가용 시간을 이용한 역할 기반 위임 모델

김 경 자[†] · 장 태 무[††]

요 약

기존의 RBAC(Role Based Access Control) 모델들은 사용자간의 역할 위임이나 역할 분리를 운용하기에는 역부족이다. 이에 RBAC을 바탕으로 역할이나 권한을 다른 사용자에게 위임하는 모델인 RBDM(Role Based Delegation Model)이 연구되고 있다. 반면에, 역할을 위임 받은 자의 악의적인 남용을 막을 수 있는 방안이 필요하다. 본 논문은 역할의 위임으로 인하여 위임받은자의 악의적인 도용을 막기 위한 모델로서 위임 역할에 대한 폐지 절차를 시간상으로 제한을 두고, 위임하는 역할에 대하여 원사용자의 권한을 그대로 유지함으로써 위임으로 인한 역할간 계층구조의 보안상 취약점을 보완하고자 한다. 즉, 역할을 위임하고자 할때에는 위임에 대한 유효 기간을 같이 부여하는 기법으로 위임된 역할의 사용 권한을 시간상으로 폐지할 수 있게 한다. 또한, 위임된 역할에 대해서는 원사용자의 역할에 대한 권한을 계속 보유할수 있도록 함으로써 위임으로 인하여 역할에 대한 사용이 정당하지 않은 경우에는 언제든지 회수가 가능할 수 있게 하였다. 본 제안 기법인 T-RBDM (Time-out based RBDM)은 기존의 위임 모델인 RBDM0, RBDM1, PBDM과 비교 분석함으로 기존의 위임 모델에 비해 보안 측면에서 더 강인함을 보인다.

키워드 : RBAC, 위임 모델

Role-Based Delegation Model Using Available Time

KyoungJa Kim[†] · TaeMu Chang[††]

ABSTRACT

The existing RBAC models are not sufficient for managing delegations or separation of roles. Researches have been done on RBDM(Role Based Delegation Model) that deal with delegating role or permission to other users. In this paper, we divide the delegated roles into two groups: periodic and temporary delegation roles. When a role is delegated, a time period is assigned together, which is used to revoke the permission of delegated role automatically. In our model, the role of monotonic delegation by an original user can be revoked at any time in case of malicious use by the delegated user. The contribution of our model is that the malicious use of delegated role can be prohibited and security vulnerability in the role hierarchy due to role delegations can be alleviated. The proposed model, T RBDM(Time out Based RBDM) is analyzed and compared with the conventional models, such as RBDM0, RBDM1 and PBDM. Our model shows an advantage over other models in terms of security robustness.

Key Words : Role Based Access Control, Deleagtion Model

1. 서 론

최근 인터넷 사용자 수의 증가로 인하여 정보의 공유가 급속도로 증가하고 있는 반면에 보안의 위협이 가장 큰 문제가 되고 있다. 이러한 문제를 해결하기 위해 역할 기반 접근 제어(Role Based Access Control)기법이 대두되었으나, 업무 양의 증가나 역할의 분리 등으로 인하여 아직까지 실생활에서 발생하는 여러 상황을 효율적으로 운영하기에는 역부족이다. 이에, 역할 기반 접근 제어 기법을 바탕으로 역할이나 권한을 다른 사용자에게 위임하는 기법을 연구하게 되었다.

NIST(National Institute of Standards and Technology)의 역할 기반 접근 제어 표준은 사용자 수준의 역할 위임에 관한 속성을 정의하지 않고, 관리적인 측면에서의 권한 위임만을 정의하고 있다. 또한, 위임을 함으로써 발생되는 보안의 문제에 대해서는 고려를 하고 있지 않다. 즉, 위임 받은자가 역할이나 권한을 악의적인 의도로 사용하거나 남용하는 경우에는 더욱 큰 문제를 야기할수 있다. 이에 본 논문에서는 사용자뿐만 아니라 관리적인 측면에서 위임을 할 때 위임 받은 자의 사용을 항상 관리할수 있는 모델을 제안하고자 한다.

위임은 일반적으로 단순 위임과 다단계 위임의 두 가지 방법이 존재한다. 단순 위임은 자신이 위임 받은 역할을 다

† 정 회 원 : 세종대학교 컴퓨터공학과 초빙교수
†† 정 회 원 : 동국대학교 컴퓨터공학과 교수
논문접수 : 2006년 7월 20일, 심사완료 : 2006년 11월 29일

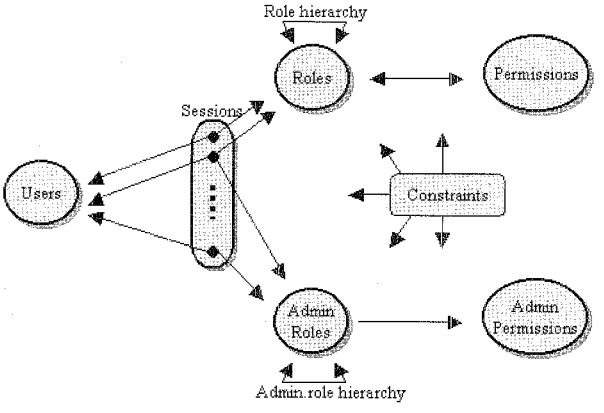
른 제3자에게 위임할 수 없다는 것을 의미하며, 다단계 위임은 위임자의 허가 하에 다시 제3자에게 역할을 위임할 수 있다는 것을 의미한다. 그러나 어떤 방법을 사용하더라고 역할 기반 접근 제어의 특성상 단순히 역할만을 위임할 경우 피 위임자에게 너무 많은 권한이 위임되게 된다. 이러한 경우에는 피 위임자의 역할 남용이 발생할 가능성이 높다. 또한, 위임된 역할에 대한 폐지도 사용자들간의 계층적인 역할과 역할간의 관계를 고려하여 적절한 시기에 폐지되어야 한다. 일반 사용자의 악의적인 용도로 위임된 역할이 사용되는 경우를 방지해야 된다. 그러나, RBAC에서의 사용자는 인증을 통하여 서로 신뢰 할 수 있는 사용자임을 바탕으로 위임이 이루어지게 되므로, 인증을 받은 사용자, 즉 내부적인 사용자로 인한 오용을 대비하여야 한다.

따라서, 본 논문에서는 역할 위임에 따른 권한의 변화가 없는 위임(Monotonic delegation)으로 사용자의 남용이나 오용을 막기 위하여 위임 역할에 대하여 원사용자가 언제든지 회수를 할 수 있도록 하는 위임을 한다. 즉, 원사용자의 권한이 위임으로 인하여 권한이 축소되거나 취소되지 않는 위임을 한다. 위임 역할을 정기적으로 위임되는 주기적인 위임 역할과 일시적으로 위임되는 역할로 구분하여 관리한다. 또한 각 위임 역할에 대해서는 시간을 고려한 권한 할당을 하고, 주어진 시간이 종료되는 시점에서는 위임을 하는 사용자와는 무관하게 시간상으로 위임 종료 시점을 가질 수 있도록 위임된 역할의 권한 사용을 제한하고자 한다. 즉, 역할 위임 시에 위임되는 역할을 위임 받는 사용자와 역할간의 세션을 연결 할 때, 세션의 유효기간을 설정함으로써, 위임을 하는 사용자와는 무관하게 시간 상으로 위임을 폐지하게 된다. 또한 각 역할에 대하여 위임 역할은 시간이라는 제약 조건에 맞게 권한과의 연결을 맺게 된다.

본 논문의 구성은 다음과 같다. RBDM에서의 위임을 고려한 새로운 모델의 필요성을 소개하는 서론에 이어, 2장에서는 RBAC96 표준 모델의 각 구성 요소들간의 관계를 설명하고, 다른 모델들과의 개략적인 관계를 설명하는 관련 연구 및 연구 동기를 보인다. 3장에서는 본 논문의 제안 기법으로 다른 모델들을 바탕으로 역할을 시간적인 측면을 고려하여 위임하게 되는 제안 모델을 제시하고, 4장에서는 기존의 모델인 RBAC, RBDM, PBDM과 본 논문의 제안 기법인 T-RBDM을 위임과 무결성 측면에서 비교 분석하였다. 마지막으로 5장에서는 본 논문의 결론 및 향후 연구 과제를 보이며 끝을 맺고 있다.

2. 관련 연구 및 연구 동기

본 장에서는 역할 기반 접근 제어 기법의 관련 연구로 RBAC96과 RBDM0, RBDM1, PBDM의 개략적인 관계와 각 구성 요소 별 관계 정의를 알아본다.

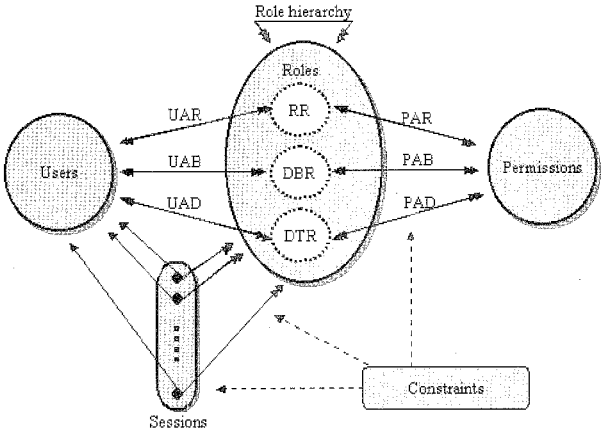


[그림 1] RBAC96의 전체적인 관계도

RBAC의 기본적인 구성 요소로는 사용자, 역할 그리고 권한으로 구성된다. 각 구성 요소들간의 관계로는 사용자와 역할과의 관계, 역할과 권한간의 관계를 나타낸다. 이 기본 모델에서의 각 관계들간의 연결을 어떻게 설정할 것 인지와 역할들을 어떻게 분리할 것 인지에 대하여 많은 연구가 진행되고 있다[1].

RBAC을 바탕으로 하는 각 모델들간의 관계로는 세 가지 구성 요소들간의 기본적인 관계만을 나타내는 RBAC0(Flat RBAC), 역할간 계층 구조가 추가된 RBAC1(Hierarchical RABC), 각 관계 설정에 있어서 제약 조건들을 추가한 RBAC2 (Constrained RBAC), 하위의 모든 모델을 병합한 RBAC3(Symmetric RBAC)의 각 모델 별 관계를 나타낸다. 각 모델들은 하위 모델에서 상위 모델로 올라가면서 하위 모델의 특징들을 내포하게 된다. RBAC0는 특정한 사용자가 어떠한 역할들에 속하게 되고, 특정 역할이 어떠한 사용자들에게 할당되는 가를 효율적으로 결정될 수 있도록 하는 사용자 역할 간 요구사항을 가진다. RBAC1은 RBAC0 모델에 역할 계층 관계가 추가된 개념이다. 역할 계층은 조직 내에서 권한과 책임의 순서를 반영하기 위해 역할을 계층적으로 구분하여 관계를 설정하게 된다. 즉, 조직내의 직위별 역할을 달리 하기 위함이다. RBAC2는 RBAC0에 제약조건을 두는 구조로써, 제약조건은 사용자 역할 할당과 사용자 세션 내에서 역할들의 활성화와 관련된다. 각 할당에서의 제약 조건을 만족하는 경우에만 역할 할당을 해주는 기법으로 RBAC에서의 각 할당에 제약 조건을 부여한 개념이 된다. RBAC3은 RBAC의 하위 모델들의 특징들을 모두 포함한 개념이 된다. 기존에 제시되어온 RBAC 모델들은 대부분 RBAC3의 형식을 따르고 있다[2-4].

[그림 1]은 RBAC96모델의 각 구성 요소들간의 관계를 전체적으로 나타낸 그림이다. 그림은 일반 사용자와 관리자에 대해서 따로 구분하여 관리하는 대칭적인 구조를 이루며, 일반 사용자의 역할과 권한, 관리자측면의 역할과 권한으로 역할간 분류로 하고, 각 역할들은 계층 구조를 이룬다. 그림



[그림 2] PBDM1의 관계도

에서 보는 바와 같이 제약 조건은 모든 할당 관계에서 적용 가능함을 보인다[5].

위의 제시된 RBAC모델로는 조직내의 역할간 관계를 효율적으로 관리하기가 부족하기에 역할간 위임을 두는 모델들이 제안되고 있다. RBDM0(Role Based Delegation Model)는 역할 기반의 위임 모델로서, 사용자와 역할과의 관계를 할당하는 데 있어서 할당 관계의 종류를 UAO(Original Member to Role Assignment Relation)와 UAD(Delegate Member to Role Assignment Relation)로 구분하여 각 할당 관계를 설정하게 된다. UAO는 일반 사용자(Original Member)와 역할을 할당해 주고, 임의의 역할을 위임 받은 사용자와 역할간의 관계를 설정해주는 UAD로 구분하여 할당 관계를 맺게 된다. 즉, RBDM0는 역할을 기반으로 위임을 하고 역할 관계에서는 위임에 관련된 역할에 대한 할당은 분리하여 관계를 설정한다[6-8].

반면에, RBDM1는 RBDM0에 역할간의 계층관계를 포함한 모델이다. 사용자와 역할간의 기본적인 관계를 나타내는 RBDM0을 기본으로 하고, 각 역할간의 계층구조를 추가한 모델로 역할 위임에 있어서 역할의 계층구조를 기반으로 역할을 위임하게 된다. 각 계층간 역할에 대한 관계를 기반으로 역할간 위임이 가능한 관계와 불가능한 관계를 명시하고 있다. 즉. 임의의 역할을 위임을 받은 사용자가 역할 계층간의 관계에서 하위 계층의 사용자에게 위임 받은 역할을 다시 상속을 해줄 수가 있다. 역할간의 계층관계로 인해 역할간 상속의 개념이 추가된 모델이 된다.

[그림 2]는 권한을 기반으로 위임을 하는 PBDM1의 각 요소 별 할당 관계를 나타내고 있다. 그림에서 보는 바와 같이, 역할을 3가지로 분류하였다. PBDM1에서의 역할은 정규 역할(RR)과 위임될 역할(DBR), 위임된 역할(DTR)로 각 분리하여 사용자와의 할당 관계를 보인다. 사용자와 정규 역할과의 할당 관계는 UAR이고, DBR과의 할당 관계는 UAB로 나타내고, 위임된 역할과의 할당은 UAD로 나타낸다. 또한 권한과의 할당 관계도 3가지의 역할과의 관계를 보이고 있다. 즉, PBDM1에서는 역할을 3가지로 분류하여 역할별 할당 관계를 맺는다. PBDM1에서의 DBR을 고정적인 위임 역할(Fixed Delegatable Role)과 일시적인 위임 역할(Temporal Delegatable Role)로 분리하여 관리하는 PBDM2도 있다[9-13].

위의 모델 별 정의와 각 요소 별 할당 관계를 보면, 사용자와 역할간의 할당관계를 좀 더 구체적으로 할당하려 하였고, 위임 할 수 있는 역할과 고정적인 역할들을 각각 분리하였다. 이는 위임에 있어서, 위임을 받은 사용자가 악의적인 용도로 역할을 남용할 것을 고려한 것이고, 또한 권한의 할당에서도 일시적인 위임 역할에 대해서는 권한을 부여하지 않는 PBDM2의 모델을 보면, 사용자와 역할, 권한의 각 할당에서 악의적인 남용을 막고자 각 요소 별 할당을 하는데 있어서 여러 가지로 고려한 것을 살펴볼 수가 있었다. 이러한 이유로 접근 제어에서 위임을 기반으로 한 연구가 여러 가지 요소를 바탕으로 연구되고 있다.

이에 본 논문에서는 위임된 역할의 악의적인 도용을 막기 위해서, 위임 역할에 있어서 위임 유효 기간을 고려한 모델을 제안함으로써 위임 역할에 대한 남용을 시간적인 측면으로 방지하고자 한다. 또한, 원사용자의 권한을 계속 유지함으로써 위임받은자의 역할 사용에 대하여 언제든지 제어 및 회수가 가능할 수 있도록 하였다.

3. 제안 모델

본 논문은 역할을 위임할 때 위임에 대한 유효 기간을 시간적인 측면으로 고려함으로써 위임에 대한 악용을 방지하고자 한다. 위임에는 크게 영구적인 위임(Permanent)과 일시적인 위임(Temporary)으로 나누어 볼 수 있다. 영구적인 위임은 한번 위임된 역할에 대하여 회수가 불가능한 위임으로 단방향의 역할 이동만이 가능하고, 일시적인 위임은 폐지 및 회수가 가능한 위임으로 양방향 역할 이동이 가능하다. 본 논문에서는 일시적인 위임인 경우로 일시적인 위임을 정기적으로 위임을 하는 역할과 일회적인 위임의 경우로 나누어 보았다.

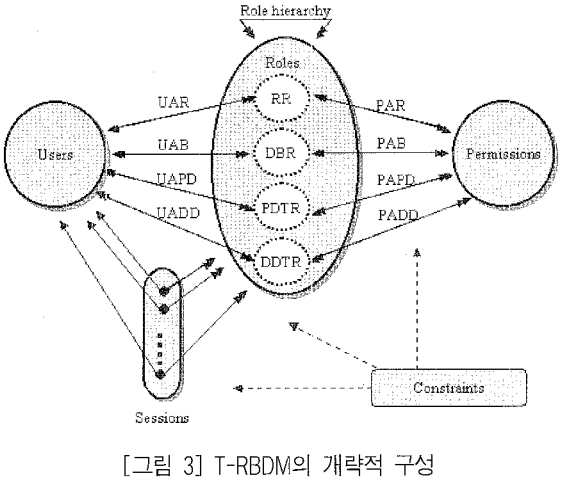
일반적으로 위임(Delegation)이란 권한의 일부 또는 전부를 제3자에게 주는 것을 의미한다. RBAC에서의 위임으로는 사용자의 역할이나 권한을 다른 제3자가 가질 수 있게 하는 기법이다. 위임이 발생되는 상황을 다음과 같이 3가지로 나누어 볼 수 있다. 첫째, 사용자가 오랜 기간 동안 자리를 비움으로써 발생되는 전체적인 업무의 흐름에 지장이 없도록 다른 제3자에게 역할을 위임하는 경우이다. 둘째, 권한의 분권화로 조직의 구성 면에서의 초기단계나 나중에 직무에 대한 기능을 상위 직무자가 하위 직무자에게 직무를 분산시키고자 하는 경우이다. 셋째로는 업무의 협력 측면으로, 경우에 따라 같은 조직 내에서나 다른 조직간의 업무의 협력을 공유하기 위하여 같은 접근 권한을 갖게 된다. 이와 같은 3

가지 상황에서 역할이나 권한의 위임이 일어나게 된다.

본 논문은 위임된 역할을 폐지(Revocation)하는데 있어서 원사용자에 의한 역할 회수와 시간적인 특징을 고려하는 폐지를 적용하고자 한다. 역할 위임에 있어서 폐지는 역할을 위임 받은 위임자의 역할 남용을 막기 위해 시간에 의한 위임 폐지나 원사용자의 역할 회수를 통해 위임된 역할에 대한 폐지가 이루어진다.

폐지의 종류로는 cascading revocation, grant dependency와 grant independency로 나누어 볼 수 있다. cascading revocation는 위임된 역할에 대하여 다단계로 위임이 되는 경우 원사용자의 위임 폐지가 이루어지면, 다음 단계의 모든 위임도 같이 폐지가 되는 방식이다. 즉, 위임이 일어난 시점에서 원사용자나 위임자의 역할이 달라지거나, 위임을 폐지하게 되면 그에 관련된 다른 위임 상황들로 같이 폐지된다. grant dependency와 grant independency는 위임된 역할에 대해서 역할 폐지를 누가 할 것인지에 관련된 것으로, grant dependency는 폐지 권한을 위임을 한 원사용자만이 할 수가 있는 방식이다. 반면에 grant independency는 위임된 역할에 대한 권한을 가지고 있는 어느 누구라도 폐지할 권한을 갖게 된다. 이는 위임을 받은 자가 부여 받은 역할로 악의적인 행동을 하는 경우에 빠르게 역할을 회수할 수 있게 된다[14].

위임된 역할에 대한 폐지의 또 다른 변수로는 위임에 대한 일시적인(Temporary)경우에 위임기간을 어떻게 부여할 것인지에 대하여 고려해볼 수가 있다. 위임 기간으로는 정기적인 형식과 기간 형식으로 폐지에 관한 시간 조건을 분류해 볼 수 있다. 정기적인 형식은 어느 기간 동안 정해진 시간에 역할을 주기적으로 위임해주는 형식이고, 기간 형식은 위임하는 시점부터 위임을 폐지하는 동안까지의 일시적인 위임 방식으로 시간이 만료되면 더 이상 위임 역할이 유효하지 않는 폐지 형식이다. 즉 위임을 부여할 당시에 위임된 역할에 대한 유효시간을 부여함으로 역할을 위임하는 방식이다.



[그림 3] T-RBDM의 개략적 구성

본 논문은 일시적인 위임만을 고려하는 경우로 역할을 분류함에 있어서 시간을 고려하여 할당을 하고, 폐지하는 방식으로 정기적인 형식과 기간형식의 두 가지 형식을 모두 고려하여 시간에 의한 위임 폐지 모델을 제안하고자 한다.

[그림 3]은 본 논문에서 제안 모델인 T-RBDM을 개략적으로 도시화한 그림이다. T-RBDM은 일시적인 위임인 경우를 바탕으로 작성된 모델로, 역할은 정기적인 형식의 위임 역할인 PDTR(Periodicity Delegation Roles)과 기간 형식의 위임 역할인 DDTR(Duration Delegation Roles)로 구분하여 역할을 할당해준다. PDTR은 시간 형식의 위임에서 정기적인 위임 할당 관계를 나타내는 것으로 매번 주기적으로 같은 시간에 같은 역할이 할당되는 정기적인 형식을 가지는 위임이 된다. 이 할당 관계는 매번 주기적으로 정해진 시간, 사용자, 역할을 위임하는 형식이다. 예를 들어, PDTR(T, U1, R1)이면 T의 기간에 U1에게 R1을 주기적으로 위임하게 된다. T=<-, 1700, 5>이면 할당 규칙이 생성된 이후부터 매일 17시부터 5시간 동안 위임된다. 반면에, DDTR은 기간 형식의 위임 할당으로 주어진 위임 주기가 끝나면 자동으로 위임이 회수되는 방식이다. 예를 들어 위임의 기간 T=<10.2, 1300, 24>이면 10월 2일 13시부터 24시간 동안 위임 역할에 대해 유효하게 된다. PDTR과 DDTR은 일시적이고 monotonic한 위임인 경우로 원사용자가 언제든지 회수가 가능하다. 위임자가 위임 받은 역할에 대해 악용을 하는 행위를 하는 경우에는 원사용자가 즉시 회수를 할 수가 있다.

제안 모델인 T-RBDM의 기본적인 요소들간의 정의를 살펴보면, 바탕이 되는 RDBM1의 기본 정의에 다음과 같은 정의가 추가된다.

T-RBDM의 정의

① UAPD⊆U*PDTR
② UADD⊆U*DDTR
③ PAPD⊆PDTR*P
④ PADD⊆DDTR*P
⑤ DTR=PDTR∪DDTR
⑥ PDTR∩DDTR= Ø

위의 정의를 보면 DTR을 주기적인 위임 역할인 PDTR과 기간 위임 역할인 DDTR로 분리하였고, UAPD는 U와 PDTR의 할당 관계를 표현하고 있다. 또한 PDTR로 분리된 역할은 동시에 DDTR로 분리될 수 없음을 보인다.

본 논문에서 위임은 일시적이고 monotonic한 위임으로 언제든지 회수가 가능하도록 함으로써 위임자의 역할 악용을 막고자 하였다. 또한 DTR을 PDTR과 DDTR로 구분함으로써 반복적으로 위임되는 역할을 분리하여 관리함으로써 직무자의 정기적인 출장이나 정기적인 일정에 관한 역할 위임을 관리하도록 하였다. 이는 매번 역할 위임에 대한 조건을 새로 부여할 필요 없이 한번의 조건 생성으로 정기적인 위

임과 폐지가 일어나도록 하였다.

4. 비교 분석

본 절에서는 기존의 RBAC모델인 RBAC96과 역할 위임에 관련된 모델인 RBDM0와RBDM1, 권한 위임에 관련된 모델인 PBDM을 제안 모델인 T-RBDM을 비교 분석하였다. 비교는 위임에 관련된 8개의 각 항목별로 비교하였고, 임무와 권한 분리에 있어서 모델이 각 항목을 지원하는지의 여부를 비교 분석하였다. 또한 보안 측면에서는 공통 평가 기준(Common Criteria)에서 명시하는 보안 기능 요구 사항을 기준으로 본 모델을 평가하였다.

다음의 <표 1>는 기존의 모델들과 제안 모델을 위임의 세부 항목인 8개 항목으로 나누어 비교 분석한 표이다[15]. Permanence항목에 대해서는 역할 기반 모델의 초기 모델인 RBAC96은 영구위임만을 고려하였고, RBDM0와 RBDM1은 일시적인 위임으로 언제든지 회수가 가능한 위임을 고려하였다. 또한 권한에 관한 위임 모델인 PBDM은 영구적인 위임과 일시적인 위임을 동시에 지원한다. T-RBDM은 영구적인 위임에서는 회수나 위임 단계를 고려할 필요가 없기 때문에 본 모델에서는 일시적인 위임만을 고려한다.

Monotonicity는 위임을 한 원사용자가 위임된 역할에 대한 권한을 계속 유지함으로 위임 받은 사용자의 부정행위가 발생되는 경우나 위임된 역할에 대한 역할 남용이 발생되는 경우 등 위임된 역할이 원사용자가 원하지 않는 경우로 사용되는 경우에는 언제든지 회수가 가능한 경우를 나타내는 것으로, 원사용자가 위임된 역할을 감시하는 경우가 Monotonic이고, 그렇지 않는 경우인 Non Monotonic으로 나누어진다. 즉, 원사용자의 권한이 변하지 않는 경우와 위임과 동시에 원사용자의 권한도 같이 위임되는 경우로 나누어 볼 수 있다. 기존 모델들은 모두 Non Monotonic한 방식이고, T-RBDM은 원사용자가 위임 받은 사용자의 부정행위를 방지하기 위해서 Monotonic한 위임을 한다.

Totality는 위임되는 역할이 원사용자의 역할을 모두 위임하는지 부분만을 위임하는지를 나타내는 것으로 T-RBDM은 전부 또는 부분적 위임을 모두 지원한다.

Administration는 위임의 관리를 원사용자가 하는지 다른 관리 에이전트를 두어 사용하는지는 나타내며, 부분 위임을 지원하는 경우에는 위임을 관리하는 에이전트를 두어 관리하게 된다. T-RBDM도 관리 에이전트에 의해 위임된다.

Levels of delegation은 위임을 하는 역할이 몇 단계까지 위임이 되는지를 나타내는 항목으로 한번의 위임이 진행되는 경우를 Single Step이라 하고, 한번 위임된 역할이 다른 사용자에게 다시 위임되는 경우가 한번 이상 진행되는 경우를 Multiple Step이라고 한다. 역할 기반의 위임 모델인 RBDM0와 RBDM1은 모두 Multiple Step을 지원하고, T-RBDM은 한번의 위임만을 고려함으로 Multiple Step의 경우의 Monotonic한 위임을 지원하기에는 위임의 단계가 많아지면 질수록 많은 경우를 고려해야 하므로, Multiple Step의 위임은 향후 과제로 남긴다.

Multiple delegations은 위임되는 역할을 한 단계에서 몇 명의 사용자에게 위임할 것인지를 나타내며, 위임 받는 사용자가 많은 경우에는 역할의 사용에 있어서 제약이 많이 따르게 된다. 즉, 같은 단계에서 같은 역할을 위임 받은 경우의 각 사용자간의 우선순위나 각 사용자간의 역할에 대한 권한 부여를 달리 해줘야 한다. 기존의 다른 위임 모델들은

〈표 1〉 기존 모델과 제안 모델의 위임 비교

	RBAC96	RBDM0	RBDM1	PBDM	T-RBDM
Permanence	Permanence	Temporary	Temporary	Permanence Temporary	Temporary
Monotonicity	Non-Monotonic	Non-Monotonic	Non-Monotonic	Non-Monotonic	Monotonic
Totality	Total	Total	Total Partial	Total Partial	Total Partial
Administration	Self-acted	Self-acted	Agent-acted	Agent-acted	Agent-acted
Levels of delegation	Multi-Step	Single-Step Multi-Step	Single-Step Multi-Step	Multi-Step	Single-Sep
Multiple delegation	-	-	-	-	n
Agreements	Unilateral	Unilateral	Unilateral	Bilateral	Bilateral
Revocation	-	Grant-dependency	Grant-dependency	Grant-dependency	Grant-independency

〈표 2〉 모델별 보안 요소 기능 여부

	RBAC96	RBDM0	RBDM1	PBDM	T-RBDM
접근 제어	○	○	○	○	○
인증					
부인 봉쇄	○	○	○	○	◎
기밀성	○	○	○	○	○
통신 보안					
무결성	○	○	○	○	◎
유용성	○	○	○	○	○
비밀성	○	○	○	○	△

동시에 한 사용자에게만 위임을 하고, T-RBDM은 여러 사용자에게 동시에 같은 역할을 위임할 수 있게 하고, 위임을 받은 사용자가 역할을 사용하기 위해서는 다른 사용자와 합의가 이루어진 후에 사용이 가능해 진다. T-RBDM에서 같은 역할을 할당 받은 사용자는 역할 수행에 있어서 모든 사용자간끼리의 합의가 이루어져야 하고, 같은 역할일지라도 권한을 달리 부여해줌으로써 같은 역할 간의 권한 사용의 충돌을 최소한으로 줄이고자 한다.

Agreements은 위임하고자 하는 역할에 대해 원사용자와 위임 받을 사용자간의 동의가 있는지 또는 단 방향으로 일방적으로 원사용자가 위임을 하는 지를 나타낸다. 다른 모델과 달리 T-RBDM은 원사용자와 위임 받을 사용자간의 서로 합의하에 위임이 이루어진다. 양방향동의를 통한 위임 기법을 적용하는 경우도 원사용자의 강제 위임으로 부정한 사용을 막기 위함이다.

마지막 항목으로 Revocation은 위임에 관련된 여러 항목 중 가장 많은 연구가 이루어지고 있는 분야로 위임된 역할을 어떠한 방법으로 폐지하느냐에 관련된 항목이다. 기존의 모델들은 원사용자만이 위임된 역할에 대한 폐지가 가능하고, T-RBDM은 폐지하고자 하는 역할에 대한 권한을 가지고 있는 어떠한 사용자라도 폐지가 가능하다. 이는 역할을 사용함에 있어서 부정한 방법으로 역할을 사용하는 경우에는 언제라도 폐지가 가능하도록 하기 위함이다.

위와 같이 RBAC96, RBDM0, RBDM1, PBDM과 제안 모델인 T-RBDM을 위임에 관련된 8개 항목으로 나누어 비교해보았다. 제안 모델은 전반적으로 위임에 있어서 다른 모델과 다르게 위임 받은 사용자의 악의적인 사용을 막기 위한 위임들로 Monotonic하고 Bilateral한 위임을 한다. 또한 위임 폐지에 있어서는 Grant independency한 방법으로 언제든지 위임된 역할에 대해서는 폐지가 가능한 위임을 하게 된다.

다음의 <표 2>는 보호에 관련된 모델 및 시스템이 가져야 하는 보안 요소들이다. 각 보안 요소별로 기존의 모델과 제안된 모델이 보안 요소의 기능을 보유하고 있는지의 여부를 나타낸 표이다. 접근 제어의 경우에는 각 모델들이 권한을 가진 사용자에게만 접근을 허용하는지의 유무를 나타내며, 각 모델들은 접근 제어를 위한 모델들로 모두 지원하고 있다. 인증에서는 사용자의 인증을 통해 허가되지 않은 사용자의 사용을 허용치 않는다. 모든 모델들이 인증을 받은 내부 사용자인 경우에 접근을 제어하는 방식으로, 접근 제어 모델에서 고려되는 부분이 아니다. <표 2>의 비교를 보면, 각 모델의 비해서 T RBDM이 부인 봉쇄 측면에서는 강인함을 보이고 있다. 상위 사용자에 대한 모니터링에서의 역할 사용으로 부인이 불가능하다. 또한 무결성 측면에서도 역할 사용에서 있어서 더욱 강인함을 보인다. 반면에, 비밀성 측면에서는 같은 역할을 가지고 있는 상위 사용자에는 하위 사용자의 역할 사용을 확인할 수가 있기 때문에 같은 역할의 권한을 가지고 있는 사용자간에는 정보를 공유하게 된다.

5. 결 론

본 논문은 기존의 RBAC모델에서의 역할간 위임에 있어서 위임을 받은 역할의 남용을 막기 위한 위임 모델을 제안함으로써, 역할 위임 모델들인 RBDM0, RBDM1보다도 위임된 역할에 대한 폐지를 언제든지 가능하게 하였다. 또한 권한 위임 모델인 PBDM은 권한을 분리하여 할당하는데, 제안 모델에서는 권한과 역할간의 할당 관계에서는 PBDM의 권한 분리를 그대로 반영함으로 역할과 권한간의 할당을 좀 더 세분화하였다.

비교 분석에서는 역할 기반 접근 모델의 기본이 되는 RBAC96과 역할을 위임하는 모델인 RBDM0, RBDM1, 권한을 위임하는 모델인 PBDM을 위임에 관한 8개 항목으로 비교 분석하였다. 분석에 의하면 역할이나 권한에 대해서는 더욱 제약이 많은 위임을 하도록 함으로써 사용자들간의 손쉬운 위임으로 인한 역할과 권한의 오용을 막을 수가 있다. 또한, 각 시스템들이 갖춰야 하는 보안 요소별로 비교를 하여 본 제안 모델이 부인 봉쇄과 무결성 측면에서의 강인함을 보이고 있다.

특히나, 보안 측면에서는 허가를 받은 사용자인 경우, 즉 내부 사용자에 의한 보안 취약성을 많이 나타내고 있다. 이러한 경우를 고려한 본 제안 모델은 내부 사용자끼리의 상호 견제 방식으로 내부 사용자에 대한 오용을 막을 수 있다고 본다. 본 제안 모델은 위임 받은 사용자의 권한 분실로 인한 폐지가 가능하다. 또한 위임자가 여전히 해당 역할에 대해 의존적이기 때문에 해당 역할에 대한 배타적인 권한을 가지는 위임자를 막을 수가 있다.

반면에, 본 모델을 실제 시스템에서 구현할 시에는 역할에 대하여 많은 사용자가 권한을부여 받게 되고, 위임 받은 사용자는 역할의 원사용자에게 사용에 대한 승인을 얻어야 하는 부하가 발생하게 된다. 이는 보안과 시스템 부하간의 trade off라 할수 있겠다. 그러나 이러한 시스템 부하가 전체 개발 시스템의 성능에 영향을 끼칠 경우에 대하여 부하를 줄일 수 있는 방안에 대하여 고려해야 할 것이다.

향후 연구 과제로는 일시적인 위임 역할에 대하여 위임의 단계를 여러 단계에 걸쳐 행해질 수 있도록 다단계 위임을 고려해볼 수 있다. 또한, 위임을 PKI(Public Key Infrastructure)의 전자 인증과 통합하는 방법으로 역할의 계층적 구조하에서 인증서를 위임함으로써 다단계에 걸쳐서 인증을 받을 수 있도록 할 수 있다.

참 고 문 헌

[1] R. Sandhu, J. Edward. Ciyne, L. Hal. Feinstein, and Charles E. Youman. Role Based access control models. IEEE Computer, 29(2):38-47, February, 1996

[2] L. Zhang, Gail J. Ahn and B. Chu, A Rule Based Framework for Role Based Delegation and Revocation, ACM Transactions on Information and System Security (TISSEC) archive Volume 6, Issue 3, August, 2003.

[3] O. Bandmann, M. Dam, B. Firozabadi, Constrained Delegation, Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on, pp.131-140, 2002

[4] O Canovas, Antonio F. Gomez, Delegation in Distributed Systems: Challenges and Open Issues, In Proceedings of IEEE International Workshop on Database and Expert Systems Applications (DEXA '03) September, 2003.

[5] A. Schaad, Detecting Conflicts in a Role based Delegation Model, Proceedings of the 17th Annual Conference on Computer Security Applications, p.117, December, 10-14, 2001.

[6] A. Zhand and Chu, A Rule Based Framework for Based Delegation. Proceeding of the 6th ACM Symposium on Access Control Models and Technologies, Pages 153-162, Chantilly, VA, May 3-4, 2001

[7] E. Barka, R. Sandhu, "Role Based Delegation Model/ Hierarchical Roles (RBDM1)", in Proceedings of 20th. Annual Computer Security Applications Conference, Tucson, AZ, USA, 2004.

[8] E. Barka and R. Sandhu. A Role Based Delegation Model and Some Extensions. Proceedings of 23rd National Information System Security Conference, pp.101-114, Baltimore, Oct. 16-19, 2000

[9] E. Barka and R. Sandhu. Framework for Role Based Delegation Models. In Proceedings of 16th Annual Computer Security Application conference, New Orleans, LA, December 11-15 2000, pp.168-176

[10] L. HyungHyo, L. YoungLok, N. BongNam, A New Role Based Delegation Model Using Sub role Hierarchies, International Symposium on Computer and Information Sciences (ISCIS 2003) LNCS 2869 pp.811-818 November, 2003.

[11] L. Hyun suk, K. Hyeog Man, and E. Young Ik, Reliable Cascaded Delegation Scheme for Mobile Agent Environments, WISA2003, Springer Verlag, Aug., 2003, pp.55-68

[12] R. Tamassia Danfeng Yao William H. Winsborough, Role Based Cascaded Delegation, SACMAT'04, June 2-4 2004

[13] X. Zhang, S. Oh, and R. Sandhu, PBDM: A Flexible Delegation Model in RBAC, In SAC MAT 2003, 8th ACM Symposium on Access Control Models and Technologies, June 2-3, 2003.

[14] A. Quan Pham, Privilege Delegation and Revocation for Distributed Pervasive Computing Environments, Proceedings of the Second Australian Students' Computing Conference, 2004.

[15] A. Hagstorm, S. Jajodia, Framxesco Parisi presicce, Revocation a Classification. 2001 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland. May 7-9, 2001

김 경 자

e-mail : kjkim@sejong.ac.kr
1997년 한서대학교 전산정보학과 학사
1999년 동국대학교 대학원 컴퓨터공학과 석사
2004년 동국대학교 대학원 컴퓨터공학과 박사
2005년~현재 세종대학교 컴퓨터공학과 초빙교수
관심분야 : 애드혹 네트워크, 라우팅 프로토콜, 유비쿼터스 컴퓨팅

장 태 무

e-mail : jtm@dgu.edu
1977년 서울대 전자공학과 학사
1979년 한국과학기술원 전산학과 석사
1995년 서울대 컴퓨터공학과 박사
1998년 미국 Southwest Louisana University 방문교수
1981년~현재 동국대학교 컴퓨터공학과 교수
관심분야 : 컴퓨터 구조, 병렬/분산 처리