분산시스템에서 Z언어를 이용한 역할기반 접근제어 메커니즘

최 은 복† · 노 봉 남††

요 약

접근제어의 목적은 컴퓨팅 자원 및 통신 정보자원 등을 부당한 사용자로부터 사용되거나, 수정, 노출, 파괴와 같은 비합법적인 행위로부터 보호하는데 있다. 대표적인 보안 정책 중에서 Biba 모델은 정보의 무결성을 보장하지만 상업적인 환경에 적용되기는 다소 미흡하며, 역할기반 접근제어 정책은 상업적인 측면의 보안정책에 적용이 가능하지만 접근되는 객체의 중요도에 따른 보안등급이 고려되지 않았다. 본 논문에서는 Biba 모델의 보안등급을 역할기반접근제어 모델에 적용함으로써 주체가 해당 객체를 부당하게 변경하는 것을 방지함과 동시에 수많은 접근권한을 관리하는데 융통성을 제공한다. 그리고 제안한 접근제어 모델의 제약조건들을 정형 명세 언어인 Z언어를 통해 명확히 표현함으로써 정책입안자나 프로그래머가 접근제어정책을 설계하고 구현하고자 할 때 프로그램 개발에 소요되는 시간을 단축할 수 있다. 또한, 제안한 모델을 망 관리객체의 연산과 등급을 갖는 역할과 제약조건을 사용하여 실제 운영되는 통신망 관리에 적용하여 봄으로써 정보의 무결성이 보장됨을 보였다.

A Role-Based Access Control Mechanism using Z language in Distributed System

Eun-Bok Choi† · Bong-Nam Noh††

ABSTRACT

The objectives of access control are to protect computing and communication resources from illegal use, alteration, disclosure and destruction by unauthorized users. Although Biba security model is well suited for protecting the integrity of information, it is considered too restrictive to be an access control model for commercial environments. And, Role-Based Access Control (RBAC) model, a flexible and policy-neutral security model that is being widely accepted in commercial areas, has a possibility for compromising integrity of information. In this paper, we present the interworking Biba and RBAC model to protect the user from modifying the information in an unauthorized way while providing the flexible permission management facility. And internetworking access control model with constraints help both the policy designer and programmers to understand and implement programs. It may also save the cost and time for network managed systems. Also, the proposed model is demonstrated on real network management systems. From this demonstration, the preservation of information integrity are confirmed.

키워드 : 역할기반접근제어(Role-Base Access Control), Z 명세 언어(Z Specification Language), 통신망 관리(Network Management)

1. 서 론

상호 독립적으로 운영되는 통신망들이 상호연동 됨에 따라 전체적인 통신망의 규모가 점점 커지고 복잡해지고 있으며 다양한 사용자들로 인해 관리객체를 저장관리하는 관리정보베이스에 대한 보안이 필수적인 요소가 되었다. 또한 통신망을 이용하는 사용자들의 요구사항이 다양해져 이를 효율적으로 관리해 줄 수 있는 망 관리 시스템이 통신망 운용에 필요하다. 그러므로 정보 통신망의 관리 정보를 이용하는 사용자의 환경이 동적으로 변화하는 현대의 네트워크 환경에서는 접근제어 정책을 어느 하나의 정책에 근거한 일괄적 관리가 쉽지않다. 따라서 실질적인 접근제어 시스템에 적용이 가능하도록 관련된 몇 가지 정책들간의 연관성을 연구할 필요가 있다.

ITU-T X.741 표준안에서는 접근제어에 관한 전반적인 관리객체와 그들의 속성들에 대해 표현하고 있다. 여기에는 관리객체 클래스의 상속계층구조와 관리객체 상호관계를 표현하고 있으며 임의적 접근제어 모델에 해당하는 접근제어 리스트와 능력리스트에 대한 관리객체를 표현하고있고 강제적 접근제어 모델에 해당하는 Biba, BLP 모델을 통해 보안등급에 관한 관리객체와 속성들을 표현하고 있다[18].

ITU-T X.812에서는 접근제어 모델의 입출력 정보와 접

† 정 회 원 : 순천제일대학 인터넷정보학부 교수
†† 종신회원 : 전남대학교 컴퓨터정보학부 교수
논문접수 : 2001년 2월 20일, 심사완료 : 2001년 4월 30일

근제어 리스트, 능력리스트, 그리고 보안등급과 문맥기반 스키마에 따른 메커니즘이 정의되어 있으며 이와 관련된 관리객체 클래스와 속성들이 표현되어 있다[19].

2. 관련연구

2.1 Biba 모델

BLP모델은 권한을 갖지 않는 사용자에게 정보가 흘러가는 것을 예방하는 비밀성에 기반을 둔 모델이다. 이 모델은 정보의 비밀성은 보장하지만 등급이 낮은 주체가 등급이 높은 객체 정보를 쓸 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 주체와 객체의 보안등급에 의해 정책이 수행되는 Biba 모델이 제안되었다.

만약, 보안등급과 범주의 집합이 각각 $C_1 \geq C_2$과 $S_1 \supseteq S_2$의 관계를 가지면 보안등급 $L_1 = (C_1, S_1)$는 $L_2 = (C_2, S_2)$를 지배(dominate)한다고 하고, 보안등급이 $L_1 \geq L_2$나 $L_2 \geq L_1$의 관계가 모두 만족되지 않으면 이 두 등급은 비교불가능(incomparable)하다고 한다.

Biba모델은 정보의 무결성을 보장하기 위해서 해당 보안 환경에 맞는 여러가지 보안 정책중에서 하나를 사용한다[2].

다음 정책에 사용되는 표기법에 대한 설명은 다음과 같다.

- L(s) : 주체의 인가등급
- L(o) : 객체의 보안등급
- 접근 모드 : Read, Write

2.1.1 주체의 최소상한 정책

- 주체의 인가등급이 객체의 보안등급을 지배한다면 주체는 객체에 쓰기 연산을 수행할 수 있다.
  ⇨ $L(s) \geq L(o) \Rightarrow$ Write
- 주체는 어떤 객체에 대해서도 읽기 연산을 수행할 수 있다.
  ⇨ whatever object ⇒ Read
  <단, L(s) = LUB[L(s), L(o)], LUB(Least Upper Bound : 최소상한)>

2.1.2 객체의 최대하한 정책

- 주체는 어떤 보안등급을 가진 객체이더라도 쓰기 연산을 수행할 수 있다.
  ⇨ whatever object ⇒ Write
  <단, L(o) = GLB[L(s), L(o)], GLB(Greatest Lower Bound : 최대하한)>

2.1.3 감사추적 정책

- 주체는 어떤 보안등급을 갖는 객체라도 쓰기 연산을 수행할 수 있다.
  ⇨ whatever object ⇒ Write

단, 주체가 자신보다 높은 객체나 비교 불가능한 등급의 객체에 대해 쓰기를 수행할 때에는 감사기록 화일에 기록된다.

2.1.4 링 정책

이 정책은 주체와 객체의 보안등급이 고정되어 있으며

- 주체의 인가등급이 객체의 보안등급을 지배한다면 주체는 객체에 쓰기 연산을 수행할 수 있다.
  ⇨ $L(s) \geq L(o) \Rightarrow$ Write
- 주체는 어떤 객체에 대해서도 읽기 연산을 수행한다.
  ⇨ whatever object ⇒ Read

2.1.5 엄격한 무결성 정책

- Simple integrity : 주체의 인가등급이 객체의 보안등급에 지배된다면 주체는 객체에 읽기 연산을 수행할 수 있다.
  ⇨ $L(s) \leq L(o) \Rightarrow$ Read
- Integrity *-property : 주체의 인가등급이 객체의 보안등급을 지배한다면 주체는 객체에 쓰기 연산을 수행할 수 있다.
  ⇨ $L(s) \geq L(o) \Rightarrow$ Write

2.2 역할기반 접근제어 모델

역할기반 접근제어 모델(Role-Based Access Control : RBAC)은 데이터 또는 객체를 몇 개의 범주로 나누었으며, 여러 명의 사용자는 역할이라고 하는 클래스들로 그룹화되어진다. 역할은 어떤 조직체의 사용자들의 임무를 여러 개의 영역으로 분할해 놓은 것으로서 역할 이름과 범주에 접근할 수 있는 권한으로 구성되어 있다. 역할은 조직체에서 사용자의 활동 위치에 따라 결정된다. 역할에 사용자 할당과 역할의 객체에 대한 권한부여의 두 단계로 나뉘어 질 수 있으므로 권한부여 관리에 효율적이다. 즉, 사용자의 역할 변경에 따른 권한 변경 작업의 단순화를 가져올 수 있다. 또한 하나의 트랜잭션을 여러 역할이 분할하여 수행되도록 하는 임무분리 정책을 통해 정보의 무결성을 보장받을 수 있다[9].

2.2.1 기본 모델 - $RBAC_0$

$RBAC_0$는 4가지 개체인 사용자(U), 역할(R), 권한(P), 그리고 세션(S)으로 구성된다. 권한은 한 개 이상의 객체에 적용되는 접근 모드를 의미하며 이는 권한을 철회하는 음성적 측면보다는 부여하는 양성적 측면을 가진다. 권한의 연산은 read, write, execute 뿐만 아니라 상업적인 측면에서 추상적인 데이터를 처리할 수 있는 연산인 select, update, delete, debit, credit 등이 있다.

2.2.2 역할 계층 모델 - $RBAC_1$

계층은 권한과 책임을 수반하는 구조적 역할이라 할 수 있으며, 역할에 대한 감사 추적시 계층구조를 이용한다. 상위역할은 자신의 권한뿐만 아니라 하위역할의 모든 권한을 포함하게 된다. 포함의 범위를 제한할 필요가 있는데, 하위역할이 상위 역할에 포함될 때 비밀을 요하는 경우에는 사

설 비밀 역할(private role)을 생성한다.

2.2.3 제약조건 모델 - $RBAC_2$

역할기반 접근제어 정책은 한명 이상의 사용자들이 한 개 이상의 역할을 수행하는 구조를 갖는데 사용자들이나 역할들의 관계에는 정보의 무결성을 침해할 수 있는 방법들이 존재하게 된다. 그러므로 올바른 정책을 수행하기 위해서는 정책에 대한 제약조건(constraint)을 기술할 필요가 있다.

2.2.4 통합 모델 - $RBAC_3$

$RBAC_3$ 모델은 역할 계층성 모델인 $RBAC_1$과 제약조건 모델인 $RBAC_2$를 결합한 모델이다. 역할 계층 구조에 제약조건이 적용되며 역할 계층은 부분 순서(partial order)관계를 갖는다. 단일 시스템에 의한 역할기반 접근제어정책이 아닌 대규모 시스템에서는 역할의 개수가 매우 많아 이를 관리하는 일이 중요하다. 역할기반 접근제어정책의 주요한 장점은 이러한 권한 관리를 효율적이고 단순화시킬 수 있다는 점이다.

2.3 Z 명세 언어

정형적 명세 언어는 시스템의 특성을 자세하게 정의하고 명확하게 기술하는데 사용되는 언어로써 명세에서 기술하는 것은 시스템이 어떻게 수행되는가(How)가 아니고 시스템이 무엇을 하는가(What)을 나타내고 있다. 이러한 명세 언어는 시스템의 오퍼레이션 뿐만 아니라 시스템의 다양한 상태를 나타내는 스키마 구조를 포함한다. 따라서 이러한 정형적 명세 언어를 이용하여 시스템을 정의하고 기술하면 비정형적 언어로 작성한 것에 비해서 많은 이점들을 얻을 수 있는데 이러한 이유들 때문에 정형적 명세 언어인 Z, VDM 등이 개발되었다. Z 명세 언어는 집합론에 기초한 스키마 구조를 이용하여 시스템을 명세화한다. Z 명세언어는 일반적으로 상태스키마(State Schema)와 오퍼레이션 스키마(Operation Schema)를 포함하고 있으며 이들 스키마는 다른 스키마에 의해 참조될 수 있도록 이름이 주어진다[15].

2.4 적용 필요성

Biba 모델은 시스템 관리자에 의해 보안등급이 결정되는 강제적 접근제어정책으로 정보의 무결성을 강조하기 위한 모델이다. 하지만 이 모델은 한 주체가 어느 한 객체를 접근하지 못하면 자신의 인가등급을 변경하지 않는 한 그 객체와 동일한 보안등급을 갖는 모든 객체에 접근이 허락되지 않는다. 또한 공통적인 기능을 수행하는 다중 사용자들이 객체를 접근할 수 있는 보안 요구사항을 표현하는데는 부적절하여 상업적인 환경에 적용하기에는 다소 미흡하다.

역할기반 접근제어 모델은 역할과 권한, 사용자와 역할, 그리고 역할과 역할의 관계와 같은 정책 구성요소를 통해 접근권한을 수행한다. 그러므로 상업적인 환경에서는 주체가 자율적으로 권한을 부여하고 철회할 수 있는 접근제어 행렬이나 리스트, 주체와 객체에 등급을 부여하여 제어하는 다단계 정책보다는 조직에 관련된 작업을 기반으로 하는 역할에 주체를 배정하는 역할기반 접근제어정책 사용이 적절하다. 하지만 실제적으로 역할을 통해 접근되는 객체에 대한 중요도에 따른 등급이 기술되어 있지 않아 해당 역할을 수행할 수 있는 모든 사용자들이 모든 객체를 사용하거나, 변경할 수 있어 정보의 비밀성과 무결성을 해칠 우려가 있다.

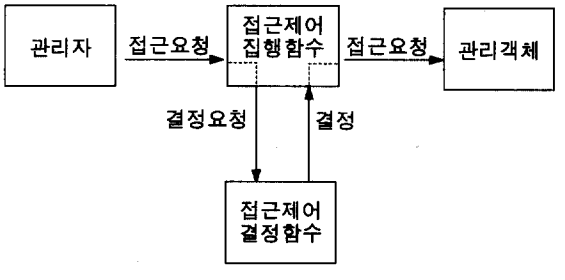
본 논문에서는 기존에 많은 연구가 진행되어온 대표적인 접근제어 정책중에서 Biba 모델과 역할기반 접근제어모델을 상호 연동[20]한 모델을 확장한 등급을 갖는 역할기반 접근제어 모델을 제시하였다. 실제 적용될 수 있는 관리자원과 보안등급을 확장된 모델에 부여하므로서 주체가 해당 객체를 부당하게 변경하는 것을 방지함과 동시에 수많은 접근권한과 역할을 관리하는데 융통성을 제공한다. 그리고 제안한 접근제어 모델의 제약조건들을 정형 명세 언어인 Z 언어를 통해 명확히 정의함으로써 정책입안자나 프로그래머가 접근제어정책을 설계하고 구현하고자 할 때 프로그램 개발에 소요되는 시간과 비용을 단축할 수 있다. 또한, 접근제어 모델을 망 관리객체의 연산을 사용하여 실제 운영되는 통신망 관리에 적용하여 봄으로써 역할과 제약조건에 의해 정보의 무결성이 보장됨을 보였다.

3. 등급을 갖는 역할기반 접근제어모델

3.1 관리정보베이스의 접근제어

망 자원에 접근을 원하는 사용자가 자신의 신원을 제시하고 인증 시스템으로부터 신원 인증을 받은 후, 확인된 사용자에 대한 망 자원을 접근하는 권한을 확인하는 과정을 접근 제어라고 한다. 접근제어는 컴퓨터 시스템의 합법적인 사용자가 수행하는 연산이나 행위를 제한하는 것이다. 이러한 접근제어를 효과적으로 수행하기 위해서는 접근권한의 불법 취득을 방지하고, 접근 권한에 관한 불법 변조가 일어나지 않도록 하여야 한다.

기본적인 접근제어의 수행을 위한 기능모델이 (그림 1)에서 나타내고 있다. 접근제어에 관련된 기본적인 개체와 기능은 접근을 요청하는 프로세스인 관리자, 접근요청을 접근제어결정함수(ADF)에 전송하고 접근에 대한 응답을 처리하는 접근제어집행함수(AEF), 접근제어집행함수로부터 전

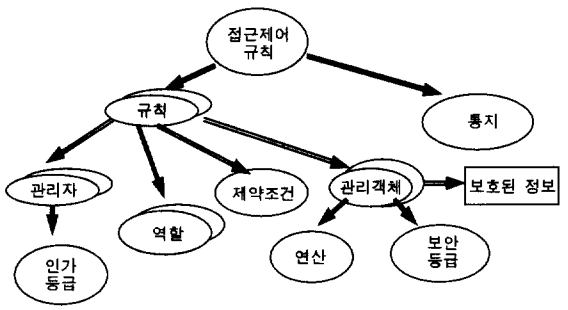


(그림 1) 접근제어 기능 모델

송받은 접근요청에 대한 가부를 결정하는 접근제어결정함수, 그리고 실제 관리객체로 나뉠 수 있다[17].

ITU-T X.741 권고안에는 정의된 접근제어를 위한 관리객체 클래스 구조를 자율적 접근제어 정책과 강제적 접근제어 정책으로 나누어 정의하고 있다. 본 논문에서는 강제적 접근제어정책에 역할기반 접근제어정책을 적용한 접근제어정책을 생성하기 위해 권고안에 정의된 강제적 접근제어 정책의 관리객체 상호관계 구조에 정보의 변경이나 삭제, 첨가 등 연산의 소유권을 갖는 역할을 부여함으로써 수많은 접근권한을 관리하는데 융통성과 효율성을 갖는다. 또한 역할을 수행하는 사용자인 주체의 인가등급과 역할에 부여된 객체의 보안등급을 제약조건에 따라 접근여부를 관리함으로써 정보의 무결성을 보장받을 수 있다.

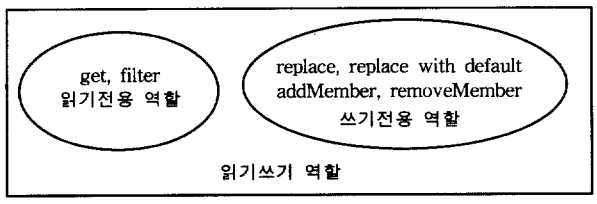
(그림 2)는 강제적 접근제어에 역할기반 접근제어를 적용한 등급기반 RBAC 모델의 관리객체 상호관계를 나타내고 있다.



(그림 2) 등급기반 RBAC 모델의 관리객체 상호관계

3.2 역할 영역

관리정보 모델에는 관리연산을 크게 전반적인 관리객체에 적용되는 연산과 속성값에 적용되는 연산으로 구분하고 있다. 전반적인 관리객체에 적용되는 연산에는 관리객체의 인스턴스를 생성하고 삭제하는 create, delete 연산과 개별적인 관리객체의 요구조건을 정의하는 action 연산이 있다. 그리고 속성값에 적용되는 연산에는 속성값을 읽는 get 연산, 속성값을 쓰는 replace 연산, 그리고 관리객체 정의시 명기되어있는 값으로 재정의하여 쓰는 replace with default 연산 등이 있다. 또한 특별한 속성 타입을 정의하기 위한 것으로 동일한 데이터 타입의 멤버들의 비순서 집합을 추가, 삭제하는 addMember와 removeMember 등이 있다[17]. 본 논문에서는 실질적으로 관리정보베이스의 속성값을 수정하고 읽는 관리연산들에 대해서 (그림 3)과 같이 읽기전용역할, 쓰기전용역할 그리고 이들 두 연산을 포함하는 읽기쓰기 역할로 세분하였다.



(그림 3) 역할 영역

3.3 제약조건

인가등급을 갖는 관리자는 역할영역에 속해있는 배정된 역할에 따라 관리객체의 관리연산을 수행할 수 있으며, 관리객체에도 보안등급이 부여되어 정보의 무결성을 보장토록 한다. 이러한 관리연산을 수행하기 위한 역할 배정규칙과 이에 따르는 제약조건을 표현하기 위한 표기법은 다음과 같다.

- 표기법 정의
  - S : 주체
  - R : 역할
  - s : 주체의 집합 $S \in s$
  - r : 역할의 집합, $R \in r$
  - R_r : 읽기전용 역할
  - R_w : 쓰기전용 역할
  - R_{rw} : 읽기쓰기 역할
  - $\lambda(S)$: 주체의 인가등급
  - RoleAssign[S, R] : 주체 S의 역할 R에 대한 배정함수
  - Dominate(a,b) : $a \geq b$ or $a \supseteq b$ (단, $a,b \in$ 등급)
  - Equal(a,b) : Dominate(a,b) AND Dominate(b,a)
  - r-scope(R) : 읽기 접근모드를 갖는 모든 객체의 권한 집합
  - w-scope(R) : 쓰기 접근모드를 갖는 모든 객체의 권한 집합
  - r-level(R) : r-scope(R)중에서 최소의 보안등급
  - w-level(R) : w-scope(R)중에서 최대의 보안등급
- 기본타입의 정의

[SUBJECT, OBJECT, ROLE, SEC_LEVEL, ACCESS_MODE]

- SUBJECT : 주체의 집합
- OBJECT : 객체의 집합
- ROLE : 역할의 집합
- SEC_LEVEL == {TS, S, C, U}
  (TS : Top Secret, S : Secret, C : Confidential, U : Unclassified)
- ACCESS_MODE == {read, write}

READ_PRIV_SET

object : P OBJECT
access_mode : ACCESS_MODE

access_mode = read

〈읽기 권한 집합〉

WRITE_PRIV_SET

object : P OBJECT
access_mode : ACCESS_MODE

access_mode = write

〈쓰기 권한 집합〉

ROLE

r-level : SEC_LEVEL
r-scope : READ_PRIV_SET
w-level : SEC_LEVEL
w-scope : WRITE_PRIV_SET

〈역 할〉

LEVEL_TO_INT

level_to_level : SEC_LEVEL → N

s : SEC_LEVEL, 1 : N •
(s = U ⇒ 1 = 1) ∪
(s = C ⇒ 1 = 2) ∪
(s = S ⇒ 1 = 3) ∪
(s = TS ⇒ 1 = 4)

〈등급의 정수화〉

INT_TO_LEVEL

int_to_level : N → SEC_LEVEL

s : SEC_LEVEL, 1 : N •
(1 = 1 ⇒ s = U) ∪
(1 = 2 ⇒ s = C) ∪
(1 = 3 ⇒ s = S) ∪
(1 = 4 ⇒ s = TS)

〈정수의 등급화〉

INIT_R_LEVEL

r-level : SEC_LEVEL
r-scope : P READ_PRIV_SET
r-temp : N
level_to_int : SEC_LEVEL → N
int_to_level : N → SEC_LEVEL

∀obj ∈ r-scope.object
r-temp = min[level_to_int(obj)]
r-level = int_to_level(r-temp)

〈읽기 등급 초기화〉

INIT_W_LEVEL

w-level : SEC_LEVEL
w-scope : P WRITE_PRIV_SET
w-temp : N
level_to int : SEC_LEVEL → N
int to level : N → SEC LEVEL

∀obj ∈ w-scope.object
w-temp = max[level_to_int(obj)]
w-level = int_to_level(w-temp)

〈쓰기 등급 초기화〉

● 읽기 전용 역할

읽기전용 역할의 모든 관리객체의 등급이 모두 같은 보안등급을 갖는 경우, 이 역할은 Biba 모델의 단순무결성 성질 정책이 적용된다. 만약, 읽기전용 역할의 모든 관리객체들이 서로 다른 보안등급을 가질 경우, 주체의 인가등급이 해당 역할의 최소 보안등급에 해당하는 r-level(R)에 지배되어야 한다. 만약 그렇지 않으면 해당 주체는 자신보다 등급이 낮은 객체를 읽게 되어 정보의 무결성을 보장받지 못하게 된다. 왜냐면, 자신보다 낮은 객체를 읽어 자신의 등급에 쓸 경우 낮은 정보가 상위 등급으로 흐를 수 있기 때문이다.

다음 (그림 4)와 같은 읽기 전용 역할(R_r)을 고려하여 보자. 이 역할에는 U, C, S, TS 등급의 객체를 수행할 수 있는 관리연산들의 집합으로 구성되어있다. 그러므로 이 역할의 r-level은 제일 낮은 등급인 U 등급이므로 이 역할을 배정 받을 수 있는 주체는 U 등급만이 가능하다. 만약 C 등급의 주체가 이 역할에 배정 될 경우 자신보다 낮은 U 등급의 관리객체를 읽어서(Ou, GET) 자신의 등급이상인 C 급과 S 등급, TS 등급에 쓸 우려가 있다. 이것은 하위등급의 정보가 상위 등급으로 상향될 우려가 있으며 불필요한 하위 등급의 정보가 상위등급에 쓰여져 상위 관리자의 관리정책에 어려움을 줄 우려가 있다.

이의 내용에 대한 제약조건과 Z언어의 표현식은 다음과 같다.

[제약조건 1] 주체의 집합 s에 해당 주체 S가 속하고, 역할의 집합 r에 읽기 전용 역할 R_r이 속할 때, 주체 S가 읽기 전용 역할(R_r)에 배정되기 위해서는 주체의 인가등급이 읽기 전용 역할(R_r)의 최소 보안등급에 지배되어야 한다.

⇨ $\forall S \in s,\ \forall R_r \in r$

$RoleAssign(S, R_r) \Rightarrow \lambda(S) \leq r\text{-}level(R_r)$

READ_ONLY_ROLE_ASSIGN

s : SEC_LEVEL
level_to_int : SEC_LEVEL → N
r-level : SEC_LEVEL

level_to_int(s) ≤ level_to_int(r-level)

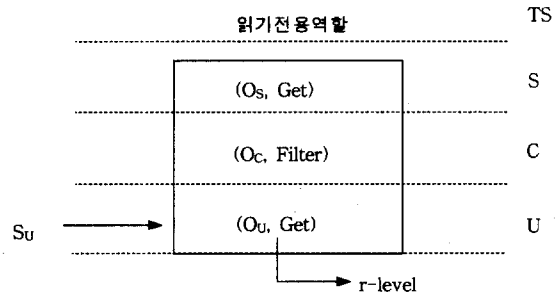
〈읽기전용 역할 배정배수〉

● 쓰기 전용 역할

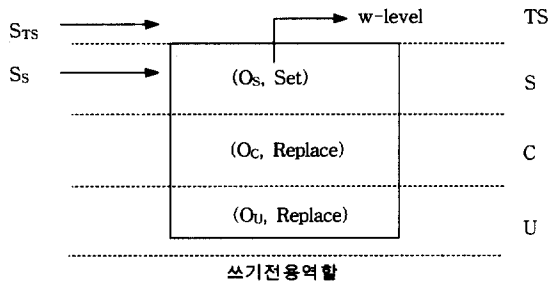
쓰기전용 역할의 관리객체 등급이 모두 같은 보안등급을 갖는 경우, 이 역할은 Biba 모델의 무결성 스타 성질 정책이 적용된다. 만약, 쓰기전용 역할의 모든 객체들이 서로 다른 보안등급을 가질 경우, 주체의 인가등급이 해당 역할의 최대 보안등급에 해당하는 w-level(R)을 지배하여야 한다. 만약 그렇지 않으면 주체가 자신보다 높은 등급이 객체를 쓰게 되어 정보의 무결성을 보장받지 못하게 된다.

다음 (그림 5)와 같이 쓰기 전용 역할(R_w)을 고려하여 보

자. 이 역할에는 U, C, S 등급의 객체를 수행할 수 있는 관리연산들의 집합으로 구성되어있다. 그러므로 이 역할의 w-level은 제일 높은 등급인 S 등급이므로 이 역할을 배정받을 수 있는 주체는 S 등급과 상위등급인 TS 등급만이 가능하다. 만약 C 등급의 주체가 이 역할에 배정 될 경우 자신보다 높은 S등급의 관리객체를 수행하거나 쓸수 있어(Os, Set) 정보의 무결성을 침해할 수 있다.



(그림 4) 읽기 전용 역할



(그림 5) 쓰기 전용 역할

이의 내용에 대한 제약조건과 Z언어 표현식은 다음과 같다.

[제약조건 2] 주체의 집합 s에 해당 주체 S가 속하고, 역할의 집합 r에 쓰기 전용 역할 R_w이 속할 때, 주체 S가 쓰기 전용 역할(R_w)에 배정되기 위해서는 주체의 인가등급이 쓰기 전용 역할(R_w)의 최대 보안등급을 지배하여야 한다.

$\Rightarrow \forall S \in s, \forall R_w \in r$

RoleAssign(S, R_w) $\Rightarrow \lambda(S) \geq$ w-level(R_w)

WRITE_ONLY_ROLE_ASSIGN

s : SEC_LEVEL
level_to_int : SEC_LEVEL → N
w-level : SEC_LEVEL

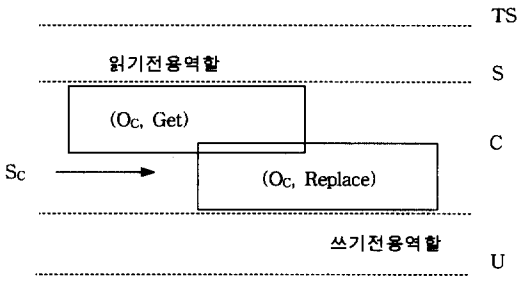
level_to_int(s) ≥ level_to_int(w-level)

〈쓰기전용 역할 배정함수〉

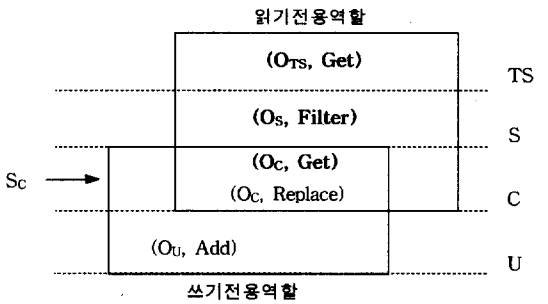
● 읽기쓰기 역할

다음으로 읽기쓰기 역할(R_{rw})을 고려하자. 이 경우에는 읽기전용 역할의 r-level(R_r)이 쓰기전용역할의 w-level(R_w)을 지배하고 주체의 등급이 r-level(R_r)보다 적거나 같고 w-level(R_w)보다는 크거나 같은 경우에만 읽기쓰기 역할에 배정이 가능하다. (그림 6)은 읽기전용 역할과 쓰기전용 역할이 하나의 등급에 존재하는 경우이다. 이 경우에는 읽기전용 역할과 쓰기전용 역할의 등급에 해당하는 주체에게만 역할이 배정된다. 만약 해당 등급에 비해 높은 등급을 갖는 주체에 역할이 배정되면 읽기 전용 역할에 해당하는 낮은 객체를 읽게되고 해당 등급에 비해 낮은 등급을 갖는 주체에 역할이 배정되면 쓰기전용 역할에 해당하는 높은 객체에 쓰게 되어 Biba 모델의 단순 무결성 성질과 무결성 스타 성질 정책에 위배된다.

(그림 7)은 읽기전용 역할과 쓰기전용 역할이 다양한 등급을 갖고 있으면서 두 역할의 공통부분이 존재하는 경우의 예이다. 이 경우에는 두 역할의 공통부분에 해당하는 등급과 일치하는 주체에게만 역할이 배정된다.

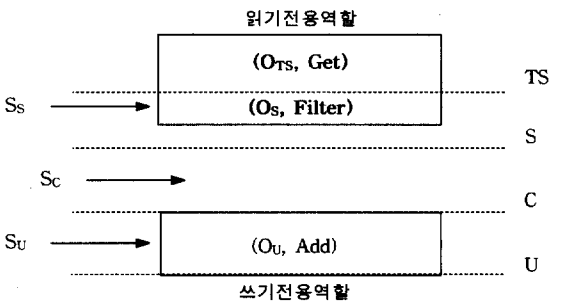


(그림 6) 읽기 쓰기 역할(동일 등급에 존재하는 경우)



(그림 7) 읽기 쓰기 역할(공통 부분이 존재하는 경우)

(그림 8)과 같이 읽기전용 역할과 쓰기전용 역할이 서로



(그림 8) 읽기 쓰기 역할(공통 부분이 없는 경우)

공통부분이 없을 경우에는 읽기전용 역할의 제일 낮은 등급과 쓰기전용 역할의 제일 높은 등급 사이에 해당하는 주체에게만 역할배정이 허가된다. 이 등급 사이에 해당하는 주체의 경우에는 Biba 모델의 정책에 따라 높은 객체를 읽을 수 있음은 물론 낮은 객체에 쓸 수도 있기 때문이다.

이와 같은 내용을 기반으로 제약조건 3을 정의하였다.

[제약조건 3] 주체의 집합 s에 해당 주체 S가 속하고, 역할의 집합 r에 읽기쓰기 역할 R_{rw}이 속할 때, 주체 S가 읽기쓰기 역할(R_{rw})에 배정되기 위해서는 읽기 전용 역할(R_r)의 최소 보안등급이 쓰기 전용 역할(R_w)의 최대보안등급을 지배하여야 하고, 주체의 인가등급이 읽기 전용 역할(R_r)의 최소 보안등급은 지배하고 쓰기 전용 역할(R_w)의 최대 보안등급에는 지배되어야 한다.

$\Rightarrow \forall S \in s, \forall R_{rw} \in r$

$RoleAssign(S, R_{rw}) \Rightarrow r\text{-}level(R_r) \geq w\text{-}level(R_w)$ AND $\lambda(S) \leq r\text{-}level(R_r)$ AND $\lambda(S) \geq w\text{-}level(R_w)$

READ_WRITE_ROLE_ASSIGN

s : SEC_LEVEL

level_to_int : SEC_LEVEL → N

r-level, w-level : SEC_LEVEL

---

level_to_int(r-level) ≥ level_to_int(w-level)

∩

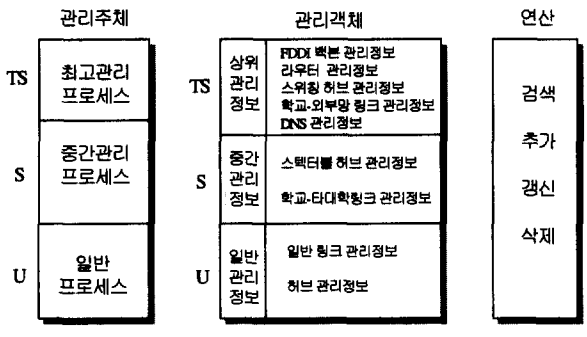
level_to_int(r-level) ≥ level_to_int(s)

≥ level_to_int(w-level)

〈읽기 쓰기 역할 배정함수〉

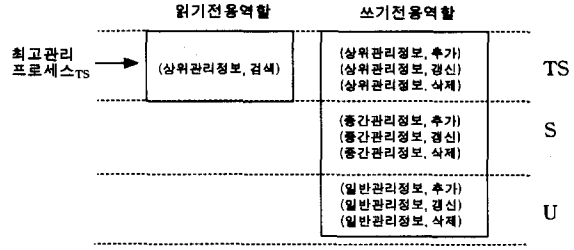
3.4 망관리 모델의 적용

현재까지 통신망을 관리하는 관리프로세스는 단일 관리자에 의한 관리 업무를 수행함으로써 업무의 효율성에 문제점을 갖고 있었다. 그러므로 관리업무 수행의 책임 권한과 관리정보의 중요도에 따라 관리주체와 관리객체에 보안등급을 부여하였다. (그림 9)에서는 관리주체의 책임권한에 따라 최고관리프로세스, 중간관리 프로세스 그리고 일반 프로세스로 나누고 관리프로세스가 관리하는 관리정보의 중요도에 따라 상위 관리정보와 중간관리정보, 일반관리정보로 구분한다. 또한 수행하는 연산에는 검색, 추가, 갱신, 삭제 등이 있다.



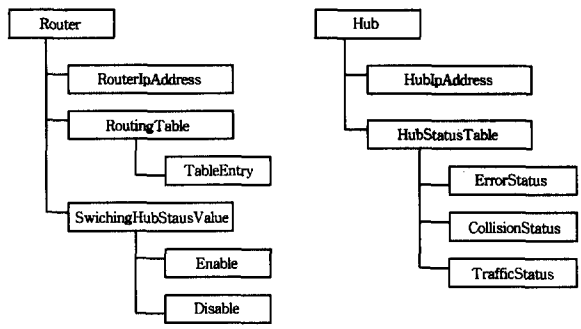
(그림 9) 보안등급에 따른 관리주체와 객체

최고관리프로세스는 (그림 10)과 같이 상위 관리정보만 검색할 수 있는 읽기전용 역할과, 모든 관리정보에 대해서 추가·갱신·삭제를 수행할 수 있는 쓰기전용 역할이 배정된다.



(그림 10) 최고관리 프로세스

· 만약, 최고관리프로세스에게 자신보다 낮은 등급의 하위 관리정보의 검색 연산을 부여할 때 발생할 수 있는 문제점을 설명하기 위해 먼저 (그림 11)과 같이 상위 관리정보에 해당하는 Router MIB 트리와 일반 관리정보에 해당하는 Hub MIB 트리를 제시하였다.



<Router MIB Tree> <Hub MIB Tree>

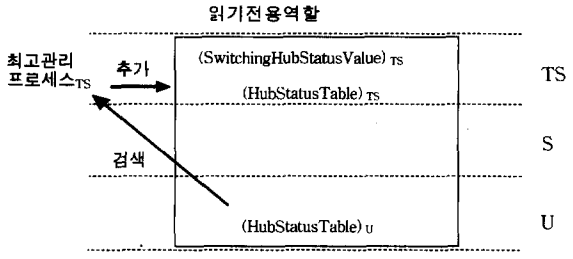
(그림 11) MIB 트리 구조

(그림 12)와 같이 최고관리프로세스가 U등급의 일반 허브 상태정보인 에러정보, 트래픽정보, 충돌정보를 검색하여 자신의 등급인 TS에 추가하였을 때 발생할 수 있는 문제점은 크게 두가지로 요약될 수 있다.

첫째, 관리 프로세스는 자신보다 보안등급이 높은 관리객체에 대해서는 검색과 같은 읽기전용 역할의 수행은 가능하나, 추가나 갱신과 같은 쓰기전용 역할의 수행을 못하게 함으로써 정보가 불법적으로 변경되는 것을 방지한다. 만약, 최고관리프로세스가 U등급의 일반 허브 상태정보를 자신의 등급인 TS에 추가하였을 경우, 일반 허브의 상태정보를 실질적으로 관리하는 U등급의 일반 프로세스는 TS등급에 존재하는 일반 허브 상태정보를 수정할 수 없게 된다. 그렇게되면 최고관리프로세스는 관리되어지지 않는 TS등

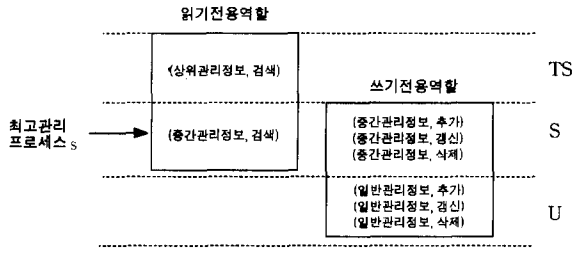
급의 일반 허브 상태정보로 인해 그릇된 정책을 집행할 수 있는 잘못을 범할 수 있다.

둘째, U등급을 갖고 있는 일반 허브 상태정보는 인가등급이 낮은 일반사용자에 의해 관리되어지기 때문에 언제든지 불법적인 사용자에 의해 변질되어질 수 있는 비신뢰적인 관리정보이다. 따라서 일반 허브의 상태정보인 트래픽정보나 충돌정보가 불법 사용자에 의해 통신망의 상태를 위협하는 과부하 상태값으로 변경되어질 수 있다. 이러한 신뢰성이 낮은 정보가 최고관리프로세스에 의해 신뢰성이 매우 높은 등급으로 이동되어 최고관리프로세스가 일반 허브를 연결하는 스위칭 허브의 상태값을 'Disable'로 바꾸어 버린다면 정상적으로 운영되는 통신망을 파괴하는 경우가 발생한다.



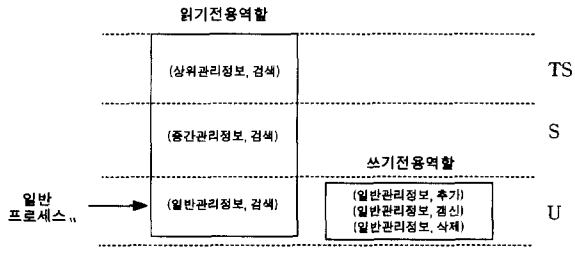
(그림 12) 최고관리 프로세스의 하위 관리정보 검색

(그림 13)과 같이 중간관리 프로세스는 자신의 등급보다 같거나 큰 중간 관리정보와 상위 관리정보를 검색할 수 있는 읽기전용 역할과 자신의 등급보다 같거나 적은 중간 관리정보와 일반 관리정보를 추가·갱신·삭제할 수 있는 쓰기전용 역할을 수행 할 수 있다



(그림 13) 중간관리 프로세스

마지막으로 (그림 14)와 같이 일반 프로세스는 자신보다 크거나 같은 관리정보를 검색할 수 있는 읽기전용 역할과 자신의 등급에 해당하는 일반 관리정보에 대해 추가·갱신·삭제 연산이 가능한 쓰기전용 역할을 수행할 수 있다.



(그림 14) 일반 프로세스

4. 결 론

분산시스템 환경에서 컴퓨터 보안은 시스템에 존재하는 정보를 부적절한 사용자로부터 보호하는데 그 목적이 있다. 상호 독립적으로 운영되는 통신망들이 상호연동 됨에 따라 전체적인 통신망의 규모가 점점 커지고 복잡해지고 있으며 다양한 사용자들로 인해 관리객체를 저장관리하는 관리정보베이스에 대한 보안이 필수적인 요소가 되었다. 또한 통신망을 이용하는 사용자들의 요구사항이 다양해져 이를 효율적으로 관리해 줄 수 있는 접근제어정책이 통신망 운용에 필요하다.

강제적 접근제어 정책은 모든 주체들이 서로 다른 인가등급을 할당받으며, 모든 객체에게도 다양한 보안등급을 부여하여 주체의 인가등급과 객체의 보안등급을 지배관계에 따라 접근여부를 결정한다. 이 두 모델들은 한 주체가 어느 한 객체를 접근하지 못하면 자신의 인가등급을 변경하지 않는 한 그 객체와 동일한 보안등급을 갖는 모든 객체에 접근이 허락되지 않는다. 또한 공통적인 기능을 수행하는 다중 사용자들이 객체를 접근할 수 있는 보안 요구사항을 표현하는데는 부적절하다.

분산시스템 환경에서 역할기반 접근제어정책은 조직체와 관련된 작업기능의 역할을 수행하는 주체와 객체들이 수없이 존재하게 되는데, 상업적인 환경에서는 정보를 사용하는 주체나 역할보다는 접근되는 객체가 실질적으로 매우 중요하게 취급되어야 한다. 하지만 이 정책은 역할에 의해 접근되는 객체에 대한 중요도에 따른 등급이 기술되어 있지 않아 해당 역할을 수행할 수 있는 모든 사용자들이 모든 객체를 사용하거나, 변경할 수 있어 정보의 비밀성과 무결성을 해칠 우려가 있다.

본 논문에서는 기존에 많은 연구가 진행되어온 대표적인 접근제어 정책중에서 Biba 모델과 역할기반 접근제어모델을 상호 연동한 모델을 확장한 등급을 갖는 역할기반 접근제어 모델을 제시하였다. 실제 적용될 수 있는 관리자원과 보안등급을 확장된 모델에 부여하므로서 주체가 해당 객체를 부당하게 변경하는 것을 방지함과 동시에 수많은 접근권한과 역할을 관리하는데 융통성을 제공한다. 그리고 제안한 접근제어 모델의 제약조건들을 정형 명세 언어인 Z언어를 통해 명확히 정의함으로써 정책입안자나 프로그래머가 접근제어정책을 설계하고 구현하고자 할 때 프로그램 개발에 소요되는 시간과 비용을 단축할 수 있다. 또한, 접근제어 모델을 망 관리객체의 연산을 사용하여 실제 운영되는 통신망 관리에 적용하여 봄으로써 역할과 제약조건에 의해 정보의 무결성이 보장됨을 보였다.

참 고 문 헌

[1] Charles P. Pfleeger, Security in Computing, Prentice Hall.

[2] Silvana Castano, DATABASE SECURITY, ADDISON-WESLEY.

[3] Warwick Ford, Computer Communications Security, Prentice Hall.

[4] Matunda Nyanchama, Sylvia Osborn, "Modeling Mandatory Access Control in Role-Based Security Systems," Database Security IX status and prospects, pp.129-144, 8, 1995.

[5] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn, "Role-Based Access Control (RBAC) : Features and Motivations," COMPUTER SECURITY APPLICATIONS Conference, IEEE, pp.241-248, 12, 1995.

[6] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models," COMPUTER SOCIETY, IEEE, FEB. pp.38-47, 1996.

[7] Sylvia Osborn, "Mandatory Access Control and Role-Based Access Control Revisited," Second ACM Workshop on RBAC, pp.31-40, 11. 1997.

[8] Ravi S. Sandhu and Pierangela Samarati, "Access Control : Principles and Practice," IEEE Communications Magazine, pp.40-48, 9, 1994.

[9] Ravi S. Sandhu, "Lattice-Based Access Control Models," IEEE COMPUTER, 11, 1993. pp.9-19.

[10] Ravi Sandhu, "Access Control : The Neglected Frontier," Proc. First Australasian Conference on Information Security and Privacy, 6. 1996.

[11] Ravi S. Sandhu, "Role Hierarchies and Constraints for Lattice-Based Access Controls," Proc. Forth European Symposium on Research in COMPUTER SECURITY, pp.1-19, 9. 1996.

[12] David d. Clark, David R. Wilson, "A Comparison of commercial and Military computer policies," IEEE, 1987.

[13] Anthony Boswell, "Specification and Validation of a Security Policy Model," IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, Vol.21, No.2, pp.63-68, 2, 1995.

[14] J. E. Dobson and J. A. McDermid. Security Models and Enterprise Models. Database Security II : Status & Prospects, pp.1-39, 1989.

[15] David Rann, John Turner and Jenny Whitworth, "Z : A Beginner's Guide," School of Computing Staffordshire University, 1994.

[16] Bryan Ratcliff, "INTRODUCING SPECIFICATION USING Z : A Practical Case Study Approach," McGRAW-HILL BOOK COMPANY, 1994.

[17] Morris Sloman, Network and Distributed Systems Management, Addison-Wesley, 1994.

[18] ITU-T X.741 : "Information Technology - Open Systems Interconnection - System Management - Objects and Attributes for Access Control".

[19] ITU-T X.812 : "Information Technology - Open Systems Interconnection - Security Frameworks For Open System - Access Control Framework".

[20] 최은복, 이형효, 노봉남, "Biba 모델과 역할기반 접근제어 모델의 상호연동", 한국통신정보보호학회 종합학술발표회 논문집, 제8권 제1호, 1998.

[21] 이형효, 최은복, 노봉남 "역할기반 접근통제 시스템에서 응용 프로그램의 설계 및 실행지원 프레임워크", 한국정보처리학회 논문지, 제6권 제11호, 1999.

최 은 복

e-mail : eunbog@suncheon.ac.kr

1992년 전남대학교 전산학과 졸업(이학사)

1996년 전남대학교 대학원 전산학과 졸업 (이학석사)

2000년 전남대학교 대학원 전산학과 졸업 (이학박사)

2001년~현재 순천제일대학 인터넷정보학부 교수

관심분야 : 통신망관리, 정보보안, 멀티미디어시스템 등

노 봉 남

e-mail : bongnam@chonnam.ac.kr

1978년 전남대학교 수학교육과 졸업(이학사)

1982년 한국과학기술원 전산학과(공학석사)

1994년 전북대학교 대학원 전산통계학과 (이학박사)

1983년~현재 전남대학교 컴퓨터정보학부 교수

관심분야 : 객체지향시스템, 통신망관리, 정보보안, 컴퓨터와 정보사회 등