역할기반 접근통제에서의 부분역할을 이용한 권한위임 기법

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

Delegation using Sub-Role in Role-based Access Control

Jin-Woo Jeon° Jun-Cheol Jeon Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

역할기반 접근통제는 많은 조직에서 효과적으로 사용되고 있다. 역할기반 접근통제에서 권한은 역할과 관련이 되어 있고 사용자는 역할과 관련된 권한을 얻기 위해 역할의 일원이 되어진다. 역할기반 접근통제에서의 사용자 권한위임은 한 사용자가 인증 된 다른 사용자에게 자신의 권한을 위임하여 권한을 위임한 자신과 같은 역할의 일원이 되게 하는 것이다. 그러나 기존의 역할기반 접근통제 모델에서는 권한의 일부를 위임하는 것이 어려웠다. 본 논문에서는 역할을 위임을 위한 부분역할로 나누어 권한의 일부를 위임 가능하게 함으로써 권한 전체를 위임했을 때의 문제를 방지하고, 접근통제에서의 최소권한 원칙과 임무분리 원칙을 만족하게 하는 권한위임 방법을 제안하였다.

1. 서 론

접근통제는 기업, 병원, 정부조직, 학교 등과 같은 큰 조직에서 중요한 보안 문제이다. 역할기반 접근통제(role-based access control : RBAC)[1]는 이러한 조직에서 증명되어졌고 점점 많이 사용되어지고 있는 기술이다. 역할기반 접근통제에서 접근권한은 역할과 관련이 있고, 사용자는 그가 가지는 책임과 자격에 기초하여 적당한 역할에 할당되어지고, 그런 후에 역할에 알맞은 권한을 얻게 된다. 사용자는 쉽게 다른 역할로 변경할 수 있다. 역할은 새로운 권한을 가질 수 있고, 필요에 따라서는 가진 권한을 취소 할 수도 있다. 역할기반 접근통제는 조직에서 역할과 책임에 대해 안전하게 설계할 수 있기 때문에 조직의 관점에서 안전한 보안 모델을 만드는데 용이하다.

대부분의 조직에서는 접근통제와 관련된 몇 가지 규정을 가지고 있는데, 권한위임[2]은 이러한 중요한 규정 중의 하나이다. 권한위임이란 권한을 위임하는 한 사람이 권한을 위임받을 다른 사람에게 그의 권한의 전부나 일부를 주는 것을 말한다. 그러나 현재의 역할기반 접근통제 모델에서는 권한이 속해 있는 역할 전체를 위임 할 수밖에 없기 때문에 정보의 유출이나, 권한 오·남용 등의 보안 문제점을 갖고 있다. 과업-역할기반 접근통제에서는 과업(task)을 위임하기 위한 새로운 위임역할을 생성한다. 이때는 새로운 역할을 생성하고 생성된 역할에 대해 과업을 할당해야 하는 번거로움 때문에 전체적인 복잡도가 증가하는 원인이 된다.

이 논문은 2003년도 두뇌한국21사업에 의하여 지원되었음.

본 논문에서는 사용자에게 할당된 역할을 좀더 세분화하여 역할의 부분역할을 만들어 권한을 할당하고 위임에 있어서는 역할의 내부에 존재하는 부분역할을 이용함으로써 기존의 접근통제에서의 권한위임 시 발생했던 문제를 방지하고, 접근통제에서 요구되는 최소권한 원칙과 임무분리의 원칙을 만족하는가를 알아본다.

본 논문의 2장에서는 역할기반 접근통제에서의 권한위임을 살펴보고, 역할을 부분역할로 나누는 방법을 알아본 후에 권한위임은 어떻게 이루어지는 가를 볼 것이다. 그리고 3장에서는 제안된 권한위임 방법이 최소권한 원칙과 임무분리 원칙에 만족하는지를 살펴본 후에 기존의 모델과 비교하였다. 마지막으로 4장에서 결론을 맺기로 한다.

2. 부분역할을 이용한 권한위임

본 장에서는 먼저 역할기반 접근통제에서의 권한을 위임하는 방법을 알아보고 문제점을 점검한다. 그리고 위임을 위한 부분역할로 나눈 모델을 제안하고, 제안된 모델에서의 권한 위임의 방법을 알아본다.

2. 1 역할기반 접근통제에서의 권한위임 방법

역할기반 접근통제에서 권한을 위임하는 방법으로 두 가지 정도를 생각해 볼 수 있다[3]. 첫째는 그림 1에서 보는 것과 같이 위임하고자 하는 역할에 사용자를 직접 할당하는 것이다. 그러나 만약 이러한 위임이 역할 계층 구조에서 일어난다면 사용자2는 역할1의 부분 계층에 있는 역할까지 상속하게 되는 문제가 있다. 또한, 위임하고자 하는 권한을 위임받을 사용자가 할당되어 있는 역할에 위임함으로써 권한을 위임하는 방법이다. 이런 경우,

그림 2에서 보는 것과 같이 의도하지 않은 사용자3에게까지 권한이 위임이 되는 문제가 발생을 하게된다.

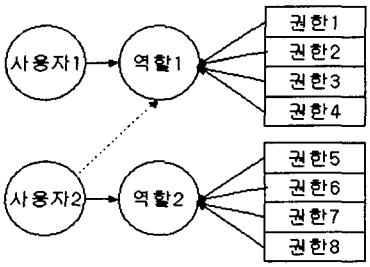

그림 1 역할기반 접근통제에서 위임1

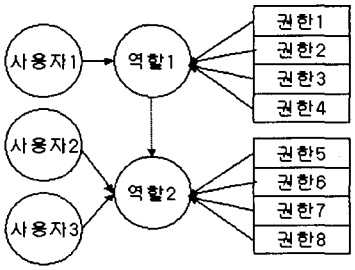

그림 2 역할기반 접근통제에서 위임2

2. 2 역할을 부분역할로 분리

하나의 역할은 위임의 정도와 업무 특성에 따라 부분역할로 나눌 수 있다. 부분 역할들은 좀더 효과적인 위임을 위해 사용되어질 수 있다. 한 역할의 분리는 그림 3에서와 같이 보여진다.

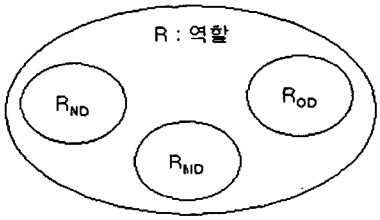

그림 3 위임에 따른 부분역할로의 분리

제안된 권한위임 방법에 따라 그림 3과 같이 하나의 역할을 세 가지의 부분역할로 나누어 생각해 볼 수가 있다. 첫째 개인에게만 한정된 부분역할(R_{ND})은 절대 위임해서는 안 되는 권한들의 집합이다. 둘째 일단계 위임만이 가능한 부분역할(R_{OD})은 역할을 가진 사용자가 바로 하위의 역할에만 위임할 수 있는 권한들의 집합이다. 마지막으로 다단계 위임이 가능한 부분역할(R_{MD})은 권한을 위임받은 사용자가 또 다른 사용자에게 위임이 가능한 권한을 모아 놓은 집합이다. 이들 세 부분역할의 권한은 역할의 전체 권한집합의 부분집합이 된다. 다음은 제안된 모델에서의 권한 위임의 예를 보여준다.

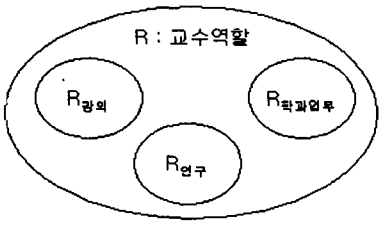

그림 4 부분역할의 예

대학이라는 조직 내에 있는 교수의 역할을 그림 4에서와 같이 세 개의 부분역할로 나누었다. 교수의 역할 중 수업은 교수의 고유한 역할이다. 강의에는 수업를 비롯해 성적처리까지 모두 교수만이 해야하는 일들로 구성되어 있다. 따라서 위임을 허용하지 않는 R_{ND}에 분류될 수 있다. 두 번째로 학과업무는 교수의 부재시 조교를 통해서 이루어 질 수 있어야한다. 따라서 한 단계 아래에만 위임을 하는 R_{OD}에 분류될 수 있다. 이때는 한 단계 아래 사용자에게만 위임이 이루어져야 한다. 세 번째로 연구는 팀의 리더를 비롯해 모든 구성원에게 합당한 역할을 부여하고 위임할 수가 있다. 따라서 교수의 감독 하에 팀장을 비롯 팀원들에게까지도 권한 또는 책임을 전달할 수 있도록 R_{MD}에 분류되어야 한다. 위의 예에서와 같이 조직 내에서 역할을 위임의 정도와 작업특성에 따라서 부분역할로 나눌 수 있다.

2. 3 구성요소의 정의

제안된 모델의 특징과 관련된 구성요소들을 다음과 같이 정의한다.

U : 사용자의 집합,
R [$R = R_{ND} \cup R_{OD} \cup R_{MD}$] : 역할의 집합
R_{ND} [$R_{ND} \subset R$] : 위임 불가능한 역할의 집합
R_{OD} [$R_{OD} \subset R$] : 일단계위임만 가능한 역할의 집합
R_{MD} [$R_{MD} \subset R$] : 다단계위임이 가능한 역할의 집합

P: 권한의 집합
P_{ND} [$P_{ND} \in R_{ND}$] : R_{ND}에 할당된 권한의 집합
P_{OD} [$P_{OD} \in R_{OD}$] : R_{OD}에 할당된 권한의 집합
P_{MD} [$P_{MD} \in R_{MD}$] : R_{MD}에 할당된 권한의 집합

또한, 제안된 구성요소는 다음과 같은 속성을 만족해야 한다.

1. 각각의 하위 역할들은 중복성을 회피한다.
   $R_{ND} \cap R_{OD} \cap R_{MD} = \varnothing$
2. 각각의 하위 역할에 할당된 권한들은 중복성을 회피한다.
   $P_{ND} \cap P_{OD} \cap P_{MD} = \varnothing$

이러한 속성들은 임무분리의 원칙을 만족한다.

2. 4 권한의 위임과 회수

RBDM0[2]에서 위임은 한 사용자가 다른 역할에 할당

되어 있는 사용자에게 자신의 역할의 일부나 전체를 위임하는 것을 말하고 있다. 또한 위임하는 사용자는 위임을 위한 역할생성이나 권한할당 등의 기능을 수행할 수가 있다. 본 논문에서는 사용자-사용자 권한위임에 초점을 맞추고 위임과 회수를 고려한다.

위임하고자 하는 사용자는 위임의 정도에 따라 나누어진 부분역할을 위임하고자 하는 사용자에게 할당함으로써 위임이 이루어진다. 여기서 위임이 일어나지 않는 R_{ND} 부분역할에 대해서 생각하는 것은 의미가 없다. 위임은 두 개의 부분역할, 즉, R_{ND}를 제외한 나머지 R_{OD}와 R_{MD} 부분역할에서 일어난다. 권한을 위임의 정도로 나누어 위임하기 때문에 위임을 위한 새로운 역할을 만들 필요가 없게 되고, 동시에 역할을 세분화한 효과가 있기 때문에 정보유출에 대한 위협을 최소화할 수 있다.

권한회수는 일단계 위임이 이루어졌을 때와 다단계 위임이 이루어졌을 때로 나누어 생각해 볼 수 있다. 일단계 위임에 대한 권한회수를 GIR(Grant-Independent Revocation)라고 하고, 다단계 위임에 대한 권한회수를 GDR(Grant-Dependent Revocation)이라고 한다[2.4]. GIR은 권한을 위임한 사람만이 권한회수도 가능한 것을 말한다. GDR은 다단계 위임에서 원래의 권한위임자 외에 권한을 위임받은 하위 사용자가 그 하위 사용자에 대한 권한회수가 가능한 것을 말한다. 그림 4의 예에서 권한회수는 $R_{학과업무}$와 $R_{연구}$의 부분역할에서 일어난다. 학과업무의 경우에는 조교에게 주어졌던 권한을 회수할 수 있는 것은 교수의 역할뿐이다(GIR). 연구의 경우에는 교수역할의 사용자가 그 하위에 있는 리더에게 연구 진행에 대한 권한을 위임하였다면, 리더는 그 하위의 구성원들에게 연구 진행과 관련된 권한을 또 다시 위임할 수 있다. 이럴 때 리더는 그 하위의 구성원에게 위임하였던 권한을 회수하는 것이 가능하다(GDR).

3. 제안된 모델의 비교 분석

본 장에서는 제안된 모델에 대해 최소권한 및 임무분리의 원칙에 만족하는가를 살펴보고, 기존의 모델과 비교한다.

3. 1 최소 권한 원칙

최소권한 원칙은 사용자가 작업을 수행함에 있어 필요 이상의 권한을 가지지 못하게 하는 것이다[4]. 하나의 역할에 필요 이상의 권한이 주어졌거나 하위 역할의 모든 권한을 상속했을 때 이 원칙에 위배된다. 본 논문에서 제안한 모델에서는 권한을 위임의 정도에 따라 부분역할로 나누었고 위임이 필요할 때는 각 부분역할의 부분집합을 만들었기 때문에 최소권한 원칙을 만족시킨다.

3. 2 임무분리 원칙

임무분리 원칙(SoD)은 한 역할에 할당된 사용자가 다른 역할에도 동시에 할당되는 것을 제한하는 원칙이다[4]. 이렇게 함으로써 역할에 주어진 임무의 중복을 막을 수 있다. 본 논문에서 제안한 모델에서는 위임이 상하 두 역할의 각각의 같은 부류의 부분역할들 사이에서의 이루어진다. 즉, 위임이 상위R_{OD}-하위R_{OD}, 상위R_{MD}-하위R_{MD}와 같은 관계에서만 이루어지므로 같은 역할에 있는 두 부분역할들 사이에 임무가 중복되지 않는다. 이러한 이유에서 임무 분리의 원칙이 지켜질 수 있다. 다음의 표는 기존의 권한위임 모델인 RBDM0와 과업-역할 기반 접근통제 모델과 비교한 표이다.

표 1 기존모델과의 비교

비교 기준	RBDM0	T-RBAC	제안된 모델
위임자	관리자	사용자	사용자
권한회수	위임한 사용자 일정시간파괴 GID 사용	위임한 사용자 위임역할파괴	위임한 사용자 GDR, GIR사용
위임단위	위임역할	작업	부분역할
위임형태	일단계 위임	일단계 위임 다단계 위임	일단계 위임 다단계 위임
무결성 (의무분리)	고려하지 않음	작업단위 의무분리지원	부분역할단위 위무분리지원
비밀성 (정보유출)	고려하지 않음	사용자 범위 경직고려가능	부분역할단위 정보유출최소화
구현방법	위임역할 생성	위임역할 생성	부분역할이용

4. 결론

역할기반 접근통제에서 권한의 위임은 반드시 필요한 원칙 중에 하나이다. 그러나 기존의 역할기반 접근통제 모델에서는 역할전체에 대한 위임이 가능하여 여러 가지 문제점이 지적되었다. 본 논문에서는 역할을 위임의 정도와 업무특성에 따라 부분역할로 나누고, 각 부분역할에 속하는 권한을 다시 더 작은 부분집합의 단위로 묶어 권한을 위임하는 형태를 제시하였다. 그리고 이러한 방법이 접근통제 모델에서 요구되어지는 최소권한 원칙과 임무분리 원칙이 만족하는지도 보였다.

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

[3]심재훈, 박석, "역할기반 접근제어에 기초한 사용자 수준의 위임기법" 정보통신보호학회논문지, 제10권, 제3호, p49-62, 2000, 9.

[4]David F. Ferraiolo, D. Richard Kuhu, Ramaswamy Chandramouli, "Role-Based Access Control" ARTECH HOUSE, INC. 2003.