다중 응용 환경에서 통합 접근통제가 가능한 그룹-역할기반 접근통제 시스템에 관한 연구

권태형✔, 남길현
국방대학교 전산정보학과
rokafa43@lycos.co.kr

A Study on Group-Role Based Access Control System for the Integrated Access Control in Muti-Applicational Computing Environment

Tae-Hyung Kwon✔, Kil-Hyun Nam
Dept. of Computer & Information Science, Korea National Denfense University

요 약

역할기반 접근통제(RBAC)는 사용자의 역할에 기반을 둔 접근통제 방법으로 Ravi S. Sandhu가 제안한 기본 모델 이후로 다양한 모델들이 제안되어졌다. 하지만, 이 모델들은 다중 응용 환경에 적합한 통합접근통제 시스템 설계에 실제 적용하기 위해서는 보완되어야 할 점이 많다. 본 논문에서는 이 모델들의 주요 구성요소를 근간으로 하여 그룹-역할기반접근통제 시스템을 제안하고자 한다. 제안된 시스템은 사용자와 역할지정에 그룹 계층을 사용하고, 조직내의 직위와 직능을 바탕으로 역할 계층을 만들며, 만들어진 역할 계층을 통한 허가의 상속을 허용한다. 또한, 시스템이 가진 접근통제 데이터베이스를 세가지 부분으로 나누어 관리하게 함으로써, 조직의 접근통제 정책의 투명성을 보장한다.

1. 서 론

조직의 컴퓨팅 환경은 초기의 메임 프레임 환경에서 클라이언트/서버 환경을 거쳐, 인트라넷 환경으로 변화되고 있고, 그 변화 과정에서 응용 체계들은 다양한 환경에서 혼재 되어 운영된다. 이런 컴퓨팅 환경에서 가장 시급한 문제중에 하나는 다중 응용 환경에서의 사용자들의 접근통제라고 할 수 있다. 이 같은 환경 하에서 통합되지 않은 접근통제는 관리자에게 상당한 업무 부하를 주고, 많은 관리 실수를 야기할 수 있다. 또 조직구조의 변동사항이나 조직원의 입사, 퇴사, 승진, 징계 및 휴직 등에 유연성 있게 대응하기란 거의 불가능하다고 볼 수 있고, 이런 상황 하에 파생된 휴면 계정이라든지, 권한 과다 등의 문제는 보안사고의 주요한 원인이 될 수 있다. 따라서, 다중 응용체계 환경에서 통합 접근통제를 가능하게 해주는 솔루션은 날로 그 중요성이 증가하고 있다. 현재 통합인증/권한관리 시스템(Single Sign-On, Privilege Management Infrastructure 등)이 제품화되고 있는 실정이지만, 통합인증에 초점이 맞추어져 있고, 역할에 의한 체계적인 허가의 관리는 미흡하다고 볼 수 있다.

본 논문에서는 역할기반접근통제(RBAC) 모델들의 주요한 장점들인 역할을 이용한 사용자와 허가 관리의 유연성을 접근통제 시스템에 반영하고 발전시켜서, 조직의 접근통제 정책을 쉽게 반영할 수 있고, 또한 관리할 수 있는 다중 응용 환경에 적합한 통합 접근통제 시스템을 제안하고자 한다.

2. 관련 연구

2.1 역할기반 접근통제 모델

RBAC(Role Based Access Control)의 중요 개념은 사용자(user)와 역할(role) 및 역할과 허가(permission)의 연관관계에 의해 접근통제가 표현된다는 것이다 [1][2][3]. 이것은 사용자나 허가의 잦은 변동에 비해 역할은 조직 내에서의 다양한 직무(job functions)에 근거하여 작성되므로 비교적 고정적이기 때문에 접근통제에 유연성을 줄 수 있다는 개념에서 출발한다[4][5].

2.2 접근통제에 있어서의 역할 계층

역할은 허가의 집합으로 볼 수 있다. 역할 계층 내에서의 상위 역할은 하위 역할이 가진 허가를 포함한다[6]. 따라서, 역할 계층 내에서의 역할의 위치는 허가를 결정하는 중요한 요소이다. 그러므로, 역할 계층은 조직의 접근통제 원칙(직무분리, 집중배제 및 위임, 관리와 사후조사 등)에 반하지 않게 설계되어 져야 한다[7].

2.3 역할기반 접근통제와 그룹 계층

사용자를 역할에 지정하는 문제에 그룹 계층을 적용함으로써 관리상의 이점을 얻을 수 있다[8]. 사용자가 속한 그룹이 역할에 지정되면, 사용자는 해당 역할이 가진 허가를 사용할 수 있고 또한, 그룹 계층에 의해 허가를 상속 할 수 있다.

2.4 유럽은행의 역할기반 접근통제 시스템

유럽은행이 사용하고 있는 FUB 시스템은 수만 명의 종업원을 사용자로 하며, 50여 개가 넘는 다양한 응용체계 권한들을 사용자들에게 연결시켜주는 통합 접근통제 시스템이다[9]. FUB 시스템은 개별 사용자를 직접 응용체계 수준의 접근 권한에 지정하지 않고, 역할에 의해 응용체계의 권한들을 획득할 수 있게 한다. 또한, FUB시스템이 가진 보안 프로파일을 세가지로 분리하여 서로 다른 부서에서 관리함으로써, 접근통제의 투명성을 보장한다. FUB시스템의 기본구조는 통합 접근통제의 좋은 예로 본 논문에서 제안된 시스템에서도 그 구조를 활용한다.

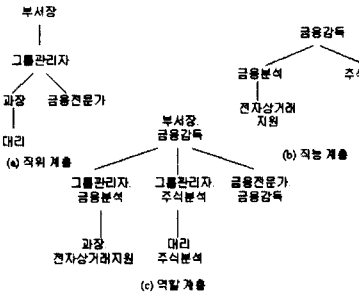
3. 그룹-역할기반 접근통제(G-RBAC) 데이터 모델

3.1 역할 계층에 의한 허가 상속

역할 계층은 직위(position) 계층과 직능(job function) 계층을 바탕으로 구성된다.

[정의 1] 역할 계층에 의한 허가의 상속

- 역할 계층은 트리 구조임
- 역할(y)가 역할(x)의 직계 존속. 즉, 역할(x)>역할(y) ⇔ (역할(x).직능>역할(y).직능 ∧ 역할(x).직위=역할(y).직위) ∨ (역할(x).직능=역할(y).직능 ∧ 역할(x).직위>역할(y).직위) ∨ (역할(x).직능>역할(y).직능 ∧ 역할(x).직위>역할(y).직위)
- 역할(x)>역할(y) 이면, 역할(x)⊃역할(y)이다. 그러므로, 역할(x)는 역할(y)의 허가를 상속한다.



[그림 1] 역할 계층 작성

[그림 1]은 직위 계층과 직능 계층을 바탕으로 만들어진 역할 계층의 한 예이다. 직위 계층 상의 상급자라고 해서 반드시 역할 계층 상위 위치에 있는 것은 아니다. 역할 계층은 직위와 직능 계층이 함께 고려된 상태에서 결정된다.

[표 1] 역할 계층에 의한 허가 상속

역할	허가		
	응용체계	접근권한	상속접근권한
대리.주식분석	금융시장분석	1.2.3.4	
	주식동향분석	1.2.3.4	
	거래실적분석	1.2.3	
그룹관리자.주식분석	금융시장분석	5.6.7	1.2.3.4
	주식동향분석	5	1.2.3.4
	거래실적분석		1.2.3
부서장.금융감독	금융시장분석	8	1.2.3.4.5.6.7
	주식동향분석	6.7	1.2.3.4.5
	거래실적분석	4.5.6	1.2.3.4
	금융상품관리	1.2.3.4	

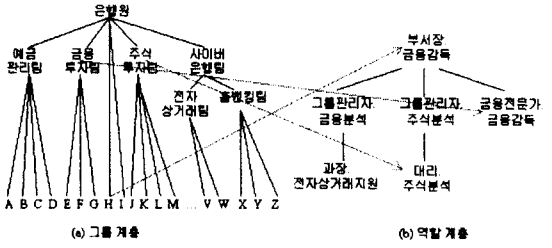
[표 1]은 [그림 1]에서 표현된 역할 계층에 의한 허가의 상속을 표현한 것이다. 허가들의 상속은 허가 자체의 상속 뿐만 아니라, 허가가 가진 응용체계의 세부 접근 권한들도 포함한다.

3.2 그룹-역할 계층에 의한 허가 상속

조직 내의 기능 단위로 그룹 계층을 작성하여, 접근통제에 접목시킨다면, 사용자를 역할에 곧바로 지정하지 않고 그룹핑해서 지정하는 편리함을 얻을 수 있다. 이것은, 반복작업(같은 역할을 가진 사용자들의 지정)에서 오는 관리실수를 제거할 수 있고, 사용자를 역할에 임의로 지정하지 못하게 하는 제약으로서도 활용될 수 있다.

[정의 2] 그룹 계층의 허가 상속

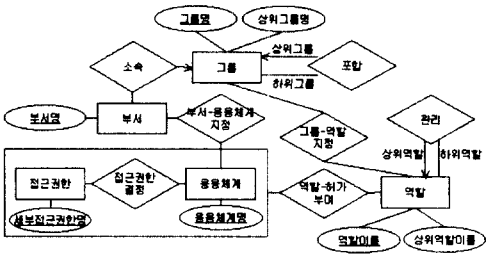
- 그룹 계층은 트리 구조임
- 그룹(y)가 그룹(x)의 직계 존속. 즉, 그룹(x)>그룹(y) 이면 그룹(x)⊃그룹(y)이며, 그룹(y)는 그룹(x)가 갖고 있는 역할을 공유한다.



[그림 2] 역할에 그룹 지정

[그림 2]는 그룹-역할 계층의 지정관계를 표현하고 있다. [(a)그룹 계층]은 [정의 2]를 만족하며, 알파벳으로 표현된 것은 개별 사용자를 말한다. [(a)그룹계층]에서 'E'는 금융투자팀의 멤버이기도 하고, 은행원의 멤버이기도 하다. 따라서 금융투자팀이 갖고 있는 역할 '금융전문가.금융감독' 을 갖는다.

3.3 G-RBAC 데이터 모델

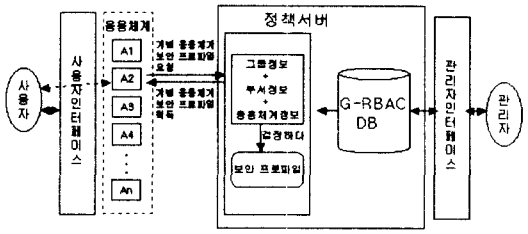


[그림 3] E-R Diagram으로 표현한 G-RBAC 데이터 모델

[그림 3]은 [정의1]과 [정의2]를 바탕으로 만들어진 G-RBAC 데이터 모델이다. [그림 3]에서 그룹과 역할 엔티티는 각각이 상위 노드의 정보를 유지함으로써 그룹과 역할 계층을 유지한다. 추가로, 제안된 데이터 모델에는 해당 부서가 사용할 수 있는 응용체계를 미리 지정함으로써, 과도한 허가의 사용을 근원적으로 차단할 수 있다.

4. 그룹-역할기반 접근통제 시스템 설계

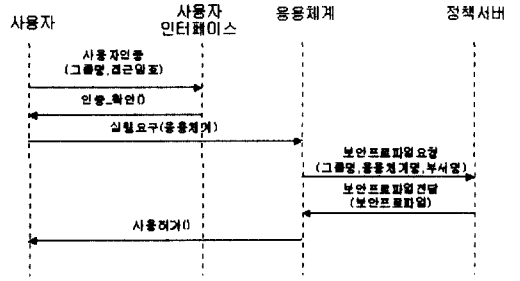
4.1 모델 설계



[그림 4] G-RBAC 시스템 구조

[그림 4]는 G-RBAC 시스템의 구조이다. 제안된 시스템은 클라이언트/서버 구조로 구성된다. 서버 단에는 정책서버가 위치하고, 클라이언트 단에는 통합 인증하고 해당 응

체계로 연결시켜주는 사용자인터페이스와 G-RBAC DB를 관리하는 관리자인터페이스가 위치한다. 정책서버가 가진 G-RBAC DB는 3.3장에서 설명한 데이터 모델을 바탕으로 구성된다. 정책서버는 사용자의 요청에 의해 보안 프로파일을 개별 응용체계에 전달하고, 사용자는 자신의 책임과 권한에 합당한 응용체계내의 권한를 사용할 수 있게 된다. [그림 5]는 접근통제가 이루어지는 시나리오를 간단한 예로 설명하고 있다.

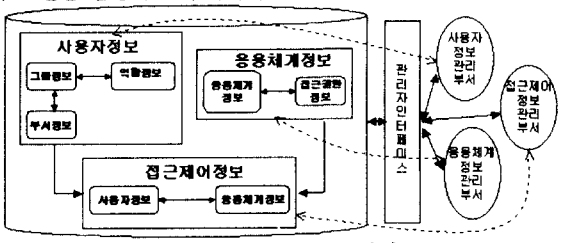


[그림 5] 접근통제 시나리오

[그림 4]와 [그림 5]에 나타난 보안프로파일은 G-RBAC DB에서 추출되며, 그룹정보, 부서정보, 응용체계정보 및 허가리스트를 가지고 있으며, 사전에 정의된 접근통제 정책을 반영한다.

4.2 G-RBAC DB 관리

본 논문에서 제안된 시스템은 G-RBAC DB 관리를 [그림 6]과 같이 세 부분으로 분리한다. 사용자정보는 조직의 인사업무를 담당하는 부서에서, 응용체계정보는 개별 응용시스템을 개발/유지보수하는 부서에서 그리고, 핵심인 접근제어정보는 조직의 보안을 담당하는 부서에서 관할한다.



[그림 6] G-RBAC DB 관리

4.3 시스템 비교

[표 2] 시스템 특징 비교

대상시스템 / 특성	FUB 시스템	G-RBAC 시스템
접근통제대상	• 사용자와 역할 • 역할과 허가	• 사용자와 그룹 • 그룹과 역할 • 역할과 허가
역할적용대상	• 사용자	• 사용자, 그룹
상속	• 허용하지 않음	• 역할상속(by그룹계층) • 허가상속(by역할계층)
장점	• 개별 사용자에 대한 역할지정으로 세부적인 허가 지정가능	• 그룹에 의한 역할 지정 • 역할 계층에 의한 허가 상속
단점	• 개별 사용자를 대상으로 하므로 복잡함 • 관리자 독단에 의한 사용자 역할 지정 가능성	• 그룹 및 역할계층에 의한 허가의 상속으로 과도한 허가 가능성

용

5. 결론

본 논문의 목적은 다중 응용체계 환경에 적합한 역할기반 접근통제 시스템을 설계하는 것이다. 역할기반접근통제 시스템에서 고려되어야 하는 문제들은 여러 가지가 있지만, 가장 중요한 것은 정책서버가 갖고 있는 보안프로파일을 어떻게 생성하고, 관리할 것인가 하는 문제이다. 본 논문에서는 유럽은행의 FUB시스템을 기본 모델로 하여, 그룹과 허가 상속 개념을 추가하여 보다 진보된 형태의 G-RBAC 시스템을 제안하였다.

접근통제 시스템의 세부 구현 사항들은 조직의 보안사항이 될 수 있기 때문에 쉽게 접하기가 어렵다. 어떤 모델을 선택하여 접근통제 시스템을 구현하는가 하는 문제도 중요한 것이지만, 실제 시스템이 어떻게 관리되어지고 있고, 무슨 문제들이 발생하는가를 아는 것도 중요한 문제라고 생각된다. 제안된 시스템도 몇 가지 보강되어져야 하는 난제가 있다. 사용자-그룹, 그룹-역할 및 역할-허가 지정에 있어서의 제약조건(constraint)문제와, 그룹이나 역할 계층에 의한 허가의 집중문제, 그리고, 사용자가 동시에 가져서는 않되는 상호배타적인 역할 문제 등이 그것이다.

참고문헌

[1] Ravi S. Sandhu, "Role Based Access Control," George Mason University, September 17, 1997

[2] Ravi S. Sandhu, " The NIST Model for Role-based Access Control: Towards a Unified Standard," The proceedings of 5th ACM workshop on RBAC, pp 47-63, 2000.

[3] E. Lupu, " A policy based role framework for access control," The proceedings of 1st ACM workshop on RBAC, 1995.

[4] Pete Epstein, " Towards a UML based approach to role engineering," The proceedings of 4th ACM workshop on RBAC, pp 135-143, 1999.

[5] Haio Roeckle, " Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization," The proceedings of 5th ACM workshop on RBAC, pp 103-110, 2000.

[6] Jonathan D. Moffett, " The uses of role hierarchies in access control," The proceedings of 4th ACM workshop on RBAC, pp 153-160, 1999.

[7] Jonathan D. Moffett, " Control principles and role hierarchies," The proceedings of 3rd ACM workshop on RBAC, pp 63 - 69, 1998.

[8] Sylvia Osborn, " Modeling users in role-based access control," The proceedings of 5th ACM workshop on RBAC, pp 31-37, 2000.

[9] Andreas Schaad, " The role-based access control system of a European bank: a case study and discussion," The proceedings of 6th ACM Symposium on Access control models and technologies, pp 3-9, 2001.