S/MIME 보안 메일 개발

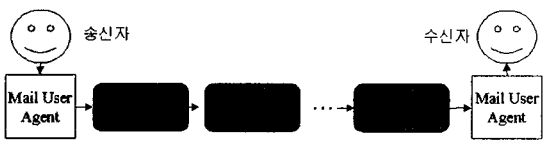
장 혜 진[1)]

목 차

1. 서 론

전자 메일은 완전히 대중화되었으며 가장 기본적인 인터넷 응용의 하나다. 하지만 전자 메일에 대한 보호 및 안전성 보장은 기대에 미치지 못하고 있는 실정이다. 인터넷에 대한 감청 및 모니터링 기술의 발전을 감안한다면 아무런 보안 장치가 되어있지 않은 전자 메일을 사용하는 것은 자신의 전자 메일을 모두에게 공개하는 것과 마찬가지라고 할 수 있다. 전자 우편의 불법 감청 및 변조는 일반 개인에게는 프라이버시 침해가 될 수 있으며, 기밀성을 요구하는 특정한 사용자에게는 심각한 위협이 될 수 있다.

이러한 위협으로부터 메일 사용자들을 보호하기 위해서는 메일의 송수신자의 신원을 확인할 수 있는 신원확인(authentication) 기술, 메일이 변조되거나 훼손되지 않고 전송되었음을 확인하기 위한 완전성(integrity) 보호기술, 메일의 내용에 대한 불법 감청이 불가능하도록 하는 기밀성(privacy) 보호 기술, 메일을 발송하거나 수신한 후에 발송하거나 수신하지 않았다고 부인하는 것을 방지하기 위한 부인 방지(Non-Repudiation) 기술 등의 보안 기술이 메일 시스템에 결합되는 것이 요구되고 있다[1].



(그림 1) 메일의 송수신 과정

위 (그림 1)은 메일의 일반적인 송수신 과정을 보여준다. 송신자가 메일 송신 클라이언트(MUA)를 통해 발송한 메일은 SMTP(Simple Mail Transfer Protocol) 서버와 같은 메일 전송 에이전트(MTA)들을 경유하여 수신자의 메일 전송 에이전트에 도착하게 되고 메일 송신 클라이언트(MUA)에 의해 읽혀져 수신자에게 보이게 된다. (그림 1)과 같은 방식 이외의 다양한 방식의 메일 시스템들이 존재한다. 예를 들어, 많은 웹 메일 시스템들이 메일 클라이언트의 부담을 줄이기 위하여 메일의 파싱(parsing) 및 처리의 대부분

1) 상명대학교 컴퓨터정보통신공학부 소프트웨어 전공 교수

을 서버가 담당하고 메일 송수신 클라이언트는 메일 서버가 파싱한 메일을 사용자에게 보여주는 기능만을 담당하는 방식을 사용한다. 또한, 송신자와 수신자간의 메일 전송의 확실성을 증가시키기 위하여 메일 전송 에이전트들의 릴레이(relay) 기능을 사용하지 않고 메일 클라이언트가 DNS (Domain Name System)의 NxLookup 기술[2]을 사용하여 메일 수신자의 메일 전송 에이전트의 주소를 알아내어 수신자의 메일 전송 에이전트로 직접 메일을 보내는 메일 시스템도 존재한다.

보안 메일은 메일의 송신자와 수신자간의 단대단(end-to-end) 보안을 보장해야 하므로, 송신자와 수신자의 메일 클라이언트에서 메일 내용의 암호화, 해독, 전자 서명, 서명 검증 등이 처리되어야 한다. 따라서 보안 메일 시스템에서는 메일 클라이언트의 역할이 중요하다.

2. 보안 메일 표준 규격

S/MIME(Secure Multipurpose Internet Mail Extension)은 보안 메일의 표준 규격이다. S/MIME의 규격은 RFC 2631, RFC 2632, RFC 2633, RFC 2634, RFC 2984, RFC 3369 등의 S/MIME 표준 규격 문서들에 의해 규정된다. S/MIME 규격은 MIME (Multipurpose Internet Mail Extension) 규격에 바탕을 두고 있고, MIME 규격을 이해하려면 먼저 RFC 822 규격[3]을 이해해야 한다. MIME 규격은 RFC 2045에서 RFC 2049까지의 표준 규격 문서들에 의해 규정된다.

RFC 822는 인터넷 기반의 텍스트 메일 메시지의 표준이다. RFC 822에 일치하는 메시지 구조는 매우 간단하다. 메시지는 복수개의 헤더(header)와 몸체(body) 쌍들로 구성된다. 헤더와 몸체 사이는 빈 줄로 구분된다. RFC 822 규격은 이진 파일을 수용할 수 없어 멀티미디어 파일이나 다양한 언어 코드를 수용이 어렵다는 등의 제약을 가지므로 RFC 822 규격에 호환하면서 동시에 알려진 제약점들을 해소하기 위하여 보다 확장된 규격인 MIME 규격이 제정되었다.

2.1 MIME

MIME은 텍스트, 이미지, 비디오, 오디오 등의 다양한 컨텐츠(content) 포맷을 정의하고, 멀티미디어 메일을 지원하는 표기들을 표준화한다. 또한 MIME은 메일 메시지의 전송 인코딩(transfer encoding) 방법들을 정의한다. 일반적으로 전자 메일은 다양한 종류의 환경을 거쳐서 배달된다. 따라서 배달 과정 중의 다양한 환경에 대응하여 메일이 깨지지 않고 배달되도록 하기 위해 MIME은 8bit, binary, quoted-printable, base64, x-token 등의 전송 인코딩 방법을 지원한다[4].

2.2 S/MIME

전자 우편에서의 정보 보호의 요구에 따라, 국내외에서 많은 연구가 진행되었다. 대표적인 보안 메일 규격에는 PEM(Privacy Enhanced Mail), PGP(Pretty Good privacy)[4], S/MIME 등이 있다. 국제 표준으로 PEM이 발표되었다. 하지만 PEM은 인터넷의 각 우편서버간의 메시지 비밀성과 인증만을 다루고 있고, 서버와 클라이언트간의 메시지 비밀성과 사용자 로깅(logging) 정보의 노출에 대해서는 다루고 있지 않다. PGP는 오랫동안 검증되었으며 보안성이 강하고 잘 설계된 규격이지만 표준 전자 인증서(certificate)의 사용을 지원하고 않는다는 문제가 있으므로 S/MIME이 상업용 및 기관용 산업 표준이 되어가고 있다. 참고로 OpenPGP(RFC 2440)[5]는 전자 인증서의 사용을 지원하는 PGP의 변형이라 할 수 있다. RFC 3369는 S/MIME 버전 3에서 지원하는 암호화된 메시지 문법을 규정한다.

RFC 3369는 RFC 2630을 대치하였다. RFC 3369에 따르면 S/MIME은 다음 〈표 1〉과 같은 종류의 컨텐츠 타입들을 지원한다.

〈표 1〉 S/MIME 버전 3의 컨텐츠 타입들

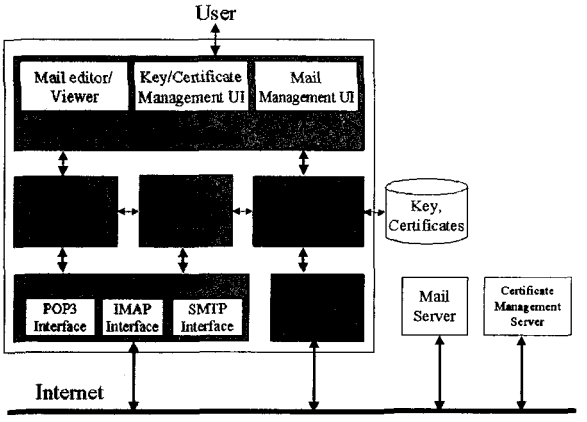
data	data 컨텐츠 타입은 ASCII 텍스트 파일과 같은 임의의 옥텟(octet) 문자열들을 나타내고 해석은 응용 프로그램에게 맡겨진다.
signed-data	signed-data 컨텐츠 타입은 임의의 타입의 컨텐츠와 0개 이상의 서명값들로 구성된다. 임의의 타입의 컨텐츠에 대하여 복수의 서명자가 병렬적으로 서명할 수 있다.
enveloped-data	enveloped-data 컨텐츠 타입은 암호화된 임의의 타입의 컨텐츠와 한명 이상의 수신자들에 대한 암호화된 컨텐츠 암호화 키들로 구성된다. 암호화된 컨텐츠와 그것의 수신자에 대한 암호화된 컨텐츠 암호키의 조합을 그 수신자에 대한 전자 봉함(digital envelop)이라 한다. 어떤 타입의 컨텐츠도 임의의 수의 수신자들에 대한 전자 봉함이 될 수 있다.
digested-data	digested-data 컨텐츠 타입은 임의의 타입의 컨텐츠와 그 컨텐츠에 대한 축약(digest)으로 구성된다. digested-data 컨텐츠 타입은 컨텐츠의 완전성(integrity)을 보장하는 데 사용되며, digested-data 타입의 컨텐츠는 일반적으로 enveloped-data 컨텐츠 타입의 입력이 된다.
encrypted-data	encrypted-data 컨텐츠 타입은 임의의 타입의 컨텐츠의 암호화 결과를 의미한다. encrypted-data 컨텐츠 타입은 enveloped-data 컨텐츠 타입과 달리 수신자나 암호화된 컨텐츠 암호 카들을 갖지 않는다. encrypted-data의 키는 enveloped-data 컨텐츠에서와 다른 방식으로 관리되어야 한다.
authenticated-data	authenticated-data 컨텐츠 타입은 임의의 타입의 컨텐츠와 그 컨텐츠에 대한 MAC(Message authentication code), 그리고 하나 또는 그 이상의 수신자에 대한 암호화된 인증키들(authentication keys)로 구성된다.

2.3 국내의 보안 메일 표준 규격

국내의 보안 메일 표준 규격은 2001년도에 인터넷 보안 기술 포럼에서 초안이 작성되었다. SEED와 같은 국내 표준 암호 알고리즘의 수용 방법에 대한 많은 논의가 있었지만 보안 메일의 국제적인 호환을 위하여 국내의 보안 메일 규격은 S/MIME 버전 3의 규격을 거의 그대로 준수하고 있다.

3. 보안 메일 시스템의 구조

메일 시스템들은 일반적으로 메일 편집, 메일 관리 등의 사용자 인터페이스를 가지며, MIME 메시지 파싱 및 조합 등의 처리를 위한 내부 모듈들과 POP3, SMTP 등의 메일 서버들에 대한 인터페이스를 갖는다. 웹 메일과 같이 보안성을 갖지 않은 일반적인 메일 시스템에서는 메일의 파싱이나 분석과 같은 메일 클라이언트의 중요 기능들을 필요에 따라 메일 서버 쪽에서 수행되도록 하여 메일 클라이언트를 가볍게 구현하는 것이 용이하다. 하지만, 보안 메일에서는 송신자와 수신자간의 단대단 보안을 지원하기 위하여 메일 클라이언트가 메일의 암호화, 해독, 서명, 서명 검증 등의 여러 가지 기능을 수행해야만 하므로 메일 클라이언트 쪽에 많은 컴퓨팅 파워가 요구된다.



(그림 2) 보안 메일 시스템의 구조

위 (그림 2)는 보안 메일 시스템의 구조의 예를

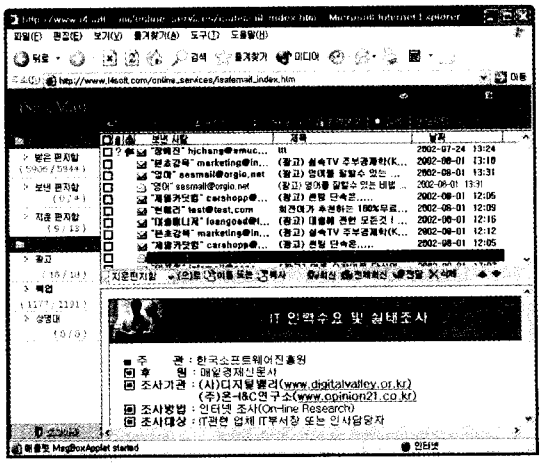
보인다. 보안 메일 시스템에서 메일 클라이언트는 일반 메일 시스템에서와 달리, S/MIME 메시지 처리 모듈, 키/인증서의 관리 모듈, 인증서 발행 및 검증을 위한 인증서 서버와의 인터페이스 모듈 등의 보안과 관련된 모듈들을 갖는다. 암호화되거나 전자 서명된 메시지는 S/MIME 메시지 처리 모듈에서 MIME 메시지로 해독되고 검증된다.

4. 보안 메일 개발 사례

iSafeMail은 송신자와 수신자간의 인증서 기반의 단대단 보안 기능을 제공하기 위하여 국내에서 제작된 보안 웹 메일 시스템의 이름이다. iSafeMail은 마이크로소프트의 IIS(Internet Information Server)나 Apache 웹 서버와 같은 일반적인 웹 서버를 사용한다. 메일 서버로는 표준 SMTP 서버를 사용한다. 메일 클라이언트는 웹 브라우저 상에서 동작하며, 암호화, 암호 해독, 전자 서명, 서명 검증 등의 보안 기능 및 MIME 메시지 처리 기능들을 서명된 자바 애플릿 및 서명된 ActiveX 콤포넌트들을 이용하여 구현하고 있다. 또한 iSafeMail은 X.509 규격의 전자 인증서를 사용하며 키/인증서 관리 기능을 갖고 있다. iSafeMail은 보안 메일의 기능과 메일 일반 기능을 잘 결합하도록 설계되었다. iSafeMail은 기밀성, 완전성, 신원 확인, 부인 방지 등의 보안 기능 이외에 다음과 같은 메일 시스템으로서의 특징을 갖는다.

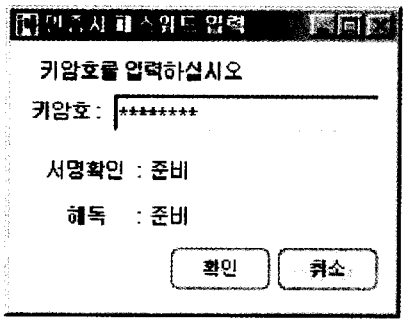
(1) 웹 브라우저와 인터넷이 연결된 어디서나 사용할 수 있다. 이동하여 보안 메일을 사용할 수 있다.
(2) 사용하기 쉽고 편리하며 직관적인 웹 기반 그래픽 사용자 인터페이스가 제공된다.
(3) 웹 브라우저를 통해 온라인상에서 즉시 사용자 가입 및 메일 클라이언트 설치가 이루어질 수 있다.
(4) 보안 메일을 위하여 새로운 메일 계정을 받지 않아도 된다. 즉, 기존 메일 서버 (POP3 서버, SMTP 서버)들의 메일 계정을 그대로 사용하여 보안 메일을 송수신할 수 있다.
(5) 복수개의 수신 메일 서버(POP3 서버)를 통합하여 메일을 수신할 수 있다.
(6) 보안 메일을 위한 특별한 H/W나 운영 체계를 필요로 하지 않는다. 범용 웹 브라우저, 범용 웹 서버, 표준 메일 서버(POP3 및 SMTP)를 사용한다.
(7) iSafeMail 시스템은 Windows, Linux, Unix, Solaris 등의 다양한 플랫폼의 서버를 지원하며, 서버의 부담을 최소화하는 구조로 설계되어 작은 용량의 서버로 많은 사용자 메일을 효과적으로 처리할 수 있다.
(8) 동적 버전 컨트롤(dynamic version control) 기술을 사용하여 메일 클라이언트 프로그램의 업그레이드가 접속할 때마다 자동으로 이루어진다.

다음 (그림 3)은 iSafeMail의 초기 화면이다. iSafeMail의 사용자 인터페이스는 일반 메일의 사용자 인터페이스와 유사하다. 보안 메일 시스템은 보안 메일뿐 아니라 일반 평문 메일도 처리하여야 하기 때문이다.



(그림 3) iSafeMail의 초기 화면

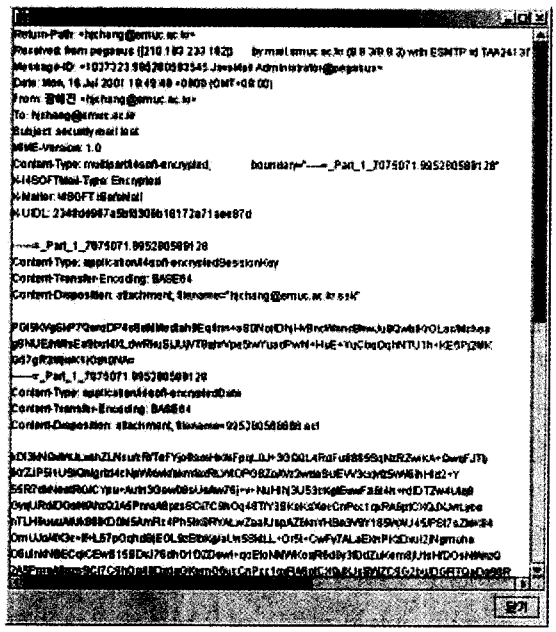
암호화되거나 서명된 보안 메일에는 자물쇠 아이콘 또는 서명 아이콘이 표시되며, 보안 메일을 클릭하면 사용자의 키 패스워드를 묻는 다이얼로그 창이 나타난다. 사용자가 올바른 키 패스워드(key password)를 입력하면 그 키 패스워드를 PBE(Password Based Encryption)[6] 암호키로 이용하여 메일 클라이언트가 관리하는 암호화된 키보관소(keystore)에 저장된 키를 해독하고, 그 해독된 키를 이용하여 메일 해독 및 전자 서명 검증을 수행한다. 메일의 암호화 및 전자 서명 과정에서도 보관소에 저장된 키와 인증서가 사용된다. 키 패스워드는 키 암호키(key encryption key)다. 다음 (그림 4)는 키보관소에 대한 키 패스워드를 사용자에게 묻는 다이얼로그 화면이다.



(그림 4) 키 패스워드 입력 다이얼로그 윈도우

다음 (그림 5)는 암호화된 보안 메일의 원문(source)의 예를 보여준다. 보안 메일은 메일 클라이언트에서 암호화되고 전자 서명되고, 해독되고, 서명 검증되므로 보안 메일을 불법 감청한다면 (그림 5)와 같이 기밀성을 갖는 내용을 보게 된다. 보안 메일을 불법으로 수정하거나 훼손하면 전자 서명 검증에서 오류 메시지가 발생하므로 메일의 완전성이 보장된다.

iSafeMail은 일반적인 메일 시스템으로서의 기본 기능들을 제공하며, S/MIME 기반의 보안 메일 기능을 제공한다. iSafeMail 만의 특징으로서는 기본적으로 단대단 보안을 제공하지만 자체적인 그룹키 기술을 사용하여 그룹용 버전의 경우 그룹 외부로 발송되는 보안 메일의 내용에 대한 모니터링이 가능하다. 단 모니터링 권한은 허용된 관리자에게만 주어진다. 모니터링 기능은 S/MIME의 규격과는 관련이 없다.



(그림 5) 보안 메일의 원문

5. 결 론

S/MIME 규격은 매우 방대한 규격이며 그 규격들을 모두 구현하는 것은 쉽지 않은 일이다. 하지만 S/MIME 규격에 맞는 보안 메일 시스템을 개발하는 것은 매우 중요하다. 점차 메일 시스템에서의 보안이 중요한 문제가 될 것이며 S/MIME은 제작자가 서로 다른 보안 메일 시스템들 간에 호환성을 보장할 수 있는 표준 규격이기 때문이다.

참고 문헌

[1] R. Kaufman, R. Perlman, M. Speciner, Network Security, Prentice Hall, pp. 329-353. 1995.

[2] Kevin Johnson, Internet Email Protocols: A Developer's Guide, Addison-Wesley, 2000.

[3] David H. Crocker, RFC 822: Standard For The Format of ARPA Internet Text Messages, IETF Working Group, Aug. 1982.

[4] William Stallings, Cryptography And Network Security, 2nd Edition, Prentice Hall, pp 355-391, 1999.

[5] OpenPGP Alliance, http://www.openpgp.org.

[6] Mohan Atreya, "Password Based Encryption", http://www.rsasecurity.com

저자약력

장 혜 진

1985년 서울대학교 사범대학 수학교육과(이학사)

1987년 서울대학교 자연과학대학 계산통계학과 전산학 전공 (이학 석사)

1987년 - 1989년: 한국전자통신연구소 근무

1994년 서울대학교 계산통계학과 (이학박사)

1994년 - 현재 상명대학교 공과대학 컴퓨터정보통신공학부 소프트웨어전공 교수

연구 분야: 분산 에이전트 시스템, 통신 보안 시스템, DRM 시스템