권한상속 제한 기능을 제공하는 역할 계층 설계 방법론

김명재*, 이용훈**, 이형효***, 노봉남*

*전남대학교 정보보호협동

**전남대학교 전산학과

***원광대학교 정보전자상거래학부

A Design Methodology of Role Hierarchies providing Restricted Permission Inheritance

Myong-Jae Kim

Dept. of Information Security, Chonnam National Univ*

Dept. of Computer Science, Chonnam National Univ**

Division of Information and Electronic Commerce, Wonkwang Univ***

요 약

RBAC은 역할 계층구조에서 권한의 계승과 의무분리와 같은 제약조건을 다룸으로써 접근 권한의 관리를 수월하게 하는 장점이 있다. 하지만 기존의 RBAC 연구에서는 현실 세계의 기업 환경에서 일어나는 역할계층을 제대로 반영한다고 볼 수 없다. 역할 계층에서 접근 권한이 항상 아래에서 위로 상속된다는 것은 최소권한의 원칙 등의 문제를 일으킬 수 있다. 본 논문에서는 기업 환경에서 조직체계를 깨뜨리지 않고 역할을 여러 개 부역할(sub role)로 세분화하여 전체 상속, 부분 상속, 상속되지 않는 역할로 나누어 계층구조를 유지할 수 있으면서 역할 상속을 제한하는 모델을 제시하고 있다.

I. 서론

RBAC의 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.

조직 내에서 계층에는 조직 구조(Organization Structure), 일반화 계층(Generalization Hierarchi- es), 집단화 계층(Aggregation Hierarhies), 관리계층(Supervision Hierarchies)등으로 나누어 볼 수 있다[2].

RBAC 모델에서 역할계층은 일반적인 조직구조와 권한 상속의 특성을 하나의 역할계층에 표현함으로써 조직의 구조가 역할계층에 반영되어 기업 환경의 조직구조를 자연스럽게 모델링하는 장점이 있다. 상위의 역할은 하위의 역할이 갖는 모든 접근권한을 상속받게 되어 권한의 관리 측면(Permission Management)에서 장점이 있다[3].

역할 계층 내에 있는 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 최상위 역할에 배정된 사용자가 실행하지 않은 경우가 존재하게 된다. 은행 업무를 예로 들어보면 지점장은 예·출금 업무를 담당하는 여직원보다 상위의 역할을 갖지만 여직원이 하는 예·출금업무는 수행하지 않는다. 이런 문제점의 해결책으로 고유 역할(private role)을 통한 권한 상속 제한이 있었는데, 단지 권한의 상속을 방지하는 기능만을 제공할 뿐이었다. 본 논문에서는 하나의 역할을 권한 상속 정도에 따라 여러 개 부역할(sub role)로 구분하여 조직에서 정의된 하나의 역할을 기능별, 상속 정도별로 세분화하였고 권한 상속을 제한 하여 최소권한의 원칙을 지킬 수 있다[3].

II. 본문

1. 관련된 역할계층 연구

역할은 조직의 특성과 그 역할을 수행하는 사용자의 책임과 자격에 따라 배정되는데, 접근권한은 하위역할이 상위역할에 상속되어진다. 역할간의 접근권한의 상속되는 방향을 (→)으로 표현할 때, 역할계층에서 부분순서 관계에 있는 역할은

접근권한 상속에 따라 그림 1과 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 구분할 수 있다[3].

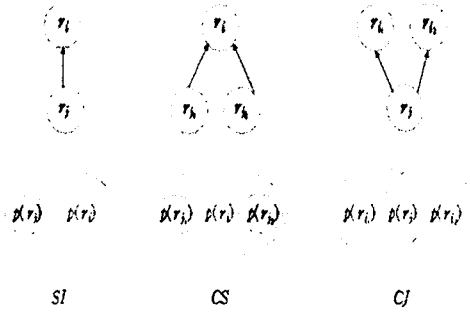


그림 1: 역할의 구성.

세 가지 유형모두 상위역할이 하위역할의 접근권한을 모두 상속받게 되는데, 이것은 상속의 원리를 준수하나 상위역할에 권한이 집중되어 권한 남용의 문제점이 발생한다. 이에 대한 해결책으로 고유 역할(private role)을 이용하게 되는데, 이는 권한의 상속만을 방지하는 기능만을 제공할 뿐이다[3]. 권한 상속의 정도(degree of inheritance)를 지정하지 못하는 단점이 있다. 특성별(조직구조, 권한상속)로 별도의 계층구조를 두어 여러 개의 계층을 정의할 경우 다수의 계층을 관리하는데 문제점이 있다[2].

2. 제안한 역할 계층 모델

본 장에서는 2장에서 제시된 문제점 해결을 위해 역할계층상에 있는 상속의 원리를 유지하면서, 권한 남용을 방지할 수 있는 방안으로 역할계층 위에서 접근권한의 상속을 제한하는 방법을 제시한다. 역할계층 위에서 역할에 배정된 접근권한의 속성에 따라 전체 상속, 부분 상속, 그리고 상속되지 않는 고유역할로 분류할 수 있으며 그림 2로 제시한다.

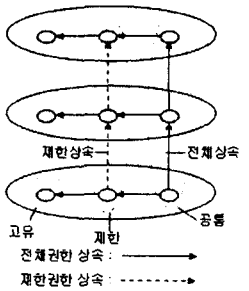


그림 2: 역할계층에서 역할의 재분류

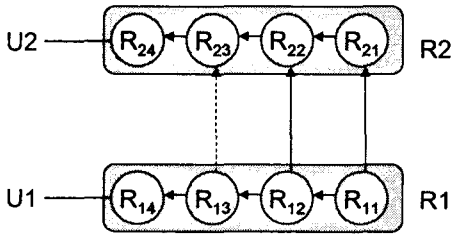
역할을 부역할(sub role)로 나누어 기업에서 흔히 볼 수 있는 역할계층에 적용해 본다. 먼저 역할에 배정된 권한들의 특징에 따라 조직 공통(Common), 부서 공통(Department), 상속 제한(Restricted Inheritance), 고유 역할(Private role)로 나누는 기준은 표 1에서 제시한다.

표 1: 기업의 조직에 맞는 역할분류 기준.

부역할의 종류	부역할에 배정된 권한 특징
조직공통 (Common) 전체 상속	조직내의 모든 구성원에게 허가된 권한 상위역할의 권한은 하위역할에 배정된 권한을 포함(proper superset)
부서공통 (Department) 전체 상속	부서에 속한 구성원들에게만 허가된 권한 상위역할은 하위 역할의 권한을 포함(proper superset)
상속 제한 (Restricted Inheritance) 제한 상속	하위역할에 속한 권한이 지정된 상위 역할까지만 상속 역할 분석과 설계 과정에서 상속이 제한되는 권한에 대한 조사 필요 역할간에 제한적 상속만이 이루어짐
역할 한정 (private role) 고유 역할	상위역할로 권한 상속이 이루어지지 않는 권한들 상위역할이 존재하지 않는 권한들

표 1에 제시된 기준으로 기업환경에 맞게 역할을 분류한 것을 그림 3에서 보여준다.

그림 3에서 역할 R1과 R2는 같은 계층구조 위에 있는데 $R_{11}\rightarrow R_{21}$, $R_{12}\rightarrow R_{22}$는 각각 조직공통과 부서공통의 역할계층으로서 하위역할에 배정된 모든 권한이 상위역할에 상속된다. $R_{13}\cdots\rightarrow R_{23}$은 상속



R_{x1}: 조직 공통 역할
R_{x2}: 부서 공통 역할
R_{x3}: 상속 제한 역할
R_{x4}: 고유 역할(private role)

그림 3: 제안된 역할 계층(R1, R2).

을 제한하는 역할계층으로서 제한적으로 권한 상속이 일어난다. 또한 R_{14}와R_{24}는 고유 역할(private role)로서 상위역할에 상속관계가 없는 자신의 고유의 역할이다. 결과적으로 R_{x1},R_{x2},R_{x3} ,R_{x4} 에도 각각 단일 역할 계층구조(Intra-Role Role Hierarchy)가 존재하고 $R_{x4}\geq R_{x3}\geq R_{x2}\geq R_{x1}$의 역할계층이 나타난다. 사용자는 고유 역할에 배정되어 그 하위의 역할인 조직공통, 부서 공통 상속 제한, 고유 역할에 배정된 모든 권한 실행이 가능하게 된다. 이렇게 하나의 역할을 세분화하였을 때 그 안에서도 역할계층이 나타남을 알 수

있다.

그림 3은 하나의 역할을 권한 상속 정도에 따라서 여러 개의 부역할(sub role)로 구분하여 조직에서 정의된 하나의 역할을 기능별, 상속 정도별로 세분화하였다 .또한 조직 구조를 유지하면서 권한 상속을 제한하는 역할계층 구조이기도 하다. 이렇게 제안된 역할 계층구조 위에 새로운 역할을 추가하는 경우 이미 작성된 조직 공통, 부서 공통역할을 활용하고, 상속 제한이 역할 한정만을 고려하므로 추가 작업이 용이한 장점이 있다.

1) 부역할(sub role)간 계층구조

이 절에서는 개개의 부역할(sub role)사이에서 관계된 계층구조의 종류와 특징에 대해서 분석한다.

가. 권한상속 제한 역할간 계층구조

상속 제한 계층구조는 제한적으로 권한 상속이 일어나는 역할을 기술한다(단, 권한 상속에 대한 명시적 명세가 빠져있으면 권한 상속이 이루어지지 않는다).

하위 역할에 배정된 권한이 모든 상위역할에 상속되지 않는 특징이 있다.

나. 조직 공통, 부서 공통 역할간 계층구조

기존 역할 계층과 동일한 구조를 갖게된다. 즉, 하위의 모든 권한이 자신의 모든 상위 역할에게 상속되게 된다.

부서공통 역할계층과 상속제한 역할계층간 상속특성에 대해서 그림 4를 바탕으로 부서공통 역할계층과 상속제한 역할계층간 상속 특성에 대해 분석한다.

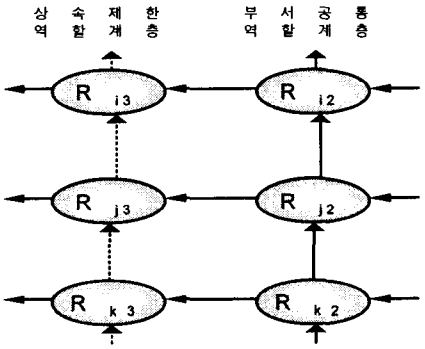


그림 4: 상속제한역할과 부서공통 역할계층.

부서공통 하위역할에서 상속제한 상위역할로의 상속은, 예를 들어 $R_{k3} \rightarrow R_{j3}$라는 역할계층구조가 있다면 $R_{k2} \rightarrow R_{j3}$: $R_{k2} \rightarrow R_{j2}$(부서공통), $R_{j2} \rightarrow R_{j3}$(단일역할계층)이므로 가능하다.

상속제한 하위역할에서 부서공통 상위 역할로의 상속은, 예를 들어 $R_{k3} \rightarrow R_{j2}$라고 하자. $R_{k3} \rightarrow R_{j2}$인 계층관계가 있다면 R_{k3}의 모든 권한이 부서공통 역할계층에서 R_{j2}의 모든 상위 역할에 상속되고 부서공통 역할계층에서 R_{j2}의 모든 상위 역할에 배정된 권한은 각 역할의 상속제한 역할계층에 상속되기 때문에 이는 결과적으로 R_{k3}의 권한이 상속제한 역할계층에서 R_{k3}의 모든 상위 역할에 상속됨을 의미하게 된다. 이 경우는 상속제한 역할계층 정의에 위배된다.

3. 상속제한 역할계층

이번 장에서는 상속 역할계층에 포함된 역할의 상속범위를 지정 명세하는 것으로 상속 범위에 대한 집합은 다음과 같은 범위를 갖는다.

R U seq R

R은 역할집합, seq R은 상속 역할의 패스(path)를 말한다.상속제한 역할계층에 대한 분석을 그림 5에 제시된 (a)-(e)를 가지고 실명하겠다.

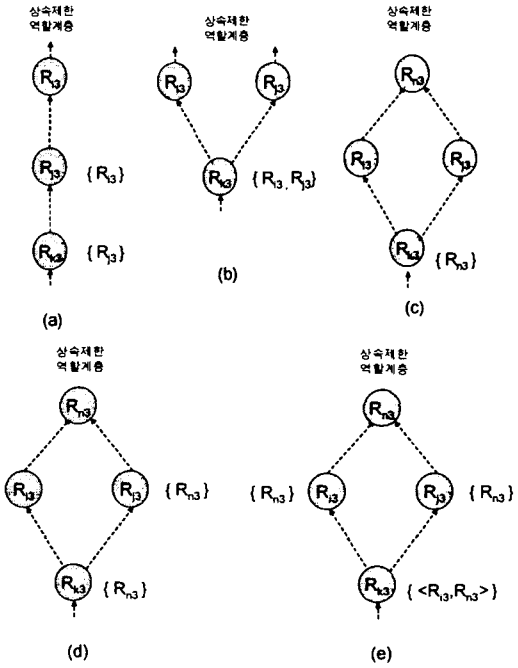


그림 5: 상속 역할 계층의 예

<경우 (a)>

- R_{k3}에 배정된 권한은 R_{j3}까지만 상속
- R_{j3}에 배정된 권한은 R_{i3}까지만 상속
- R_{k3}에 배정된 권한은 R_{i3}에 의해 상속되지 않음

<경우 (b)>

- R_{k3}에 배정된 권한은 R_{i3}, R_{j3}까지만 상속

<경우 (c)>

- R_{k3}에 배정된 권한은 R_{i3}, R_{j3} 그리고 R_{n3}까지만 상속

<경우 (d)>

- R_{k3}의 권한은 R_{i3}, R_{j3}, 그리고 R_{n3}까지 상속
- R_{j3}의 권한은 R_{n3}까지 상속되지만 R_{i3}의 권한은 R_{n3}로 상속되지 않음

<경우 (c)>

- R_{k3}의 권한이 R_{i3}와 R_{n3}까지 상속
- R_{k3}의 권한은 R_{j3}로 상속되지 않음
- 즉, R_{k3}의 권한이 마름모 형태의 한 쪽 편(path)만을 따라 권한이 상속
- R_{j3}의 권한은 R_{n3}로 상속

제안된 실계 방법론을 바탕으로 구성된 역할 계층구조는 다음과 같은 장점이 있다.

첫째, 조직 구조를 반영하는 계층 구조에 권한 상속 기능 추가, 둘째, 일반적인 기업환경에서 권한상속 관점에서 역할의 종류 분류: 조직 공통, 부서 공통, 상속 , 고유 역할, 셋째, 기존 역할계층에서 문제점인 최소권한 원칙 위배가능을 권한 상속 을 통한 해결 방안을 제시하였다.

이 방법론의 문제점으로는 기존 역할의 한 역할이 4종류의 세부 역할로 세분화되면서 발생하는 역할의 개수 증가가 문제점이 될 수 있다.

Ⅲ. 결론 및 향후 연구방향

기업 환경에서 조직 구조를 유지하면서 권한 상속 하는 역할 계층구조를 제시하여 역할 계층에서 상위역할에 배정된 사용자에게 불필요한 권한 실행 허가를 하였다. 또한 조직에서 정의된 하나의 역할을 상속 정도에 따라 4개의 부역할(sub role)로 구분하고 권한 상속의 정도(degree of inheritance)를 지정하여 필요한 계층까지만 역할이 상속되도록 하였다. 향후 연구방향으로는 제안된 역할계층에서 정적, 동적 의무분리를 추가 하고 제안된 모델에 대한 정형적 기술을 통하여 보다 안전한 역할계층모델 및 세션을 통한 역할계층에서 상속된 접근권한과 계층구조 위에서 접근권한의 차이에 대한 연구를 하고자 한다. 끝으로 이와 같은 방법론에서 잘 정의된 부역할(sub role) 을 이용하여 역할위임모델에 대한 연구가 필요하다.

참고문헌

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

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

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