역할의 상속성을 이용한 접근통제 시스템 설계

조아앵[O] 이경효 박익수 오병균
목포대학교 정보보호학과
{agcho[O], mediakh, ispark, obk}@mokpo.ac.kr

Design of Access Control System Using Inheritance of Roles

A-Aeng Cho[0] , kyoung-Hyo Lee, Ik-Su Park, Byeong-Kyun Oh
Dept. of Informaion Scurity, Mokpo National University

요 약

최근에 역할기반 접근통제와 역할계층에 관한 많은 연구가 이루어지고 있다. 이는 역할기반 접근통제 모델에서 역할계층은 역할과 접근허가권이 상속성을 이용하여 사용자에게 접근가능 여부를 결정할 수 있기 때문이다.

본 연구에서는 기존의 접근허가 방식보다 강력한 허가권한의 특성을 갖는 새로운 역할기반의 계층적 접근통제 모델을 제안하였다. 계층적 접근통제 구조는 역할의 상속성에 의해 접근허가 여부를 결정하는 새로운 기법의 역할기반 접근통제 모델이다.

본 연구는 제안된 모델이 어떻게 여러 보안등급에서 역할에 의해 접근통제가 이루어 질 수 있는지를 실험하였다. 실험의 결과는 일정하게 접근허가권이 실행되도록 역할을 할당함으로서 발생할 수 있는 문제점을 파악하였고, 그러한 문제를 어떻게 역할계층으로 해결할 수 있는지를 보였다.

1. 서 론

오늘날 컴퓨터와 통신의 결합으로 구성된 정보시스템은 의사결정에 필요한 정확하고 다양한 정보서비스를 실시간으로 제공함으로서 정보화 사회의 기반을 구축하고 있다. 그러나 정보시스템을 통한 정보서비스를 제공하는 과정은 여러 사용자에게 공유자원에 대한 접근을 통제함으로서 정보자원을 보호할 수 있는 방안이 필요하게 되었다. 이를 위하여 정보시스템의 데이터와 공유자원에 대한 접근통제 기법들이 국내외적으로 활발하게 연구되고 있다. 정보시스템의 자원에 대한 접근은 공유자원에 대하여 수행하는 기본적 활동으로서 접근에 관여하는 사용자의 역할에 따라 사용자를 주체(subject)와 객체(object)로 구분하며, 주체와 객체사이에 접근이 수행된다[6].

접근통제(Access control)는 공유자원에 대한 접근을 요구하는 사용자 식별과 정당성 확인 그리고 보안정책에 근거하여 접근의 승인여부를 결정함으로서 공유자원을 보호하고 관리하기 위한 기법이다[7].

접근통제의 분류는 공유자원에 대한 접근권한을 갖는 주체를 결정하는 보안정책의 설정이 주체나 주체에 소속된 그룹의 신분(Identity)에 근거하여 객체에 대한 접근을 허가하는 방법을 임의적 정책(Discretionary policy)이라 하고, 비밀성을 갖는 객체(관리자)에 의하여 공유자원에 대한 접근권한을 부여하는 방법을 강제적 정책(Mandatory policy)이라 하며, 관리자가 사용자에게 역할을 할당한 다음 그 역할에 따라 접근권한을 부여하는 방법을 비 임의적 정책(Non-discretionary policy)라 한다[12].

따라서 접근권한은 다수의 주체와 객체를 갖는 경우에 이러한 구조를 관리하기 위하여 중간수준의 통제방법을 도입하는데, 주체는 중간수준에 있는 어떤 접근방식에 따라 객체에 접근한다. 이처럼 주체와 객체의 관계를 이용하여 접근통제를 구현하는 기법으로 접근통제 매트릭스(Matrix), 접근통제 리스트(List), 자격(Capability) 등을 이용한다.

본 논문은 역할기반에서 접근권한(자격) 상속성을 이용한 접근통제의 새로운 기법을 제안하였고, 제안된 기법은 사용자에게 역할을 할당하여 접근허가권에 대한 접근계층과 상속성을 명시적으로 규정함으로서 접근통제를 수행할 수 있음을 보였다.

본 논문의 연구내용은 역할기반과 접근통제 사이의 관계를 명시적으로 규정하여 역할계층 내에서 접근권한 상속이 이루어질 수 있는 기법을 제안하였고, 제안된 기법의 연구결과는 역할기반 모델에서 사용자, 역할, 허가권한 사이의 관련성을 규명하고, 다중 보안등급 시스템에 대한 역할기반의 접근통제가 가능함을 보였다.

논문의 구성은 2장에서 역할기반 접근통제의 특성을 규정하고, 3장과 4장에서 역할의 상속성을 이용한 계층적 접근통제 시스템을 제안하고, 계층적 접근통제의 관리기법을 제시하였으며, 5장에서 결론과 제언에 대하여 기술하였다.

2. 역할기반의 접근통제

일반적으로 컴퓨터 시스템은 운영체제에 의해 다중 사용자들로부터 데이터와 공유자원을 보호하기 위하여 접근통제가 가능해야 한다. 정보시스템의 자원은 접근에 관여하는 사용자의 역할에 따라 주체(Subject)와 객체(Object)로 구분하며, 주체는 특정한 접근방식을 이용하여 객체에 접근한다.

이처럼 주체와 객체의 역할관계를 이용하여 접근통제를 구현하는 메카니즘으로 특권(접근권한)을 이용하는데, 특권은 운영체제의 중요한 기능으로서 시스템 관리, 공유자원이나 네트워크에 대한 접근활동을 통제한다. 특권은 주체(User)와 역할(Roles)의 중간계층에 상주하며, 특정한 역할을 실행할 수 있는 특권이 접근권한이다.

다음은 접근통제의 모델과 주체, 특권, 역할의 관계를 나타낸 것이다.

* 주체 --> 접근요청 --> 참조 모니터(접근여부 결정) --> 객체에 접근
* 주체(s1, s2, ...) --> 특권(중간계층) --> 역할(role1, role2, ..)

운영체제는 사전에 특권을 규정하여 제공하며, 절차의 집합체를 역할(role)이라 하고, 주체는 수행하는 역할에 따라 자신의 접근권한 여부가 결정된다.

따라서 역할기반 접근통제(Role-Based Access Control)에서는 사용자와 사용자가 수행하는 역할을 다음과 같이 규정한다[9, 13].

i) 역할은 절차의 집합체로서 사용자에게 할당되며, 사용자는 하나 이상의
역할을 수행할 수 있고, 여러 사용자가 동일한 역할을 수행할 수도 있다.

ii) 절차는 읽기나 쓰기를 위한 접근권한 이외의 접근통제 방법으로서 특정
데이터 타입의 객체에만 적용될 수 있다.

iii) 각 객체는 특정한 데이터 타입을 가지며, 데이터 타입에 정의된 절차를 통해서만 객체에 접근함으로서 접근을 통제할 수 있다. 위의 규정에 따라 역할기반의 접근통제는 정의된 절차를 통해서만 공유자원에 접근할 수 있으므로 중앙관리자는 주체와 객체의 상호관계에 의하여 주체가 객체에 접근하는 것을 통제할 수 있고, 조직 내의 역할에 의해 자원에 대한 접근 허용 여부를 결정할 수 있다.

3. 역할의 계층과 상속성

역할계층의 개념은 역할기반 접근통제의 중심적 이론으로서, 접근허가권의 관계를 나타내기 위하여 다음과 같은 계층별 기능을 규정한다[5, 6, 8].

i) 역할계층에서 상위역할은 하위역할에 할당된 접근권한을 상속한다.

ii) 역할의 계층에 의해 사용자가 접근 가능한 영역을 결정한다.

iii) 특정역할에 할당된 사용자는 하위계층에 할당된 역할을 실행할 수 있다.

위에서 규정한 역할계층은 몇 가지 문제점을 갖는 것으로 파악되었는데, 가장 중요한 문제점은 상위의 역할이 하위의 역할에 할당된 모든 접근권한에 접근할 수 있다는 것이다. 이러한 문제는 상위자가 모든 하위자의 활동을 책임지기에는 충분하지 않을 뿐 아니라 조직 내에서도 관리가 부적절하며, 상위자의 역할을 임무에 따라 분리하고 규정하기도 어렵기 때문이다. 이처럼 역할계층의 상속특성은 역할기반 기법을 사용하여 다양한 등급의 시스템 구현을 어렵게 하는데, 그 이유는 접근권한의 모든 상속이 역할계층 내에서 상향적이기 때문이다. 이러한 문제점을 해결하기 위하여 본 연구에서는 계층 내에서 접근권한의 관계를 나타낼 수 있는 새로운 계층적 접근통제 모델을 제안하였다. 새로운 모델에서는 접근권한을 계층 내에서 상위역할, 하위역할, 기타의 세 가지 부류로 구분하여 이들 중 하나에 상속시킨다. 이렇게 함으로서 접근권한은 역할을 통하여 다음과 같은 계층적 접근통제 기능을 수행할 수 있다.

i) 사용자는 역할관계로 주체들 사이의 보안등급을 생성할 수 있다.

ii) 허가권은 상속에 의하지 않고, 보안단계에 의해 획득할 수 있다.

iii) 소유권은 강제적으로 유지되는 임무분리의 형태를 배제할 수 있다.

따라서 계층적 접근통제 모델은 역할기반 접근통제의 문제점을 해결할 수 있을 뿐 아니라 다음과 같은 장점을 갖는다.

첫째, 접근허가를 결정하기 위하여 사용자의 요청에 대한 평가를 단순화할 수 있고, 둘째 강제적인 임무분리의 사용을 배제할 수 있으며, 셋째, 역할기반 접근통제를 다중 보안등급으로 구현할 수 있다.

계층적 접근통제 모델은 역할의 계층에 의해 접근을 통제하기 위하여 접근권한은 상위에 상속하고, 사용자가 수행할 역할은 하위에 상속한다. 예를 들면, 역할기반 접근통제에서 역할 R이 R' 보다 하위의 역할이라면 R에 할당된 허가권은 무조건 R' 에 할당되고, R' 에 할당된 사용자는 R을 실행할 수 있다. 역할의 계층에서 사용자의 역할과 허가권한의 관계는 다음과 같이 보다 더 구체적으로 나타낼 수 있다.

$UA \subseteq U \times R$과 $PA \subseteq P \times R$ 의 2진 관계에 의해 역할을 관련시켜 보자.

여기서, U는 사용자의 집합을 나타내고, P는 접근허가권의 집합을 나타내며, $R' < R$ 이고 $(U, R) \in UA$ 이면, 사용자 U는 역할 R' 에 할당된다.

다음에 정의한 기호표시는 이후에 기술하고 적용하기 위하여 규정한 것이다

부분 순서 X가 주어지고, $y \in Y$ 이고, $Y \in X$ 이면,

$\downarrow Y = \{x \in X : x \leq y\}$ 이고, $\downarrow Y = \{x \in X : \exists y \in Y, x \leq y\}$ 이다.

이 정의에서 사용자의 역할할당 관계는 사용자 u 에 할당된 역할의 집합은 $R(u) \subseteq R$로 표시하고, u에 할당된 역할의 집합은 $\downarrow R(u)$로 표시한다. 마찬가지로, R(p)는 허가권한 p에 할당된 역할의 집합을 나타내고, $\downarrow R(p)$는 p에 할당된 역할의 집합을 나타낸다.

4. 역할의 상속성을 이용한 접근통제 시스템

이 장에서는 역할기반의 접근통제를 실행하기 위하여 접근권한의 상속성을 적용할 수 있는 새로운 계층적 접근통제 모델을 제안하였다. 각 절은 제안 모델에서 적용할 역할과 접근권한 그리고 이들의 관계를 규정하고, 역할계층에서 역할의 할당에 의한 접근허가 기법을 기술하였으며, 이를 이용하여 보안시스템의 관리 방법을 도출하였다.

4.1 계층적 접근통제 모델의 특성

일반적으로 정보시스템은 정보보안의 기본적인 속성과 보안관계를 기술하기 위하여 속(lattice)을 이용하고, 보안정책을 구현하기 위해서는 주체와 객체에 대한 보안등급(label)을 이용한다[3, 4]. 여기서는 역할기반의 접근통제를 구현하는 보안시스템에 대하여 알아보자.

보안 시스템에서 보안등급의 선형순서만을 강조하면 제한된 보안정책만 표현할 수 있으므로 선형순서 대신에 일반적인 순서구조가 필요하다. 이를 위하여 보안등급의 부분순서(≤)는 보안등급의 집합 L의 두 원소가 선형순서만을 요구하지 않기 때문에 제한성에서 벗어날 수 있고, 주체의 보안등급이 객체의 보안등급보다 높을 때만 주체가 객체에 접근을 허용할 수 있다. 이 처럼, 서로 다른 보안등급을 갖는 두 개의 주체 또는 객체 사이에 동일한 접근을 요구하면 어떻게 등급을 정할 것인가는 속을 이용하여 해결한다.

* 속(lattice)의 정의

속 (Level, ≤)은 보안등급의 집합 Level과 부분순서(≤)로 구성되고,

임의의 두 원소 a, b∈ Level에 대하여 u∈Level 과 l∈Level이 존재한다.

속 (R, ≤)이 역할의 집합 R과 부분순서(≤)를 나타낸다면, Hasse Diagram 에 의해 역할의 계층은 2진 관계 $RH \subseteq R \times R$로 표시하고, 사용자 역할의 할당관계는 $UA \subseteq U \times R$ 로 나타낼 수 있다. 이 때, U는 사용자의 집합이다.

사용자와 역할의 관계가 $(u, r) \in UA$ 이면, 역할 r는 사용자 u에 할당되고, u는 $\downarrow r$에 의해 모든 역할이 상속된다. u에 할당된 역할의 집합은 R(u)이다.

보안시스템에서 사용자의 상호작용은 사용자 u가 할당된 역할의 부분집합 S(u)를 실행하는 작업과정으로 나타낼 수 있다. 즉, $Si(u) \subseteq \downarrow R(u)$, $1 \leq i \leq k$ 일 때, 사용자는 작업과정 S1(u), .., Sk(u) 중에서 하나를 실행한다.

4.2 계층적 접근통제 모델에서 접근허가권

접근권한(P)과 역할(R) 및 할당(A)의 관계는 $PA \subseteq P \times R$ 로 규정한다.

할당관계가 $(p, r) \in PA$ 이면, 접근권한 p는 역할 r에 할당되고, p에 할당된 역할의 집합은 R(p)로 나타낸다. 또한, o가 객체이고, mi (i =1,... k)이 접근 모드라면, 접근권한은 (o, {m1, ..., mk}) 형식으로 나타낸다.

따라서, $M \subseteq M'$에 대하여

i) $p = (o, M)$ 이고 $p' = (o, M')$ 이면 $p \leq p'$ 로 표시하고,

ii) $p \leq p'$ 이고 $p \neq p'$ 이면 $p < p'$ 로 표시한다.

계층적 접근통제 시스템의 가장 중요한 특징은 각 접근권한이 상속성을 중심으로 허용되도록 상속을 상위, 하위, 중위로 구분하고, 접근권한은 이들 중에 속하도록 한다. 즉, 접근권한 P는 P+, P−, P0로 구분하여 P+는 상위 허가권을, P−는 하위 허가권을, P0는 중위 허가권을 나타낸다.

$p \in P$ 일 때, 접근권한 p는 역할계층에서 P의 부분집합이며 수행 가능성은 RE(p)로 나타낸다. 즉, 함수 $RE : P \rightarrow P(R)$은 다음과 같이 정의한다.

$: p \in P+$ 이면 $\uparrow R(p)$

RE(p) = : p ∈ P- 이면 ↓R(p)
: p ∈ P0 이면 R(p)

위의 정의는 역할 r에 할당된 접근권한의 집합은 {p∈P : r ∈ RE(p)}이고, 접근권한 p에 할당된 역할의 집합은 간단히 RE(p)로 나타낸 것이다.

계층적 접근통제 시스템은 일반적인 역할기반 접근통제 모델로 설명할 수 있으며, 모든 접근권한은 상속성에 의해 상향적으로 허용된다.

예를 들면, S(u) ⊆ ↓R(u)로 주어진 작업과정에서 접근권한 p를 실행하기 위하여 u의 요청은 u가 p의 역할들 중 하나를 수행할 때만 인증되며, 그렇지 않을 때는 S(u) ∩ RE(p) ≠ ∅ 이다.

이상의 사실을 종합하면, 역할에 대한 접근권한의 할당은 접근권한의 허가권을 요구한 것으로서 다음 두 가지 제한조건을 만족해야한다.

<제한조건1> p<p' 이면, p와 p'는 같은 방향이거나 p'∈P0 이다.

<제한조건2> p<p' 이면, RE(p) ⊄ RE(p') 이다.

<제한조건1>은 일관성 제한조건으로서 접근권한에 대한 상속성의 방향을 일정하게 하는 조건이고, <제한조건2>는 접근권한의 중복성을 점검하는 제한조건으로서 접근권한은 많은 역할을 할당하지 못하게 하는 조건이다.

4.3 계층적 접근통제 시스템의 관리

역할에 의한 계층적 접근통제 시스템은 여러 형태의 역할을 규정해야 하기 때문에 안정적이지 못하다. 예를 들면, 역할의 할당은 부가나 제거가 가능해야 하고, 역할계층은 조직구조의 변화에 따라 갱신이 필요하기 때문이다.

즉, PA가 변하면 UA와 RH의 관계는 변화된 역할에 따라 수행하게 되는데이러한 기법을 역할기반 관리(RBA: Role-Based Administration)라 한다. RBA에서는 접근권한을 통제하기 위하여 역할이 중요한 관리 요소이다.

본 연구에서는 역할계층관리(RHA :Role Hierarchy Administration) 모델을 이용하였다. 이 모델을 선정한 이유는 RHA 모델의 관리범위가 그 어떤 모델보다도 쉽게 통합할 수 있기 때문이다.

RHA 모델은 Admin-Authority ⊆ R x R의 관계로 표현한다. 이 때, (a, r)∈ Admin-Authority 이면 a는 관리역할이고, r은 a에 의한 통제를 나타내며, C(a)는 a에 의해 통제되는 집합을 나타낸다. a에 의해 관리될 수 있는 범위가 역할계층의 부분집합이고, 역할 r이 a의 관리범위 내에 있다는 것을 σ(a) = {r∈ R : ↓r∈C(a), ↑r / ↑C(a)⊆↓r∈C(a)}로 나타낸다.

PHA 모델에서 R, UA, RH, PA 관계의 변화에 대한 합리성은 갱신해야 할 역할의 관리영역에 의해 모두 결정된다.

따라서 모든 접근권한 P는 역할 RE(p)의 집합과 관련을 갖기 때문에 접근권한의 할당을 제어하기 위하여 RHA 모델은 다음과 같은 기능을 갖는다.

* p∈P+이면 (p, r)은 r∈σ(a)에 의해 PA에 부가 또는 삭제할 수 있다.
* p∈P0이면 (p, r)은 r∈σ(a)에 의해 PA에 부가 또는 삭제할 수 있다.
* p∈P-이면 (p, r)은 ↓r⊆σ(a)에 의해 PA에 부가 또는 삭제할 수 있다.

RHA 모델은 접근권한과 역할할당의 관계를 만족하기 위하여 대칭성을 갖는 것이다. 이러한 대칭성은 관리범위에서 역할계층을 통하여 상향적 상속성을 갖기 때문이다.

5. 결론 및 제언

본 연구에서는 기존의 접근허가 방식보다 역할의 상속성에 의해 접근권한을 부여하는 새로운 계층적 접근통제 모델을 제안하였다. 제안된 모델은 역할의 계층관계에서 접근허가권 상속이 허용되는 접근통제 모델이다.

계층적 접근통제 모델에 적용된 기법은 여러 보안등급에 의해 어떻게 접근통제가 실행될 수 있는지를 실험한 결과 다음과 같은 결론을 도출하였다.

첫째, 일정하게 접근 허가권이 부여되도록 역할을 할당함으로서 발생할 수 있는 문제점을 파악하고, 그러한 문제는 역할계층을 상위역할, 하위역할, 기타로 구분함으로서 접근허가권 문제가 해결될 수 있다는 것을 보였다.

둘째, 역할기반에서 역할의 변화에 따른 접근권한의 변화를 역할계층과 역할의 상속성에 의해 접근여부를 결정할 수 있음을 알 수 있었다.

셋째, 역할기반의 접근통제는 새로운 역할을 할당하거나 제거함에 따라 역할계층의 구조에 대한 갱신이 필요함으로 이러한 문제는 RHA에 의해 해결할 수 있음을 보였다.

앞으로 역할기반의 접근통제는 다양한 역할의 규정과 역할의 범위에 따라 간단하게 역할계층구조를 변경할 수 있어야 하고, 대규모 보안 시스템의 구축을 위해서는 이 분야에 대한 더 많은 연구가 요구된다.

참고문헌

[1] Bell, D., and LaLadula, L. Secure computer systems: Unified exposition and Multics interpretation. Tech. Rep. MTR-2997, 1976.
[2] Crampton, J., and Loizou, G. Administrative scope: A foundation for role-based administrative models. ACM Trans. on Information and System Security 6, pp. 201-231. 2003.
[3] Davey, B., and Priestley, H. Introduction to Lattices and Order. Cambridge University Press, 1990.
[4] Denning, D. A lattice model of secure information flow. Comm. of the ACM 19, pp. 236-243. 1976.
[5] Ferraiolo, D., and Chandramouli, R. Proposed NIST standard for role-based access control. ACM Trans. on Information and System Security 4, pp. 224-274. 2001.
[6] Gavrila, S., and Barkley, J. Formal Specification for role based access control user/role and role relationship management. In Proceedings of Third ACM Workshop on Role-Based Access Control, pp. 81-90. 1998.
[7] Goh, C., and Baldwin, A. Towards a more complete model of role. In Proceedings of Third ACM Workshop on Role-Based Access Control, pp. 55-61. 1998.
[8] Kuhn, D. Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems. In Proceedings of Third ACM Workshop on Role-Based Access Control, pp. 23-30. 1998.
[9] Moffett, J., and Lupu, E. The uses of role hierarchies in access control. In Proceedings of Fourth ACM Workshop on Role-Based Access Control, pp. 154-160. 1999.
[10] Nyanchama, M., and Osborn, S. The role graph model & conflict of interest. ACM Transaction on Information and System Security 3, 2, pp. 3-33. 2000.
[11] Sandhu, R. Role hierarchies and constraints for lattice-based access controls. In Proceedings of Fourth European Symposium on Research in Computer Security. pp. 65-79. 1996.
[12] Osborn, S., Sandhu, R., and Munawer, Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Transaction on Information and System Security 3, 2, pp. 85-106. 2000.
[13] Sanhu, R., Coyne, E., Feinstein, H., and Youman, R., Role-based access control models. IEEE Computer 29, 2, pp. 38-47. 1996.