접근권한의 상속성을 이용한 역할계층 접근통제 모델

**양성훈° *오정현 **이경효 **임도연 **오병균
*고려대학교 컴퓨터학과 **목포대학교 정보공학부
*Jhoh@formal.korea.ac.kr **{bbs510d°, mediakh, dylm, obk}@mokpo.ac.kr

Role Hierarchy Access Control Model Using Permission Inheritance

Seong-Hoon Yand° Jung-Hyun Oh Kyoung Hyo Lee Do-Yoen Im Byeong-Kyun Oh
*Dept. of Computer Science & Engineering, Korea University
**Division of Information Engineering, Mokpo National University

요 약

기존의 역할기반 접근통제(RBAC: Role Based Access Control) 모델은 역할(R), 사용자(U), 접근권한 할당(A), 접근권한의 상속성의 관계에 의해 접근통제를 실행할 때, 하위역할에 할당된 사용자의 모든 접근권한은 상위역할에 할당된 사용자의 접근권한에 상속됨으로서 권한의 집중으로 인하여 최소권한 정책을 위배하고, 권한의 남용문제가 발생한다.

본 논문에서는 기존의 RBAC 모델에서 제기되는 문제를 해결하기 위하여 역할에 보안등급(허용등급, 허용범위)을 이용하여 접근권한의 상속성을 제한하고, 속(보안등급, 부분순서)의 이론을 적용하여 접근권한의 흐름을 통제할 수 있는 역할계층 접근통제 모델을 제안하였다.

제안한 모델은 역할의 특정영역을 지정함으로서 부분적인 역할계층을 구성할 수 있기 때문에 새로운 역할을 추가하거나 제거를 용이하게 할 수 있고, 역할의 계층구조를 간편하게 갱신할 수 있게 함으로서 다단계 보안시스템에서도 효과적으로 접근통제를 할 수 있을 뿐 아니라 대규모 보안시스템으로 확장할 수 있는 장점을 갖는다.

1. 서 론

정보 시스템(컴퓨팅 자원, 네트워크 자원, 정보 자원)은 의사결정에 필요한 다양한 정보서비스를 실시간으로 제공함으로서 정보사회를 주도하고 있다. 그러나 정보 시스템은 정보서비스를 제공하는 과정에서 많은 사용자들이 정보자원을 공유함으로서 불법적으로 공유자원에 접근하려는 보안문제들이 발생되고 있는데, 이러한 보안문제를 해결하기 위해서는 정당한 접근권한을 갖는 사용자만이 규정된 절차에 따라 자원을 활용할 수 있도록 접근을 통제하는 방안이 필요하다.

접근통제(Access Control)는 정보 시스템의 자원에 허가되지 않은 사용자에 대하여 접근을 통제함으로서 불법적인 자원의 사용, 노출, 수정 및 파괴 등을 방지하여 자원에 대한 기밀성, 무결성, 가용성을 유지한다[1, 2].

정보 시스템에서 접근통제를 실행하기 위한 절차는 첫째, 시스템 자원에 접근하는 사용자의 접근모드와 접근권한의 조건을 규정하는 접근통제 정책(policy)을 수립하고, 둘째, 접근요청을 정의된 규칙에 적용하여 불법적인 접근을 방어하는 접근통제 기법(mechanism)을 설정하여, 셋째, 시스템의 보안요구를 기능적으로 표현하는 접근통제 보안서비스 모델(model)이 구성되어야 한다[1, 3].

다음 표 1은 정보보안 시스템에서 접근통제를 위한 정책의 유형과 각 정책의 유형별 기법을 나타낸 것이다.

표 1 접근통제 정책의 유형과 각 유형별 접근통제 기법

접근통제 정책의 유형	유형별 접근통제 기법
임의적 정책 (Discretionary Policy)	신분 기반(Identity-based) 기법 사용자 기반(User-based) 기법
강제적 정책 (Mandatory Policy)	규칙 기반(Rule-based) 기법 관리 기반(Administrative) 기법
비 임의적 정책 (Non-discretionary)	역할 기반(Role-based) 기법 래티스 기반(Lattice-based) 기법

정보보안 시스템은 표 1에서 제시된 접근통제 정책을 적용하기 위여 자원에 대한 접근요청을 정의된 규칙에 의하여 불법적인 접근을 구별할 수 있는 접근통제 기법(mechanism)이 규정되어 있어야 한다.

접근통제 기법으로는 접근행렬(사용자, 권한)에서 신분을 중심으로 객체에 대한 접근을 통제하는 ACL(Access Control List) 기법, 주체가 소유할 수 있는 사용자의 자격에 의해 접근을 통제하는 CL(Capability List) 기법, 식별자, 시간제한, 주체의 식별정보 등에 대한 규칙에 의해 데이터 흐름통제가 가능한 SL(Security Level) 기법, ACL 기법을 수정한 형태로서 각 객체에 대하여 접근허가를 나타내는 비트를 사용하는 Protection Bits 기법, 분산 환경에 적합하도록 ACL, CL, SL을 통합(Integrated information)한 기법 등이 있다. 그리고, 정보보안 시스템은 정보 서비스를 제공하기 위하여 외부망의 불특정 사용자들이 접근 허가권에 근거하여 정보자원에 접근하려는 사용자(주체: subject)와 기밀성을 내포하고 있는 접근대상 자원인 객체(object) 사이에 정보서비스를 제공하는 접근통제 모델이 필요하다.

접근통제 시스템에서 역할기반 기법을 적용한 기존의 역할기반 접근통제(RBAC: Role Based Access Control) 모델은 역할, 사용자, 접근권한 할당, 접근권한의 상속성의 관계에 의해 사용자의 자원에 대한 접근을 통제한다. 이때, 하위역할에 할당된 사용자의 모든 접근권한은 상위역할에 할당된 사용자의 접근권한에 상속됨으로서 접근권한의 집중에 의한 기밀성 보호가 어렵고, 최소권한 정책을 위배함으로서 권한의 남용 문제가 발생한다[1, 3].

본 논문에서는 기존의 RBAC 모델에서 제기되는 문제를 해결하기 위하여 역할에 보안등급(허용등급, 허용범위)을 적용하여 접근권한의 상속을 제한하고, 속(lattice)의 이론을 적용하여 접근권한의 흐름을 통제할 수 있는 역할계층 접근통제 모델을 제안하였다.

제안한 모델은 역할의 특정영역을 지정함으로서 부분적인 역할계층을 구성할 수 있기 때문에 새로운 역할을 추가하거나 제거를 용이하게 할 수 있고, 역할의 계층구조를 간편하게 갱신할 수 있게 함으로서 다단계 보안시스템을 효율적으로 접근을 통제할 수 있을 뿐 아니라 대규모 보안시스템으로 확장할 수 있다.

논문의 구성은 2장에서 역할계층과 접근 허가권의 상속성에 대하여 기술하고, 3장에서 제안한 역할계층 접근통제 모델에 대하여 기술하였으며, 4장에서는 제안 모델에 대한 결론과 향후 과제에 대하여 기술하였다.

2. 역할계층과 접근권한의 상속성

2.1 역할과 역할계층

역할(role)은 조직 내에서 부여된 책임과 권한을 기술한 업무기능으로 정의하며, 역할에는 사용자가 배정되고, 사용자는 역할을 수행하기 위하여 필요한 자원에 대한 접근권한을 갖는다. 이러한 역할은 관리자가 조직 내에서 수행되는 작업기능에 따라 생성한다. 접근통제 모델은 시스템에서 부여하는 권한의 기능과 상속정도에 따라 하나의 역할을 전역공통, 지역공통, 상속제한, 고유역할의 네 가지 부역할(sub-role)로 구분한다.

역할계층(role hierarchy)은 하나의 역할을 여러 개의 부역할로 세분화함으로서 기존의 역할과 부역할 사이에 이루어지는 역할의 계층관계를 말한다. 역할계층에서 부역할 사이에 하위역할의 모든 권한은 자신의 상위역할에 상속되기 때문에 접근권한에 대한 제한조건에 의해 역할에 대한 접근권한의 흐름과 상속범위를 통제할 수 있다.

접근통제 시스템에서는 자원에 접근을 요구하는 사용자의 식별과 접근요구에 대한 정당성 확인, 자원에 대한 불법적인 접근을 감시하기 위하여 사용자에게 자격(Capability)을 부여하고, 사용자는 부여된 자격에 따라 필요한 자원에 접근하여 역할을 수행한다.

2.2 역할계층에서 접근권한의 상속성

역할계층의 개념은 역할기반 접근통제의 중심이론으로서, 접근통제 시스템의 관리자는 시스템에서 사용자의 권한(authority)과 자격(capability)에 따라 역할을 할당하고, 그 역할에 사용자를 배정한다. 이 때, 하나의 역할은 여러 개의 부역할로 세분함으로서 부역할 사이에는 계층관계가 형성되고, 하위역할에 배정된 사용자의 모든 접근권한은 그 상위역할의 접근권한을 갖는 사용자에게 상속된다.

다음은 역할계층에서 역할들 사이에 접근권한의 상속성을 규정한 것이다[1, 2, 3].

i) 상위역할에 할당된 권한은 하위역할에 할당된 권한을 포함한다.
ii) 역할계층은 각 사용자의 접근이 가능한 계층과 영역을 결정한다.
iii) 특정계층의 역할에 할당된 사용자는 그 하위계층에 할당된 역할을 실행할 수 있다.

위에서 규정한 역할계층에서 접근권한의 상속은 몇 가지 문제점을 갖는데, 가장 중요한 문제점은 상위역할에 배정된 사용자에게 접근권한이 집중됨으로서 최소권한 원칙에 위배될 뿐 아니라 상위역할 사용자는 하위역할 사용자의 모든 접근권한을 갖기 때문에 기밀성에 대한 보안유지가 어렵다. 이 처럼 역할계층에서 접근권한의 집중 문제는 모든 접근권한이 역할계층 내에서 항상 상향적으로 상속되기 때문이다

위에서 지적된 역할계층에서 접근권한이 집중되는 문제를 해결하고, 다단계 보안시스템에서 여러 사용자들 사이에 자원에 대한 접근을 통제하는 방법으로 역할(주체와 객체)에 보안등급(Security Level)을 적용한다. 이 때, 보안등급은 역할의 영역에 따라 허용등급(Authority Class)과 허용범위(Category Class)를 설정함으로서 집합의 포함관계를 이용하여 다음과 같이 역할계층에서 접근 허가권의 상속성을 정의할 수 있다.

보안등급의 집합을 SC = {A, C} (A: 허용등급, C: 허용범위)로 나타낼 때,

임의의 두 개의 보안등급의 집합 SC = {A, C}와 SC' = {A', C'}에 대하여

SC < SC' 이면 A<A' 이고 C<C'이다

다음은 역할의 계층관계를 부분순서 집합을 이용하여 접근권한의 상속관계를 규정한 것이다

부분순서 $X, y \in Y,\ Y \subseteq X$ 에 대하여

$\downarrow y = \{x \in X : x \le y\}$ 이고, $\downarrow Y = \{x \in X : \exists y \in Y,\ x \le y\}$ 이면

i) 사용자와 역할의 할당관계는 사용자 u 에 할당된 역할의 집합은 $R(u) \subseteq R$로 표시하고,

ii) u에 할당된 역할의 계층은 $\downarrow R(u)$로 표시한다.

$R(p)$는 접근권한 p에 할당된 역할의 집합을 나타내고, $\downarrow R(p)$는 p에 할당된 역할의 계층관계를 나타낸 것이다.

역할계층에서 역할에 보안등급을 적용한 역할계층 접근통제 모델은 특정계층 내에서 접근권한을 상위역할이나 하위역할 중 하나에 배정한다. 이렇게 함으로서 주체의 접근권한은 특정한 계층내의 역할을 통하여 다음과 같은 역할계층에 의한 접근통제 기능을 갖는다.

i) 사용자는 역할계층으로 주체와 객체 사이에 보안등급을 생성할 수 있다.
ii) 접근허가권은 상속에 의하지 않고, 보안계층에 의해 획득할 수 있다.
iii) 특정계층 내에서 역할의 추가 또는 제거에 따라 접근권한을 갱신할 수 있다.

기존의 역할기반 접근통제 모델들은 상위역할에 배정된 사용자에게 권한을 집중되기 때문에 최소권한의 원칙에 위배되고, 임무분리의 어려움이 야기되는 등 많은 문제점이 지적되었으나, 역할계층 접근통제 모델에서는 역할에 보안등급을 적용함으로서 기존의 문제점들을 해결할 수 있을 뿐 아니라 다음과 같은 장점을 갖는다.

첫째, 접근허가를 실행하기 위하여 사용자 요청의 평가를 단순화할 수 있고, 둘째 강제적인 임무분리의 적용을 배제할 수 있으며, 셋째, 역할계층 접근통제를 다중 보안단계로 확장할 수 있다.

2.3 역할기반 접근통제 모델

역할기반 접근통제(RBAC)는 자원에 대한 접근권한이 조직내의 책임과 자격에 따라 역할이 배정되고, 그 역할에 사용자가 할당됨으로서 역할, 사용자, 접근권한 사이의 관계를 역할계층의 구조로 표현함으로서 기존의 강제적 접근통제나 임의적 접근통제에 비하여 정교함과 유연성을 제공하는 접근통제 기법이다.

역할기반 접근통제 모델(RBAC model)은 개발 목적과 특성에 따라 RBAC0, RBAC1, RBAC2, RBAC3의 4가지 형태로 구분되는데, 각 모델의 특성은 다음과 같다.

i) RBAC0 모델

user, role, permission, session으로 구성하여 역할기반 접근통제 정책을 다양한 시스템에 적용할 수 있도록 개발된 기본적인 역할기반 접근통제 모델.

ii) RBAC1 모델 : RBAC0 + 역할계층

역할은 자격(권한)과 책임에 따라 계층적인 관계를 가지며, 상위역할은 자신의 권한 이외에 하위역할의 모든 권한을 포함하며, 상속의 범위를 제한할 수 있는 역할기반 접근통제 모델.

iii) RBAC2 모델 : RBAC0 + 제약조건

의무분리 , 역할의 개수 제한, 사용자에게 필요한 역할에 제한조건 등을 부여할 수 있는 모델

iv) RBAC3 모델 : RBAC1 + RBAC2

RBAC0, RBAC1, RBAC2 모델을 통합하여 제한조건을 계층에 포함한 역할기반 접근통제 모델.

일반적으로 역할기반 접근통제의 특성은 비 임의적이고, 사용자와 역할 및 역할과 접근허가의 관계에 의하여 편리한 관리능력을 제공하고, 추상적인 트랜잭션 개념으로 접근을 통제하기 때문에 다음과 같은 장점을 갖는다.

첫째, 권한관리(authorization management) 효율성: 사용자의 권한을 두 부분(주체와 객체)으로 나누어 논리적 독립성을 유지하기 때문에 보안관리가 단순함.

둘째, 계층적 역할(hierarchical roles) 관계: 역할에 계층을 두어 상속할 수 있게 함으로서 접근허가권 부여에 대한 관리를 단순하게 함

셋째, 최소권한(least privilege) 배정: 사용자에게 최소한의 권한만을 허용함으로서 권한의 남용을 방지하거나 예방할 수 있음.

넷째, 임무의 분리(separation of duty): 시스템 상에서 오용을 일으킬 정도의 특권이 사용되지 못하도록 사용자의 임무분리가 가능함.

다섯째, 객체에 등급(object class) 부여: 수행하는 역할에 따라 사용자를 보안등급으로 분류가 가능함. 그러나 기존의 역할기반 접근통제 모델에서 사용자, 역할, 주체 및 객체의 보안등급에 따른 접근권한의 관계를 실제로 다단계 보안시스템에 적용하기에는 무리가 있다.

본 연구에서는 사용자(user), 역할(role), 역할계층(role hierarchy), 접근권한(permission), 상속성(inheritance), 관계(relationship), 제약조건(Constraint condition)을 정립하여 접근권한 상속의 범위와 영역을 제한함으로서 보안관리자가 사용자의 접근권한을 규제할 수 있고, 확

장이 가능한 새로운 역할계층 접근통제 모델을 제안하였다.

다음 그림 1는 기존의 역할기반 접근통제에 두 가지 특성을 추가하여 제안한 역할계층 접근통제 모델이다.

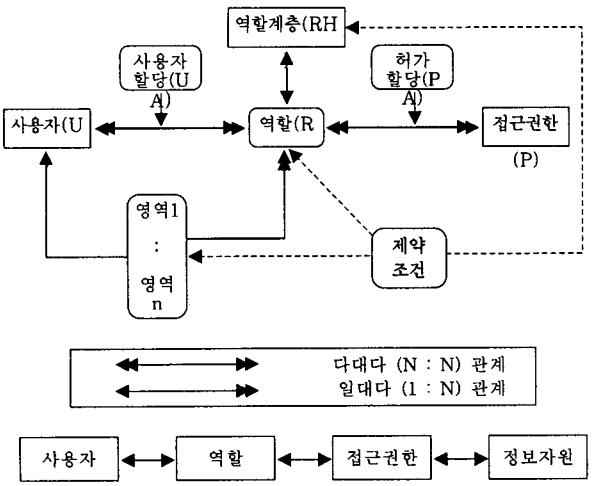

그림1 제안한 역할계층 접근통제 모델

<특성-1> 다른 역할로부터 접근권한을 상속받을 수 있는 역할계층(Role Hierarchy) 구조

<특성-2> RBAC 요소들에 보안등급(허용등급, 허용범위)을 부가할 수 있는 제약(Constraint) 조건

3. 접근권한 상속성과 역할계층 접근통제 모델

3.1 역할계층 접근통제 모델의 기본 특성

정보시스템에서 접근통제 기법은 주체와 객체에 보안등급(Security Label)을 부여함으로서 접근권한의 상속관계를 나타낼 수 있고, 속(Lattice)을 이용하여 정보흐름을 통제할 수 있다.[3] 그러나, 접근통제 모델이 보안등급에 의한 선형순서만을 지나치게 강조하면 제한된 접근통제정책만 실현하기 때문에 선형순서를 개선할 수 있는 순서구조가 필요하다. 따라서 보안시스템에 부분순서 구조(≤)를 적용하면 선형순서의 제한에서 벗어날 수 있고, 주체의 보안등급이 객체의 보안등급보다 높을 때만 주체가 객체에 접근을 허용할 수 있는 장점이 있다. 또한, 서로 다른 보안등급을 갖는 두 개의 주체 또는 객체 사이에 동시에 자원에 대한 접근을 요구하면 이들에 대한 접근통제의 흐름은 속의 개념을 이용하여 조정할 수 있다.

Lattice (Level, ≤)은 보안등급의 집합 Level과 부분순서(≤)로 구성되는데, 이는 임의의 두 원소 a, b∈Level에 대하여 최대 상한등급 u ∈Level 와 최소 하한등급 l∈Level이 존재함을 의미한다. 같은 방법으로 속 (R, ≤)을 역할의 집합 R과 부분 순서(≤)로 나타내면, 이것은 Hasse Diagram에 의해 역할의 계층관계를 $RH \subseteq R \times R$로 표시할 수 있고, 사용자와 역할의 할당관계는 $UA \subseteq U \times R$로 나타낼 수 있다.

다음은 Hasse Diagram에 의한 역할의 상속성을 나타낸 것이다.

i) 사용자와 역할의 관계가 $(u, r) \in UA$ 이면, 역할 r는 사용자 u에 할당되고, u는 $\downarrow r$에 의해 역할을 상속한다.

이 때, u에 할당된 역할의 집합은 $R(u)$로 나타낸다.

ii) 역할계층에서 사용자의 역할 수행은 u에 할당된 역할의 부분집합 $S(u)$를 실행하는 것이다.

즉, $S(u) \subseteq \downarrow R(u)$ $(1 \le i \le k)$일 때, 사용자의 역할은 $S_1(u)$, .., $S_k(u)$ 중에서 하나를 실행할 수 있다.

3.2 역할계층 접근통제 모델에서 접근허가권

역할계층에서 접근권한(P)과 역할(R) 그리고 할당(A)의 관계를 집합을 이용하여 $PA \subseteq P \times R$ 로 나타낼 때, 할당관계 $(p, r) \in PA$ 에 대하여 접근권한 p는 역할 r에 할당되고, p에 할당된 역할의 집합은 $R(p)$로 나타낸다. 또한, 객체 o의 접근 모드가 m_i(i =1,... k) 이면, o의 접근권한은 $(o, \{m_1, ..., m_k\})$으로 나타낸다.

즉, 접근모드 $M \subseteq M$에 대하여

i) $p = (o, M)$ 이고 $p' = (o, M)$ 이면 $p \le p'$ 관계가 성립하고,

ii) $p \le p'$ 이고 $p \ne p'$ 이면 $p < p'$ 관계가 성립된다.

역할계층 접근통제 모델의 가장 중요한 특징은 각 접근권한이 상속성을 중심으로 허용되기 때문에 특정계층 내에서 접근권한은 상위권한, 하위권한, 중위권한으로 구분하여, 접근권한이 이들 사이에서 상속되도록 한다. 즉, 접근권한 P는 P^+, P^-, P^0로 구분하여 P^+는 상위 허가권을 나타내고, P^-는 하위 허가권을 나타내며, P^0는 중위 허가권을 나타낸다.

함수 $R_E : P \rightarrow P(R)$은 다음과 같이 접근권한의 상속관계를 정의한다.

$$R_E(p) = \begin{cases} : p \in P^+ \text{ 이면 } \uparrow R(p) \\ : p \in P^- \text{ 이면 } \downarrow R(p) \\ : p \in P^0 \text{ 이면 } R(p) \end{cases}$$

위의 정의에 의하여 역할 r에 할당된 접근권한의 집합은 $\{p \in P : r \in R_E(p)\}$로 나타내고, 접근권한 p에 할당된 역할의 집합은 $\{R_E(p)\}$로 나타냄으로서 역할계층 접근통제 모델은 일반적인 역할기반 접근통제 모델에서도 설명이 가능하며, 모든 접근권한은 상속성에 의해 사용자(U)-역할(R)-할당(A)의 흐름은 통제할 수 있다.

예를 들면, $S(u) \subseteq \downarrow R(u)$로 주어진 역할의 수행과정에서 접근권한 p를 실행하기 위하여 u의 요청은 u가 p의 역할들 중 하나를 수행할 때만 인증되며, 그렇지 않을 때는 $S(u) \cap R_E(p) \ne \varnothing$이다.

따라서, 역할계층 접근통제 모델에서 역할에 의한 접근권한의 할당은 다음 두 가지 제한조건을 만족해야한다.

<제한조건1> $p < p'$ 이면, p와 p'는 같은 방향이거나 $p' \in P^0$ 이다.

<제한조건2> $p < p'$ 이면, $R_E(p) \not\subset R_E(p')$ 이다.

<제한조건1>은 일관성 제한조건으로서 접근권한에 대한 상속성의 방향을 일정하게 하는 조건이고, <제한조건2>는 접근권한의 중복성을 점검하는 제한조건으로서 역할의 접근권한을 중복하여 할당하지 못하게 하는 조건이다.

4. 결론 및 향후 연구과제

정보시스템에서 자원에 대한 접근은 사용자의 기본적인 활동이며, 사용자의 자원에 대한 접근을 효율적으로 통제하는 것은 보안기술의 가장 중요한 영역이다.

본 연구에서는 특정계층 내에서 역할의 주체와 객체에 보안등급(허용등급과 허용범위)을 부여함으로서 접근권한의 상속성과 정보흐름을 통제할 수 있는 개선된 새로운 역할계층 접근통제 모델을 제안하였다. 제안된 역할계층 접근통제 모델은 특정 역할계층에 보안등급(허용 등급, 허용 범위)을 적용하여 접근권한의 상속성을 표현할 수 있고, 속(lattice)의 개념을 이용하여 역할(R)-사용자(U)-접근권한 할당(A)의 관계를 정형화된 문장(formal statement)으로 표현함으로서 다단계 보안시스템에서 효율적으로 접근을 통제할 수 있다.

앞으로의 과제는 다양한 역할과 역할범위의 변화에 따라 역할계층 구조를 간편하게 갱신하여 관리할 수 있는 기법 개발과 대규모 다단계 보안시스템을 구성하여 접근을 통제하는 모델개발의 연구가 요구된다.

참 고 문 헌

[1] 이용, 김용민, 이형효, 진승현. "권한상속 기능을 제공하는 역할계층 모델". 정보보호학회 논문지, 13권 4호, pp. 37 - 45. 2003. 8.

[2] 이상하, 조인준, 천은홍, 김동규. "역할기반 접근통제에서 역할계층에 따른 접근권한 상속의 표현", 한국정보처리학회 논문지, 7권 6호, pp. 3-13. 2000. 6

[3] 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.