역할기반 접근통제에서의 단방향과 양방향이 고려된 하이브리드한 위임기법

양혜진° 전준철 전진우 김용석 유기영
경북대학교 컴퓨터공학과
{ruwji°, jcjeon33, jwjeon, shadowguys}@infosec.knu.ac.kr yook@knu.ac.kr

Hybrid Technique based on one way and two way delegation in Role-based Access Control

Hye-Jin Yang° Jun-Cheol Jeon Jin-Woo Jeon Yong-Sok Kim Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

권한위임은 역할기반-접근통제에서 중요한 정책의 하나로 한 역할에서 다른 역할로 권한의 일부 또는 전부를 위임하는 것을 말한다. 대부분의 계층적 역할기반-접근통제 시스템에서는 권한위임 시에 회수까지 고려한 위임을 지원하는 모델이 일반적이다. 하지만 권한위임에 있어서 역할권한의 회수가 불필요하거나 회수를 할 때 문제가 발생할 수 있다. 본 논문에서는 역할권한의 회수가 필요하지 않는 경우에 시스템의 복잡성을 감소시키기 위한 방안으로써 단방향 권한 위임기법을 정의하며, 일반적인 위임과 단방향 권한 위임이 같이 고려된 하이브리드한 위임기법을 제안한다.

1. 서 론

최근의 정보 시스템에서는 다중 프로그램과 다중 사용자에 의해 많은 데이터에 대한 접근들이 이루어지고 있다. 이러한 복잡한 접근들을 관리하기 위해 시스템 관리자나 개발자는 인증과 역할을 이용한 접근통제 정책을 제안 적용하고 있다. 접근통제 시스템에서는 역할기반, 업무기반, 작업기반등 다양한 요소기반을 가지는 접근통제 정책들이 제안되어 있다. 이 중에서 역할기반 접근통제 정책들이 많이 제안되었다.

역할기반 접근통제란 어떤 특정 업무에 대한 개개의 역할을 규정하여 역할에 사용자와 업무에 필요한 권한이나 책임을 부여하는 것이다. 이러한 기법을 사용하는 것은 사용자에게 직접적으로 권한을 부여하였을 때 사용자의 임의적인 권한의 오·남용을 피하고자 제시되었다. 잘 알려진 모델로서 Sandhu와 Youman이 제안한 RBAC96이 있다[1]. 그리고 2001년에 Sandhu등이 역할기반 접근통제 모델의 표준을 제안하기도 했다[2]. 역할기반 접근통제에서는 상호배제와 제약사항 등의 중요 정책들이 있는데, 그 중 하나로서 권한위임이 있다. 권한위임이란 시스템 내에서 활동 중인 어떤 역할이 다른 역할에게 권한의 일부 또는 전부를 위임하는 것을 말하며 이러한 권한위임을 적용한 모델들이 많이 제안되고 있다[3-5].

Barka와 Sandhu가 제안한 역할기반 위임모델(RBDM)에서는 권한위임에 있어서 위임과 부분위임, 다중단계위임, 계층적 구조에서의 위임, 위임한 역할권한의 회수를 제안하였다[4]. 2002년에는 Bandmann등이 제약사항을 적용한 권한위임 모델을 제안하였다[5]. 지금까지 제안된 모델에서는 모든 권한위임에 대해서 역할권한의 회수를 고려하고 있다. 하지만, 권한위임에 있어 역할권한의 회수가 불필요한 경우나 회수가 일어났을 때 문제점이 생기는 경우가 있다. 이때 만약, 제안된 모델들을 적용할 경우 회수를 위한 무의미한 동작이 일어날 수 있다.

본 논문에서는 이러한 경우에 적용 가능한 새로운 위임기법을 제안한다. 먼저, 단방향 권한위임기법을 제안하고 이를 바탕으로 권한위임의 유형으로 분류하여 각 유형의 구체적인 예를 들어 그 필요성에 대해서 설명한다.

2. 제안된 권한위임 기법

본 절에서는 역할기반 접근통제 모델에서 단방향 권한위임을 정의하고 각 권한위임을 분류한다. 또 분류된 유형을 바탕으로 어떤 경우에 위임한 권한에 대해서 회수가 불필요한지 설명한다.

2.1 권한위임의 정의

단방향 권한위임은 권한회수가 필요하지 않은 경우에 적용할 수 있는 위임기법이다. 기존의 역할기반 접근통제에서 권한위임이란, 위임과 회수 두 가지를 모두 고려하여 수행하였다. 그러나, 본 논문에서 권한위임을 양방향과 단방향의 두 가지 형태로 나누어 생각하기로 한다.

정의 1. (양방향 권한위임) 양방향 권한 위임이란 역할기반 접근통제에서 위임한 역할이 위임과 회수를 수행 할 수 있다.

정의 2. (단방향 권한위임) 단방향 권한위임이란 역할기반 접근통제에서 위임한 역할이 자신의 역할권한 중 일부 또는 전부를 위임만을 수행 할 수 있다.

단방향 권한위임에서는 역할권한의 회수가 불가능하므로 이에 따른 권한의 오·남용이 발생하는 새로운 문제점

을 방지하기 위해서 단방향 권한위임은 한 단계로만 제한한다. Sandhu가 제안한 영구위임모델[3]에서는 각각 역할에 할당된 역할권한 전부를 넘겨주는 특징을 가진다. 그러나, 본 논문에서는 위임하는 역할의 업무에 따라 역할권한을 부분집합으로 나누어 역할권한의 전부뿐만이 아니라 일부분만 위임할 수 있다.

2.2 권한 위임의 분류와 단방향 권한위임의 필요성

역할권한의 회수가 모든 권한위임에서 필요한 것은 아니다. 사용자 부재나 역할의 통합 및 세분화 시, 역할권한의 회수를 생각하지 않아도 되는 권한위임을 생각해 볼 수 있다. 이에 따라 권한위임을 네 가지의 유형으로 나눈다.

- **일반(general) 유형** - 일반적인 위임유형으로 위임하는 역할이 위임받을 역할의 권한 회수를 할 수 있다.
- **부재(absence) 유형** - 위임 후 위임하는 역할의 사용자는 그 역할권한의 일부를 회수 가능하나, 진행중인 업무의 완료를 위해 위임받은 역할의 사용자가 사용하고 있는 역할권한의 경우에는 회수를 할 수 없다.
- **통합(unification) 유형** - 위임 후 위임하는 역할의 역할권한은 위임받은 역할의 역할권한으로 대체되므로 위임하는 역할의 사용자는 역할권한의 회수를 할 수 없다.
- **세분화(subdivision) 유형** - 위임 후 위임하는 역할의 역할권한은 위임받은 역할의 권한으로 대체되므로 위임하는 역할의 사용자는 역할권한의 회수를 할 수 없다.

위에서 설명한 각 유형에서 일반유형, 세분화유형과 통합유형은 역할권한의 전부를 위임할 수 있으며, 부재유형은 역할권한의 일부 또는 전부를 위임할 수 있다. 구체적인 실례를 살펴보면 다음과 같다.

일반 유형의 경우는 다음에 열거된 세 가지 경우를 제외한 모든 일반적인 경우에 사용되어 진다.

부재 유형의 경우, 역할에 할당된 사용자가 부재인 경우를 생각해 볼 수 있다. 사용자의 부재 기간 동안에 처리, 완료되어야 할 업무가 있거나, 복귀 후에 위임한 역할권한에 대한 회수가 일어난다면 위임받은 역할이 처리중이었던 업무가 중단되어 버리는 상황이 발생할 것이다. 이 때, 그 처리경과에 따른 자원 소모만이 일어날 뿐 중간 처리결과가 사라질 가능성이 존재한다.

예를 들어, 두 모바일 프로젝트 팀이 있을 때 모바일1팀의 프로젝트 매니저(PM1)가 일정 기간 동안 자리를 비움으로서 모바일2팀의 프로젝트 매니저에게 권한을 위임하는 경우가 있을 수 있다. 이 때 PM1이 있지 않는 기간 동안 진행 중이던 프로젝트들은 권한 회수를 할 경우에 프로젝트 진행과정 상의 중간 결과물의 손실에 대한 위험이 크다. 따라서 이때 권한회수를 하지 않도록 하는 처리가 필요하다.

통합유형의 경우로 역할기반 접근통제에서 역할의 세분이 심할 경우나 시스템의 축소가 필요할 경우를 생각해 볼 수 있다. 이때는 각 역할과 역할을 통합할 필요가 생긴다. 그림 1에서와 같이 상품매입담당, 대차대조담당, 현금입출금담당의 세분화된 역할을 경리담당의 한 역할로 통합하고자 할 수 있다. 기존의 여러 역할들이 한 역할로 역할 권한을 위임 후, 폐기될 경우에 권한회수의 동작이 고려되어질 필요가 없다.

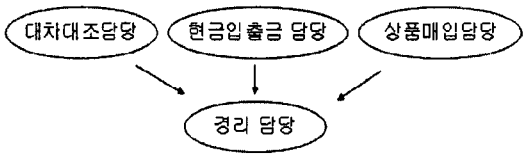

그림 1 통합유형의 예

세분화 유형의 경우, 역할기반 접근통제에서 역할의 통합이 심할 경우나 시스템의 확장이 필요할 경우 각 업무에 대한 역할의 세분화를 할 필요가 생긴다. 이때에 고려해야 할 점은 위임하는 역할에서 같은 역할권한을 여러 역할에 나눠서 주는 것이 가능할 수 있다는 것이다. 그림 2에서와 같이 광고기획담당의 역할을 마케팅담당, PR담당, 영업기획담당과 같이 세분화 할 수 있다.

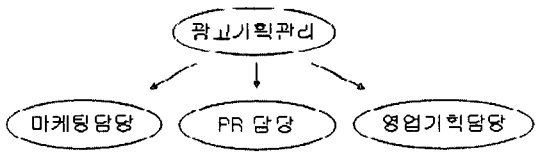

그림 2 세분화유형의 예

앞에서 설명한 일반유형을 제외한 세 가지 유형에서 권한위임은 역할권한의 일부 또는 전부의 위임만이 이루어지는 단방향 권한위임이 필요하다.

3. 하이브리드 형식의 권한 위임 알고리즘

본 절에서는 2절에서 제안한 역할권한 위임유형에 따라 양방향 권한위임과 단방향 권한위임을 수행하는 함수를 알고리즘으로 나타낸다. 함수는 delegate(RoleSet SRS, RoleSet TRS, DType DT)의 형태로 나타낸다.

- get_permissions(Role R) : 위임하는 역할의 역할권한의 전부를 가져오는 함수.
- twoway_delegate(SourceR, TargetR, permission p 또는 permissionSet PS) : 위임하는 역할 SourceR이 위임대상이 되는 역할 TargetR에 역할권한의 일부 또는 전부를 위임하는 양방향 권한위임 수행함수.

이 때 SourceR을 매개변수로 받는 것은 회수가 필요할 때 되추적을 하기위해서 쓰인다.

- oneway_delegate(TargetR, permission p 또는 permissionSet PS) : 위임대상이 되는 역할 TargetR에 역할권한의 일부 또는 전부를 위임하는 단 방향 권한위임 수행함수.

```
Delegation Algorithm

Input : delegate RoleSet SRS, delegated
RoleSet TRS, delegationType DT
Output : delegate
Function :
delegate(RoleSet SRS, RoleSet TRS, DType DT)
begin
  Role TargetR
  PermissionSet PS = get_permissions(SRS)
  if DT is ABSENCE TYPE
  then begin
    TargetR = TRS
    for all permission p_i ∈PS do begin
      if p_i can revoke
          SourceR  = SRS
          twoway_delegate(SourceR,TargetR, p_i)
      else if p_i cannot revoke
          oneway_delegate(TargetR, p_i)
    end
  end
  else if DT is UNIFICATION TYPE
  then begin
    TargetR = TRS
    oneway_delegate(TargetR, PS)
  end
  else if DT is SUBDIVISION  TYPE
  then begin
    PermissionSet SubPS
    for each SubPS_i ⊂PS do begin
     for each TargetR_j ∈TRS do begin
      oneway_delegate(TargetR_j, SubPS_i)
     end
    end
  end
  else //DT is GENERAL TYPE
  then begin
    SourceR  = SRS
    for each TargetR_i ∈TRS
    do begin
        twoway_delegate(SourceR, TargetR_i, PS)
    end
  end
end
```

그림 3. 역할권한 위임유형에 따른 위임알고리즘

부재유형의 경우 위임은 한 역할에서 그 와 다른 역할로 이루어진다. 역할권한은 뒤에 권한회수가 되는지 아닌지에 따라, 양방향 권한위임이 이루어지거나 단방향 권한위임이 이루어진다. 통합유형일 경우 위임은 한 역할에서 그 와 다른 역할로 이루어지며, 역할권한의 전부가 단방향 권한위임이 이루어진다. 세분화유형일 경우 위임은 한 역할에서 그 와 다른 역할집합으로 이루어진다. 각 위임대상 역할들에 해당 역할권한의 부분집합이 단방향 권한위임으로 주어진다. 이 때, 같은 역할권한 부분집합이 주어질 수 있다. 일반유형일 경우 위임은 한 역할에서 그 와 다른 역할집합으로 이루어진다. 각 위임대상 역할들에 양방향 권한위임으로 역할권한 집합이 주어진다.

4. 제안 기법 고찰

제한된 권한위임은 다음과 같은 장점을 가진다. 일반 권한위임의 경우 역할권한의 회수를 위해 권한위임이 어느 쪽에서 이루어졌는지에 대한 정보를 저장하고 있어야 한다. 하지만 단방향 권한위임의 경우, 역할권한의 회수가 고려될 필요가 없다. 따라서, 단방향 권한위임이 고려된 하이브리드 형식의 기법이 사용될 경우, 위의 경우와 같이 많은 정보를 저장할 필요가 없다. 더욱이 조직의 세분화나 통합 또는 시스템이 확장 및 축소가 빈번한 경우 아주 유용한 위임기법으로 사용될 것이라 기대된다. 그리고 부재유형에서와 같이 권한회수를 막음으로써 실제 시스템에 적용하였을 때 작업의 중단으로 인한 손실을 줄일 수 있을 것이라 기대된다. 또한, 기존의 위임기법과 함께 하이브리드하게 사용할 수 있다는 장점이 있다.

5. 결론

본 논문에서는 권한위임 후 역할권한 회수가 필요한 경우와 필요하지 않은 경우를 고려하여 하이브리드한 권한위임의 기법을 제시하였다. 또한 이를 위해 권한위임을 네 가지의 유형으로 구분하였다. 제안된 기법은 조직의 세분화나 통합 또는 시스템이 확장 및 축소가 빈번한 경우 아주 유용한 위임기법으로 사용될 것으로 기대한다.

참고문헌

[1] Ravi S. Sandhu, Edward J. Coyne, HalL. Feinstein and Charles E. Youman, *"Role-Based Access Control Models," IEEE Computer*, Volume 29, Number 2, Feb.1996.

[2] D.F.Ferraiolo, R.Sandhu, S.Gavrila, D.R. Kuhn, R.Chandramouli, *"Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security*, pp.224-274, Vol. 4, No. 3, August 2001

[3] Ezedin Barka and Ravi Sandhu, *"Framework for Role-Based Delegation Models," Proc. of 16th A unual Computer Security Application Conference(ACSAC 2000)* , pp. 168-176, Dec.2000,

[4] Ezedin Barka and Ravi Sandhu, *"A Role-Based Delegation Model and Some Extensions," Proc. of23rd National Information Systems Security Conference (NISSC 2000).* December, 2000.

[5] O. Bandmann, M. Dam, B.S. Firozabadi, *"Constrainted Delegation," Proceedings of the 2002 IEEE Symposium on Security and Privacy*, 2002.