전자영사시스템의 접근제어 모델 구현에 관한 연구

이경희*, 최진영**
*고려대학교 컴퓨터정보통신대학원 디지털정보공학과
**고려대학교 컴퓨터학과
e-mail: *forkhlee@empal.com **choi@formal.korea.ac.kr

A Study on Implementation of Access Control Model in e-Consul System

Kyoung-Hee Lee*, Jin-Young Choi**
*Dept. of Digital Information Engineering, Graduate School of Computer & Information Technology, Korea University
**Dept. of Computer Science and Engineering, Korea University

요 약

정보시스템에서 자원에 대한 접근 통제는 핵심 보안기술의 하나다. 최근에는 역할을 중심으로 접근을 제어하는 RBAC모델이 웹 어플리케이션에 널리 활용되고 있으나, 대규모 기업이나 분산 환경 조직에서는 다수의 사용자, 역할과 상호관계로 인해 관리에 상당한 노력이 요구되고 있다. 본 논문에서는 조직의 구조를 반영한 역할 관리 모델(OS-RBAC)을 기반으로 사용자와 역할과의 할당 관계에 그룹(Groups)이라는 개념을 추가한 전자영사시스템의 접근제어 모델을 구현함으로서 역할관리의 효율성을 제고하였다.

1. 서론

전자영사시스템(이하 e-Consul) 은 재외공관에서 여권·사증의 발급, 재외국민 등록, 공증·호적사무, 해외 사건사고 기록관리, 사법서류의 송달 등의 다양한 영사업무를 처리하기 위해 개발된 웹 기반의 온라인 시스템이다. 업무 프로세스 중심의 시스템에서 서비스의 접속은 곧 업무처리 책임 및 권한을 의미하며, 시스템에서 다루어지는 행정정보에서부터 개인정보까지의 다양한 정보는 보호를 필요로 한다. 모든 업무가 정보시스템에 의해 처리 되면서 다중 프로그램과 다중 사용자에 의해 다루어지는 정보시스템의 접근 통제(Access Control)는 핵심 보안 기술의 하나로 많은 연구가 이루어져 왔다[4][6]. 역할기반 접근제어(RBAC) 모델은 e-Commerce, e-Government 등과 같은 웹 어플리케이션에서 필수적으로 요구되는 웹에서의 정보보호를 제공하기 위한 가장 적합한 기법으로 알려져 있으며, 이는 사용자와 서비스에 대한 접근권한간의 관계성을 역할(권한그룹)이라는 추상화된 개념을 적용하여 유연한 접근 통제를 가능하게 해 준다.

접근 통제 정책은 조직의 환경과 밀접한 관련이 있다. 특히 관리해야 하는 사용자와 역할의 수가 많은 대규모 기업이나 분산 환경 조직에서는 다수의 보안 관리자가 접근 제어를 관리한다. 이러한 분산 관리를 제공하기 위해 여러 RBAC 관리모델들이 제안 되었으나[1][2][5][7], 역할 관리를 위한 관리역할(Administration Role)의 선행조건과 역할범위를 추가로 관리하여야 함에 따라 실제 조직에서의 적용이 용이하지 않다. 본 논문에서는 실제 조직 환경을 보다 효과적으로 반영할 수 있는 관리 모델인 OS-RBAC [3] 에 그룹(Groups)이라는 개념을 추가하여 사용자와 역할과의 할당 관계를 편리하게 관리할 수 있는 시스템을 구현하였다.

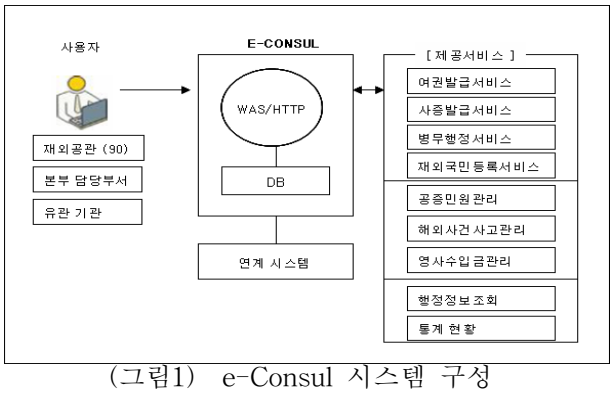
본 논문의 구성은 다음과 같다. 2장에서는

RBAC 관리 모델에 대한 관련 연구에 대해 살펴보고, 3장에서는 본 논문에서 제안한 역할기반 접근통제 모델을 설계 및 구현하며, 끝으로 4장에서는 본 연구에 대한 결론을 맺는다.

2. 관련연구

2-1. e-Consul 개요

e-Consul 은 한국의 본부에 설치되어 있고, 90여개의 전 세계에 분포한 재외공관에서 전용망을 통하여 접속하는 웹 기반의 인트라넷 환경으로 구축되어 있다. (그림2)에서 보여주는 바와 같이 9개 주요서비스가 있으며, 모든 데이터는 중앙 데이터베이스에 저장되고 다른 기관의 시스템과 연계되어 각종 행정정보를 공유하고 있다.



(그림1) e-Consul 시스템 구성

사용자 인증과 접근제어는 DB를 이용한 자체 인증과 접근제어 모듈을 사용 하며, 사용자는 시스템에 최초 접속 시 입력한 ID와 패스워드로 사용자 인증과정이 수행되고 이후 시스템이 유지하는 세션정보를 이용하여 접근 제어를 활성화 한다.

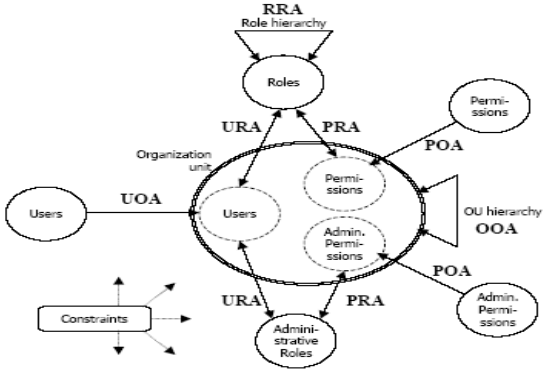
2-2. 역할기반 접근제어(RBAC)의 관리 모델

Sandhu는 RBAC 모델에서 역할의 관리를 위해 관리역할(Administration Roles)을 두고 사용자 역할 계층과 동일하게 계층을 두어 역할계층간의 권한 상속이 이루어지는 ARBAC97 모델을 제안하였다[1]. ARBAC97에는 관리영역(Administrative rages)과 선행조건(Prerequisite conditions)이라는 두 가지 중요 개념이 있으며, 관리영역은 관리자의 권한 범위를 제한하고 선행조건은 관리자가 역할을 부여할 수 있는 사용자 집단(user pool)을 제한하도록 하고 있다. 관리 역할은 선행조건을 만족할 때 허가된 역할 범위에서 사용자를 역할에 할당(can-assign)하거나 회수(can_revoke)할 수 있다.

이러한 방식은 역할 계층에서 상위 역할을 부여받기 위해 다단계 사용자 할당을 요구하여 다수의 보안 관리자의 개입을 필요로 하게 되며, 선행조건은 하위 보안 관리자의 사용자 풀을 제한하게 되어 유연한 사용자 풀을 요구하는 현실의 요구에 융통성 있게 대응하지 못한다. ARBAC02 모델[2]에서 선행조건 대신 조직단위로 사용자 풀(User Pool)과 권한 풀(Permission Pool)을 생성하여 사용자 풀과 선행조건간의 불필요한 결합을 제거하였으나, 역할 계층 구조가 변경될 경우 발생되는 예상치 못한 부작용(side effect)과 불법적인 권한 변화의 문제는 여전히 존재한다.

2-3. OS-RBAC (Organizational Structure and Role-Based Access Control)

OS-RBAC 모델은 기존 모델의 역할계층 변경으로 발생하는 관리 권한 범위의 문제를 조직 구조로 해결하고 있다[3]. 이전 모델과의 가장 큰 차이점은 보안 담당자의 권한범위를 역할계층 대신 보안담당자가 속한 조직 단위(Organizational Unit) 개념을 적용한 것이다. 또한, 기존 모델들이 보안 담당자 그룹의 관리 작업을 점검하기 위해 권한 정보를 이용하는데 비해 OS-RBAC에서는 관리 규칙을 이용하고 있다. (그림2)는 전체적인 OS-RBAC 모델의 관계를 보여준다.



(그림2) OS-RBAC 관리모델

OS-RBAC 는 조직 구조를 생성하고 사용자와 권한을 해당 조직 단위에 배정하는 조직구조관리모델(Organization Structure Administration Model) 과 각 보안담당자의 역할과 관련된 관리 활동들을 설명한 역할관리모델(Role Administration Model)로 구성되어 있다. 조직구조관리모델에는 UOA User-Organization unit Assignment) 과 POA(Permission-Organization unit Assignment)와

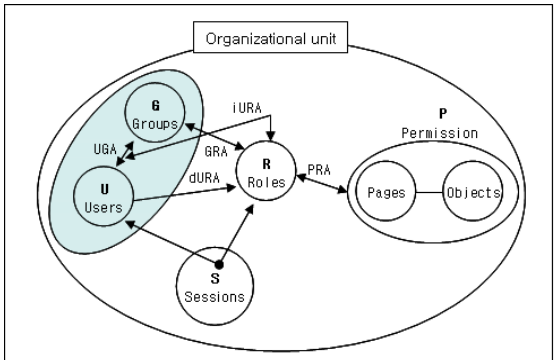
OOA(Organization unit-Organization unit Assignment) 규칙이 있으며, 10개 과정을 반복하면서 조직 구조를 형성 한다. 역할관리모델은 보안담당자가 역할을 생성하고 삭제하며, 역할에 사용자와 권한을 할당하고 역할계층을 형성하기 위한 URA, PRA, RRA 규칙들로 구성되어 있다.

3. 제안 모델 설계

3.1 기본 개념

RBAC 모델에서 역할의 정의는 전반적인 보안관리 방법을 결정하는 중요한 개념이다. 일반적으로 기존 RBAC 에서 역할은 사용자가 속한 조직의 직위로 간주된다. 그러나 실제 조직에서는 같은 직위에 있는 사용자라도 다른 자격과 책임을 가지고 직무를 수행한다. 예를 들어, e-Consul 에서 영사 직위를 가진 자는 영사업무 전반을 담당하기도 하지만 조직의 규모에 따라 여권, 사증, 공증 등 세부 업무로 나누어진다. 특히 비정규직인 업무보조원은 조직의 인적구성에 따라 수시로 업무가 변경된다. 이렇게 역할이 직위가 아니라 직무로 부여 될 경우 RBAC의 역할 계층으로 완전한 조직 구조를 설계할 수 없다. 이러한 조직 환경에서는 실제 조직 구조에 기초한 역할 관리 모델이 적합하게 된다.

또한, 기본적으로 보안담당자는 사용자에게 정규역할을 개별적으로 할당하여 권한을 부여하게 되나, 다수의 사용자와 역할을 효과적으로 관리하기 위해서는 보다 더 편리한 권한관리 방식이 요구된다. 이러한 방법을 제공하기 위해 사용자와 역할과의 할당 관계에 그룹(Groups)이라는 개념을 추가하였다. 역할이 권한의 집합이라고 보면, 그룹은 같은 보안 속성을 가진 사용자의 집합이다. 사용자는 하나의 그룹에 포함됨으로서 그룹에 할당되어 있는 기본 역할 권한을 간접적으로 부여받을 수 있다. 이는 다른 조직에 속한 동일 역할을 가진 사용자들에게 반자동적으로 권한을 부여하고 회수할 수 있다는 것을 의미함으로서 보안담당자의 관리 노력을 줄여주게 된다. (그림3) 은 RBAC 모델에 사용자와 그룹, 그룹과 역할의 할당 관계를 보여준다. 사용자와 그룹, 그룹과 역할 간에는 제한 조건을 두어 그룹에 속할 수 있는 사용자와 역할의 범위를 규정할 수 있다. 따라서 본 모델에서 역할은 '그룹역할', '정규역할', '위임역할'로 구성된다. 사용자가 시스템에 로그인 할 때, 사용자는 본인이 속한 그룹의 기본 그룹역할, 직접 할당된 정규역할과 위임역할을 동시에 할당 받게 된다.



U: 사용자 u의 집합, G: 그룹 g의 집합, R: 역할 r의 집합, P: 페이지 p의 집합
- GRA ⊆ G × R, 그룹과 역할과의 다대다 할당 관계
- UGA : U - G, 사용자와 그룹과의 일대다 할당 관계
- URA ⊆ iURA ∪ dURA, 사용자와 역할과의 할당관계

(그림3) 그룹개념이 추가된 RBAC 모델

.

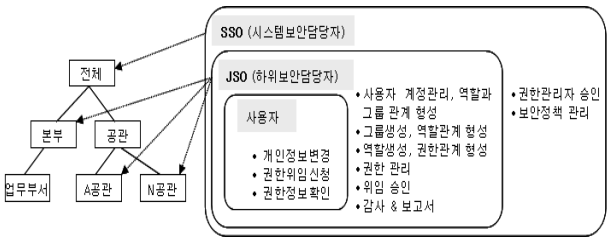
조직 구조를 기반으로 분산 권한관리를 위해 사용자, 그룹, 역할, 권한에 조직 단위라는 속성이 정의되며, 보안담당자는 같은 조직에 있거나 하위 조직에 있는 사용자, 그룹, 역할, 권한들을 관리하게 된다. 다음은 보안담당자가 그룹을 생성하고 그룹에 역할과 사용자를 할당하거나 회수할 수 있는 OS-RBAC 규칙을 정의한 것이다.

(SO: 보안담당자, u: 사용자, g:그룹, r:역할, p: 권한, org_unit: 조직단위)

- UPA (User-Permission Assignment) 규칙
  - assignment : (SO.org_unit ≥ u.org_unit) ∧ (SO.org_unit ≥ p.org_unit) ∧ (u.org_unit ≥ p.org_unit) ∧ (u.type = p.type)
  - revocation : (SO.org_unit ≥ u.org_unit) ∧ (SO.org_unit ≥ p.org_unit)
- UGA (User-Group Assignment) 규칙
  - assignment : (SO.org_unit ≥ u.org_unit) ∧ (SO.org_unit ≥ g.org_unit) ∧ (u.org_unit ≥ g.org_unit)
  - revocation : (SO.org_unit ≥ u.org_unit) ∧ (SO.org_unit ≥ g.org_unit)
- GRA (Group-Role Assignment) 규칙
  - group 생성 : SO.org_unit ≥ g.org_unit, g.org_unit의 값을 지정한다.
  - assignment : (SO.org_unit ≥ r.org_unit) ∧ (SO.org_unit ≥ g.org_unit) ∧ (g.org_unit ≥ r.org_unit)
  - revocation : (SO.org_unit ≥ g.org_unit) ∧ (SO.org_unit ≥ r.org_unit)

3.2. 구 현

상기 제안 모델을 e-Consul에 구현하였으며, 접근제어시스템의 조직 구조와 관리 역할은 (그림4)와 같다. 시스템보안담당자(SSO)는 최상위 보안 관리자로서 하위보안담당자(JSO)의 모든 관리역할 권한을 상속 받는다.

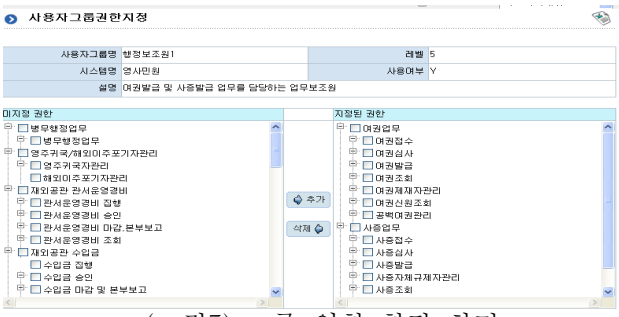


(그림4) 조직구조와 관리 역할

보안담당자(SO)는 다음과 같은 순서로 사용자에게 권한을 부여한다.

① 시스템에 접속한다. 보안담당자로 승인되어 있으면 관리 역할들이 활성화된다. 그러나 보안담당자가 관리할 수 있는 사용자, 그룹, 역할, 권한은 보안담당자의 소속으로 제한된다.
② 역할을 생성하고 페이지(권한)를 할당한다.
③ 그룹을 생성하고, 그룹에 기본 그룹역할과 사용자를 지정한다.
④ 사용자에게 그룹을 지정하고 직접 정규역할을 할당한다.
⑤ 사용자에게 직접 정규역할을 할당한다.

(그림5)는 보안담당자가 그룹을 생성하고 그룹에 역할을 할당하는 실제 구현된 화면이다. 전체 재외공관에 해당하는 '행정보조원1'그룹에 '여권발급', '사증발급' 이라는 역할이 할당되어 있다면, '행정보조원1' 그룹에 속한 A공관의 사용자가 로그인 할 때 자동으로 '여권발급'과 '사증발급' 역할에 해당하는 웹페이지가 활성화 된다.



(그림5) 그룹-역할 할당 화면

4. 결론

분산 보안 관리조직에서 정보를 보호하고 사용자가 적절한 권한을 획득하기 위해서는 다수로 구성된 보안 관리자로부터 유발되는 권한의 오용과 남용을 최소화 시키는 것이다. 본 논문에서 그룹과 조직 구조를 이용한 RBAC 관리모델을 제안하여 복잡한 분산 권한관리를 단순화하였으며, 전자영사시스템에 구현하여 접근 통제 정책을 효과적으로 관리하는데 실질적인 개선 효과가 있음을 확인할 수 있었다.

참고문헌

[1] R.Sandhu, V.Bhamidipati, and Q.Munawer, "The ARBAC97 model for role-based administration of roles", ACM Transactions on Information and System Security, Vol.2, 1999.

[2] Sejong Oh and R.Sandhu, "A Model for Role Administration Using Organization Structure", SACMAT'02, 2002.

[3] Jason Crampton and George Loizou, "Administration Scope and Role Hierarchy Operation", SACMAT02, 2002.

[4] Mohammad A. Al-Kahtani, "A Family of Models for Rule-Based User-Role Assignment", A PhD. dissertation submitted to the Graduate Faculty of George Mason University, 2004.

[5] Frederic Cuppens and Alexandre Miege, "AdOrBAC : An Administration Model for Or-BAC", International Journal of Computer Systems Science and Engineering, 2004.

[6] Alexandre Miege, "Definition of a formal framework for specifying security policies. The Or-BAC model and extensions", A PhD. dissertation submitted to the Graduate Faculty of Ecole Nationale Superieure des Telecommunications, 2005.

[7] Sejong Oh, Changwoo Byun and Seog Park, "An Organizational Structure-Based Administration Model for Decentralized Access Control", Journal of Information Science and Engineering 22, 1465-1483, 2006.