論 文

MHS의 정보보호 프로토콜 설계 및 구현연구

正會員 李 亨 洙* 正會員 丁 仙 伊** 正會員 鄭 鎭 旭**

The Design and Implementation for the Secure Protocol of MHS

Hyung Soo Lee*, Sunny Jung**, Jin Wook Chung** *Regular Members*

要 約

전자우편서비스가 확대됨에 따라 정보 보호 문제가 중요한 현안으로 대두될 것이다. 이러한 필요성에 따라, MHS(Message Handling System) 시스템의 정보보호(Information Security) 서비스에 관련된 표준화(X.400 series)와 보안 서비스에 관련된 키 관리 메카니즘 표준화(X.509)를 분석하였다. 본 연구에서는 여러가지 보안서비스 중, 안전한 메시지 전송을 위해 1차적으로 메시지 비밀보장, 메시지 무결성, 발신처 인증 서비스를 위한 SMP(Secure Message Protocol) 프로토콜을 설계하여 UNIX BSD 4.3 시스템 환경에서 구현하였다.

ABSTRACT

It will not take too long that the problem of information protection becomes an important issue as the electronic mail services grow. In this paper, we first analyzed various existing security services recommunded in CCITT. The analysis includes security services of message handling system specified in CCITT Recommendation X.400 series and its key management mechanism specified CCITT Recommendation X.509. We then proposed a secure message protocol for the following three services : the message confidentiality, the message integrity, and the data origin authentication. We also implemented the proposed protocol under the UNIX BSD 4.3 environment.

I. 서 론

현재 국내에서는 네트워크의 확산과 컴퓨터 시스템의 보급 증대로 인하여 활발한 정보교환이 이루어지고 있다. 이러한 정보 교환에 많은 역할을 하고 있는 것이 전자우편(electronic mail)시스템으로서 CCITT에서 1984년 처음 X.400 series(Message Handling System)로 표준화가 발표되었으며 1988년에 보완되었다.

국내에서도 정보의 원활한 유통과 세계 표준화 추세에 맞추어 MHS시스템에 근거한 전자우편시스템을 한국통신, 한국 데이타통신(주) 등 여러 기관에서 개발하여 서비스중에 있다.

*韓國電子通信研究所
ETRI
**成均館大學校 情報工學科
Dept. of Infor. Eng., Sungkyunkwan Univ.
論文番號 : 93-115

그러나 전자 우편시스템의 사용이 증대되고 사용자의 수가 확대됨에 따라 향후 개인정보의 불법 노출에 따른 프라이버시 문제, 컴퓨터 바이러스 프로그램에 의한 네트워크 성능저하, 메시지 내용의 수정 및 변경에 따른 재산 상의 피해 등 문제점이 발생할 가능성이 높아지고 있다. 특히 MHS는 최근 전세계적으로 활발한 도입이 추진되고 있는 무역, 운송, 유통업계 등의 전자문서교환 시스템인 EDI(Electronic Data Interchange)의 구현을 위한 기반을 제공하고 있어 MHS상에서의 정보보호 문제는 그 중요성이 더욱 제고되고 있다.

본 연구는 이러한 문제점을 막기 위하여 MHS시스템의 표준화 작업(X.400 series) 중 위협요소별 보안서비스 분석 및 MHS시스템의 디렉토리에 관한 표준화(X.500 series)에서 인증 및 공개키 관리에 관한 표준화를 분석하였다. 분석된 보안서비스 중 국내에서 우선적으로 개발이 요구되는 보안서비스를 선정하여 구현에 필요한 메카니즘과 안전한 메시지 전송을 위한 프로토콜(SMP : Secure Message Protocol)을 설계하였다.

특히 기존에 대부분의 연구들이 프로토콜의 설계 및 단순히 비밀보장(confidentiality) 서비스만을 구현한 것에 반하여, 본 연구에서는 MHS에서 요구되는 다양한 정보보호 서비스들을 UNIX BSD 4.3 시스템 환경에서 구현하여 그 결과를 분석하였다.

Ⅱ. MHS 보안 표준화 개요

공중통신망에 연결된 컴퓨터의 정보처리 기능과 축적기능을 이용하여 메시지를 전송, 축적, 처리 등의 서비스와 이 서비스를 제공하기 위한 메카니즘을 MHS(Message Handling System)라고 한다. 이 MHS에 대한 표준화는 1984년 X.400 series라는 표준안이 처음 제시되었으며 1988년에 수정, 보완되었다[1]. 이 중 보안(security)에 관련된 사항으로는 1984년 표준안에서 메시지 내용(message content)에 보안 파라미터를 넣었으며, MTS(Message Transfer System) 보안서비스는 제공하지 않았으나 1988년 표준안에서는 정보의 누출, 수정, 파괴 등의 위협에 대한 위협요소(risk)와 보안서비스를 규정하고 있으며 MTS, MS(Message Store), directory에도 보안서비스를 정의하고 있다. X.402 부록에서 정의한 MHS 환경의 위협요소는 위장(Masquerade), 메시지 순서변경, 정보수정, 서비스 거절, 정보의 누출, 서비스 부인, 기타 위협으로 분류하고 있다. 또한 이러한 위협요소에 따라 어떤 MHS 보안서비스가 제공되어야 하는지는 ISO OSI 7498-2(Network Security Architecture)[2]에 기인하고 있다.

MHS 시스템의 위협요소별 보안서비스 명칭은 표 1과 같이 정의되고 있다.

표 1. 위협요소에 대한 보안서비스
Table 1. Security services for threat factors

위 협 요 소		보안서비스
위 장	Impersonnation and misuse of the MTS	Message Origin Authentication Probe Origin Authentication Secure Access Management
	Falsely acknowledge receipt	Proof of Delivery
	Falsely claim to Originate a message	Message Origin Authentication
	Impersonnation of an MTA to an MTA	Proof of Submission Report Origin Authentication Secure Access Management
	Impersonnation of an MTA to another MTA	Report Origin Authentication Secure Access Management
메세지 순서변경	Replay of Message	Message Sequence Integrity
	Re-ordering of Message	Message Sequence Integrity
	Pre-play of Message	
	Delay of Message	

정보수정	Modification of Message Destruction of Message Corruption of Routing and other management information	Connection Integrity Content Integrity Message Sequence Integrity
서비스 거절	Denial of Communication MTA Flooding MTS Flooding	
부인봉쇄	Denial of origin Denial of submission Denial of Delivery	Non-repudiation of Origin Non-repudiation of Submission Non-repudiation of Delivery
정보누설	Loss of confidentiality Loss of anonymity Misappropriation of message Traffic analysis	Connection Confidentiality Content Confidentiality Message Flow Confidentiality Secure Access Management Message Flow Confidentiality
기타위협	Originator not cleared for Message Security Label MTA/MTS-user not cleared for Security context Misrouting	Secure Access Management Message Security Labelling Secure Access Management Secure Access Management Secure Access Management

또한 이러한 보안서비스가 MHS 시스템의 UA (User Agent), MTS, MS 구간 중 어느 구간에 위치해야 될지에 대한 MHS 서비스 구간은 표 2와 같이 정의하고 있다.

이 표에서 볼 수 있듯이 각 보안서비스가 여러 구간에서 중복되어 제시되어 있고 보안서비스의 종류도 다양하게 제시되어 있기 때문에 현재 각국에서는 어떤 보안서비스를 어느 구간에 구현시킬지에 대한 논의가 주된 관심사로 부상하고 있으며, 국내에서도 이에 대한 논의가 진행중인 것으로 사료된다.

이러한 MHS 보안서비스 메카니즘 중 인증과 공개키관리는 X.509[3]에서 정의하고 있다. X.509에서는 사용자에게 directory에 대한 보안서비스로서 인증에 대한 기법을 크게 단순 인증(Simple Authentication)과 강한 인증(Strong Authentication)으로 구분하고 있다. 즉 패스워드를 이용하여 DUA(Directory User Agent)와 DSA(Directory System Agent) 사이 또는 DSA와 DSA 사이와 같은 제한된 대등 실체(peer entity) 인증에 이용되는 기법을 단순인증이라 하고 있으며, 공개키 암호시스템(Public Key Crypto System : PKCS)을 사용하여 공개키와 비밀키의 쌍(pair)으로 암호화와 복호화를 하여 인증하는 것을 강한 인증으로 분류하고 있으나 강한 인증을 권고하고 있다.

한편 directory시스템에서는 공개키의 분배에 대해서 키의 변경, 재전송 등의 신뢰문제 때문에 디렉토리로 부터 읽은 공개키를 사용자가 검증할 수 있는 수단이 필요한데 이는 certificate라는 데이터구조를 사용함으로써 제공되어지며 이러한 키 관리를 위해 모든 사용자는 CA(Certification Authority)라 불리는 offline entity와 서로 공개키를 교환해야 한다. 이 CA는 certificate를 디렉토리시스템을 통해 요청한 사용자에게 보내지며 사용자는 이 certificate의 정당성을 조사하여 공개키를 얻게 된다.

그러나 이런 기법은 서로 다른 CA에 의해 제공되는 상황에서는 적절하게 못하므로 한쪽의 CA가 다른쪽 CA의 공개키 certificate를 발생시켜야 하는데 이것을 cross certificate라고 하며 그림 1과 같은 계층구조의 연결 모양을 가진 certificate path를 제시하고 있다.

즉 A가 C의 공개키(여기서 Cp : C의 공개키, Xp : X의 공개키)를 얻고자 할 때는 Cp = Xp. X≪C≫로

표 2. 각 agent간의 보안서비스

Table 2. Security services applying between agents

서비스 \ 각 구간		UA/UA	UA/MS	MS/MTA	UA/MTA	MTA/MS	MTA/MTA	MTA/UA	MS/UA
Origin Authentication	Message Origin Authentication	○	○		○				
	Probe Origin Authentication			○	○				
	Report Origin Authentication					○	○	○	
	Proof of Submission						○		
	Proof of Delivery		○						N*
Secure Access Management	Peer Entity Authentication		○	○	○	○	○	○	○
	Security Context		○	○	○	○	○	○	○
Data Confidentiality	Connection Confidentiality		○	○	○	○	○	○	○
	Content Confidentiality	○							
	Message Flow Confidentiality	○							
Data Integrity	Connection Integrity		○	○	○	○	○	○	○
	Content Integrity	○							
	Message Sequence Integrity	○							
Non-repudiation	Non-requdiation of Origin	○				○			
	Non-repudiation of Submission							○	
	Non-repudiation of Delivery	○							
Message Security Labelling	Message Security Labelling	○	○	○	○	○	○	○	○
Security Management	Change Credentials		○		○	○	○	○	
	Register		○		○				
	MS-Register		○						

*N : 수신 MS가 발신측 UA에게 행함.

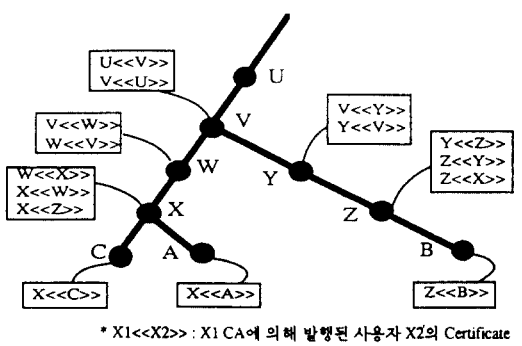


그림 1. Certification authority의 계층적 구조

Fig 1. Hierarchical architecture of certification authority

서 certificate path를 풀 수가 있으며 CA가 계층구조로 배열된 A에서 B의 공개키(Bp)를 얻고자 할 때는 사용자의 상위 계층의 CA 공개키 certificate와 역방향 certificate를 directory에서 저장하고 있어야 하며 이를 이용하여 Bp=Xp. X≪W≫W≪V≫V≪Y≫Y≪Z≫Z≪B≫를 풀 수 있다.

Ⅲ. Secure Message Protocol 설계

X.402에서 제시된 보안서비스는 너무 광범위하고 각 구간에서 중복되는 서비스가 많기 때문에 현재 각국에서는 자국에서 가장 긴급한 위협요소를 추출하여 요구되는 서비스를 선정한 후 최적의 구간에서 구현해 가고 있다.

최근 국내에서도 안전한 메시지전송을 위해 MHS상에 부인봉쇄 서비스를 제공하기 위한 연구[4]가 발표된 바 있으며, EDI서비스를 위한 보안관련 연구가 일부 진행되고 있다. 그러나 현재까지 이들 연구는 정보보호 서비스를 제공하기 위해 표준안에 제안된

메카니즘을 이용한 프로토콜 설계에 그치고 있어, 실제 운용중인 메시지전송을 위한 서비스 제공에는 미치지 못하고 있는 실정이다. 따라서 이미 운영중인 메시지전송 및 전자우편 서비스 등에의 적용을 고려한 현실적인 보안서비스의 설계 및 구현연구가 이루어져야 할 것으로 보인다.

이러한 동향에 따라 본 연구에서는 X.402와 X.509의 표준안에 근거, 실제 사용자측에서 요구되는 보안서비스를 제공하기 위해 UA측에 정보보호프로토콜을 설계하고, 현재 일반 사용자간에 가장 널리 이용되고 있는 UNIX시스템의 전자우편 소프트웨어인 SMTP상에 구현하였다.

본 연구에서는 먼저 1차적으로 향후 국내에서 발생될 위협 요소로서 메시지 노출로 인한 프라이버시 침해 및 중요 내용의 노출 문제와 메시지수정 문제 및 발신처가 없는 컴퓨터 바이러스 문제를 위협요소로 선택하였으며 이를 막기 위한 보안서비스를 UA(User Agent)측에서 MTS(Message Transfer System)로 메시지를 발송하기 전인 구간을 선정하여 메시지 비밀보장(confidentiality), 무결성(integrity), 데이타발신처 인증(data origin authentication)의 3가지 보안서비스를 연구 대상으로 선정하였다.

또한 위 선정된 보안서비스에 따라 구현에 요구되는 보안 메카니즘과 공개키 관리를 비롯하여 메시지를 안전하게 송수신하기 위한 SMP 프로토콜을 제안하였으며 그 위치는 UA에 그림 2와 같이 설계하였다. 원래의 메시지 내용(content)에 3가지 보안서비스 처리를 한 결과는 그림 3과 같이 메시지 헤더(header)에 security heading을 부가시킨 새로운 메시지 내용(protected content)를 형성하게 된다.

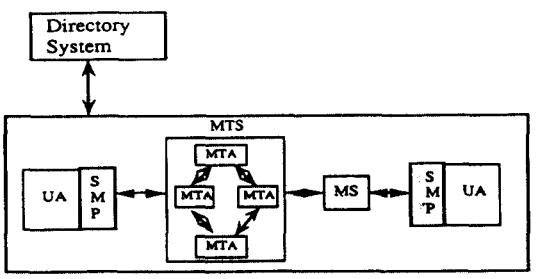


그림 2. MHS상에서의 SMP(Secure Message Protocol) 위치
Fig 2. The location of SMP on MHS

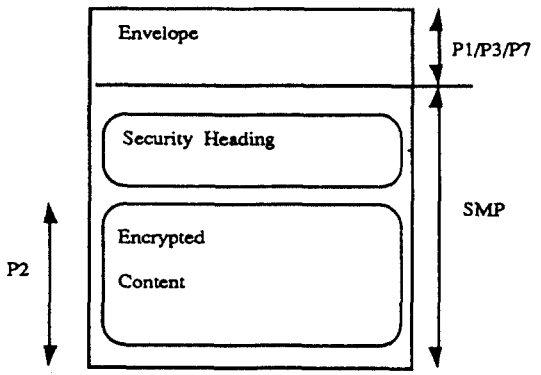


그림 3. SMP가 적용된 메세지 구조
Fig 3. Protected message frame

그림 3과 같은 새로운 메시지 내용에는 원래의 내용을 암호화하거나 수신측에서 복호화 또는 증명에 요구되는 보안 파라미터, 무결성 검사치, 전자 서명 등을 수행하는데 필요한 알고리즘에 관한 파라미터 등이 요구되는데 이러한 일을 처리하는 것이 P2 content type이라 정의하고 있으므로 이것에 정보보호에 관련된 정보가 추가되어 encapsulate되게 된다. 그 다음, 정보보호 처리가 끝난 메시지가 MTS로 발송되게 된다.

본 장에서는 먼저 정보보호 프로토콜을 설계하는데 필요한 메카니즘을 분석하고, 다음으로 SMP프로토콜을 설계하였다.

1. 비밀보장 메카니즘

이 기능은 메시지의 불법 노출로부터 데이터를 보호하기 위한 것으로 암호화 메카니즘이 사용된다.

본 연구에서 채용된 메카니즘은 그림 4와 같이 난수(random number)를 발생하여 이 난수를 사용자키(UK)로 이용하도록 하였으며 UK를 이용하여 메시지 전체를 암호화 하게 된다. 이때, 사용되는 암호알고리즘은 처리 속도를 고려하여 본 연구에서는 대칭키 암호시스템으로 가장 널리 알려진 DES(Data Encryption Standard)[5]알고리즘을 채택하였다.

DES와 같은 대칭키 시스템은 비밀키(사용자키)를 반드시 상대방에게 전송시켜야 하므로 이 키를 안전하게 전송하기 위해서 공개키 암호 시스템을 사용하여 다시 암호화한 후 전송한다. 즉, 사용자 키는 수신측 공개키에 의해 암호화되어 전송되며 수신측은 수신측의 비밀키를 이용하여 사용자키를 복호화한 후

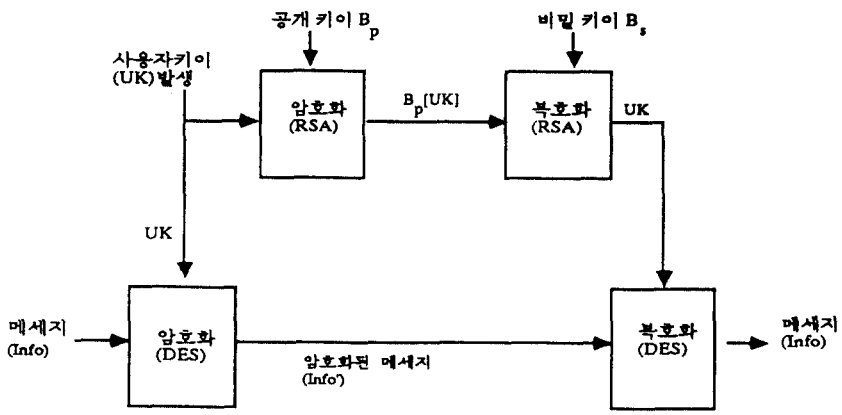


그림 4. 비밀보장 메카니즘
Fig 4. Confidentiality mechanism

다시 복호화된 키를 이용하여 메시지를 복호화하게 된다.

2. 전자서명 메카니즘

CCITT의 X.509에서는 메시지의 전송과정과 수신과정중 메시지의 불법 수정이나 변경을 감지하기 위한 무결성 기능과, 수신된 메시지가 자격을 가진 정당한 발신처에서 보내진 것인지를 보장하기 위한 발신처 인증기능을 제공하기 위해서 전자서명 메카니즘(digital signature mechanism)을 사용하도록 권고하고 있다.

또한 무결성 기능과 발신처 인증시 암호화해야 될 메시지의 길이(N)가 클 때 처리시간이 많이 소요되므로 메시지 길이가 짧은 블럭단위의 길이로 변환시킬 필요가 있다. 이때 사용되는 것이 hashing함수로서 송수신측에서 동일한 것을 사용하도록 권고하고 있다.

X.509에 제시된 hashing함수는 square-modular n 방식을 적용하고 있으나 본 연구에서는 최근 32비트 머신상에서의 효율성 및 안전성이 고려된 Rivest의 MD4 Message Digest알고리즘[6]을 채용하였다. 특히 MD4는 실제 시스템구현시에 32비트 SUN Sparc 상에서 초당 약145만바이트의 속도를 제공할 뿐만아니라 서로 다른 두개의 메시지로부터 동일한 다이제스트를 취할 가능성은 2^{64}의 연산, 또 알려진 다이제스트로부터 메시지를 취하기 위해서는 2^{128}의 연산을 수행하여야 되므로, 계산적 안전성을 제공한다.

MD4의 기본동작은 다음 5단계로 수행되며, 구체적인 연산방법에 대한 내용을 본 논문에서 생략한다.

단계 1 : 입력된 임의 길이의 모든 메시지에 대해 다음 과정에 의해 최대 512개의 비트를 메시지 뒤에 부가한다.
$(b+b')\bmod 512 \equiv 448$
(여기서 b는 입력된 메시지의 길이이며, b'는 부가되는 패딩메시지로서 1000...의 비트열을 갖는다.)

단계 2 : 단계 1에서 생성된 메시지에 b의 64비트 2진값을 구하여 부가한다.
즉, 메시지 전체 길이가 512(64, 32, 16)의 배수가 되도록 한다.

단계 3 : 다이제스트값을 저장하기 위한 32비트의 MD버퍼(A, B, C, D)를 초기화한다.

단계 4 : 다이제스트를 생성하기 위해 다음과 같이 3개의 32비트 워드의 입력에 대해 1개의 32비트 워드를 생성하는 3개의 함수를 정의하여, 단계 2에서 완성된 전체 메시지에 대해 이들 각 함수를 3개 round에서 수행한 다음, 최종적으로 생성된 32비트 워드 4개의 값을 A, B, C, D의 버퍼에 저장한다.

단계 5 : 마지막으로 단계 4에서 생성된 A, B, C, D의 값을 A의 저차 바이트에서 부터 D의 고차 바이트까지의 순서로 최종적으로 128비트의 MD(Message Digest)를 출력한다.

위 과정에서 생성된 MD(이하 이를 HV(Hashing

Vector)라 한다)를 서명하기 위하여 공개키 암호시스템을 사용하였으며 여기에 사용된 암호 알고리즘은 RSA[7]알고리즘을 이용하였다.

본 논문에서 적용된 전자서명 과정은 그림5와 같다. 먼저 송신측(A)에서 hashing함수의 수행에 의해 얻어진 HV를 송신측의 비밀키 As로 서명한 정보(X=As(HV)를 메시지 헤더(header)에 부가하여 수신측에 보내면, 수신측(B)은 서명된 X를 송신측의 공개키 Ap로 복호화시켜 HV를 얻게 된다. 그 다음, 송신측으로 부터 수신된 암호화 메시지를 UK를 사용하여 복호화시킨 후 송신측과 동일한 hashing 함수를 사용하여 HV'의 값을 구하여 송신측으로부터 수신된 HV와 수신측이 hashing 함수를 적용하여 구한 HV'의 값을 비교하여 같으면 정당한 발신처에서 도중에 수정없이 보내어진 것으로 보장할 수 있게된다. 만약, 이 값이 같지 않다면 도중에 메시지의 변경이 있었거나 발신처가 잘못된 것으로 간주할 수 있다.

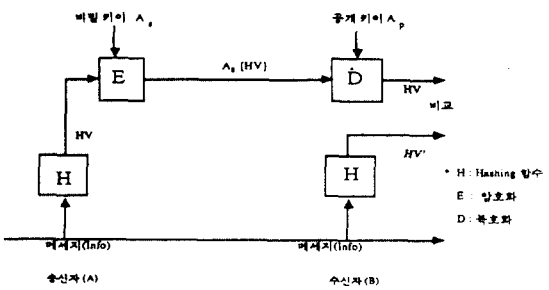


그림 5. 전자서명 메카니즘
Fig 5. Digital Signature Mechanism

3. 공개키 관리 메카니즘

공개키 관리는 X.509에서 정의하고 있다. 즉, directory Server에 공개키를 등록시키고 있으며 이곳으로 부터 읽어낸 공개키가 수정되거나 재사용(Replay)되지 않았다는 것을 검증하기 위하여 certificate라는 수단을 제공한다. 또한 certificate를 할당하거나 새로이 생성하는 신뢰할 수 있는 authority를 CA(Certificate Authority)라 한다[8].

Certificate의 데이터 구조는 다음과 같다.

CA≪A≫=CAs(AI, CA, A, Ap, T)

여기서 CAs : CA의 비밀키, AI : 알고리즘 구분, CA : CA의 이름, A : A의 이름, A_p : 공개키, T : 키 유효기간

동 메카니즘에서 CA는 각 사용자에게 CA의 공개키를 미리 제공한 다음, CA는 사용자 이름, 사용자 공개키, 키 유효기간 등을 CA의 비밀키로서 전자서명한 후 directory Server에 각 사용자의 공개키를 암호화하여 certificate를 등록하게 된다. 이때 특정 사용자의 공개키를 취하고자 하는 사용자는 directory server를 통해 그 사용자의 certificate를 읽어오게 된다. 그 다음, 사용자는 미리 알고 있던 CA의 공개키를 이용하여 certificate를 복호화시켜 정당성을 조사한 후 상대편의 공개키를 취할 수 있다.

그림 6은 공개키 관리를 동일 CA에서 관리하는 메카니즘을 대상으로 한, 본 연구에서 설계된 SMP프로토콜의 메카니즘에 따른 흐름도를 나타낸 것으로, 다음에 나오는 SMP프로토콜 설계에서 이 그림과 관련하여 설명한다.

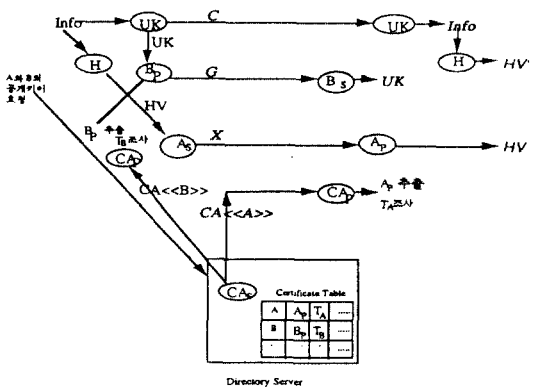


그림 6. SMP 메카니즘의 흐름도
Fig 6. The procedure of SMP mechanisms

4. Secure Message Protocol 설계

제시된 보안서비스 구현 메카니즘의 처리 절차와 공개키 관리를 위하여 공개키 certificate를 저장하고 있는 디렉토리 서버를 이용하여 송수신측 사용자들 간에 메시지를 안전하게 주고 받기 위한 SMP(Secure Message Protocol)를 다음과 같이 정의하였다.

1) 송신측

단계 1 : 일방향 hashing함수를 사용하여 hashing 값(HV)을 계산한 후

HV=H(Info)

$X = A_s(HV)$

디렉토리시스템내의 CA에게 A와 B의 공개키 certificate를 요청한다.

단계 2 : CA는 CA의 비밀키(CA_s)로 서명한 후 certificate를 A에게 보낸다.

$CA\ll B\gg = CA_s(AI, CA, T1, B, B_p)$

$CA\ll A\gg = CA_s(AI, CA, T2, A, A_p)$

단계 3 : A는 미리 알고 있던 CA의 공개키로서 복호화하여 시간 T1을 조사한 후, B의 공개키(B_p)를 얻는다.

$AI, CA, T1, B, B_p = CA_p(CA\ll B\gg)$

단계 4 : 난수(UK)를 발생시켜 메시지의 내용을 암호화시킨 후 이 UK를 B의 공개키로 암호화한다.

$C = UK(Info)$

$G = B_p(UK)$

단계 5 : 보안에 필요한 데이터를 메시지 내용위의 Header에 부가시킨 후 MTS로 보냄으로써 송신절차를 완료한다.

2) 수신측

단계 1 : 수신측(B)는 미리 알고 있던 CA의 공개키로 A의 certificate를 복호화한다.

$AI, CA, T2, A, A_p = CA_p(CA\ll A\gg)$

여기서 시간 T2를 조사하여 이상이 없다면 A의 공개키를 취한다.

단계 2 : A의 공개키를 이용하여 전자서명된 X를 복호화한다.

$HV = Ap(X)$

단계 3 : B의 비밀키로서 암호화된 사용자키 정보(G)를 복호화하고,

$UK = B_s(G)$

이 UK를 이용하여 암호화된 메시지 내용을 복호화한다.

$Info' = UK(C)$

단계 4 : 복호화된 메시지 내용(Info')에 Hashing 함수를 수행하여 HV'를 구하고,

$HV' = H(Info')$

이 HV'를 단계 2에서의 HV와 비교하여 같다면 메시지 무결성과 발신처 인증이 입증된다.

Ⅳ. 구 현

앞에서 설계된 SMP를 4.3 BSD UNIX운영체제의 Mail S/W(usr/src/ucb/mail)에 3가지 보안서비스를 수행할 수 있는 메카니즘을 삽입하였으며 SMP 절차에 따라 송수신이 이루어질 수 있도록 구현하였다[9][10][11].

또한 directory시스템의 certificate 정보는 동일 시스템 내에서 Test하였으나 certificate 생성 및 제거와 여기에 사용되는 비밀키 안전성은 본 연구대상에서 제외하였다.

본 시스템에서는 MTA로서 UNIX시스템이 제공하고 있는 SMTP(Simple Mail Transfer protocol)를 이용하고 있는데, 이 SMTP는 전송시 7비트 ASCII부호만 전송시키므로 암호화시 나오는 8비트 ASCII부호의 처음 1비트의 유지 문제와 암호화시 발생되는 특수문자로 인하여 메시지의 내용이 화면에 출력 불가능한 문제가 발생하게 된다.

따라서 본 구현시 이러한 문제점을 해결하기 위하여 3개의 문자를 4개의 문자로 확장할 수 있도록 부호화시켰으며 이때 출력가능한 문자로 변환되도록 구현하였다.

동 연구에서 구현된 보안 메카니즘을 거쳐 수신측으로 발송되는 메시지의 형태는 그림 7의 한 예와 같이 암호화 처리가 된 메시지 내용에 보안에 관련된 정보가 헤더에 부가된 메시지 형태를 갖고 있다.

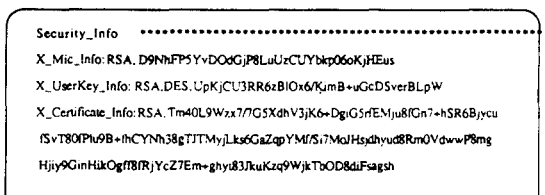


그림 7. 정보보호 서비스가 수행된 메시지의 일예
Fig 7. The example of Protected message content

이 그림에서 보듯이 UK를 B의 공개키로 암호화한 결과가 메시지 header의 "X_Userkey_Info"필드에 나타나 있으며 전체 메시지가 hashing 함수를 거쳐 A의 비밀키로 전자서명을 한 결과가 "X_Mic_Info" 필드에 나타나 있다. 이것은 메시지 무결성과 데이터 발신처 인증에 필요한 정보이다.

또한 송신측 공개키를 보내기 위한 certificate정보는 "X_Certificate_Info"에 나타나 있다. 이 certificate가 수신측에서 유효한 것으로 판정되면 이 정보로 부터 송신측의 공개키를 추출할 수 있으며 이 공개키를 사용하여 "X_Mic_Info"를 복호화하는데 사용한다. 이때 복호화된 내용이 hashing 값(HV)이 된다.

사용자키는 "X-UserKey_Info" 필드의 정보를 수신측의 비밀키로 복호화함으로써 얻을 수 있으며, 이 사용자 키를 사용하여 송신시 암호화되어 있는 메시지 내용을 복호화하게 한다. 이 복호화된 메시지 내용을 다시 송신측과 동일한 hashing함수를 거치게 하여 생성한 내용(HV')과 앞에서 복호화된 Mic내용(HV)을 비교함으로써 메시지 내용의 무결성과 데이터 발신처 인증을 수행할 수 있다.

설계된 SMP를 UNIX시스템에 구현하여 이 3가지 보안서비스를 전부 처리하여 수신측에 보내는데 약 5초의 시간이 소요되었는데, 그 이유는 RSA 암호알고리즘 자체의 많은 계산량 이외에도, 보안성을 고려하여 키의 길이를 512비트로 하였을 분만아니라 S/W로 구현하였기 때문이다. 따라서 처리성능을 개선시키기 위해서는 공개키 암호시스템을 하드웨어화 시키거나 처리속도가 빠른 암호 알고리즘을 선택하여 사용하여야 할 것으로 사료된다.

또한 메시지의 전체 길이는 원래 메시지 보다 약 20%가 증가하였는데 그 이유는 UNIX시스템의 SMTP 프로토콜상에서 발생되는 문제와 화면에 출력 불가능한 문제점을 해결하기 위하여 8비트를 6비트로 부호화한 관계로 인하여 발생하였으므로 이 문제는 MHS시스템상에서 수행한다면 일어나지 않을 것으로 판단된다.

본 논문에서는 구현한 시스템의 성능을 분석하기 위해 RSA 암호 알고리즘의 p, q의 크기를 각각 256bit로 하여 n을 512bit로 하였다. 그리고 메시지의 용량을 각각 임의로 1kbyte, 3kbyte 두 경우에 대해 송, 수신에 소요되는 평균 시간을 측정한 결과, 표 3과 같았다.

이 표3에서 보듯이 메시지의 용량에는 소요 시간이 큰 영향을 받지 않는데 이는 메시지의 내용을 비밀화하는데는 대칭키 방식인 DES 알고리즘을 채택하였기 때문이며 시간이 많이 소요되는 비대칭 방식인 RSA 알고리즘은 단지 짧은 MIC 코드부분만 수행하도록 하였기 때문이다. 그리고 송신시나 수신시의 소요 시간이 비슷한 것은 처리시간에 큰 영향을 미치는 RSA 알고리즘의 암호화 과정과 복호화 과정이 송신측과 수신측에서 1번씩은 일어나므로 비슷한 시간이 소요된다.

표 3. 메세지크기에 따른 보안서비스 수행시간
Table 3. Execution time of Security Service depending on message size

소요시간 / 메세지크기	송신시(sec)		수신시(sec)	
	e=32	d=512	e=512	d=32
1k	13		14	
2k	15		17	

그러나, 이러한 처리시간에 있어서 성능문제는 전자우편 시스템 자체가 forward-and-store 특성을 가지고 있으므로, 메시지를 매우 빨리 상대방에게 전달한다든지 매우 빠르게 수신된 내용을 볼 경우는 극히 적으며 전자 메시지의 평균 용량 역시 약 2kbyte 정도의 적은 양이므로 큰 문제가 되지 않을 것으로 생각된다. 또한 컴퓨터 시스템의 성능향상과 더불어 암호화 기능의 하드웨어적 구현에 의해 보다 빠른 처리 속도를 향후 기대할 수 있을 것으로 판단된다[12][13].

V. 결 론

본 논문에서는 MHS시스템에서의 여러가지 보안서비스중 메시지 비밀보장, 메시지 내용의 무결성, 데이터 발신처 인증서비스를 1단계로 선정하여 certificate를 이용한 키관리를 수행하는 SMP프로토콜을 제시하였으며 제시된 프로토콜을 UNIX에 있는 Mail 소프트웨어에 구현하였다.

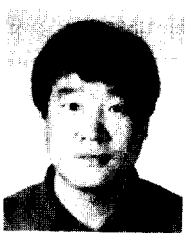
구현된 보안서비스는 불법 사용자의 메시지 불법 노출 문제, 메시지 내용의 불법 수정과 발신자의 인증문제 등으로 부터 정보를 보호할 수 있을 뿐만아니라, UA측에서 제공가능한 부인봉쇄서비스를 비롯한 보안서비스로의 확장에도 효율적으로 구현가능하도록 하였다. 현재 본 논문에서 구현된 3가지 서비스에 부가하여 부인봉쇄서비스를 제공하기 위한 확장작업을 진행하고 있다.

그러나 본 프로토콜은 공개키 암호알고리즘으로서 RSA 사용과 S/W로만 구현되었기 때문에 처리시간에 문제점을 안고 있어, 효율적인 메시지전송 서비스의 제공을 위한 암호화 모듈의 하드웨어적 접근과 보다 효율적인 암호알고리즘에 관한 연구가 병행되어야 할 것이다.

향후, X.509에 제시된 여러 노드를 통과할 때 발생되는 certification path에 의거한 공개키 관리 방법과 저장된 메시지의 불법 사용자 접근을 막기 위한 접근제어(Access Control)메카니즘 및 session 연결시의 대등실체 인증(Peer Entity Authentication) 등에 관한 보안서비스에 대한 연구도 진행되어야 할 것이다.

참 고 문 헌

1. CCITT, Recommendation X.400~X.430, Data Communication Networks Message Handling Systems, Geneva, 1989
2. ISO, 7498/2 Security Architecture, Information Processing System-Open System Interconnection Reference Model, 1984
3. CCITT, Recommendation X.509, The Directory-Authentication Framework, Geneva, 1989
4. 차경돈, 홍기융, 김동규, "Secure MHS를 위한 무인봉쇄 서비스," 통신정보보호학술발표 논문집 Vol.1, No.1, 1990
5. U.S.NBS, Data Encryption Standard, FIPS PUB.46 National Bureau of Standard U.S. Departent of Commerce, 1977.1
6. Rivest, R., The MD4 Message Digest Algorithm(REC 1186), October 1990
7. Rivest, R., Shamir, A., Adleman.L, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM 21(2), pp120~126, 1978.2
8. Joseph J.Tardo, Kannan Alagappa, "SPX : Global Authentication Using Public Key Certificates," IEEE Security & Privacy Symposium, 1991.5
9. Kent, S., Linn, J., "Privacy Enhancement for Internet Electronic Mail," Internet Activities Board Privacy Task Force, 1989.8
10. Kurt Shoens, Mail Reference Manual, UC Berkeley, 1983
11. Bart Anderson, Harry Henderson, UNIX Communications, Howard W.SAMS Company, 1987
12. Naoto Sone외 2인, "Application to Electronic Mail of Public-key Cryptosystem and it's consideration," 일본전자정보통신학회(ISEC 91-44)
13. 원유재외 2인, "E-mail에서 public-key 크립토시스템을 이용한 사용자 메시지 보호," 정보통신연구회 동계컴퓨터통신워크샵, 1990



李 亨 洙(Hyung Soo Lee) 정회원
1957년 12월 28일생
1980년 : 경북대학교 공학사(전자공학)
1986년 : 인제대학교 공학석사(전자계산)
1992년~현재 : 성균관대학교 정보공학과 박사과정
1983년~현재 : 한국전자통신연구소 선임연구원
※주관심분야 : 네트워크 보안, 데이타 통신, 무선 통신망 설계

丁 仙 伊(Sunny Jung) 정회원
1981년 2월 : 한국항공대학 통신공학과 학사
1991년 2월 : 성균관대학교 정보공학과 석사
1991년 3월~현재 : 성균관대학교 정보공학과 박사과정 재학중
1981년 2월~1988년 10월 : 월간 전자과학 편집장
※주관심분야 : 네트워크 보안, 고속무선 통신프로토콜

鄭 鎭 旭(Jin Wook Chung) 정회원
1974년 2월 : 성균관대학교 전기공학과 학사
1979년 2월 : 성균관대학교 전자공학과 석사
1991년 2월 : 서울대학교 계산통계학과 박사
1973년 9월~1981년 12월 : 한국과학기술연구소 연구원
1982년 1월~1985년 2월 : 한국과학기술연구소 실장
1981년 9월~1982년 8월 : Racal-Milgo Co. 객원연구원
1985년 3월~현재 : 성균관대학교 교수
1992년 1월~1993년 1월 : 미국 Maryland대 객원교수
※주관심분야 : 네트워크 보안, 네트워크 관리, 고속 및 무선 통신 프로토콜