통합 정보 모델을 이용한 접근제어 메커니즘 설계 및 구현

강 창 구[†] · 박 진 호[††] · 최 용 락[†††]

요 약

본 논문은 현대의 정보 통신 응용에서 접근제어 요구 사항의 복잡한 문제를 해결하기 위한 접근제어 메커니즘의 설계 방안을 제시 한다. 본 논문에서는 자원의 기밀성, 무결성 및 가용성의 공통적 목적을 달성하기 위한 통합 정보 모델을 제안 하고, 신분-기반, 규칙-기반 및 직무-기반의 관점에서 각 관련된 정책과 규칙을 정의 하였으며, 필요한 접근제어 오퍼레이션들을 구현하였다. 제안된 통합 정보 모델은 보안 레이블, 무결성 등급, 직무 및 소유권 등의 다단계 보안 정책을 기반으로 하여 자원에 대한 불법적인 접근을 방어 할 수 있다.

A Design and Implementation of Access Control Mechanism based on the Integrated Information Model

Chang-Goo Kang[†] · Jin-Ho Park[††] · Yong-Rak Choi[†††]

ABSTRACT

This paper presents a design of an access control mechanism that can resolves the complicated problems of access control requirements in modern information communication applications. In this paper, we proposed an integrated information model which can satisfy the combined goals of confidentiality, integrity and availability of any resource. We defined an integrated information model from the view points of identity-based, rule-based and role-based policy and implemented six access control operations. The proposed integrated information model can protect to unauthorized access to any resource based on the multilevel security policies of security label, integrity level, role and ownership.

1. 서 론

접근제어의 목적은 컴퓨팅 자원, 통신 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다[1][2]. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령어의 실행등을 포함한다. 즉, 접근제어는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며, 이러한 서비스들의 권한 부여를 위한 수단이 된다[3][4].

개방형 정보 통신망에서 접근제어는 실제의 어떤 개방 시스템에 있는 물리적 실체, 파일과 같은 논리적 실체, 그리고 일반적 사용자와 같은 다양한 형태의 실체들과 연관된다[5]. 접근제어를 위한 일반적 모델에서 능동적인 실체의 집합을 개시자(initiator) 또는 주체(subject)라고 하며, 수동적 자원의 집합을 타겟(target) 또는 객체(object)라고 부른다[1][5]. 그러나, 본 논문에서는 주체/객체 용어가 현대의 컴퓨터와 통신

† 정 회 원:한국전자통신연구원
†† 정 회 원:대전대학교 컴퓨터통신공학부
††† 종신회원:대전대학교 컴퓨터통신공학부
논문접수:1996년 12월 19일, 심사완료:1997년 8월 1일

분야에서 널리 사용되고 있는 개념과 혼동될 수 있으므로 명시적으로 접근을 시도하는 개시자 및 접근을 수용하는 타겟의 개념으로 제한하여 주체 및 객체로 사용한다.

접근제어의 결정은 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고, 어떤 조건하에서 접근할 수 있는지를 다루는 문제이다. 즉, 이러한 결정은 접근제어 정책에 반영이 되고, 접근 요청은 접근 정책을 시행하는 접근제어 메커니즘을 통하여 시행된다[2].

접근제어 정책은 다음과 같이 다양한 형태로 서술될 수 있다.

- 권한 부여의 과정에서 어떤 정책은 기관의 부서별로 모든 결정이 제어되거나, 또는 특정 객체에 대하여 개인별 권한부여가 서술될 수 있다.
- 사용자 및 객체들이 공통의 처리를 위하여 함께 그룹을 형성하여 서술될 수 있다.
- 어떤 정책이 시스템 요소에 의하여 강제적으로 시행될 수 있는 일반적 규칙들로 서술될 수 있다.

미 국방성에서 기밀 분류된 방법으로부터 유래하는 MAC(Mandatory Access Control)과 DAC(Discretionary Access Control) 정책의 개념은 위에서 제시된 3가지 요소를 확장 혼합하고 있다. MAC정책은 자동적으로 시행되는 어떤 규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위하여 사용자와 객체에 대해서 광범위한 그룹 형성이 요구된다. DAC 정책은 특별한 사용자별로 정보에 대한 접근를 제공하고 추가적 접근제어를 그 사용자에게 일임한다[2][6].

OSI 보안 구조에서는 MAC/DAC 용어를 사용하지 않고 신분-기반(identity-based)과 규칙-기반(rule-based) 정책으로 구분하고 있다. 실제적인 목적에 있어서 신분-기반과 규칙-기반 정책은 각각 DAC 및 MAC 정책과 동일하다[1].

신분-기반 정책은 개인-기반(Individual-Based Policy : IBP)과 그룹-기반(Group-Based Policy : GBP) 정책을 포함한다. 한편, 규칙-기반 정책은 다중-수준(Multi-Level Policy : MLP)과 부서-기반(Compartment-Based Policy:CBP)정책을 포함한다. 이외에 직무-기반(Role-Based) 정책은 신분-기반과 규칙-기반 정책의 양쪽 특성을 갖고 있다. 또한, 이러한 정책들은 서로 연합될 수 있으며, 임계값 의존 제어(Value-Dependent Control : VDC), 다중 사용자 제어(Multi-User Control : MUC) 및 배경-기반 제어(Context-Based Control : CBC) 등의 추가적 수단을 사용하여 제한 될 수 있다.

접근제어 메커니즘은 접근 행렬의 열을 표현하는 ACL(Access Control List), 접근 행렬의 행을 표현하는 CL(Capability List), 제어 대상에 레이블을 붙이는 SL(Security Label)등의 형태가 있다[1][5][7][8]. 그러나, 현대의 복잡한 정보 통신 응용에서 한가지 정책이나 모델이 필요한 접근제어 요구사항을 모두 만족 시킬 수 없다. 또한, 다양한 정책들을 배타적인 관계가 아니라 공통의 목적을 위하여 상호 보완적으로 사용 할 수 있다.

따라서, 본 논문에서는 실질적인 정보 통신 응용 환경에서 복합적 접근제어 요구 사항을 만족 시킬 수 있는 통합적 접근 제어 모델을 제안하고, 구현함으로써 접근제어의 궁극적 목적인 자원의 기밀성, 무결성 및 가용성을 보장하고자 한다.

2. 접근제어 정책 및 모델

정보 통신 응용 시스템의 안전한 서비스를 위해서는 시스템 설계시 요구되는 보안 사항을 명시하고, 적합한 보안 정책을 수립하여 보안 모델을 구성해야 한다[2]. 보안 모델 구성의 목적은 시스템이 보안 요구를 나타내는 요구 명세를 효과적으로 명시하고 설계할 특정 시스템의 소프트웨어와 독립적인 개념 모델을 만드는 데 있다. 보안 모델은 명시된 보안 시스템의 기능적 구조에 관한 성질을 정의하는 표현 수단을 제공 하므로 목표하는 시스템의 보안 요구사항을 간결하고 정확하게 제공하는것 뿐만 아니라 궁극적인 시스템 구현의 기본 정책이 된다[6][9].

접근제어에서 기본이되는 정책은 크게 3 가지 범주로 나눌 수 있다. 신분-기반 정책은 주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한할뿐 접근되는 객체 정보의 중요성에는 아무런 지식을 가지고 있지 않으므로 단순한 신분 위장에 의해서 접근제어가 파괴될 수도 있다.

규칙-기반 정책은 주체와 객체들간의 관계를 정의하고, 정보의 흐름이 일어났을때 정보가 소유한 제한 규칙을 상속하며, 각 주체와 객체에 대해서 규칙-기반 정책이 일정하므로 단순한 신분 위장으로는 접근제어를 파괴할 수 없다.

직무-기반 정책은 신분-기반 정책과 규칙-기반 정책의 특성을 모두가진 상업용 환경에 적합한 정책으로서, 개별적 신분이 아닌 자신의 직무에 따라 접근할 수 있는 정보가 결정되고, 사용할 수 있는 정보의 한계가 정해진다[10].

신분-기반 정책의 가장 기본적 모델로는 접근 행렬을 이용한 HRU(Harrison-Ruzzo-Ullman) 접근행렬 모델이 있다[11][12]. 이 모델은 보안을 지원하기 위해 처음 제안된 모델로서, 객체와 주체 및 권한 부여 집합에 의하여 특징 지워지는 상태의 식으로 보안 시스템을 보여준 모델이다. 대부분의 신분-기반 정책은 접근 행렬 모델의 확장형을 반영 하고 있다.

한편, 규칙-기반 정책은 시스템의 주체와 객체의 등급에 기초해서 정보에 대한 접근을 통제하는 모델로서, 객체는 정보를 저장하고 있는 피동적 존재이고, 주체는 객체를 접근하는 능동적 존재로 다룬다. 규칙-기반 정책으로 가장 잘 알려진 모델로는 BLP 모델이 있으며, 이와 비슷한 모델로는 정보의 무결성을 위한 Biba 모델, 안전한 정보 흐름 제어를 위한Lattice 모델등이 있다[5][14][15].

일반적인 보안 모델은 매우 다양한 형태로 여러 가지가 있으나 본 연구에서 심도 있게 검토한 모델은 다음과 같다.

- HRU 접근 행렬 모델은 주체의 객체에 대한 접근을 객체에 대하여 각 주체가 소유한 접근 권한을 나타내는 접근 행렬에 의해서 결정하는 모델이다. 이 모델은 접근 행렬 관리와 정보의 표현에 있어서의 비효율성과 접근제어 규칙들의 제어를 주체가 임의적으로 행사할 수 있으므로 안전성에 문제가 있다[12].
- Take-Grant 모델은 접근제어 행렬 모델의 단점 보완과 확장을 위해서 그래프 구조를 이용하여 권한 부여를 나타내는 모델로 구성되었다. 그러나, 접근 권한 확대에 대한 통제가 불가능하여 임의적인 접근 권한 확대를 방지할 수 없다[11].
- BLP 모델은 정보의 불법적 유출을 방어하기 위한 최초의 수학적 모델로서, 보안 등급과 범주를 이용한 강제적 정책에 의한 접근제어 모델이다. 보안 등급을 기초로 하여 No Read-Up Secrecy, No Write-Down Secrecy 기본 원리를 수행하여 기밀성을 보장하고, 접근 권한 결정을 위해서 신분-기반과 규칙-기반 정책을 모두 사용한다. 그러나, 군사 보안과 같이 엄격한 제한성을 갖고 보안 등급을 경직되게 취급하기 때문에 적용 환경의 융통성이 결여되어 있다[15][16]
- Biba 모델은 BLP 모델의 단점인 무결성을 보장할 수 없다는 점을 보완한 모델로서, 무결성 등급을 기초로한 No Read-Down Integrity, No Write-Up Integrity 기본 원리를 만족시킴으로써 무결성을 보장한다. 정보의 무결성 보장을 위한 정책으로는 서로 다른 상황에 적합한 다양한 정책을 사용하였다[17].
- Lattice 모델은 실제적인 정보보호의 문제점인 부적절한 정보의 흐름을 방지하기 위한 흐름제어를 위한 모델로서, 안전한 정보의 흐름을 위해서 수학적 구조인 lattice를 이용하고, 정보의 흐름을 나타내는 흐름 관계를 기초로 하여 구성한 모델이다. 각 주체와 객체간의 정보의 흐름은 보안 레이블에 기초하여 결정되고, BLP 모델의 기본 원리인 No Read-Up, No Write-Down Secrecy를 따른다[15][18].

3. 통합 정보 모델

규칙-기반 정책은 신분-기반 정책의 완전한 대체물이 아니듯이 직무-기반 정책이 신분-기반 정책과 규칙-기반 정책의 완전한 병합물도 아닌 상호보완의 관계이다. 이러한 3가지의 접근제어 정책에 기초한 새로운 접근제어 정책을 수립하고 적용할 환경에 적합한 정책으로 발전 시킬 필요가 있다.

따라서 본 논문에서는 3 가지 정책이 상호 보완적인 관계에서 작용 하도록 정의하고자 한다. 또한, 기밀성 보장을 위해서 BLP 모델의 기본 원리인 No Read-Up Secrecy과 No Write-Down Secrecy을 만족시키는 단순-보안 성질(simple-security property), 임의-보안 성질(discretionary-security property)과 스타-보안 성질(*-security property)을 이용하고, 무결성 보장을 위해서는 Biba 모델에서 엄격한 무결성 정책(strict integrity policy)과 접근제어 리스트(access control list)를 이용한 새로운 정책 및 접근제어 규칙을 정의한다.

각 접근제어 정책을 수행하기 위한 접근제어 메커니즘에는 접근제어 리스트, Capability 리스트, 보안 레이블 등이 있다[5][19]. 이러한 각각의 접근제어 메커니즘은 별개의 것으로 간주 되어 왔으나, 주체와 객체

의 모집단이 동적으로 변화하는 현대의 네트워크 환경에서의 접근제어 메커니즘은 어느 한 메커니즘에 근거한 일괄적 정의로는 부적절하다[20]. 따라서, 실제적인 접근제어 시스템에 적용이 가능 하도록 UNIX의 접근제어 메커니즘을 기본적으로 수용하고[21], 동일한 보안 정책에 포함하여 통합 정보 모델을 정의한다.

한편, 접근제어 결정을 위한 접근제어 정책과 함께 접근제어 결정을 위한 정보를 관리하는 정책이 필요하다. 접근제어 정보는 기밀성, 무결성 및 정확성이 보장되어야 한다. 이러한 기본적인 요구 사항이 만족되지 않으면, 주체의 객체에 대한 정확하고 안전한 접근제어 결정을 수행할 수 없고, 접근제어 시스템 자체의 기밀성과 무결성을 보장할 수 없다. 그러므로, 접근제어 정보(ACI) 관리를 위한 정책으로 ACI 관리 정책, 소유권 관리 정책 및 보안 레이블 관리 정책을 함께 통합적으로 고려하여 정의한다.

3.1 접근제어 정책

(1) 용어 정의

- 실체(entity)
  시스템에서 보안 대상이 되는 모든 요소들을 실체라 한다. 즉, 실체에는 사용자, 프로세스, 프로그램 및 데이터 파일등이 있다.
- 주체(subject)
  상대 실체들에 대해서 접근을 시도하는 능동적 실체이다. 본 논문에서의 주체는 사용자 및 프로세스이다.
- 객체(object)
  주체에 의해서 접근이 시도될 수 있는 피동적 실체이다.
- 접근제어 정보(ACI : Access Control Information)
  접근제어 결정을 위해 접근제어 결정 정보와 함께 접근제어 규칙에 적용되는 정보. ACI를 구성하는 항목 : identifier, owner, security label, integrity level, role, 통신망상의 위치(IP address)등.
- 접근제어 결정 정보(ADI : Access control Decision Information)
  특정한 접근제어 결정을 하는데 있어서 접근제어 결정 함수(ADF : Access control Decision Function)에서 이용하는 부분적인 ACI.
- 보유한 ADI
  미래의 접근제어를 결정할 때 사용하기 위해서 이전의 접근제어 결정으로부터 ADF에 보유하고 있는 접근제어 결정 정보(ADI).
- 접근제어 시행 함수(AEF : Access control Enforcement Function)
  개별 접근제어 요구에 대한 하나의 주체와 하나의 객체간에 설정된 접근 경로의 일부이면서, ADF에 의해서 만들어지는 접근제어 결정을 시행하는 함수이다.
- 접근제어 결정 함수
  모든 접근제어 요구에 대해서, ACI와 ADI를 가지고 접근제어 정책 규칙을 적용하여 접근제어 결정을 하는 함수이다.
- 감사 파일(audit file)
  주체가 객체에 대하여 요구한 접근제어 모드, 접근제어 결정, ACI 변경, 접근제어 정책 및 규칙의 변경에 관한 모든 자료를 보유하여 정보 시스템에 대한 감사를 수행할 수 있게 해주는 파일.
- 기밀성 등급(security level)
  실체의 기밀성 수준을 나타내는 계층적 분류 체계로서 Top Secret > Secret > Confidential > Unclassified와 같이 분류한다.
- 무결성 등급
  실체가 소유하는 정보의 수정에 관한 권한의 수준을 나타내는 계층적 분류 체계로서 Crucial > Very Important > Important와 같이 분류한다.
- 보안 범주(category)
  실체의 집합을 분류하는 비계층적 분류 체계로서, 각각의 범주에 속하는 실체들은 자신이 속한 범주에 맞는 기밀성 등급과 무결성 등급을 소유하며, 수행할 수 있는 일의 종류도 다르다.
- 직무(role)
  실체를 분류하는 비계층적 분류 체계로서, 조직이나 그룹에 있어서의 실체의 역할.
- 보안 레이블(security label)
  통신 되거나 저장되어 있는 데이터 항목, 물리적 자원 및 사용자와 같은 실체에 부여된 보안 속성 정보의 집합이다. 보안 레이블은 기밀성 등급과 보안 범주로 구성되며, 규칙-기반 정책 수행에 사용되는 정보이다.

SL=(C, S), SL; 보안 레이블, C; 보안 범주,
S; 기밀성 등급.

- 지배(domination) 관계
  두 실체에 대해서 각각의 보안 레이블을 상호비교하여 계층적 분류 체계인 보안 등급이 우세하고, 비계층적 분류 체계인 보안 범주가 다른 보안 범주를 포함할 때 지배 관계가 성립한다.
  $SL_1=(C_1, S_1)$, $SL_2=(C_2, S_2)$일 때, $SL_1 \geq SL_2$ ($C_1 \supseteq C_2$, $S_1 \geq S_2$); SL_1은 SL_2와 지배 관계에 있으며, SL_1은 우세하고, SL_2는 열세하다.
- 접근 모드(access mode)
  주체가 객체에 대하여 수행할 수 있는 접근 권한을 접근 모드라고 한다.
- 오퍼레이션(operation)
  주체가 객체에 대하여 수행할 수 있는 동작을 오퍼레이션이라고 한다.

(2) ACI 관리 정책

접근제어 결정에 필요한 모든 정보를 가지고 있는 ACI의 유지 및 관리를 위한 정책으로서 ACI 관리에 필요한 규칙들을 표현한다.

- 모든 실체는 ACI에 존재한다.
- 모든 실체는 ACI에 보안 레이블을 명시한다.
- 모든 실체는 ACI에 무결성 등급을 명시한다.
- 모든 실체는 ACI에 직무를 명시한다.
- 모든 실체는 ACI에 소유권자를 명시한다.
- 새로운 실체 생성시 ACI에 등록한다.
- 실체의 보안 정보 수정시 ACI에도 수정한다.
- 실체의 삭제시 ACI에서도 삭제한다.
- 실체 생성시 생성된 실체는 생성자의 ACI를 상속한다.
- ACI는 암호화된 상태로 보관된다.
- ACI는 ADF에 의해서 검증될 수 있는 방법으로 전달된다.

(3) 소유권 관리 정책

각 실체의 소유권을 관리하기 위한 정책으로서, 소유권을 이용하여 권한의 분산된 관리를 제공한다.

- 모든 실체는 자신의 소유권자가 있다.
- 생성된 실체는 생성자의 소유권자를 상속한다.
- 소유권자의 변경은 소유권자 및 허가 받은 자만이 변경한다.
- 정보의 전달 후 전달된 정보에 대한 소유권자는 정보를 전달받은 객체가 된다.

(4) 보안 레이블 관리 정책

실체의 보안 레이블 관리를 위한 정책으로서, 보안 레이블에 대한 무결성을 제공한다. 보안 레이블의 무결성 보장은 실체가 소유할 수 있는 정당한 접근 권한에 대하여 엄격한 제한을 제공한다.

- 모든 실체는 자신의 보안 레이블을 소유한다.
- 보안 레이블에는 보안 범주, 보안 등급을 명시한다.
- 새로운 실체 생성시 생성자의 보안 레이블을 상속받는다.
- 주체는 자신의 보안 레이블을 변경할 수 없다.
- 주체는 객체의 보안 레이블을 변경할 수 없다.
- 객체는 객체의 보안 레이블을 변경할 수 없다.
- 실체의 보안 레이블 변경은 보안 레이블 변경 권한자만이 할 수 있다.

(5) 신분-기반 정책

BLP 모델의 임의-보안 성질과 Biba 모델의 접근제어 리스트를 기초로 한 주체 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한한다.

- 모든 실체는 자신의 소유 객체에 대한 접근 권한 결정권을 가진다.
- 객체의 소유권자로부터 허가 받은 주체만이 객체에 접근할 수 있다.
- 주체는 객체의 보안 범주를 지배한다.

(6) 규칙-기반 정책

정보의 기밀성과 무결성을 보장하며, 주체가 자신과 동일한 보안 레이블을 가진 객체의 정보를 하위의 보안 레이블을 가진 객체로 전달하는 것을 방지하기 위한 정보 흐름 제어를 제공한다. 복사하는 정보의 보안 레이블과 복사되는 객체의 보안 레이블이 동일해야 하고, 주체의 보안 레이블이 객체의 보안 레이

블을 지배해야 정보의 흐름을 허가한다.

- 다음을 만족 시킬 때 read 동작을 수행할 수 있다.
  - 주체의 보안 레이블은 객체의 보안 레이블을 지배한다.
  - 객체의 무결성 등급이 주체의 무결성 등급을 지배한다.
- 다음을 만족 시킬 때 write 동작을 수행할 수 있다.
  - 주체는 객체의 소유권자이다.
  - 주체와 객체의 보안 레이블이 일치한다.
  - 주체와 객체의 무결성 등급이 일치한다.
- 다음을 만족 시킬 때 delete 동작을 수행할 수 있다.
  - 주체는 객체의 소유권자이다.
  - 주체의 보안 레이블이 객체의 보안 레이블을 지배한다.
  - 주체의 무결성 등급이 객체의 무결성 등급과 일치한다.
- 다음을 만족 시킬 때 move 동작을 수행할 수 있다.
  - 주체는 객체 정보의 소유권자이다.
  - move를 수행하는 주체는 객체 정보와 객체의 보안 레이블을 지배한다.
  - 객체 정보와 객체의 보안 레이블이 일치한다.
  - 객체 정보와 객체의 무결성 등급이 일치한다.

(7) 직무-기반 정책

직무-기반 정책에서는 주체의 직무를 판단하고, 객체와의 규칙-기반 정책을 수행한 결과를 이용해서 주체가 객체에 대해서 수행할 수 있는 직무의 프로그램을 허가한다.

- 주체는 객체의 소유권자이다.
- 주체의 직무로서 수행 가능한 프로그램이어야 한다.
- 주체의 보안 레이블이 요구한 프로그램의 보안 레이블을 지배한다.
- 주체의 무결성 등급이 요구한 프로그램의 무결성 등급과 일치한다.

3.2 접근 제어 규칙

(1) 접근제어 규칙 표기법 정의

접근제어 규칙의 표현에서 사용된 심볼들을 정의한다. 집합 표현에서의 대소문자는 집합과 원소를 나타내며, 함수 표현에서의 매개 변수들은 실체를 나타낸다.

- S: 접근제어의 주체 집합, $s \in S$
- O: 접근제어의 객체 집합, $o \in O$
- M: 접근 모드 집합, $M = \{r, w, e\}$; $m \in M$, (r; read, w; write, e; execute)
- R: 주체 및 객체의 직무 집합, $r \in R$
- S_Level(a): 기밀성 등급 함수
- I_Level(a): 무결성 등급 함수
- Category(a): 보안 영역 함수
- S_Label(a): 보안 레이블 함수
- permit(s, o, m): 주체 s의 객체 o에 대한 접근모드 m의 검색함수
- Role(a): 직무 함수
- owner(a): 소유권자 함수
- get_ACI(a): ACI 요구 함수
- inherit(a, b, c): 상속 함수; a의 b를 c에게 상속한다.
- dominate(a, b): $a \geq b$ or $a \supseteq b$
- equal(a, b): dominate(a, b) AND dominate(b, a)
- exist_ACI(a): ACI에 대해서 a의 존재 여부 확인 함수
- C_SLabel: 현재 보안 레이블
- C_ILevel: 현재 무결성 등급
- S_Label_V: 보안 레이블 변수
- I_Level_V: 무결성 등급 변수
- Login_ACI: login을 수행하는 실체의 ACI
- create_ACI(a): a의 ACI 신규 등록 함수
- delete_ACI(a): a의 ACI 삭제 함수

(2) 임의 접근제어 규칙

BLP 모델의 임의-보안 특성을 반영한 규칙으로서 주체가 객체에 대하여 수행하고자 하는 접근 모드가 있을 때 주체는 객체에 대한 적절한 접근권한을 소유해야 하고, 주체와 객체의 보안 레이블 함수중에서 주체의 보안 범주가 객체의 보안 범주를 지배해야 한다.

```
discret_acr(s, o, m) =
    TRUE : if permit(s, o, m) and
              dominate(Category(s), Category(o))
    FALSE: otherwise
```

(3) 강력 접근제어 규칙

강력 접근제어 규칙은 기밀성 보장을 위하여 주체

의 기밀성 등급이 객체의 기밀성 등급을 지배할때만 read 또는 execute 권한을 허용하고, 무결성 보장을 위해서는 주체의 무결성 등급과 객체의 무결성 등급이 일치할 때만 write 또는 execute 권한을 허용한다. 그러나, 기밀성과 무결성을 동시에 보장하기 위해서는 각 오퍼레이션특성에 따라 공통적으로 적용한다.

```
strict_acr(s, o, m) =
    TRUE : if m = 'r' and
               dominate(S_Label(s), S_Label(o)) and
               dominate(I_Level(o), I_Level(s))
    TRUE : if m = 'w' and
               equal(S_Label(s), S_Label(o)) and
               equal(I_Level(s), I_Level(o))
    TRUE : if m = 'e' and
               dominate(S_Label(s), S_Label(o)) and
               equal(I_Level(s), I_Level(o))
    FALSE: otherwise
```

(4) 실행 제어 규칙

실행 제어 규칙은 자신의 직무로 수행할 수 있는 프로그램만을 실행할 수 있는 규칙이다. 주체의 직무가 객체(프로그램)을 수행할 수 있는 직무이고, 주체의 보안 레이블이 객체의 보안 레이블과 지배 관계에 있고, 두 실체간의 무결성 등급이 일치해야만 execute 접근 모드를 수행할 수 있다.

```
execute_cr(s, o) =
    TRUE : if equal(Role(s), Role(o)) and
               dominate(S_Label(s), S_Label(o)) and
               equal(I_Level(s), I_Level(o))
    FALSE: otherwise
```

(5) 흐름 제어 규칙

흐름 제어 규칙은 상위의 보안 레이블을 가진 실체가 하위 보안 레이블을 소유한 실체로의 상위 보안 레이블 정보를 전달해 주는 것을 방지하기 위한 규칙이다. 즉, 주체가 한 객체가 소유한 정보(o1)를 다른 객체(o2)로 전달하기 위한 move 오퍼레이션은 주체가 두 객체에 대하여 보안 레이블이 지배 관계에 있어야 하고, 두 객체간에는 보안 레이블과 무결성 등급이 일치 해야만 한다.

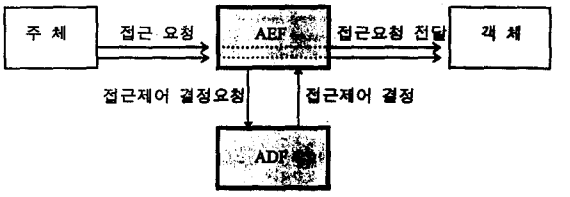
```
flow_cr(s, o1, o2) =
    TRUE : if dominate(S_Label(s), S_Label(o1)) and
               dominate(S_Label(s), S_Label(o2)) and
               equal(S_Label(o1), S_Label(o2)) and
               equal(I_Level(o1), I_Level(o2))
    FALSE: otherwise
```

4. 접근제어 메커니즘 설계 및 구현

4.1 접근제어 모델 구조

네트워크 환경에서 접근제어를 구현하는 것은 단일 컴퓨터 시스템에서 접근제어를 수행 하는데서 만나지 못했던 수많은 문제들을 일으킨다. 이것은 시스템에 관련된 실체들이 분산되어 있기 때문이다. 일반적으로, 어떤 동작을 희망하는 주체와 객체가 각각 다른 보안 영역에 있는 시스템 요소일 수 있다. 따라서, 접근를 결정하고 시행하는 기능이 몇 개의 다른 시스템들과 보안 영역을 포함하여 수행될 필요가 있을 수 있다. 개방형 시스템의 접근제어 구조(ISO/IEC10181-3)는 이와 같이 분산 환경의 접근제어 문제를 다루는 구조적 기반을 제공하는데 가치 있는 표준이다[5].

OSI 접근제어 모델에 따르면 접근제어 메커니즘을 시행함수(AEF)와 결정함수(ADF)의 두가지 개념적 요소를 구성함으로써 모델링 할 수 있다. (그림 1)은 접근제어 결정을 만들고 시행하는 기본 논리적 요소들을 나타내고 있다. 실제로, 이러한 요소들을 이용한 물리적인 구조가 널리 사용되고 있으며, 접근제어 서비스는 이러한 요소들과 접근제어 정보를 통신하여 제공된다.



(그림 1) 접근제어의 기본 개념 모델
(Fig. 1) Basic conceptual model of access control

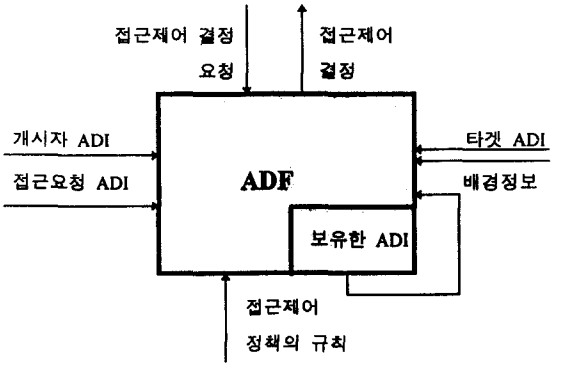
주체가 객체에서 특정한 동작을 수행하기 위하여 요청을 하면, AEF는 접근 허가의 검사를 위하여 어떤 결정이 요구된다는 것을 ADF에게 알린다. ADF는 본 논문에서 정의한 각종 접근제어 정책 및 규칙들을 갖고 있다. AEF는 ADF에 의하여 접근이 허용될 때만 요청된 동작이 주체에 의하여 객체에서 수행됨을 보장한다.

이러한 결정을 수행하기 위하여 ADF는 결정 요청의 한 부분으로서 원하는 동작과 몇 가지 ADI를 필요로 한다. ADF의 또다른 입력은 접근제어 정책의 규칙들과 ADI 및 정책으로 이용할 필요가 있는 기타 배경의 정보들이 필요할 수 있다. 여기서, 기타 배경 정보는 주체의 위치, 접근 시간, 또는 특정한 통신 경로와 같은 접근제어 조건들이 될 것이다. 이러한 입력들과 먼저의 결정에서 유지되고 있는 가능한 ADI를 근거로 하여 ADF는 주체가 객체에 대하여 요청한 접근를 허용할 것인지 아닌지 결정하게 된다. 결정은 AEF에 전달되고 그때 객체에 동작을 허용하거나 또는 기타 다른 동작을 취하게 된다. (그림 2)는 ADF의 개념적 모델을 나타내고 있다.

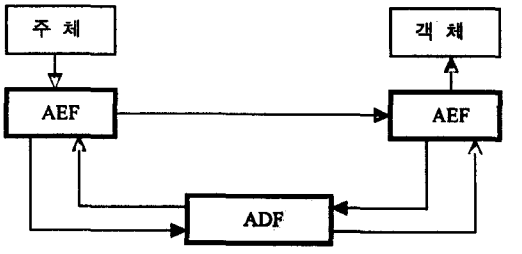
ADF는 접근 요청에 대하여 접근제어 정책을 적용하여 접근제어 결정을 만드는 네트워크의 논리적인 부분이다. AEF는 주체와 객체 사이의 접근 통로 상에 있는 네트워크의 한 논리적 부분으로서 ADF에 의하여 만들어진 결정을 시행한다.

한편, 접근제어의 요소인 AEF 및 ADF를 배치 구성하는 방법은 시스템 환경 및 서비스 특성에 따라서 다양할 수 있다. 객체에 진입하는 기점에서 접근제어를 수행하는 입력 접근 제어는 사용자 환경이 단순한 경우에 적합하고, 주체의 위치에서 접근제어를 수행하는 출력 접근제어는 네트워크 환경의 부담을 경감시키는 효과가 있다. 그러나, 실제의 일반적 응용에서 접근 요청이 다수의 보안 영역 경계를 가로 지르거나, 중간에서 보안 기관이 바람직하지 않은 요청을 차단하고 싶을 경우에는 네트워크의 어떤 중간 지점에서 접근제어 결정을 수행하는 것이 유리하다. 따라서, 본 논문에서는 병합된 형태로써 (그림 3)과 같은 중재된 중앙 접근제어 구조를 모델로 설계 하였다.

본 모델에서는 주체가 요청한 접근을 주체의 AEF에 제출하고, ADF로부터 승인을 받으면 주체의 AEF가 요청된 접근을 객체 AEF에게 제출하고, 다시 ADF에게 승인을 요구한다. ADF로부터 승인을 받으면 객체에 대하여 승인 받은 접근을 수행한다. 이 경우에 주체의 AEF가 수행한 출력 접근제어는 네트워크 중간 및 입력 접근제어의 위치에서 객체에 대한 불법적 접근제어를 방어할 수 있고, 객체 지역의 접근제어 시스템에 대한 신뢰도와 관계없이 안전한 접근제어를 제공할 수 있다. 출력 접근제어가 수행된 후 다시 객체에서의 입력 접근제어를 수행하면, 주체의 출력 접근제어에 대한 접근제어 결정 정보가 ADF의 ADI에 기록되므로 객체에 의한 입력 접근제어 수행시 보유 된 ADI를 검색 함으로써 권한 없는 제3자의 출력 접근제어 결정에 대한 위장 접근제어를 방어할 수 있다. 이러한 ADI의 사용은 접근제어 처리 및 통신 오버헤드를 줄이고 반면에 신뢰도를 향상 시키는 효과가 있다.



(그림 2) ADF의 개념적 모델
(Fig. 2) Conceptual model of ADF



(그림 3) 중재된 접근제어 구조
(Fig. 3) Interposed access control structure

4.2 접근제어 오퍼레이션 설계

설계한 통합 정보 모델에서 제공하는 접근제어 모드는 기밀성과 무결성 보장을 위해서 정보의 관찰과 수정에 대하여 엄격한 제한을 두지만, 정당한 사용자의 합법적 접근 모드에 대해서는 가용성을 보장하는 read, write, execute 3 가지의 접근 모드를 기준으로 하였다. 그리고, 주체가 객체에 대하여 정당한 접근 모드를 가지고 수행할 수 있는 오퍼레이션들은 아래의 7 가지를 대상으로 하였다.

- login 오퍼레이션

실체가 통신망에 접속된 시스템을 사용하기 위해서 시스템에 로그인 할 수 있게 해주는 오퍼레이션

- read 오퍼레이션

자신이 로그인한 시스템이나 통신망 상의 다른 시스템에 있는 정보의 내용을 read할 수 있게 해주는 오퍼레이션

- write 오퍼레이션

객체의 정보 내용을 read와 write할 수 있게 해주는 오퍼레이션

- execute 오퍼레이션

객체 프로그램을 실행시켜 주는 오퍼레이션

- delete 오퍼레이션

객체의 정보를 삭제할 수 있는 오퍼레이션

- create 오퍼레이션

새로운 정보를 생성시켜 주는 오퍼레이션

- move 오퍼레이션

객체의 정보를 통신망 상의 다른 시스템으로 전송시키는 오퍼레이션

〈표 1〉 오퍼레이션과 접근제어 규칙과의 관계
〈Table 1〉 Relations of operations and access control rules

규칙 / 오퍼레이션	임의 접근 제어 규칙	강력 접근 제어 규칙	실행 제어 규칙	흐름 제어 규칙
login	Y			
create	Y	Y		
read	Y	Y		
write	Y	Y		
delete	Y	Y		
execute	Y	Y	Y	
move	Y	Y		Y

〈표 2〉 오퍼레이션과 접근제어 정책과의 관계
〈Table 2〉 Relations of operations and access control polices

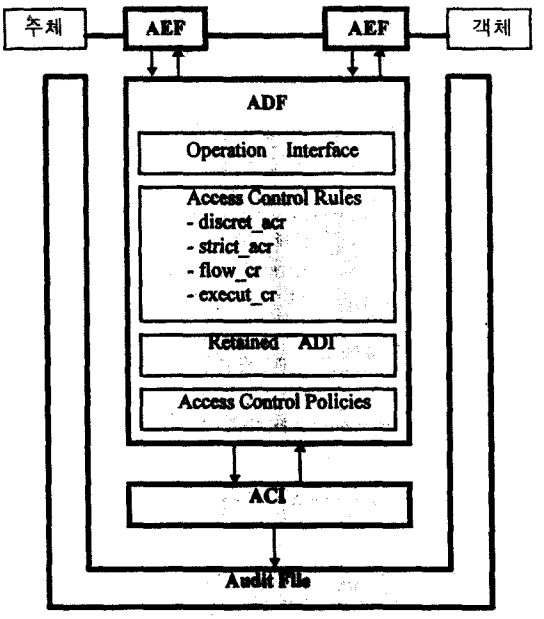
정책 / 오퍼레이션	ACI 관리 정책	소유권 관리 정책	보안레이블 관리 정책	신분-기반 정책	규칙-기반 정책	직무-기반 정책
login	Y			Y		Y
create	Y	Y	Y	Y	Y	
read			Y	Y	Y	
write		Y	Y	Y	Y	
delete	Y	Y	Y	Y	Y	
execute			Y	Y	Y	Y
move	Y	Y	Y	Y	Y	

이러한 오퍼레이션들은 필요에 따라 부가적으로 정의될 수 있으며, 각 오퍼레이션들의 설계에 적용된 접근제어 정책 및 규칙과의 관계를 요약하면 〈표 1〉 및 〈표 2〉와 같다.

4.3 접근제어 메커니즘 구현

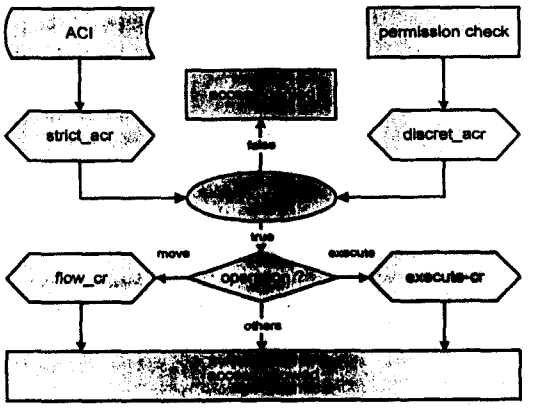
설계한 통합 정보 접근제어 모델에 대한 구현은 2대의 워크스테이션에서 SUN OS 4.1, ANSI C 및 TCP/IP 등의 환경을 이용 하였다. 구현에 적용된 각 보안 정책 및 규칙을 요약한 접근제어 메커니즘의 논리적 구조는 (그림 4)와 같다. 이 구조에서 주체 지역의 AEF는 주체로부터의 출력 접근제어를 수행하고, 객체 지역의 AEF는 객체에 대한 입력 접근제어를 수행함으로써, 각 주체와 객체간의 접근제어 시스템에 대한 상호 신뢰가 미약해도 상호 보완적으로 안전한 접근제어를 수행할 수 있다.

접근제어 메커니즘의 안전성을 위해서 접근제어에 사용되는 ACI는 암호화하여 보관 하였으며, 필요에 따라서 암호화 알고리즘을 선택적으로 변경할 수 있도록 하였다. 그리고, 정보 시스템에 대한 서비스 부인이나 부당한 접근을 탐지하기 위하여 감사 자료가 필요한 경우는 시스템 상에서 이루어진 모든 접근제어 요구나 결정에 관한 자료를 감사 파일에 기록 되도록 연결할 수 있다.



(그림 4) 접근제어 메커니즘 구조
(Fig. 4) Access control mechanism structure

통합 정보 모델을 기반으로 한 접근제어의 구현은 다양한 형태의 정책 및 규칙들이 복합적으로 작용하므로 이 규칙들간의 효과적이고 올바른 적용이 특히 중요한 사항이다. 설계된 접근제어 정책 및 규칙에 따라서 구현한 접근제어의 처리 과정을 요약하면 (그림 5)와 같다.



(그림 5) 접근제어 규칙 수행 순서도
(Fig. 5) Flow chart of access control rules

임의 접근제어 규칙과 강력 접근제어 규칙은 상호 종속적이거나 독립적 관계가 아니고, 상호 보완적 관계로서 정확한 접근제어 규칙의 수행을 위해서는 두 접근제어 규칙을 모두 만족시켜야 한다. 또한, 수행하고자 하는 오퍼레이션의 특성에 따라 흐름제어 규칙과 실행제어 규칙을 선별하여 만족시켜야 한다.

5. 결 론

본 논문에서는 복합적 접근제어 요구사항을 만족시킬 수 있는 통합정보 모델을 이용한 접근제어 방안을 제시 하였다. 그리고, 통합 정보 모델을 이용한 접근 제어 요구사항을 ACI 관리 정책, 소유권 관리 정책, 보안 레이블 관리 정책, 신분-기반 정책, 규칙-기반 정책 및 직무-기반 정책의 6 가지 보안 정책들로 표현하고, 각 정책들의 목적을 만족시키기 위한 4 가지의 접근제어 규칙을 정의 하였으며, 접근제어 서비스를 제공하기 위한 7 가지의 오퍼레이션을 설계 및 구현 하였다.

제안한 통합 정보 모델은 보안 레이블, 무결성 등급, 직무, 소유권 등을 이용하는 다단계 보안 체계를 이용하여 권한의 불법적 사용을 방지하였다. 이러한 다단계 보안 체계를 이용하여 각 보안 등급간의 정보의 흐름을 제한함으로써 정보의 불법적 유통을 차단하였다. 그리고, 정보의 전송 경로에서의 정보의 불법적 노출에 대한 보안 문제는 주체와 객체가 일정한 접근제어 규칙을 만족시키면 정보의 전송을 허락하고, 전송되는 정보는 인증과 암호화 기법에 의해서 암호화된 상태의 정보이므로 권한 없는 사용자에 대한 정보의 노출 위협을 방어할 수 있다.

또한, 중재된 중앙 접근제어 구성 방법을 사용함으로써 정보 통신망에서 이루어지는 모든 접근제어에 대한 감시 및 감사가 용이하고, 전체 통신망에 대한 ACI의 관리가 용이해진다. AEF를 포함하고 있는 모든 주체와 객체는 자신의 시스템에 접근하여 접근제어를 수행한 모든 주체에 대한 감사 파일 작성이 용이하며, 제3기관에서 보유하고 있는 감사 파일과 ADI를 이용하여 접근제어 결과에 대한 부인 봉쇄를 제공하도록 발전 시킬 수 있다.

본 논문에서 제안된 접근제어 모델 및 구성 방법은 엄격한 보안등급을 갖는 국가 기관 및 군사 기관의

기밀성 보장을 위한 접근제어 모델이나 기업이나 은행 등의 무결성 보장을 위한 접근제어 모델로서 사용할 수 있다. 또한, 현재 개발 시험중에 있는 안전한 EDI 시스템에서도 메시지 처리 시스템에 정의된 보안 레이블과 필요한 배경 정보들을 로컬 환경에 적합하게 연합하여 적용이 가능할 것이다.

참 고 문 헌

[1] Warwick Ford, Computer Communications Security-Principles, Standard Protocols and Techniques, Prentice Hall, pp. 149-176, 1994.

[2] Ingrid M. Olson, Marshall D. Abrams, "Computer Access Control Policy Choices", Computer & Security, Vol. 9, pp. 699-714, 1990.

[3] Shari Lawrence Pfleeger, "A Framework for Security Requirements", Computer & Security, Vol. 10, pp. 511-523, 1991.

[4] Wen-Pal Lu, Maluk K. Sundareshan, "A Model for Multilevel Security in Computer Networks", IEEE Transactions on Software Engineering, Vol. 16, No. 6, pp. 647-659, June 1990.

[5] ISO/IEC DIS 10181-3 Information Technology-Open Systems Interconnection-Security Frameworks in Open Systems-Part 3:Access Control, 1993.

[6] McLean J., "The Specification and Modeling of Computer Security", IEEE Computer, Vol. 23, pp. 9-16, 1990.

[7] Leonard J. LaPadula, "Formal Modeling in a Generalized Framework for Access Control", IEEE Proceeding of the Computer Security Foundation Workshop III, pp. 100-109, 1990.

[8] Landwer C. E., "Formal Models for Computer Security", ACM Computing Surveys, Vol. 13, No. 3, pp. 247-278, Sept. 1981.

[9] Gregory B. White, Eric A. Fisch, Udo W. Pooch, "Computer System and Network Security", CRC Press, Inc., 1996.

[10] Ravi S. Sandhu, Hal Feinstein, "A Three Tier Architecture for Role-based Access Control", In 17th NIST-NCSC National Computer Security Conference, Baltimore, MD., pp. 34-46, Oct. 1994.

[11] Silvana C., Maria G. F., Giancarlo M., Pierangela S., "Database Security", ACM Press, 1995.

[12] Harrison M. A., Ruzzo W. L., Ullman J. D., "Protection in operating systems", Comm. ACM, 19(8), pp. 461-471, 1976.

[13] Jonson P., Molva R., "Security in Open Networks and Distributed Systems", Computer Networks and ISDN Systems, Vol. 22, pp. 323-346, 1991.

[14] Clark D. D., Wilson D. R., "A Comparison of Commercial and Military Computer Security Policies", IEEE Symp. On Security and Privacy, New York, pp. 184-194, 1987.

[15] Ravi S. Sandhu, "Lattice-Based Access Control Models", IEEE computer, pp. 9-19, Nov., 1993.

[16] Roos Lindgreen, Herschberg I. S., "On the Validity of the Bell-LaPadula Model", Computer & Security, Vol. 13, pp. 317-338, 1994.

[17] Biba K. J., "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, The MITRE Corp., 1977.

[18] Denning D. E., "A Lattice Model of Secure Information Flow", Comm. ACM, 19(5), pp. 236-243, May, 1976.

[19] Silberschatz Galvin, "Operating System Concepts", Addison-Wesley, 1994.

[20] Ian M. Symonds, "Security in Distributed and Client/Server Systems-A Management Views", Computer and Security, Vol. 13, pp. 473-480, 1994.

[21] Simson Garfinkel, Gene Spafford, "Practical UNIX Security", O'Reilly and Associates, 1994.

강 창 구

1979년 한국항공대학교 전자공학과(공학사)

1986년 충남대학교 대학원 전자공학과(공학석사)

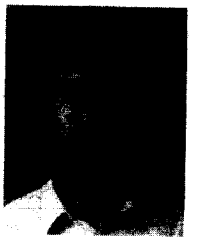
1993년 충남대학교 대학원 전자공학과(공학박사)

1987년~현재 한국전자통신연구원 실장 책임연구원

관심분야: 디지탈 서명, 정보보호 메카니즘, 정보보호 시스템 기술, 부호이론

박 진 호

1995년 대전대학교 전자계산학과(학사)
1997년 대전대학교 컴퓨터공학과(석사)
1997년~현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정
관심분야: 컴퓨터 시스템 및 통신망 보안, 통신망 관리



최 용 락

1976년 중앙대학교 전자계산학과(학사)
1982년 중앙대학교 전자계산학과(석사)
1989년 중앙대학교 전자계산학과(박사)
1982년~1986년 한국전자통신연구원 선임연구원
1986년~현재 대전대학교 컴퓨터통신공학부 교수
관심분야: 운영체제, 컴퓨터통신보안