通信情報保護學會誌
第8卷 第4號, 1998. 12

접근통제 기술 동향

김 의 탁*, 최 용 락*, 김 기 현**, 박 정 호**

요 약

본 논문은 각 시스템 자원의 안전성을 보장하기 위한 접근통제 기술을 다룬다. 현대의 분산 정보통신망 환경은 광역화되고 응용 서비스의 형태가 다양화 됨에 따라서 접근통제의 요구사항이 매우 복잡해졌다. 따라서, 하나의 접근통제 정책이나 메커니즘으로 모든 보안 요구사항을 해결할 수 없으며, 다양하게 연합된 정책과 기능별 복합적 시스템의 개발이 요구된다. 본 논문에서는 전통적인 접근통제 기술의 개념과 국제표준의 핵심내용을 분석하고, 최근 접근통제 제품들의 평가내용을 조사함으로써 접근통제 관련제품의 개발에 대한 기준을 제시한다.

1. 서 론

접근통제의 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 실행 등을 포함한다. 즉, 접근통제는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며, 이러한 서비스들의 권한 부여를 위한 수단이 된다[3][4].

대부분 컴퓨터 시스템의 사용자는 시스템을 사용하기 위하여 식별과 인증이라고 하는 검사과정을 통하여 시작된다. 식별과 인증은 각 시스템 자원을 보호하기 위한 외부의 1차적인 보호 계층이다. 인증이 성공하면 각 시스템 자원에 대한 사용자의 요청을 보안정책이 적용된 접근통제 절차에 따라서 허용여부를 인가한다. 접근통제 시스템의 분석은 기능적으로 3가지 요소적 측면으로 구분하여 관찰할 수 있다.

첫째, 시스템 자원에 접근하는 사용자의 접근 모드 및 모든 접근제한 조건 등을 정의하는 접근통제 정책

둘째, 시도된 접근 요청을 정의된 규칙에 대응시켜 검사함으로써 불법적 접근을 방어하는 접근통제 메커니즘

셋째, 시스템의 보안요구를 나타내는 요구명세로부터 출발하여 정확하고 간결한 기능적 모델을 표현하는 접근통제 관련 보안모델

가장 잘 알려진 접근통제정책은 미 국방성에서 분류된 방법으로부터 유래하는 MAC (Mandatory Access Control)과 DAC (Discretionary Access Control) 개념이 있다. MAC정책은 자동적으로 시행되는 어떤 규칙에 기반하고 있으며,

* 대전대학교 컴퓨터공학과
** 한국정보보호센터 기술개발부

그러한 규칙을 실제로 시행하기 위하여 사용자와 객체에 대해서 광범위한 그룹 형성이 요구된다. DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근통제를 그 사용자에게 일임한다[4][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-단계(Multi-Level Policy: MLP)와 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.

접근통제 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 접근통제 요구사항을 모두 만족시킬 수 없다. 또한, 다양한 정책들을 배타적인 관계가 아니라 공통의 목적을 위하여 상호 보완적으로 사용할 수 있다.

접근통제 보안모델은 접근행렬을 이용한 HRU 모델, 엄격한 기밀성 적용을 위한 BLP 보안모델, 무결성 정책을 지원하는 Biba 모델, 그리고 실행할 수 있는 프로그램에 의하여 통제하는 Clark-Wilson 모델 등이 있다.

국제적 접근통제표준은 ISO 7498-2의 보안구조와 ISO/IEC 10181-3 접근통제 구조가 널리 인용되고 있으며, 제품의 평가인증 기준은 TCSEC(Trusted Computer System Evaluation Criteria)과 ITSEC을 중심으로 수많은 제품들이 평가를 받고 있다. 본 논문에서는 이러한 동향과 연관된 주요 핵심적 기능들을 분석함으로써 국내의 접근통제 제품개발 및 평가기준의 참조 모델로 활용할 수 있도록 하고자 한다.

2. 접근통제 기술

2.1 접근통제 정책

시스템의 보안정책은 접근통제 시스템의 설계 및 관리를 다루기 위한 상위 지침들이다. 일반적으로, 대상 시스템 자원들을 보호하기 위해서 조직이 희망하는 기본적인 원칙들의 표현이다. 즉, 정책은 어떤 주체(who)가 언제(when), 어떤 위치에서(where), 어떤 객체(what)에 대하여, 어떠한 행위(how)를 하도록 허용(또는 거부)할 것인지 접근통제의 원칙을 정의한다. 접근할 수 있는 범위를 제한하는 접근통제 원칙은 다음의 2가지 기본정책으로 구분할 수 있다.

- 최소권한정책(Minimum Privilege Policy) : 이 정책은 "need-to-know" 정책이라고 부르며, 시스템 주체들은 그들의 활동을 위하여 필요한 최소분량의 정보를 사용해야 한다. 이것은 객체접근에 대하여 강력한 통제를 부여하는 효과가 있으며, 때때로 정당한 주체에게 소용없는 초과적 제한을 부과하는 단점이 있을 수 있다.
- 최대권한정책(Maximum Privilege Policy) : 이 정책은 데이터 공유의 장점을 증대 시키기 위하여 적용하는 최대 가용성 원리에 기반 한다. 즉, 사용자와 데이터 교환의 신뢰성 때문에 특별한 보호가 필요하지 않은 환경에 효과적으로 적용할 수 있다.

이러한 원리는 폐쇄 시스템(closed system) 및 개방 시스템(open system)에서 개념적 적용의 차

이를 볼 수 있다. 폐쇄 시스템에서는 명백히 권한 부여된 접근만을 허용하고, 개방시스템에서는 명백히 금지되지 않은 접근들을 허용하는 정의 방법이다. 폐쇄 시스템 정책은 시스템 객체에 대하여 그 주체의 접근권한을 명시하는 규칙을 정의하고, 접근통제 메커니즘에 의하여 확인되는 주체의 접근만을 허가한다. 개방시스템 정책은 주체가 시스템 객체에 갖고 있지 않은 권한을 명시하는 규칙을 정의하고, 접근통제 메커니즘에 의하여 부인되는 주체의 접근을 검사한다[9]. 이러한 적용원칙의 선택은 사용자 및 응용의 환경과 조직의 전략적 선택 문제이다.

보안 정책은 크게 신분-기반과 규칙-기반의 두 가지 범주로 분류된다. 신분-기반 접근통제 정책은 주체의 측면에서 행동하는 엔티티 또는 규정된 역할의 행위자로서 개인과 그룹에 명시된 규칙에 따르고 있다. 규칙-기반 접근통제정책은 보안 영역에 있는 어떤 객체에 대하여 어떤 주체에 의한 모든 행위를 적용한다.

한편, 직무-기반 접근통제 정책은 행정 편의상 분리하여 식별될 수 있는 신분-기반 정책의 그룹 개념에 의한 특별한 사용으로 생각할 수 있다. 직무란 개인이 아닌 조직의 직무기능상의 특별한 지위에 연관된 속성을 반영한 것이다[10][11].

2.1.1 신분-기반 정책

TCSEC에서는 신분-기반 접근통제정책과 동일한 개념을 DAC으로 정의하고 있다. 즉, 주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근를 제한하는 방법을 DAC이라고 정의한다. MAC에 의하여 제한되지 않을 때 접근통제는 임의적이므로 어떠한 접근 허가를 넘겨줄 수 있다.

DAC정책은 각 주체에 대하여 시스템 객체들에 부여된 권한을 명시하는 권한부여 규칙을 요구한다. 접근 요청은 DAC 메커니즘에 의하여 검사되고 권한부여 규칙이 존재하고 해당접근이 검증되는 주체에게만 허가된다

DAC 정책에서 내재적으로 상속되어지는 결점은 첫째, DAC속성상 통제는 주체의 신분에 전적으로 근거를 두고 있으며, 메커니즘은 데이터의 의미에 대한 아무런 지식도 갖고 있지 않으며, 이에 근거하여 결정할것도 없다. 둘째, 이와 같이 주체의 신분이 매우 중요하므로 만약, 다른 사람의 신분을 사용하여 행위가 이루어진다면 DAC은 파괴될 수 있다. 셋째, 트로이 목마에 대하여 취약하다.

신분-기반 정책은 다음과 같이 각 개인 및 그룹들로 나누어 표현될 수 있다.

(1) IBP(Individual-Based Policy)

IBP는 신분-기반 정책 형태의 하나로써 어떤 사용자가 어떤 행동을 할 수 있는지 각 객체별로 목록을 표현한다. 이것은 하나의 객체에 대하여 접근 행렬의 열을 나타내는 것과 같다. IBP정의문은 항상 디폴트 정책을 기본으로 서술된다. 즉,

- 객체 x에 대하여 사용자 a에게 읽기 권한을 허가한다.

라는 정의에서 a를 제외한 모든 사용자와 읽기를 제외한 모든 권한들은 허가되지 않음을 디폴트로 하고 있다. 이것을 "최소 권한의 원칙(*principle of least privilege*)" 이라고 하며, 우연한 사고나 오류들로부터 손상을 제한하는 효과가 있다.

(2) GBP(Group-Based Policy)

신분-기반 정책의 다른 경우로써 GBP는 다수의 사용자가 하나의 객체에 대하여 동일한 허가를 부여받는 방식이다. 이것은 하나의 팀 또는 부서에 속한 모든 인원에게 동일한 허가를 부여할 때 편리하다. 예를들면, 사용자 c1과 c2를 하나의 그룹으로 형성하고 공통의 식별자를 부여할 수 있다.

- 사용자 그룹 c는 사용자 c1과 c2를 포함한다.
- 객체 x에 대하여 사용자 a에게 *read, write* 권한을 부여하고, 사용자 그룹 c에게는 *read* 권

한을 부여한다.

이러한 정책의 첫번째 문장은 다른 객체 z 에 대하여 재사용 될 수 있다. 그리고, 두 번째 접근 허가 문장을 바꾸지 않고 그룹의 멤버를 변경할 수 있는 장점이 있다. 즉, IBP에서처럼 개별적으로 허가를 표현하는 대신에 그룹으로 묶어서 표현함으로 보다 쉽고, 효율적인 정책표현이 가능하다.

2.1.2 규칙-기반 정책

TCSEC에서 규칙-기반 접근통제정책과 동일한 개념을 MAC으로 정의하고 있다. 즉, 객체에 포함된 정보의 비밀성(레이블로 표현된 허용등급)과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한(즉, 접근허가(clearance))에 근거하여 객체에 대한 접근을 제한하는 방법을 MAC이라고 한다.

접근통제를 위한 MAC정책은 분류된 시스템 데이터와 각 등급의 사용자간에 강력한 보호를 위하여 요구되는 많은 정보들을 적용한다. MAC은 또한 하위 비밀등급의 객체로 정보의 흐름을 방어하기 때문에 흐름-제어 정책으로 정의될 수 있다. 데이터에 대한 접근은 주체와 객체가 갖는 보안등급의 정의를 통한 강제적인 정책에 의하여 결정된다.

MAC 정책은 DAC 정책에 비하여 일반적으로 다음과 같은 특성을 갖는다. 첫째, MAC정책은 객체의 소유자가 변경할 수 없는 주체들과 객체들간의 접근통제관계를 정의한다. 둘째, 한 주체가 한 객체를 읽고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제약사항이 복사된 객체에 전파된다. 세째, MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체/객체 단위로 접근 제한을 설정 할 수 없다. 즉, MAC가 어느 한 객체를 접근하지 못하면, 이때에 그 주체는 그러한 특정의 비밀 등급을 갖는 모든 객체들을 접근하는 것이 금지될 것이다.

규칙-기반 정책은 다음과 같이 사용자 및 객체별로 부여된 기밀 분류에 따른 정책과 조직내의 각 부서별로 구분된 기밀 허가에 따르는 정책으로 표현될 수 있다.

(1) MLP(Multi-Level Poicy)

MLP는 정부의 기밀 분류된 환경에서 사용될 수 있다. 이 정책은 자동화된 강제적 시행정책을 따르는 방식으로서 일반적으로 허가되지 않은 노출로부터 정보를 보호하기 위하여 사용된다.

MLP는 *TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED* 와 같이 각 객체별로 지정된 허용등급(classification)을 할당하여 운영한다. 각 사용자는 접근허가(clearance)를 부여받고 객체에 대한 접근를 제한 받는다.

이러한 형태의 정책과 연관된 규칙의 정의는 미 국방성의 컴퓨터 보안 평가 지표에서 사용되고 있으며 BLP(Bell and LaPadula) 수학적 모델로 표현이 가능하다. 이 모델은 dominance relation 이라고 알려진 사용자와 객체 사이의 정규 보안 수준사이의 관계를 정의한다. 그리고, 명시 규칙은 read-only와 write-only 접근을 허가하기 위하여 정의된다.

read-only접근에 대한 규칙은 SSC(Simple Security Condition)으로 알려져 있으며 비교적 분명하다. 이것은 어떤 수준의 접근허가를 갖는 사용자가 같거나 또는 하위수준의 허용등급을 갖는 정보만을 읽을 수 있도록 한다. write-only접근에 대한 규칙은 *-Property로 알려져 있으며, 어떤 수준의 접근수준을 갖고있는 사용자가 같거나 또는 상위수준의 허용등급을 갖는 객체에 정보를 기록할 수 있도록 한다. 이 규칙은 권한없이 정보를 기밀분류 지정에서 삭제하는 것을 방지하고, 트로이 목마공격을 방어하기 위한것이다. 또한, 정보가 여러개의 객체로부터 연결될 경우에, 결과적으로 최고 상위의 기밀 수준이 적용되도록 반영한다.

(2) CBP(Compartment-Based Policy)

CBP에서는 일련의 객체 집합이 다른 객체들과 분리된 이름의 부서(Compartment) 또는 범주(category)를 갖고 연결된다. 사용자는 그 부서에 있는 객체를 접근할 수 있도록 부서에 대하여 명백히 구분된 접근허가를 보유해야 할 필요가 있다.

예를 들면, 회사에서 구분된 부서는 계약부 및 인사부 등이 있을 수 있다. 이러한 경우 계약부에 대한 접근허가가 인사부 내에서 동일한 수준의 접근허가를 의미하는 것은 아니다. 다른 부서에서의 접근들은 별도의 특정규칙에 적용을 받아야 한다. 또한, 하나의 특정한 부서내에서 접근수준을 갖는 두 명의 사용자는 정보를 검색할 수 있도록 하기 위하여 연결된 요청을 나타낼 필요가 있을 수 있다.

2.1.3 직무-기반 정책

직무-기반 정책은 현대의 상업용 환경에서 특히 가치가 있는 다른 형태의 정책이다. 이것은 GBP의 한가지 변형으로 생각할 수 있으며, 접근통제정책을 정형화하는 구문 의미적 측면에서 직무(role)가 그룹에 대응된다. 즉, 정보에 대한 사용자의 접근은 개별적인 신분이 아니라 조직내에서 개인의 직무(또는 직책)에 따라서 결정된다. 예를 들면, 은행의 경우에 사용자의 역할을 직무별로 출납계, 지점장, 고객, 시스템 관리자 및 감사 등으로 분류하고, 이들에 대한 접근통제정책을 다음과 같이 각각 정의할 수 있다.

- 출납계는 예금을 처리하기 위하여 고객의 계정 기록을 수정하고, 출금은 지정된 금액 범위까지만 허용하며, 모든 계정기록에 대한 조회를 할 수 있도록 권한을 부여한다.
- 지점장은 예금 및 출금 거래를 하는 고객의 계정기록을 금액의 한도없이 허용하고, 모든 계정기록의 조회와 계정의 개설 및 폐지를 할수 있도록 권한을 부여한다.
- 고객은 자신의 계정에 관해서만 계정 조회를 할 수 있도록 권한을 부여한다.
- 시스템 관리자는 시스템의 운영과 시스템 기록에 대한 조회만을 할 수 있으며, 고객의 계정 정보는 읽거나 수정할 수 없도록 한다.
- 감사는 시스템에 있는 어느 데이터든지 읽을 수는 있지만 아무것도 수정할 수 없는 권한을 부여한다.

이러한 형태의 정책 서술문은 비기술적인 조직의 정책 입안자들이 쉽게 이해 할 수 있다는 의미에서 중요한 가치가 있다. 또한, 접근통제를 구현하기가 용이한 접근행렬, 또는 GBP에 쉽게 대응시킬 수 있는 장점이 있다. 그리고, 이 정책은 보안영역을 횡단하여 자동으로 시행될 수 있는 MAC의 한가지 형태로 생각하는 것이 가능하다. GBP와 직무-기반 정책에서 하나의 개별적 사용자는 한개 이상의 그룹 또는 직무에 종속될 수 있다. 그러나, 은행의 예에서 지점장과 감사의 역할 양쪽 모두를 갖지 못하도록 금지하는 제한을 적용할 수 있다.

2.1.4 접근통제조건

접근통제정책에 적용할 수 있는 몇 가지 조건들로써 어떤 임계값, 사용자간의 동의, 그리고, 사용자의 특정 위치 및 사용되는 시간 등을 지정할 수 있다. 해당되는 정책은 이러한 별도의 예상되는 데이터 환경을 조건으로 통제를 시행 할 수도 있을 것이다.

(1) VDC(Value-Dependent Control)

객체에 저장된 데이터의 값에 상관없이 대부분의 정책들이 고정된 접근통제허가를 갖는 것을 가정하고 있다. 그러나, 객체의 기밀성이 현재 저장된 값에 따라서 다양할 수 있다. 예를 들면, 어떤 임계값을 초과하는 계약에 관한 정보는 일반적 계약보다 높은 기밀수준을 갖고 보호할 필요가 있다.

(2) MUC(Multi-User Control)

지정된 객체에 대하여 다수의 사용자가 연합하여 요청할 경우의 접근통제정책을 지원하는 수단이 있어야 한다. 즉, 명시된 두 개인이 동의할 것을 요구하는 경우, 두 개의 역할에 대응한 개인들이 동의 할 경우, 그리고 하나의 그룹에서 특별히 명시된 몇 명의 멤버들(다수결)에 의하여 접근통제를 수행할 필요가 있을 수 있다.

(3) CBC(Context-Based Control)

이 제어방법은 다음과 같은 외부적인 요소에 의존하여 객체의 접근을 제어하는 정책에 이용될 수 있다.

a) 하루의 특정시간
b) 사용자의 현재 위치
c) 주체와 객체사이의 통신 경로
d) 주체의 신분을 확인하는데 사용된 인증 수준

이러한 제어들은 신분-기반 또는 규칙-기반 정책들에 첨가될 수 있다. 이 제어들의 목적은 접근통제메커니즘, 인증 메커니즘, 또는 물리적 보안대책에 대하여 가능한 어떤 취약점을 보완하는 것이다.

예를들면, 특정 객체에 대한 접근이 지정된 근무 시간, 또는 지정된 터미날 이외의 위치에서 접근할 수 없도록 제한하는 것이다. c) 형태의 제어는 네트워크의 특정한 부분에 대한 침투를 방어하기 위하여 지정할 수 있으며, d)는 주체의 신분을 특별히 인증하고자 할 때 이용될 수 있다. 예를들면, 어떤 객체에 접근 할 경우 패스워드에 의한 인증이 적절하다고 생각할 수 있지만, 보다 기밀의 객체에 대한 접근은 암호학적인 강한 인증 메커니즘을 사용하여 제어할 필요가 있다.

2.2 접근통제 메커니즘

접근통제 시스템은 보안규칙과 정책의 구현기능을 갖는 보안 메커니즘에 의존한다. 보안 메커니즘은 부당한 접근의 예방(접근통제 메커니즘)과 부당한 접근의 탐지(감사와 침입탐지 메커니즘)에 관련이 있다.

우수한 예방과 탐지는 강력한 인증 메커니즘을 요구한다. 사용자 신분의 인증은 어떤 동작에 대한 사용자 권한을 통제하기 위하여 정당한 사용자를 검증하는 기초가 된다. 접근 통제 메커니즘은 예방이 선호될 때 보다 기본적인 수단이며, 선택적으로 탐지가 부당한 접근의 탐색을 위하여 보완적으로 강구된다. 보안 메커니즘은 하드웨어 또는 소프트웨어로 행정관리 절차에 따라 구현될 수 있으며, 정책과 메커니즘은 다음과 같은 측면에서 분리하여 생각할 수 있다.

- 구현 메커니즘의 접근 규칙을 독립적으로 분석할 필요가 있다. 이러한 원칙은 설계자가 보안 요구사항의 정확성 검증에 집중할 수 있도록 한다. 그러나, 이것은 정책의 보안 요구사항이 구현 메커니즘에서 누락되지 않도록 보안정책의 일관성 있는 준수를 보장할 수 있는 체계이어야 한다.
- 동일한 보안정책에 대하여 다른 접근통제 정책 또는 다른 구현메커니즘들을 비교분석 할 필요가 있다. 하나의 보안정책은 다양한 형태의 구현 메커니즘으로 수행될 수 있을 것이다.
- 다른 정책을 수용할 수 있는 메커니즘을 설계할 수 있어야 한다. 이것은 응용환경에 따라 보안 정책이 변경될 때 구현 메커니즘에 밀접한 영향을 미치기 때문이다. 구현 메커니즘은 변경된 정책을 반영 할 수 있어야 할 것이다.

설계된 정책의 각 요구사항을 준수하는 메커니즘의 성취는 대단히 어려운 문제이나, 사실상 보안정책의 부정확한 구현 메커니즘은 다음과 같은 유형의 시스템 오류를 발생하는 부당한 규칙을 수행할 수 있다.

- 합법적인 접근의 부인
- 불법적인 접근의 허가

2.2.1 ACL(Access Control List)

ACL은 어떤 사용자들이 객체에서 어떤 행위를 할 수 있는지 나타낸다. ACL의 유지와 접근통제의 시행은 본질적으로 객체의 시스템 책임이다. ACL은 관련된 객체에 대하여 접근 행렬에서 열의 내용을 반영한다. 그러므로, IBP, GBP 및 직무-기반 정책을 포함한 신분-기반 접근통제정책은 ACL을 사용하여 직접적인 방법으로 실현될 수 있다. 또한, 기본적 ACL 개념은 특정의 선택된 사용자 엔트리에 대해서 접근통제조건을 추가하여 수행하는것과 같은 여러 가지 방법으로 확장 이용될 수 있다

ACL 메커니즘은 구분될 필요가 있는 사용자(개인, 그룹, 또는 직무)가 비교적 소수일때와 그러한 사용자의 분포가 안정적일 때 가장 적합하다. ACL의 관리는 대상되는 사용자가 너무 많고 자주 변경될 때 어려운 문제가 될 수 있다. 다른 메커니즘과는 달리 ACL은 객체 단편들이 넓은 영역인 경우에 적합하다. 또한, 객체의 소유자 또는 관리자가 앞서서 부여된 허가를 사용하기 쉽게 하는 장점이 있다.

2.2.3 CL(Capability List)

CL은 일찍이 컴퓨터 접근통제 개념으로 소개되었다. capability는 명시된 객체를 규정된 방법으로 접근하도록 권한을 부여 받은 주체가 소유할 수 있는 하나의 티켓으로 볼 수 있다. capability는 한 사용자에서 다른 사용자로 전달될 수 있고, 변경될 수 없으며, 또한 권한없이 복제될 수 없는 특성을 갖고 있다.

CL은 사용자에 대하여 저장된 접근 허가 목록에 근거하여 주체의 환경에서 생성된다. 접근 행렬의 항목에서 CL의 생성은 관련된 사용자에 대하여 접근 행렬의 행에 있는 지식을 사용한다

CL은 밀결합 시스템에서 보다 네트워크 환경에서 적용성이 적다. 네트워크는 보통 다중 보안 영역을 포함하고 있으며, 객체를 포함하고 있는 보안 영역은 그 객체에 관련된 접근통제결정에 발언권을 요구한다. 그러나, CL 메커니즘은 비교적 객체가 적을 경우에 적합하며 주체와 가까운 곳에서 접근통제결정이 일어날 때 편리하다. CL 메커니즘의 구현은 시스템 사이에 CL을 전달하는 안전한 수단에 의존적이다. CL의 단점은 객체의 소유자 또는 관리자가 먼저 승인된 허가를 취소하기가 쉽지 않다는 점이다.

2.2.3 SL(Security Label)

일반적으로 사용되는 용어로서 보안 레이블은 통신되거나 또는 저장되어 있는 데이터 항목, 물리적인 자원 및 사용자와 같은 객체에 부여된 보안속성 정보의 집합이다. 접근통제의 배경에서 보안 레이블은 사용자, 객체, 접근요청 또는 전송중인 접근통제 정보에 부여된다.

접근통제 메커니즘으로서 보안 레이블의 가장 일반적 사용은 다중-단계 접근통제 정책을 지원하는 것이다. 주체의 환경에서 주체의 비밀수준을 식별하는 레이블이 모든 접근요청에 부여된다. 이 레이블은 신뢰된 프로세스에 의하여 생성 및 부여되어야 한다. 모든 객체는 또한 자신에게 부여된 비밀수준을 나타내는 레이블을 갖고 있다. 접근요청을 처리할 때 객체환경은 객체에 있는 레이블과 요청에서 받은 레이블을 비교하고 접근을 승인할 것인지, 또는 부인 할 것인지 결정하기 위하여 정책규칙을 적용한다.

레이블은 전형적으로 제시된 것 보다는 복잡하며 접근통제결정을 만들기 위하여 추가적인 속성들을 포함하고 있다. 예를 들면, 이러한 속성들은 처리 및 분배경고, 부서 식별자, 시간제한, 또는 주체 식별정보를 포함할 수 있다. 레이블은 또한 보안정책/권한 식별과 확인 및 감사를 위하여 사용할 참조 식별자를 포함할 수 있다.

2.2.4 Protection Bits

ACL방식의 한가지 수정된 형태로써 각 객체에 대하여 접근허가를 나타내는 비트들을 사용한다. ACL에서처럼 모든 사용자와 허용된 모드들의 완전한 리스트를 제공하지 않고 명시된 사용자의 종류에 따라서 허가를 나타내는 보호 비트들이 각 파일에 부가된다.

보호 비트들의 사용에 대한 가장 일반적인 예는 UNIX 환경에서 볼 수 있다. 일반적 UNIX 시스템은 read/write/execute 3가지 접근모드를 갖는 파일접근에 대하여 Owner/Group/World 전략을 채택하고 있다. 이러한 메커니즘은 특정주체가 접근할 수 있는 모든 객체들을 리스트 하기가 어려운 단점을 갖는다.

2.2.5 패스워드-기반 메커니즘

패스워드-기반 접근통제 메커니즘은 현대의 안전한 네트워크에 적합하지는 않지만 기능상으로 간단한 제어 구조이기 때문에 유용하게 이용되고 있다. 패스워드는 원리 측면에서 객체에 대하여 티켓을 부여하는 CL과 유사하다. 특정 객체에 대한 접근 시도는 사용자가 그 객체와 연결된 접근 형태를 나타내는 패스워드를 제시함으로써 시행된다.

이러한 메커니즘은 패스워드를 비밀로 유지하고 관리하는데 심각한 문제가 있으며 특히 그룹이 공유할 경우는 더욱 어려움이 있다. 따라서, 패스워드는 인증 목적을 위하여 가치 있게 이용되고 있지만 접근통제 목적을 위해서는 권장할만하지 않다.

2.3 접근통제 보안모델

정보통신 응용 시스템의 안전한 서비스를 위해서는 시스템 설계시 요구되는 보안사항을 명시하고, 적합한 보안정책을 수립하여 보안모델을 구성해야 한다[5]. 보안모델 구성의 목적은 시스템이 보안요구를 나타내는 요구명세를 효과적으로 명시하고 설계 할 특정 시스템의 소프트웨어와 독립적인 개념모델을 만드는 데 있다. 보안모델은 명시된 보안 시스템의 기능적 구조에 관한 성질을 정의하는 표현수단을 제공 하므로 목표하는 시스템의 보안 요구사항을 간결하고 정확하게 제공하는것 뿐만 아니라 궁극적인 시스템 구현의 기본 정책이 된다[6][10].

보안 모델링의 목적은 시스템의 보안요구를 나타내는 요구 명세로부터 출발하여 소프트웨어와 독립적인 개념모델을 만드는데 있다. 보안모델은 기술된 보안 시스템의 기능적 구조에 관한 성질을 정의하는 표현수단을 제공한다. 즉, 설계자는 보안모델을 이용하여 바람직한 시스템 행동의 간결하고 정확한 설명을 제공하는것 뿐만 아니라 궁극적인 보안요구 명세와 시스템 정책을 정의할 수 있다.

보안모델은 크게 2가지의 범주로 나눌 수 있다. 즉, 사용자의 신분에 기초하여 접근을 통제하는 임의적 보안 모델(DAC)과 사용자가 임의적으로 변경할 수 없는 엄격한 보안등급에 따라서 접근을 통제하는 강제적 보안 모델(MAC)로 나누어진다.

MAC과 DAC의 모델범주 외에 다음과 같은 관점에 따라서 모델들이 분류될 수 있다.

- 대상 시스템에 따라서 다른 자원 및 접근모드가 고려될 수 있는 객체 시스템 관점(OS 보호 또는 DB 보안 등을 위한 모델)
- MAC 또는 DAC과 같은 접근통제 정책의 형태적 관점
- 기밀성 또는 무결성을 다루는 보안 기능적 관점
- 직접 접근통제 또는 정보흐름에 대한 간접적 접근통제를 허용하는 통제의 형태 관점

즉, 보안시스템의 개발에서 보안 모델의 선택은 객체 시스템 환경, 목표하는 보안기능, 보안정책, 그리고 의도하는 통제의 수단에 의존적이다. 때때로, 하나의 모델이 복잡 다양한 보호요구조

건을 나타내기 위하여 불충분하고, 모델의 연합이 보다 만족스러울 수 있다. 특히 이 경우에 한하여 기존모델의 연합과 특수조건 반영 또는 확장된 정의가 명시된 문제를 해결하기 위하여 효과적으로 응용될 수 있을 것이다.

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

한편, 규칙-기반 정책은 시스템의 주체와 개체의 등급에 기초해서 정보에 대한 접근을 통제하는 모델로써, 객체는 정보를 저장하고 있는 피동적 존재이고, 주체는 객체를 접근하는 능동적 존재로써 다룬다. 규칙-기반 정책으로 가장 잘 알려진 모델로는 BLP 모델이 있으며, 이와 비슷한 모델로써 정보의 무결성을 위한 Biba 모델, 안전한 정보 흐름제어를 위한Lattice 모델등이 있다[9][14][15].

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

- HRU 접근행렬 모델은 주체의 객체에 대한 접근을 객체에 대하여 각 주체가 소유한 접근권한을 나타내는 접근 행렬에 의해서 결정하는 모델이다. 이 모델은 접근행렬 관리와 정보의 표현에 있어서의 비효율성과 접근통제 규칙들의 제어를 주체가 임의적으로 행사할 수 있으므로 안전성에 문제가 있다[12].
- Take-Grant 모델은 접근통제 행렬모델의 단점 보완과 확장을 위해서 그래프 구조를 이용하여 권한부여를 나타내는 모델로 구성되었다. 그러나, 접근권한 확대에 대한 통제가 불가능하여 임의적인 접근권한 확대를 방지할 수 없다[9].
- BLP 모델은 정보의 불법적 유출을 방어하기 위한 최초의 수학적 모델로서, 보안등급과 범주를 이용한 강제적 정책에 의한 접근통제 모델이다. 보안등급을 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 보안등급을 경직되게 취급하기 때문에 적용 환경의 융통성이 결여되어 있다[15][16].
- Biba 모델은 BLP 모델의 단점인 무결성을 보장할 수 없다는 점을 보완한 모델로서, 무결성 등급을 기초로 한 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 흐름관계를 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. 접근통제 표준동향

ISO 7498-2에서는 OSI 환경에서 다양한 정보보호 위협요소에 대응하여 총괄적인 보안구조를 서술하고 있으며, ISO/IEC 10181-3에서는 접근통제 구조를 정의하고 있다. 2가지 모두 접근통제기술과 관련하여 중요한 표준이며, 이외에 OSI 관련 계층에 대응한 보안과 시스템 관리객체와 관련된 표준들이 있다.

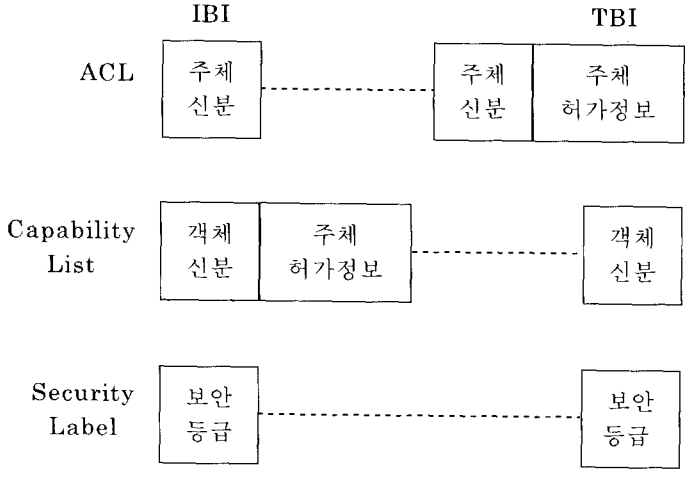
ISO/IEC 10181-3에서는 ACL, CL 및 SL 3가지

형태의 메커니즘을 통합적 관점에서 다루고 있다. 접근통제결정은 IBI(Initiator-Bound Information)와 TBI(Target-Bound Information) 같은 다양한 형태의 접근통제정보에 기반하고 있다. IBI는 직접 주체에 연관되어 있고, 그것의 출처는 주체의 영역이다. TBI는 객체에 직접 연관되어 있고, 그것의 출처는 객체의 영역이다.

[그림 1]은 ACL, 보안 레이블 및 capability메커니즘에서 사용되는 ACI가 어떻게 IBI와 TBI에 대응하는지 나타내고 있다. ACL에 대하여 단지 요구되는 IBI는 주체의 신분에 대한 지식이고, 반면에 주체의 신분과 동작 허가를 기술하고 있는 TBI가 있다. 역으로, capability에 대해서는 객체 신분과 허가에 관한IBI가 capability를 생성하는데 사용되고, 반면에 요구되는 TBI는 객체의 신분에 관한 지식 뿐이다. 보안 레이블 메커니즘은 IBI 와 TBI로서 각각 접근허가와 허용등급으로 불리는 레이블-기반 구조를 이용 한다.

ACL에서 주체의 이름이 TBI로서 사용하기 위하여 객체에 유지 된다면, 주체의 모집단이 동적인 시스템에 대해서 TBI의 관리는 대단히 어렵다. 거꾸로, CL에서 객체 이름이 IBI로서 유지 된다면, 객체의 모집단이 동적인 시스템에 대해서 IBI의 관리는 마찬가지로 어려운 문제이다. 관리적 측면은 분명히 정책 표현에 반영 되어야 하며, 어떤 하나의 메커니즘에 근거한 일괄적인 정의는 부적절하다. 따라서, 실제적인 시스템은 각각의 환경에 가장 적합한 여러가지의 접근통제 메커니즘들을 통합적으로 고려해야 할 것이다.

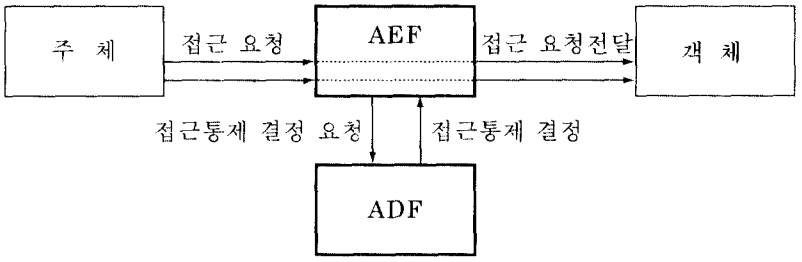
[그림 2]는 접근통제 오퍼레이션의 개념적 모델을 나타낸다. 주체가 객체에서 특정한 동작을 수행하기 위하여 요청을 하면, AEF는 접근허가의 검사를 위하여 어떤 결정이 요구된다는 것을



[그림 1] ACI의 형태

ADF에게 알린다. ADF는 정의한 각종 접근통제 정책 및 규칙들을 갖고 있다. AEF는 ADF에 의하여 접근이 허용 될 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 접근통제 정책의 규칙들과 ADI 및 정책으로 이용할 필요가 있는 기타 배경의 정보들이 필요할 수 있

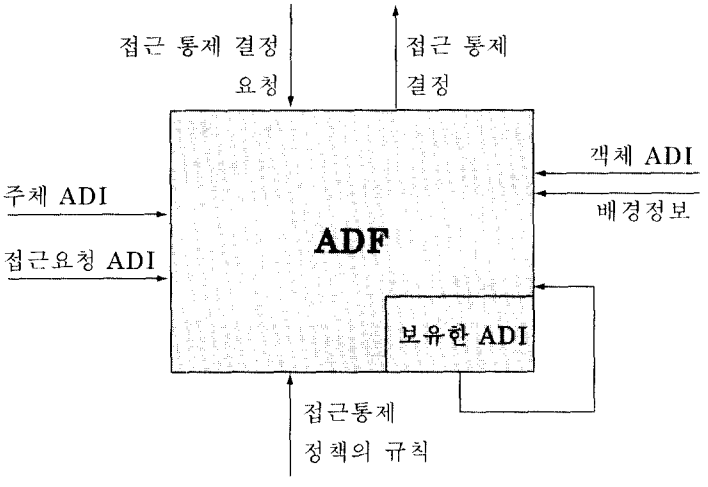


[그림 2] 접근통제의 기본 개념 모델

다. 여기서, 기타 배경 정보는 주체의 위치, 접근 시간, 또는 특정한 통신 경로와 같은 접근통제 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 3]은 ADF의 개념적 모델을 나타내고 있다.

ADF는 접근요청에 대하여 접근통제 정책을 적용하여 접근통제 결정을 만드는 네트워크의 논리적인 부분이다. AEF는 주체와 객체 사이의 접근통로 상에 있는 네트워크의 한 논리적 부분으로서 ADF에 의하여 만들어진 결정을 시행한다.

한편, 접근통제의 요소인 AEF 및 ADF를 배치 구성하는 방법은 시스템 환경 및 서비스 특성에 따라서 다양할 수 있다. 객체에 진입하는 기점에서 접근통제를 수행하는 입력 접근 통제는 사용자 환경이 단순한 경우에 적합하고, 주체의 위치



[그림 3] ADF의 개념적 모델

에서 접근통제를 수행하는 출력 접근통제는 네트워크 환경의 부담을 경감시키는 효과가 있다. 그러나, 실제의 일반적 응용에서 접근요청이 다수의 보안 영역경계를 가로 지르거나, 중간에서 보

안기관이 바람직하지 않은 요청을 차단하고 싶을 경우에는 네트워크의 어떤 중간 지점에서 접근통제 결정을 수행하는 것이 유리하다.

4. 접근통제 제품동향

4.1 평가 기준

정보통신 기술의 발달로 정보시스템 사용이 증가함에 따라 인터넷 등 정보통신망에 대한 취약성 및 위험 역시 증가하고 있다. 정보 유출, 위·변조, 파괴 등의 컴퓨터 범죄 및 해킹이 급증하고 있으며 불건전 정보 유통, 바이러스 감염, 서비스 방해 등의 정보화 역기능 또한 확산되고 있다. 이에 체계적인 총체적 정보보호 대책이 절실히 요구되며 평가 인증된 정보보호 제품 사용을 통하여 컴퓨터 범죄, 해킹, 바이러스 등의 위협요소의 확산을 방지하고, 정보통신망을 이용한 국가사회의 안전성 확보가 절실하게 되었다.

따라서, 시스템 평가인증에 대한 요구가 계속 증가하고 있으며, 각 국가들은 국제적 동향을 분석하여 자국별 평가기준을 만들고 있는 추세이다. 미국에서는 이미 오래 전부터 이러한 작업이 진행되어 왔으며 1985년에 DOD에서 일명 "Orange Book"이라고 하는 TCSEC(Trusted Computer System Evaluating Criteria) 평가기준을 만들었고, 유럽에서는 EC 주도하에 정보보호 시스템 보안등급을 평가하기 위해 1991년 ITSEC(Information Technology Security Evaluation Criteria)을 개발하였으며, 1993년에는 미국, 캐나다, 영국, 프랑스, 독일, 네덜란드의 공동 작업으로 기존 평가기준들의 조화를 위해 국제 평가기준(Common Criteria)을 마련하였다. [표 1]은 각 평가기준의 등급에 대한 기준을 요약하고 있다.

미국의 평가기준이 되는TCSEC은 모두 7개 등급으로 구분된다. D 등급은 부적합 판정을 나타내고, C1, C2, B1, B2, B3, A1 등급에서 A1등급이 가장 안전한 등급을 의미한다. 유럽의 평가 기준인 ITSEC은 영국, 독일, 프랑스, 네덜란드 4 개국이 작성한 평가기준으로 E0는 부적합 판정을 의미하고 E1, E2, E3, E4, E5, E6의 총6등급으로 분류된다. 그 중에서 E6등급이 가장 안전한 등급을 의미한다. 국제적인 정보보호시스템 평가기준은 CC로서 EAL0의 부적합 판정이 있고, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7의 총 7개 판정이 있다. 그 중에서 EAL7등급이 가장 안전한 등급이다.

4.2 TCSEC 제품군

가. UTS/MLS Release 2.15+

UTS/MLS Release 2.15+는 Amdahl Corpora-

[표 1] 미국, 유럽, 국제 평가기준 등급별 비교

TCSEC		ITSEC		CC	
평가등급	평가내용	평가등급	평가내용	평가등급	평가내용
D	최소한의 보호	E0	부적절한 보증	EAL0	부적절한 보증
				EAL1	기능시험
C1	임의적 보호	E1, F-C1	비정형적 기본설계	EAL2	구조시험
C2	통제된 접근보호	E2, F-C2	비정형적 기본설계	EAL3	방법론적 시험과 점검

TCSEC		ITSEC		CC	
평가등급	평가내용	평가등급	평가내용	평가등급	평가내용
B1	레이블된 보호	E3, F-B1	소스코드와 하드웨어 도면제공	EAL4	방법론적 설계 시험 및 검토
B2	구조적 보호	E4, F-B2	준정형적 기능명세서 상세설계	EAL5	준정형적 설계 및 시험
B3	보안 영역	E5, F-B3	보안요소 상호관계	EAL6	준정형적 검증된 설계 및 시험
A1	검증된 설계	E6, F-B3	정형적 기능명세서 상세설계	EAL7	정형적 검증

tion 사의 제품으로서 TCSEC에서 B1 등급 판정을 받았다. 이 제품은 UNIX System V 호환 제품으로 65,000명의 사용자를 지원할 수 있는 멀티유저, 멀티타스킹을 제공하는 운영체제 시스템이다.

이 시스템에서 제공하는 보호 메커니즘은 DAC과 정보에 접속하고자 하는 사용자에 대한 보안등급과 정보의 기밀성 보안에 근간을 둔 정보의 흐름을 제한하기 위해 MAC을 지원한다. 보안정책으로는 Bell-LaPadula 모델과 DOD 정책으로 구성되어 있으며, 감사추적 기능을 제공한다. UTS/MLS는 255개의 계층적 보안 등급과 1024개의 비계층적 범주(category)까지 지원할 수 있는 융통성 있는 레이블 구조를 제공한다. DAC은 파일, 디렉토리, 이름을 갖는 파이프, 디바이스 특정 파일, 심볼릭 링크, 공유 메모리, 메시지 큐, 세마퍼 집합에 적용되고, MAC은 프로세스, 라인 프린터 큐 엔트리, 메일 메시지와 같은 객체의 집합에 적용된다. DAC 정책은 전통적인 UNIX Owner/Group/Other의 보호비트 구조를 사용한다.

나. CA-Access Control Facility 2(CA-ACF2 MVS)

CA-Access Control Facility 2는 Computer Associates International, Inc.의 제품으로 1998년 초에 TCSEC에서 B1의 등급 판정을 받았다. 이 제품은 IBM MVS/ESA(Multiple Virtual Storage/Enterprise System Architecture) 운영체제에서 사용하는 데이터에 대한 정보보호 기능을 제공한다.

CA-ACF2는 ACL를 통해서 DAC을 지원하고 시스템에서 모든 자원들은 디폴트로 외부로부터 보호되며, 자원의 규칙과 접근규칙에 의하여 명명된 사용자와 객체 간의 통제된 접근을 제공한다. 또한, CA-ACF2는 CA-ACF2 MAC 컴포넌트를 통하여 MAC을 지원한다. 이 컴포넌트는 모든 주체와 객체에 대한 레이블 정보를 유지하기 위한 기능을 제공한다. 그 밖에도 이 제품에서는 감사추적기능이 있다.

다. Open VMS VAXVersion 6.1 Alpha Version 6.1

Digital Equipment Corporation의 Open VMS Version 6.1은 1996년도에 TCSEC에서 C2 판정을 받았다. 이 제품은 Digital 사의 32 비트 VAX 프로

세서와 64 비트 알파 프로세서 상에서 수행되는 범용 멀티 유저 운영체제이다.

이 시스템에서는 사용자 목록(시스템, 소유자, 그룹 그리고 전체 사용자)에 의해 기본적인 DAC이 제공된다. 추가로, ACL은 식별자와 식별자에 대해 허가된 엑세스를 포함한다. 식별자에 기반을 둔 접근 허가를 그룹화할 수 있는 유동적인 메커니즘을 제공하기 때문에, 하나의 사용자가 여러 개의 다른 식별자를 사용할 수 있다. Open VMS의 특징은 주소공간의 격리, 로그인에 대한 신뢰된 통로, 그리고 ACL을 제공한다는 점이다.

라. GTNP Version 1.01

Gemini Computers, Incorporated에서 개발한 GTNP(Gemini Trusted Network Processor)는 1994년 중반에 TCSEC에서 가장 높은 A1 등급을 받은 네트워 컴포넌트 제품으로 MAC 정책을 수행하는 네트워 컴포넌트를 위한 M-NTCB(Mandatory Network Trusted Computing Base)를 지원한다. 또한, DES 암호 알고리즘과 동시처리 기능을 제공한다.

GTNP는 다중보안레벨의 이기종의 분산 정보시스템에 대한 안전한 데이터 공유 컴포넌트와 안전한 네트워 연동을 구축하기 위하여 다른 제품과 기술들의 정합을 지원하기 위해 설계되었다.

GTNP는 GEMSOS(Gemini Multiprocessing Secure Operating System) 보안 커널을 기반으로 하는데 이 커널은 BLP 모델을 바탕으로 한 기밀성과 Biba 모델을 바탕으로 한 무결성을 동시에 제공하는 격자-기반 MAC 정책의 보안 참조 모니터 이다.

4.3 ITSEC 제품군

가. OMEGA Version 7.10

OMEGA Version 7.10은 ICL Defense 사에서 만든 통신관련 제품으로 1997년에 ITSEC으로부터 E3 등급을 판정 받았다. 이 제품은 멀티레벨 보안 메시지를 다루는 제품으로 네트워과 안전한 메시지 기능을 제공한다.

이 제품은 MAC, DAC 그리고 보안 레이블 등이 모든 컨트롤 데이터와 메시지에 적용되고, LAN, WAN을 통해 접속된 PC와 CMW 플랫폼에 접속할 수 있는 기능이 있다. Omega는 사용자 친화적인 제품이다.

나. INFORMIX Online/Secure B1 & C2 Version 5.0

Informix Software Ltd.에서 만들어진 이 제품은 1995년도에 ITSEC에서 E3 등급을 받았다. 이 제품은 F-B1 등급의 OS와 연동하여 사용할 때, F-B1 등급의 기능을 요구하는 시스템에서 데이터베이스 보안을 제공한다.

주요 보안기능으로는 식별, 인증 그리고 객체의 재사용 기능을 제공하고 DAC, 데이터 무결성, 그리고 감사 기능을 제공한다. 또한, Online Secure B1에서는 이기종의 보안 레벨에서 수행중인 프로세스간의 비밀 채널을 제거하기 위한 메커니즘과 함께 MAC을 제공하며 신뢰된 유닉스 플랫폼에 이식되도록 설계되었다.

다. DXE Router

Storage Tek Network Systems Group에서 개발한 DXE Router는 1995년에 평가 받은 네트워 제품으로 E3 등급을 받았다. 이 제품은 데이터그램과 네트워들 간의 접근 중계를 제공한다.

이 접근 중계는 MAC과 DAC을 기본으로 한다. DAC은 프로토콜 헤더에 포함된 정보, 예를 들어, 출발지/행선지 주소, 포트번호 등을 기반으로 수행된다. 관리자 콘솔로의 접근 혹은 외부의 감사 호스트로 진행중인 감사 데이터를 이용하여 강제적 혹은 임의의 접근 변화를 감사한다. 이 라우터가 제공하는 인터페이스는 Synchronous Link(9.6kbps~52Mbps), HSSI, FDDI, Ethernet, Token Ring, IBM, Channel 과 HIPPI등이 있다.

라. GUARDIAN ANGEL Version 5.01D1

이 제품은 Portcullis Computer Security Ltd에서 만든 데이터 보호를 위한 PC상에서의 접근통제를 제공하는 소프트웨어로 1998년도에 ITSEC에서 E2 등급을 판정 받았다.

GUARDIAN ANGEL의 특징은 시스템에 불법적인 접근을 막기 위해 사용자 식별과 패스워드 기능을 갖고 있다. 패스워드는 CESG FIREGUARD 알고리즘을 사용하여 암호화 하였다. 보안 프로파일, 감사 추적, 그리고 파일 접근 통제 행렬을 통해서 데이터와 파일에 대한 접근을 통제하며, 사용자 신원을 바탕으로 파일 접근과 소유권을 제한한다. 또한, GUARDIAN ANGEL에 의해 포맷되지 않은 플로피 디스크의 사용을 방지하는 디스크 인증 기능이 있다.

5. 결 론

본 논문에서는 다양한 접근통제 정책 및 국제표준동향의 주요내용을 분석하고, ITSEC과 TCSEC의 접근통제 제품의 인증동향을 조사하였다.

접근통제 정책은 신분-기반과 규칙-기반의 두 가지 범주로 나눌 수 있으며, 이것은 개인별 및 그룹별 또는 다중-단계 및 부서-기반 등으로 정의될 수 있다. 그리고, 조직내에서 부여된 직무를 나타내는 직무-기반 정책이 그룹-기반 정책의 변형으로 다르게 표현될 수 있다. 또한, 이러한 정책들은 시간 및 장소, 특정의 임계 값 등에 의하여 추가적인 배경정보들을 조건으로 요구함으로써 복합적인 접근통제 정책수립이 가능할 것이다.

접근통제 메커니즘은 전통적으로 ACL, CL, SL을 중심으로 연구되어 왔으며, 특히 ACL 형태에 대응하는 보호 비트들을 각 객체에 부가하여 통제하는 것이 일반화된 기법이었다. 그러나, 오늘날 정보통신 네트워크가 확산됨에 따라서 접근통제 대상이 되는 시스템 자원이 다양해지고, 응용 서비스가 광역화 되었으므로 어떤 하나의 메커니즘 및 제한된 기능제품으로 안전하고 효율적인 접근통제시스템 개발이 어려워졌다.

접근통제 보안모델은 기밀성과 무결성 보장을 위한 범주로 대분류하여 볼 수 있다. 또한, DAC 및 MAC 정책을 수행하기 적합한 모델, 운영체제 보안모델 및 DB 보안모델 등으로 나누어 관찰할 수 있으나 모두가 실제의 복합적 접근통제 요구사항을 총괄적으로 만족시키기에는 부적합하다. 이러한 보안 모델들의 연합적 적용 및 각 모델의 특성을 검증할 수 있는 새로운 개념의 시스템 커널 보안모델이 필요할 수 있다.

접근통제 표준에서는 각 형태의 접근통제정책 및 메커니즘들을 통합적 개념에서 서술하고 있으며, 이러한 원리에 입각하여 다양한 접근통제 오퍼레이션과 기타 관리지원 서비스들을 정의하고 있다. 그러나, 이러한 내용을 모두 반영한 제품은 찾기 힘들은 실정이며, 다만 접근통제 기술의 방향과 제품개발의 기준으로서 중요한 참조모델이 될 것이다.

접근통제 제품의 개발동향을 조사하고 국제적으로 인증된 제품의 접근통제기능을 분석하는 일은 시스템 개발의 기능적 목표를 수립하는데 중요한 과정이다. 조사한 TCSEC과 ITSEC의 접근통제 인증제품들의 동향 및 기능분석은 국내의 제품개발을 위한 검토기준이 될 수 있을 것이다.

참고문헌

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

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

[11] 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.

[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] ISO 7498-2:1989 Information Processing Systems-OSI-Basic Reference Model Part 2: Security Architecture.

부록 A : TCSEC 평가 제품

제 품 명	평 가 등 급	개 발 사	평 가 시 기	제품의 특징
MLS LAN Version 2.1	A1	Boeing	1994	· MAC, DAC제공 · 다른 보안등급의 호스트,터미널, 네트웍연결
Trusted UNICOS 8.0 Release 8.0.2	B1	Cray Research, Inc.	1995	· ACL과 permission bit에 기반한 DAC 제공 · 기밀 레이블에 기반을 둔 MAC 제공
ACS/VS II Version 3.10	C2	Data General Corporation	1994	· ACLs 사용을 통한 사용자와 객체간의 DAC제공
DiamondLAN 6.0 DiamondLANe 6.0	B2	Cryptek Secure Communications, LLC.	1995	· MAC, DAC 제공 · 네트웍상에서 전송되는 모든 데이터를 DES로 암호화
CX/SX Version 6.2.1	B1	Harris Computer Systems Corporation	1995	· 전통적인 유닉스 상에서 permission bits를 이용한 DAC 제공 · BLP모델을 이용한 MAC 제공
HP/UX BLS Release 9.09+	B1	Hewlett-Packard	1994	· 유닉스 상의 permission bits와 함께 ACL을 사용하여 DAC 제공 · BLP모델과DOD정책을 따르는 MAC 제공
ULTRIX MLS+Version2.1 (VAX Station 3100)	B1	Digital Equipment Corporation	1996	· 전통적인 유닉스 상에서permission bits를 이용한 DAC 제공 · Sensitivity Label비교를 통한MAC제공
Trusted Oracle 7.0.13.1DBMS	B1	Oracle Corporation	1994	· MAC보안 정책을 위해 Sensitivity Labels을 사용 · Privilege의 사용을 통한 DAC 제공
SISTex Assure EC 4.11 (Novell Network Component)	C2	SISTex, Inc	1997	· 워스테이션의 파일, 디렉토리, I/O장치에 DAC 제공 · ACL에 의한 파일과 디렉토리 DAC 제공
Trusted IRIX/B Release 4.0.5EPL	B1	Silicon Graphics Computer Systems, Inc.	1995	· 유닉스 기반으로 제공되는 DAC 사용 · BLP 모델의 기밀성과 Biba 모델의 무결성 기반한 MAC
Tandem Guardian 90 With Safeguard	C2	Tandem Computers, Inc.	1993	· 디스크, 파일, 장치, 프로세스등과 같은 객체형태에 따른 DAC지원 · ACL에 의한 개인과 그룹의 접근통제
AS/400 OS 400 Version3 Release	B3	IBM	1997	· 개인/그룹/공용기반 DAC제공 · Multilevel 보안을 위한 MAC, Sensitivity Label제공
Trusted XENIX Version 4.0	B2	Trusted Information Systems, Inc	1993	· 유닉스 permission bits 및 ACL을 이용한 DAC 제공 · BLP모델을 이용한 MAC 정책 지원
OS 1100/2200 Release SB4R7	B1	Unisys Corporation	1994	· BLP모델을 이용한 MAC 정책 지원 · 개인과 그룹의 ACL 기반한 DAC 제공
XTS-300 Release 4.4.2	B3	Wang Government Services, Inc.	1998	· BLP 기반 보안 정책과 Biba기반 무결성 정책의 MAC 제공 · 사용자 식별과 인증, 감사, DAC구현

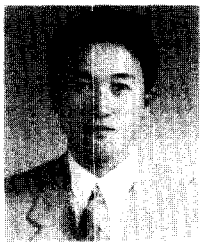
부록 B : ITSEC 평가 제품

제 품 명	평 가 등 급	개 발 사	평 가 시 기	제품의 특징
Racal SAFE 5100	E3	Racal Data Group	1995	· 통신용 암호장비 · 암호를 통한 접근통제
ED2048RU RAMBUTAN Data Encryption Unit	E3	Zergo Ltd	1995	· ACL과 permission bit에 기반한 DAC 제공 · 기밀 레이블에 기반을 둔 MAC 제공
AOS/VS II Versiion 3.10	C2	Data General Corporation	1994	· CCITT G703인터페이스를 사용하는 2Mbps multiplexor통신간의 기밀성 제공
Trusted Oracle 7 Release 7.1.5.9.3	E3	Oracle Corporation	1998	· MAC 지원, 보안 레이블링 제공
Oracle and Trusted Oracle 7 Release 7.0.13.6	E3	Oracle Corporation	1994	· 각각 MAC, DAC 지원 · 보안 레이블링 제공
CA-OpenINGRESS Security Release 1.1	E3	Computer Associates	1994	· 데이터베이스 제품 · MAC, DAC 지원, 감사기능 제공
Access Manager Version250	E2	Platinum Tech. Ltd	1994	· 접근허가 정보가 담긴Role을 통한 통제
Gauntlet Internet Firewall Version 3.2	E3	Trusted Information Systems(UK) Ltd	1997	· 침입차단시스템 · 네트웍간의 안전한 접근통제기능 제공
VINES Version 7.0	E2	Banyan Systems Inc	1997	· 네트웍 상의 모든 서비스에 접근통제 제공
CyberGuard Firewall 2.2.1e	E3	CyberGuard Europe Ltd	1997	· 침입차단시스템 · 네트웍상의 사용자 접근 모니터링
Novell Trusted Netware 4.11	E2	Novell(UK) Ltd	1994	· 네트워킹 제품 · DAC, 공개키 기반 인증
NetSeq Enterprise Network Security Workstation 2.2	E3	Persetel(UK) Ltd	1997	· 네트워킹 제품 · 침입차단, 사용자인증, 암호화, 접속제한
Check Point FireWall-1 Version 3.0	E3	Check Point Software Technologies	1997	· 침입차단시스템 · 접근통제, 인증, 암호화, 감사기능 제공
CyberGuard Firewall for Windows NT, Unixware	E3	Cyberguard Europt Ltd	1998	· 침입차단시스템 · IP패킷에 대한 접근통제, 인증, 무결성보호
Gauntlet Internet Firewall For Windows NT	E3	Trusted Information Systems(UK) Ltd	1998	· 침입차단시스템 · 어플리케이션 레벨의 보안제공
BEST-X/C2(Bull Enhanced Security Technology)1.1.1.9	E3	Bull Information Systems Ltd	1997	· 운영체제 제품 · 패스워드 암호화, 감사, DAC 제공
BEST-X/B1(Bull Enhanced Security Technology)1.1.1.9	E3	Bull Information Systems Ltd	1997	· 운영체제 제품 · MAC, DAC, 패스워드 암호화,인증,감사기능
HP-UX Version 10.10	E3	Hewlett Packard Ltd	1997	· 운영체제 제품 · 각종 인증기능,.ACL 제공
Microsoft Windows NT Workstation 3.51	E3	Microsoft Ltd	1996	· 운영체제 제품 · ACL, User Role, Privileges 제공
DEC MLS+ CMW V3.1A	E3	Digital Equipment Co Ltd	1996	· 운영체제 제품 · POSIX, ACL, 유동적인 감사시스템제공
Sun Trusted Solaris 1.2	E3	Sun Microsystems Federal	1995	· 운영체제 제품 · MAC, DAC, Least Privilege제공
Trusted IRIX/CMW on Cellular IRIX O/S	E3	Silicon Graphics Computer Systems	1997	· 운영체제 제품 · ACL, MAC, DAC, 정보레이블 제공
KILGETTY 1.2g KILGETTY PLUS 1.2g	E3	Software BOX Ltd	1997	· PC기반 접근통제 제품 · Boot, 분산키, 네트웍 접근통제 기능제공

부록 B : ITSEC 평가 제품

제 품 명	평 가 등 급	개 발 사	평 가 시 기	제품의 특징
STOPLOCK V Various Versions	E3	PCSL	1996	· PC기반 접근통제 제품 · Boot, 분산키, 네트웍 접근통제 기능제공
Disknet NT Version 1.65	E2	Reflex Magnetic Ltd	1996	· PC기반 접근통제 제품 · 패스워드를 이용 접근통제,악의S/W보호
Latches 95 Version 5.0	E3	Rhea International Ltd	1997	· PC기반 접근통제 제품 · MAC & DAC, 암호화, Boot, Single Sign on

□ 著者紹介



김 의 탁

1997년 2월 대전대학교 컴퓨터공학과 졸업 (공학사)
1997년 8월 ~ 현재 대전대학교 대학원 컴퓨터공학과 석사과정중

※ 주관심 분야 : CAPI, 접근통제,암호알고리즘

최 용 락

1976년 중앙대학교 전자계산학과
1982년 중앙대학교 전자계산학과 석사
1989년 중앙대학교 전자계산학과 박사
1982년 ~ 1986년 한국전자통신연구원 선임연구원
1986년 ~ 현재 대전대학교 컴퓨터공학과 교수
1997년 한국통신정보보호학회 충청지부 지부장

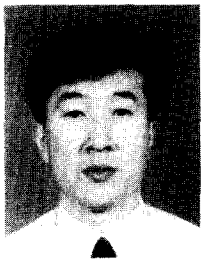
※ 주관심 분야 : 운영체제, 접근통제, 보안API, 컴퓨터통신보안

□ 著者紹介

김 기 현

1993년 2월 경북대학교(학사, 전자공학과)
1995년 2월 경북대학교(석사, 전자공학과)
1995년 7월 ~ 1996년 7월 데이콤 시외전화구축팀
1996년 7월 ~ 현재 한국정보보호센터 기술개발부 시스템기술팀 주임연구원
1997년 10월 ~ 현재 한국정보통신기술협회 정보보호기술연구위원회 간사

※ 주관심 분야 : 컴퓨터 및 네트워크 정보보호



박 정 호

1984년 2월 한양대학교(학사, 산업공학)
1986년 2월 한양대학교(석사, 산업공학)
1990년 7월 ~ 1992년 9월 데이콤 종합연구소 연구원
1992년 10월 ~ 1996년 5월 한국전산원 기술지원단 선임연구원
1996년 5월 ~ 현재 한국정보보호센터 기술개발부 시스템기술팀장

※ 주관심 분야 : 컴퓨터 및 네트워크 정보보호