제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

능동적 역할 할당과 수동적 역할 할당을 수행하는 역할 할당 프로토콜의 설계 및 구현

나 상 엽*, 김 점 구*
* 남서울대학교 컴퓨터학과

요 약

역할-기반 접근 통제 모델은 역할을 정의하고 역할이 수행할 수 있는 접근 권한을 명시하여 사용자에게 미리 정의되어진 역할을 부여하므로 사용자는 자신에게 할당된 역할에 의하여 시스템 내부의 객체에 접근하게 된다. 따라서 조직이나 기업은 각각의 특성에 적합한 접근통제 정책을 일관성 있게 유지할 뿐 아니라 주체와 자원의 접근 권한 관계를 독립적으로 유지하므로 접근 권한이 변경될 때 새로운 권한을 사용자가 아닌 역할에만 적용하면 되므로 복잡한 보안 정책을 추상화 하여 효율적으로 관리할 수 있는 장점을 가진다. 역할-기반 접근 통제 모델에 존재하는 역할 간의 계층 관계에 의하여 상위 역할은 하위 역할의 권한을 수행 할 수 있지만 반대의 경우는 허가 되지 않는다. 본 논문에서는 이러한 문제를 해결하기 위하여 동적 역할 할당을 정의 하였으며, 이를 통하려 하위 역할이 일시적으로 상위 역할이 가지는 권한을 수행할 수 있는 방법을 제시하며 동적 역할 할당의 방법을 자신이 다른 역할의 권한을 할당받는 능동적 역할 할당과 다른 사용자의 요청에 의하여 역할 할당이 이루어지는 수동적 역할 할당을 정의하고 이를 수행하기위한 역할 할당 프로토콜을 제시 역할 할당의 여부를 판단하는 역할 할당 서버를 구현 하였다.

Design and Implementation of Role Assignment Protocol for Active Role Assignment and Passive Role Assignment

SangYeob Na*, JeomGoo Kim*

ABSTRACT

In distributed-computing environments, there is a strong demand for the authentication and the access control of distributed-shared resources. I have presented role-based access control (RBAC) concept that is in the spotlight recently. RBAC model shows the standardized access control of complicated organization's resources. In RBAC, senior role has junior role's permission by virtue of role hierarchy. But, junior role cannot perform the permission, which is granted to the senior or other role groups. Inheritances of permissions in role hierarchies are static. In order to tackle this problem, I propose a dynamic role assignment, which classified into passive role assignment and active role assignment, and design dynamic role assignment protocol and implement role assignment server.

1. 서 론

정보 시스템의 취약성을 공격하여 시스템에 보안 문제를 야기하는 원인은 여러 가지가 존재하지만 정보의 무결성 침해(Integrity Violation), 정보 누출(Information Leakage), 그리고 서비스 거부(Denial of Service) 같은 위험 요소들이 대표적인 경우이다[6].

위와 같은 정보의 안전성에 대한 위험 요소에 대응하여, 정보 보호는 정보의 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 등을 보장하고, 정보시스템의 내부 또는 외부 침입자들로 인한 정보의 파괴, 변조, 불법 유출 등의 행위로부터 정보를 보호하는 것을 의미한다.

최근의 클라이언트-서버(Client-Server) 분산 컴퓨팅 환경에서는 여러 사용자가 상호 작용을 통하여 기업이나 조직의 기능을 수행하고 서로의 자원을 공유하며 보다 효율적으로 작업을 수행한다. 분산 컴퓨팅 환경에서 공유하는 자원이나 정보가 증가함에 따라 허가되지 않은 정보의 접근이 발생하고 정보의 불법적인 사용으로 인한 정보의 누출이 발생한다. 따라서 분산 컴퓨팅 환경의 정보를 보호하기 위하여 사용자의 인증이나 사용자의 작업에 대한 접근 통제 정책을 통한 정보 보안의 필요성이 증가하고 있으며 이러한 접근 통제 정책은 시스템 사용의 편리성을 위하여 응용프로그램이나 사용자의 작업을 방해하지 않고 투명하게 제공되는 것을 목적으로 한다[5].

많이 사용되어지는 접근 통제 정책은 강제적 접근 통제(Mandatory Access Control : MAC), 임의적 접근 통제(Discretionary Access Control : DAC), 그리고 역할-기반 접근 통제(Role-Based Access Control : RBAC)로 나누어진다[2][7][8]. 강제적 접근 통제 정책은 정보의 보안등급과 사용자나 그가 속한 그룹에 의하여 접근을 통제하는 방식이고 임의적 접근 통제 정책은 해당 정보의 소유자에 의하여 접근 통제 관계가 정의되는 방식이다. 마지막으로 역할-기반 접근 통제 정책은 시스템 내에 필요한 역할(Role)과 그 역할이 수행할 수 있는 권한(Permission)을 정의하고 각 사용자에게 역할을 할당함으로써 각 객체의 접근을 통제하는 방식이다[6][7].

역할-기반 접근 통제의 경우 미리 정의된 역할, 역할이 수행할 수 있는 접근 권한(Permission)을 명시하고 사용자에게 역할을 부여하므로 사용자는 자신에게 할당된 역할에 의하여 객체를 접근할 수 있다. 따라서 조직은 조직의 특성에 적합한 접근통제 정책을 일관성 있게 유지할 수 있을 뿐 아니라 주체와 자원의 접근 권한 관계를 독립적으로 유지하므로 접근 권한이 변경될 때 새로운 권한을 사용자가 아닌 역할에만 적용하면 되고 복잡한 보안 정책도 추상화하여 효율적으로 관리할 수 있다[1][7].

역할-기반 접근 통제에서 역할은 조직 내에서 객체에의 접근이 허가된 권한과 책임들의 집합으로 볼 수 있다[1]. 역할-기반 접근 통제에서 각각의 역할은 조직의 접근 정책에 따라 다른 역할과의 상관관계를 가지고 계층구조로 표현되며 상위 역할은 하위 역할의 권한을 상속(Inheritance) 받는다[7][8]. 이 경우 하위 역할이나 계층구조로

포함되지 않은 역할은 상위 역할이 가지는 권한을 수행할 수 없는 문제가 있다. 본 논문에서는 동적 역할 할당을 통하여 하위 역할이 일시적으로 상위 역할이 가지는 권한을 수행할 수 있는 방법을 제시하며 역할 할당의 방법을 자신이 다른 역할의 권한을 역할 할당받는 능동적 역할 할당과 다른 사용자에게 역할의 역할 할당을 수행하는 수동적 역할 할당으로 구분한다. 또한 역할 할당의 결정을 내리는 역할 할당서버와 역할 할당을 위한 간략화 한 역할 할당 프로토콜을 제시한다. 최근의 역할-기반 접근 통제는 의료기관의 정형화된 모델을 제시하기 위한 연구가 활발하므로[9] 이 논문에서 사용하는 예도 이를 이용하도록 한다.

본 논문의 구성은 2장에서 역할-기반 접근 통제의 정의와 제시하는 모델을 설명하고, 3장에서는 능동적 역할 할당과 수동적 역할 할당의 정의, 능동적, 수동적 역할 할당의 개념과 정의, 이를 수행하기위한 프로토콜과 역할 할당 서버에 대하여 설명하고 4장에서 결론 및 향후 연구를 기술한다.

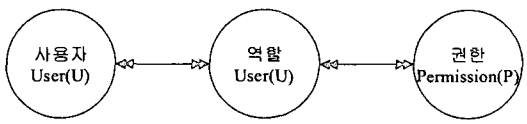
2. 역할-기반 접근 통제 모델

접근 통제 정책(Access Control Policy)은 식별 또는 인증된 사용자가 허가된 범위 안에서 시스템 내부 정보로의 접근을 허용하는 방법을 기술한다. 사용자는 자신이 가진 접근 허가권에 의하여 정보에의 접근이 허가 또는 거부된다. 이때 사용자는 주체(Subject)가 되고 사용자가 접근을 원하는 정보는 객체(Object)가 된다. 객체는 사용자가 가지는 권한에 따라 접근이 허용되므로 동일한 객체라도 역할에 따라 수행할 수 있는 연산은 달라진다.

기존의 임의적 접근 통제의 경우 객체는 사용자가 소유하게 되고 객체의 소유자는 객체의 모든 접근 권한을 가지고 다른 사용자에게 임의로 접근 정책을 부여하고 강제적 접근 통제는 조직 내의 관리자가 객체의 중요도에 따라 접근 권한을 사용자에게 할당하여 준다. 이에 비해 역할-기반 접근 통제에서는 시스템 관리자가 역할에 접근 권한을 부여하고 사용자는 자신의 책임과 권한에 따라 역할을 부여받으므로 복잡한 조직의 형태를 보다 효율적으로 표현할 수 있다[8].

2.1 역할-기반 접근 통제 개념

역할-기반 접근 통제에서 역할은 조직 내에서의 권한과 의무의 집합으로 시스템 관리자에 의하여 사용자에게 할당된다. 이는 [그림 1]로 표현되며[6] 역할에는 필요에 따라 권한이 부여되거나 삭제될 수 있다. 역할-기반 접근 통제 모델의 기본 구성요소로는 사용자(User), 역할(Role), 그리고 권한(Permission)등이 있다.



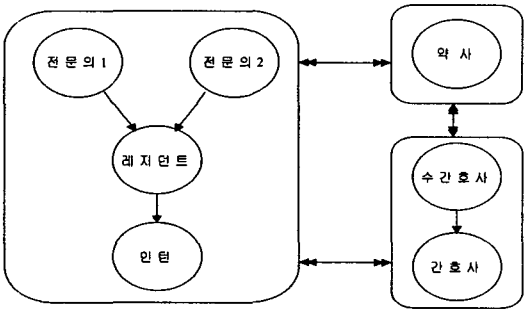
[그림 1] 역할-기반 접근 통제의 기본 모델

사용자는 시스템내의 응용프로그램이나 사람을 나타내고, 역할은 조직 내에서 권한과 의무를 가지는 직위를 표현한다. 권한은 역할이 하나 이상의 객체에 접근할 수 있는 방법을 나타내며 의무, 허가 등으로 세분화되어지며[1] 역할도 특정 기능을 가지는 객

체로 표현된다. 행위는 역할이 특정 객체에 수행할 수 있는 연산의 집합으로 표현된다. 역할-기반 접근 통제에서 사용자는 하나 이상의 역할에 할당되며 사용자는 자신에게 할당되어진 역할이 가지는 권한에 따라 객체에 연산을 수행한다. 역할-기반 접근 통제에는 사용자-역할(UA) 관계, 역할-권한(RP) 관계, 역할-역할(RR)의 관계가 존재한다.

2.2 역할과 역할간의 상관관계 (Role-Role Relationship)

역할-기반 접근 통제 모델에서 역할은 조직 내에서 역할의 책임과 권한 등에 따라 계층구조(Hierarchical Structure)로 표현되며 유사한 권한을 가지는 역할들은 그룹으로 관리된다[5]. 그룹은 역할의 관리를 위하여 조직 내의 관리자나 조직의 구성에 의하여 분리된다. 역할은 역할 그룹 내 역할 계층구조에서 역할의 위치에 따라 상위 역할과 하위 역할로 구분되며 상위 역할은 하위 역할의 권한을 가지는 상속관계와 다중 상속 관계도 성립한다. 또한 서로 이웃하는 역할 그룹 간에 연산관계도 존재한다[4].



[그림 2] 역할 그룹과 그룹 내의 상속관계, 그리고 그룹간의 연산 관계

[그림 2]의 경우에서처럼 병원 조직의 의사 그룹 내의 인턴이 가지는 환자에 대한 권한은 상위 역할인 레지던트와 전문의에게 상속되며 의사 그룹과 간호사 그룹 그리고 약사는 상호간에 연산관계가 존재한다.

2.3 역할과 권한의 상관관계 (Role-Permission relationship)

역할은 역할이 조직 내에서 수행해야 하는 임무에 따라 권한을 할당 받게 된다. 권한은 의무와 허가로 나뉘는데 의무는 해당 역할이 반드시 수행하거나 하지 말아야 하는 연산의 집합이고 허가는 역할에게 허용되거나 허용되지 않은 연산의 집합이다. 의무와 허가의 표현은 [4]에서 정의한 방법을 사용하도록 한다.

{식별자, 모드, 역할, {행위}, 대상, 조건, 예외}
[모드] o : 의무(Obligation),
a : 허가(Authorization)
+ : positive, - : negative

예를 들어 "간호사는 매일아침 8시 환자의 상태를 체크하여야 한다"라는 의무는 {np1, o+, 간호사, {체크}, 환자, 매일08:00, -}와 같이 표현될 수 있다.

역할 그룹	권 한
의 사	{dp1, a+, 전문의, {read, fix}, 차트by인턴, -,-}
	{dp2, a-, 인턴, {조제}, 약, -, 응급}
간 호 사	{np1, o+, 수간호사, {배정}, 간호사-환자, 매일09:00,-}
	{np2, a+, 간호사, {주사by차트}, 환자, 매일12:00, -}
약 사	{drp1, a+, 약사, {조제by차트}, 환자 , -, -}
	{drp2, o+, 약사, {수량정리}, 사용한약, 매일퇴근시, -}

[표 1] 역할-권한 관계 모델

본 논문에서 사용하게 되는 역할-권한 관계의 예는 [표 1]과 같다.

3. 능동적 역할 할당과 수동적 역할 할당 프로토콜

역할 계층이 가지는 상속성에 의하여 상위 역할은 하위 역할의 권한을 묵시적으로 수행할 수 있으므로 본 논문에서는 상위 역할의 권한을 하위 역할이 일시적으로 수행하기 위한 동적인 역할 할당을 제안하였다. 동적인 역할 할당은 능동적 역할 할당과 수동적 역할 할당으로 구분하였다. 능동적 역할 할당과 수동적 역할 할당은 역할 할당을 요청하는 역할 할당자와 역할 할당을 받는 수여자의 동일 주체 여부에 의하여 구분되는데, 역할 할당자와 수여자가 동일한 주체일 경우를 능동적 역할 할당으로 정의하고, 역할 할당자와 수여자가 다른 객체일 경우를 수동적 역할 할당으로 정의한다. 능동적 역할 할당은 자기 자신에게 부정 책임 모드(a-)로 부여된 권한을 긍정 책임 모드로 바꾸어 수행할 수 있도록 하는 방법이고, 수동적 역할 할당은 역할 할당을 요구하는 역할 할당자의 임의적 판단에 근거하여 역할 할당을 요청하고 수여자는 역할 할당 서버에 의하여 새로운 역할을 부여받아 해당 역할의 권한을 수행하는 형태이다.

3.1 능동적 역할 할당 프로토콜(Active Role Assignment Protocol)

능동적 역할 할당은 역할 할당을 요청하는 역할 할당자와 역할 할당의 결과 새로운 역할을 부여받는 수여자가 동일한 주체인 경우로, 자기 자신에게 부정 책임 모드(a-)로 부여된 권한을 수행할 수 있게 하는 방법이다. 능동적 역할 할당은 역할에 부여된 권한들 중에 예외 상황과 부정 책임 모드를 가지고 있고 권한에 대하여서만 수행 가능하다. 자신에게 부정 책임 모드로 부여된 권한을 가지고 있는 역할은 해당 권한을 수행하기 위한 예외 상황이 발생하기 전까지는 부정 모드의 권한은 수행 할 수 없다. 예외 상황이 발생하여 부정 모드의 권한을 수행해야 하는 역할이 역할 할당 서버에게 역할 할당요청을 하면 역할 할당 서버는 역할 할당 여부를 판단하여 역할 할당이 가능한 경우 부정 책임 모드의 권한을 긍정 모드로 전환함으로써 권한을 수행할 수 있게 하여준다. 따라서 시스템 내에서 부정 책임 권한을 가지고 있는 역할이 동적으로 자신에게 새로운 권한을 동적으로 부여하여, 명시된 예외 상황 발생시에 자신의 역할을 계속 하여 수행하는 역할 할당 방법이다.

[표 1]에서 제시된 역할-권한 관계 모델에서 의사 그룹과 간호사 그룹은 약을 조제하는 권한이 주어지지 않는다. 의사 그룹 중 인턴의 경우 역할-권한 관계 내에 **{dp2, a-, 인턴, {조제}, 약, -, 응급}** 권한을 가지고 있으며, 예외 조건(응급)이 명시되어 있으므로 예외 조건이 만족하는 경우 모드 a- 는 a+로 변환되어 약사의 역할을 할당받을 수 있다. 또한 의사 그룹에서 인턴의 상위 개념인 레지던트, 전문의의 경우 하위 역할의 권한을 상속받으므로 예외조건이 만족하면 약사 역할이 가지는 권한을 수행할 수 있다.

3.2 수동적 역할 할당 프로토콜(Passive Role Assignment Protocol)

수동적 역할 할당은 역할 할당을 요청하는 역할 할당자와 수여자가 서로 다른 주체로, 수여자는 역할 할당자의 역할 할당 요

청에 의하여 새로운 역할을 동적으로 부여받아 그 역할을 수행하게 된다.

[그림 2]에서 의사 역할을 가지는 사용자가 간호사에 약사의 역할이 필요하다고 판단되면 동적 역할 할당 서버에게 {의사, 약사, 간호사, 응급}의 동적 역할 할당 메시지를 전송하고 역할 할당 서버는 동적 역할 할당의 여부를 판단하여 역할 할당 메시지를 의사에게 전달한다. 의사는 역할 할당 서버로부터 받은 역할 할당 메시지를 간호사에게 전달하여 간호사가 제한된 시간동안 약사의 역할을 수행할 수 있도록 한다.

임의적 접근 통제 정책은 자신에게 할당된 권한의 임의 역할 할당이 가능 하지만, 역할-기반 접근 통제 정책은 비임의적 접근 통제 정책이므로 시스템 보안 관리자만이 역할-권한 관계의 설정을 변경할 수 있다. 수동적 역할 할당에서 역할 할당을 요구하는 역할 할당자는 역할이 할당되는 역할, 역할 할당을 받는 역할, 그리고 역할 할당이 발생하여야 하는 조건을 명시하여 역할 할당 서버에게 역할 할당을 요청한다. 역할 할당 서버에 의하여 역할 할당이 허가되는 경우 역할 할당을 받은 수여자는 역할 할당 서버에 의하여 부여된 자신의 새로운 역할을 이용하여 필요한 권한을 수행하는 방식으로, 역할 할당의 요청은 역할 할당자의 임의적 판단에 근거하므로 기본적으로 비임의적 접근 통제 방식인 역할-기반 접근 통제 모델에 임의적으로 권한을 역할 할당하는 요소를 추가한 형태이다.

수동적 역할 할당의 경우 역할-권한 관계에 대상 역할의 권한이 명시되지 않은 경우인데 이러한 경우에는 역할-역할 관계에 의하여 동일 그룹 내에서 상위 역할의 권한을 하위 역할이 동적으로 할당받거나 그룹간의 연산관계에 의하여 다른 그룹의 역할에 권한을 동적으로 할당하는 경우이다. 이때는 그룹간 연산 관계에 존재하는 제약 조건이나 역할의 자격(qualification) 존재 여부 등에 의하여 역할 할당 여부가 결정된다.

4. 결론

본 논문에서는 현재 활발한 연구가 진행되고 있는 역할-기반 접근 통제 개념을 살펴보고 이의 간단한 모델을 정의하였다. 역할-기반 접근 통제 모델의 경우 복잡화된 조직의 접근 통제를 정형화하여 표현할 수 있으며 접근 통제 정책의 변화 시에 사용자-권한의 변환이 아닌 역할-권한의 관계를 수정하면 되므로 정책 변환에 보다 융통성 있게 적용할 수 있다. 그러나 역할의 계층 구조에 의한 권한의 상속이 정적이고 조직 내의 상호 작용에서 역할이 갖지 않는 권한에 대한 연산을 수행할 필요가 있는 경우 기존의 역할-기반 접근 제에 모델에는 적용하기 어려운 문제가 발생한다.

본 논문에서는 이러한 문제를 해결하기 위하여 일시적으로 필요한 역할을 수행하기 위한 역할 할당 프로토콜과 역할 할당 여부를 결정하는 역할 할당 서버를 제시하여 이를 해결하였으며 동적 역할 할당을 능동적 역할 할당과 수동적 역할 할당으로 분리하여 적용하였다.

역할-기반 접근 통제 정책은 비임의적 접근 통제 정책이므로 시스템 보안 관리자만이 역할-권한 관계의 설정을 변경할 수 있

다. 그러나 본 논문에서 제시하는 수동적 역할 할당에 의하여 수여자가 새로운 역할을 수행하는 경우 역할 할당의 요청이 역할 할당자의 임의적 판단에 근거하므로 기본적으로 비임의적 접근 통제 방식인 역할-기반 접근 통제 모델에 임의적으로 권한을 역할 할당하는 요소를 추가한 형태로 시스템 수행 중에 동적으로 역할을 할당받아 해당 권한을 수행하게 함으로서 역할-기반 접근 제어 정책의 역할 계층 구조에 의한 정적으로 표현되는 역할 상속을 해결할 수 있고, 조직 내에서 역할들의 상호 작용에서 역할에 부여되지 않은 권한을 수행하여야 하는 경우 동적 역할 할당을 통하여 필요한 권한을 부여해주는 방법을 제시하였다.

참고문헌

[1] E. C. Lupu, D. A. Marriott, M. S. Sloman, and N. Yialelis, "A Policy Based Role Framework for Access Control", First ACM/NIST Role Based Access Control Workshop, Dec, 1995

[2] Department of Defence(USA), Department of Defence Trusted Computer System Evaluation Criteria, DoD 5200-78-STD, DoD, 1985

[3] L. Giuri, "Role-Based Access Control in Java", 3rd ACM Role-Based Access Control Workshop, 1998.

[4] E. C. Lupu, M. S. Sloman, "A Policy Based Role Object Model", Proceeding of IEEE EDOC'97, Oct, 1997.

[5] N. Yialelis, M. S. Sloman, "A Security Framework Supporting Domain Based Access Control in Distributed Systems", ISOC Symposium on Network and Distributed System Security(SNDSS96), Feb 1996

[6] David F. Ferraiolo and Richard Kuhn, "Role-based access control," Proceedings of the 15th NIST-NSA National computer security conference, 1992

[7] Ravi S. sandhu, Edward J.Coyne, Hal L. Feinstein and Charles E. Youman, "Role_-Based Access Control Models," IEEE computer, Volume 29, number 2, Feb 1996

[8] David F. Ferraiolo, J. Cugini and Richard Kuhn, "Role-Based Access Control: Features and Motivations," National Institute of standards and technology, 1995

[9] J. Barkley, "RBAC in Health Care", 1995 http://hissa.ncsl.nist.gov/rbav/

[10] C. Goh, A. Baldwin, "Towards a more Complete Model of Role", 3rd ACM Role-Based Access Control Workshop, 1998.

나 상 엽

동국대학교 전자계산학과 공학사
동국대학교 컴퓨터공학과 공학석사
동국대학교 컴퓨터공학과 공학박사
(주) 일은시스템
현재 남서울대학교 컴퓨터학과교수
<관심분야> 정보보안, 모바일 컴퓨팅, Electrinic Commerce

김 점 구

광운대학교 전자계산학과 이학사
광운대학교 전자계산학과 이학석사
한남대학교 컴퓨터공학과 공학박사
(주) 제성프로젝트 연구원
(주) 시사컴퓨토피아인터넷사업 본부장
현재 남서울대학교 컴퓨터학과교수
<관심분야> 정보보호, 컴퓨터 네트워크, 무선통신