情報保護學會論文誌
第13券 第4號, 2003. 8

권한상속 제한 기능을 제공하는 역할계층 모델*

이 용 훈**, 김 용 민**, 이 형 효***, 진 승 헌****

A Model of Role Hierarchies providing Restricted Permission Inheritance

Yong-Hoon Yi**, Yong-Min Kim**, Hyung-Hyo Lee***, Seung-Hun Jin****

요 약

역할기반 접근통제 모델(RBAC)은 역할 계층구조에서 권한의 상속과 임무분리와 같은 제약조건을 다룸으로써 접근 권한의 관리를 수월하게 하는 장점이 있다. 하지만 기존의 RBAC 연구에서는 현실세계의 기업 환경에서 일어나는 역할계층을 제대로 반영한다고 볼 수 없다. 역할 계층에서, 하위의 접근 권한이 모두 상위 역할로 상속된다는 것은 최소권한(least privilege) 원칙이 위배로 인한 권한 남용의 문제를 일으킬 수 있다. 본 논문에서는 기업 환경에서 조직체계를 유지하면서 역할을 여러 개의 부역할(sub role)로 세분화하여 전체 상속, 부분 상속, 상속되지 않는 역할로 나누어 부역할 간 계층관계를 새롭게 정의함으로써 무조건적인 권한의 상속을 제한하는 모델을 제시한다. 특히, 권한 상속제한에 있어서는 역할 계층 내에서 상속되는 상위역할을 명시함으로써 불필요한 권한 상속으로 인한 권한남용을 방지한다.

ABSTRACT

Role-based Access Control(RBAC) model has advantage of easy management of access control with constraints such as permission inheritance and separation of duty in role hierarchy. However, previous RBAC studies could not properly reflect the real-world organization structure with its role hierarchy. User who is a member of senior role can perform all permissions because senior role inherits all permissions of junior roles in the role hierarchy. Therefore there is a possibility for senior role members to abuse permissions due to violation of the least privilege principle. In this paper, we present a new model of role hierarchy, which restricts the unconditional permission inheritance. In the proposed model, a role is divided into sub roles(unconditional inheritance, restricted inheritance, private role), keeping organization structure in corporate environment. With restricted inheritance, the proposed model prevents permission abuse by specifying the degree of inheritance in role hierarchy.

keyword : *Role-based Access Control, Role Hierarchy, Permission inheritance, Least privilege, permission abuse*

Ⅰ. 서 론

최근 들어 기업 및 정부 조직의 보안체제 구축 요구가 급증하여 이에 대한 연구가 활발히 진행되고 있다. 대부분의 기업과 정부기관들이 관련 업무를 정보처리 시스템에 의존함에 따라 인가된 주체나 사용자에게 자원들(resources)들이 불법 노출되면 조직운영이 어렵게 될 수 있다. 따라서 권한이 있는 사용자

* 본 연구는 한국전자통신연구원 연구과제(0701-203-0021) 지원으로 수행하였습니다.
** 전남대학교 전산학과({yhyi, ymkim}@athena.jnu.ac.kr)
*** 원광대학교 정보·전자상거래학부(hlee@wonkwang.ac.kr)
**** 한국전자통신연구원(ETRI) 정보보호연구본부 인증기반연구팀(jinsh@etri.re.kr)

들에게만 특정 데이터 또는 자원들이 제공 되는 것을 보장하기 위해 서로 다른 종류의 접근통제(access control)를 구현하기 위해 노력하였다. 접근통제는 일반적으로 어떤 사용자(users) 또는 사용자 집단(groups of users)이 자원에 대해서 조회, 변경 등의 연산(operations)을 수행할 수 있는가 없는가에 대하여 제한할 수 있는 수단이다.[1]

지금까지 연구된 접근통제 모델로는 임의적 접근통제(Discretionary Access Control: DAC)와 강제적 접근통제(Mandatory Access Control: MAC)가 있다. 이러한 접근통제 방법은 기업 환경에 적용하는데 한계가 있기 때문에 여러 대안이 연구되고 있는데 역할기반 접근통제(Role-Based Access Control: RBAC)는 기업의 조직구조를 바탕으로 구성되었으므로 전통적인 접근통제 방식인 MAC과 DAC의 대안으로 평가되고 있다.[2]

RBAC은 역할을 기반으로 접근통제 서비스를 제공하고자 제시된 모델로서 그 중심내용은 권한이 역할에 부여되고, 사용자는 조직 내에서 책임과 자격에 맞는 역할에 할당된다는 것이다. 따라서 역할에 할당된 사용자만이 그 역할에 배정된 접근권한을 사용할 수 있다. 특히, 기업의 관리 및 업무 구조 체계를 RBAC모델의 역할(role)로 사상한 역할 계층(Role Hierarchy)구조 개념의 도입으로, 관리가 용이하기 때문에 DAC이나 MAC에 비해 복잡한 기업 환경을 자연스럽게 모델링 하는 장점이 있다.

그러나 기업 환경에서 접근통제는 단순히 역할을 사상한 역할 계층구조의 도입으로 모든 문제가 해결되는 것은 아니다. 그 이유를 살펴보면 다음과 같다.

- 조직구조와 역할 계층의 불일치 : 현실 세계에서는 상위역할에 속한 과장 역할이 하위 계층인 대리 역할과 아무런 관계가 존재하지 않을 수도 있다. 이때는 과장에 속하는 역할을 업무의 특성상 상속범위에 따라 나눌 수 있어야 한다.
- 권한의 남용 우려 : 역할계층은 하위 역할의 모든 권한을 상위역할이 모두 상속받는다는 개념을 의미한다.[4] 현실세계에서는 이를 적절히 통제하는 방안들이 있지만, 현실을 컴퓨터에 투영한 컴퓨터 세계에서는 단순히 역할 계층 개념으로 해결하려 한다면 상위역할에 배정된 사용자가 그 하위의 모든 역할의 권한을 다 소유하여 권한 남용(permission abuse)이 발생할 수 있다. 때문에 효율적인 인가 권한관리가 필요하다.

이와 같은 이유로 인해 기업 환경에 적합한 접근통제모델을 설계하는 일은 어렵고 기업의 특성을 충분히 반영한 모델이 부재한 실정이다. 지금까지 RBAC 모델에서는 역할 계층위에서 상위 역할에 배정된 사용자는 하위 역할의 모든 접근 권한을 상속받게 되는데, 이는 불필요한 권한의 실행을 허가 받게 되어 최소권한 원칙을 위배하게 된다. 실생활에서 하위 역할에 배정된 권한을 최 상위 역할에 배정된 사용자가 실행하지 않은 경우가 종종 일어나게 된다. 예를 들어, 부장(manager)는 사원(clerk)의 상위 역할이지만 부장(manager)은 사원(clerk)이 수행하는 "register purchase"업무를 자동적으로 상속받지는 않는다.[5] 이는 부장이 사원의 상위 역할이지만, 실제 생활에서 하위 역할인 사원의 모든 업무를 다 상속받아 수행하지는 않는다는 것을 의미한다. 이런 문제점의 해결책으로 고유 역할(private role)을 통한 권한 상속제한이 있었다. 하지만 이것은 단지 권한의 상속을 방지하는 기능만을 제공할 뿐, 상속의 정도 제한이 요구되는 현실 세계에 적용하는 데는 한계가 있다.

본 논문에서는 이러한 문제점들에 대한 해결책으로 하나의 역할을 권한 상속 정도에 따라 여러 개의 부역할(Sub role)로 세분화 하였다. 하나의 역할을 조직공통(Corporate Common), 부서공통(Department Common), 상속제한(Restricted Inheritance), 고유역할(Private Role)로 나눔으로써, 조직구조와 역할 계층을 일치시키고 권한 남용의 우려를 해결할 수 있는 장점을 가진다. 또한 권한 상속을 제한하여 최소권한의 원칙을 지킬 수 있는 부가적인 이점도 얻는다.[6,7] 본 논문의 2장에서는 RBAC에서 역할 계층과 관련된 연구를 살펴본다. 3장에서는 제안한 모델에 대해 설명하고, 4장에서는 제안한 모델의 정형화된 표현과 기존 모델과 비교 한다. 마지막으로 5장에서는 결론 및 향후 연구과제에 대해 설명한다.

II. 관련 연구

RBAC의 중심적인 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이와 같이, RBAC에서 역할은 가장 중요한 구성요소이며, 이러한 아이디어는 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유

연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도 역할의 변경을 쉽게 할 수 있다.

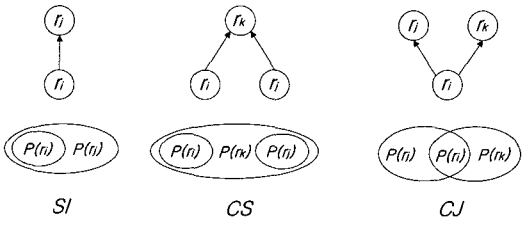
Sandhu는 RBAC96에서 권한을 효율적으로 관리하기 위해 역할 계층을 제안했다.[4] RBAC의 모든 권한은 역할에 의해 의존되기 때문에 RBAC내에서 역할들 간의 관계를 나타내는 역할 계층의 개념은 매우 중요하며, 복잡하고 거대한 기업 환경을 모델링하기 위해 RBAC에서의 역할 계층의 도입은 필수 불가결한 사항이다. RBAC96에서 역할 계층은 관련성이 있는 역할들 간의 부분순서(partial order)관계로서 정의되며 특히, 역할 계층은 기업의 권한과 책임의 체계와 매우 유사하여 기업의 권한체계를 모델링 하는데 적합하다. 이런 특징으로 RBAC은 기업 환경에 매우 적합한 접근 통제 방법으로 인식되고 있다. 또한 현실세계에서 상위 역할이 하위의 역할보다 더 많은 권한과 책임을 가지는 것을 의미하는 조직구조가 시스템 내의 구현에서는 하위 역할이 갖는 모든 접근권한을 상위역할이 무조건적으로 모두 포함하는 역할계층의 상속(inheritance)으로 표현된다.[8]

Moffet은 현실적인 기업 환경에서 여러 가지 다양한 역할 계층이 존재함을 제시하였다.[3] 그는 상위 역할은 그들의 하위 역할의 모든 접근권한을 상속하지만, 조직에서의 계층구조를 고려할 때, 어떤 환경에서 접근권한의 무조건적인 상속은 바람직하지 않음을 설명하고, 역할계층과 상속과 관련하여 다양한 역할 계층이 기업 환경에 존재함을 보였다.

Moffet이 제시한 대표적인 역할 계층은 다음과 같다.

- 일반화 계층(Generalization Hierarchy)
- 집단화 계층(Aggregation Hierarchy)
- 관리 계층(Supervision Hierarchy)

Nyanchama는 역할 계층을 위해 역할 그래프(role graph)을 도입하였다.[9] 역할은 조직의 특성과 그 역할을 수행하는 사용자의 책임과 자격에 따라 생성되며, 하위 역할의 접근권한은 상위역할에 상속되어진다. 역할간의 접근권한의 상속되는 방향을 (→)으로 표현할 때, 역할계층에서 부분순서 관계에 있는 역할은 접근권한 상속에 따라 [그림 1]과 같이 단순 접근권한(SI: Simple Inheritance), 공통 상위 접근권한(CS: Common Senior Inheritance)과 공통 하위 접근권한(CJ: Common Junior Inheritance)의 세 가지 유형으로 구분



〔그림 1〕 역할의 구성

할 수 있다. Nyanchama가 제안한 세 가지 유형 모두 상위역할이 하위역할의 접근권한을 모두 상속받게 되는데, 이것은 상속의 원리를 준수하나 상위역할에 권한이 집중되어 권한 남용의 문제점이 발생한다.

이처럼 기존의 RBAC 연구는 권한을 효율적으로 관리하기 위해 접근 권한의 무조건적인 상속과 기업 환경에 적합한 다양한 역할 계층의 도입, 상속 관계를 기초로 한 간단한 그래프 표현 등을 제시하고 있다. 하지만 이들 연구는 다음과 같은 한계를 나타내고 있다. 첫째, 현실 세계에서는 하위역할의 모든 권한이 상위 역할로 무조건적으로 상속이 이루어지지 않는 역할이 존재한다. 둘째, Moffet처럼 기업 환경에 적합한 여러 역할 계층의 도입은 하나가 아닌 여러 개의 역할 계층을 관리해야하기 때문에 관리의 어려움이 발생한다. 셋째 그래프 표현이 효율적이긴 하지만 현실세계에서 요구되는 권한상속 정도(degree of inheritance)를 표현하지 못하는 한계를 지니고 있다. 또한, 기존연구에서 무조건적인 권한상속을 방지하기 위한 대안으로 고유역할(private role)을 도입했으나,[4] 이는 권한 상속을 방지 기능만을 제공할 뿐, 권한 상속 제한에 대한 해결책은 되지 못해 고유역할 또한 그 한계를 나타낸다. 그러므로 이런 한계점을 극복하기 위해서는 권한상속 제한 기능을 제공하고, 다양한 역할 계층이 아닌 조직 체계와 유사한 단순한 역할 계층을 도입하여 간단한 관리 기능을 제공하여야 한다. 또한 상속관계를 기본 배경으로 권한상속 제한 기능을 간단한 그래프로 표현하고 정형화하는 연구가 요구된다.

Ⅲ. 권한상속제한 기능을 제공하는 역할계층 모델

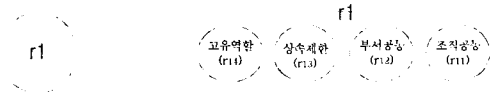
RBAC은 일반적으로 조직구조와 권한 상속 특성이 하나의 역할계층에 표현됨에 따라 기업 환경의 조직구조를 자연스럽게 모델링 하는 장점이 있다. 그러나 역할계층의 상위 역할에 배정된 사용자는 하위 역할에 배정된 전체권한을 상속받게 되어 불필요한

권한을 갖게 됨으로써 권한의 남용과 그로 인해 최소권한원칙에 위배됨을 알 수 있다. 이러한 문제점을 해결하기 위해 본 논문에서는 역할을 여러 개의 부역할로 세분화하여 상위역할에 무조건적인 상속을 제한하는 기능을 제공하는 모델을 제안한다.

3.1 역할(role)

역할의 정의는 역할에 부여된 책임과 권한을 기술하는 조직 내의 업무 기능(job function)으로 정의할 수 있다.[4] 또한, 역할이 컴퓨터 시스템 안에 표현될 때는 업무기능을 수행하기 위해 필요한 여러 자원들에 대한 접근 권한들의 집합으로 표현된다.[9] 본 논문에서는 상위역할로의 무조건적인 상속을 제한하기 위해 기업의 한 역할을 각 업무별 상속정도의 특성에 따라 4개의 속성으로 표현된 부역할(sub role)로 분할한다. [그림 2]는 기존의 역할과 본 논문에서 제안한 업무별 상속정도에 따라 분할한 부역할을 나타내고 있다.

[그림 2]의 (a)에서 역할 r1은 기업 내에서의 하나의 역할을 표현한 것이고 (b)는 역할에 배정된 권한들의 특징에 따라 조직 공통, 부서공통, 상속제한, 고유역할로 나눈 것이다. [표 1]은 하나의 역할을 여러 개의 부역할로 분류하는 기준을 설명한 것이다.



(a) 기존의 역할 (b) 상속정도 및 업무 특성에 따른 역할의 분류

[그림 2] 기존의 역할과 제안된 모델에서의 역할

[표 1] 기업환경에 따른 부역할 분류 기준

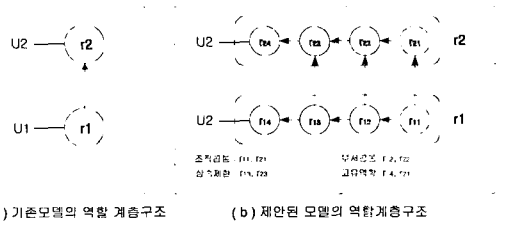
부 역할의 종류 및 상속정도	부 역할에 배정된 권한 특징
조직공통 (전체 상속)	• 조직 내 모든 구성원에게 허가된 권한 • 상위역할은 하위역할의 모든 권한을 포함
부서공통 (전체 상속)	• 부서에 속한 구성원들에게만 허가된 권한 • 상위역할은 하위역할의 모든 권한을 포함
상속 제한 (제한적 상속)	• 하위역할의 권한이 지정된 상위역할에만 상속 • 역할 분석과 설계 과정에서 상속이 제한되는 권한에 대한 조사 필요 • 역할 간에 제한적 상속이 가능함
고유역할 (상속 없음)	• 상위역할로 권한 상속이 이루어지지 않는 권한들 • 상위역할이 존재하지 않는 권한들

3.2 권한상속 제한 역할계층의 구조

RBAC96에서 역할 계층은 관련성이 있는 역할들 간의 부분순서(partial order: ≥)로 정의한다. [그림 3]은 기존 모델의 역할 계층구조와 제안된 모델의 역할 계층구조를 비교하여 나타내고 있다.

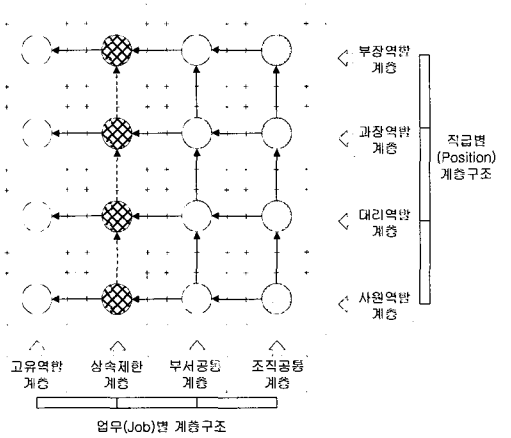
[그림 3]에서 $r_{11} \rightarrow r_{21}$, $r_{12} \rightarrow r_{22}$는 각각 조직공통과 부서공통의 역할계층으로서 하위역할에 배정된 모든 권한이 모든 상위역할에 상속된다. $r_{13} \dashrightarrow r_{23}$은 상속제한 역할계층으로서 제한적인 권한상속이 일어나는 계층이다. 마지막으로 r_{14}와 r_{24}는 고유 역할(private role)로서 상위역할에 대한 상속관계가 없는 역할이다. 그리고 사용자는 고유 역할에 배정한다. 기존의 RBAC에서는 보안관리자가 모든 역할에 사용자를 배정하는 것이 가능하지만, 제안된 모델에서는 하나의 역할을 여러 개의 부역할로 분할하였기 때문에 기존의 역할과 동일한 권한을 행사할 수 있도록 하기위해 모든 부역할의 권한을 상속받는 고유역할에 사용자를 배정한다. 이렇게 함으로써 제안된 모델을 기 구축된 RBAC모델에 적용할 때, 사용자 배정 부분과 동일한 효과를 줄 수 있을 뿐 아니라 상속제한 계층을 둠으로써 사용자가 하위의 모든 권한을 가짐으로써 발생할 수 있는 최소권한의 위배를 해결할 수 있는 장점을 가진다. 역할 r1을 r_{11}, r_{12}, r_{13} ,r_{14}의 부역할로 세분화할 때, 부역할 사이에서 $r_{14} \geq r_{13} \geq r_{12} \geq r_{11}$의 단일 역할 내 계층구조(Intra-Role Role Hierarchy)가 존재한다. 사용자는 고유 역할에 배정되므로 그 하위의 역할인 조직공통, 부서공통, 상속제한 그리고 고유 역할에 배정된 모든 권한의 실행이 가능하다. 상속제한 역할 계층에서는 조직구조를 고려하여 역할들 간의 관계를 설정할 수 있기 때문에 조직구조와 역할 계층을 일치시킬 수 있으며, 상속제한 계층구조에서 상속을 제한 할 수 있기 때문에 권한 남용의 문제점을 해결할 수 있는 장점이 있다.

[그림 4]에서는 상속제한 역할 계층구조를 나타낸 것으로 가로와 세로로 업무(Job)별, 직위(Position)별

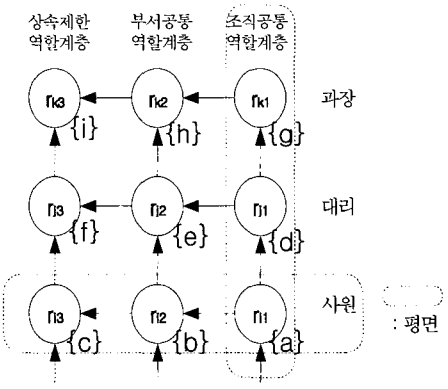


(a) 기존모델의 역할 계층구조 (b) 제안된 모델의 역할계층구조

[그림 3] 기존의 역할계층과 제안된 모델의 역할계층 구조



〔그림 4〕 상속제한 역할 계층 구조의 예



〔그림 5〕 부역할간 역할 계층 구조

계층구조를 가진다. 여기서 업무별 계층구조에서 조직공통계층은 조직구성원 모두가 이용 가능한 역할들이 여기에 해당되며, 직위별 계층구조에서 사원역할계층은 사원이 갖게 되는 전체 역할을 나타낸다. 또한 [그림 4]에서 하나의 역할을 선택하면, 그 역할은 동시에 업무별, 직위별 계층구조에 속한다. 직위별 계층구조는 직위에 따라 나뉘어, 무조건적인 상속이 이루어지는 특징이 있고, 실선(→)으로 이루어진 관계이다. 또한 업무별 계층구조에서 고유역할은 상속이 안 되고, 조직공통과 부서공통계층 내에 있는 역할들은 배정된 권한 뿐 아니라 상속받은 권한 전체가 모두 상위역할에 상속된다. 특히, 본 논문의 중심인 상속제한계층에 있는 역할은 점선(⇢)으로 표시되고, 역할에 배정된 접근권한의 상속이 이루어진다.

3.3 부역할(subrole)간 계층구조

조직공통, 부서공통 역할 간 계층에서는 하위 역할의 모든 권한이 자신의 모든 상위 역할에 상속되므로 기존의 역할 계층과 같다. 하지만 상속제한 계층구조는 제한적으로 권한 상속이 일어나는 역할을 나타낸 것으로 기존의 모든 것이 상속되는 역할 계층과 구분이 된다. 조직공통 및 부서공통 역할계층과 상속제한 역할계층간 상속특성에 대해서 [그림 5]를 바탕으로 설명한다. [그림 5]에서 상속관계를 표현할 때, 조직공통 역할과 부서공통 역할은 실선화살표(→)를 사용하며, 상속제한 역할은 점선화살표(⇢)로 표기하며, 각각의 분할된 부 역할에 각각 {a,b,c ...} 등의 권한이 배정되어 있음을 알 수 있다. 역할 r_{i1}에는 {a}라는 권한이 배정되어있고 역할 r_{j1}에는 {d}라는 권한이 배정되어 있지만, 상속관계에 의해서 역할 r_{j1}은 초기에 배정받은 {d}라는 권한 외에도 상속관계에 의해 권한 {a}를 상속 받는다. 이때 역할 r_{j1}에 대해서, 권한 {d}는 명시적 권한(explicit permission)이라 하고, 권한 {a}는 묵시적 권한(implicit permission)이라 하며, 명시적, 묵시적 권한의 합인 {a,d}를 유효권한(effective permission)이라고 정의한다. 여기서 상속관계의 표현에서 실선 화살표는 유효권한 상속을 나타내며, 점선 화살표는 명시적 권한 상속을 의미한다. 따라서 이들 실선 화살표와 점선화살표는 권한의 상속관계에 있어 역할이 가지고 있는 어느 권한을 상속하고 어느 권한을 상속하지 않는 지에 대한 표현을 가능하게 한다.

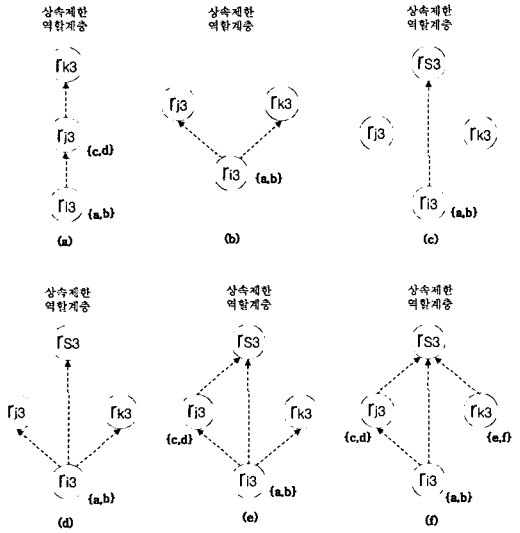
[그림 5]에서 부서 공통 및 조직공통 역할계층 내 역할들의 관계는 실선 화살표 표시되어, 하위역할의 모든 유효 권한이 상위역할에 상속된다. 예를 들어 직위별 역할계층 $r_{k1} \rightarrow r_{k2}$인 관계에 의해, 역할 r_{k2}는 자신에게 배정받은 권한 {h} 이외에 역할 r_{k1}의 유효권한인 {a,d,g}를 갖게 되며, 또한 업무별 역할계층 $r_{j2} \rightarrow r_{k2}$인 관계에 의해 자신에게 배정받은 권한 {h} 이외에 역할 r_{j2}의 유효 권한인 {a,b,d,e}를 상속받게 된다. 결국 r_{k2}의 유효권한은 {a,b,d,e,g,h}가 된다.

또한 제안된 모델에서 동일한 직위별, 업무별 계층에 있지 않는 두 부역할에 대해서도 상속관계는 형성된다. [그림 5]에서 예를 들어 $r_{j2} \rightarrow r_{k3}$이라는 관계가 있다고 할 때, 부역할 r_{j2}, r_{k3}은 서로 다른 직위별, 업무별 계층에 속하는 부역할이지만 이들 부역할 사이에도 상속 관계가 존재한다. $r_{j2} \rightarrow r_{k3}$은 부서공통 역할계층에서 $r_{j2} \rightarrow r_{k2}$관계가 형성되며, 과장직위 역할계층에서 $r_{k2} \rightarrow r_{k3}$의 관계가 있으므로 $r_{j2} \rightarrow r_{k3}$관계에서도 상속관계가 형성함을 알 수 있다. 이렇게 서

로 다른 두 업무별, 직위별에 있는 임의의 두 역할 간에도 제안된 계층구조를 이용하여 업무별과 직위별사이에서 나타난 상속관계를 알 수 있다.

3.4 상속제한 역할계층의 특징

상속제한 역할계층은 하위의 역할이 가지는 유효 권한을 상위로 상속하는 것이 아니라, 명시적 권한만 상속함으로써 상속을 제한 할 수 있는 계층이다. 따라서 상속제한 역할계층에서는 역할에 배정된 명시적 권한만 상속관계에 영향을 미치며, 묵시적 권한은 상속관계에서 배제된다. 상속제한 역할계층에서는 상속을 원하는 상위의 역할을 구체적으로 명세하여 상속을 제한한다. [그림 6]에 제시된 (a)~(f)는 상속제한 역할계층에 대한 대표적인 예제를 나타낸 것이며, [표 2]는 [그림 6]과 같은 상속제한 역할계층이 주어졌을때, 상속관계를 나타낸 것이다.



[그림 6] 상속제한 역할계층의 다양한 예

[표 2] 상속제한 역할계층에서의 상속관계

경우	역할	권한	상속
(a)	r_{i3}	{a,b}	{r_{j3}}
	r_{j3}	{c,d}	{r_{k3}}
(b)	r_{i3}	{a,b}	{r_{j3},r_{k3}}
(c)	r_{i3}	{a,b}	{r_{s3}}
(d)	r_{i3}	{a,b}	{r_{j3},r_{k3},r_{s3}}
(e)	r_{i3}	{a,b}	{r_{j3},r_{k3},r_{s3}}
	r_{j3}	{c,d}	{r_{s3}}
(f)	r_{i3}	{a,b}	{r_{j3},r_{s3}}
	r_{j3}	{c,d}	{r_{s3}}
	r_{k3}	{e,f}	{r_{s3}}

Ⅳ. 제안된 모델의 정형화

본 절에서는 제안한 모델을 정형화하여 기술한다.

4.1 정 의

4.1.1 역할의 정의

- R = 부역할들의 집합 ($r_{ij} \in R$, where i = 1..n , j = 1..4)
- $R_{CC} = R_{JOB1}$, $R_{DC} = R_{JOB2}$, $R_{RI} = R_{JOB3}$, $R_{PR} = R_{JOB4}$; R_{CC}(조직공통 = R_{JOB1}), R_{DC}(부서공통=R_{JOB2}), R_{RI}(상속제한 = R_{JOB3}), R_{PR}(고유역할=R_{JOB4})부역할들의 집합
- $R_{POSi} = \{r_{ik} \mid k=1..4\}$ where, $1 \le i \le n$; 각 직위와 연관된 부역할들의 집합
- $R_{JOBi} = \{r_{ki} \mid k=1..n\}$ where, $1 \le i \le 4$; 각 업무와 연관된 부역할들의 집합
- R_{POS} = 모든 직위와 관련된 부역할집합의 합집합
- R_{JOB} = 모든 업무와 관련된 부역할집합의 합집합

4.1.2 역할계층의 정의

- $RH \subseteq R \times R$, 역할 계층; 부분 순서관계
- $RH_{CC} \subseteq R_{CC} \times R_{CC}$, 조직공통 역할간의 부역할 계층; 부분 순서관계
- $RH_{DC} \subseteq R_{DC} \times R_{DC}$, 부서공통 역할간의 부역할 계층; 부분 순서관계
- $RH_{RI} \subseteq R_{RI} \times R_{RI}$, 상속제한 역할간의 부역할 계층; 부분 순서관계
- $RH_{POSi} \subseteq R_{POSi} \times R_{POSi}$, where $1 \le i \le n$, 각 직위별 내의 역할 계층; 부분 순서관계
- $RH_{JOBi} \subseteq R_{JOBi} \times R_{JOBi}$, where $1 \le i \le 4$, 각 업무별 내의 역할 계층; 부분 순서관계
- RH_{POS} = 각 직위별 역할계층들의 합집합
- RH_{JOB} = 각 업무별 역할계층들의 합집합
- $RH_{PL} \subseteq R \times R$, 각 업무별 또는 직위별 부역할들의 계층
- $RH_{D} \subseteq R \times R$, 각 대각선에 위치한 부역할들의 계층
- $\ge$: 역할 계층 위에서의 부분 순서관계(partial order)

4.1.3 함수 및 기타 정의

- role_jobs: $R \rightarrow CC \cup DC \cup RI \cup PR$ (단, $PR \ge RI \ge DC \ge CC$) 어떤 부역할이 어느 업무특성에 속하는지 말해주는 함수
- role_positions: $R \rightarrow N$ (N: 자연수), 어떤 부역할이 속해 있는 직위를 반환해주는 함수
- ancestor_roles: $R \rightarrow 2^R$, 역할에 배정된 접근권한을 상속받는 상위역할들의 반환하는 함수
- assigned_users: $r_{ij} \rightarrow 2^{USERS}$, 단 $r_{ij} \in R_{PR}$ 사용자 배정을 나타내는 함수
- mutex_roles_set $\subseteq R \times R$, 상호 배타적인 관계에 있는 역할들의 순서쌍의 집합

4.2 성 질

(1) $R = R_{JOB} = R_{POS}$
(2) $R_{JOB} = R_{CC} \cup R_{DC} \cup R_{RI} \cup R_{PR} = \cup_{i=1}^{4} R_{JOBi}$
(3) $RH_{JOB} = RH_{CC} \cup RH_{DC} \cup RH_{RI} = \cup_{i=1}^{3} RH_{JOBi}$
(4) $R_{POS} = R_{POS1} \cup R_{POS2} \cup ..... R_{POSn-1} \cup R_{POSn} = \cup_{i=1}^{n} R_{POSi}$
(5) $RH_{POS} = RH_{POS1} \cup RH_{POS2} \cup RH_{POS3} \cup ... \cup RH_{POSn} = \cup_{i=1}^{n} RH_{POSi}$
(6) $RH_{PL} = \{(r_{ij}, r_{nm}) \mid i=n \vee j=m$ 단, $r_{ij} \neq r_{nm}\}$
(7) $RH_{PL} = RH_{POS} \cup RH_{JOB}$
$(r_{ij}, r_{nm}) \in RH_{PL} \Rightarrow (r_{ij}, r_{nm}) \in RH_{POS} \vee (r_{ij}, r_{nm}) \in RH_{JOB}$
(8) $(r_{in}, r_{im}) \in RH_{POSi}$, $role\_jobs(r_{in}) \geq role\_jobs(r_{im})$ 단, $1 \leq i \leq k$
$(r_{ni}, r_{mi}) \in RH_{JOBi}$, $role\_positions(r_{ni}) \geq role\_positions(r_{mi})$ 단, $1 \leq i \leq 4$
(9) $RH_D = \{(r_{ij}, r_{nm}) \mid i > n \wedge j > m\}$
(10) $(r_{ij}, r_{nm}) \in RHD$
$\Rightarrow (r_{ij}, r_{nm}) \notin RH_{POSn} \wedge (r_{ij}, r_{nm}) \notin RH_{JOBm}$ (10-①)
$\Rightarrow (role\_positions(r_{ij}) \geq role\_positions(r_{nm})) \wedge (role\_jobs(r_{ij}) \geq role\_jobs(r_{nm}))$ (10-②)
$\Rightarrow \exists r_{st} \in R \cdot (role\_positions(r_{ij}) \geq role\_positions(r_{st})) \wedge (role\_jobs(r_{st}) \geq role\_jobs(r_{nm}))$ (10-③)

4.3 임무 분리

임무분리 특성은 대부분의 상업 환경에서 요구되는 주요 보안성질이며, 상호배타성(mutual exclusiveness)은 임무분리 특성을 구현하기 위한 방법들 중의 하나이다.[10,11] 임무분리의 종류[12]로는 정적 임무분리(Static SoD), 동적 임무분리(Dynamic SoD), 연산 임무분리(Operational SoD), 객체 임무분리(Object SoD) 등 다양하게 존재하지만 본 논문에서의 임무분리는 정적 임무분리를 나타낸다.

역할기반 접근통제 모델의 기본은 역할이며 역할단위로 상호배타성을 부여함으로써 임무분리 특성을 구현할 수 있다. 하지만, 정보객체에 대한 실질적인 접근은 권한에 의해 이루어지므로 역할단위의 상호배타성은 권한단위의 상호배타성과 관련되게 된다. 또한, 상호배타적 역할은 정보의 무결성 보장을 위한 제약조건이며, 두 역할이 상호배타적 역할임을 결정하는 기준은 두 역할에 배정된 권한의 의미적 기능에 따르며 일반적인 규칙은 존재하지 않는다.[13]

임무분리는 역할기반 접근통제 모델 관리과정의 사용자 배정 단계에서 상호 배타적 역할에 동일 사용자를 배정시키지 않음으로써 정보 시스템의 보안을 유지하는 보안특성이다. 이 특성은 역할에 대한 사용자의 권한부여 시점(authorization time)에서 역할 단위의 상호배타성을 적용한다. 만일 역할 r_{ij}, r_{nm}가 상호배타적 역할인 관계이면, 사용자는 두 역할을 동시에 배정 받지 않아야 한다는 조건을 말한다.

제안된 모델에서 부역할 간에 임무분리를 만족하는 기본 규칙을 기술하면 다음과 같다.

4.3.1 제안된 부역할의 상호배타 관계

제안된 모델에서 부역할 간의 상호배타관계를 나타내면 다음과 같다.

- 부역할 r_{ij}, r_{nm}이 성질 (6)과 (7)을 만족하면 상호 배타적 관계는 없음
  $\forall (r_{ij}, r_{nm}) \in RH_{PL} \Rightarrow (r_{ij}, r_{nm}) \notin mutex\_roles\_set$
- 부역할 r_{ij}, r_{nm}이 성질 (9)와 (10)을 만족하면 상호 배타적 관계는 없음
  $\forall (r_{ij}, r_{nm}) \in RH_D \Rightarrow (r_{ij}, r_{nm}) \notin mutex\_roles\_set$

4.3.2 임무분리 표현

제안된 모델에서 임무분리 제약조건을 만족하는 기준은 다음과 같다.

$\forall (r_{ij}, r_{nm}) \in mutex\_roles\_set \mid assigned\_users(r_{ij}) \cap assigned\_users(r_{nm}) = \varnothing$

4.4 기존모델과의 비교

접근통제 모델에 대한 평가는 그 특성상 성능평가나 정량적인 평가가 어렵다. 따라서 본 논문에서는 제안한 모델이 RBAC의 근본 취지와 현실세계를 얼마나 잘 반영하고 있는가에 대해서 [4]와 [5]의 논문을 이용하여, [표 3]에서 비교 평가한다. [4]의 private

〔표 3〕 기업환경에 따른 부역할 분류 기준

비교 대상	RBAC	T-RBAC	제안된 모델
역할개념 지원	○	○	○
역할단위의 접근제어	○	○	○
역할계층지원	○	○	○
하위역할에서 상위역할로의 제한적 상속 기능	×	×	○
임무분리지원	○	○	○
서로 다른 역할계층간의 상속 관계 지원	×	×	○
구조의 단순함	○	×	×
선택적인 상속제한 제공	보통	보통	우수
기업 조직구조에 대한 적합성	×	×	○

role이나 [5]의 Class P는 상속의 방지(block)에 매우 효율적이지만, 선택적인 상속이 이루어지는 경우에는 접근통제 적용에 어려움이 있다. 제안된 모델은 기업 환경의 조직구조와 상속 특성을 기준으로 역할을 구분한 것으로 기업 내의 역할에서 발생할 수 있는 다양한 상속제한 기능을 제공하기위해 제안되었다.

V. 결론 및 향후 연구과제

역할기반 접근통제는 기업의 조직구조에 적합하고 정보자원을 효율적으로 관리할 수 있다. 하지만 기존 연구에서는 상위역할이 하위역할이 가지는 모든 권한을 그대로 행할 수 있어 발생하게 되는 권한남용 문제를 내포하고 있다. 본 논문에서는 RBAC 모델의 속성을 유지하면서 역할을 업무별 상속정도에 따라 여러 개의 부역할로 세분화하는 모델을 제안하였다. 제안된 모델은 다음과 같은 장점이 있다. 첫째로 권한상속의 관점에서 역할의 종류를 분류하여 조직공통, 부서공통, 상속제한, 고유역할 부역할로 분할하였기 때문에 하위역할이 상위역할로 무조건적으로 상속되는 것을 제한하는 상속제한 기능을 제공한다. 둘째로, 권한 상속을 유효 권한과 명시적 권한의 상속을 구분하여 나타냈으며, 이는 부수적으로 상속제한 역할 구조를 이용하여 무조건적인 상속을 방지함으로써 권한 남용문제를 해결하고 최소권한의 원칙을 유지하는 장점이 있다. 셋째로, 역할계층의 관리에 있어 기업 내에 존재하는 여러 역할 계층으로 분리하여 관리하는 기존의 방안보다, 조직 체계와 유사한 역할계층 안에 업무별, 직위별 역할계층을 표현하여 조직체계와 유사한 모델링이 가능하게 했다.

향후 연구 분야는 논문에서 언급하지 않았지만 역할의 수가 증가 하면서 발생하는 문제점을 해결하기 위해 부 역할을 잘 정의하여 실제 조직을 그대로 반영할 수 있는 시스템을 구현할 필요가 있다. 또한 권한의 하위에서 상위로 상속되는 모델뿐만 아니라 권한이 상위 역할에서 하위로 위임되는 권한 위임모델에 대한 연구가 필요하다.

참 고 문 헌

[1] Warwick Ford, Computer Communications Security, *Prentice Hall*, 1994.

[2] David F. Ferraiolo, John F. Barkley, and D. Ricard Kuhn, "A Role-Based Access Control Model and Reference Implementation With a Corporate Intranet". *ACM Transactions on Information and System Security*, Vol.2, No.1, pp.34~64, Feb. 1999.

[3] Jonathan D. Moffett, "Control Principles and Role Hierarchies", *Proc of Third ACM Workshop on Role-Based Access Control*, October, 1998.

[4] Ravi S. Sandhu: "Role-Based Access Control Models", *IEEE Computer*, Feb, 1996.

[5] Sejong Oh, Seog Park: "Task-Role Based Access Control(T-RBAC): An Improved Access Control Model for Enterprise Environment". *DEXA2000*, Sep. 2000.

[6] 김명재, 이용훈, 이형효, 노봉남, "권한상속 기능을 제공하는 역할계층 설계방법론", *한국정보보호학회 학술대회*, pp.326~329, 2002.

[7] YongHoon Yi, MyongJae Kim, Young- Lok Lee, HyungHyo Lee, BongNam Noh, "Applying RBAC Providing Restricted Permission Inheritance to a Corporate Web Environment", Web Technologies and Applications, LNCS 2642, pp.287~292, Sep 2003 *to be appeared.*

[8] Ravi Sandhu, "Role activation hierarchies", *Proceedings of the third ACM workshop on Role-based access control*, pp.33~40, 1998.

[9] Matunda Nyanchama, "Commercial Integrity, Role and Object Orientation", *University of Western Ontario*, Phd thesis, Sep. 1994.

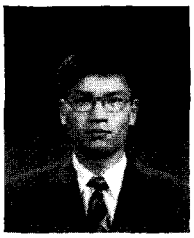
[10] Ferraiolo, Cugini, and Kuhn, "Role Based Access Control: Features and Motivations", *Computer Security Applications Conference*, 1995.

[11] Richard Kuhn, "Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems", *Second ACM Workshop on Role-Based Access Control*, 1997.

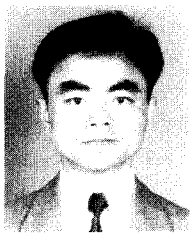
[12] Virgil D. Gligor, Serban I. Gavrila, and David Ferraiolo, "On the Formal Definition of Separation of Duty Policies and their Composition", *Proceedings of the IEEE Symposium on Security and Privacy*, pp.172~183. May 1998.

[13] 이형효, 최은복, 노봉남, "역할기반 접근제어 시스템 환경에서 무결성 보장을 위한 세션기반 응용 프로그램의 설계 및 운영구조", *한국통신정보보호학회 종합학술발표회논문집*, 제8권, pp.389~401, 1998.

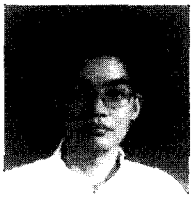
〈著者紹介〉



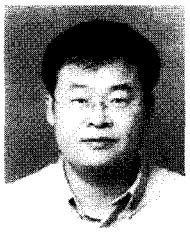
이 용 훈 (Yong-Hoon Lee) 정회원
1990년 2월 : 전남대학교 전산통계학과(이학사)
1994년 2월 : 전남대학교 전산통계학과 석사(이학석사)
2003년 8월 : 전남대학교 전산통계학과 박사(이학박사)
1994년~1997년 : Hewlett Packard Korea.
1997년~2000년 : 한국교육학술정보원(주임연구원)
<관심분야> 정보보호(보안모델, 인증/인가 기술, 보안명세), 컴퓨터/네트워크 보안



김 용 민 (Yong-Min Kim) 정회원
1989년 : 전남대학교 전산통계학과(이학사)
1991년 : 전남대학교 전산통계학과(이학석사)
2002년 : 전남대학교 전산통계학과(이학박사)
2003년 6월~현재 : 전남대학교 리눅스시스템 보안연구센터 Post-doc.
<관심분야> 시스템 및 네트워크 보안, 전자상거래 보안, 네트워크 관리, 퍼지 이론



이 형 효 (Hyung-Hyo Lee) 정회원
1987년 2월 : 전남대학교 계산통계학과(이학사)
1989년 2월 : 한국과학기술원 전산학과(이학석사)
2000년 2월 : 전남대학교 대학원 전산학과(이학박사)
1990년~1997년 : 삼보컴퓨터 기술연구소, 한국통신 연구개발원
2001년 3월~현재 : 원광대학교 정보·전자상거래학부 조교수
<관심분야> 보안모델, 통신망 보안관리, 전자상거래보안, 침입탐지시스템



진 승 헌 (Seung-Hun Jin) 정회원
1995년 2월: 숭실대학교 석사
1996 년 4월 : (주)대우통신 종합연구소 연구원
1999 년 5월 : (주)삼성전자 통신연구소 전임연구원
2003 년 7월 현재 : 한국전자통신연구원 정보보호연구본부 인증기반연구팀 팀장
< 관심분야> 정보보호(PKI, 인증/인가 기술, 프라이버시보호기술), 컴퓨터/네트워크 보안