情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

Secure OS 보안정책 및 메커니즘

홍 기 융*, 김 재 명**, 홍 기 완***

요 약

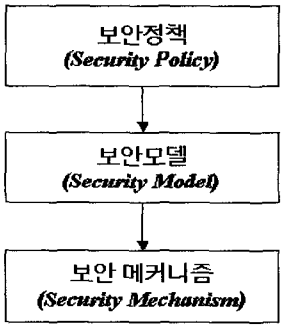
정보보호기술이 '수동형'에서 점차로 '능동형'으로 진화하고 있는 가운데, Secure OS가 능동형 정보보호기술의 핵심으로 주목받고 있다. Secure OS는 서버시스템 보안의 원천적 기술로 접근통제에 관한 보안정책, 보안모델 및 보안메커니즘에 대하여 검증 가능한 방법으로 안전·신뢰성이 확보되어야 한다. 이에 본 논문에서는 Secure OS 핵심기술의 이해와 더불어 Secure OS 개발 시 안전·신뢰성을 확보하기 위하여 이론적으로 잘 정립되고 정형화된 보안정책, 보안모델 및 보안메커니즘에 대하여 살펴본다.

Ⅰ. 서 론

최근의 IT 정보보호기술동향은 '수동형(Reactive) 방어' 개념에서 '능동형(Proactive) 방어'개념으로 진화하고 있다. 기존의 방어개념은 보안침해사고의 단순 모니터링 또는 탐지만 할 수 있는 특성을 갖고 있는 것에 반해, 새로운 개념인 '능동형 방어기술'은 불법 침입이나 해킹으로부터 불법 행위가 발생하기 이전에 능동적으로 탐지하고 차단한다[1].

이렇듯 능동형 정보보호기술은 차세대 정보보호기술의 핵심기술로 연구가 활발하며, 특히 보안침해사고의 최종 목적인 시스템과 저장 데이터에 대한 보호기술로 Secure OS가 주목을 받고 있다. Secure OS는 컴퓨터 운영체제(OS: Operating System) 상에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안기능이 통합된 보안커널(Security Kernel)을 이식한 운영체제이다[2].

한편, Secure OS 등의 정보보호시스템은 안전·신뢰성을 증명하기 위하여 개발공정의 정확성과 보안모델 등에 대하여 보증 요구사항(Assurance Requirements)을 만족해야 한다. 특히, Secure OS는 이러한 요구사항을 만족하기 위하여 초기 요구사항 분석부터 구현에 이르는 개발공정 상의 안전·신뢰성을 확보해야 하며, 이를 위한 Secure OS의 개발공정은 [그림 1]과 같다[3].



[그림 1] Secure OS 개발공정

보안정책은 조직에서 정의한 최상위 보안 요구사항의 모음이며, 보안모델은 보안정책을 검증 가능한 형태로 지원하기 위한 정형화된 보안규칙이며, 보안메커니즘은 보안정책 및 보안모델을 실현하기 위한 구체적인 구현 방법론이다[4].

보안정책에 대한 정의는 다수 존재하나, 일반적으로 TCSEC(Trusted Computer Security Evaluation Criteria)[5]과 ISO(International Standard of Organization)[6]의 기준을 준용한다. TCSEC의 경우는 보안정책을 임의적 접근통제(DAC: Discretionary Access Control) 정책과 강제적 접근통제

* (주)시큐브/(주)케이사인 대표이사
** (주)시큐브 상무이사
*** (주)시큐브 기술이사

(MAC: Mandatory Access Control) 정책으로 구분하며, ISO의 경우에는 임의적 접근통제와 강제적 접근통제 용어를 사용하지 않고 신원기반(Identity-based Access Control) 정책과 규칙기반(Rule-based Access Control) 정책으로 구분하고 있다. 실제적인 목적에 있어서는 신원기반 정책과 규칙기반 정책은 각각 임의적 접근통제 및 강제적 접근통제 정책과 동일하다. 한편, 이와는 다르게 최근에 디지털 저작권을 보호하기 위한 보안정책으로 개시자 접근통제(ORCON: Originator Control)[7]도 유용한 보안정책으로 인식되고 있다.

보안모델은 보안정책을 정형화하기 위한 수단으로 자체개발할 수도 있으나, 이론적으로 잘 정립된 모델을 많이 이용하며, 대표적으로 HRU[8], BLP[9], BIBA[10], Lattice[11], Take-Grant[12]모델 등이 널리 알려져 있다.

보안메커니즘은 보안정책 및 보안모델을 실현하기 위한 구체적인 구현 방법론으로, 널리 사용되는 보안메커니즘으로는 ACL(Access Control List)[3], CL(Capability List)[3], SL(Security Label)[3], II (Integrated Information)[13], Protection Bits[13] 메커니즘 등이 존재한다.

이와 같이, Secure OS의 보안성을 강화하기 위해서는 잘 정의되고 검증된 보안정책, 보안모델 및 보안메커니즘을 사용하여 Secure OS 개발공정에 대하여 안전·신뢰성을 확보해야 한다. 이에 본 논문에서는 Secure OS와 관련된 보안정책, 보안모델 및 보안메커니즘의 기술 및 동향에 대하여 상세히 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서는 Secure OS와 관련된 보안정책에 대하여 기술하며, 3장에서는 Secure OS와 관련된 보안모델을 기술한다. 4장에서는 Secure OS와 관련된 보안메커니즘에 대하여 기술하며, 5장에서는 본 논문의 결론에 대하여 기술한다. 마지막으로 참고문헌에서는 본 논문에서 참조한 참고문헌을 기술한다.

II. 보안 정책(Security Policy)

Secure OS 보안정책은 일반적으로 신원기반 정책과 규칙기반 정책 또는, 임의적 접근통제 정책과 강제적 접근통제 정책으로 구분되며, 최근에는 금융 등의 환경에서 조직원의 역할에 따라 접근통제가 이뤄지는 직무기반(Role-based) 접근통제 정책이 사용되기도 한다. 또한, 최근에 디지털 저작권 보호를 위한 개시자 접근통제(ORCON) 정책도 등장하였다.

1. 신원기반 정책(Identity-based Policy)

ISO의 신원기반 접근통제 정책과 동일한 개념을 TCSEC에서는 임의적 접근통제 정책으로 정의하고 있다. 즉, 주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한하는 방법을 임의적 접근통제 정책이라고 정의한다. 접근통제는 임의적이므로 어떠한 접근 허가를 넘겨줄 수 있다.

임의적 접근통제 정책은 각 개인 및 그룹들로 나누어 IBP(Individual-Base Policy)와 GBP(Group-Based Policy)두 가지로 분류된다. IBP는 어떤 사용자가 어떤 행동을 할 수 있는지 각 대상별로 목록을 표현하며, 이것은 하나의 대상에 대하여 접근행렬의 열을 나타내는 것과 같다. GBP는 다수의 사용자가 하나의 대상에 대하여 동일한 허가를 부여받는 방식이다.

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

임의적 접근통제 정책은 접근을 요청하는 사용자의 식별에 기초하며, 어떤 객체에 대하여 사용자가 접근권한을 추가 및 철회할 수 있다는 의미에서 임의적이다. 이것은 소유권을 통한 관리적 제어가 분산됨을 의미한다. 그러나, 임의적 접근통제 정책은 중앙 집중관리를 위해서도 적합하며, 이 경우에 권한부여는 시스템 관리자에 의하여 관리될 것이다. 임의적 접근통제 정책이 갖는 일반적인 속성을 살펴보면 다음의 3가지로 요약할 수 있다.

- 임의적 접근통제 정책은 허가된 주체(즉, 객체의 소유자)에 의하여 변경 가능한 하나의 주체와 객체간의 관계를 정의한다.
- 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근통제정보가 복사된 객체로 전파되지 않는다.
- 임의적 접근통제 정책은 모든 주체 및 객체들 간에 일정하지 않고 하나의 주체/객체 단위로 접근제한을 설정할 수 있다. 즉, 비록 임의적 접근통제 정책이 어느 한 주체로 하여금 특정 비밀등급의 한 객체를 접근하지 못하게 할지라도, 그 주체

는 다른 주체가 그러한 비밀등급을 갖는 다른 객체들을 접근하는 것을 방지할 수 없다.

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

2. 규칙기반 정책(Rule-based Policy)

ISO의 규칙기반 접근통제 정책과 동일한 개념을 TCSEC에서는 강제적 접근통제 정책으로 정의하고 있다. 즉, 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법을 강제적 접근통제 정책이라고 한다. 강제적 접근통제 정책은 사용자 및 대상별로 부여된 기밀 분류에 따른 정책과 조직 내의 각 부서별로 구분된 기밀 허가에 따르는 정책으로 분류되며, 전자의 경우는 MLP(Multi-Level Policy)이며, 후자의 경우는 CBP(Compartment-Based Policy).

강제적 접근통제 정책은 분류된 시스템 데이터와 각 등급의 사용자간에 강력한 보호를 위하여 요구되는 많은 정보들을 적용한다. 강제적 접근통제 정책은 또한 하위 비밀등급의 객체로 정보의 흐름을 방어하기 때문에 정보흐름 통제(Information Flow control) 정책으로 정의될 수 있다. 데이터에 대한 접근은 주체와 객체가 갖는 보안등급의 정의를 통한 강제적인 정책에 의하여 결정된다. 객체 보안 등급의 2가지 주요특성을 포함하고 있는 정보를 반영한 허용등급(Classification Level)과 객체 정보가 언급하는 응용분야의 범주(Category)로 구성된다.

각 주체와 객체는 객체의 허용등급을 나타내는 기밀수준과 범주의 집합으로 구성된 보안등급을 할당한다. 이 2개의 요소는 시스템에서 주체 및 객체 자신의 역할과 대응되는 것이다. 주체의 등급은 그 주체에 할당될 수 있는 신뢰의 정도를 나타내고 객체의 등급은 정보의 부당한 사용에 의한 손상정도를 고려한 객체에 포함된 정보의 기밀성을 반영한 것이다.

공리의 집합은 보안 평가지침에 따라 객체를 접근하려는 주체를 허용하기 위하여 주체와 객체 사이에 검증될 관계를 결정한다. 이러한 관계는 접근 모드에 의존한다. 접근권한 전송과 관련하여 할당된 권한은 변경될 수 없고 권한을 갖는 관리자에 의해서만 수정이 허용된다. 이것은 접근통제 시스템상의 모든 권한 통제가 권한을 갖는 보안관리자에 의해서만 유지됨을 의미한다.

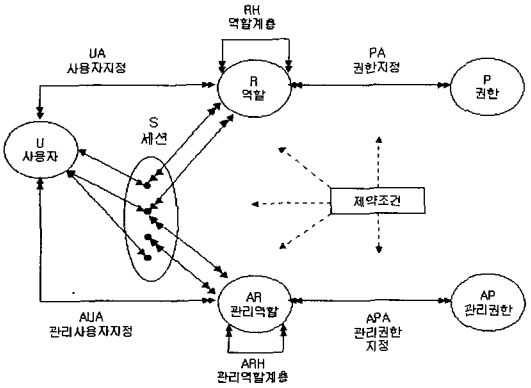
주체 및 객체 강제적 접근통제 관계에서 존재하여야 할 접근 조건은 다음과 같다:

- 한 주체는 하나의 객체를 오직 다음의 경우에 판독할 수 있다.
  : 주체의 비밀 등급에서의 계층적 분류들이 객체의 비밀등급에서의 계층적 분류보다 크거나 같고, 주체의 비밀등급에서의 비계층적 범주들이 객체의 비밀등급에서의 모든 비계층적 범주들을 포함하는 경우.
- 한 주체는 하나의 객체를 오직 다음의 경우에 기록할 수 있다.
  : 주체의 비밀 등급에서의 계층적 분류가 객체의 비밀 등급에서의 계층적 분류보다 작거나 같고, 주체의 비밀 등급에서의 비계층적 범주들이 객체의 비밀 등급에서의 비계층적 범주들에게로 포함되는 경우.

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

3. 직무기반(Role-based) 정책

직무기반 정책은 현대의 상업용 환경에서 특히 가치가 있는 다른 형태의 정책으로 접근통제 정책을 정형화하는 구문 의미적 측면에서 직무(Role)가 그룹에 대응된다. 즉, 정보에 대한 사용자의 접근은



[그림 2] 직무기반의 접근통제

개별적인 신분이 아니라 조직 내에서 개인의 직무(또는 직책)에 따라서 결정된다.

[그림 2]는 Ravi S. Sandhu의 직무기반 접근통제 모델로 상위 부분은 일반적인 자원에 대한 사용자의 권한과 역할을 나타내고 있다. 하위 부분은 관리 권한과 관리 역할을 나타낸다.

직무기반의 접근통제 모델은 개념적으로 보면 크게 사용자(U), 역할(R), 권한(P)으로 구성된다. 일반적으로 이 모델에서 사용자는 사람을 나타낸다. 역할은 사용자와 권한의 집합으로 구성되며, 조직 내의 작업 함수(Job Function) 또는 작업의 제목(Job Title)을 나타낸다.

권한은 자원에 대한 접근권한을 나타낸다. 권한은 자원에 대한 특정한 접근권한을 나타낸다. 하나 혹은 그 이상의 자원에 적용될 수 있다. 세션(Session)은 사용자가 속해있는 역할에서 부분집합을 활성화 시킬 때 생성이 되기 때문에 일시적이다. 사용자는 자격과 책임을 기반으로 역할에 지정되고, 하나의 역할에서 다른 역할로 쉽게 재 지정될 수 있다. 또한, 여러 가지의 역할을 할당받을 수도 있다. 사용자와 권한의 관계는 일시적이다. 역할은 특정한 작업을 수행할 수 있는 능력과 특정한 위치에 지정됨으로써 가질 수 있는 권한 및 책임으로 표현된다. 따라서 사용자는 역할에 지정됨으로써 그 역할에서 특정 작업을 수행할 수 있는 능력을 갖게 된다.

다른 접근 모델에서 일반적으로 표현하고 있는 그룹과 직무기반 접근통제 모델에서 정의한 역할의 가장 큰 차이점은 그룹에는 자원에 대한 접근권한이 나타나지 않는다는 것이다. 그룹은 권한의 집합이 아니라, 사용자의 집합으로 표현되며, 역할은 사용자와 그 역할이 갖는 권한들의 집합으로 나타낸다.

직무기반 접근통제 모델의 구성요소들을 간단히 정리하면 다음과 같다.

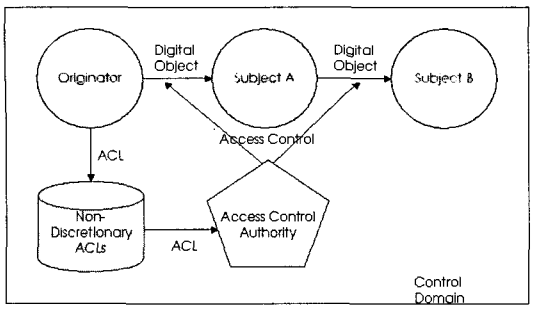
- U, S : 사용자 집합, 세션의 집합
- R과 AR : 정규역할과 관리역할
- P와 AP : 정규권한과 관리권한
- PA⊆P×R : 권한과 역할지정 관계(Many-to-Many)
  APA⊆AP×AR : 권한과 관리역할 지정 관계 (Many-to-Many)
- UA⊆U×R : 사용자와 역할지정 관계 (Many-to-Many)
  AUA⊆U×AR : 사용자와 관리역할 지정 관계 (Many-to-Many)
- RH⊆R×R : 역할계층이나 역할의 유전 관계를 부분 순서로 나타냄
  ARH⊆AR×AR : 부분 순서화된 관리역할 계층
- Constraint : 제약조건

4. ORCON 정책

ORCON 정책은 디지털 객체에 대해 개시자의 동의를 얻기 위한 접근제어 정책이다. ORCON 정책은 강제적 접근통제 정책과 임의적 접근통제 정책을 합친 중간 정도의 특성을 갖는다. 원본 객체의 보안 정책이 파생 객체에게 전달되는 면에서는 강제적 접근통제 정책과 유사하다. 그러나 ORCON 정책은 기본 주체/객체 정보가 수정될 수 있는데 반해 강제적 접근통제 정책은 주체에 대한 객체의 정책이 일관 된다는 점에서 다르다. 또한 객체의 개시자(Originator)에 의해 객체의 접근 정책이 변경될 수 있는 면에서 임의적 접근통제 정책과 유사하다.

ORCON 정책은 객체의 개시자만이 객체의 접근 정책을 변경할 수 있는데 반해, 임의적 접근통제 정책은 소유주가 복사된 객체에 대해서도 접근 정책을 변경할 수 있다는 면에서 다르다.

[그림 3]은 ORCON 정책의 개념을 도식화 한 것으로 이에 대한 설명은 다음과 같다. 개시자가 생성한 객체는 "ORCON"으로 표시되게 되고, 주체 A가 접근할 수 있도록 접근제어 정책을 수립한다. 그러면 주체 A는 객체를 접근할 수 있게 된다. 그러나 같은 객체에 대해서 주체 B가 객체에 접근하려고 하면 접근 정책에 의해 접근이 거부 된다. 객체가 복사 되더라도 "ORCON" 표시도 복사되기 때문에 개시자는 복사된 객체의 접근 제어 정책을 수립할 수 있게 된다. 이러한 ORCON 보안정책은 디지털 컨텐츠를 보호하기 위한 목적으로 사용되고 있다.



〔그림 3〕 ORCON 보안정책

Ⅲ. 보안모델(Security Model)

Secure OS 보안모델은 보안정책을 검증가능한 형태로 지원하기 위한 정형화된 모델로, 보안정책에 따라, DAC 보안정책에는 HRU 모델을, MAC 보안정책에는 BLP, BIBA 모델 등을, 정보흐름 정책에는 Lattice 모델을, RBAC 보안정책에는 RBAC 보안모델을 적용한다.

1. HRU 모델

HRU 모델은 Michael A. Harrison과 Walter L. Ruzzo 그리고 Jeffery D. Ullman이 개발한 모델로서 접근행렬 모델에 근간을 둔 보안모델로, 접근 행렬 모델의 표현 방법과 그 의미는 다음과 같다.

- 모델은 상태와 상태 전이로 정의된다.
- 상태는 행렬로 표현된다.
- 상태 전이는 명령어로 기술된다.

HRU 모델에서 보호 시스템은 접근 권한에 대한 유한 집합 R과 명령어에 대한 유한 집합 C의 2가지 부분으로 구성되며, 유한집합 C의 명령어 구조는 다음과 같다.

```
Command ∝(X1 ,X2,...., Xk)
if   r1 in (Xs1,Xo1)and
     r2 in (Xs1,Xo2)and
      ..................
     rm in (Xsm,Xom)
then
     OP1
     OP2
     .....
     OP
end
```

상기의 명령어 구조에서 의미하는 기호의 정의는 다음과 같다.

- ∝ : 명령어 이름 / X1, X2, …, Xk : 파라메터 / OPi : 오퍼레이션
- r, r1, r2, …, rm : 접근 권한 / s, s1, s2, …, sm, o, o1, o2 …, om : 정수

한편, HRU 모델에서는 6개의 기본적인 연산이 존재하는데, 이를 설명하면 다음과 같다.

- Enter r into (Xs, Xo) : 이 연산은 주체/객체 쌍에 대한 접근 모드를 접근 행렬의 해당 엔트리에 입력한다.
- Delete r from (Xs, Xo) : 이 연산은은 주체/객체 쌍에 대한 접근 모드를 접근 행렬의 해당 엔트리에서 제거한다.
- Create Subject Xs : 이 연산은 새로운 주체를 생성한다.
- Create Object Xo : 이 연산은 새로운 객체를 생성한다.
- Destroy Subject Xs : 이 연산은 주체를 제거한다.
- Destroy Object Xo : 이 연산은 객체를 제거한다.

2. BLP 모델

MITRE의 D. Bell과 L. LaPadula에 의해 개발된 Bell and LaPadula(이하 BLP) 모델은 컴퓨터 보안 모델에서 가장 널리 사용되고 있는 모델 중 하나로, 유한 상태머시인(Finite State Machine) 모델에 근간을 둔 Formal 모델이다. 대표적 특성으로는 "No Read Up"과 "No Write Down"이 있으며, BLP 모델에서 정의되는 시스템 상태 V는 다음과 같이 정의한다.

- V=(B×M×F×H)
  - B : 현재의 접근 집합, S×O×A의 부분집합
    ※ S : 주체들의 집합, O : 객체들의 집합
    ※ A : 접근모드(r:읽기, w:쓰기, a:기록, e:수행)의 집합
  - M : 접근 허가 행렬
  - F : 3개의 함수로 구성됨.

i) Fs : 각 주체에 대한 신원(Clearance)
ii) Fo : 각 개체에 대한 비밀등급(Security Level)
iii) Fc : 각 주체에 대한 현재의 비밀등급(Current Security Level)
- H : 현재의 객체 계층(Object Hierarchy)

한편, BPL 모델에서의 시스템의 안전한 상태 개념은 다음의 3가지 보안 특성에 의하여 결정되며, "시스템 상태는 ss-특성, S'에 대한 *-특성, 그리고 ds-특성을 만족해야만, 시스템 상태가 안전하다"고 정의한다.

• ss-특성(simple-security property)
- Read access 또는 write access 모드를 갖는 B의 각 원소에 대하여 주체의 신원이 객체의 비밀 분류보다 크거나 같으면 상태는 ss-특성을 만족한다.
- Access 모드가 execute 또는 append이거나, access 모드가 read 또는 write이고 Fs(S)가 Fo(O)를 지배하면 (S, O, x)는 F에 대한 ss-특성을 만족한다.

• *-특성(star property)
- B에 있는 각 (S, O, x)에 대하여 다음과 같은 경우에 상태는 *-특성을 만족한다.
  → Access 모드가 read 및 write일 때, S의 현재 비밀 등급이 O의 비밀 등급과 같다.
  → Access 모드가 read일 때, S의 현재 비밀 등급이 O의 비밀 등급과 크거나 같다.
  → Access 모드가 write일 때, S의 현재 비밀 등급이 O의 비밀 등급 보다 작거나 같다.

• ds-특성(discretionary property)
- B의 각 원소에 대하여, 명시된 접근 모드가 주체/객체 쌍을 위한 접근 행렬에 포함되어 있다면 상태는 ds-특성을 만족한다.

BLP 모델은 강제적 접근통제 정책 및 임의적 접근통제 정책의 보안정책을 지원하는데, 강제적 접근통제 정책은 ss-특성(simple-security property) 및 *-특성(star property)에 의해 결정되며, 임의적 접근통제 정책에 있어서는 ds-특성(discretionary property)에 의하여 결정된다.

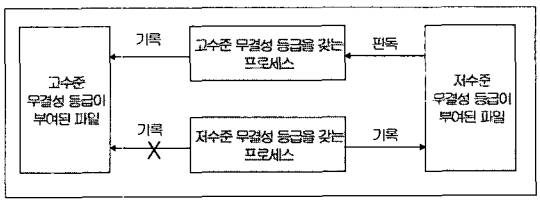
3. BIBA 모델

MLS(Multi Level Security)[5] 정책은 비밀성 보장에 중점을 두고 있으나 정보의 불법적인 수정을 방지하고자 하는 보안 특성은 결여되어 있었다. BIBA 무결성 모델은 MLS의 이러한 점을 보완하여 정보의 불법적 수정을 방지하기 위해 고안된 모델이다. BIBA 모델은 무결성을 보장하기 위해 무결성 등급에 따라 Read 및 Write를 통제한다. BIBA 모델에서 제시하는 보안 규칙은 2가지가 있으며, 이에 대한 설명은 다음과 같다.

• 규칙 1 : Simple Integrity
- 주체의 무결성 등급이 객체의 무결성 등급을 지배한다면(Dominate) 주체는 객체에 대하여 기록할(Write) 수 있다("No Write Up" 특성).

• 규칙 2 : Confinement Integrity
- 객체의 무결성 등급이 주체의 무결성 등급을 지배한다면(Dominate) 주체는 객체를 판독할(Read) 수 있다.

BIBA 모델은 BLP 모델과 비교하였을 경우, 다음과 같은 차이점이 있다. 보안속성인 등급의 경우 BLP 모델은 비밀등급을 사용하나, BIBA 모델은 무결성 등급을 사용한다. 또한, BLP 모델의 특성은 "No Read Up"의 정보흐름 특성을 갖고 있으나, BIBA의 경우 "No Write Up"의 특성을 가지고 있다. [그림 4]는 무결성 보안 모델에 의해 등급에 따라 기록 및 판독 접근권한이 제한된 것을 보여주고 있다.



[그림 4] 무결성 보안모델

4. Lattice 모델

Lattice 보안 모델은 컴퓨터의 정보 흐름을 통제할 목적으로 D. E. Denning에 의해 개발되었다. 기존의 보안 모델은 정보의 보안성이나 무결성을 보장하기 위한 모델이라면 lattice모델은 보안성이 있

는 정보의 흐름을 통제하기 위한 모델이다. 일반적으로 보안정책에서는 각 객체가 지니고 있는 정보의 비밀수준에 따라 비밀 등급이 부여되고 있으며 각 주체도 어떤 종류의 정보를 접근할 수 있는가를 나타내는 비밀 인가를 갖는다. 이러한 주체나 객체에 부여된 비밀 인가나 비밀등급은 비밀 클래스로 나타내기도 한다. 비밀 클래스가 부여된 각 객체와 주체는 한 컴파트먼트에 속해 있는데 모든 객체는 최소권한 원칙에 따라 분류된다. 그리고 객체나 주체의 비밀 클래스는 비밀 수준과 컴파트먼트로 이루어지는 순서쌍이다.

- 비밀 클래스 SC=(A,B)
- 단, A는 비밀 수준, B는 컴파트먼트를 의미한다.

따라서 컴퓨터 시스템의 모든 객체와 주체는 보안정책면에서 위와 같은 비밀 클래스의 집합으로 볼 수 있는데, 이러한 시스템에서 정보의 안전한 흐름을 보장하기 위해서 비밀 클래스의 집합에 부분 순서를 부여한 후 이들 집합을 하나의 래티스로 구성한다. 이러한 개념에 근간을 둔 정보 흐름 모델은 다음과 같이 정의한다.

FM = <N, P, SC, ⊕, →>

- N={a, b, ……,} : 논리적 기억장소 객체 집합 N의 원소는 파일, 세그먼트, 사용자 등임
- P={p, q, ……} : 프로세스 집합
- SC={A, B, ……} : 보안등급
- ⊕ : 보안등급 결합 연산자
- → : 흐름 관계

예를 들어, A→B는 클래스 A의 정보가 클래스 B로 흐르는 것을 허용한다는 것을 의미 한다. 〈SC, →, ⊕〉는 래티스를 구성하며 다음의 의미를 갖는다.

1) 〈SC, →〉는 부분 순서 집합이다.
2) SC는 유한하다.
3) SC는 하한 L을 갖는다.
4) ⊕는 SC의 최소 상한(Least Upper Bound)을 의미하는 오퍼레이터임

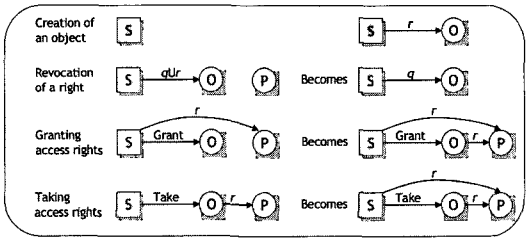
여기서 4)는 최대 하한 오퍼레이터 ⊕가 존재함을 의미하며, 유일한 상한 H가 존재함을 의미한다. 따라서 〈SC, →, ⊕〉는 하한 L과 상한 H를 가진 래티스이다.

래티스에서 안전한 흐름을 보장하는 정보 흐름 통제는 비밀 클래스의 부분 크기 순서에 따라 통제되는 것으로 어느 한 객체 X에서 다른 객체 S로의 가능한 정보 흐름 조건은 다음과 같다.

조건 1 : 객체 S는 객체 X의 비밀 수준보다 크거나 같다.
조건 2 : 객체 S가 속해 있는 컴파트먼트는 객체 X가 속해 있는 컴파트먼트를 포함한다.

5. Take-Grant 모델

Take-Grant 보안 모델은 Jones에 의해 소개되었고 Lipton과 Synder에 의해 확장되었다. 이 모델에서는 Create, Revoke, Take, Grant의 4개의 연산만 가능하다. [그림 5]는 Take-Grant 모델의 접근권한을 나타낸 것이다.



[그림 5] Take-Grant 모델 접근권한

- Create(o, r) : S는 O에 대해 권한을 생성한다. [그림 5]에서는 S의 O에 대한 권한을 r로 표시한다.
- Revoke(o, r) : S는 O에 대한 권한을 취소한다. [그림 5]에서는 S의 O에 대한 권한이 취소를 q로 표시했다.
- Grant(O, P, r) : 만약 S가 O에 대해 Grant 권한을 갖고 있고, P에 대해 권한도 있으면 S는 O에게 P의 권한을 가지도록 권한을 양도 할 수 있다. S가 O에 대해 Grant 권한만 있으면 S는 O와 권한을 공유 할 수 있다.
- Take(O, P, r) : 만약 S가 O에 대해 Take 권한을 갖고 있고, O가 P에 대해 권한이 있다면 주체 S는 O의 P에 대한 권한을 얻을 수 있다.

Ⅳ. Secure OS 보안메커니즘

Secure OS 보안메커니즘은 보안정책 및 보안모델을 실현하기 위한 구체적인 구현 방법론으로 하드웨어 또는 소프트웨어로 구현될 수 있다. 널리 알려진 보안메커니즘으로는 ACL(Access Control List), CL(Capability List), SL(Security Label), II(Integrated Information), Protection Bits 메커니즘이 있다.

1. ACL(Access Control List) 메커니즘

ACL 메커니즘은 어떤 사용자들이 대상에서 어떤 행위를 할 수 있는지 나타낸다. ACL의 유지와 접근통제의 시행은 본질적으로 대상의 시스템 책임이다. ACL 메커니즘은 관련된 객체에 대하여 접근행렬에서 열의 내용을 반영한다. 그러므로 신원기반 접근통제 정책은 ACL을 사용하여 직접적인 방법으로 실현될 수 있다. 또한, 기본적 ACL 개념은 특정의 선택된 사용자 엔트리에 대해서 접근통제조건을 추가하여 수행하는 것과 같은 여러 가지 방법으로 확장 이용될 수 있다. [표 1]은 ACL의 예를 나타내고 있다.

[표 1] 객체 A의 ACL 예제

사용자	접근허가
a	1, 2
b	
c1	1
c2	1

※ 1 : read, 2 : write, 3 : execute

ACL 메커니즘은 구분될 필요가 있는 사용자(개인, 그룹, 또는 직무)가 비교적 소수 일 때와 그러한 사용자의 분포가 안정적일 때 가장 적합하다. ACL의 관리는 대상이 되는 사용자가 너무 많고 자주 변경될 때 어려운 문제가 될 수 있다. 다른 메커니즘과는 달리 ACL은 대상 단편들이 넓은 영역인 경우에 적합하다. 또한, 대상의 소유자 또는 관리자가 앞서 부여된 허가를 사용하기 쉽게 하는 장점이 있다. ACL 메커니즘은 FTAM(File Transfer, Access, and Management)과 디렉토리 응용분야에서 일반적으로 사용된다.

ACL의 기본적 특징을 요약하면 다음과 같다.

- 이 메커니즘의 접근통제는 대상-기반 ACI(Access Control Information)로써 개시자 및 동작의 수식어 목록, 그리고 개시자-기반 ACI로서 개인, 그룹, 또는 직무 식별자 등의 정보를 이용하여 관리된다.
- 개시자 또는 개시자의 그룹이 소수일 때 편리하다.
- 대상 또는 대상의 그룹에 접근을 할 때 편리하다.
- 하나의 대상에 모든 사용자가 대응되므로 목록이 길어지면 유지 및 탐색 오버헤드가 크다.
- 특정 개시자에 대한 대상들의 지역성이 없으므로 다수의 대상을 찾는데 시간이 많이 걸리고, 비효율적이다.
- 개인 또는 그룹의 개시자 모집단이 자주 변경 될 때는 불편하지만 대상의 모집단이 유동적인 경우는 편리한 점이 있다.

2. CL(Capability List) 메커니즘

CL 메커니즘은 일찍이 컴퓨터 접근통제 개념으로 소개되었다. Capability는 명시된 대상을 규정된 방법으로 접근하도록 권한을 부여받은 개시자가 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.

CL 메커니즘은 사용자에 대하여 저장된 접근 허가 목록에 근거하여 개시자의 환경에서 생성된다. 접근 행렬의 항목에서 CL의 생성은 관련된 사용자에 대하여 접근 행렬의 행에 있는 지식을 사용한다. [표 2]는 CL의 예를 나타내고 있다.

[표 2] 사용자 A의 CL 예제

대상	접근자격
x	1, 2
y	
z	1, 2, 3

※ 1 : read, 2 : write, 3 : execute

CL 메커니즘은 밀결합 시스템에서 보다 네트워크 환경에서 적용성이 적다. 네트워크는 보통 다중 보안 영역을 포함하고 있으며, 대상을 포함하고 있는 보안 영역은 그 대상에 관련된 접근통제결정에 발언권을 요구한다. 그러나, CL 메커니즘은 비교적 대상이 적을 경우에 적합하며 개시자와 가까운 곳에서 접근통제결정이 발생할 때 편리하다. CL 메커니

즘의 구현은 시스템 사이에 CL을 전달하는 안전한 수단에 의존적이다. CL의 단점은 대상의 소유자 또는 관리자가 먼저 승인된 허가를 취소하기가 쉽지 않다는 점이다.

CL의 기본적인 특징은 다음과 같다.

- 접근통제는 어떤 대상에 대하여 허용된 동작들의 집합을 정의하는 개시자-기반 ACI(capability)를 갖고 관리된다.
- 대상의 수효가 적을 때 편리하다.
- 하나의 개시자가 접근할 수 있는 다수의 대상을 쉽게 찾을 수 있다.
- 보안이 부분적으로 깨질 때 그 영향을 최소화 시킬 수 있다.
- 주어진 객체를 접근할수 있는 사용자를 파악하는데 시간이 많이 걸리고 비효율적이다.
- 개시자에게 일단 승인된 Capability를 개별적으로 식별해야 하므로 하나의 대상에 대한 접근을 취소하는 것이 불편하다. 그러나, 개시자의 보안 영역 권한을 이용하여 개시자의 접근 권한을 취소하는 것은 편리하다.

3. SL(Security Label) 메커니즘

일반적으로 사용되는 용어로서 보안 레이블은 통신되거나 또는 저장되어 있는 데이터 항목, 물리적인 자원 및 사용자와 같은 객체에 부여된 보안 속성 정보의 집합이다. 접근통제의 배경에서 보안 레이블은 사용자, 대상, 접근 요청 또는 전송중인 접근통제정보에 부여된다.

접근통제 메커니즘으로서 보안 레이블의 가장 일반적 사용은 다중-수준 접근통제정책을 지원하는 것이다. 개시자의 환경에서 개시자의 비밀수준을 식별하는 레이블이 모든 접근요청에 부여된다. 이 레이블은 신뢰된 프로세스에 의하여 생성 및 부여되어야 한다. 모든 대상은 또한 자신에게 부여된 비밀 수준을 나타내는 레이블을 갖고 있다. 접근 요청을 처리할 때 대상 환경은 대상에 있는 레이블과 요청에서 받은 레이블을 비교하고 접근을 승인할 것인지, 또는 부인할 것인지 결정하기 위하여 정책규칙을 적용한다.

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

보안 정책/기관 식별은 특히 중요한데, 이것은 모든 다른 항목들의 의미가 보안정책에 의존적이기 때문이다. 하나의 보안 영역에서 생성된 레이블은 다른 영역에서는 중요하지 않을 수도 있다. 예를 들면, 동일한 형식의 레이블이 두 개의 다른 기관에 의하여 다중 수준 정책을 갖고 생성된다고 하자. 첫번째 기관에서 기밀(confidential)로 분류된 정보가 다른 기관에서 기밀 레이블을 갖는 사람에게 반드시 개방될 필요가 있는 것은 아니다. 그러나, 만일 두 기관이 적절한 보안정책 관계(하나의 공통 집단 회원일 경우)를 갖는다면 몇 가지 접근허가/허용등급은 양쪽 영역에서 의미가 있게 할 수 있다. 레이블-기반 접근통제 메커니즘은 MHS(Message Handling System)에서 사용될 수 있다.

보안 레이블의 기본적 특징을 요약하면 다음과 같다.

- 이 기법의 접근통제는 시스템 사이에서 전달되는 개시자와 대상, 그리고 데이터에 할당 될 수 있는 보안 레이블을 사용한다.
- 다수의 대상을 다수의 개시자들이 접근하고 있을 때, 또는 접근통제의 일부분만이 요구될 때 가장 편리하다.
- 주어진 어떤 정책 제한이 하나의 보안 영역 안에서 데이터의 흐름을 제어하기 위하여 사용될 수 있다. 또한, 보안 레이블이 영역 사이의 접근통제를 제공하는데 편리하다.
- 허용된 동작이 개시자-기반 또는 대상-기반 ACI에 명확히 포함되지 않을 때 보안 정책의 부분으로서 정의하기 편리하다.

4. II(Integrated Information) 메커니즘

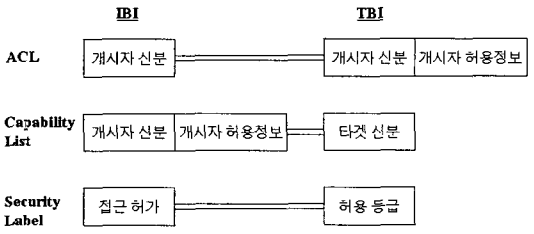
ACL, CL 및 SL의 세가지 형태의 메커니즘은 역사적으로 접근통제 정책을 구현하는 별도의 방법으로 고려되어 왔다. 그러나, 현대의 네트워크 접근통제 메커니즘들은 세가지 형태중의 한가지로 실현되지 않고 적어도 두 가지의 복합된 특성으로 실현되는 추세이다.

ECMA(European Computer Manufacturers Association)에 의하여 제청되고 나중에 ISO/IEC

10181-3에서 인정된 새로운 관점이 있다. 즉, 3가지 형태의 메커니즘과 그들의 변형을 분리하여 인식할 수 없는 하나의 연속체로 생각하는 통합적 정보(Integrated Information)에 의한 접근통제 메커니즘 관점이다.

접근통제결정은 IBI(Initiator-Bound Information)과 TBI(Target-Bound Information)과 같은 다양한 형태의 접근통제정보에 기반하고 있다. IBI는 직접 개시자에 연관되어 있고, 그것의 출처는 개시자의 영역이다. TBI는 대상에 직접 연관되어 있고, 그것의 출처는 대상의 영역이다.

〔그림 6〕은 ACL, 보안 레이블 및 Capability 메커니즘에서 사용되는 ACI가 어떻게 IBI와 TBI에 대응하는지 나타내고 있다. ACL에 대하여 단지 요구되는 IBI는 개시자의 신분에 대한 지식이고, 반면에 개시자의 신분과 동작 허가를 기술하고 있는 TBI가 있다. 역으로, capability에 대해서는 대상 신분과 허가에 관한 IBI가 Capability를 생성하는데 사용되고, 반면에 요구되는 TBI는 대상의 신분에 관한 지식뿐이다. 보안 레이블 메커니즘은 IBI와 TBI로서 각각 접근허가와 허용등급으로 불리는 레이블-기반 구조를 이용한다.



〔그림 6〕 ACI 형태

5. Protection bits 메커니즘

보호 비트 메커니즘은 ACL의 수정된 형태로서 각 객체에 접근허가를 나타내는데 비트를 사용한다. 접근 권한 구조 및 접근 모드의 정의는 다음과 같다.

① Owner/Group/World 구조에 대해서
② Read/Write/Execute/Delete/List 접근모드로 정의함

예를 들어 World 구조에 Read/Execute 비트가 설정되어 있다면, 파일을 소유한 주체와 주체가 속한 그룹을 제외한 나머지 주체는 그 객체에 대해서 읽기와 실행권한을 가지는 것이다. 이러한 Protection bits를 사용함으로써 객체에 부과되는 메모리를 절약할 수 있는 장점이 있으며, 특정 주체가 접근 할 수 있는 모든 객체의 목록을 알기 어려운 관리상의 단점이 있다.

V. 결 론

Secure OS의 안전·신뢰성을 위해서는 이론적으로 잘 정립된 이론과 모델의 개발이 필수조건이다. 이에 본 고에서는 접근통제 관련 보안정책, 보안모델 및 보안메커니즘에 대하여 살펴보았다. 보안정책 조직에서 정의한 최상위 보안 요구사항의 모음으로 국제표준인 ISO에 서는 신원기반 접근통제 정책(TCSEC의 DAC 정책)과 규칙기반 접근통제 정책(TCSEC의 MAC 정책)으로 구분되며, 보안모델은 보안정책을 검증 가능한 형태로 지원하기 위한 정형화된 보안모델로, BLP, BIBA 등의 이론적으로 잘 정립된 모델들이 존재한다. 보안메커니즘은 보안정책 및 보안모델을 실현하기 위한 구체적인 구현 방법론으로 ACL, CL, SL 등의 널리 사용되는 보안메커니즘이 존재하며 구현시스템의 용도에 적절하게 사용된다.

전 세계적으로 정보보호기술이 점차로 '수동형'에서 점차로 '능동형'으로 진화하고 있다. 이러한 가운데 Secure OS가 능동형 정보보호기술의 핵심으로 주목받고 있으나, 국내의 경우 아직 이에 대한 연구개발 수준이나 상업화 수준은 미약하다. 따라서 향후 IT 보안강국에 진입하기 위해서는 Secure OS 관련 원천기술의 연구개발 및 법·제도의 정비 등을 준비해야 한다.

참 고 문 헌

〔1〕 홍기융, 은유진, 김재명, 이규호, Secure OS 기반의 지능형 다단계 정보보호시스템, 정보처리 학회, 2003
〔2〕 전산망정보보호 - 접근통제기술, 한국정보보호센터, 1996.12.
〔3〕 Morrie Gasser, Building A Secure Computer System, Van Nostrand Reinhold Company Inc, 1988.
〔4〕 Charles P. Pfleeger, Security in Computing, PTR Prentice-Hall, Inc. 1985.

[5] NCSC, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, DEC, 1985.
[6] ISO/IEC 9594-8, Information technology - Open Systems Interconnetion - The Directory : AUthentication framework, 1995.
[7] Abrams, Marshall., et al., "Generalized Framework for Access Control: Towards Prototyping the ORGCON Policy", Proceedings of the 14th National Computing Security Conference, pp.257~266, 1991.
[8] Harrison, M.; Ruzzo, W. L.; and Ullman, "Protection in Operation Systems", Aug 1976.
[9] Bell, D., and La Padulla, L. "Secure Computer Systems", Nov, 1973.
[10] BIBA, K. "Integrity Considerations for Secure Computer Systems", 1977.
[11] Denning, D. "A Lattice Model of Secure Information Flow", May, 1976.
[12] Jones, A. "Protection Mechanism Models : Their Usefulness", 1978
[13] Matt Bishop, "Computer Security: Art and Science".

〈著 者 紹 介〉

홍 기 융 (Ki-Yoong Hong)
종신회원

1985년 2월 : 전남대 전자계산학과 졸업(학사)
1990년 2월 : 중앙대 대학원 전자계산학과 졸업(석사)
1996년 2월 : 아주대 대학원 컴퓨터공학과 졸업(박사)
1985년 9월~1995년 10월 : 한국전자통신연구원 선임연구원
1995년 10월~1996년 4월 : 한국전산원 선임연구원
1996년 4월~2000년 2월 : 한국정보보호센터(응용기술팀장, 평가체계팀장, 인증관리팀장)
1998년 3월~현재 동국대학교 국제정보대학원 겸임교수
2000년 3월~현재 : (주)시큐브/(주)케이사인 대표이사
관심분야 : 시스템보안, 보안운영체제, 전자서명 인증관리(PKI) 등

김 재 명 (Jae-Myung Kim)

1997년 2월 : 충남대 컴퓨터과학과 졸업(학사)
1999년 2월 : 충남대 대학원 컴퓨터과학과 졸업(석사)
2001년 2월 : 경기대 정보보호기술공학과 박사과정 재학 중
1996년 8월~1997년 7월 : 한국전자통신연구원 위촉연구원
1998년 12월~2000년 3월 : 한국정보보호센터 연구원
1999년 2월~2000년 2월 : 공인인증기관 실질심사위원
2000년 3월~현재 : (주)시큐브 상무이사
2003년 1월~현재 : 국방과학기술 검토자문위원
관심분야 : PKI, 시스템보안, 보안운영체제 등

홍 기 완 (Ki-Wan Hong)

1997년 2월 : 전남대 산업공학과 졸업(학사)
2002년 2월 : 동국대 정보보호학과 졸업(석사)
2003년 2월 : 전남대 정보보호학과 박사과정 재학 중
1996년 11월~1997년 7월 : LG-EDS 사원
1997년 7월~2000년 7월 : 한국정보보호센터 연구원
1999년 7월~2000년 7월 : 공인인증기관 실질심사위원
2000년 8월~현재 : (주)시큐브 기술이사
관심분야 : PKI, 취약성분석, 보안운영체제 등