通信情報保護學會論文誌
第4卷 第2號, 1994. 12

메세지 처리 시스템의 안전한 정보 흐름을 위한 네트워크 액세스 제어 메카니즘의 설계

홍 기 융*, 임 병 렬**, 김 동 규***

A Design of Network Access Control Mechanism for Secure Information Flow of Message Handling System

Ki Yoong Hong*, Byung Ryul Lim**, Dong Kyoo Kim***

요 약

전자 우편(E-Mail)이나 메세지 처리 시스템(MHS : Message handling System)과 같은 축적 후 전송(Store-and-Forward) 방식의 네트워크 시스템에서 다중 등급의 기밀성을 갖는 메세지를 처리하고자 할 때 중요한 메세지의 내용이 누출되거나 또는 허가되지 않은 자가 메세지를 액세스할 수 있는 안전성 문제의 해결이 중요하다.

본 논문에서는 다중 등급 메세지의 보호를 위하여 요구되는 네트워크 보안 정책을 임의적 액세스 제어, 보안 레이블, 레이블 무결성, 강제적 액세스 제어, 그리고 최소 권한 정책 측면에서 제시하였다. 정의한 보안 정책을 만족하는 보안 특성 함수와 보안 오퍼레이션을 기반으로 하여 안전한 MHS을 위한 네트워크 액세스 제어 메카니즘과 그 구조를 설계하였다. 제안한 액세스 제어 메카니즘은 네트워크상에서 중요한 메세지의 불법적인 액세스 또는 불안전한(Insecure) 정보 흐름의 보호문제를 해결한다.

Abstract

On the network system using store-and-forward scheme such as E-Mail and MHS (Message Handling System), it is recognized as an important thing to solve the security problems that are the disclosure of the sensitive message contents and the illegal access of the message by unauthorized person.

In this paper, a network security policy for the protection of multilevel secure message is presented from the view points of discretionary access control, security label, label

* 종신회원, 한국전자통신연구소
** 정 회 원, 아주대학교 컴퓨터공학과
*** 종신회원, 아주대학교 컴퓨터공학과

integrity policy, mandatory access control policy, and least privilege policies. We give a formal design of network access control mechanism and its architecture for secure MHS based on the derived security properties and security operations to enforce the defined security policy. The proposed access control mechanism provides a solution of security problems such as illegal access on sensitive message and insecure information flow.

Key words: Access Control, Message Handling System, Multilevel Security

1. 서 론

서로 다른 등급의 기밀성(sensitivity)을 갖는 다수의 컴퓨터 시스템으로 구성된 네트워크 환경에서 보안 요구사항은 중요한 고려사항으로 인식되어야 한다. 일반적으로 네트워크 상에는 안전한 시스템(Trusted Systems)과 안전하지 못한 시스템(Untrusted System)들이 함께 존재한다. 컴퓨터 시스템 보안을 위하여 미 국방성(U.S DoD)은 보안정책(Security Policy), 표시(Marking), 식별(Identification), 기록성(Accountability), 보증(Assurance), 그리고 연속적 보호(Continuous Protection)의 기본적인 6가지 보안 요구사항을 제시하였으며 이 국방성 산하의 국가 컴퓨터 보안 센터(DoD NCSC: National Computer Security Center)는 컴퓨터 시스템의 보안 요구사항과 평가 등급에 대한 보안 평가 지침서(TCSEC : Trusted Computer System Evaluation Criteria)를 제시하였고 이 보안 평가 지침서를 기준으로 하여 많은 컴퓨터 시스템들이 개발되었다[1,16]. 하지만 여러 다른 네트워크들과의 상호 접속이 증가하고 있는 오늘날의 상황에서 안전한 컴퓨터 시스템 자체만으로 네트워크 보안에 대한 해결책을 제공하기에는 불충분하다. 비록 컴퓨터 시스템이 안전하다고할지라도 통신 프로토콜의 근본적인 속성으로 인하여 컴퓨터 네트워크상에는 여전히 다른 측면의 위험 요소들이 존재한다. 컴퓨터 네트워크상에서 정보 보호를 위하여 NIST, NCSC, ISO/OSI, CCITT, ECMA, 그리고 IEEE등의 기관에서 보안 서비스와 메카니즘에 대한 많은 논의와 그 연구가 진행되고 있다[1,2,3,4,5,6,8,9,10,11,12,13]. 또한, NCSC는 TCSEC의 평가개념을 네트워크 시스템에 확장 해석한 TNI(Trusted Network Interpretation)를 통하여 통신 무결성(Communication Integrity), 서비스 거절(Denial of Service), 그리고 전송 보안(Transmission Security)등의 추가적인 보안 서비스 개념을 제시하였다[2]. OSI는 ISO 7498/2 보안 구조(Security Architecture)를 통하여 보안 위협요소와 많은 개방형 시스템들간에 사용될 수 있는 보안 서비스 및 기법에 대하여 논하였으며, CCITT는 메세지 처리 시스템 보안에 대하여 CCITT X.400 MHS 권고안을 통하여 안전한 액세스 관리(Secure Access Management and Administration)와 안전한 메세지 처리(Secure Messaging)의 2가지 측면에서 기술하고 있다[3,4,5,8,12,13]. 그러나, 안전한 메세지 처리를 위해 X.400에서 보안기능들을 정의하고는 있으나 이를 위한 명백한 모델이나 또는 메카니즘을 제공하고 있지는 못하다. PEM(Privacy Enhanced Mail)과 같은 경우에도 암호화를 통해서만 메세지를 보호할 뿐 액세스 제어에 대해서는 아직 고려하고 있지 않은 실정이다[6,7,13,15]. 그러나 이와같은 축적후 전송(Store-and-Forward) 방식의 메세지처리 시스템에서도 정보에 대한 불법적인 액세스를 방지하기 위하여 정보의 흐름을 안전하게 제어할 필요성이 있다.

본 논문에서는 메세지 처리 시스템에서의 정보 흐름 제어를 가능케하는 다중 기밀 등급 네트워크 액세스 제어 메카니즘을 제안한다. 이를 위하여 다중 기밀 등급을 다루기 위한 보안정책이 정의되

며, 이 정책은 임의적 액세스 제어, 강제적 액세스 제어, 레이블, 최소 권한 정책 측면의 보안 요구사항들로 구성된다. 또한, 보안 정책을 만족하는 보안 특성 함수와 보안 오퍼레이션을 정의하였으며 이를 이용하여 액세스 제어 메카니즘과 그 구조에 대한 설계를 정형적으로 제시한다.

2. MHS 보안 개념

MHS에 대한 보안 위협은 위장, 메세지 순서 변경, 정보의 변조, 서비스 거부, 정보 누출, 그리고 서비스 부인 등의 다양한 형태로 나타날 수 있다. X.400 권고안에서는 MHS의 보안을 위하여 두가지 측면을 기술하고 있는데 이들은 안전한 액세스 관리 측면과 안전한 메세지 처리 측면이다[13,8,12,14]. 안전한 액세스 관리를 위한 능력(capabilities)들은 이웃한 구성요소간에 인증된 제휴의 설립과 보안 파라미터들의 설정을 지원한다. 이 능력들은 MHS에서 어떤 쌍을 이루는 구성요소, 즉, UA/MTA, MTA/MTA, 그리고 MS/MTA 등에 적용될 수 있다. MHS의 보안 서비스들은 메세지 제출, 전송, 그리고 배달 동작에서 파라미터들을 사용하는 보안 특징에 의해 제공된다. 이들 파라미터들은 서비스와 서비스를 제공하기 위해 채택된 선택에 의존하여 메세지 봉투 또는 토큰내에 분리된 아규먼트와 같이 전송된다. [8]에서는 발신-수신 간의 보안 서비스를 제공하기 위해 사용될 수 있는 많은 보안 특징들과 투명적으로 파라미터들을 전송하기 위해 사용되는 MTS에 관해 기술하고 있다. 이들 보안 서비스에 대한 기능적인 개요는 X.400 권고안에 제시된 바 있다[13,8,12]. NIST는 MHS 보안 기능 그룹을 여섯 개의 보안 클래스(S0, S0A, S1, S2A, S2B, 그리고 S3)로 기술하고 있다[11]. 대칭 또는 비대칭 기법들은 각 보안 클래스 내에 사용될 수 있고, 등록된 알고리즘 식별자에 의해 식별된다. TCSEC의 보안 레이블과 같은 의미의 보안 레이블과 안전한 액세스 관리는 보안클래스 S1, S2A, S2B, 그리고 S3를 위해 사용되는 것으로 정의된다. 이들 보안클래스는 MTA, MS, 그리고 UA의 다중등급 보안을 제공하기 위해 보안 측정을 요구한다. 안전한 액세스 관리는 다양한 MHS 구성 요소들이 다중 등급 보안을 지원하도록 보장함으로 다중 등급 보안 서비스가 구현될 수 있도록 한다. 이와 같이 CCITT와 NIST 등의 MHS 보안 기능 정의는 표준화에 따르는 개념적이고 추상화된 내용으로 기술된 것이므로 보다 정형화된 보안 정책의 제시가 필요하며 제시된 보안 정책을 만족하는 보안 메카니즘의 설계 및 구현이 수반되어야 한다.

3. MHS를 위한 보안 정책

3.1 용어 정의

본 절에서는 보안 정책을 기술하기 위하여 필요한 용어를 다음과 같이 정의한다.

- 사용자(User)

  사용자는 컴퓨터 및 네트워크 시스템을 통하여 MHS를 사용하는 사람으로서 메세지의 송신자(Originator) 또는 수신자(Recipient)이다. 컴퓨터 및 네트워크를 사용하는 각 사용자에게는 허가된 보안 자격(Security Clearance)이 부여되어야 한다. 이 자격은 네트워크 보안 관리자에 의하여 안전하게 관리되어야 한다.

- 사용자 ID(UID)

  사용자 ID는 네트워크 사용자를 식별할 수 있는 유일한 ID 정보이다. 사용자 ID는 일반적으로 문자열의 형태로 주어질 수 있다. 각 송신자 또는 수신자는 메세지를 송수신하기 위하여 자신의 ID를 갖는다.

- 주체(Subject)

  주체는 사용자에게 MHS 서비스를 제공하기

위하여 동작하는 프로세스 또는 실체(Entity)를 의미한다. 본 논문에서 주체는 MHS의 구성 요소인 UA(User Agent), MTA(Message Transfer Agent), 그리고 MS(Message Store)로 정의한다.

- 메세지 객체(Object)

  메세지 객체는 네트워크상에서 MHS에 의하여 처리 및 전송되는 메세지를 의미한다. 메세지 객체에게는 보안 레이블이 부여되는데 이 메세지 객체의 보안 레이블은 메세지의 내용에 대한 기밀성(Sensitivity)을 나타낸다. 한 메세지 객체가 생성될 때에는 이 메세지 객체를 생성한 주체의 보안 레이블이 그 메세지 객체에게 부여된다.

- 메세지 스풀(Spool) 객체

  메세지 스풀 객체는 제출, 전송, 그리고 배달 과정 중에 있는 메세지들을 저장하는 메모리 공간을 의미한다. 메세지 스풀 객체에게는 보안 레이블이 부여된다.

- 보안 등급(Security Level)

  보안 등급은 TopSecret, Secret, Confidential, 그리고 Unclassified 등과 같은 기밀성을 나타내는 계층적 분류를 의미한다. 예를 들면, 보안 등급간의 내재된 의미는 다음과 같이 표현할 수 있다.

  (보안 등급 예) TopSecret 〉 Secret 〉 Confidential 〉 Unclassified

  위의 (예)에서 TopSecret는 다른 세 개의 보안 등급에 비하여 최상의 등급을 갖는다는 것을 알 수 있다.

- 범주(Compartment)

  사용자 또는 주체가 액세스할 수 있는 취급 분야에 대한 기밀성을 나타내는 비계층적 분류를 의미한다. 예를 들면, 사용자 A에게 허가된 보안 등급이 Secret이면서 X 분야의 기밀 정보를 취급할 수 있고 사용자 B에게 허가된 보안 등급은 Secret이나 Y 분야의 기밀 정보를 취급할 수 있고, 또한 객체 O의 보안 등급과 범주는 각각 Secret과 X로 부여되어 있다고 하자. 이때, X와 Y가 서로 같지 않으면 사용자 A는 객체 O를 액세스할 수 있으나 사용자 B는 범주가 서로 다르므로 객체 O를 액세스 할 수 없다.

- 보안 레이블(Security Label)

  사용자와 주체 및 객체의 기밀성을 나타내는 정보로써 보안 등급과 범주의 조합으로 구성된다. 이 보안 레이블은 강제적 액세스 제어 결정을 위한 근간이 되며 모든 주체와 객체에게 반드시 부여되어야 하는 정보이며, 사용자에게 부여되는 보안 자격은 사용자의 보안 레이블임을 의미한다. 보안 레이블의 내용이 NULL인 경우에는 시스템내에서 정의한 보안 등급의 범위중에서 최하의 보안 등급으로 해석하지 않고 최상의 보안 등급보다도 높은 보안 등급의 개념으로 해석한다.

- 현재 보안 레이블(Current Security Label)

  사용자가 시스템을 사용하기 위하여 로그인할 때 사용자는 자신에게 허가된 보안 자격의 범위내에서 현재 보안 레이블을 결정하여야 한다. 사용자의 현재 보안 레이블은 사용자가 시스템내에서 실행하는 모든 오퍼레이션에 대한 강제적 액세스 제어 결정의 근간이 된다.

- 최대 및 최소 보안 레이블(Maximum and Minimum Security Label)

  사용자와 주체에게 부여된 보안 레이블에 대해서 최대와 최소 값이 명시적으로 표현되어야 한다. 사용자의 보안 자격을 부여할 때 네트워크 보안 관리자는 사용자에게 허가된 최대와 최소의 보안 자격을 명시적으로 부여하여야 한다.

● 지배(Dominate)

2개의 보안 레이블간의 관계를 의미한다. 보안 레이블 S1과 S2에 대하여 S1의 보안 등급이 S2의 보안 등급보다 크거나 같고 S1의 범주 집합이 S2의 범주 집합을 포함하는 관계가 성립한다면 보안 레이블 S1은 보안 레이블 S2를 지배한다고 한다.

● 액세스 모드

시스템에서 주체는 다음의 액세스 모드에 의하여 메세지 객체를 액세스 할 수 있다.

▶ 판독 액세스(Read Access)
어느 한 주체가 어느 한 메세지 객체에 대하여 판독 액세스를 가지고 있을 때 그 주체는 메세지 객체내의 내용(또는 데이타)을 얻을 수 있다. 그러므로 판독 액세스를 가지고 있지 않은 주체는 메세지 객체에 대하여 판독 행위를 실행할 수 없다.

▶ 기록 액세스(Write Access)
어느 한 주체가 어느 한 메세지 객체에 대하여 기록 액세스를 가지고 있을 때 그 주체는 메세지 객체에 대하여 내용(또는 데이타)을 기록할 수 있다. 그러므로 쓰기 액세스를 가지지 않은 주체는 메세지 객체에 대하여 쓰기 행위를 실행할 수 없다. 기록 액세스 권한은 시스템에서 어느 한 메세지 객체를 생성하거나 제거할 때에도 요구된다.

▶ 삭제 액세스(Delete Access)
어느 한 주체가 어느 한 메세지 객체에 대하여 삭제 액세스를 가지고 있을 때 그 주체는 메세지 객체를 삭제할 수 있다. 그러므로 삭제 액세스를 가지고 있지 않은 주체는 메세지 객체에 대하여 삭제 행위를 실행할 수 없다.

● 오퍼레이션

오퍼레이션은 어느 한 주체가 어느 한 객체에 대하여 취할 수 있는 함수를 의미한다. 시스템 구성의 확장이나 또는 특정의 네트워크 응용을 위하여 부가적인 오퍼레이션을 보안 정책에 정의할 수 있다. 다음의 오퍼레이션들은 안전한 메세지 처리를 위하여 본 논문에서 정의하고자 하는 기본적인 것들로 이들 함수에 대한 정형적인 기술은 4.3절에서 정의한다.

▶ Login
이 Login 함수는 사용자가 시스템을 사용하기 위하여 로그인할 수 있도록 한다.

▶ CreateMsg
이 CreateMsg 함수는 어느 한 주체가 어느 한 메세지 객체를 생성할 수 있도록 한다.

▶ ReadMsg
이 ReadMsg 함수는 어느 한 주체가 어느 한 메세지 객체를 읽을 수 있도록 한다.

▶ WriteMsg
이 WriteMsg 함수는 어느 한 주체가 어느 한 메세지 객체를 기록, 변경, 또는 첨가할 수 있도록 한다.

▶ DeleteMsg
이 DeleteMsg 함수는 어느 한 주체가 어느 한 메세지 객체를 삭제할 수 있도록 한다.

▶ Bind
이 Bind 함수는 MHS내에서 어느 한 주체가 다른 한 주체에 대하여 바인드할 수 있도록 한다.

▶ Submit
이 Submit 함수는 어느 한 주체가 어느 한 메세지 객체를 제출할 수 있도록 한다. 이 함수는 UA 또는 MS가 어느 한 메세지 객체(즉, 메세지의 내용과 제출 봉투(Submission Envelope))를 MTA에게 제출하기 위하여 사용된다.

▶ Transfer
이 Transfer 함수는 MHS내에서 어느 한

MTA가 다른 MTA에게 메세지 객체를 전송할 수 있도록 한다. 이것은 어느 한 MTA가 다른 MTA에게 메세지의 내용과 전송 봉투(Transfer Envelope)를 전송하는 하나의 방법을 제공한다. 전송 봉투는 MTS의 오퍼레이션에 관련된 정보와 송신 UA에 의하여 요청된 서비스 요소를 제공하기 위하여 MTS가 요구하는 정보를 포함하고 있다.

▶ Deliver

이 DELIVER 함수는 주체가 메세지 객체를 수신자에게 배달할 수 있도록 한다. 이것은 MTA가 메세지의 내용과 배달 봉투(Deliver Envelope)를 UA나 또는 MS에게로 전송하는 것을 의미한다. 배달 봉투는 메세지의 배달에 관련된 정보를 포함한다.

▶ SetSbjLabel

이 SetSbjLabel 함수는 주체가 자신의 현재 보안 레이블을 사용자에게 허가된 보안 등급의 범위내에서 현재 보안 레이블보다 낮거나 또는 높은 등급의 보안 레이블로 변경할 수 있도록 한다.

▶ SetObjLabel

이 SetObjLabel 함수는 주체가 메세지 객체의 보안 레이블을 사용자에게 허가된 보안등급의 범위내에서 현재 객체에게 할당된 보안 레이블보다 낮거나 또는 높은 등급의 보안 레이블로 변경할 수 있도록 한다.

3.2 보안정책

본 절에서는 네트워크상에서 전송되는 다중 등급 메세지의 안전한 정보 흐름 제어를 위하여 필요한 보안 정책을 제시한다. 보안 정책은 임의적 액세스 제어 정책, 보안 레이블 정책, 레이블 무결성 정책, 강제적 액세스 제어 정책, 그리고 최소권한 정책들로 구성된다.

1) 임의적 액세스 제어 정책 (DAC : Discretionary Access Control)

다음의 사항들은 임의적 액세스 제어 정책을 기술한다.

● 〈보안 규정-1〉 메세지 객체의 소유권(Ownership) 부여 규정

모든 메세지 객체에게는 반드시 소유권(Ownership)이 부여되어야 한다. 소유권은 네트워크상에 등록된 사용자의 ID로 인식된다.

● 〈보안 규정-2〉 소유권 상속 규정

어느 한 메세지 객체가 생성될 때 그 객체에게는 반드시 객체를 생성한 사용자의 ID와 동일한 소유권이 부여되어야 한다.

● 〈보안 규정-3〉 소유권 변경 규정

소유권을 갖는 사용자는 그 객체에 대한 임의적 액세스 권한을 임의적(Discretionary)으로 변경할 수 있는 권한을 가진다.

● 〈보안 규정-4〉 메세지 객체의 생성시 액세스 제어 리스트(ACL) 부여 규정

어느 한 메세지 객체가 생성될때 그 객체에게는 반드시 하나의 액세스 제어 리스트(ACL : Access Control List)가 부여되며 이때의 ACL의 내용은 NULL로 초기화되어야 한다. 임의적 액세스 제어 결정은 이 ACL에 의하여 이루어지는데 어느 한 메세지 객체에 대한 ACL의 내용은 오직 그 메세지 객체의 소유자가 설정, 추가, 또는 변경할 수 있다. NULL로 초기화된 ACL은 소유자외의 어떠한 주체도 이 메세지 객체를 액세스할 수 없다고 하는 강한 의미를 갖는다.

● 〈보안 규정-5〉 임의적 액세스 권한 규정

어느 한 주체는 단지 다음의 경우를 만족하는 경우에만 어느 한 객체를 원하는 액세스 모드로 액세스 할 수 있다.

① 액세스하고자 하는 액세스 모드가 액세스 모드 집합에 정의되어 있다.

② 액세스하고자 하는 액세스 모드가 액세스하고자 하는 객체의 ACL에 명시되어 있다.

임의적 액세스 제어 결정은 위에서 기술한 〈보안 규정 1, 2, 3, 4, 5〉를 근간으로 하여 이루어진다. ACL에 대한 액세스 모드는 오직 객체의 소유자나 또는 네트워크 보안 관리자와 같은 권한이 부여된 사용자에 의해서만 초기화되거나 새로운 액세스 모드로 변경될 수 있다. 초기화되어 비어있는 ACL은 어떠한 주체가 그 객체에 대하여 어떠한 액세스도 얻어낼 수 없음을 의미한다.

2) 보안 레이블 정책

각 주체와 객체에게는 보안 등급을 식별할 수 있도록 하기 위하여 반드시 자신에게 해당된 보안 레이블이 부여되어야 한다. 이것은 MHS의 각 요소에 대하여 적합한 보안 레이블이 부여되어야 함을 의미한다. 이 보안 레이블은 강제적 액세스 제어 결정을 위하여 사용된다. 다음의 사항들은 보안 레이블 정책에 대하여 기술한 것이다.

- 〈보안 규정-6〉 보안 레이블 소유 규정

  사용자, 주체, 그리고 객체는 반드시 자신에게 허가된 보안 레이블을 소유하고 있어야 한다. 사용자와 주체에게는 보안 레이블의 최소와 최대 값이 명시적으로 허가 및 할당되어야 하며 시스템내에서 안전하게 유지되어야 한다.

- 〈보안 규정-7〉 사용자의 보안 레이블 상속 규정

  어느 한 주체가 생성될때, 그 주체를 생성(또는, 실행)한 사용자의 현재 보안 레이블과 최대 및 최소 보안 레이블 정보들은 생성된 주체에게 상속되어 부여되어야 한다. 그러므로 생성된 주체의 현재 보안 레이블, 최대 보안 레이블, 그리고 최소 보안 레이블들은 주체를 생성한 사용자의 것들과 각각 동등한 것이 되어야 한다.

- 〈보안 규정-8〉 주체의 보안 레이블 상속 규정

  어느 한 객체가 생성될때, 그 객체를 생성한 주체의 현재 보안 레이블과 동일한 보안 레이블이 생성된 객체에게 상속되어 부여되어야 한다.

- 〈보안 규정-9〉 사용자의 보안 레이블 변경 금지 규정

  사용자는 사용자 자신의 보안 레이블을 변경할 수 없다.

- 〈보안 규정-10〉 주체의 보안 레이블 변경금지 규정

  사용자는 주체의 보안 레이블을 변경할 수 없다. 또한, 주체는 자신의 보안 레이블을 변경할 수 없다.

- 〈보안 규정-11〉 객체의 보안 레이블 변경 금지 규정

  사용자는 객체의 보안 레이블을 변경할 수 없다. 또한, 주체는 객체의 보안 레이블을 변경할 수 없다.

- 〈보안 규정-12〉 보안 레이블의 보안 등급 소유 규정

  어느 한 사용자나 주체 또는 객체의 보안 레이블은 단일 등급(Single Level)의 보안 등급을 가질 수도 있으며 또한 다중 등급(Multilevel)의 보안 등급을 가질 수도 있다. 다중 등급 보안(MLS : Multilevel Security)의 경우에는 최대와 최소 보안 레이블에 의하여 그 허가된 범위가 명시적으로 유지된다.

3) 레이블 무결성(Label Integrity)정책

주체와 객체에 부여된 보안 레이블에 대한 무결성 정책은 다음과 같다.

● 〈보안 규정-13〉 보안 레이블의 보안 등급 정확성 규정

네트워크 시스템과 MHS내에서 보안 레이블은 주체나 또는 객체의 보안 등급을 정확하게 표현하고 있어야 한다.

● 〈보안 규정-14〉 메세지 객체의 보안 레이블 정확성 규정

네트워크상에서 외부로 전송중인 메세지 객체에 대해서도 그 기밀성이 정확하게 표현될 수 있도록 하기 위하여 보안 레이블이 부여되어야 한다.

4) 강제적 액세스 제어 정책

강제적 액세스 제어 정책은 낮은 보안 등급을 갖는 MHS 사용자 또는 주체(즉, MHS agent)를 통하여 높은 등급의 기밀 정보가 유출되는 것을 보호하기 위하여 시행되어야 한다. 주체의 객체에 대한 모든 액세스들은 다음의 강제적 액세스 정책으로 통제되어야 한다.

● 〈보안 규정-15〉 판독 액세스 규정

주체의 현재 보안 레이블이 객체의 보안 레이블을 지배하는 경우에만 주체는 객체를 판독할 수 있다.

● 〈보안 규정-16〉 기록 액세스 규정

객체의 현재 보안 레이블이 주체의 보안 레이블을 지배하는 경우에만 주체는 객체에 대하여 기록할 수 있다.

● 〈보안 규정-17〉 삭제 액세스 규정

주체의 현재 보안 레이블과 메세지 객체의 보안 레이블이 서로 같으며 주체의 현재 보안 레이블과 메세지 객체를 저장하고 있는 메세지 스풀의 보안 레이블이 서로 같은 경우에만 주체는 객체를 삭제할 수 있다.

● 〈보안 규정-18〉 접속 규정

MHS내에서 각 구성 요소(즉, MHS-agents : UA, MTA, MS)들간에 상호 접속하기 위해서는 반드시 양자의 현재 보안 레이블이 서로 같아야 한다. 이는 다중 등급을 갖는 구성 요소들간에 예기치 않은 정보의 흐름을 방지하기 위한 것이다.

● 〈보안 규정-19〉 메세지 제출 규정

주체(즉, 사용자 또는 송신 UA)는 다음의 조건들을 모두 만족하는 경우에만 대응 실체인 주체(즉, MTA)에게 메세지를 제출할 수 있다.

① 주체의 현재 보안 레이블은 제출하고자 하는 메세지의 보안 레이블과 같다.

② 수신자의 보안 자격은 메세지의 보안 레이블을 지배한다.

③ 제출 주체의 현재 보안 레이블과 이에 대응하는 대등 실체인 주체의 현재 보안 레이블은 같다.

● 〈보안 규정-20 : 메세지 전송 규정〉

주체(즉, MTA)는 다음의 조건들을 모두 만족하는 경우에만 이와 대응하는 대등 실체인 다른 주체(즉, MTA)에게 메세지 객체를 전송할 수 있다.

① 송신 주체의 현재 보안 레이블과 수신 주체의 현재 보안 레이블은 서로 같다.

② 송신 주체의 현재 보안 레이블은 메세지 객체의 보안 레이블과 같다.

● 〈보안 규정-21〉 메세지 배달 규정

주체(즉, MTA)는 다음의 조건들을 모두 만족하는 경우에만 다른 주체(즉, UA나 또는 MS)에게 메세지 객체를 배달할 수 있다.

① 배달 주체의 현재 보안 레이블은 수신 주체의 현재 보안 레이블과 같다.

② 배달 주체의 현재 보안 레이블은 메세지의 보안 레이블과 같다.

③ 수신자의 보안 자격은 메세지의 보안 레이블을 지배한다.

5) 최소 권한(Least Privilege) 정책

권한(Privilege)이란 제한된 서비스를 실행할 수 있는 능력을 의미한다. 즉, 어느 한 사용자 또는 주체는 제한된 서비스를 실행하기 위하여 필요한 능력인 권한을 반드시 소유하여야 한다. 최소 권한은 주체가 객체에 대하여 수행할 행위를 최소한으로 제한하기 위하여 필요하다. 이러한 최소 권한 정책을 시행함으로써 각 사용자들에게 모든 권한들을 주지 않고서도 각 사용자 및 주체에게 보안 관리적인 작업의 분배·할당 및 책임의 부여가 가능케 된다. 다음에서 기술한 권한들은 본 논문에서 정의하고자 하는 것으로 강제적 액세스 제어 및 레이블 정책을 위하여 요구되는 최소한의 것 들이다.

- 〈보안 규정-22〉 권한 부여 규정

  사용자와 주체에게는 오직 네트워크 보안 관리자에 의해서 권한이 부여되어야 한다. 아무런 권한이 부여되지 않는 사용자나 주체는 특정의 제한된 서비스를 실행할 수 없다.

- 〈보안 규정-23〉 사용자의 권한 상속 규정

  사용자가 시스템에 로그인할 때 사용자를 대신하여 최초로 생성된 주체에게는 사용자에게 허가된 권한 집합이 상속된다.

- 〈보안 규정-24〉 유효 권한(Effective Privilege) 부여 규정

  어느 한 주체에 의해서 다른 하나의 주체가 실행될 때 이들 두 주체에게 부여된 권한 집합의 공통권한 집합만이 실행될 주체에게 할당되어야 한다. 즉, 이 공통 권한 집합만이 오직 주체가 실행할 때 권한으로써 유효한 것이 되며 최소 권한 정책을 만족시키는 근간이 된다.

- 〈보안 규정-25〉 메세지 제출 권한 (PRIV_MSG_SUBMIT) 규정

  어느 한 사용자 또는 주체가 어느 한 메세지 객체에 대하여 제출 권한을 가지고 있을 때 그 주체는 메세지 객체를 제출할 수 있다. 그러므로 제출 권한이 허가되지 않은 주체는 메세지 객체를 제출할 수 없다. 이 제출 액세스는 UA나 또는 MS가 MTA에게 메세지를 제출하기 위하여 필요한 최소한의 권한이다.

- 〈보안 규정-26〉 메세지 전송 권한 (PRIV_MSG_TRANSFER) 규정

  어느 한 사용자 또는 주체가 어느 한 메세지 객체에 대하여 전송 권한을 가지고 있을 때 그 주체는 메세지 객체를 전송할 수 있다. 그러므로 전송 권한이 허가되지 않은 주체는 메세지 객체를 전송할 수 없다. 이 전송 권한은 어느 한 MTA가 다른 MTA에게 메세지를 전송하기 위하여 필요한 최소한의 권한이다.

- 〈보안 규정-27〉 메세지 배달 권한 (PRIV_MSG_DELIVER) 규정

  어느 한 사용자 또는 주체가 어느 한 메세지 객체에 대하여 배달 권한을 가지고 있을 때 그 주체는 메세지 객체를 배달할 수 있다. 그러므로 배달 권한이 허가되지 않은 주체는 메세지 객체를 배달할 수 없다. 이 배달 권한은 어느 한 MTA가 다른 MTA에게 메세지를 배달하기 위하여 필요한 최소한의 권한이다.

- 〈보안 규정-28〉 주체의 보안 레이블 변경 권한(PRIV_MAC_RELABEL_SBJ) 규정

  이 권한은 어느 한 사용자 또는 주체가 주체 또는 주체 자신의 현재 보안 레이블을 변경할 수 없다고 하는 보안 규정에 제한을 받지 않고 주체의 현재 보안 레이블을 변경할 수 있도록 하는 최소한의 권한이다. 단, 현재 보안 레이

블의 변경은 사용자에게 허가된 보안 레이블의 범위내에서만 가능하다.

- 〈보안 규정-29〉 객체의 보안 레이블 변경 권한(PRIV_MAC_RELABEL_OBJ) 규정

  이 권한은 어느 한 사용자 또는 주체가 객체의 보안 레이블을 수정할 수 없다고 하는 보안 규정에 제한을 받지 않고 객체의 보안 레이블을 변경할 수 있도록 하는 최소한의 권한이다. 단, 보안 레이블의 변경은 사용자에게 허가된 보안 레이블의 범위내에서만 가능하다.

4. 네트워크 액세스 제어 메카니즘 설계

본 장에서는 제 3장에서 기술한 보안 정책을 만족하는 네트워크 액세스 제어 메카니즘을 제안한다. 먼저 네트워크 액세스 제어 메카니즘을 기술하기 위하여 필요한 표기를 정의하고, 보안 특성 함수를 도출하며, 이러한 보안 특성 함수를 만족하는 안전한 오퍼레이션을 설계한다. 이들을 이용하여 네트워크 액세스 제어 메카니즘을 정형적으로 기술한다.

4.1 표기 정의

- 사용자의 집합(USET : User Set)

  USET는 네트워크상에 존재하는 모든 사용자들의 집합이다.

- 주체의 집합(SSET : Subject Set)

  SSET는 네트워크상에 존재하는 모든 MHS 주체들의 집합이다. 즉, 집합 SSET는 다음과 같이 정의된다.

  SSET = { UA, MS, MTA }

- 객체의 집합(OSET : Object Set)

  OSET는 네트워크상에 존재하는 모든 메세지 객체들의 집합을 의미하며 주체의 집합을 포함한다. 즉, 집합 OSET과 SSET사이에는 다음과 같은 관계가 성립한다.

  OSET ⊃ SSET

- 메세지 스풀(MSPOOL : Message Spool)

  메세지 스풀 MSPOOL는 MHS 서비스를 위하여 네트워크상에 존재하는 메세지 저장 스풀이다.

- 권한의 집합(PRIVSET : Privilege Set)

  PRIVSET은 사용자 또는 주체에게 허가된 권한의 집합으로 다음과 같이 정의된다.

  PRIVSET = {PRIV_MSG_SUBMIT,
  PRIV_MSG_TRANSFER,
  PRIV_MSG_DELIVER,
  PRIV_MAC_RELABEL_SBJ,
  PRIV_MAC_RELABEL_OBJ}

- 권한 조회(GetPRIV : Get Privilege) 함수

  GetPRIV(X)는 어떤 사용자(또는 주체) X에게 허가된 권한의 집합을 반환한다.

- 유효 권한 조회(GetEPRIV : Get Effective Privilege) 함수

  GetEPRIV (S)는 어떤 주체 S에게 할당된 유효 권한의 집합을 반환한다.

- 권한 저장소($PRIV_s$)

  $PRIV_s$는 주체 S에게 부여된 권한을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 유효 권한 저장소($EPRIV_s$)

  $EPRIV_s$는 주체 S에게 부여된 유효 권한을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 사용자 ID 조회(GetUID) 함수

  GetUID 함수는 사용자 ID를 반환하는 함수이다. 즉, GetUID (U)는 사용자 U에 대한 사용자 ID를 얻어냄을 의미한다.

- 액세스 제어 리스트 조회(GetACL) 함수

  GetACL 함수는 객체의 액세스 제어 리스트를 반

환하는 함수이다. 즉, GetACL(O)는 객체 O에 대한 액세스 제어 리스트를 얻어냄을 의미한다.

- 액세스 제어 리스트 저장소(ACL_O)

  ACL_O는 객체 O에게 부여된 액세스 제어 리스트를 표현 및 저장하기 위하여 할당된 기억장소이다.

- 보안 레이블 조회(GetSL : Get Security Label) 함수

  GetSL 함수는 주체 또는 객체의 보안 레이블을 반환하는 함수이다. 즉, GetSL(X)는 주체(또는 객체) X에 대한 보안 레이블을 얻어냄을 의미한다.

- 현재 보안 레이블 조회(GetCSL : Get Current Security Label) 함수

  GetCSL 함수는 주체의 현재 보안 레이블을 반환하는 함수이다. 즉, GetCSL(S)는 주체 S에 대한 현재 보안 레이블을 얻어냄을 의미한다.

- 최대 보안 레이블 조회(GetMaxSL : Get Maximum Security Label) 함수

  GetMaxSL 함수는 주체에게 부여된 최대 보안 레이블을 반환하는 함수이다. 즉, GetMaxSL(S)는 주체 S에 대한 보안 레이블의 최대 값을 얻어냄을 의미한다.

- 최소 보안 레이블 조회(GetMinSL : Get Minimum Security Label) 함수

  GetMinSL 함수는 주체에게 부여된 최소 보안 레이블을 반환하는 함수이다. 즉, GetMinSL(S)는 주체 S에 대한 보안 레이블의 최소 값을 얻어냄을 의미한다.

- 보안 레이블 저장소(SL_X)

  SL_X는 주체 또는 객체 X에게 부여된 보안 레이블을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 현재 보안 레이블 저장소(CSL_S)

  CSL_S는 주체 또는 객체 S의 현재 보안 레이블을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 최대 보안 레이블 저장소($MaxSL_S$)

  $MaxSL_S$는 주체 S의 최대 보안 레이블을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 최소 보안 레이블 저장소($MinSL_S$)

  $MinSL_S$는 주체 S의 최대 보안 레이블을 표현 및 저장하기 위하여 할당된 기억장소이다.

- 보안 등급(LEVEL) 함수

  LEVEL 함수는 보안 레이블내의 계층적 분류 정보인 보안 등급을 반환하는 함수이다. 즉, LEVEL(A)은 보안 레이블 A에 포함되어 있는 보안 등급을 얻어냄을 의미한다.

- 범주(COM : Compartment) 함수

  COM 함수는 보안 레이블내의 비계층적 분류 정보인 범주를 반환하는 함수이다. 즉, COM(A)은 보안 레이블 A에 포함되어 있는 범주를 얻어냄을 의미한다.

- 지배(dom : dominate) 함수

  dom 함수는 2개의 보안 레이블간의 지배 관계를 나타내는 함수로 2개의 보안 레이블 A1과 A2에 대하여 다음과 같이 정의된다.

$$dom(A1, A2) = \begin{cases} TRUE & \text{if } LEVEL(A1) \geq LEVEL(A2) \text{ .and. } COM(A1) \supseteq COM(A2) \\ FALSE & \text{otherwise} \end{cases}$$

$$eqv(A1, A2) = \begin{cases} TRUE & \text{if } dom(A1,A2) \text{ .and. } dom(A2,A1) \\ FALSE & \text{otherwise} \end{cases}$$

● 액세스 모드의 집합(M)

액세스 모드의 집합은 판독(r) 액세스, 기록(w) 액세스, 그리고 삭제(d) 액세스를 포함하는 집합으로 다음과 같이 정의된다.

$$M = \{ 'r', 'w', 'd' \}$$

4.2 네트워크 액세스 제어를 위한 보안 특성

본 절에서는 네트워크 액세스 제어 메카니즘을 위하여 제시한 보안 정책을 수행하기 위한 보안 특성들을 제안한다. 제안된 보안 특성들은 기존의 BLP(Bell-LaPadula) 모델[16]에서 제시한 단순 보안 특성(simple security property), 스타 보안 특성 (* security property), 그리고 임의적 보안 특성(discretionary security property)을 포함하며, 또한 네트워크 액세스 제어를 위하여 본 논문에서 새롭게 추가한 접속 보안 특성(connect security property), 흐름 보안 특성(flow security property), 단순 일치 보안 특성(simple compatibility security property), 그리고 권한 보안 특성(privilege security property)들로 구성된다.

● 임의적 보안 특성(discretionary security property)

임의적 보안 특성은 액세스 제어 리스트(ACL)와 같은 임의적 액세스 제어 메카니즘을 요구한다. 이 보안 특성은 주체의 객체에 대한 액세스 모드가 객체의 ACL 엔트리에 허가되어 있을 때, 주체가 객체에 액세스할 수 있도록 허용한다. 이 임의적 보안 특성 함수 ds는 다음과 같이 정의한다.

$$ds(S, O, m) = \begin{cases} \text{TRUE} & \text{if } m \in M \text{ .and. } \{S,m\} \in GetACL(O) \\ \text{FALSE} & \text{otherwise} \end{cases}$$

● 단순 보안 특성(simple security property)

이 보안 특성은 주체가 액세스하고자 하는 액세스 모드가 액세스 모드 집합 M에 정의되어 있으며, 또한 주체의 현재 보안 레이블이 객체의 보안 레이블을 지배해야만 객체로의 주체의 판독(r) 액세스를 허용한다. 이 규칙은 다음과 같이 "read-up" 금지 보호를 제공한다. 아래에서 m은 액세스 모드로 'r', 'w', 또는 'd' 어느 것이 되어도 상관이 없다. 다음은 단순 보안 특성 함수 ss를 나타낸 것으로 주체 S와 객체 O간에 주체 S의 현재 보안 레이블이 객체 O의 보안 레이블을 지배하는 관계가 성립한다면 단순 보안 특성을 만족하며 그렇지 않은 경우에는 단순 보안 특성을 만족하지 못한다.

$$ss(S, O, m) = \begin{cases} \text{TRUE} & \text{if } m \in M \text{ .and. } dom(CSL(S), SL(O)) \\ \text{FALSE} & \text{otherwise} \end{cases}$$

● 스타 보안 특성(* security property)

이 보안 특성은 주체의 현재 보안 레이블이 객체의 보안 레이블에 의해 지배된다면 객체로의 주체의 기록(w) 액세스를 허용한다. 이 규칙은 다음과 같이 "write-down" 금지 보호를 제공한다. 다음은 스타 보안 특성 함수 star를 나타낸 것으로, 주체의 객체에 대한 액세스 모드가 판독 액세스이고 주체 S와 객체 O간에 주체 S의 현재 보안 레이블이 객체 O의 보안 레이블을 지배하는 관계가 성립한다면 스타 보안 특성을 만족하며, 주체의 객체에 대한 액세스 모드가 기록 액세스이고 주체 S와 객체 O간

에 객체 O의 보안 레이블이 주체 S의 보안 레이블을 지배하는 관계가 성립한다면 스타 보안 특성을 만족하며, 또한 주체의 객체에 대한 삭제 액세스의 경우에는 주체 및 객체의 보안 레이블이 서로 같아야 한다. 그렇지 않은 경우에는 스타 보안 특성을 만족하지 못한다.

$$star(S, O, m) = \begin{cases} TRUE & \text{if } m = 'r' \text{ .and. } dom(CSL(S), SL(O)) \\ TRUE & \text{if } m = 'w' \text{ .and. } dom(SL(O), CSL(S)) \\ TRUE & \text{if } m = 'd' \text{ .and. } eqv(CSL(S), SL(O)) \\ FALSE & \text{otherwise} \end{cases}$$

이들 기본적인 보안 특성들을 네트워크 환경이 아닌 단일의 컴퓨터 시스템에서의 보안 특성들로 제시된 것이므로 본 논문에서는 이외에 네트워크 액세스 제어 메카니즘을 위하여 다음과 같은 추가적인 보안 특성들을 제안한다.

- 접속 보안 특성(connect security property)

  개시측(Initiator)인 MHS 에이전트의 현재 보안 레이블과 상대측(Target) MHS 에이전트의 보안 레이블의 공통 집합이 개시측 MHS 에이전트의 현재 보안 레이블과 서로같다면 상호 접속이 가능하다. 이 접속 보안 특성은 높은 레이블을 갖는 MHS 에이전트로 부터 낮은 레이블을 갖는 MHS 에이전트로의 접속을 방지하기 위하여 요구된다. 이러한 접속 보안 특성 함수 cs는 다음과 같다. 즉, MHS 에이전트 S1의 현재 보안 레이블에 대하여 MHS 에이전트 S1의 현재 보안 레이블과 MHS 에이전트 S2의 공통 집합이 서로 동등하면 S1은 S2에 대하여 접속 보안 특성을 만족한다.

$$cs(S1, S2) = \begin{cases} TRUE & \text{if } eqv(CSL(S1), CSL(S1) \cap SL(S2)) \\ FALSE & \text{otherwise} \end{cases}$$

- 흐름 보안 특성(flow security property)

  개시측인 MHS 에이전트의 현재 보안 레이블과 상대측 MHS 에이전트의 현재 보안 레이블이 서로 같다면 메세지 객체의 제출, 전송, 또는 배달이 가능하다. 이 흐름 보안 특성은 높은 레이블을 갖는 MHS 에이전트로 부터 낮은 레이블을 갖는 MHS 에이전트로의 불법적인 정보 흐름을 방지하기 위하여 요구된다. 이러한 흐름 보안 특성 함수 fs는 다음과 같다. 즉, MHS 에이전트 S1의 현재 보안 레이블과 MHS 에이전트 S2의 현재 보안 레이블이 서로 동등하면 S1은 S2에 대하여 흐름 보안 특성을 만족한다.

$$fs(S1, S2) = \begin{cases} TRUE & \text{if } eqv(CSL(S1), CSL(S2)) \\ FALSE & \text{otherwise} \end{cases}$$

- 단순 일치 보안 특성(simple compatibility security property)

  단순 일치 보안 특성은 단일 등급의 기밀성을 갖는 메세지 스풀 객체와 단일 등급의 기밀성을 갖는 메세지 객체간의 보안성 관계를 정의한 것으로, 메세지 객체의 보안 레이블과 이들을 저장하는 메세지 스풀의 보안 레이블은 서로 동등해야 함을 의미한다. 이러한 단순 일치

보안 특성 함수 scompat는 다음과 같다. 즉, 메세지 스풀 MSPOOL의 보안 레이블 A와 생성되는 메세지 객체의 보안 레이블 B는 서로 동등하여야 한다. 예를 들면, 기밀성이 Secret인 메세지 기밀성이 Secret인 메세지 스풀에 저장되어야 함을 의미한다.

$$\text{scompat}(A, B) = \begin{cases} \text{TRUE} & \text{if } \text{eqv}(A, B) \\ \text{FALSE} & \text{otherwise} \end{cases}$$

- 권한 보안 특성(privilege security property)

  주체에 대하여 특정 기능이나 서비스를 제한하기 위한 것으로 주체가 제한된 서비스를 실행하기 위해서는 이와 관련된 특정 권한(privilege)을 가져야 한다. 제한된 기능과 이를 실행하기 위하여 필요한 권한 관계는 다음의 〈표 4-1〉에 나타난 바와 같이 정의한다.

제한된 기능	오퍼레이션	오퍼레이션 ID	필요한 권한
1. 바인드	Bind	OP_Bind	PRIV_MAC_RELABEL_SBJ
2. 메세지 제출	Submit	OP_Submit	PRIV_MSG_SUBMIT
3. 메세지 전송	Transfer	OP Transfer	PRIV_MSG_TRANSFER
4. 메세지 배달	Deliver	OP Deliver	PRIV MSG DELIVER
5. 주체의 보안 레이블 변경	ChSbjLabel	OP_ChSbjLabel	PRIV_MAC_RELABEL_SBJ
6. 객체의 보안 레이블 변경	ChObjLabel	OP_ChObjLabel	PRIV_MAC_RELABEL_OBJ

〈표 4-1〉 제한된 기능과 권한

다음은 위의 〈표 4-1〉의 제한된 기능과 권한에 대하여 주체 S가 만족해야 할 권한 보안 특성 함수 pp를 기술한 것이다.

$$\text{pp}(S, OP) = \begin{cases} \text{TRUE} & \text{if } ((OP = OP\_Bind \text{ .and. } PRIV\_MAC\_RELABEL\_SUBJ \in \text{GetPRIV}(S)) \text{ .or.} \\ & \quad (OP = OP\_Submit \text{ .and. } PRIV\_MSG\_SUBMIT \in \text{GetPRIV}(S)) \text{ .or.} \\ & \quad (OP = OP\_Transfer \text{ .and. } PRIV\_MSG\_TRANSFER \in \text{GetPRIV}(S)) \text{ .or.} \\ & \quad (OP = OP\_Deliver \text{ .and. } PRIV\_MSG\_DELIVER \in \text{GetPRIV}(S)) \text{ .or.} \\ & \quad (OP = OP\_ChSbjLabel \text{ .and. } PRIV\_MAC\_RELABEL\_SBJ \in \text{GetPRIV}(S)) \text{ .or.} \\ & \quad (OP = OP\_ChObjLabel \text{ .and. } PRIV\_MAC\_RELABEL\_OBJ \in \text{GetPRIV}(S))) \\ \text{FALSE} & \text{otherwise} \end{cases}$$

이와 같이 본 논문에서 제시한 보안 정책과 보안 특성과의 관계를 요약하여 나타내면 다음의 〈표 4-2〉와 같다. (단, 표에서 기호 '●'의 의미는 관계성이 있음을 의미한다.)

보안 정책 \ 보안 특성		임의적 보안 특성	단순 보안 특성	스타 보안 특성	접속 보안 특성	흐름 보안 특성	단순 일치 보안 특성	권한 보안 특성
DAC	1. 메세지 객체의 소유권 부여 규정	●						
DAC	2. 소유권 상속 규정	●						
DAC	3. 소유권 변경 규정	●						
DAC	4. 메세지 객체의 생성시 액세스 제어 리스트 부여 규정	●						
DAC	5. 임의적 액세스 권한 규정	●						
SL	6. 보안 레이블 소유 규정		●	●	●	●	●	
SL	7. 사용자의 보안 레이블 상속 규정		●	●	●	●	●	
SL	8. 주체의 보안 레이블 상속 규정		●	●	●	●	●	
SL	9. 사용자의 보안 레이블 변경 금지 규정		●	●	●	●	●	●
SL	10. 주체의 보안 레이블 변경 금지 규정		●	●	●	●	●	●
SL	11. 객체의 보안 레이블 변경 금지 규정		●	●	●	●	●	●
SL	12. 보안 레이블의 보안 등급 소유 규정		●	●	●	●	●	
LI	13. 보안 레이블의 보안 등급 정확성 규정		●	●	●	●	●	
LI	14. 메세지 객체의 보안 레이블 정확성 규정		●	●	●	●	●	
MAC	15. 판독 액세스 규정		●	●				
MAC	16. 기록 액세스 규정		●	●			●	
MAC	17. 삭제 액세스 규정		●	●				
MAC	18. 접속 규정				●			
MAC	19. 메세지 제출 규정					●		●
MAC	20. 메세지 전송 규정					●		●
MAC	21. 메세지 배달 규정					●		●
LP	22. 권한 부여 규정							●
LP	23. 사용자의 권한 상속 규정							●
LP	24. 유효 권한 부여 규정							●
LP	25. 메세지 제출 권한 규정							●
LP	26. 메세지 전송 권한 규정							●
LP	27. 메세지 배달 권한 규정							●
LP	28. 주체의 보안 레이블 변경 권한 규정							●
LP	29. 객체의 보안 레이블 변경 권한 규정							●

DAC : Discretionary Access Control
SL : Security Label
LI : Label Integrity
MAC : Mandatory Access Control
LP : Least Privilege

〈표 4-2〉 보안 정책과 보안 특성과의 관계

4.3 보안 오퍼레이션(Security Operation)의 설계

MHS 네트워크 보안을 위하여 오퍼레이션은 보안 정책을 위반하지 않도록 안전하게 설계되어야만 한다. 본 논문에서, MHS 네트워크 보안을 위해서 설계된 오퍼레이션은 Login, CreatMsg, ReadMsg, WriteMsg, DeleteMsg, Bind, Submit, Transfer, Deliver, ChSbjLabel, 그리고 ChObjLabel이며 다음과 같이 정형적으로 기술된다.

- Login 오퍼레이션

Login 오퍼레이션은 사용자 U가 시스템을 사용하기 위하여 실행하는 것으로 다음과 같이 정의된다.

```
Login(U, S, LoginSL)
Begin
   MaxSL_U    ← GetMaxSL(U);
   MinSL_U    ← GetMinSL(U);
   PRIV_U     ← GetPRIV(U);

   if     U ∈ USET .and.
          dom(LoginSL, MinSL_U)
          .and.
          dom(MaxSL_U, LoginSL)
   then   SSET    ← SSET ∪ S;
          EPRIV_S ← PRIV_U;
          CSL_S   ← LoginSL;
          MaxSL_S ← MaxSL_U;
          MinSL_S ← MinSL_U;
   endif
End
```

사용자 U가 네트워크에 로그인하기 위하여 안전한 주체 S를 통하여 보안 레이블 LoginSL 수준으로 로그인 가능하려면 LoginSL은 사용자에게 허가된 보안 자격 범위내의 보안 레이블이어야 한다. 로그인이 성공하면 사용자를 대신하여 실행되는 주체 S는 자신의 현재 보안 레이블, 최대 보안 레이블, 최소 보안 레이블에 대하여 각각 LoginSL, MaxSL_U, MinSL_U가 할당된다. 단, MaxSL_U는 사용자에게 허가된 보안 자격의 최대 보안 레이블 값이며 MinSL_U는 사용자에게 허가된 보안 자격의 최소 보안 레이블 값이다.

- CreateMsg 오퍼레이션

CreateMsg 오퍼레이션은 주체 S가 메세지 객체 O를 생성하기 위한 것으로 다음과 같이 정의된다.

```
CreateMsg(S, O, MSPOOL)
Begin
   CSL_S     ← GetCSL(S);
   SL_MSPOOL ← GetSL(MSPOOL);

   if     S ∈ SSET .and.
          ds(S, MSPOOL, 'w') .and.
          ss(S, MSPOOL, 'w') .and.
          star(S, MSPOOL, 'w') .and.
          scompat(SL_MSPOOL, CSL_S)
   then   OSET ← OSET ∪ O;
          SL_O ← CSL_S;
          ∀S ∈ SSET, ACL_O ← φ;
   endif
End
```

메세지 객체 O가 생성되기 위해서는 주체의 현재 보안 레이블과 메세지 객체가 생성되어 저장되어질 메세지 스풀(MSPOOL)의 보안 레이블이 같아야 한다. CreateMsg 오퍼레이션에 의하여 생선된 메세지 객체 O는 객체의 집합 OSET에 추가되며 생성된 객체 O의 보안 레이블은 주체 S의 현재 보안 레이블로 할당된다. 또한, 모든 객체에 대하여 생성된 객체 O의 액세스 제어 리스트는 공집합이 된다.

- ReadMsg 오퍼레이션

ReadMsg 오퍼레이션은 주체 S가 메세지 객체 O를 읽기하기 위한 것으로 다음과 같이 정의된다.

```
ReadMsg(S,O)
Begin
   if    S ∈ SSET .and.
         O ∈ OSET .and.
         ds(S,O,'r') .and.
         ss(S,O,'r') .and.
         star(S,O,'r')
   then  S reads the contents of O;
   endif
End
```

MHS 사용자는 오직 이 ReadMsg 오퍼레이션을 통하여 메세지를 읽을 수 있다. 이와 같이 주체 S가 메세지 객체 O를 읽기 위하여 요구되는 주체 및 객체간의 보안레이블 관계는 주체의 현재 보안 레이블이 메세지 객체의 보안 레이블을 지배해야 하는 것이다.

- WriteMsg 오퍼레이션

WriteMsg 오퍼레이션은 주체 S가 메세지 객체 O를 기록하기 위한 것으로 첨가 또는 수정에 해당하는 액세스도 이에 포함된다.

```
WriteMsg(S, O)
Begin
   if    S ∈ SSET  .and.
         O ∈ OSET  .and.
         ds(S,O,'w')  .and.
         ss(S,O,'w')  .and.
         star(S,O,'w')
   then  S writes to O;
   endif
End
```

MHS 사용자는 오직 이 WriteMsg 오퍼레이션을 통하여 메세지를 기록할 수 있다. 이와 같이 주체 S가 메세지 객체 O를 기록하기 위하여 요구되는 주체 및 객체간의 보안 레이블 관계는 메세지 객체의 보안 레이블이 주체의 보안 레이블을 지배해야 하는 것이다.

- DeleteMsg 오퍼레이션

DeleteMsg 오퍼레이션은 주체 S가 메세지 객체 O를 삭제하기 위한 것으로 다음과 같이 정의된다.

```
DeleteMsg(S,O)
Begin
   if    S ∈ SSET  .and.
         O ∈ OSET  .and.
         ds(S,O,'d')  .and.
         ss(S,O,'d')  .and.
         star(S,O,'d')  .and.
         ds(S,MSPOOL,'d')  .and.
         ss(S,MSPOOL,'d')  .and.
         star(S,MSPOOL,'d')
   then  OSET ← OSET - O;
   endif
End
```

MHS 사용자는 오직 이 DeleteMsg 오퍼레이션을 통하여 메세지를 삭제할 수 있다. 이와같이 주체 S가 메세지 객체 O를 삭제하기 위하여 요구되는 주체 및 객체간의 보안 레이블 관계는 두 가지 측면에서 고려되어야 한다. 첫째, 주체의 현재 보안 레이블과 객체의 보안 레이블이 서로 같아야 한다. 둘째, 주체의 현재 보안 레이블과 메세지 객체가 저장된 메세지 스풀의 보안 레이블은 서로 같아야 한다.

- Bind 오퍼레이션

Bind 오퍼레이션은 주체 S1이 주체 S2를 바인드하기 위한 것으로 다음과 같이 정의된다.

```
Bind(S1,S2)
Begin
   CSL_S1   ← GetCSL(S1);
   SL_S2    ← GetSL(S2);
   EPRIV_S1 ← GetEPRIV(S1);
   PRIV_S2  ← GetPRIV(S2);

   if    S1,S2 ∈ SSET   .and.
         cs(S1,S2)      .and.
         pp(S1,OP_Bind) .and.
         pp(S2,OP_Bind)
   then  SSET   ← SSET ∪ S2;
         OSET   ← OSET ∪ S2;
         EPRIVs2 ← EPRIV_S1
         ∩ PRIV_S2;
         CSLs2  ← CSL_S1 ∩ SL_S2;
   endif
End
```

주체 S1이 주체 S2를 바인드하기 위해서 S1의 현재 보안 레이블은 S1의 현재 보안 레이블과 S2의 보안 레이블의 공통 집합과 같아야 하며, S1의 유효 권한 집합과 S2의 권한 집합간의 공통 집합은 PRIV_MAC_RELABEL_SUBJ 권한을 포함해야 한다. 바인드 오퍼레이션의 결과로 S2의 유효 권한 집합은 S1의 유효 권한 집합과 S2의 권한 집합간의 공통 집합으로 할당되며, S2의 현재 보안 레이블은 S1의 현재 보안 레이블과 S2의 보안 레이블의 공통 집합으로 할당된다.

● Submit 오퍼레이션

Submit 오퍼레이션은 주체 S1이 수신자 R에게 보낼 메세지 객체 O를 주체 S2에게 제출하기 위한 것으로 다음과 같이 정의된다.

```
Submit(S1,S2,O,R)
Begin
   CSL_S1   ← GetCSL(S1);
   CSL_S2   ← GetCSL(S2);
   SL_R     ← GetSL(R);
   SL_O     ← GetSL(O);
   SL_MSPOOL ← GetSL(MSPOOL);

   if    S1,S2 ∈ SSET .and.
         O ∈ OSET .and.
         R ∈ USET .and.
         pp(S1,OP_Submit) .and.
         fs(S1,S2)      .and.
         ds(S1,O,'r')   .and.
         ss(S1,O,'r')   .and.
         star(S1,O,'r') .and.
         scompat(SL_MSPOOL,
            CSL_S2) .and.
         ds(S2,O,'r')   .and.
         ss(S2,O,'r')   .and.
         star(S2,O,'r') .and.
         ds(S2,MSPOOL,'w')   .and.
         ss(S2,MSPOOL,'w')   .and.
         star(S2,MSPOOL,'w') .and.
         ds(R,O,'r')   .and.
         ss(R,O,'r')   .and.
         star(R,O,'r')
   then  OSET ← OSET ∪ O;
         SLo ← CSL_S1;
   endif
End
```

여기서 S1은 UA, S2는 MTA, O는 제출코자 하는 메세지 객체, 그리고 R은 수신자를 의미한다.

● Transfer 오퍼레이션

Transfer 오퍼레이션은 주체 S1이 주체 S2에게 메세지 객체 O를 전송하기 위한 것으로 다음과 같이 정의된다.

```
Transfer(S1,S2,O)
```

```
Begin
   CSL_S2 ← GetCSL(S2);

   if    S1,S2 ∈ SSET .and.
         O ∈ OSET .and.
         pp(S1,OP_Transfer) .and.
         fs(S1,S2)      .and.
         ds(S1,O,'r')   .and.
         ss(S1,O,'r')   .and.
         star(S1,O,'r') .and.
         scompat(SL_MSPOOL,
           CSL_S2) .and.
         ds(S2,O,'r')   .and.
         ss(S2,O,'r')   .and.
         star(S2,O,'r') .and.
         ss(S2,O,'w')   .and.
         star(S2,O,'w')
   then  OSET ← OSET ∪ O;
         SL_O ← CSL_S2;
   endif
End
```

여기서 S1과 S2는 MTA를 의미하며 O는 전송하고자 하는 메세지 객체를 의미한다.

- Deliver 오퍼레이션

Deliver 오퍼레이션은 주체 S1이 주체 S2에게 메세지 객체 O를 배달하기 위한 것으로 다음과 같이 정의된다.

```
Deliver(S1,S2,O)
Begin
   CSL_S2 ← GetCSL(S2);

   if    S1,S2 ∈ SSET .and.
         O ∈ OSET .and.
         pp(S1,OP_Deliver) .and.
         fs(S1,S2)      .and.
         ds(S1,O,'r')   .and.
         ss(S1,O,'r')   .and.
         star(S1,O,'r') .and.
         scompat(SL_MSPOOL,
           CSL_S2) .and.
         ds(S2,O,'r')   .and.
         ss(S2,O,'r')   .and.
         star(S2,O,'r') .and.
         ss(S2,O,'w')   .and.
         star(S2,O,'w')
   then  OSET ← OSET ∪ O;
         SL_O ← CSL_S2;
   endif
End
```

여기서 S1은 MTA를 의미하며, S2는 UA 또는 MS를 의미하며, 그리고 O는 배달하고자 하는 메세지 객체를 의미한다.

- SetSbjLabel 오퍼레이션

SetSbjLabel 오퍼레이션은 주체 S가 자신의 현재 보안 레이블을 변경하기 위한 것으로 다음과 같이 정의된다.

```
SetSbjLabel(S,new_SL)
Begin
   CSL_S ← GetCSL(S);
   MaxSL ← GetMaxSL(S);
   MinSL ← GetMinSL(S);

   if    S ∈ SSET .and.
         pp(S,OP_ChSbjLabel) .and.
         dom(MaxSL,new_SL)   .and.
         dom(new_SL,MinSL)
   then  CSL_S ← new_SL;
   endif
End
```

여기서 S는 보안 레이블을 변경하고자 하는 주체이며 new_SL은 변경하고자 하는 새로운 보

안 레이블이다. 주체 S가 PRIV MAC_RELABEL_SBJ 권한을 가지고 있고 변경하고자 하는 새로운 보안 레이블이 주체 자신에게 허가된 보안 레이블 범위내의 값이면 주체 자신의 현재 보안 레이블을 새로운 값으로 변경할 수 있다.

- SetObjLabel 오퍼레이션

SetObjLabel 오퍼레이션은 주체 S가 객체 O의 현제 보안 레이블을 변경하기 위한 것으로 다음과 같이 정의된다.

```
SetSbjLabel(S,O,new_SL)
Begin
   CSL_S ← GetCSL(S);
   MaxSL ← GetMaxSL(S);
   MinSL ← GetMinSL(S);
   SL_O  ← GetSL(O);

   if    S ∈ SSET .and.
         O ∈ OSET .and.
         pp(S,OP_ChObjLabel) .and.
         dom(MaxSL,new_SL)   .and.
         dom(new_SL,MinSL)   .and.
         dom(new_SL,SL_O)
   then  SL_O ← new_SL;
   endif
End
```

여기서 S는 주체, O는 객체, 그리고 new_SL은 변경하고자 하는 새로운 보안 레이블을 각각 나타낸다. 주체 S가 PRIV_MAC_RELABEL_OBJ 권한을 가지고 있고, 변경하고자 하는 새로운 보안 레이블이 주체에게 허가된 보안 레이블 범위내의 값이며, 그리고 새로운 보안 레이블 new_SL이 객체의 변경전 보안 레이블을 지배하는 경우에만 객체의 보안 레이블을 새로운 값으로 변경할 수 있다.

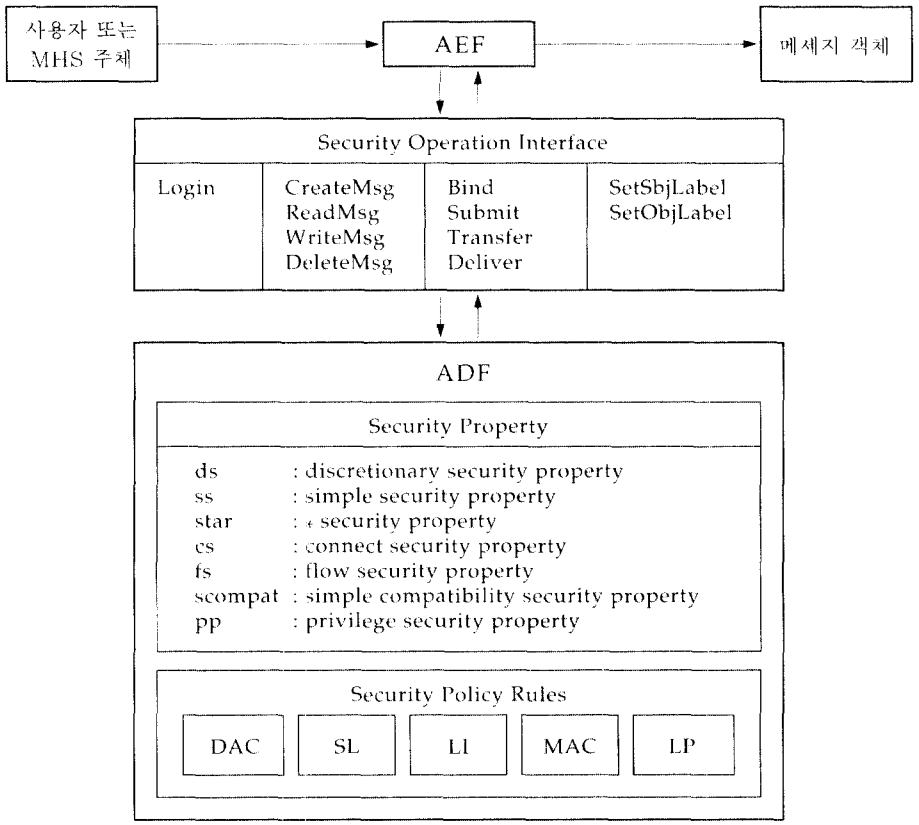
이와 같이 본 논문에서 제시한 보안 특성과 보안 오퍼레이션과의 관계를 요약하여 나타내면 다음의 〈표 4-3〉와 같다. (단, 표에서 기호 '●'의 의미는 관계성이 있음을 의미한다.)

보안 특성 함수 / 보안 오퍼레이션	임의적 보안 특성 (ds)	단순 보안 특성 (ss)	스타 보안 특성 (star)	집속 보안 특성 (cs)	흐름 보안 정책 (fs)	단순 일치 보안 특성 (scompat)	권한 보안 특성 (pp)
1. Login							●
2. CreateMsg	●	●	●			●	
3. ReadMsg	●	●	●				
4. WriteMsg	●	●	●				
5. DeleteMsg	●	●	●				
6. Bind				●			●
7. Submit	●	●	●		●	●	●
8. Transfer	●	●	●		●	●	●
9. Deliver	●	●	●		●	●	●
10. SetSbjLabel							●
11. SetObjLabel							●

〈표 4-3〉 보안 특성과 보안 오퍼레이션과의 관계

4.4 네트워크 액세스 제어 메카니즘 구조

이상으로 제시한 보안 정책, 보안 특성, 그리고 보안 오퍼레이션을 기반으로 하는 MHS를 위한 네트워크 액세스 제어 메카니즘은 AEF(Access Control Enforcement Facility), 보안 오퍼레이션 인터페이스, 그리고 ADF(Access Control Decision Facility)로 구성되며 그 구조는 다음의 〈그림 4-1〉과 같다. 사용자 또는 주체의 메세지 객체에 대한 액세스는 AEF를 통하여 이루어지는 것으로, 사용자 또는 주체의 액세스 요구에 해당하는 보안 오퍼레이션을 실행함으로써 액세스 서비스를 제공한다. 이러한 액세스 서비스에 대한 액세스 제어 결정은 ADF를 통하여 이루어지는 것으로, 이 ADF는 액세스 제어 결정을 위하여 보안 정책 규정(Security Policy Rules)을 근간으로 한 보안 특성 함수들의 실행 결과에 의존한다.



AEF : Access Control Enforcement Facility
ADF : Access Control Decision Facility
DAC : Discretionary Access Control
SL : Security Label
LI : Label Integrity
MAC : Mandatory Access Control
LP : Least Privilege

〈그림 4-1〉 액세스 제어 메카니즘 구조

6. 결 론

메세지 처리 시스템(MHS : Message Handling System)에서 다중 등급의 기밀성을 갖는 메세지를 안전하게 처리하고 네트워크상에서 정보 흐름을 안전하게 제어하기 위해서는 네트워크 보안 정책과 이를 만족하는 보안 메카니즘이 설계되어야 한다. 액세스 제어 및 정보 흐름 제어는 암호화 기법을 이용한 정보 보호와는 서로 다른 측면의 정보 보호 기능을 제공하는 것으로 상호 보완적이며 혼합시에 보안성을 높일 수 있게 된다. 그동안 네트워크 시스템에서는 암호화 기법을 이용한 정보의 비밀성(Confidentiality)에 대한 연구가 대부분이었으나, 전자 우편(E-Mail)이나 메세지 처리 시스템(MHS : Message handling System)과 같은 축적후 전송(Store-and-Forward) 방식의 액세스 제어와 정보 흐름 제어 문제는 해결해야 할 문제로 남아 있다.

본 논문에서는 MHS의 다중 등급 보안(MLS : Multilevel Security)을 위하여 MHS 에이전트인 UA(User Agent), MTA(Message Transfer Agent), 그리고 MS(Message Store)들의 보안에 관련된 액세스 및 오퍼레이션을 정의하고, 네트워크 사용자의 메세지에 대한 액세스 행위가 이들 오퍼레이션을 통하여 안전하게 이루어질 수 있도록 네트워크 액세스 제어 메카니즘을 설계하는 것에 중점을 두었다. 이를 위하여 첫째, 네트워크 보안 정책을 임의적 액세스 제어, 보안 레이블, 레이블 무결성, 강제적 액세스 제어, 그리고 최소 권한 정책 측면에서 제시하였으며, 둘째로 정의한 보안 정책을 만족하는 보안 특성 함수와 보안 오퍼레이션을 정형적으로 제시하였다. 셋째, 이러한 보안 특성 함수와 보안 오퍼레이션에 기반하여 안전한 MHS을 위한 네트워크 액세스 제어 메카니즘과 그 구조를 설계하였다. 제안한 액세스 제어 메카니즘은 네트워크상에서 중요한 메세지의 불법적인 액세스 또는 불안전한(Insecure) 정보 흐름의 보호 문제를 해결한다.

참 고 문 헌

1. National Computer Security Center (NCSC), "Department of Defense Trusted Computer System Evaluation criteria, Department of Defense," DoD 5200, 28-STD, Washington, D.C., Dec. 1985, pp. 7 - 54.

2. National Computer Security Center (NCSC), "Trusted Network Interpretation of the Department of Defense Trusted Computer System Evaluation Criteria," NCSC-TG-005, Version-1, Washington, D.C., Jul. 1987, pp. 223 - 260.

3. Pietro Schicker, "Message Handling System, X.400," Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elservier Science Publishers B.V., North-Holland, 1989, pp. 3 - 41.

4. Bernhard Plattner and Hannes Lubich, "Electronic Mail Systems and Protocols Overview and Case Study," Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elsevier Science Publishers V.B., North-Holland, 1989, pp. 55 - 99.

5. Susan Klein Lebeck, "Implementing

MHS: 1984 versus 1988," Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elsevier Science Publishers B.V., North-Holland, 1989, pp. 101 - 114.

6. John Linn and Stephen T.Kent, "Privacy for Dalpa-Internet Mail," Proceeding of 12th National Computer Security Conference, Washington, D. C., Oct. 1989, pp. 215 - 229.

7. Matt Bishop, "Privacy-Enhanced Electronic Mail," Distributed Computing and Cryptography: Proceedings of a DIMACS Workshop, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 2, Joan Feigenbaum and Michael Merritt, Editors, American Mathematical Society ACM, Oct. 1989, pp. 93 - 106.

8. Christopher Mitchell, Michael Walker, and David Rush, "CCITT/ISO Standards for Secure Message Handling," IEEE Journal on Selected Areas in Communications, Vol.7, No. 4, 1989, pp. 517 - 524.

9. Charles Dinkel, "SDNS Network, Transport, and Message Security Protocols," NISTIR 90-44250, U.S. DoC NIST, Gaithersburg, MD, Feb. 1990, pp. 63 - 83.

10. Ruth Nelson, "SDNS Services and Architecture," Advances in Cryptology-CRYPTO'89 Proceedings (Lecture Notes in Computer Science 435), G. Doos, J. Hartmanis, and G. Brassard, Editors, Springer-Verlag, 1989, pp. 348 - 352.

11. Stephen T. Walker, "Network Security: The Parts of the Sum," Proceedings of 1989 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 1989, pp. 2 - 9.

12. Carl Edgar Law, "X.400 and OSI Electronic Messaging into the 1990s," IBC Technical Services Ltd., 1989, pp. 76 - 82.

13. Martha Branstad, W. Curtis Barker, and Pamela Cochrane, "The Role of Trust in Protected Mail," Proceedings of 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 1990, pp. 210 - 215.

14. Tim Boland, "Working Implementation Agreements for Open Systems Interconnection Protocols," U.S. DoC National Institute of Standards and Technology(NIST), Gaithersburg, MD pp. 6 - 42.

15. Stephen t. Kent, "Internet Privacy Enhanced Mail," Communications of the ACM, Vol.36, No.8, Aug. 1993, pp. 48 - 60

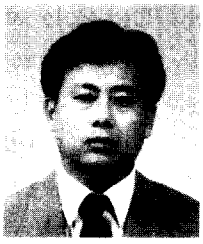
16. John McLean, "Reasoning About Security Models," Proceedings of 1987

IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, Apr. 1987, pp. 123 - 131.

□ 著者紹介

홍 기 융 (종신회원)

전남대학교 자연과학대학 계산통계학과 졸업(학사)
중앙대학교 공과대학원 전산학과 졸업(석사)
아주대학교 공과대학원 컴퓨터공학과 박사과정
1992.9. - 1993.6. : 이탈리아, Alenia Spazio S.p.A.사
(위성 지구국 시스템 공동개발, Senior Engineer)
1985 - 현재 : 한국전자통신연구소 선임연구원
1994. 8. 8. : 정보처리 기술사(전자계산조직응용)
※ 주관심분야 : 컴퓨터 및 네트워크, O.S 및 정보통신 Security
위성통신시스템 관제, 위성망 관리 및 정보보호



임 병 렬 (정 회 원)

아주대학교 공과대학원 컴퓨터공학과 박사과정

※ 주관심분야 : 컴퓨터 및 네트워크, O.S 및 정보통신 Security

김 동 규 (종신회원)

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1973. 3 - 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이타 통신시스템, 회중당, 1986년
컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 개방형 컴퓨터통신 연구회(OSIA) 이사,
한국 ISO/TC97/SC6/SC21/SC27 전문기술 연구위원,
한국통신정보보호학회 부회장
※ 주관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링, 정보통신 Security, 분산처리 시스템