역할기반 접근제어 기반에서의 중복 및 협의에 의한 권한 위임 모델

강병헌[O] 전준철 유기영
경북대학교 컴퓨터공학과
bhkang@tksun.aiit.or.kr[O] jcjeon33@infosec.knu.ac.kr yook@knu.ac.kr

Duplication and Deliberation Delegation Model in Role based Access Control

Byung-Heon Kang[O] Jun-Cheol Jeon Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

역할기반 접근제어(RBAC)는 기업, 정부, 은행 등의 계층적 역할을 구성하는 다양한 조직체계에서 보안관리의 비용이나 복잡성을 줄일 수 있는 접근통제 메커니즘으로 기존의 임의적 접근제어(DAC)나 강제적 접근제어 기능을 포괄하는 접근제어 기법으로 각광 받고 있다. 또한 RBAC은 기업의 관리규칙에서 중요한 부분을 차지하는 위임과 철회 기법을 제공하고 있다. 현재 RBAC에서의 위임 정책은 조직 내에서 발생하는 다양한 상황에 대한 완벽한 위임 모델을 제시하고 있지 못하고 있다. 실제 조직체계에서 위임받은 사용자가 부재일 경우 이는 업무공백으로 이어진다. 그리고 상호 유기적으로 연결되어 있는 업무 또는 중요한 사안에 대한 업무의 경우 사용자 단독 권한 위임은 권한 남용의 소지가 있다. 따라서 본 논문에서는 업무의 공백 최소화와 감시감독 기능의 강화를 위한 중복 권한 위임 모델과 상호공유가 필요한 업무와 중요한 사안의 결정에 적용 가능한 협의에 의한 권한 위임 모델을 제시한다.

1. 서 론

역할기반 접근제어(RBAC)는 네트워크 기반 응용 프로그램의 보안관리 용이성으로 인하여 정부나 기업 등 다양한 조직체계에서 많은 관심을 받고 있는 분야이다. 또한 RBAC은 현재 가장 각광받는 접근제어 기법 중 하나이다. RBAC은 기본적으로 사용자, 역할 그리고 권한으로 구성되어진다. 역할은 조직에서 발생되는 다양한 업무와 연관되어 생겨지고, 사용자는 자신의 지위와 책임에 합당한 역할을 지정받는다. 사용자는 기존의 역할에서 새로운 역할을 생성하여 위임할 수 있으며, 다양한 방법에 의해서 철회되어진다. 이와 같은 방법을 통하여 권한의 관리를 용이하게 해준다.

RBAC 개념은 1970년대 네트워크 온라인 시스템 상에서 다중 사용자와 다중 응용으로부터 시작되었다[1]. RBAC 모델은 Sandhu 등에 의해서 RBAC96 모델이 소개되어졌다[2]. RBAC96 모델에서 권한은 역할과 관련되어지고 사용자는 적절한 역할을 할당받는다. RBAC96 모델을 확장한 모델로는 RBDM0 위임 모델이 있다[3]. RBDM0 모델에서 주목할 부분은 규칙에 기초한 접근방법을 보여주고 있다는 것이다[4]. 현재 RBAC96 모델을 확장한 다양한 형태의 모델이 제시되고 있으며, 앞으로도 많은 연구가 계속되어 질 것이다.

RBAC분야에서 현재 많은 연구가 이루어지고 있는 가장 중요한 논점중의 하나는 위임과 관련되어진 것이다. 위임은 일상생활에서도 흔히 발생하는 사건으로서, 특히, 군대, 기업, 은행 등의 계층그룹에서 빈번하게 발생한다[5]. 즉, 사용자는 또 다른 사용자에게 자신의 역할을 위임할 수 있다. 휴가 등의 사유로 인하여 사용자가 더 이상 역할을 수행할 수 없을 경우 그 역할을 대신할 사용자에게 역할을 위임하고 위임받은 사용자는 일정기간 그 역할을 수행한다. 하지만 위임받은 사용자가 부재일 경우 일정기간 업무공백이 발생되어진다.

이와 같이 위임받은 사용자가 부재일 경우 발생할 수 있는 문제점을 해결하기 위하여 중복 권한 위임 모델을 제시한다. 이는 조직의 계층적 구조에서 동일레벨에 해당되는 2명 이상의 사용자에게 동등한 권한을 위임함으로서 한 사용자의 부재 상황이 발생하더라도 동일 권한을 위임받은 또 다른 사용자에 의해서 업무공백 없이 연속적인 업무처리가 가능하다. 또한, 2명 이상의 협의에 의한 권한 위임 여부가 결정되어지는 경우도 존재한다. 이를 위해 협의에 의한 권한 위임 모델을 제시한다.

따라서 본 논문에서는 업무처리의 연속성을 위한 중복 권한 위임 모델과 중요한 사안의 권한 위임에 적용 가능한 협의에 의한 권한 위임 모델을 제시한다.

2. 제안 모델

앞에서 언급했듯이 조직체계 내에서의 위임 모델은 역할 담당자의 휴가 등의 이유로 인한 부재 상황 발생에 대한 백업(back-up) 기능 수행과 역할에 대한 분배 개념이 적용되어 진다. 본 논문에서 제시하는 중복 권한 위임 모델은 조직체계의 계층적 구조에서 동등한 레벨에

있는 2명 이상의 사용자에게 동일한 권한을 위임함으로서 위임받은 사용자가 부재일 경우 업무공백을 최소화할 수 있다. 그리고 중요도가 높은 사안에 대하여 한 사용자를 통한 권한 위임은 권한 남용으로 인한 문제의 소지가 있다. 따라서 중대 사안에 대한 권한 위임의 경우 2명 이상의 협의에 의해서만 가능하도록 함으로서 권한 오용을 미연에 방지할 수 있다.

2.1 중복 권한 위임 모델

현 정부, 기업 등의 조직체계에서 관리 정책은 반복적인 위임과 철회에 의해서 이루어지고 있다. 조직 구성원이 휴가 등의 사유로 인하여 업무 처리가 불가할 경우 다른 사용자에게 그 권한은 위임되어지고 위임받은 사용자는 그 권한을 대신 사용하게 된다. 그 후 위임받은 권한을 이용하여 또 다른 위임을 발생시키거나 철회되어지는 과정을 반복한다. 하지만 권한을 위임받은 사용자 또한 부재일 경우 업무공백을 피할 수 없다. 그리고 한 사용자에게만 권한이 위임되어질 경우 위임받은 사용자의 수행업무에 대한 감시감독의 기능을 위임한 사용자 또는 관리자가 담당해야만 한다. 이 경우 위임한 사용자 또는 관리자에 대한 책임의 증가와 이로 인한 업무효율의 저하를 초래하게 된다.

이와 같은 문제점을 해결하기 위해서 중복 권한 위임 모델을 적용할 경우 업무공백을 최소화하여 업무의 연속성을 추구할 수 있고, 동등한 권한을 위임받은 2명 이상의 사용자가 상호간의 감시감독을 수행할 수 있기 때문에 한 사용자에 대한 권한 남용을 줄일 수 있다. 그림 1은 중복 권한 위임 모델의 예를 보여주고 있으며, 다음은 그림 1에서의 사용자와 역할, 역할과 역할간의 연결 관계를 표현한다.

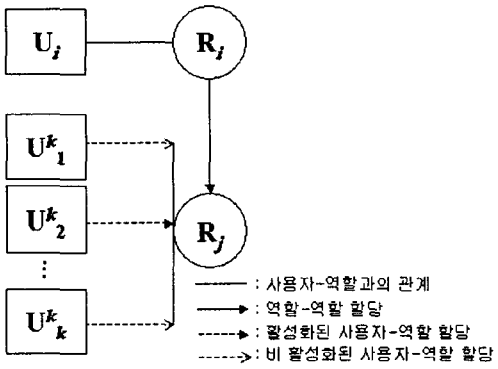

그림 1 중복 권한 위임 모델의 예

위 그림에서 사용자 U_i는 자신에게 할당된 역할 R_i의 일부분을 위임하기위해 새로운 역할 R_j를 생성한다. 새로 생성된 역할 R_j를 동등한 레벨의 사용자 U^k_1, U^k_2, ...,U^k_k에게 중복 권한 위임한다. 이때 권한 할당은 모두에게 이루어지지만 역할 R_j에 대한 권한 활성화는 단 한 사용자에게만 이루어진다. 이와 같이 함으로서 동일 업무에 대한 중복 수행을 막을 수 있고, 사용자 U^k_2가 부재이더라도 역할 R_j에 할당된 다른 사용자에 의해 동일업무를 수행할 수 있다. 또한 다른 사용자들에 의해 상호간에 감시감독 기능과 백업기능을 수행할 수 있다.

2.2 협의에 의한 권한 위임 모델

실제 조직내부의 업무흐름에서 어느 한 사람의 결정에 의해서 의사결정이 이루어지는 경우는 그렇게 많지 않다. 이는 부서간의 업무가 서로 유기적으로 연결되어 처리되기 때문이다. 특히, 중대한 사안에 대한 의사결정의 경우 한 사용자에 의한 권한 위임은 권한 남용의 문제점을 유발시킬 수 있다. 이와 같은 문제점을 해결하기 위해 2개 이상의 부서가 서로 유기적으로 연결되어 처리되는 업무 또는 중대한 사안의 권한위임 방법으로 협의에 의한 권한 위임 모델을 제안한다. 그림 2는 협의에 의한 권한 위임 모델의 예를 보여주고 있으며, 다음은 그림 2에서의 사용자와 사용자, 사용자와 역할 및 역할과 역할간의 연결 관계를 표현한다.

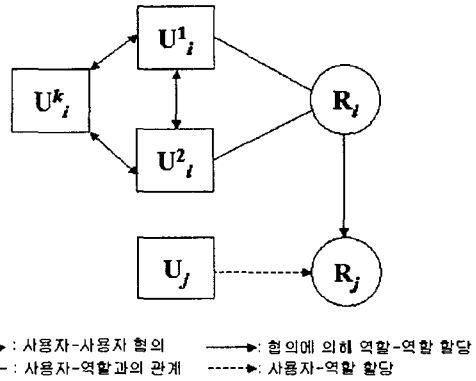

그림 2 협의에 의한 권한 위임 모델의 예

위 그림에서 사용자 U^1_i, U^2_i, ..., U^k_i는 상호 유기적인 관계를 가지고 있는 동일한 역할, R_i에 할당된 사용자이며 . 사용자들은 상호협의에 의해 새로운 역할 R_j은 생성하고 이를 사용자 U_j에게 권한을 위임한다. 역할 R_j에 대한 감시감독 기능 또한 사용자 그룹 U_i에 의해 동시에 수행함으로서 좀더 강력한 보안 관리가 가능하다. 이를 통해서 상호간의 협의가 필요하거나 중대한 사안에 대한 감시감독 기능과 업무에 대한 책임을 강화할 수 있다.

3. 제안모델의 정형화

본 절에서는 앞에서 제안된 모델을 위한 함수를 정의한다.

<정의 1> 다음은 중복 권한 위임 모델에서의 구성요소 사이의 관계를 정의한다.

- Create_role(R_j) : 위임하고자 하는 사용자가 위임기간동안 사용될 임시역할(R_j)을 생성한다.
- Delegate_role(R_i, R_j) : 역할 R_i를 가진 사용자가 역

할 R_j에게 위임한다.

- Duplicate_Assign(R_j, U^k) where $k \geq 2$: 생성된 임시역할(R_j)에 복수의 사용자를 할당한다.
- Activate_user(U_i) where $i \leq k$: 임시역할(R_j)을 할당받은 복수의 사용자 중 한명만이 활성화된다.

위와 같은 관계에 의해서 새로 생성된 임시역할(R_j)을 복수의 사용자에게 할당하고 그 중 한 사용자에게만 위임된 권한을 활성화시킨다.

<정의 2> 다음은 협의에 의한 권한 위임 모델에서의 구성요소 사이의 관계를 정의한다.

- Deliberate_delegate(R_i, R_j) : 역할 R_i를 가진 2명 이상의 사용자들의 협의에 의해서 임시역할(R_j)을 생성한다.
- Single_assign(R_j, U_i) : 생성된 임시역할(R_j)에 한명의 사용자를 할당한다.

위와 같은 관계에 의해서 협의에 의해 생성된 임시역할(R_j)을 사용자 U_i에게 권한 위임하게 된다.

4. 분 석

기존에 제안된 권한 위임 모델의 경우 권한을 위임하는 대상과 권한을 위임 받는 대상과의 관계에 중점을 두어왔다. 예를 들어, RBDM0와 RDM2000 모델은 사용자와 사용자 사이의 권한 위임에 중점을 두고 제안되어 졌다[6]. 이를 확장한 PBDM0 모델은 단일 권한 위임과 다중 권한 위임의 기능을 제공하고 있다[6]. PBDM1 모델은 PBDM0 모델에 비하여 좀 더 세분화된 권한 위임의 계층구조를 제시하고 있으며, PBDM2 모델은 주로 역할 대 역할 사이의 권한 위임에 중점을 두고 있다[6].

위의 모델에서 알 수 있듯이 기존 권한 위임 모델의 경우 권한 위임 받은 사용자의 부재 상황 발생으로 인한 업무공백 또는 중대 사안에 대한 보안 기능 강화를 위한 모델로 평가하기에는 어려움이 있다. 물론 PBDM0 모델에서 다중 권한 위임을 이용하여 권한 위임 받은 사용자 부재로 인한 문제점을 해결할 수 는 있지만 동등한 레벨의 사용자가 아닌 하위레벨의 사용자에게 권한이 위임됨으로 인한 권한 남용의 문제점을 유발할 수 있다.

따라서 본 논문에서 제안된 중복 권한 위임 모델을 적용하면 업무공백을 최소화하여 연속적인 업무수행이 가능하고 사용자간의 감시감독 기능 강화도 기대할 수 있다. 그리고 협의에 의한 권한 위임 모델을 적용할 경우 상호 유기적인 협력이 필요한 업무를 처리하거나 중대한 사안에 대한 권한 위임에 신중을 기할 수 있기 때문에 감시감독 기능 및 보안 관리 측면을 강화할 수 있는 대안으로 적용 가능하다.

5. 결 론

현 조직체계에 가장 적합한 접근제어 모델로 인정받고 있는 역할기반 접근제어에서 조직관리에 필수적으로 요구되어지는 권한 위임을 표현하는 것은 매우 중요한 문제이다. 앞 절에서 기술되었듯이 기존에 제안되어진 권한 위임 모델들은 현 조직체계에서 발생하는 다양한 권한 위임 상황을 완벽하게 제공하고 있지 못하고 있다.

본 논문에서 제안한 중복 권한 위임 모델은 조직 내에서 발생할 수 있는 위임 받은 사용자의 부재 상황에 대한 대안으로 제안되어졌으며 이를 통해서 업무 공백을 최소화하여 연속적인 업무처리가 가능해짐에 따라 업무 효율을 높일 수 있다. 또한 동일 레벨에서 동등한 권한을 위임받은 사용자 상호간의 감시감독 기능과 백업 기능을 강화할 수 있다.

그리고 협의에 의한 권한 위임 모델의 경우 실제 조직체계에서 발생하는 상호 협의에 의한 의사 결정과 중요한 업무처리와 관련된 권한 위임을 효과적으로 처리하기 위해서 제안되어졌다. 이를 통해서 상호간의 권한 위임에 더욱더 신중을 기함으로 인해서 권한 남용을 막을 수 있다. 또한 부서간의 감시감독 기능과 업무 처리에 대한 책임 기능을 강화할 수 있다.

기존 모델과의 비교분석에서 살펴본 바와 같이 본 논문에서 제안된 중복 권한 위임 모델과 협의에 의한 권한 위임 모델은 기존 모델의 부족한 부분인 위임된 권한 사용에 대한 감시감독의 기능을 강화하고 위임된 권한의 남용을 줄여줌으로서 보다 안정된 권한 위임의 기법을 제공하고 실제 조직체계에도 적용 가능하다. 향후 다국적 기업과 같은 분산 환경의 조직체계에 적용 가능한 연구가 필요하다.

[참 고 문 헌]

[1] R. Sandhu and Q. Munawar, "How to do Discretionary Access Control Using Roles," *Proceeding of 3rd ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October, pp. 22-23, 1998.

[2] R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role-based access control models," *IEEE Computer*, Vol. 29, No. 2, pp. 38-47, 1996.

[3] E. Barka and R. Sandhu, "Framework for Role-Based Delegation Models," *Proc of 16th Annual Computer Security Application Conference(ACSAC 2000)*, December, 2000.

[4] Z. Longhua, G. Ahn and Dhu. B, "A Rule-based Framework for Role-Based Delegation," *In ACM SACMAT*, Chantilly, VA, USA, 2001.

[5] 박소영, 이상호, "계층 그룹에서 반복적 권한 위임을 허용하는 임계 대리서명 프로토콜," *한국정보과학회 논문지*, 제30권, 1호, pp. 251-253, 2003.

[6] X. Zhang, S. Oh and R. Sandhu, "PBDM: A Flexible Delegation Model in RBAC," *Proc. Of 2003 ACM Symposium on Access Control Modes and Technologies(SACMAT'03)*, pp. 149-157, June, 2003.