위험분석시스템을 위한 역할기반접근통제 모델

박현우, 최상수, 이강수
한남대학교 컴퓨터공학과

A Role Based Access Control Model for Risk Analysis System

Hyun-Woo Park, Sang-Soo Choi, Gang-Soo Lee
Dept. of Computer Engineering, Hannam University

요 약

정보시스템관리를 위한 위험분석시스템은 다수의 사용자가 각각의 역할과 임무에 따라 평가대상조직의 민감한 내용을 다루므로, 대상조직에 대한 역기능을 초래할 수 있다. 이에 위험분석시스템 자체의 보안을 위한 접근통제가 필요하다.

본 논문에서는 위험분석시스템을 위한 RBAC정책 모델을 제안한다. 제시한 모델은 위험분석시스템의 특성을 고려하여 연구되었으며, 역할의 상속성에 의한 권한남용 방지를 위해 금지적접근목록(n-ACL)을 적용하였다.

1. 서론

IT의 발전으로 정보시스템은 기존의 보조설비개념에서 생산설비의 개념으로 의미와 중요성이 확대되어 조직의 부가가치를 창출하는 중요한 요소가 되었다. 그러므로 정보시스템은 잘 관리되어야 하며 그렇지 않은 경우 조직에 막대한 피해를 초래할 수 있다.

정보시스템 보호 및 관리방법으로 위험기반관리방법이 널리 쓰이고 있다. 위험관리는 위험분석과 대책단계로 나눌 수 있으며, 위험분석은 파악과 측정단계로 구성되어 있다. 위험분석은 자산, 위협, 취약성 등으로 위험을 형상화하여 각각을 파악하고 측정하는 것으로 위험도를 산출한다. 위험분석공정(process)에 대해 많은 연구가 이루어 졌으며 현재는 자산기반 분석 방법이 주를 이루고 있다[1].

위험분석은 많은 비용, 인력, 시간 등을 투자해야하는 프로젝트의 개념을 내포하고 있다. 그러므로 성공적인 프로젝트 수행을 위해 도구의 지원이 필수적이다. 현재 연구 및 상용제품으로 많은 위험분석도구가 개발되어 있다[2,3].

[1]에서 연구된 위험분석 방법에 따르면 위험분석은 상·하위 단계로 나누어지며, 각 단계에서 여러 인력이 설문자, 평가자, 평가책임자 등의 역할을 가지고 임무를 수행하게 된다. 이처럼 위험분석도구는 단순한 도구의 개념에서 시스템의 개념으로 확대되어 있고, 시스템에 접근하는 사용자도 역할별로 구분되어 있다.

위험분석은 보안에 관하여 조직의 민감한 부분에 접근하는 것이므로, 위험분석 프로젝트 자체의 보안도 고려되어야 한다. 그러므로 위험분석시스템은 접근통제 하에서 운영되어야 한다.

접근통제는 여러 가지 보안 서비스들과 밀접한 연관을 가지며 그 하나만으로는 완전한 해결책을 제시할 수 없다. 보안 서비스들에는 감사, 인증, 접근통제, 보안관리 등이 있다. 본 논문에서는 범위를 접근통제부분으로 제한하며, 나머지에 대해서는 [4]를 참조한다.

미 국방성에서 기밀 분류된 방법으로부터 유래하는 접근통제 정책은 규칙기반 정책인 MAC(Mandotory Access Control)과 신분기반 정책인 DAC(Discretionary Access Control)을 들 수 있다. 그리고 이들의 단점을 보완하는 RBAC은 보안이 필요한 환경에 적합한 접근제어를 이룰 수 있는 정책으로 알려져 있으며 NIST의 연구는 이를 확인하는 계기가 되었다[5].

본 논문은 위험분석시스템을 위한 RBAC 모델을 제안하였으며 구성은 다음과 같다. 2장에서는 RBAC을 적용할 위험분석시스템에 대하여 다룬다. 3장은 RBAC 모델의 개념을 설명하고 위험분석 시스템에 적용하기 위한 RBAC정책모델을 기술한다. 4장에서는 RBAC정책 모델을 위험분석시스템에 적용한 사례를 보여주며, 5장에서 결론을 맺는다.

2. 위험분석시스템

본 논문에서 적용한 시스템은 [1]의 위험분석방법론을 따르고 있으며 전체적으로 위험분석도구, 데이터베이스, 웹 설문시스템의 3부분으로 구성되어 있다.

위험분석도구부분은 시스템관리, 평가프로젝트관리, 사용자관리, 평가관리 등의 시스템의 전반적인 기능을 포함하고 있다. 또한 위험분석시스템 인터페이스 기능을 하므로, 사용자는 도구를 통해서만 위험분석시스템에 접근할 수 있다.

데이터베이스는 관리DB, 평가DB, 참조DB 등으로 구성되어 있다. 참조 DB는 평가에 필요한 참조자료 및 공통자료를 포함하고 있으므로 공개되어도 무방하지만 관리DB, 평가DB는 보안상 민감한 내용을 담고있으므로 접근통제를 통하여 보호되어야 할 부분이다.

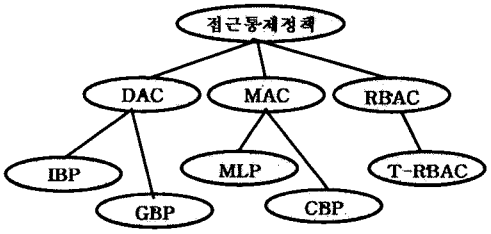
웹 애플리케이션 부분은 평가대상조직의 인원들에게 설문을 실시할 때 웹기반 설문기능을 지원하므로써 편리한 설문관리를 수행할 수 있도록 한다. 설문결과 또한 위험분석에 중요한 영향을 미치기 때문에 보호되어야 할 대상이 된다.

3. RBAC정책 모델

3.1 접근통제정책의 개요

접근통제를 위한 일반적 모델에서 능동적인 실체의 집합을 주체 또는 개시자라고 하며, 수동적 자원의 집합을 집합을 타겟 또는 객체라고 부른다. 접근통제의 결정은 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고, 어떤 조건하에서 접근할 수 있는지를 다루는 문제이다. 즉, 이러한 결정은 접근통제정책에 반영이 되고, 접근 요청은 접근 정책을 시행하는 접근통제 메커니즘을 통하여 시행된다.

<그림 1>은 접근통제정책의 계보를 보여주고 있다[6]. DAC정책은 신분기반 접근통제정책으로서 주체나 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한하는 방법을 말한다. IBP는 신분기반 정책의 하나로써 어떤 사용자가 어떤 행동을 할 수 있는지 각 객체별로 목록을 표현한다. GBP는 다수의 사용자가 하나의 객체에 대하여 동일한 허가를 부여받는 방식이다.



<그림 1> 접근통제정책 계보

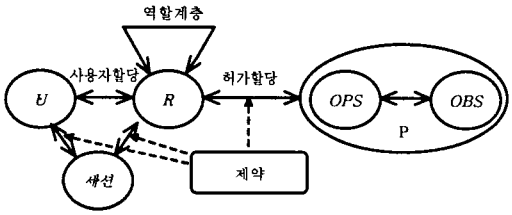
MAC정책은 규칙기반 접근통제정책으로서 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근정보에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법을 MAC라고 한다. MLP 자동화된 강제적 시행정책을 따르는 방식으로서 일반적으로 허가되지 않은 노출로부터 정보를 보호하기 위하여 사용된다 CBP는 일련의 타겟 집합이 다른 타겟들과 분리된 이름의 부서 또는 범주(category)를 갖고 연결된다. 사용자는 그 부서에 있는 타겟을 접근할 수 있도록 부서에 대하여 명백히 구분된 접근허가를 보유해야 할 필요가 있다.

RBAC정책은 GBP의 한가지 변형으로 생각할 수 있으며, TRBAC은 RBAC정책을 확장하여 작업의 개념으로 허가의 흐름을 반영한 정책이다.[7]

3.2 RBAC정책 모델

<그림 2>는 RBAC 모델을 설명하고 있다. 사용자(U), 역할(R), 허가(P) 등의 엔티티가 있다. 사용자는 시스템을 이용하는 주체 또는 개시자라고 할 수 있으나 사람이라고 정의한다. 역할은 역할의 구성원에게 부여된 책임 및 권한과 연관된 의미를 가진 조직내의 직무 기능이나 직무 이름이다. 허가는 시스템 내에 특별한 모드의 접근의 승인이다. 사용자는 역할에 할당(assignment)되고 역할에 허가를 할당한다. RBAC의 핵심은 이러한 두 관계들에 있다. 사용자가 허가를 실행할 수 있도록 매개자로서 역할의 배치는 사용자와 허가를 관계시키는 것보다 접근 설정에 대한 제어와 감사를 제공한다.

NIST[9]에서는 <표 1>과 같이 RBAC모델을 4수준으로 구분하고 있다. 수준1은 기본적인 특성으로서 사용자-역할, 역할-허가 할당의 관계를 만족하며 각각은 다대다 할당을 지원한다. 수준2는 수준1에 역할계층을 적용함으로써 역할간 상속관계를 지원한다. 수준3은 제약을 적용하여 직무의 분리를 실현하며, 수준4는 이들을 통합한 모델이다.



<그림 2> RBAC 모델

RBAC에서 사용되는 대표적인 제약은 다음과 같다.

(1) 상호배타(Mutual Exclusion)

같은 사용자는 상호배타적인 집합내에서 하나만의 역할에 할당될 수 있다. 이것은 직무의 분리를 지원한다. 예를 들면, 구매팀장과 경리팀장은 한 개인이 두 역할에 할당이 되어서는 안된다.

(2) Cardinality

사용자 할당 제약의 또 다른 예로서 역할은 멤버의 최대 숫자를 제한할 수 있다. 예를 들어 각 분야의 대표는 단 한 사람만이 할당될 수 있다. 유사하게 각 사용자가 속하는 역할의 수도 제한할 수 있다. 이것을 카디널리티(cardinality) 제약이라고 한다.

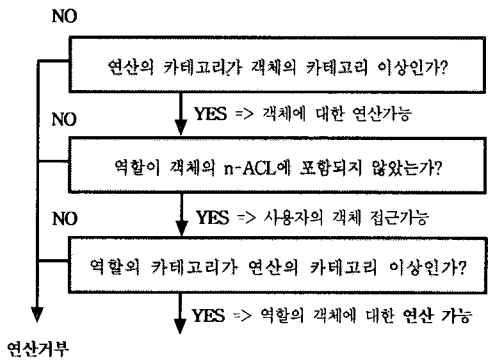
<표 1> RBAC 수준별 기능요구

수준	명칭	RBAC 기능적 특성(수준을 위한 요구조건)
1	Flat RBAC	• 사용자가 역할을 통하여 허가를 획득함. • 사용자-역할 다대다 할당을 지원해야함. • 허가-역할 다대다 할당을 지원해야함. • 사용자-역할 할당 감사를 지원해야함. • 사용자는 동시에 여러 역할을 통하여 허가를 사용할 수 있음.
2	Hierarchical RABC	Flat RBAC+ • 계층적 역할을 지원해야 함. • 수준2a는 독단적(arbitraty) 계층을 요구함. • 수준2b는 제한된(limited) 계층을 의미함.
3	Constrained RBAC	Hierarchical RBAC+ • 직무의 분리를 강제해야 함. • 수준3a는 독단적(arbitraty) 계층을 요구함. • 수준3b는 제한된(limited) 계층을 의미함.
4	Symmetric RBAC	Constrained RBAC+ • 실제적으로 사용자-역할 감사에 필적하는 수행을 갖는 허가-역할 감사를 지원해야 함. • 수준4a는 독단적(arbitraty) 계층을 요구함. • 수준4b는 제한된(limited) 계층을 의미함.

3.3 위험분석시스템을 위한 RBAC정책 모델

<표 2>는 위험분석시스템을 위한 RBAC정책 모델을 설명하고 있다. 이 모델은 RBAC 모델에 n-ACL, 보안카테고리 등의 개념을 더하여 변형된 RBAC모델이라 할 수 있다. 사용자는 역할과 매핑된다. 역할, 연산, 객체 등의 엔티티는 보안카테고리를 부여받게 된다. 역할은 부여된 보안카테고리와 연산의 보안카테고리의 비교를 통하여 허가를 할당받게 된다. 보안카테고리는 상속성을 가지고 있어서 상위 카테고리는 하위카테고리의 권한을 상속받는다. 이를 통해 역할간에도 상속성이 생긴다. 단, 역할간의 상속성은 상호배타적인 역할의 분리에 위배가 발생할 수 있다. 이는 금지적접근통제목록(n-ACL)을 제공함으로써 해결한다.

<그림 3>은 RBAC정책을 수행하기 위한 수행규칙을 보여주고 있다. 수행규칙은 역할에 허가를 할당하기 위한 부분만 나타나 있으며, 사용자-역할 관계에서 카디널리티 제약은 접근통제정책을 반영하여 개발자가 현실화해야한다.



<그림 3> 수행규칙

4. 적용사례

4.1 보안정책

접근통제정책의 수립에 앞서 보안정책의 수립이 선행되어야 한다. 위험분석시스템의 보안정책 예는 다음과 같다. 본 논문의 사례를 위해 일부분만 표시한다.

- 시스템관리자는 평가 도메인에 접근하지 않는다.
- 평가자는 관리도메인에 접근하지 않는다.
- 평가책임자와 일반평가자는 직무분리가 된다.
- 평가책임자는 할당된 평가에 대한 전반적인 책임과 권한이 있다.

4.2 역할도출

위험분석 조직의 직무 및 임무를 분석하여 도출한 역할은 <표 3>과 같다. 시스템관리자 역할은 1명에게만 할당되어야 하며, 평가책임자 역할은 평가프로젝트당 1명이어야 한다.

<표 3> 역할의 보안카테고리 및 카디널리티

역할(R)	보안카테고리(SC)	카디널리티(C)
R1.시스템관리자	SC4	1
R2.평가책임자	SC3	1
R3.일반평가자	SC2	n
R4.설문응답자	SC1	n

4.3 사용자-역할 매핑

<표 4> 사용자-역할 매핑

사용자ID	역할(R)
U1.admin	R1
U2.lion	R2
U3.cat	R3
U4.tiger	R3
U5.horse	R4
U6.dog	R4

4.4 객체 파악

<표 5>는 위험분석시스템에 사용되는 객체의 목록을 보여주고 있다. 각 객체들은 중요도 및 기능에 따라 보안카테고리를 부여받고 있다.

4.5 연산 파악

<표 6>는 위험분석시스템의 연산을 보여주고 있다. 각 연산에 보안카테고리를 부여하였다.

<표 2> 위험분석시스템을 위한 RBAC 모델

요소	정형명세	설명
사용자(User)	$U = \{u_i \mid i = 1, ..., n\}$	- 사용자는 역할과 매핑됨.
역할(Role)	$R = \{r_i \mid i = 1, ..., n\}$	- 역할은 연산과 매핑됨.
카디널리티(Cardinality)	$C = \{c_i \mid i = 1, ..., n\}$	- 특정역할에 할당될 수 있는 사용자 수에 대한 제약
객체(Object)	$O = \{o_i \mid j = 1, ..., m\}$	- n-ACL이 할당됨.
연산 (Operation)	$OP = \{op_k \mid k = 1, ..., p\}$	- 시스템에서 지원하는 객체에대한 모든 행동 - 기밀성과 허가 관계의 정의를 통해 기술됨
보안 카테고리	$SC = \{sc_i \mid i = 1, 2, 3, 4$ $sc_1 \subset sc_2,\ sc_2 \subset sc_3,$ $sc_3 \subset sc_4\}$	- 역할-연산간의 처리활동에 대한 "can-perform 관계" - 상위 카테고리는 하위 카테고리의 특권(privilege)이 추가됨
사용자 역할 매핑	$\alpha: U \rightarrow R$	- 사용자-역할 관계 부여 - 역할의 카디널리티에 따라 사용자-역할관계가 제한됨.
역할의 분류	$\beta: R \rightarrow SC$	- 직무에 관련된 최소의 보안카테고리를 역할에 부여함
연산의 분류	$\gamma: OP \rightarrow SC$	- 연산을 수행하는데 요구되는 최소의 보안카테고리를 연산에 부여함(최소특권 원칙) - 복합연산은 단위연산으로 분해후 연산분류 실시
객체의 분류	$\delta: O \rightarrow SC$	- 객체를 다루기위한 보안카테고리를 부여함(최소특권 원칙)
기밀성 (confidentiality)	$\varepsilon: O \rightarrow U^n$	- 어떤 사용자가 어떤 객체에 접근할수 없는지를 명세 - 금지적 ACL(n-ACL)통해 통제됨
허가(clearance)	$\zeta: OP \times R \rightarrow RC$	- 역할-연산쌍에 보안카테고리를 부여 - 주체의 행동은 가변적이며 주체에 부여된 역할과 문맥에 따름(문맥종속적) - 무결성 해결
수행규칙	$\eta: OP \times O^n \times R \rightarrow O^m$	접근통제 규칙에 해당

<표 5> 파악된 객체

객체(OPS)	보안카테고리(SC)	설명
O1.M_Table	SC4	시스템관리 테이블
O2.U_Table	SC4	사용자관리 테이블
O3.A_Table	SC2	평가용 테이블
O4.T_Table	SC2	참조 테이블
O5.R_Table	SC3	평가결과 테이블
O6.A_File	SC2	평가자별 파일
O7.S_Web	SC1	설문 웹

<표 6> 파악된 연산

연산(OP)	보안카테고리(SC)	설명
OP1.시스템설정	SC4	시스템설정
OP2.사용자관리	SC4	사용자 등록
OP3.위험평가	SC2	일반평가자의 위험평가
OP4.평가척도참조	SC2	평가를 위한 척도 참조
OP5.평가결과입력	SC3	평가결과 결정하고 입력
OP6.평가결과파일	SC2	일반평가자의 평가결과 임시파일 저장
OP7.설문응답	SC1	웹을 통한 설문 응답

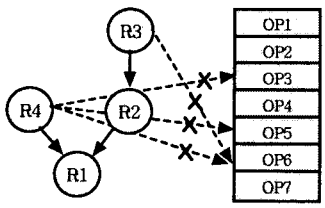
4.6 n-ACL

<표 7>은 n-ACL 설정을 보여주고 있다. n-ACL은 보안카테고리의 상속성에 의해 상위 권한을 가진 역할이 하위 권한을 가진 역할의 객체에 대한 무결성 보안을 해칠 수 있는 권한남용 위협을 방지하기 위하여 설정한다. n-ACL은 위험분석시스템 운영조직의 보안정책에 따라 달라질 수 있다.

<표 7> n-ACL 설정

구분	O1	O2	O3	O4	O5	O6	O7
R4	·	·	deny	·	deny	deny	·
R3	·	·	·	·	·	deny	·
R2	·	·	·	·	·	·	·
R1	·	·	·	·	·	·	·

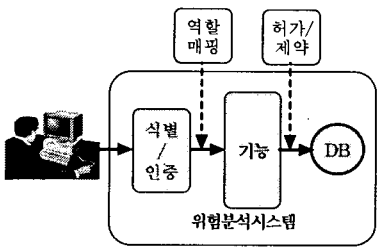
<그림4>는 보안카테고리에 의한 역할의 상속과 n-ACL에 의한 허가거부를 보여주고 있다.



<그림 4> 역할의 상속과 n-ACL

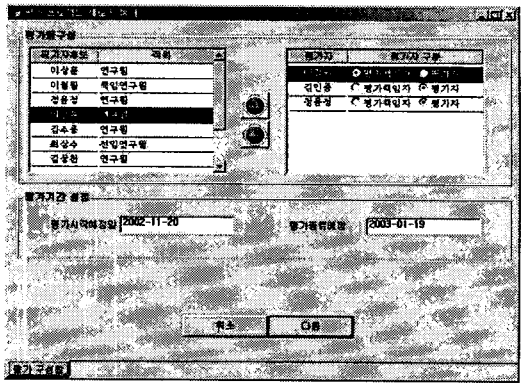
4.7 RBAC기반 위험분석시스템

<그림5>는 위험분석시스템상에서의 RBAC을 보여주고 있다.



<그림 5> RBAC기반 위험분석시스템

<그림 6>은 관리자에 의해 사용자-역할 관계를 할당하는 것을 보여주고 있다.



<그림 6> 사용자-역할 할당 GUI

5. 결론

효율적인 정보시스템 위험분석을 위해 위험분석시스템을 사용하고 있다. 위험분석 시스템 사용자는 각각의 역할과 임무에 따라 평가를 수행하게 된다. 위험분석과정에서의 정보보호를 위하여 시스템 자체의 접근통제가 이루어져야 한다. 이에 본 논문에서는 위험분석시스템을 위한 RBAC정책 모델을 제안하였으며 적용예제를 보였다.

제안한 모델은 역할, 연산, 객체 등에 보안카테고리를 적용한 후 사용자를 역할과 매핑하여 수행규칙에 따라 접근통제를 하는 변형된 RBAC정책 모델이다. 상위 보안카테고리는 하위 보안카테고리의 특권을 상속함으로써 권한남용의 문제점이 발생할 수 있는데, 이는 금지적접근목록(n-ACL)을 통하여 해결하였다.

[참고문헌]

[1] 박현우 외 5명, "정보시스템을 위한 범용 웹기반 위험분석 프로세스", 한국디지털컨텐츠학회지, 3권 1호, 2002.12

[2] 김정덕 (외), "위험 분석 도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.

[3] 송관호(외), "정보시스템 보안을 위한 위험분석 소프트웨어 개발" 한국전산원 연구보고서, 1997. 12.

[4] Ravi S.Sandhu, Pierangela Samarati, "Access Control: Principles

[5] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn, "Role-Based Access Control(RBAC): Features and Motivations", NIST Computer Security Applications Conference, 1995.

[7] 한국정보보호진흥원(KISA). "접근통제 기술 개요", http://www.kisa.or.kr/technology/sub3/AC_9901.html

[8] 백종명, "안전한 워크플로우 시스템을 위한 역할기반 접근제어 모델", 고려대학교, 1999

[9] David F. Ferraiolo, et. al. "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, Vol. 4, No. 3, pp.224-274, Aug. 2001.

[10] S. Murugesan and Y. Deshpande(Eds): WebEngineefing 2000, LNCS 2016, pp.90-104, 2001.