타원곡선 알고리즘을 이용한 안전한 자바 메일 시스템의 설계 및 구현

이원구[0], 조한진, 이재광
한남대학교 컴퓨터공학과
wglee@netwk.hannam.ac.kr

Implementation of Secure E-Mail System based on Java

Won-Goo Lee[0], Han-Jin Cho, Jae-Kwang Lee
Dept. of Computer Engineering, Hannam University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보 전달이 일상 생활처럼 되고 있다. 또한 인터넷, 무선통신, 그리고 자료교환에 대한 증가로 인해 다른 사용자와 접속하기 위한 방식은 빠르게 변화하고 있다. 그러나 이러한 전자메일에도 많은 문제가 존재한다. 기존의 전자메일은 간단한 방법으로 내용을 열람하거나 변조할 수 있어 중요한 정보나 사생활 노출의 위험에서 벗어날 수 없다. 이러한 데이터에 대한 보안이 기대에 미치지 못하고 있기 때문에 암호학적으로 강력한 전자메일 시스템의 개발이 시급하다. 본 논문에서는 기본적인 정보보호 서비스 외에 기존의 전자메일 시스템에서는 제공되지 않는 배달 증명 및 내용 증명 기능을 제공하고 자바 암호 API를 사용하여 안전한 키 교환이 가능하도록 하였다.

Abstracts

As computers and networks become popular, distributing information on the Internet is common in our daily life. Also, the explosion of the Internet, of wireless digital communication and data exchange on Internet has rapidly changed the way we connect with other people. But secure mail is gaining popularity abroad and domestically because of their nature of providing security. That is. it has been used a variety of fields such as general mail and e-mail for advertisement. But, As the data transmitted on network can be easily opened or forged with simple operations. Most of existing e-mail system don't have any security on the transmitted information. Thus, security mail system need to provide security including message encryption, content integrity, message origin authentication, and non-repudiation. In this paper, we design implement secure mail system with non-repudiation service and encryption capability to provide services for certification of delivery and certification of content as well as the basic security services.

1. 서 론

전자 메일은 시간과 공간을 초월하는 서비스로 사용범위가 점차 확대 되어가고 있지만, 전송되고 있는 데이터에 대한 보호 및 안전성은 기대에 미치지 못하고 있는 실정이다. 전자 메일 시스템에서의 정보보호에 대한 취약성을 보완하기 위하여 PEM에 대한 RFC 문서를 발표하였다. 여기에는 암호화 기법을 기반으로 하는 키 관리 및 분배에 대해서 기술되어 있으며 메시지 기밀성, 메시지 무결성, 송신자 신분 인증, 송신 부인 방지 등의 정보보호 서비스를 제공하고 있다. 본 논문은 다음과 같이 구성된다. 2장에서는 보안 솔루션으로서 제시되고 있는 S/MIME, 대표적인 전자메일 보안 프로그램인 PGP와 PEM에 대한 기술들을 설명한다. 3장에서는 전자 메일 시스템 구조, 서비스 등에 관한 내용을 기술한다. 4장에서는 설계한 내용을 구현한 구현 결과에 대해서 기술한다. 끝으로, 5장에서는 메시지 보안 프로토콜과의 비교 결과를 보여주고, 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 SMTP

SMTP는 Simple Mail Transfer Protocol의 약자로서 모든 RFC 표준 규약의 메일 서버들이 서로 다른 메일서버 간에 메일을 주고받는데 사용되는 규약(Protocol)이다[1]. 단점으로는 7비트의 ASCII 텍스트만 처리할 수 있다는 것으로 인해 일반화되고 있는 멀티미디어 자료를 전송할 수 없으며 영문 텍스트 외에 다른 글자들은 전송할 수 없다. 또한 어느 한 사이트에서 MTA를 향상한다고 해서 그 기능이 혁신적으로 개선되지 않는다는 단점을 가지고 있다[1].

2.2 POP3

POP3(Post Office Protocol - Version 3)는 SMTP를 제공하지 못하는 호스트들이 SMTP를 제공하는 워크스테이션을 서버로 하여 메일을 처리할 수 있도록 고안된 서비스로, 메일 서버에 저장되어 있는 메일을 원하는 시간과 장소에서 가져오는 프로토콜이다[2]. POP3의 문제점은 사용자가 자신의 사서함에 배달된 메일을 선택적으로 가져올 수 없다는 것이다.

2.3 메시지 보안 프로토콜

인터넷 전자메일은 전자문서가 목적지에 도착할 때까지 여러 호스트들을 거치는 과정에서 제 3 자에 의해 도청이나 가로채기 또는 변조되기 쉬운데, 이러한 데이터 무결성 및 기밀성은 메시지 보안 프로토콜로서 해결할 수 있다[3].

2.3.1 PEM

PEM은 대칭키 또는 비대칭키 암호화 알고리즘을 사용하여 암호화(envelopin g) 한 후 PEM에서 사용하는 인코딩 방식에 따라서 문자로 변환하여 전자메일을 사용하여 전송하며 인증 (Authentication), 무결성(Integrity), 기밀성 (Confid entiality), 부인방지 (Non-repudiation), 키관리 등과 같은 서비스를 제공하지만 다자간 (Multipart)전자메일이 지원되지 않고, 키발급을 위하여 엄격한 인증기관의 계층구조를 요구하기 때문에 사용이 점차 줄고 있다[4].

2.3.2 PGP

PGP(Pretty Good Privacy)는 전자메일용 암호화 도구로 기밀성, 인증, 무결성, 부인방지 등의 기능을 제공한다. 초기의 PGP에서는 데이터를 암호화하기 위한 대칭형 알고리즘으로 IDEA를 사용하였으며, 대칭형 암호화키를 암호화하는데는 RSA를 사용하였다. 단점으로는 키 관리에 있어서 시간이 많이 소모되며 상당량의 수작업을 필요로 하고 또한 다수 사용자 그룹에 적용하기에는 그 관리

가 너무 어렵다는 점을 들 수 있다.

2.3.3 MIME

MIME(Multipurpose Internet Mail Extensions)은 RFC 1521과 1522 에 규정돼 있으며, 영어 외 문자나 멀티미디어 데이터 등을 전자메일으로 보내기 위한 기술에 사용되는 표준이다[5, 13]. 인터넷 표준 포맷의 헤더를 확장해서 메시지 종류를 인식할 수 있도록 했으며 첨부파일이나 멀티미디어 데이터를 포함하고 있는 전자메일의 포맷에 관한 표준을 가리킨다.

2.3.4 S/MIME

S/MIME(Secure Multipurpose Internet Mail Extensions)은 인터넷 MIME 메시지에 전자서명과 암호화기능을 첨부한 프로토콜로 안전한 MIME 데이터를 주고받을 수 있는 방법을 제공한다[6]. 널리 대중적으로 쓰이는 Internet MIME 표준에 근거하여 S/MIME은 안전한 보안 서비스를 제공한다.

3. 전자 메일 시스템의 설계

3.1 키 교환 모델

공개된 통신로에서 암호 통신을 하기 위하여 둘 이상의 개체는 암·복호에 사용될 키를 사전에 공유하는 키 교환 과정을 수행하게 된다. 즉, 발신자와 수신자가 안전하게 메일을 주고받기 전에, 반드시 상호 키 교환이 필요하게 된다. 본 논문에서는 이러한 안전하게 키 교환을 하기 위해 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘을 이용한 키 교환 모델을 구현하였다. 이 모델은 타원 곡선상에서 이산 대수를 계산하는 난이도를 이용하여 안전한 키 교환을 지원하게 된다. 이러한 키 교환 과정을 구현한 모델은 다음의 그림 1과 같다[1].

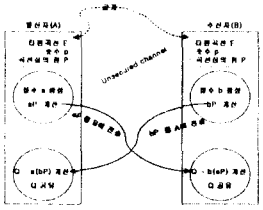

그림 1 ECDH 알고리즘을 이용한 키 교환모델

3.2 암호화 모델

발신자가 메시지를 암호화하여 생성하는 암호 메시지는 암호화된 세션키 부분, 암호화된 메시지 부분, 그리고 서명 부분으로 구성된다. 그림 2는 다음에 기술한 메시지 암호화 과정을 거쳐 암호 메시지를 생성하는 과정 및 구현 코드를 보여주고 있다.

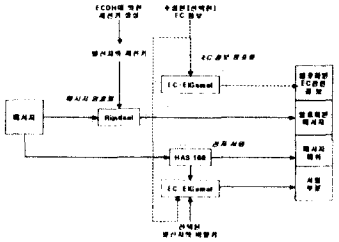

그림 2 Rijndael 알고리즘을 이용한 메시지 암호화 모델

우선, 메시지를 Rijndael 알고리즘을 사용해서 발신자의 세션키로 메시지를 암호화한다. 그리고 메시지 암호화에 사용된 Rijndael 세션키(또는 선택된 EC 정보)를 EC-ElGamal 알고리즘을 사용해서 암호화한다. 마지막으로, HAS160 알고리즘을 사용해서 메시지 다이제스트를 생성하고, 이 메시지 다이제스트를 ElGamal 알고리즘으로 암호화하여 전자 서명을 생성한다.

3.2.3 복호화 모델

수신된 암호 메시지는 메시지의 각 부분별로 복호화 및 서명을 증명하는 데, 그림 3은 이러한 과정을 보여주고 있다.

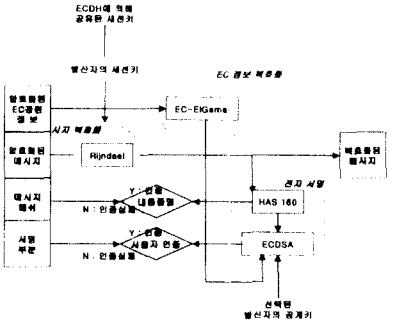

그림 3 Rijndael 알고리즘을 이용한 복호화 모델

우선, EC-ElGamal 알고리즘을 사용해서 Rijndael 세션키를 복호화한다. 그리고 Rijndael 알고리즘을 사용해서 복원된 Rijndael 세션키를 가지고 암호문을 복호화 한다. 끝으로, 복원된 평문 메시지를 HAS160 알고리즘을 사용해서 메시지 다이제스트로 변환하고, ECDSA[EC ElGamal] 알고리즘을 사용해 검증한다.

3.3.3 배달증명 모델

그림 4는 제안된 배달증명 방식을 기반으로 한 배달증명 모델을 통해서 의도된 수신자가 올바르게 메일 메시지를 수신하였음을 송신자에게 증명하는 과정을 보여주고 있다.

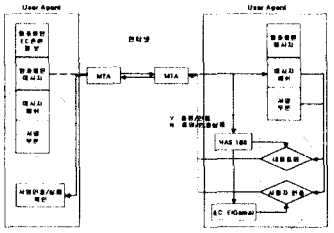

그림 4 암호화 알고리즘을 이용한 배달 증명 모델

발신자가 배달증명 서비스를 요청했을 때, 메시지 암호화와 동일한 과정으로 암호화된 세션키, 암호화된 메시지, 및 서명된 메시지로 구성된 암호 메시지를 생성하고, 이 메시지에 다음과 같이 배달증명을 요청하는 플래그를 함께 붙여서 수신자에게 송신한다. 그리고 수신자 쪽의 UA는 수신된 메시지에서 플래그를 확인하여 배달증명 요청 플래그가 있다면, 전자 서명을 증명하여 증명이 성공하면, 암호화된 메시지를 수신자의 비밀키를 사용하여 서명한 후에 발신자의 암호화된 메시지와 함께 처음 메시지를 송신한 발신자에게 회신한다. 발신자는 배달 증명 요구에 대한 회신 메시지임을 메시지에 삽입된 플래그를 통해서 확인하고, 메시지의 전자서명을 증명하여 의도된 수신자에게 메일이 올바르게 배달되었음을 확인한다. 이러한 절차를 통해서 향후에 발생할 수 있는 전자 메일 메시지의 수신에 대한 수신자의 부인을 방지할 수 있다.

4. 안전한 전자 메일 시스템의 구현

4.1 메시지 작성 및 송신

메시지를 작성하기 위해서는 시작 윈도우의 메뉴에서 메시지 작성 메뉴 혹은 버튼을 선택한다.

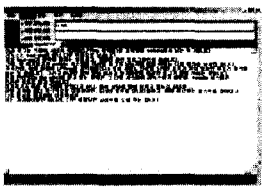

그림 5 메시지 작성

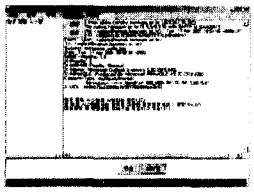

그림 6 메시지 암호화 및 서명

그림 5에서는 메시지 작성 윈도우의 메뉴 바에서 '보안 기능 사용' 메뉴와 '배달 증명 사용', 그리고 '내용 증명 사용' 메뉴를 선택하여 기본 보안 기능과 배달증명 서비스, 그리고 내용증명 서비스를 제공받을 수 있도록 설정하였다. 마지막으로 메시지 전송 버튼을 누르면 그림 6과 같이 메일 메시지의 암호화 및 서명 등의 과정을 거쳐 의도된 수신자에게 메시지를 전송한다.

4.2 메시지 수신 및 서명 증명

메시지를 수신한 수신자의 메일 프로그램은 배달 증명과 내용 증명을 요구하는 메시지임을 메시지 내의 플래그를 인지하여 확인하고, 서명을 증명하여 그림 7, 그림 8과 같이 서명이 올바르게 증명되었음을 다이얼로그 박스에 출력한다. 그리고 수신된 메시지 중에서 암호화된 메시지만을 서명하고 발신자의 암호화된 메시지와 함께 "Receipt:" 플래그와 "Content" 플래그를 메시지의 처음에 첨부하여 발신자에게 회신한다.

그림 7 수신된 메시지의 서명 증명

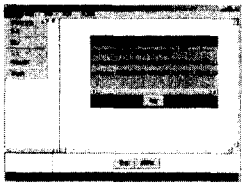

그림 8 회신된 메시지의 부인증명

4.3 메시지 회신 및 부인방지

회신 메시지를 수신한 발신자는 메시지에 붙어있는 두 플래그가 배달 증명과 내용 증명에 대한 회신 메시지를 나타냄을 확인한다. 그리고 수신된 메시지의 서명을 증명하여 배달증명과 내용 증명이 확인되었음을 나타내는 다이얼로그 박스를 그림 15와 같이 출력한다.

5. 비교 분석

본 논문에서 구현한 메일 시스템은 메시지 기밀성, 메시지 무결성, 송신자 인증, 송신자 부인 봉쇄 서비스 등을 제공하며, PGP와 PEM에서 아직까지 제공하지 않고 있는 배달증명 서비스를 제공한다. 표 1은 본 논문에서 구현한 메일 시스템과 PGP 및 PEM에서 제공하고 있는 정보보호 서비스에 대한 비교를 기술하고 있다.

표 1 PGP 및 PEM과 제안된 메일 시스템 비교

정보 보호 서비스	제안된 시스템	PGP	PEM
메시지 기밀성	제공함	제공함	제공함
메시지 무결성	제공함	제공함	제공함
송신자 인증	제공함	제공함	제공함
송신부인봉쇄	제공함	제공함	제공함
배달증명	제공함	제공하지 않음	제공하지 않음
내용증명	제공함	제공하지 않음	제공하지 않음

6. 결론

현재 네트워크 환경에서 널리 사용되고 있는 전자메일 시스템은 많은 보안상의 취약점에 노출되어 있다. 이러한 전자메일의 취약점을 극복하기 위해서 다양한 보안 메일 시스템들이 소개되고 있는 추세이지만 사용자에게 만족스런 서비스를 제공하지 못하고 있다. 본 논문에서는 기존의 메일 시스템에서 제공되는 기본 보안 서비스를 제공하며, 의도된 수신자가 메시지를 올바르게 수신하였음을 증명하는 배달증명 서비스와 내용이 변경되지 않았음을 증명하는 내용증명 서비스, 그리고 메시지 교환 이전에 안전하게 키를 교환하기 위한 키 교환 모델을 설계·구현하였다. 구현은 자바 암호 API를 기반으로 하였으며, 이를 포함한 자바 플랫폼은 네트워크 및 보안 서비스를 제공하는 데 필수적인 모든 요소들을 클래스로 갖추고 있기 때문에 개발자에게 프로그램의 작성을 용이하게 한다.

향후 보안 메일 시스템에서는 부인방지 서비스 및 안전한 키 교환 서비스를 제공하면서도, 기존의 시스템(암호화하지 않은 채, 메일을 전송하는 시스템)과 전송속도 차이가 나지 않는 전자 메일 시스템을 구현함으로써, 상호간에 신뢰하면서도 빠른 메일 서비스를 제공하는 방법을 모색해야 할 것이다.

참 고 문 헌

[1] 최용락, 소우영, 이재광, 이임영, "통신망 정보 보호", 그린출판사, 1995

[2] 조한진, 김봉한, 이재광, "정보보호 서비스를 위한 Secure E-mail 시스템 설계", 한남대학교 산업기술연구소, 1998

[3] 손진욱 편저, "Java 2 Programing Bible", 정보문화사, 1999

[4] 박춘식, "배달 및 내용 증명이 가능한 전자메일", 통신정보보호학회지, 제7권 제2호, 1997. 6.

[5] 강명희, "인터넷 메일 시스템에서의 정보 보호 서비스 구현", 광운대학교 전자계산학과 석사학위 논문, 1995

[6] 이재용, 이기수, 장춘서, "PGP를 이용한 WWW 메일 시스템의 설계 및 구현", 한국정보과학회 가을 학술발표논문집, 제24권 제 2호, 1997

[7] 홍주영, 윤이중, 김대호, "전자우편 시스템의 보호 방식 분석", 통신정보보호학회지 Vol.4 No.2, 1994. 6

[8] Jonathan Knudesen, "Java Cryptography", O' REILLY, 1998

[9] Sun Microsystems, "Java 2 SDK, Standard Edition Documentation", 1999

[10] Scott Oaks, "Java Security", O' REILLY, 1998

[11] Elliotte Rusty Harold, "Java Network Programing", O' REILLY, 1997

[12] Bruce Schneier, "Applied Cryptography", John Wiley & Sons Inc., 1996

[13] J.Zhou and D. Gollmann, "A Fair Non-repudiation Protocol", Proc. of the 1996 IEEE Symposium on Security and Privacy, 1996

[14] Stephen T. Kent,"Internet Privacy Enhanced Mail", CACM, Vol. 36, No. 3, 1993

[15] Stephen T. Kent,"An Overview of Internet Privacy Enhanced Mail", INET '93, June 1993

[16] N. Borenstein, "MIME(Multipurpose Internet Mail Extensions)" Part One: "Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, 1993