Secure MHS를 위한 부인봉쇄 서비스

차 경 돈*, 홍 기 웅**, 김 동 규*
* 아주대학교 전자계산학과 ** 한국전자통신연구소

The Non-Repudiation Service for Secure Message Handling System

Kyung-Don Cha*, Ki-Yoong Hong**, Dong-Kyoo Kim*
* Dept. of Computer Science, Ajou Univ. ** ETRI

요 약

컴퓨터가 널리 보급되고 정보통신 기술이 발전함에 따라 지리적으로 먼거리에 있는 사람에게 정보를 주고받을 수 있게 되었는데, 안전한 데이타의 송수신은 그 중요성이 더해가고 있다. 이런 시점에서 ISO가 OSI 환경에서 안전성 제공을 위해 IS 7498-2로 발표한 OSI Security Architecture에서는 5가지 안전성 서비스를 제공하였다. 본 논문에서는 이들 중 이미 발생한 통신 사실을 부인할 수 없도록 하는 부인봉쇄 서비스를 제공할 수 있는 부인봉쇄 서비스 구현 모델을 MHS(Message Handling System)상에 설계하였으며, 구현방안을 제시하였다.

I. 서론

컴퓨터의 보급이 확산되고 사무자동화 시대로 나아감에 따라 MHS의 필요성은 절실해 졌으며 실제로 컴퓨터 시스템 혹은 업체별로 여러 방식의 MHS가 개발되어 사용되고 있다.

MHS는 Store-and-Forward 방식의 전자우편(Electronic Mail) 서비스를 제공해주는 시스템으로[3,10], 다른 일반적인 네트워크 응용 서비스에서 안전성 서비스들이 필요하듯이 MHS에서도 안전성 서비스의 필요성이 증가하게 되었다. 필요한 안전성 서비스는 ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) JTC1/SC21에서 발표한 OSI(Open Systems Interconnection) Security Architecture (ISO 7498-2) 내에 정의된 신분확인 (Authentication/Identification) 서비스, 액세스 제어(Access Control) 서비스, 데이타 무결성 (Data Integrity) 서비스, 데이타 비밀성(Data Confidentiality) 서비스,

그리고 부인봉쇄(Non- Repudiation) 서비스 등이 있다[16]. 따라서 본 논문에서는 안전한 MHS를 구현하기 위한 방편으로 이러한 안전성 서비스중 이미 발생한 통신 사실을 부인할 수 없도록 하기 위한 부인봉쇄 서비스를 제공할 수 있는 모델을 설계하였으며, 구현방안을 모색해 보았다.

Ⅱ. MHS에서의 부인봉쇄(Non-Repudiation) 서비스 개념

1. 개요

OSI 응용계층(Application Layer)의 특정 응용 서비스 요소 (SASE : Specific Application Service Element)중 MHS(Message Handling System)는 Real Time 내에 직접적으로 통신하는 대등실체 통신(예 : FTAM, VT 등)과 달리 Store-and-Forward 방식의 전자우편 서비스를 제공해 주는 시스템이다[3,10].

이러한 MHS는 일반적인 문서처리와 마찬가지로 어떤 전문을 컴퓨터 통신망을 통하여 전송하였을 때, 수신자가 고의적으로 전문 내용을 자신에게 이롭도록 고칠 수도 있고, 또 비양심적인 송신자가 전문을 보내지 않았다고 부인하거나 혹은 전문 내용을 수신자가 위조해서 자신이 보낸 내용과 틀리다고 주장하면 결국 송신자와 수신자 사이에 분쟁이 발생하게 되며 이를 근본적으로 해결할 방법이 필요하다.

이와 같은 문제를 해결하기 위해 이미 발생한 통신 사실을 부인할 수 없도록 하는 것을 부인봉쇄라 하며, 발신부인봉쇄와 수신부인봉쇄로 나눠진다[18].

① 발신부인봉쇄 (Non-Repudiation of Origin) : 전송된 데이타나 내용에 대한 발신사실을 부인할 수 없게 한다.

② 수신부인봉쇄 (Non-Repudiation of Delivery) : 수신된 데이타나 내용에 대한 수신 사실을 부인할 수 없게 한다.

본 논문에서는 MHS환경에 부인봉쇄 서비스를 제공하기 위해 새로운 형태의 안전성 서비스 요소를 OSI 7계층 중 응용계층에 두었는데, 이는 현재의 안전성 표준화 동향이 응용계층에 안전성 기능들을 위치시키려는 경향이 강하며 부인봉쇄 서비스는 그 성격상 응용계층에서만 제공 가능하기 때문이다[16].

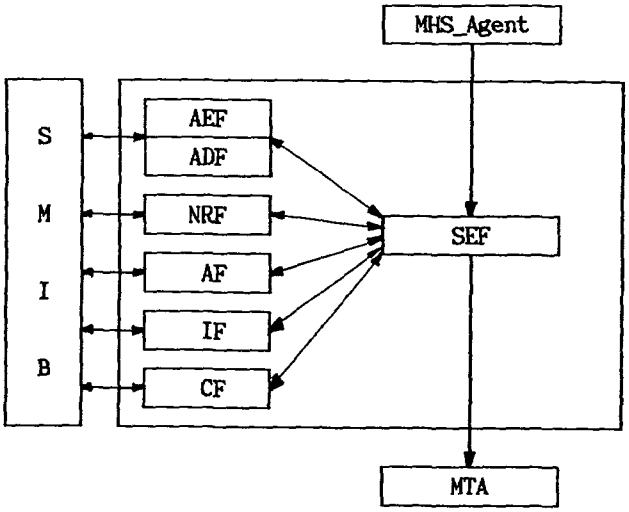
2. MHS_SSE의 구성

본 논문에서 제안한 MHS_SSE(MHS_Security Service Element) 모델에서도 ECMA와 ISO/IEC JTC1/SC21/WG6 에서 제안한 안전성을 논리적으로 완전하게 분해한 기능적인 요소, 즉 안전성 서비스의 최소 단위인 *Facility*의 개념을 사용하고 있으며[19], 이 Facility들이 서로 결합하여 하나의 응용 서비스 요소를 구성하게 된다.

그림 1.에서는 이러한 MHS_SSE의 구조에 대해 나타내고 있다.

3. 부인봉쇄 메카니즘

부인봉쇄 서비스를 제공하기 위한 메카니즘으로는 디지탈 서명, 데이타 무결성과 공증을 들 수 있다[16].



⊙ SMIB : Secure Management Information Base
⊙ AEF : Access Control Enforcement Facility
⊙ ADF : Access Control Decision Facility
⊙ NRF : Non-Repudiation Facility
⊙ AF : Authentication Facility
⊙ IF : Integrity Facility
⊙ CF : Confidentiality Facility
⊙ SEF : Security Enforcement Facility

그림 1. MHS_Security Service Element의 구조

(1) 디지탈 서명 (Digital Signature)

이 메카니즘의 요체는 비밀키를 사용하지 않고서는 데이타 전문을 생성할 수 없다는 사실을 이용하는 것이다[9]. 이것은 세가지 조건으로 대별할 수 있다.

① 제삼자 조건 : 비밀키의 소지자가 아닌 어느 누구도 서명된 데이타 단위를 생성할 수 없다.

② 수신자 조건 : 수신자는 서명 데이타 단위를 생성할 수 없다.

③ 송신자 조건 : 송신자는 서명 데이타 단위를 송신하였음을 부인할 수 없다.

직접서명은 제삼자 조건과 수신자 조건으로 구성된다. 서명 데이타가 수신되면 공개되어 있는 정보(Public-Key)를 사용하여 서명자를 확인할 수 있다. 서명자는 해당 비밀키의 소지자이어야 한다.

중재서명은 송신자 조건이 추가로 관련된다. 이 경우는 신뢰성있는 제삼자가 데이타의 정확성과 송신자 신분을 수신자에게 증명한다. 이를 위해서는 디지탈 서명과 공증 (Notarization) 메카니즘이 결합되어야 한다.

(2) 데이타 무결성(Data Integrity)

데이타 무결성은 Checksum과 Sequencing (Timestamping)을 사용하여 전송된 데이타가 사고

혹은 고의로 수정 되지 않았음을 확인하기 위한 것으로, 내용의 정확성을 점검하는 내용무결성(Context Integrity)과 전송되는 전문의 순서를 점검하는 순서무결성(Sequence Integrity)으로 나누어볼 수 있다. 내용무결성을 위해서는 전송되는 PDU (Protocol Data Unit)에 전문에 대한 특정값(예 : MDC, MAC)을 추가하고 수신측이 이를 확인함에 의해 수정, 삽입, 제거, 재전송을 막을 수 있다. 순서무결성을 위해서는 전송되는 PDU에 전문의 순서번호를 부여함으로써 전문의 순서전도 공격을 검출할 수 있게 한다.

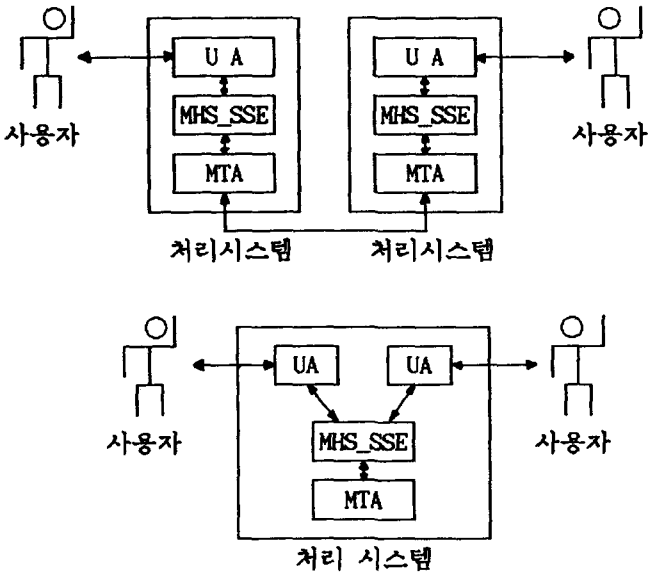
(3) 공증(Notarization)

안전성 서비스를 제공하는데 있어 송신자와 수신자가 아닌 제삼자의 위치에 있는 중재자의 개입을 통하도록 한다. 이는 보통 디지탈 서명 메카니즘과 함께 사용되며 송신사실의 부인과 수신사실의 부인을 봉쇄하는데 필요하다[18].

Ⅲ. 부인봉쇄 서비스의 설계와 구현방안

1. 구현환경 및 적용모델

부인봉쇄 서비스를 MHS에 적용하여 구현하기 위해 본 논문에서는 MHS_SSE(MHS_Security Service Element)를 제안 하였으며, IF(Integrity Facility)와 CF(Confidentiality Facility)로부터 데이타 비밀성과 무결성 서비스를 제공 받도록 하였다. 그림 2.에서는 안전한 MHS를 위해 MHS_SSE를 적용한 MHS의 기능적인 개념을 나타내었으며, 그림 3.에서는 MHS와 접속시킨 부인봉쇄 서비스의 구현 모델을 나타내었다.



⊙ UA : User Agent ⊙ MTA : Message Transfer Agent
⊙ MHS_SSE : MHS_Security Service Element

그림 2. 안전한 MHS의 기능적 개념

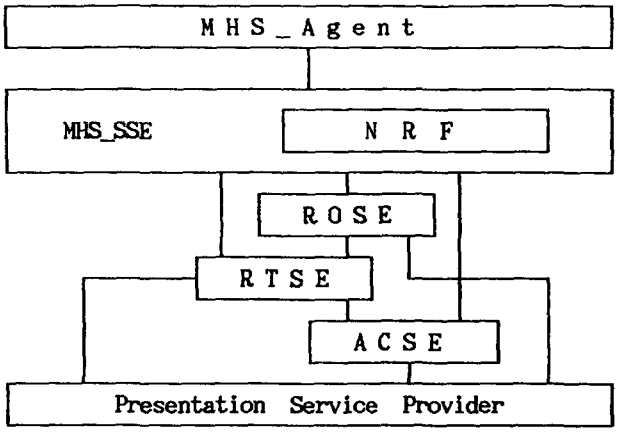


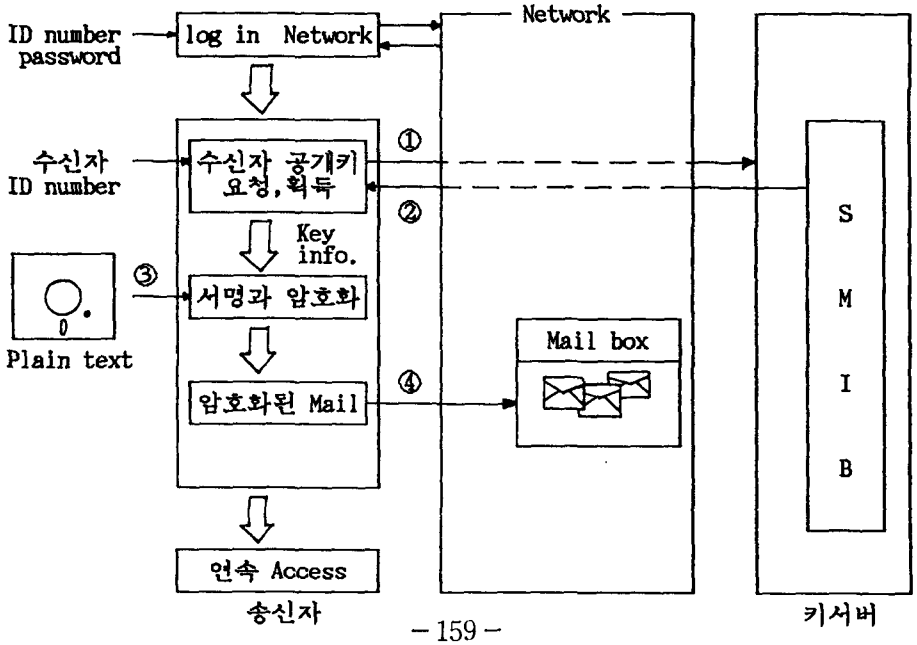
그림 3. 부인봉쇄 서비스 구현 모델

2. 부인봉쇄 서비스의 수행절차

NRF(Non-Repudiation Facility)를 구현하기 위해 필요한 수행절차는 다음과 같다.

(1) 송신자 부인봉쇄의 수행

송신자는 수신자에게 Mail을 전송하고자 할 경우에 디지탈 서명을 이용하여 서명된 전문 단위를 생성하고, 이를 수신자의 공개키로 암호화하여 전송한다. 서명된 전문은 송신자만이 생성할 수 있으므로 송신자의 송신사실 부인을 막을 수 있다. 그림 4.에서는 송신자 부인봉쇄의 수행절차에 관하여 나타내었다.



Step 1 : 송신자는 송신하고자 하는 상대방의 공개키가 자신의 SMIB내에 없을 경우 수신자의 공개키(P_R)를 키서버에게 요청한다. 자신의 SMIB내에 수신자의 공개키가 있는 경우에는 키서버에게 키의 요청없이 Step 3을 실행한다.

Step 2 : 키서버는 자신의 Directory(SMIB)내에 있는 수신자의 공개키를 송신자에게 분배한다.

Step 3 : 송신자는 Message Digest Algorithm(Hash Function)을 통해 전문(Plain Text)에 대한 축소문 m을 구한후, 이 m을 자신의 비밀키(S_S)로 서명하여 전문(Plain Text)에 덧붙여 수신자의 공개키(P_R)로 암호화 한다. 즉,

$$m = MD(\text{Plain Text})$$

$$C_1 = P_R(\text{ Plain Text} + S_S(m))$$

Step 4 : 송신자는 Mail C_1을 네트워크를 통해 수신자측에 전송한다(이 Mail은 네트워크내의 System Mail box 내에 저장됨).

Step 5 : 수신측에서는 수신자가 Mail을 액세스할 때 자신의 비밀키(S_R)를 이용해 암호전문을 해독함으로써 전문(Plain Text)과 서명 데이타단위를 취할 수 있다. 서명 데이타단위를 송신자의 공개키(Ps)를 이용하여 m을 유추해 냄으로써 송신자의 송신사실 부인을 막을 수 있다(서명된 전문단위는 비밀키의 소지자만이 생성할 수 있으므로). 또한, 후에 송신자가 전문의 위조 여부를 문제삼을 경우에 수신자는 전문(Plain Text)을 Message Digest Algorithm을 통해 m'를 구한후 이 m'와 유추해낸 m을 비교함으로써 해결할 수 있다.

그림 4. 송신자 부인봉쇄 수행 절차

(2)수신자 부인봉쇄의 수행

수신자가 System Mail box로부터 Mail을 취하고자 할 경우 Mail의 Envelope 부분을 송신자에게 전송하도록 함으로써 Mail에 대한 액세스 권한을 주고 Kernel에 이 사실을 등록해 놓음으로써 수신자의 수신사실 부인을 막을 수 있다. 이것은 일반적인 등기 우편의 경우에서처럼 우편 수취시 수취인의 도장을 찍어야만 우편을 수취할 수 있는 것과 같은 이치이다.

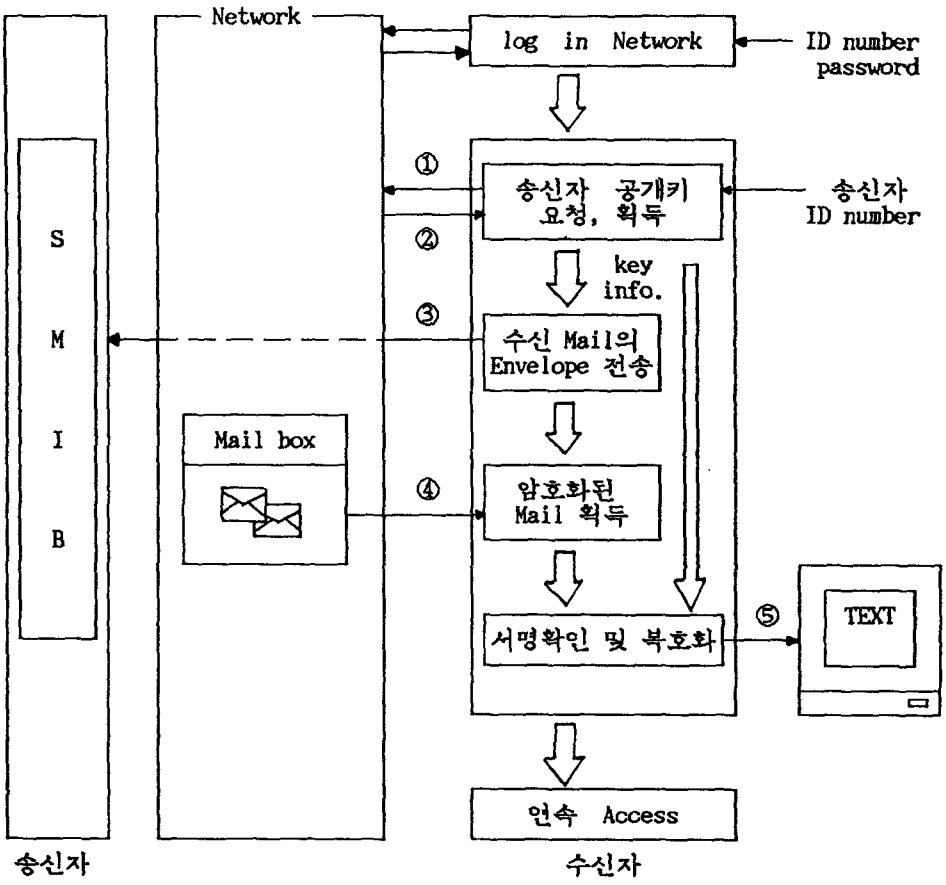
그림 5.에서는 이러한 수신자 부인봉쇄의 과정을 나타내었다.

Step 1 : 수신자는 수신된 Mail의 송신자에 대한 공개키가 자신의 SMIB 내에 없을 경우 키서버에게 송신자의 공개키를 요청하게 된다. 자신의 SMIB 내에 송신자의 공개키가 있을 경우에는 키서버에게 키의 요청없이 Step 3을 실행한다.

Step 2 : 키서버는 자신의 Directory(SMIB) 내에 있는 송신자의 공개키를 수신자에게 분배한다.

Step 3 : 수신자는 송신자의 Mail을 액세스 하고자 할 경우 Mail의 Envelope(E) 부분을 자신의 비밀키로 서명하고, 송신자의 공개키로 암호화(C_2) 하여 송신자에게 전송한다. 이 사실을 Kernel상의 Log File에 등록함으로써 Mail에 대한 액세스 권한을 갖게된다.

$$C_2 = P_S(\ S_R(E)\ )$$



Step 4 : Step 3을 통해 수신자는 암호화된 Mail을 획득한다.

Step 5 : 암호화된 Mail을 자신의 비밀키와 송신자의 공개키를 이용하여 송신자의 서명을 확인하고 Mail을 복호화 한다.

Step 6 : 송신측에서는 수신자가 수신사실을 부인할 경우 Kernel상의 Log File을 이용하여 수신사실을 부인할 수 없도록 한다.

그림 5. 수신자 부인봉쇄 수행 절차

이상에서 살펴본 절차들을 통합하여 개괄적으로 나타내면 그림 6.과 같다.

먼저 송신자와 수신자는 각각 상대방의 공개키를 키서버로부터 분배받아야 한다(①,②번 과정). 송신자는 수신자에게 전문을 전송하기 위해 자신의 ID와 수신자의 ID, 그리고 전문(Message)을 UA(User Agent)를 통해 Mail System에 제공한다(③번과정). Mail System 내의 SEF(Security Enforcement Facility)는 필요한 서비스를 선택하여 부인봉쇄 서비스를 요청할 경우 NRF(Non-Repudiation Facility)를 호출하게 된다. NRF는 이 요청에 대해 우선 Message Digest Algorithm을 통해 전문의 축소문 m을 구하고, 자신의 SMIB(Secure Management Information Base)내에 저장되어있는 정보를 이용하여 전송을 위한 암호화된 Mail C_1을 MTA(Message

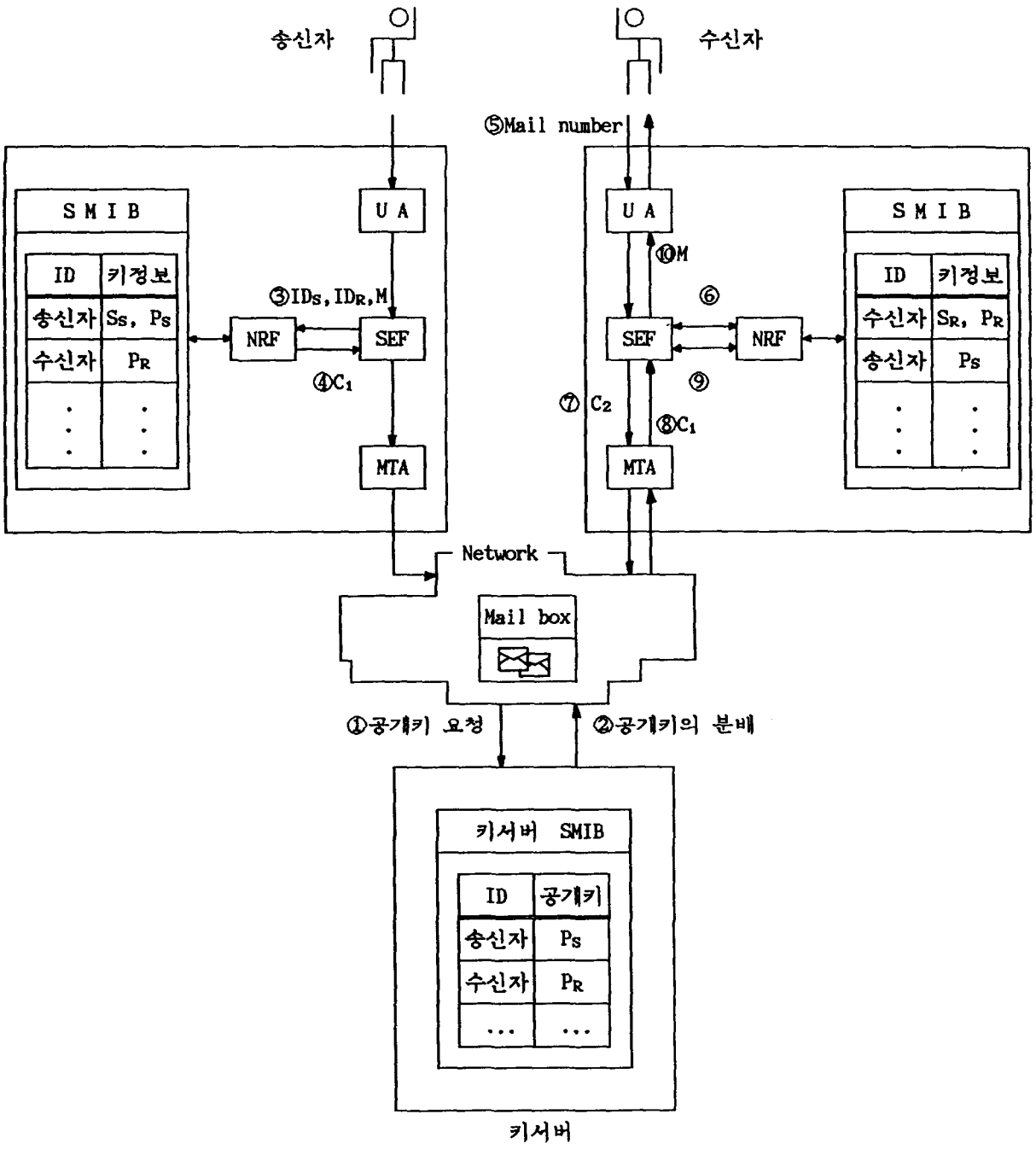


그림 6. 부인봉쇄 서비스의 수행

Transfer Agent)를 통해 네트워크 내의 System Mail box로 전송한다(④번과정).

Mail을 수신하기 위해 수신자측에서는 Mail box에 저장되어 있는 Mail들 중에서 액세스하고자 하는 Mail의 번호를 선택한다(⑤번과정). SEF는 필요한 서비스를 선택하여 부인봉쇄를 요청할 경우 NRF를 호출한다. NRF는 SMIB내에 저장되어 있는 정보를 이용하여 선택한 Mail에

대한 액세스 권한을 받기위해 C_2전문을 생성하여 SEF에게 넘겨준다(⑥번과정).

SEF는 C_2전문을 MTA를 통해 송신자에게 전송하며, 또한 이 사실을 Kernel상의 Log File에 등록한다(⑦번과정). 이때 Kernel은 수신자에게 선택한 Mail에 대한 액세스 권한을 부여한다.

액세스 권한을 부여받은 수신자는 Mail C_1을 취하여(⑧번과정) NRF를 통해 암호화된 Mail의 해독을 요청한다(⑨번과정).

NRF는 SMIB 내의 키정보를 이용해 암호화된 Mail을 해독하여 전문을 SEF에게 넘겨주며, SEF는 이 전문 M을 UA를 통해 수신자에게 제공한다(⑩번과정).

이와같은 과정을 통해 후에 송신사실과 수신사실의 부인 문제가 발생할 경우 각 사용자들은 서명된 전문단위와 Kernel상의 Log File을 이용하여 해결할 수 있다.

Ⅳ. 결론

점점 일반화 되어가는 정보통신 환경에서 불법적인 내용의 유출이나 비자격자의 네트워크 액세스, 그리고 불법적인 사용자에 의한 내용과 순서의 변경 등과 같은 여러가지 안전성 문제들이 두각되게 되었다. 이러한 안전성 문제들은 MHS나 EDI(Electronic Data Interchange)와 같은 전자우편 서비스에서도 예외없이 발생하며, 따라서 이러한 안전성 문제들을 해결하기 위한 필요성이 대두되게 되었다.

본 논문에서는 안전성 문제들을 해결하기 위해 Secure MHS를 구현하기 위한 방편으로 ISO/IEC JTC1/SC21에서 정의한 안전성 서비스 중 이미 발생한 통신 사실을 부인할 수 없도록 하는 부인봉쇄 서비스를 제공할 수 있는 구현모델을 설계하였으며, 부인봉쇄 서비스의 수행절차를 기술함으로써 구현방안을 모색 하였다.

[참고문헌]

[1] Bransted, K.Dennis, *"Consideration for Security in the OSI Architecture,"* IEEE Network Magazine, 1987.

[2] C.H.Meyer, S.M.Matyas, *"Cryptography : A New Dimension in Computer Data Security,"* John Wiley & Sons, 1983.

[3] C.Mitchell, M.Walker and D.Rush, *"CCITT/ISO Standards for Secure Message Handling,"* IEEE Journal on Selected Areas in Comm., Vol.7, No.4, May, 1989.

[4] D.W.Davies, *"Applying the RSA Digital Signature to Electronic Mail,"* IEEE Comm. Magazine, Feb., 1983.

[5] D.W.Davies, M.Hellman, *"Security for Computer Network,"* 2nd Ed. John Wiley & Sons, 1989.

[6] John Linn, Stephen T.Kent, *"Privacy for Darpa-Internet Mail,"* 12th NCSC, PP.215 - 229, 1989.

[7] Kazue Tanaka and Eiji Okamoto, *"Key Distribution System for Mail Systems Using ID-Related Information Directory,"* Computers & Security Vol.10, No.1, 1991.

[8] Ki Yoong Hong, Kyung Don Cha, Yun Hee Cheong and Dong Kyoo Kim, *"An Access Control Service for Secure Message Handling,"* '91 JWCC, July, 1991.

[9] S.G.Akl, *"Digital Signatures : A Tutorial Survey,"* Computer Vol.16, No.2, Feb. 1983

[10] Uyless Black, *"OSI A Model For Computer Communications Standards,"* Prentice-Hall, 1991.

[11] CCITT, Recommendation X.400, *"Message Handling : System and Service Overview"*

[12] CCITT, Recommendation X.402, *"Message Handling Systems : Overall Architecture"*

[13] CCITT, Recommendation X.411, *"Message Handling Systems : Message Transfer System Abstract Service Definition and Procedures"*

[14] CCITT, Recommendation X.500, *"The Directory - Overview of Concepts, Models, and Services"*

[15] CCITT, Recommendation X.509, *"The Directory - Authentication Framework"*

[16] *"ISO 7498/2 Part 2 to ISO 7498 on Security Architecture,"* ISO/TC97/SC21/WG1, 1987.

[17] Natinal Computer Security Center, *"Department of Defense Trusted Computer System Evaluation Criteria,"* U.S. Department of Defense, DoD 5200.28-STD, 1985

[18] *"Revised Working Draft - Non-Repudiation Framework,"* ISO/IEC JTC1/SC21, May 30, 1991.

[19] *"Security framework for the Application layer of open systems,"* ECMA/TC32/87/282, Dec,1987.

[20] 차경돈, 김동규, "OSI 환경에서 부인봉쇄 서비스에 관한 연구", 한국정보과학회 '91 봄 학술발표논문집 Vol.18 No.1, PP.183-186, 1991.4.

[21] 김동규, 차경돈 외, "OSI 통신망 구조에서의 네트워크 안전체제 연구", 과학기술처 최종 보고서 (3차 년도), 아주대, 1991.6.