CSCW환경에서의 Work개념을 수용한 RBAC모델에 관한 연구

심완보

충청대학교 컴퓨터학부

Study on the RBAC Model including the work concept in the CSCW environment

Won-Bo Shim

Division of Computer, ChungCheong College

요 약

앞으로 전산 시스템에서는 독자적인 사용자의 전산 시스템 이용보다는 조직내의 다수의 작업 참여자 간의 의사소통과 정보의 교환 및 공유가 원활히 이루어지도록 할 수 있는 시스템의 지원이 필요하게 되었다. 이러한 전산환경을 CSCW(Computer Supported Cooperative Work)환경이라고 하며 많은 구성원이 공통된 자원을 공유함으로 해서 발생할 수 있는 보안 문제가 발생하게 된다.

이 문제를 해결하기 위한 방안으로 최근 다수의 사용자가 공유자원을 사용하는데 있어 발생할 수 있는 관리의 복잡성을 해결하기 위해 RBAC(Role Based Access Control) 개념이 연구되고 있다.

그러나 CSCW환경과 같이 Work개념이 중요한 환경에서는 기존의 RBAC개념만으로는 공유자원의 접근제어문제 해결에 어려움이 있어 본 논문에서는 Work개념을 RBAC모델에 도입한 CSCW환경 하에서의 RBAC 모델을 제시해 보고자 한다.

1. 서론

컴퓨터 지원 협력작업이란 다수의 작업 참여자 간의 의사 소통과 정보의 교환 및 공유가 원활히 이루어지도록 하여 공동작업을 돕는 컴퓨터 기술을 통칭한다.

협력작업에 있어서 다양한 사용자의 공동 작업을 지원하기 위해서는 많은 사항을 고려해야 하며 자원접근 및 작업의 편이성을 위한 고려사항으로는 다음과 같은 것들이 있다.

1) 작업 참가자는 작업의 상세한 절차보다는 작업의 개요만을 지정할 수 있어야 한다.

2) 동시에 복수개의 작업에 관여 할 수 있어야 하며 작업의 우선 순위에 따라 처리할 수 있어야 한다.

3) 트랜잭션의 개념을 지원하여 일련의 여러 하위 작업을 한 개의 상위작업으로 처리할 수 있어야 한다.

4) 인가되지 않은 다른 참여자로부터 작업환경과 데이터를 보호할 수 있어야 한다.

그러나 이러한 CSCW환경 하에서의 공유자원을 관리하는 방법으로 RBAC 모델을 사용하고자 할 때 기존의 RBAC 모델로는 업무의 동적인 측면들을 잘 수용할 수 없다.

이에 본 논문에서는 업무를 수행하는 사용자의 시간과 장소에 따른 역할의 동적인 변화를 수용할 수 있는 Work개념을 수용한 역할기반 접근제어 모델을 제시 하고자 한다.

2. RBAC(Role Based Access Control)의 이해

2.1 RBAC의 기본 개념

RBAC의 중심적인 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 아이디어는 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도 역할의 변경을 쉽게 할 수 있다.

RBAC 모델의 개념은 다음과 같이 잘 알려진 세가지 보안 원리를 지원한다..

- 최소 권한 원칙(least privilege principle) : 역할 계층성을 이용하여 작업에 꼭 필요한 최소한의 허가 사항만을 역할에 배정하는 정책이다.
- 임무 분리(separation of duty) : 정보의 무결성을 침해하는 사기 행위나 부정 수단을 유발 할 수 있는 작업은 상호 감시적인 역할로 지정하여 임무를 분리시켜 수행한다.
- 데이타 추상화(data abstraction) : 전형적인 운영체제나 응용시스템에서 사용되어졌던 데이타를 처리하는 read, write, execute 등의 연산 대신에 다양한 기능을 수행할 수 있고 명령어를 추상화시키는 상업적인 처리명령어 credit(입금), debit(출금), transfer(이체), create account(계좌개설), delete account(계좌해지)등을 지원한다.

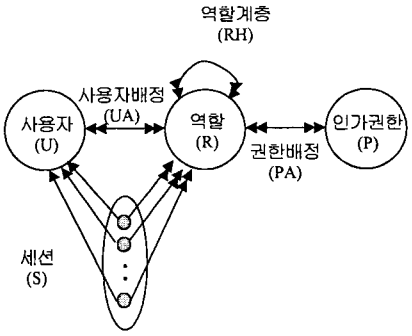
2.2 RBAC의 기본 모델

그림 1은 RBAC의 기본 모델을 보여준다. RBAC의 기본 모델은 사용자(U: user), 역할(R: role), 인가권한(P: permission), 세션(S: session)으로 구성되어 있다.

사용자와 역할 : 모델의 간략화를 위해서 사용자는 사람을, 역할은 역할에 부여된 책임과 권한을 기술하는 조직내의 업무 기능의 이름으로 간주한다. 사용자는 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체로서 한 사용자는 한 명의 사람에 대응된다. 역할은 접근제어 정책을 구현하는 중요한 의미적 구조이다.

RBAC 시스템에서는 시스템 관리자가 회사나 조직의 업무 기능에 따라 역할을 생성하고 역할에 권한을 부여한다. 역할 계층(role hierarchy)은 관련성이 있는 역할들간의 부분순서 관계로서 정의되며 기업의 권한과 책임의 체계와 매우 유사하여 기업의 권한체계를 모델링하는데 매우 적합하다.

그림 1. RBAC의 기본 모델



인가권한(permission) : 인가권한은 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(예 : read, write, update)의 승인을 나타낸다. RBAC에서의 인가권한은 권한허가(authorization), 접근권리(access right), 권한(privilege)과 같은 의미를 갖는다. 여기서 객체는 기업 또는 조직내의 정보시스템을 구성하고 있는 자료나 시스템 자원을 말한다. 인가권한은 네트워크 수준으로부터 특정 레코드의 특정 필드에 대한 접근 단위에 이르기까지 다양한 레벨, 다양한 범위로 주어질 수 있다.

세션(session) : 사용자는 시스템에 로그인등을 통해 그들이 가진 역할의 부분집합을 활성화할 때 세션을 형성한다. 각 세션은 하나의 사용자와 여러 개의 권한을 매핑 한다. 그림 1에서 이중 화살표는 다중 역할이 동시에 활성화한다는 것을 말한다. 사용자에게 사용 가능한 권한은 그러한 세션에 활성화된 모든 역할이 가진 권한의 합집합이다. 각 세션은 그림 1에서 보듯이 단일 화살표에 의해 지시되는 단일 사용자와 관련된다. 이러한 관계는 세션이 존속하는 동안 지속된다.

사용자 배정(user assignment)과 인가권한 배정(permission assignment) : 사용자 배정과 인가권한 배정은 다대다 관계이며 RBAC 모델에서 매우 중요한 구성요소이다. RBAC의 특징중의 하나는 사용자가 정보 객체들에 대해서 실행할 수 있는 연산들을 직접 사용자에게 부여하는 대신 조직의 업무 수행에 필요한 역할에 배정하고(인가권한 배정), 사용자는 해당

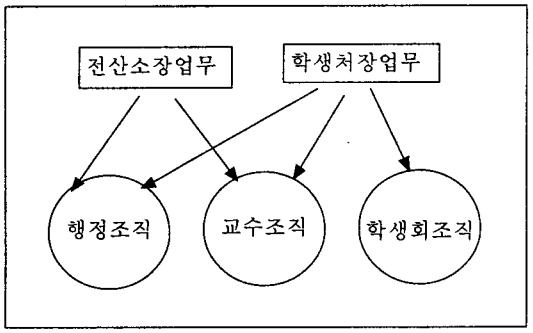
역할의 구성원이 됨으로써(사용자 배정) 정보 객체에 대해 지원하는 연산을 수행하도록 하는 것이다. 이러한 방법은 사용자와 정보 객체수가 많은 일반 기업 환경에서 권한의 관리를 매우 용이하게 수행할 수 있는 장점을 제공한다.

3. CSCW환경에서의 역할

위에서 설명한 RBAC개념을 CSCW환경 하에 적용시키기 위해서는 기존의 역할 개념에 변화가 필요하게 된다.

복합적인 역할을 수행하여야할 CSCW환경 하에서는 단일한 역할 구조로는 모든 업무를 정의하기 어렵다. 또한 사용자는 자신의 업무를 적절히 수행하기 위해서는 복수개의 역할을 선택해야 하는 경우가 많다.

그림2. 업무의 복합화



예를 들어 그림2에서와 같이 사용자가 전산소장업무를 수행하기 위해서는 행정조직상의 역할도 필요하고 교수조직상의 역할도 필요하게 된다.

그러나 각각의 조직은 상하 관계를 같이 묶어서 규정하기 어려운 독립적인 별도의 조직체계이므로 하나의 역할 구조로 통합되기 어렵게 된다. 이러한 구조에서 사용자는 자신이 수행해야 하는 업무만을 선택하는 것으로 자신의 업무를 원활히 수행할 수 있게 해준다면 사용자는 자신의 상황에 맞는 적절한 역할을 그때 그때 부여받아 업무를 원활히 수행해 나갈 수 있을 것이다.

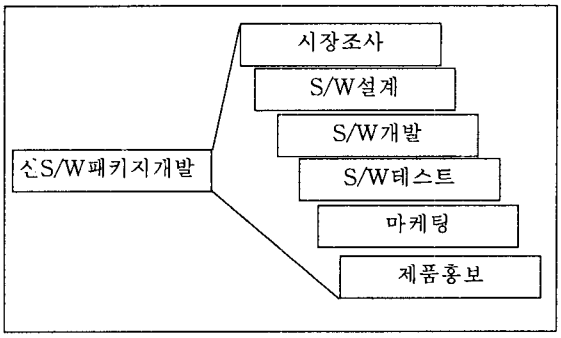
다음은 CSCW환경에서의 역할에 고려해야할 사항들이다.

1) 사용자의 역할이 세션이 성립된 후에 시간과 장소에 따라 동적으로 바뀔 수 있다.
2) 다양한 형태의 정책사용이 필요하다.
3) 동적으로 변할 수 있는 사용자의 역할이 그때 그때의 역할 선택으로 인한 번거로움이 제거되어야 한다.
4) 역할 개념보다 더 광범위한 Work개념 도입이 필요하다.

예를 들면 하나의 업무는 몇 개의 하부업무인 Task들로 구성되어 있다.

신 소프트웨어 패키지를 개발하는 업무를 수행한다고 할 때 이 업무를 완수하기 위해서는 시장조사, S/W설계, S/W개발, S/W테스트, 마케팅, 제품홍보 등의 Task들을 수행하여야 한다.

그림3. Work과 Task의 구성



그런데 각 Task들을 수행하기 위해서는 해당 Task를 수행하기 위한 권한인 역할권한을 가져야 하는데 이러한 역할 권한이 여러 개의 역할구조에 걸쳐 존재할 수 있어 기존의 단일 역할구조로는 해결할 수 없게 된다.

그림4는 Work개념을 수용한 RBAC 모델이다.

이 모델을 사용한다면 다음과 같은 장점을 얻을 수 있다.

1) 여러 개의 실제에 존재할 수 있는 Role구조를 지원할 수 있다.
2) 사용자는 좀 더 실세계의 업무와 같은 선택을 할 수 있다.
3) 사용자는 한가지 업무를 수행하기 위해 여러 번의 Role을 선택해야하는 번거로움과 부담을 덜 수 있다.

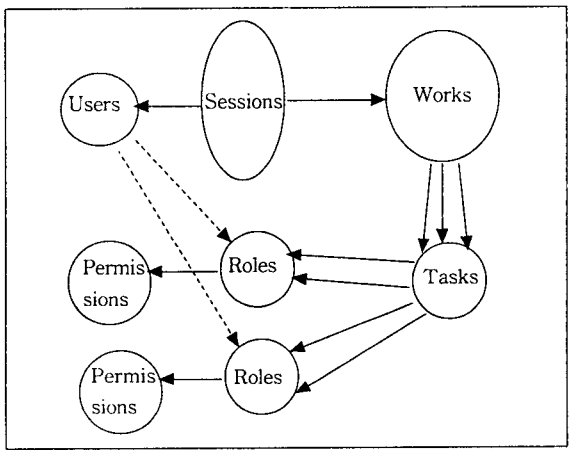
4) 사용자는 다소 까다로운 Role의 개념을 이해하지 않고도 시스템에서 업무를 수행할 수 있다.

5) 기존의 Role의 개념을 수용하여 Integration이 용이하다.

6) 장소나 시간 등의 상황변화에 대해 사용자는 그때 그때 적절하고도 최소한의 권한이 보장되는 Role을 부여받아 업무를 수행해 나갈 수 있다.

7) Work과 Role사이에 있는 Task개념의 도입으로 보다 융통성 있는 관리가 가능하다.

그림4. Work개념의 RBAC모델



4. 결론

CSCW상에서의 공유자원 관리는 최근 기업의 생존을 좌우하는 경쟁력의 핵심 요소로 자리 매김을 하고 있다. CSCW상에서의 공유자원 관리에 있어 가장 큰 문제는 보안이라고 할 수 있다. 보안문제는 지금까지는 주로 외부의 침입자들로부터 시스템을 보호하는 일에 초점이 맞추어져 있었다. 그 결과 내부에 있는 다수의 사용자가 동일한 정보 시스템을 이용하게 될 때 개인, 부서 혹인 기업 차원의 기밀 정보를 효과적이고 안전하게 보호하면서도 사용자에게는 불편을 최소화시키는 보안 문제가 대두되었다. RBAC은 이에 대한 하나의 대안으로 주목받고 있는데 동적으로 사용자의 Role이 변해 나갈 수 있는 CSCW환경을 충분히 수용하는 데는 문제가 있다.

이에 이 논문에서는 RBAC을 CSCW상에서 적용하는데 필요한 모델을 찾기 위해 기존의 RBAC 모델에 Work개념을 도입하고 이들 Work을 Task로 구성시켜 각각의 Task들을 수행하는데 필요한 Role들을 부여하게 하여 사용자는 업무의 선택만으로 다중 역할에 대한 부담이 없이 업무를 원활히 수행할 수 있는 RBAC 모델을 제시해 보았다.

[참고문헌]

1. D. Ferraio, J. Cugini and R. Kuhn, "Role-based Access Control(RBAC): Features and motivations", Proc. of 11th Annual Computer Security Application Conference, (1995).

2. John Barkley, "Managing Role/Permission Relationships Using Object Access Types", NIST., (1998).

3. R. Sandhu and Gail-Joon Ahn, "Group Hierarchies with Decentralized User Assignment in Windows NT", ASTED-CSE, (1998).

4. R. Sandhu, V. Bhamidipati, E. Coyne, S. Ganta, and C. Youman, "The ARBAC97 model for role-based administration of roles : Preliminary description and model", Proc. of the second ACM Wrokshop on rRole-Based Access Control, ACM, (1997).

5. R. Sandhu and V. Bhamidipati, "The URA97 Model for Role-Based User-Role assignment", Proc. of IFIP WG 11.3, (1997).

6. R. Sandhu and Q. Munawer, "The RRA97 Model for Role-Based Administration of Role Hierarchies", ACSAC, (1998).

7. J. F. Barkely, A. V. Cincotta, D. F. Ferraiolo, S. Gavrilla and D. R. Kuhn, "Role Based Access Control For the World Wide Web", 20th NCSC, (1997).

8. R. Sandhu, E. Coyne, H. Feinstein, and C. Younman, "Role-Based Access Control Models", IEEE Computer Magazine Vol. 29, (1996).

9. 오세종, 박석, "역할기반 접근제어에서 기업환경에 적합한 역할계층의 구성에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집 제9권 1호, (1999)

10.송동호, "CSCW기능확장을 위한 검색형 미들웨어와의 통합", 정보과학회지 110호, 1998.7

11. Sejong Oh, Seog Park, "Task-Role Based Access Control(T-RBAC):An Improved Access Control Model for Enterprise Environment", P264 - P273 (2000)

12. Ehud Gudes, "Modeling, Specifying and Implementing Workflow Security in Cyberspace"

13. W.Keith Edwards, "Policies and Roles in Collaborative Applications"