-R : RSA 암호화
Z : 압축
E-ID : IDEA 암호화
⊕ : 병합

(그림 5) 송신측 모듈 블록 다이어그램

메시지 암호와 관련된 모든 루틴은 클라이언트 측에 다운 로드되어 수행되는 애플릿 상에서 이루어진다. 이는 클라이언트 측에서 메시지가 완벽하게 암호화된 상태에서 전송되기 위함이다. 메시지 수신측 복호 모듈의 블록 다이어그램은 (그림 6)에 있다. 메시지 암호 모듈과 마찬가지로 복호에 관련되는 모든 루틴들도 클라이언트 측의 애플릿 코드로 다운 로드되어 수행되어진다.



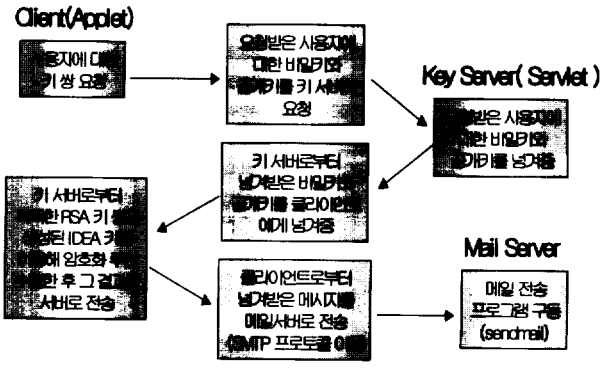
OM : 암호화된 원문 메시지
OK : 암호화된 IDEA 키
D-R : RSA 복호화
D-ID : IDEA 복호화
Z⁻¹ : 압축
CH : 암호화된 해쉬값
M : 원문 메시지
H : MD5 해쉬 함수

(그림 6) 수신측 모듈 블록 다이어그램

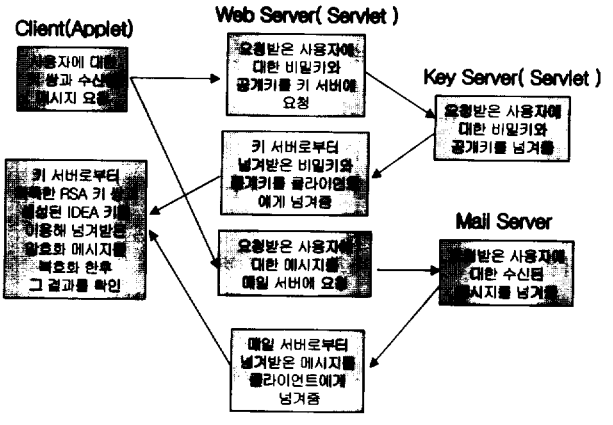
3.2.4 서버간 통신

클라이언트-서버간, 서버-서버간 통신은 객체 기반의 HTTP 통신을 기본으로 하였고, 그 중에서도 홈페이지에서 서블릿으로 데이터를 전송할 때는 POST 방식을 사용하였다. 클라이언트-서버간 통신을 구현하는 경우 소켓 프로그래밍을 사용하는 것이 보다 일반적이지만, 자바 애플릿 경우 샌드 박스에 의한 보안 방식으로 인하여 자유로운 데이터 통신이 불가능하였다[5, 9, 11]. 객체 기반의 HTTP 통신에서는 요청하고 응답받는 데이터들을 일반 프리미티브 자료형(정수형, 문자형, 실수형, boolean형) 단위로 처리하는 것이 아니라 객체 단위로 처리한다. 이를 위해서는 Java언어가 지원하는 I/O 클래스 중에 ObjectInputStream 클래스와 ObjectOutputStream 클래스를 사용하였다.

이를 보다 자세히 나타내면 (그림 7)은 클라이언트-서버간, 서버-서버간 메시지 송신 과정을 나타낸 블록 다이어그램이고, (그림 8)은 클라이언트-서버간, 서버-서버간 메시지 수신 과정을 나타내는 나타낸 블록 다이어그램이다.



(그림 7) 송신측 데이터 이동 과정



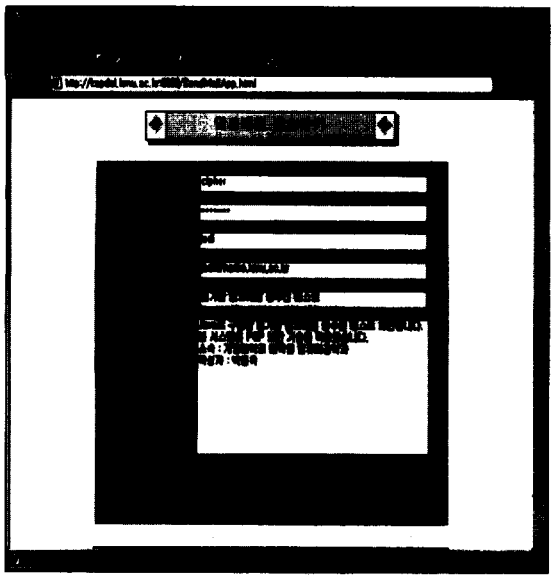
(그림 8) 수신측 데이터 이동 과정

4. 웹 기반 전자우편 보안 시스템의 구현 결과

개발된 웹 기반 전자우편 보안 시스템은 Intel Pentium MMX 166MHz, 128M 메모리의 PC상에서 Microsoft In-

ternet Explorer v5.5의 웹 브라우저를 사용하였으며, 개발 도구는 JDK 1.2.2와 Java Web Server 2.0을 사용하였다.

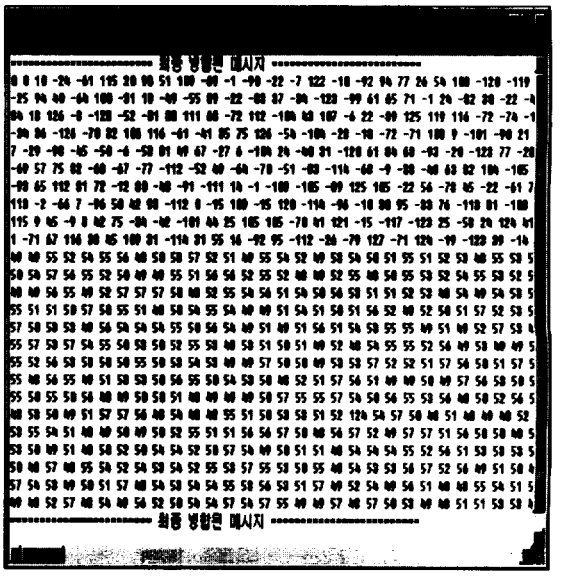
암호 메일을 송수신 하기 위해서는 먼저 새로운 사용자에 대한 키를 생성해 키 서버에 등록하는 작업을 거쳐야 한다. 사용자가 비밀키로 사용될 키의 크기를 결정하고 등록할 사용자 ID와 passphrase를 입력한 후 "생성하기" 버튼을 누르면 키는 자동으로 생성되어 키 서버로 전송되어지고 보관된다. 사용자 ID는 각 개인의 키를 식별할 목적으로 사용되므로 유일해야 하며, passphrase는 추후 이 키를 사용하고자 할 때 키에 대한 사용자의 진위 여부를 결정할 중요한 단서이므로 제 3자에게 누출되지 않도록 한다. (그림 9)는 앞에서 생성된 키를 사용하여 메일 주소가 "jedi@home.kmu.ac.kr"이라는 사용자에게 암호 메시지를 전송하는 화면을 보인 것이다.



(그림 9) 암호 메시지 전송 화면

송신자는 일반 전자우편 전송에서와 동일한 방법으로 메시지의 내용을 기록한 후 "전송"이라는 버튼을 누르기만 하면 나머지 과정은 애플릿에서 내부적으로 메시지 암호화 과정을 거친 후 암호화된 결과물을 서버로 전송하게 되고 서버는 이를 받아서 곧바로 메일 서버를 통해 수신 대상자의 메일 서버로 전송하게 된다. (그림 10)은 암호화된 메시지가 목적지 클라이언트에 도착하기까지 네트워크를 따라 이동하는 데이터 스트림을 보인 것이다.

메시지를 수신하는 과정은 크게 두 가지로 나뉘어진다. 먼저 메일 서버에 접속하기 위한 사용자 인증 과정을 거친 후 서버에 정상적으로 접속이 되면 수신된 메일에 대한 정보를 받아와 화면에 보여준다. 수신된 메시지가 복수개일 경우에도 메일에 번호를 붙여 그에 대한 정보를 보여준다. 그런 다음 사용자가 메일을 선택하고 정확한 passphrase를 입력한 후 "복호하기" 버튼을 누르면 비로소 해당 메일에

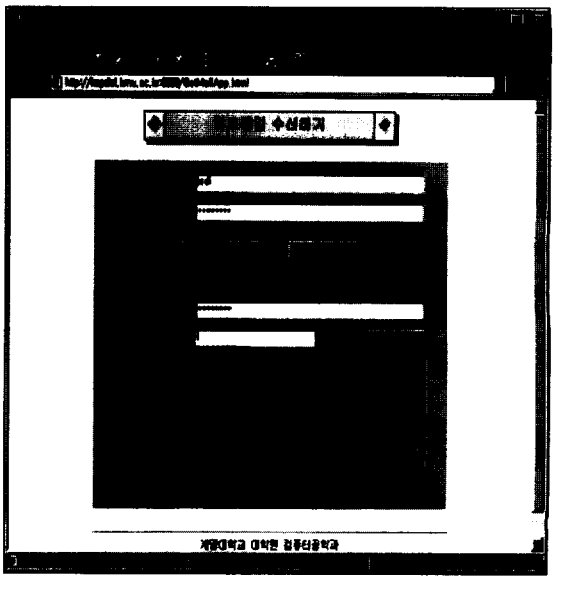


(그림 10) 암호화된 데이터 스트림

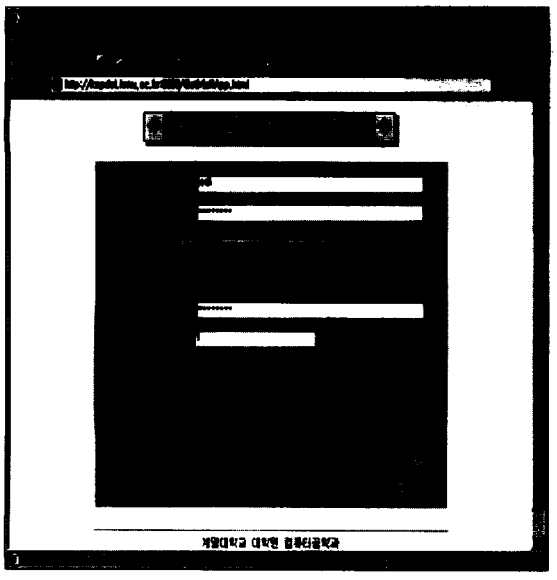
대한 복호화 작업이 수행된 후 화면에 그 내용을 보여준다.

암호화 메시지의 복호화 성공, 실패 여부는 오로지 정확한 passphrase가 입력되었는지의 여부에 달려있으므로 사용자는 특히 passphrase의 관리에 신경써야 한다. (그림 11)은 정당한 사용자가 서버에 접속한 후 자신에게 배달된 암호화 메시지를 받아와서 복호하고 있는 화면(그림 12)을 보인 것이다.

본 암호 시스템의 핵심은 사용자가 입력하는 passphrase에 있다. passphrase를 유출당하면 이 passphrase로 부터 128-bit의 IDEA 키를 추출할 수 있고 추출된 키로 해당 사용자의 비밀키를 복호화한 후 메시지에 포함된 세션 키(메시지 암호화 키)를 복호화하여 원문 메시지를 해독할 수 있



(그림 11) 암호화된 메시지 복호중 화면



(그림 12) 암호 메시지 복호 성공 화면

는 것이다. 메시지를 암호화하는데 사용된 128-bit의 IDEA 키는 1998년까지 암호 알고리즘의 표준으로 채택되어 사용되어 온 DES 암호 알고리즘의 64-bit 키 사이즈보다 두 배 큰 사이즈이다. 128-bit의 키를 해독하기 위해서는 전수검사를 할 경우 2^{128}개의 키 즉, 10^{38}개의 키를 조사해야 한다. 이는 1초당 10억개의 키를 검사할 수 있는 칩을 설계해서 전수검사에 사용할 경우 10^{13}년이라는 엄청난 시간이 소요된다[13]. 또한 이 128-bit의 IDEA 키를 암호화하는데 사용된 1024-bit의 RSA키를 해독하는 것은 309자리의 큰 정수를 인수분해 하는 것과 동일한 계산량을 가진다.

5. 결 론

본 논문에서는 웹 기반 환경에 전자우편 보안 서비스와 통합한 방식으로 운영되는 시스템을 구현하였다. 전자우편 내용의 기밀성과 무결성을 보장하기 위한 방법으로는 현재 전자우편 보안 분야에서 가장 활발히 사용되고 있는 PGP 기술을 채택하여 높은 보안성을 유지하였고, 웹 기반 전자우편 서비스 방식을 채택하기 위하여 기존의 WWW 보안 방법과는 다른 형태로 HTTP 암호 프로토콜을 제안하였다.

기존의 웹 메일은 서버간의 보안은 중요시 하지만, 서버와 클라이언트간의 보안은 거의 구현되지 않은 실정이다. 일부 사용 웹 브라우저가 클라이언트 서버간의 보안을 구현하였으나 사용자가 웹 브라우저의 설정을 바꾸어야 하는 불편함이 있었다. 본 논문에서 구현된 시스템으로 전자우편 송수신을 할 경우 기존의 시스템들에서 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 높은 이식성을 갖고 있다.

본 논문에서 제안된 시스템은 웹 기반 전자우편 서비스에서의 보안을 목적으로 하고는 있으나 전자 상거래에서의 지불 시스템과 같은 웹 기반 정보 제출 응용 시스템의 구현 시에도 SSL이나 S-HTTP같은 기존의 보안 프로토콜을 사용하는 것보다 훨씬 더 높은 융통성과 활용도를 보일 것으로 생각된다.

참 고 문 헌

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

[2] 박창섭, 「암호이론과 보안」, 대영사, pp.272-286, 1999.

[3] 박현동, "PGP(Pretty Good Privacy)와 WWW", WWW-kr '96 강의자료, 1996.

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

[5] 윤지수, 「자바 서블릿 프로그래밍」, SAMGAKHYUNG Press, 1998.

[6] 이은성, 박현동, 류재철, "안전한 WWW통신을 위한 Net-Crypt 설계", 「한국통신정보보호학회 종합학술발표회논문집」, pp.191-200, 1998.

[7] 장윤희, 박선종, 「인터넷 보안 가이드」, 위저드, 1998.

[8] 한국전자통신연구원, 「암호학의 기초」, 경문사, 1999.

[9] Hunter,J. and Crawford,W., JavaTM Servlet Programming. O'REILLY, 1999.

[10] Katagishi, K., Ebihara, Y., Toraichi, K., Sugiyama, T. and Tohru. "A Public Key Cryptography-Based Security Enhanced Mail Gateway with the Mailing." 1999 IEEE Pacific Rim Conference on Communications, 262-265, 1999.

[11] Morrison, M., et al. JavaTM UNLEASHED. Sams.net Publishing, 1996.

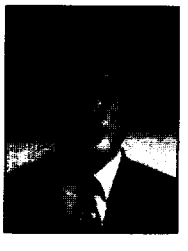
[12] R. Stinson, D., Cryptography : Theory and Practice. CRC Press, 1995.

[13] Schneier, B., Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., 1994.

[14] Siyank, K. and Hare, C., Internet Firewalls and Network Security. New Riders,Publishing, 1995.

[15] Sol, S. and Berznieks, G., CGI/PERL : Web Scripts. M&T Books, 1997.

[16] Stallings, W, Network and Internetwork Security : Principles and Practice. Prentice Hall, 1995.



박 동 욱

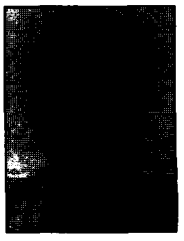
e-mail : okjedi@kebi.com

1998년 계명대학교 컴퓨터공학과 학사

2000년 계명대학교 컴퓨터공학과 석사

2000년~현재 (주)나라비전 근무

관심분야 : 정보보호, 전자우편 보안



김 진 상

e-mail : jsk@kmu.ac.kr

1978년 경북대학교 사대 수학과 학사

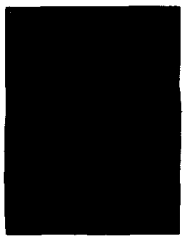
1981년 한국과학기술원 전산학과 석사

1990년 임페리얼칼리지 전산과 박사수료

1981년~1982년 KAIST 전산개발센터 연구원

1982년~현재 계명대학교 컴퓨터전자공학부 교수

관심분야 : 기계학습, 텍스트마이닝, 인공지능, 알고리즘



박 재 희

e-mail : jpark@kmu.ac.kr

1984년 경북대학교 전자공학과(학사)

1992년 Texas A&M 전자공학과(석사)

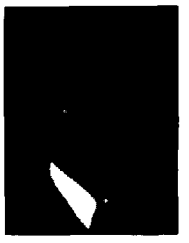
1995년 Texas A&M 전자공학과(박사)

1984년~1990년 국방과학연구소(연구원)

1995년~1997년 삼성전기 주식회사(부장)

1997년~현재 계명대학교 조교수

관심분야 : 음성보안, 메일보안



김 일 민

E-mail : ikim@hansung.ac.kr

1984년 경북대학교 전자공학과(학사)

1989년 뉴저지 공과대학 전산과(석사)

1995년 아리조나 주립대 전산과(박사)

1985년~1987년 전자통신 연구원(ETRI) 연구원

1996년~1997년 삼성 SDS 교육개발센터

1997년~현재 한성대 컴퓨터공학과 교수

관심분야 : 자바, 분산처리