通信情報保護學會誌
第4卷 第2號, 1994. 6

전자 우편 시스템의 보호 방식 분석

홍 주 영*, 윤 이 중**, 김 대 호***

요 약

전자 우편 시스템은 컴퓨터와 네트워크를 이용하는 이용자들이 가장 빈번히 사용하고 있는 서비스 중의 하나로서 그 이용률은 매년 급증하고 있으며 이와 더불어 교류되는 정보에 대한 보호 및 안전성에 대한 요구도 제기되고 있다.

본 고에서는 이러한 전자 우편 시스템에 보호 서비스를 제공하기 위한 여러 제안된 방식들중에 X.400 MHS과 Internet의 PEM(Privacy Enhanced Mail), 미국의 SDNS MSP(Message Secure Protocol)에 관하여 각각의 보호 서비스 제공 방식과 보호 서비스의 유형, 범위, 특성들을 논의하며 이들 접근 방식간의 관련성과 차이점들을 분석하고자 한다.

1. 개 요

컴퓨터와 네트워크를 이용한 전자 우편 시스템은 네트워크의 이용자들이 가장 빈번히 사용하고 있는 서비스중의 하나로서 개인간의 서신 교환이나 공고, 안내문의 배포, 기술적인 정보 교류 등은 물론 기업간의 공식적인 문서 교환에 이르기까지 다양한 용도로 이용되고 있다. 전자 우편시스템의 이용률은 매년 급증하고 있으며 교류되는 정보에 대한 보호 및 안전성에 대한 요구도 높아지고 있다.

메세지의 부당한 노출은 일반 개인에게는 프라이버시 침해가 될 수 있으며 비밀성을 요구하는 사용자들의 입장에서는 심각한 위협이 될 수 있다. 또한 메세지가 전송도중 변경되거나 송신자가 자기의 신원을 허위로 조작하여 발신하는 것, 송수신 행위를 부정하는 등의 일들을 방지하는 것이 공식적인 메세지 교류환경에서는 더욱 중요한 문제가 되었다. 건전한 메세지 교류를 해치는 이러한 위협들에 대처하기 위해 메세지 발신자의 신원에 대한 진위를 확신시켜줄 수 있는 인증 기술과 오류없이 안전하게 보호되어 전송되었음을 확인하는 방법, 송수신 사실 여부에 대한 증거 확보등 신뢰성있는 정보 교류 서비스를 제공하기 위한 보호 서비스들이 연구되고 있으며 안전한 전자 우편 시스템 개발을 위한 여러가지 방식들이 제안되고 있다[1][2]. 이러한 시도들은 TCP/IP 프로토콜을 사용하는 Internet과 OSI프로토콜을 사용하는 MHS(Message Handling System)의 두 대표적인 전자 우편 아키텍춰 환경에서 각각 논의되고 있다[3][4].

* 정회원, 한국전자통신연구소 연구원
** 정회원, 한국전자통신연구소 선임연구원
*** 정회원, 한국전자통신연구소 책임연구원

본고에서는 X.400 MHS의 보호서비스와 Internet의 PEM(Privacy Enhanced Mail), 미국의 SDNS MSP(Message Secure Protocol)에서의 보호 서비스 제공 방식과 보호 서비스의 유형, 범위, 특성들을 논의하며 이들 접근 방식간의 관련성과 차이점들을 분석하고자 한다.

2. X.400 MHS 보호 서비스

MHS 표준화 작업은 CCITT에서 시작하여 1984년 X.400을 발표하였다. 그후 CCITT와 ISO/IEC의 공동 작업을 통하여 1988년 수정된 X.400과 ISO/IEC 10021(MOTIS : Message Oriented Text Interchange System)이 발표되었는데 1984년에 발표된 문서와의 큰 차이점은 정보보호 서비스를 포함시킨 것이다. 1990년에 EDI(Electronic Document Interchange)와 그에 관련된 보호 서비스가 추가되어 1992년에 개정 발표되었다[5].

2.1 MHS 모델

MHS는 OSI 통신 시스템을 이용하여 사용자 사이에 다양한 종류의 정보를 상호 교환할 수 있게 해 주는 시스템이다. 이 시스템은 그림 1에서처럼 UA(User Agent), MS(Message store), AU(Access Unit)와 MTA(Message Transfer Agent)로 이루어진 MTS(Message Transfer System)의 다섯개 객체들로 이루어 진다.

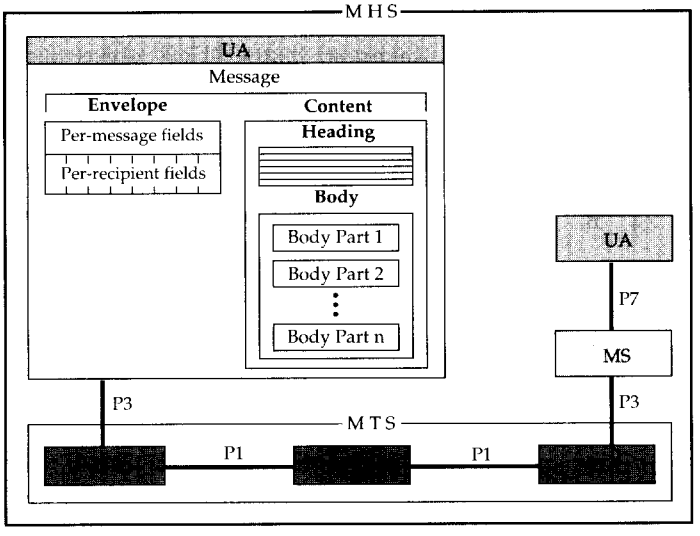


그림 1 MHS 모델

UA는 MTS또는 MS에 연결되어 사용자의 메세지의 작성, 제출, 수신등의 작업을 제공한다. MS는 메세지를 저장해 놓는 역할을 담당하는데 이는 UA가 항상 동작 상태가 아닌 경우 즉 UA가 PC에 탑재된 경우에 필요한 객체다. AU는 non-MHS 시스템과의 연계를 담당하는 객체로 MTA와 동일 시스템에 위치한다. MTA는 UA, MS, AU 등과 접속되어 메세지의 전송을 담당하는 객체다.

MHS가 처리하는 메세지는 현재 EDI, IPM(InterPersonal Message) 두가지가 표준화되어 있다. IPM의 구조를 살펴보면 MTS가 데이타를 전달하는데 필요한 정보로 구성된 봉투(envelope)와

송수신자가 전달하고자 하는 데이타를 나타내는 내용물(content)의 두 부분으로 나누어 진다.

봉투는 모든 수신자에게 공통으로 적용되는 정보로 구성된 메세지 필드(per message fields)와 각 수신자마다 달리 적용되는 정보로 구성된 수신자별 필드(per recipient fields)의 두가지로 나누어 진다. 내용물은 다시 내용물 형태를 정의한 정보로 구성된 헤딩과 여러 개의 바디들로 이루어 진다. 각각의 바디는 음성, 팩시밀, 텍스트 등의 다양한 데이타를 포함할 수 있다.

MHS를 구성하는 각 객체들 사이의 통신을 위하여 필요한 프로토콜은 MTA 사이의 통신을 위한 P1, UA 또는 MS가 MTA에 접근하기 위한 P3, UA와 MS 사이의 P7 세가지가 표준화되어 있다[16,17].

2.2 MHS 정보보호 서비스

MHS 환경에서 제공되는 정보보호 서비스는 18개가 있고 이들은 각각의 특성에 따라서 아래와 같이 다섯개의 부류로 나눌 수 있다.

2.2.1 단대단(end-to-end)서비스

이 서비스들의 특징은 하부 MTS의 신뢰성에 영향을 받지 않고 정보보호 서비스를 데이타의 송수신자에게 제공한다.

- 메세지 발신처 신분인증(message origin authentication : end-to-end): 메세지의 수신자에게 메세지의 발신자를 확인시켜준다. 이 서비스는 내용물 무결성 서비스와 함께 제공되어야 효과적이다.
- 배달 증명(proof of delivery): 메세지의 송신자에게 메세지가 변형없이 의도한 수신자에게 전달되었음을 확인시켜 준다.
- 내용물 무결성(content confidentiality): 송수신자 사이에서 발생할 수 있는 메세지의 누출을 막아준다.
- 내용물 무결성(content integrity): 송수신자 사이에서 발생할 수 있는 메세지의 변경을 막아준다.
- 메세지 순서 무결성(message sequence integrity): 메세지 순서의 변경, 삭제, 재송신 등을 막아준다.

2.2.2 메세지 경로(message path)서비스

이 서비스들의 특징은 MHS를 구성하는 모든 객체 사이의 안전한 통신을 제공한다는 것이다.

- 대등 실체 신분인증(peer-entity authentication): 통신이 설정된 상대방 객체의 신원을 확인하는데 사용된다.
- 메세지 정보보호 레이블링(message security labeling): 메세지에 그 메세지의 비밀 수준과 권한 영역을 표시하는 정보보호 레이블을 할당한다. 이 정보보호 레이블은 MHS의 보안 정책을 실현하는데 사용된다.
- 메세지 전달 제어(security context): MHS를 구성하는 객체들 사이에 전달될 수 있는 정보보호 레이블의 집합을 정하는데 사용된다. 메세지 정보보호 레이블링과 메세지 전달 제어 서비스를 이용하여 MHS의 강제적 또는 규칙 중심의 접근 제어 정책을 실현한다.

2.2.3 MTS 확인(MTS corroborative)서비스

이들은 MTS와 메세지 발신자 사이에서 제공되는 서비스들이다.

- 메세지 발신처 신분인증(message origin authentication : MTS): MTA에게 메세지의 발신자를 확인시켜 준다. 단대단 메세

지 발신처 신분인증과 유사하지만 여기서는 메세지에 할당된 정보보호 레이블의 무결성과 그 레이블을 할당한 곳을 검사한다는 점에서 차이가 있다.

- 조사 메세지 발신처 신분인증(probe origin authentication): MTA에게 조사 메세지의 발신자를 확인시켜 준다.
- 리포트 발신처 신분인증(report origin authentication): 발신자 또는 전달(relay) MTA에게 배달 또는 배달 불가 보고서를 작성한 송신자를 확인시켜 준다.
- 제출 증명(proof of submission): 메세지의 발신자에게 이 메세지를 발신 MTA가 접수했음을 확인시켜준다. 사설 UA가 공용 MHS 네트워크에 접속된 경우 유용한 서비스다.

2.2.4 부인 봉쇄(non-repudiation)서비스

- 발신처 부인 봉쇄(non-repudiation of origin): 메세지 수신자에게 메세지 발신자에 대한 증거를 제공한다.
- 배달 부인 봉쇄(non-repudiation of delivery): 메세지 발신자에게 메세지가 변경없이 수신자에 전달되었다는 증거를 제공한다.
- 제출 부인 봉쇄(non-repudiation of submission): 메세지 발신자에게 발신 MTA가 그 메세지를 접수했다는 증거를 제공한다.

2.2.5 정보보호 관리(security management) 서비스

- 신원증명 변경(change credentials): MHS를 구성하는 객체들이 자신의 패스워드, 공개키 등을 변경할 수 있는 기능을 제공한다.
- 등록(register): UA가 MTA에게 자신이 허용하는 보호 레이블의 집합을 지정할 수 있게 한다.
- MS-등록(MS-register): UA가 MS에게 자신이 허용하는 보호 레이블의 집합을 지정할 수 있게 한다.

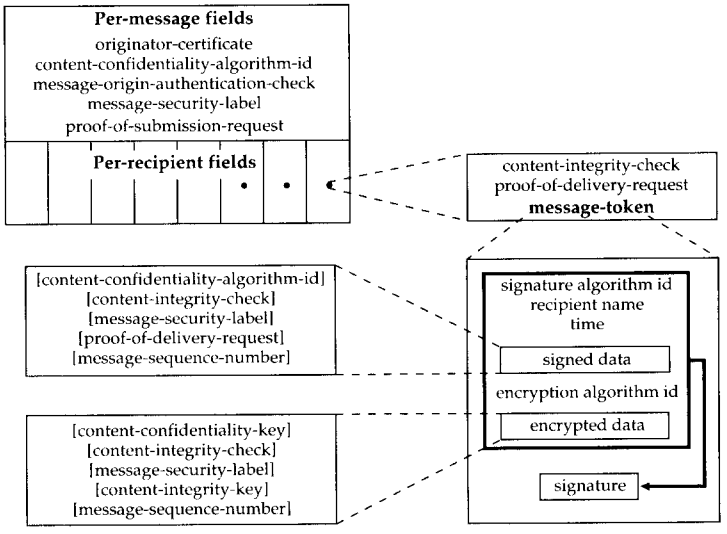


그림 2 정보보호 서비스 관련 파라메타와 메세지 토큰 구조

MHS 정보보호 서비스를 제공하기 위해 사용되는 메카니즘은 ISO/IEC 9594-2에 정의되어 있는 신분인증 프레임워크를 기반으로 한다. 이 메카니즘은 매우 간단하다. 메세지 발신처 신분인증 서비스를 예를 들어 이 메카니즘을 설명하면 다음과 같다. 각각의 MHS사용자는 각자 비밀키를 가지고 있고 UA-a라는 사용자가 UA-b라는 사용자에게 메세지를 송신하는 경우 UA-a는 해쉬 함수와 UA-a의 비밀 키로 암호 함수를 이용하여 서명을 만든다. UA-a는 서명과 메세지를 UA-b에게 보낸다. UA-b는 수신 메세지에 동일 해쉬 함수를 적용하고 UA-a의 공개 키를 이용하여 UA-a의 서명을 복화하여 이들을 비교하여 동일한 경우 UA-b는 수신 메세지가 UA-a로 부터 온 것임을 확신할 수 있다.

이들 정보보호 서비스를 제공하기 위해서 필요한 관련 파라메타들이 봉투의 메세지 필드와 수신자별 필드에 위치한다. 특히 수신자별 필드에는 파라메타에 비밀성과 무결성 서비스를 제공하기 위해 그림 2에서 보이는 것과 같은 메세지 토큰 구조를 정의했다[6][8].

2.3 MHS 정보보호 서비스 프로화일

MHS 표준은 많은 부분을 구현자의 선택 사항으로 정의해 놓았다. 이러한 이유로 북미 OIW (The Open Systems Environment Implementors' Workshop)와 유럽의 EWOS(European Workshop on Open Systems)에서 다음과 같은 MHS 보호 프로화일을 정의 채택하였다. 각 프로화일의 특성은 다음과 같이 정의되어 있으며 MHS에서 정보보호 서비스 구현시 각 환경에 따라 요구되는 서비스를 선택도록 권고한다[6][31].

- Class SO : 데이타 비밀성을 제외한 단대단 서비스
- Class SOA : Class SO에 데이타 비밀성 서비스 추가
- Class S1 : Class SO에 메세지 경로 서비스와 정보보호 관리 서비스 추가
- Class S1A : Class S1에 데이타 비밀성 서비스 추가
- Class S2 : Class S1 MTS확인 서비스와 부인 봉쇄 서비스 추가
- Class S2A : Class S2에 데이타 비밀성 서비스 추가

3. Privacy Enhanced Mail(PEM)

TCP/IP 프로토콜을 사용하는 거대 네트워크인 Internet의 IAB(Internet Architecture Boaud)산하에는 인터네트의 각종 기술 지원 및 연구 개발을 담당하는 두 기구(IRTF, IETF)가 있다. PEM은 IETF(Internet Enginneering Task Force)내의 보호분야(Security Area)의 작업 그룹들 중에 하나로 Internet 전자 우편 프로토콜인 RFC 822를 사용하여 전송되는 전자 우편에 보호 서비스를 제공하기 위한 Internet 표준 문서들을 발표하였다[12].

PEM을 정의한 4개의 연속물로된 문서들은 다음과 같다.

- RFC 1421 : Privacy Enhancement for Internet Electronics Mail : Part Ⅰ : Message Encryption and Authentication Procedures
- RFC 1422 : Privacy Enhancement for Internet Electronics Mail : Part Ⅱ : Certificate Based Key Management
- RFC 1423 : Privacy Enhancement for Internet Electronics Mail : Part Ⅲ : Algorithms, Modes, and Identifiers
- RFC 1424 : Privacy Enhancement for Internet Electronics Mail : Part Ⅳ :

Key Certification and Related Services

각 문서들은 암호 기법을 토대로 한 메세지 암호화와 인증 프로토콜의 확장과 처리 절차, 공개키 인증(certificate)을 이용하는 키 관리 구조와 하부 구조에 대해 기술하고 있다.

PEM은 메세지의 암호화에는 대칭적 암호 기법(DES)을 키 분배 방식에서는 비대칭적 암호기법(RSA)을 권고한다 이는 비대칭적 키 분배 방식은 안전하게 키를 공유할 방법이 없는 Internet의 광범위한 규모와 관리의 비균일성이라는 환경적 특성등을 고려할때 보다 적절하기 때문이다. PEM이 채택한 표준 양식은 CCITT X.509(Directory Authentication Framework)권고안을 따르는 프로화일이다.

3.1 PEM 동작 환경

Internet의 전자 우편환경을 X.400표준의 UA, MTA와 대비하여 살펴보면 RFC822 메세지 처리를 구현한 프로세스, 예를 들면 Ucb-mail, Elm등이 UA 역할을 하는 것이며 메세지의 전송과 릴레이 역할을 하는 SMTP(Simple Mail Transfer Protocol)가 MTA에 해당한다.

PEM은 기존의 전자 우편 환경과의 호환성(compatibility)을 최대화 하기 위해 MTA에 변경을 주지 않는 방식으로 서비스를 제공하도록 설계되었다. 즉, 기존의 전자 우편 전송을 위한 하부 구조가 그대로 PEM 메세지를 전송할 수 있도록 한다.

PEM을 구현시 UA에게도 투명성을 제공하도록 필터(filter)방식과 UA내에 PEM처리 기능을 통합시키는 두가지 방식이 있다[10]. 이때 전자의 경우 어떤 UA를 사용하느냐에 독립적으로 PEM 서비스를 사용할 수 있는 반면 사용자가 명시적으로 필터를 수행시켜야 하므로 후자에 비해 사용자의 입장에서 다소 번거로운 방식이 될 수 있다.

그림 3은 PEM의 동작 환경을 보인 것으로 송신측 UA는 필터 방식을 수신측 UA는 통합 방식을 사용한 예이다.

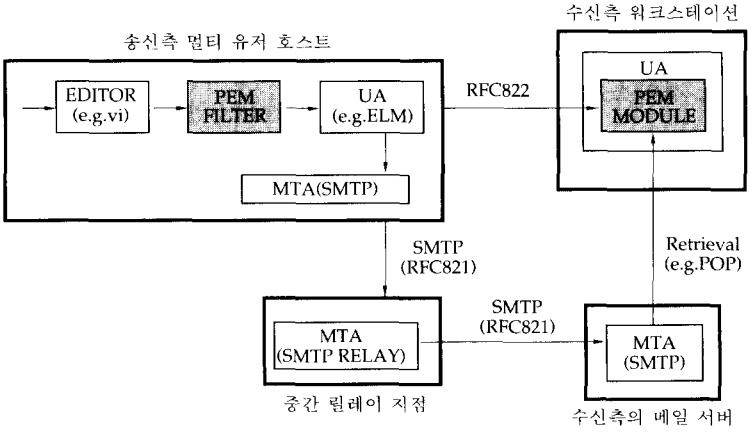


그림 3 PEM 동작 환경

3.2 PEM 보호 서비스

PEM은 다음 4가지 보호 서비스를 제공하며 자료 비밀성은 선택 사항이고 발신처 부인 봉쇄 서비스는 공개키 시스템을 기반으로 한 신분 인증 기법이 사용된 경우 제공될 수 있다[11].

- 무결성(Integrity)
- 데이타 발신처 신분 인증(data-origin

authentication)

- 비밀성(confidentiality): 선택 사항
- 발신처 부인 봉쇄(non-repudiation of origin): 공개키 시스템을 기반으로한 신분 인증 기법이 사용된 경우

보호 서비스를 구현하기 위해 PEM프로토콜의 절차는 MHS의 경우와 절차상 유사하다. 먼저 Message Digest를 계산하고, 이를 송신자의 비밀키를 이용하여 암호화 시킨다. 이것은 송신자를 식별하기 위한 정보임과 동시에 메세지에 대한 전자 서명으로써 제공된다. 비밀성을 제공하는 경우, 랜덤(random) DES를 생성시켜 이를 이용하여 메세지를 암호화한다. 메세지가 암호화되면 DES키는 수신자의 공개키로 암호화한 후 메세지에 포함시켜 전송한다.

그런데 이러한 보호 서비스를 위한 PEM 처리 작업은 여러 게이트웨어를 거치면서 발생할 수 있는 코드 변환 문제를 해결하기 위해 다음과 같은 일련의 제출 처리(Submission Processing)절차가 수행되어야 한다.

- step 1 : "SMTP" 표준 표현으로 변환(canonicalization)

메세지의 내용을 네트워크 표준 표현 방식으로 변환한다. PEM 무결성 서비스 처리 이후에 메세지에 어떤 변경이 발생한다면 수신측의 무결성 검증 결과가 올바로 나올 수 없으므로 이러한 변환은 정규 e-mail처리 이전에 이루어져야 한다.

- step 2 : PEM 보호 서비스 처리(MIC 계산과 암호화 등)
- step 3 : 6비트 엔코딩(Printable encoding and line length limiting)

3.3 PEM 서비스 유형

PEM은 제공하는 서비스 조합에 따라 세가지 유형의 PEM 메세지들을 정의하고 있다[3][11].

- MIC-clear

무결성과 신분 인증 서비스를 제공하며 이를 위한 MIC(Message Integrity Code)를 사용한다. 비밀성 서비스는 제공하지 않고 엔코딩 절차가 생략되므로 PEM을 구현하지 않은 수신측에서 볼수 있도록 해준다. 즉, PEM 사용자와 non-PEN 사용자들이 섞여 있는 메일링 목록에 메세지를 전송할 수 있으며 누구든 읽을 수 있으나 PEM 사용자들만이 메세지에 대한 무결성과 신분 인증성을 검증할 수 있다.

- MIC-only

MIC-CLEAR와 동일한 서비스를 제공하나, 선택적인 엔코딩을 제공한다. PEM 처리가 된 메세지가 다양한 e-mail 게이트웨이를 거칠때 무결성과 신분 인증성 처리 결과를 잘못되게 하는(invalidate)형태로 변환되지 않고 통과될 수 있도록 도와 준다.

- Encrypted

무결성, 신분 인증성, 비밀성, 발신처 부인 봉쇄(단, 공개키 기반의 인증 기법이 적용되는 경우에 한하여)가 제공된다. MIC-only와 마찬가지로 엔코딩 변환을 사용한다. 그렇지 않으면 binary로 만들어지는 암호 처리 결과가 binary가 아닌 텍스트 전송용으로 되어 있는 많은 e-mail 시스템들을 거쳐갈 수 없다.

선택적인 처리 절차의 여부를 PEM메세지 헤더 첫부분(Proc-Type)에 알려준다. Step 2,3에서 처리되어 필요한 정보 및 처리 결과 데이타들은 이후에 PEM 헤더부분에 모여진다. PEM의 메세지 형식은 그림 4에 보인다. 기존의 전자 우편의 헤더와 메세지 부분에서 메세지 부분이 다시 PEM을 위한 헤더와 실제 메세지 영역으로 나뉘어 전송되는 것이다.

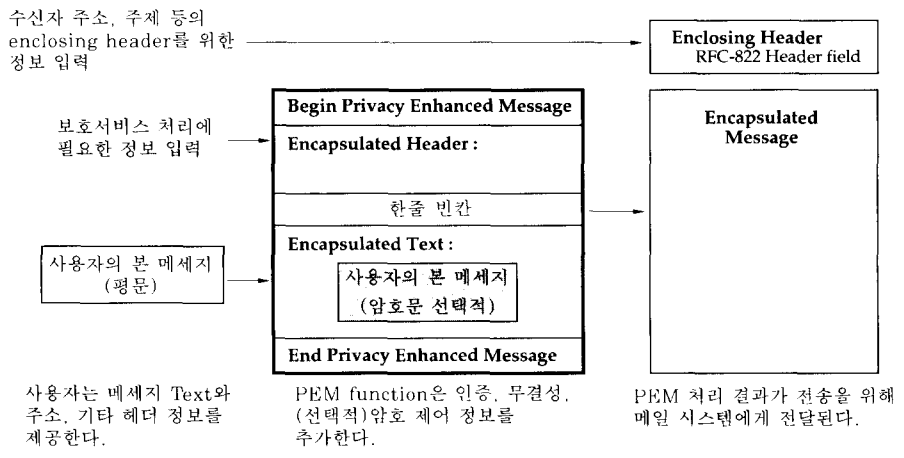


그림 4 PEM 메세지 형식

3.4 PEM 메세지 수신 처리

수신측에서는 PEM S/W가 먼저 PEM 메세지를 검사하여 PEM 메세지의 경계점을 찾고 헤더를 분석하여 PEM 버젼과 메세지 유형을 확인하여 수신측에서 해야할 처리 절차를 결정한다.

3.4.1 디코딩과 복호화

PEM 메세지 타입이 "Encrypted"와 "MIC-only"인 경우 수신측은 발신자에 엔코딩의 역절차를 통해 암호문 혹은 표준 표현 형식의 평문 형태로 돌려 놓는다. "Encrypted"인 경우 수신자는 PEM 헤더를 조사하여 그를 유일하게 식별하는 Recipient-ID-Asymmetric 필드를 찾아낸다. Key-Info에서 메세지를 암호화 시킨 키에 대한 정보를 알아내어 자신의 비밀키로 그 키를 복호화 한다. PEM-info 필드에서 메세지 복호화를 위한 알고리즘 정보를 통해 복호화 시킨다.

이후 과정은 "MIC-only"나 "MIC-clear"와 동일하다.

3.4.2 메세지 무결성과 신분 인증성 검증

MIC-Info에서 MIC알고리즘과 서명 알고리즘을 알아내어 메세지의 표준 표현 형식상에서 MIC를 계산후 비교하여 무결성을 체크한다. 먼저 서명된 MIC값을 발신자의 공개키를 이용해 복호화하고 비교한다. 만일 일치하면 메세지의 무결성은 검증된것이다. 부가적으로 수신자는 발신자의 신원과 그의 키와의 연결성을 검증함으로써 발신자 인증을 검증하게 된다.

3.4.3 시스템 로컬 표현으로 변환

모든 것이 완료되면 메세지의 표준 표현 형식은 해당 시스템의 표현 형식으로 번역되어 사용자에게 보여진다. 수신측의 PEM UA는 그 메세지의 무결성이 검증된 것임을 알리고 인증된 발신자의 신원을 표시해준다. 이 표시된 신원은 그의 신원 증명서(certificate)에 있는 발신자 이름과 그 이름을 검증받는 정책의 모두를 포함해야 한다. 이 신원은 메세지내에 포함된 신원 정보, 예를 들면 "From:",과는 독립적이다.

3.4.4 메세지의 처분

복호화된 표준 표현 형식으로 PEM 헤더 없이

저장하거나, 복호화된 표준 형식으로 PEM헤더와 함께 저장, 혹은 암호화된 상태로 저장 될 수 있다.

3.5 Internet 공개키 인증 시스템(Public Key Certificate System)

Internet은 single-rooted 트리 형태의 인증 시스템을 채택하였다. IRPA(Internet PCA Registration Authority)는 Internet Society 산하에서 운영되는 비영리, 전문조직으로 세계적인 Internet 테크놀로지 사용 확산을 증진시키기 위한 단체로서 이 인증 계층 구조(hierarchy)하에 발급되는 모든 신원 증명서(certificate)에 적용하는 공통된 정책을 수립한다.

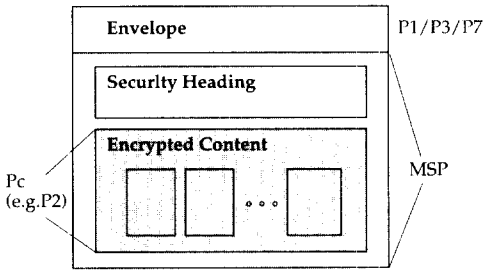


그림 5 Message Secure Protocol

4. SDNS MSP (Message Secure Protocol)

SDNS(Secure Data Network System)는 미국 NSA(National Security Agency)주관으로 연방 OSI 네트워크를 안전하게 하기 위한 프로토콜들을 개발하는 작업이다. 안전한 전자 우편과 안전한 메세지 전송에 대한 요구로 인해 SDNS 아키텍춰내에 X.400 MHS에 보호 서비스 기능을 지원하기 위해 개발된 것이 MSP이다[9]. MSP는 X.400의 88년 버전에서 보호 서비스를 첨가하기 이전인 1986년에 개발되기 시작하였다.

4.1 서비스 적용 범위 및 영역

MSP는 내용물에 관한 프로토콜에 해당하며 송/수신 UA내에 구현되어진다. MSP처리는 MTS에 메세지를 제출하기 이전에 그리고 MTS로부터 메세지 배달을 받은 후에 이루어진다. 즉, MSP는 MHS의 내용물(IPM, EDI 등)을 보호 하기 위한 서비스를 제공하는 것이다. 그러나 이들 실제의 내용물 프로토콜(content protocol)과는 독립적이다.

SDNS MHS의 UA에서 메세지 내용물을 캡슐화(encapsulating)시키고 MTS에 제출하기 전에 MSP 헤딩을 첨부함으로써 보호 서비스들을 제공한다. SDNS MSP는 X.400 MHS에는 투명성을 제공한다.

4.2 제공하는 보호 서비스

6개의 보호 서비스를 세가지 그룹으로 분류하여 제공한다.

- 메세지 비밀성, 무결성, 자료 발신처 신분 인증 및 접근 제어(message confidentiality, integrity, data origin authentication and access control)
- 발신처의 부인 봉쇄(non-repudiation with proof of orign)
- 수신 사실에 대한 서명된 확인서 요청과 반송(request/return of signed receipt of the received message) : 발신자 부인 봉쇄 서비스가 제공되는 경우에 한해 제공된다.

4.3 서비스 제공 방식

4.3.1 MSP 구성

"Protected Content" 라는 새로운 내용물 유형(content type)을 정의한다. 이 새로운 내용물은 본래의 X.400 내용물과 함께 복호화 및 검증 등에 필요한 다양한 보호 서비스 파라메터들을 포함

한다. 암호화, 무결성 체크, 서명 생성/검증 등을 수행하기 위해 사용된 알고리즘 정보들도 포함된다. 선택적으로 원 메세지의 한 부분 필드가 보호 서비스 헤딩 부분에 포함될 수 있는데 이는 수신자에게 복호화에 앞서 선행 정보를 제공하기 위한 것이다. 감싸여진(Encapsualted) 내용물은 MTS에 제출된다. 그림 5에 MSP의 구성을 보인다.

4.3.2 MSP 메세지 처리

MSP의 액세스 제어 기능은 비밀성, 무결성, 발신처 신분 인증 서비스들이 선택된 경우 적용될 수 있다. MSP에서도 MHS의 다중 수신자 처리 문제를 해결하기 위해 "protected token" 이라는 각 수신자에 관련된 보호 서비스 파라메터들을 위한 자료 구조를 정의하고 있다. 발신자는 message key, sensitivity label, message content상에 적용할 해쉬 함수 및 기타 보호 제어 정보를 선택하고 각수신자에 대한 protected token을 형성하기 위해 이를 pairwise key로 암호화한다. 수신자들에 대한 신분 증명 및 키관련 정보를 디렉토리 서버를 이용해서 얻어 오는 경우를 위한 상세 사항은 SDN.702 SDNS Directory Specification에서 기술하고 있다. 발신자는 이 각 수신자에 대한 토큰을 MSP 헤딩에 배치시킨다. 이 절차동안 발신자는 각 수신자들이 메세지를 수신할 권한이 있는가를 확인하기 위한 엑세스 제어 체크를 수행한다.

메세지를 수신하는 측에서는 각 수신자들이 자신의 메세지 토큰을 보호 서비스 헤딩으로부터 받는다. 이때 자신의 토큰을 찾아내는 search key로서 tag을 이용하게 된다. 각 수신자는 자신의 pairwise key로써 메세지 키, 해쉬, 기타 보호 제어 정보를 얻기 위해 자신의 토큰을 복호화한다. 엑세스 제어 정책을 시행하기 위해 정보 보호 수준 레이블이 검사되고, 메세지 키는 메세지 복호화에 사용되며, 단방향 해쉬는 메세지의 무결성 검증을 위해 사용된다.

서명과 서명된 수신확인을 위한 메세지 처리를 위해서는 MSP 헤딩내에 서명 정보를 포함시켜야 한다. 이러한 서명 정보와 수신 확인 요청등을 담기 위한 필드를 "Signature Block" 이라 하며 그 구성은 다음과 같다.

Signature Block :

- 서명 알고리즘 식별자
- 발신자의 서명 인증서
- 제어 정보
  - — 서명 정보
  - — 수신 증명 정보
- 서명 결과값

메세지에 서명하기 위해 발신자는 원래의 메세지 내용물 상에 단방향 해쉬를 계산하고 다시 계속해서 서명 정보를 포함시켜 해쉬값을 계산한다. 최종 계산된 해쉬값은 서명된 후 Signature Block 내의 서명 결과 값으로 포함된다.

발신자가 서명된 수신 확인 요청 서비스를 사용하는 경우에 이를 서명 정보내의 수신 증명자 필드에 명시한다. 만일 모든 수신자에게 이 서비스를 적용하는 경우 flag가 셋팅되나 부분적으로 요청하는 경우 그들의 O/R Name(Originator/Receipient Name)이 그 필드에 명시된다.

4.3.3 MSP 메세지 수신처리

수신자는 두가지 절차로 메세지 서명을 검증한다. 수신된 메세지의 내용물(message content)와 서명 정보에 대한 단방향 해쉬값이 계산된다. 서명 인증서에 담긴 정보를 이용하여 제공된 서명 결과 값을 검증하기 위한 계산을 수행한다.

수신측에서는 서명된 수신 확인 요청을 받았을 때 그 수신 확인서를 생성할 수도 있고 그렇지 않을 수도 있다. 수신 확인을 보내기 위해 수신자는 새로운 Signature Block을 만든다. 이것은 수신자의 서명 증명서를 담게 된다. 제어 정보 필드에 그 블럭이 서명된 메세지에 대한 서명된 수신 확

인임을 알린다. 원래의 해쉬값을 수신 확인을 위한 제어 정보 필드를 포함하기 위해 확장되어 수신자에 의해 서명된다. 버젼 번호와 Signature Block을 담은 MSP 헤딩만으로 구성된 메세지는 서명된 메세지의 발신자에게 전송된다.

서명된 수신확인서를 요청만 메세지의 발신자는 그 수신 확인 메세지 응답을 받아 이미 저장해 두었던 원래의 메세지에 대한 해쉬를 수신측의 제어 정보를 포함하기 위해 확장 적용한다. 이 계산된 값이 수신 메세지의 검증된 서명 결과 값과 비교된다. 만일 그 값이 맞는 경우 그 반환되어 온 Signature Block는 원래 메세지에 대한 서명된 수신 확인으로써 제공된다.

5. 세가지 방식의 특징 비교

X.400 MHS는 18개 보호 서비스를 제공하며 이들은 5개의 그룹으로 나뉘어 진다. 보호 서비스에 관한 파라메터들이 메세지의 봉투(envelop)에 놓이며 여러 바디 부분들을 담은 메세지 내용물 전체를 균일하게 보호한다. 즉, 내용물속의 바디 각각에 대해 구분된 보호 서비스를 제공하지는 않는다. 이 방식은 제공하는 보호 서비스의 종류에 따라 UA에 보호 서비스를 첨가할 수도 있고 MTA에 첨가 할 수도 있다. 그러나 전송로 상에 있는 각 MTA들이 보호 서비스 파라메타들을 포함하고 있는 봉투의 정보를 해석할 수 있어야 한다.

PEM의 경우 4가지 보호 서비스를 제공한다. 단대단 보호 서비스만을 제공하며 X.400 모델 관점에서 볼때 바디 부분에 보호 서비스를 제공하는 것으로 그 바디의 시작 부분에 보호 서비스 파라메터들을 실제의 내용물과 함께 담게 된다. 연속적인 바디에 보호 서비스를 각기 달리 선택적으로 적용할 수 있다. 따라서 공개 정보에는 평문으로 중요도가 높은 부분은 암호화 등의 보호 처리를 해서 전송시킬 수 있다. UA가 보호 서비스를 제공하도록 되어 있으며 MTA에는 아무런 제약 사항이 없다.

MSP 방식은 앞의 두방식의 혼합 형태를 띠고 있다. 메세지 내용물에 대한 보호 서비스를 제공하나 보호 서비스 파라메터들은 봉투가 아닌 " protected content" 의 앞부분에 놓인다. MSP는 보호 파라메터들과 기타 다른 내용물들을 캡슐화하고 있는 새로운 유형의 내용물 종류를 정의한 것이다. 이러한 방식으로 MTA의 변경없이 UA에 의해서만 보호 서비스를 적용하도록 하고 있다.

이 세가지 방식중에 PEM은 보호 파라메터를 전달하는 하나의 새로운 바디 부분을 정의하는 것으로 간주할때 X.400 모델에서 수용할 수 있는 것으로 실제, NIST OIW의 Security 작업 그룹에서는 X.400 메세지 시스템의 바디 부분에 PEM 메세지를 담을 수 있도록 정의하고 있다[10]. 그러나 MSP 에서의 protected content는 다른 내용물들을 모두 감싸는(encapsulate)방식을 취하고 있으므로 이러한 수준의 캡슐화는 현재 X.400 모델에서는 인식될 수 없다. MTA 변경 차원에서 볼때 X.400 보호 서비스 방식에서는 보호 서비스 관련 정보가 봉투 부분에 위치하게 되므로 MTA 변경성을 배제할 수 없는 반면 다른 두 방식은 MTA의 투명성을 제공한다. 그러나 전송 경로 서비스와 같은 부가 서비스를 X.400에서는 제공할 수 있다. UA변경은 세가지 방식 모두 필요하며 PEM의 경우 각 바디 부분을 선택적으로 보호할 수 있는 기능을 제공할 수 있다.

PEM과 다른 두가지 방식은 대상 환경과 하부 구조, 사용자 부류가 다르다는 면에서 다소 비교의 의미가 적을 수 있다. 그러나 X.400 MHS 보호기능과 SDNS의 MSP는 하나의 선택 사항이 될 수 있다. 실제 MSP는 X.400의 보호 기능이 추가된 88버젼 이전에 이와는 독립적으로 개발되었다.

6. 결 언

지금까지 전자 우편 서비스를 안전하게 하려는 대표적인 방식에 대해 각 방식의 환경과 특성들을 비교 분석하였으며 이들 간의 관련성을 비교 검토

해보았다. 외국에서는 이러한 여러 접근 방식들을 적용 시킨 소프트웨어 및 툴킷(toolkit)들은 물론 업체들 자체의 전자 우편 서비스에 보호 서비스를 강화하는 제품들을 제공하는 등 전자 우편 시스템의 유용성을 감안한 보호 서비스 분야의 인식들이 높아가고 있다. 우리나라에서도 Internet 사용자들의 계속적인 증대와 MHS 환경을 기반으로 하는 일반 기업체들의 EDI 사용 증가 추세를 볼때 이러한 전자 우편 시스템의 안전성에 관한 주요 논의들을 검토해 봄으로써 향후에 보다 효과적인 해결 방식의 도출이나 합리적인 프로화일을 개발하는데 도움이 될 수 있으리라 본다.

참 고 문 헌

[1] David J. Stang, Sylvia Moon, Network World-Network Secuirty Secrets, pp. 575-580, IDG Books Worldwide, 1993.

[2] Russell Housley, "Electronic Messaging Security : A Comparison of Three Approaches", the Fifth Annual Computer Security Applications Conference Proceeding, pp.28,December, 1989.

[3] Warwick Ford, Computer Communication Security,pp.325-373, Prentice-Hall, 1994.

[4] Paul Korzeniowski, "Closing the Gaps in E-mail", pp.20-21, InfoSecurity News, Vol.4, No.5, September/October 1993.

[5] ITU, CCITT Blue Book(X.400-X.420), 1988.

[6] Adrian Tang, Sophia Scoggins, Open Networking with OSI, pp.322-362, Prentice-Hall, 1992.

[7] Michelle J. Gosselin, "Message Handling Systems(X.400) Threats, Vulnerabilities, and Countermeasures", 16th NCSC Computer Security Conference Proceeding, pp.226-235, September, 1993.

[8] Brad Tipler, "X.400 Security : Overview and Implementation Experience", the Fifth Annual Canadian Computer Security Symposium Proceeding, pp. 557-575, May, 1993.

[9] NIST, SDNS Secure Data Network System Message Security Protocol, SDN.701, V.1.5, August 1989.

[10] Stephen T. Kent, "Internet Privacy Enhanced Mail", CACM, Vol. 36, No. 3, pp.48-60, August 1993.

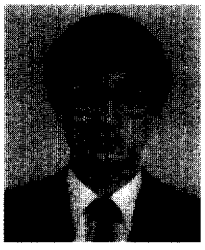
[11] Stephen T. Kent, "An Overview of Internet Privacy Enhanced Mail", INET' 93, June 1993.

[12] 홍주영, 임채호, "인터네트 보안 관련 연구 개발 현황", 통신정보보호학회지, 제3권 제4호, pp.50-55, 1993.12.

□ 著者紹介

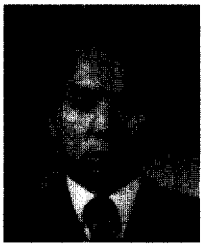
홍 주 영(정회원)

1990년 2월 홍익대학교 전산학과 졸업 (학사)
1990년 2월 ~ 현재 한국전자통신연구소 연구원
※ 주관심분야 : 컴퓨터 보안, 네트워크 보안



윤 이 중(정회원)

1988년 2월 인하대학교 전산학과 졸업 (학사)
1990년 2월 인하대학교 전산학과 졸업 (석사)
1990년 2월 ~ 현재 한국전자통신연구소 선임연구원
※ 주관심분야 : 컴퓨터 보안, 네트워크 보안, DBMS



김대호(정회원)

1977년 2월 한양대학교 전자공학과 졸업 (학사)
1984년 8월 한양대학교 산업대학원 전자공학과 졸업 (석사)
1993년 1월 ~ 1993년 12월
Univ. of Maryland at College Park
Dept. of Computer Science Visiting Scholar
1977년 2월 ~ 현재 한국전자통신연구소 책임연구원
※ 주관심분야 : 전송분야, 통신 및 컴퓨터 보안 분야