韓國 컴퓨터情報學會 論文誌
第9卷 第4號, 2004. 12.

2004-9-4-1-8

통합 접근 제어를 위한 시뮬레이션 모델 설계

이 호*

Design of a Simulation Model for Integrated Access Control

Ho Lee*

요 약

규칙 기반 접근 제어가 신분 기반 접근 제어의 완전한 대체 방법이 아니듯이 직무 기반 접근 제어도 신분 기반 접근 제어와 규칙 기반 접근 제어의 병합이 아닌 상호 보완적인 방법이다.

본 논문에서는 기존의 접근 제어 메커니즘을 통합하여 보안성 무결성 및 흐름 제어 보안 기능을 제공하며 직무 중심 조직의 접근 제어 요구를 용이하게 수용할 수 있는 새로운 방식의 통합 접근 제어를 위한 시뮬레이션 모델을 설계하여 이를 실제의 응용 시스템에 적용할 수 있도록 한다.

Abstract

Rule-based access control can not completely be replaced by identity-based access control. Neither can role-based access control be a merger of identity-based access control and rule-based access control, but can be used complementarily for each other.

In this paper, is proposed a simulation model designed for a new integrated access control method that has been created by means of integrating the existing access control methods. The integrated access control method is equipped with security, integrity and flow control and can easily accomodate the requirements for access control from role-based corporate bodies. The simulation model proposed in this paper can be applied for real working system designs.

▸ Keyword : Access Control (접근 제어)

• 제1저자 : 이호
• 접수일 : 2004.10.17, 심사완료일 : 2004.11.13
* 국립 한국재활복지대학 정보보안과 부교수

Ⅰ. 서 론

접근 제어는 크게 세 가지 범주로 나눌 수 있다. 신분 기반 접근 제어는 주체나 또는 그들이 속해 있는 그룹의 신분에 근거하여 객체에 대한 접근을 제한하며 접근하는 객체 정보의 중요성에 대한 아무런 지식을 가지지 않으므로 단순한 신분 위장에 의해서도 접근 제어가 파괴될 수 있다.

규칙 기반 접근 제어는 주체와 객체들 간의 관계를 정의하고, 정보의 흐름이 일어났을 때 정보가 소유한 제한 규칙을 상속하며, 각 주체와 객체에 대한 규칙이 일정하므로 단순한 신분 위장으로는 접근 제어를 파괴할 수 없다.

직무 기반 접근 제어는 신분 기반 및 규칙 기반 접근 제어의 특성을 포함하고 있는 기술로서, 개별적 신분이 아닌 자신의 직무에 따라 접근할 수 있는 정보가 결정되고 사용할 수 있는 정보의 한계가 정해진다.

규칙 기반 접근 제어가 신분 기반 접근 제어의 완전한 대체 방법이 아니듯이 직무 기반 접근 제어도 신분 기반 접근 제어와 규칙 기반 접근 제어의 병합이 아닌 상호 보완적인 방법이다.

본 논문에서는 기존의 접근 제어 메커니즘을 통합하여 보안성 무결성 및 흐름 제어 보안 기능을 제공하며 직무 중심 조직의 접근 제어 요구를 용이하게 수용할 수 있는 새로운 방식의 통합 접근 제어를 위한 시뮬레이션 모델을 설계하여 이를 실제의 응용 시스템에 적용할 수 있도록 한다.

Ⅱ. 관련 연구

접근 제어의 결정은 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고 어떤 조건 하에서 접근할 수 있는지를 다루는 문제이다. 즉, 이러한 결정은 접근 제어 정책에 반영이 되고, 접근 요청은 접근 정책을 시행하는 접근 제어 메커니즘을 통하여 시행된다. 접근 제어 정책은 다음과 같은 세 가지 형태로 서술될 수 있다.

① 권한 부여의 과정에서 어떤 정책은 기관의 부서별로 모든 결정이 제어되거나, 또는 특정 객체에 대하여 개인별 권한 부여가 서술될 수 있다.
② 사용자 및 객체들이 공통의 처리를 위하여 함께 그룹을 형성하여 서술될 수 있다.
③ 어떤 정책이 시스템 요소에 의하여 강제적으로 시행될 수 있는 일반적 규칙들로 서술될 수 있다.

미 국방성의 보안 분류 방법으로부터 유래하는 MAC (Mandatory Access Control)과 DAC(Discretionary Access Control) 정책의 개념은 위에서 제시된 세 가지 요소를 확장 혼합하고 있다. MAC 정책은 자동적으로 시행되는 어떤 규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위하여 사용자와 객체에 대해서 광범위한 그룹 형성이 요구된다. DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근 제어를 그 사용자에게 일임한다[2][6].

OSI 보안 구조에서는 MAC/DAC 이라는 용어 대신에 신분 기반(identity-based)과 규칙 기반(rule-based) 정책으로 구분하고 있다[4][5]. 실제적인 목적에 있어서 신분 기반과 규칙 기반 정책은 각각 DAC 및 MAC 정책과 동일하다[2].

신분 기반 정책은 개인 기반(IBP)과 그룹 기반(GBP) 정책을 포함한다. 규칙 기반 정책은 다중 수준(MLP)과 부서 기반(CBP) 정책을 포함한다. 직무 기반(RBAC) 정책은 신원 기반과 규칙 기반 정책의 양쪽 특성을 갖고 있다. 또한, 이러한 정책들은 서로 연계될 수 있으며, 임계값 의존 제어(VDC), 다중 사용자 제어(MUC) 및 배경 기반 제어(CBC) 등의 추가적 수단을 사용하여 제한 될 수 있다.

접근 제어 메커니즘은 접근 행렬의 열을 표현하는 ACL(Access Control List), 접근 행렬의 행을 표현하는 CL(Capability List), 제어 대상에 레이블을 붙이는 SL(Security Label), 그리고 이러한 세 가지 모델을 하나의 연속체로 생각하는 통합적 정보 모델 등의 기법이 있다.

본 논문에서 다루는 시뮬레이션 모델의 설계 근거가 되는 직무 기반 접근 제어를 위한 연구로서 직무 기반 접근 제어 참조 모델[1]이 정의되어 있는데, (그림 2-1)에서 RBAC0은 기본 모델로서 직무 기반 접근 제어를 위한 최소한의 요구 조건을 가진다. 상위 모델인 RBAC1과 RBAC2는 RBAC0을 포함하면서 RBAC1은 직무 계층(직무가 다른 직무로부터 접근 허가를 상속할 수 있다)이 부가되어 있

고, RBAC2는 제약 조건(constraints)이 부가되어 있다. 통합 모델인 RBAC3은 순차적으로 RBAC0, RBAC1, RBAC2의 특성들을 모두 포함하는 모델이다[1][7].

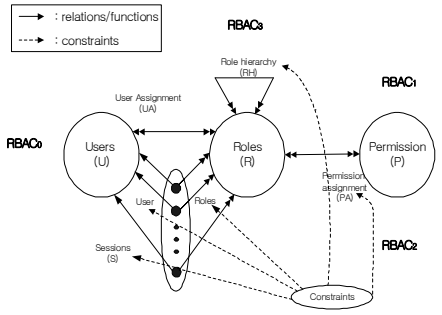

그림 2-1. 직무 기반 접근 제어 참조 모델
Figure 2-1. Role-Based Access Control Reference Models

참조 모델은 다음의 요소들로 구성된다[1][8][9] :

- U, R, P, S (users, roles, permissions, sessions)
- PA P x R, many-to-many permission-to-role assignment relation
- UA U x R, many-to-many user-to-role assignment relation
- user : S U, 각 세션 si를 하나의 사용자 user(si)에 사상하는 함수
- RH ⊆ R x R 는 직무 계층 관계라 불리는 R에 대한 partial order이다
- Roles : S→2R, 각 세션 si를 직무 집합 roles(si)에 사상하는 함수 :
  roles(si) {r| (∃r′ ≥r)[(user(si),r′) UA]} ;
  세션 si는 접근 허가 r ∈ roles(si) {p| (∃r″ ≤ r)[(p,r″) PA]}를 갖는다.

III. 통합 접근 제어 엔진 구성

3.1 접근 제어 정보(ACI)

주체에 있어서, 직무는 실체가 수행할 수 있는 역할을 말한다. 각 직무 식별자와 이에 따른 보안성 등급 및 무결성 등급이 주체의 접근 제어 정보에 명시된다. 객체에 있어서, 식별자는 시스템에서 주체가 객체에 접근을 시도할 때 객체를 식별할 수 있도록 하는 식별자이다. 소유권자는 객체의 소유권을 가지는 실체를 나타내는 식별자로서 여기서는 특정한 직무이다. 각 객체 식별자와 이에 따른 보안성 등급, 무결성 등급 및 소유권자가 객체의 접근 제어 정보에 명시된다[3][10].

3.2 접근 제어 규칙

통합 접근 제어에 적용되는 접근 제어 규칙을 다음과 같이 정의한다[11].

```
s, o, p : 주체, 객체, 접근 허가
S_Level(a) : 보안성 등급 함수
I_Level(a) : 무결성 등급 함수
permit(role, a) : role의 a에 대한 접근 권한 검색 함수
owner(a) : 소유권자 함수
get_ACI(a) : ACI 요구 함수
exist_ACI(a) : ACI에 a의 존재 여부 확인 함수
r, w, x, d : read, write, execute, delete operation
```

(1) 규칙-1 : 접근 제어 정보 존재

```
role_acr(s, o, p)
{
  if ( exist_ACI(s) and exist_ACI(o) ) then
    role ← get_ACI(s)
    if ( p = permit(role, o) ) then
      return TRUE
    else if
      return FALSE
    endif
  else if
    return FALSE
  endif
}
```

(2) 규칙-2 : 보안성 및 무결성 등급간의 지배 관계

```
rule_acr(s, o, p)
{
  case p = 'c'
        if ( S_Level(s) = S_Level(o) and
      I_Level(s) = I_Level(o) )
    then
      return TRUE
    endif
  case p = 'r'
        if ( S_Level(s) ≥ S_Level(o) and
      I_Level(o) ≥ I_Level(s) )
        then
        return TRUE
```

```
            endif
    case p = 'w'
            if ( s = owner(o)  and
            S_Level(s) = S_Level(o)  and
        I_Level(s) = I_Level(o) )
            then
                return TRUE
            endif
    case p = 'x'
      if ( S_Level(s) ≥ S_Level(o)  and
        I_Level(s) = I_Level(o) )
            then
        return TRUE
            endif
    case p = 'd'
            if ( s = owner(o)  and
                S_Level(s) = S_Level(o)  and
                I_Level(s) = I_Level(o) )
            then
            return TRUE
            endif
    otherwise
      return FALSE
}
```

(3) 규칙-3 : 흐름 제어

```
flow_acr(s, o1, o2)
{
    if ( s = owner(o1)  and
        S_Level(s) ≥ S_Level(o1)  and
        S_Level(s) ≥ S_Level(o2)  and
        S_Level(o1) = S_Level(o2)  and
        I_Level(o1) = I_Level(o2) )
    then
                return TRUE
    else if
        return FALSE
    endif
}
```

IV. 시뮬레이션 모델 설계

여기서는 주체가 객체에 대해 접근 요구를 하고 그 접근 요구가 처리되는 접근 제어 전체 과정을 수행하기 위한 시뮬레이션 모델을 제시한다.

4.1 모델 구성 요소

(1) 사용자

접근 제어의 주체로서의 사용자는 (그림 4-1)에서 최상위 계층의 직무인 Project Leader를 부여 받는다고 전제한다.

(2) 직무와 직무 계층

(그림 4-1)에서와 같은 네 종류의 직무들이 존재하며 이 직무들이 직무 계층을 형성한다.

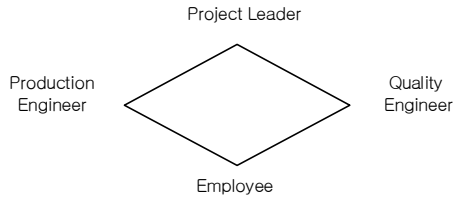

그림 4-1. 직무 및 직무 계층
Figure 4-1. Roles and Role Hierarchies

(3) 제약 조건

다음의 제약 조건을 적용한다.

- 사용자는 하나의 직무에만 속한다.
- 직무 계층은 세 개의 계층으로 구성된다.

(4) 접근 허가

접근 허가는 접근 제어 규칙을 적용하여 주체의 ACI와 객체의 ACI를 서로 비교하여 결정된다.

4.2 모델 접근 제어 정보

(1) 주체의 ACI

직무 식별자	보안성 등급	무결성 등급
PL	Top Secret	Crucial
PE	Secret	Very Important
QE	Secret	Very Important
E	Confidential	Important

(2) 객체의 ACI

객체 식별자	보안성 등급	무결성 등급	소유권자
PLDir	Top Secret	Crucial	PL
PEDir	Secret	Very Important	PE
QEDir	Secret	Very Important	QE
EDir	Confidential	Important	E

4.3 직무와 직무 계정의 처리

각각의 직무에 대응하는 직무 계정(PL, PE, QE, ED, E)을 (그림 4-2)와 같이 생성한다.

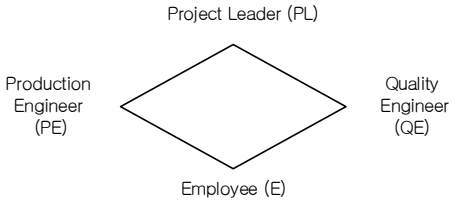

그림 4-2. 직무와 직무 계정의 맵핑
Figure 4-2. Mapping between Roles and Role Accounts

4.4 직무 계층의 처리

각 직무 계정에 대응하는 접근 가능한 디렉터리가 (그림 4-3)과 같이 생성되어 있다. 여기서 객체는 디렉터리로만 제한하고 각 직무 계정은 자신에게 할당된 디렉터리 및 하위 계층의 직무 계정에 할당된 디렉터리만을 접근할 수 있다.

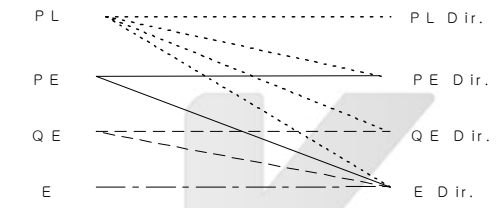

그림 4-3. 직무 계정에서 객체로의 접근 허가 지정
Figure 4-3. Assigning Access Permission from Role Accounts to Objects

4.5 접근 제어 엔진의 동작

(1) 접근 제어 엔진의 입출력 및 동작

(그림 4-4)는 접근 제어 엔진을 구성하는 ADF의 접근 제어를 위한 입출력 및 동작을 보여준다[13].

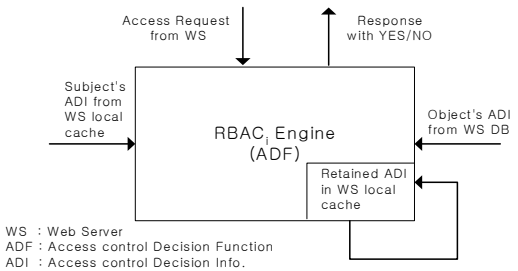

그림 4-4. 접근 제어 엔진의 접근 제어 결정
Figure 4-4. Access Control Decision by Access Control Engine

(2) 접근 제어 엔진의 접근 제어 규칙 적용

(그림 4-5)는 통합 접근 제어 엔진이 접근 제어 규칙을 적용하는 과정을 보여준다[12].

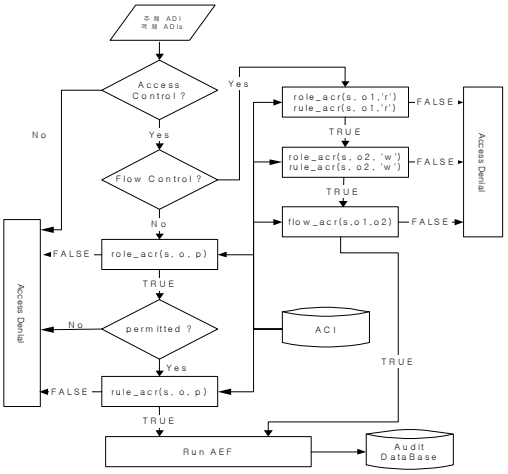

그림 4-5. 접근 제어 엔진의 접근 제어 규칙 적용
Figure 4-5. Applying of Access Control Rules by Access Control Engine

(3) 접근 제어 엔진의 접근 제어 수행 결과

<표 4-1>은 접근 제어 엔진이 주체와 객체의 ACI 정보를 근거로 규칙을 적용하여 결정한 접근 제어 결과를 보여준다.

표 4-1. 접근 제어 엔진의 접근 제어 결과
Table 4-1. Results by Access Control Engine

접근 제어 사례	접근 요구 종류	접근 요구 대상	적용 접근 제어 규칙	규칙 적용 결과
1	READ	PLDir	role_acr() rule_acr()	Accepted
2	WRITE	PLDir	role_acr() rule_acr()	Accepted
3	READ	PEDir	role_acr() rule_acr()	Accepted
4	CREATE	Edir	role_acr() rule_acr() flow_acr()	Denied

V. 결론 및 향후 연구 과제

본 논문에서는 기존의 접근 제어 모델들이 서로 다른 보안 기능과 특성을 가지고 있지만, 동시에 상호 보완적인 요소들도 가지고 있다는 사실에 착안하여 보안 기능을 만족시킬 수 있으면서도 빠른 접근 제어 처리가 가능한 새로운 통합 접근 제어 방법을 제안하였다. 보안성과 무결성을 보장하고 흐름 제어가 가능한 접근 제어를 위하여 직무 및 규칙을 근간으로 하는 접근 제어 규칙들을 정의하였고, 이를 접근 제어 엔진으로 사용하는 접근 제어 시뮬레이션을 위한 모델을 설계하였다. 이 시뮬레이션 모델은 사용자의 직무를 기반으로 하는 접근 제어 방법을 사용하는데, 특정 직무에 대해 접근 허가를 어떻게 결정하느냐 하는 문제에 대한 해답으로 주체와 객체의 보안 속성 정보와 보안 규칙을 사용하여 접근 허가를 결정하는 단순하면서도 안전한 방법으로 접근 제어 문제를 해결하는 새로운 방법을 제시했다.

접근 제어는 실제의 컴퓨터 시스템에서는 운영체제나 특정한 보안 소프트웨어의 기능인데 이 기능을 위해 보안이 보장되면서 동시에 빠른 접근 제어 처리를 할 수 있는 방법을 찾는 것이 필수적이라고 할 수 있다. 따라서 본 논문에서 제안한 통합 접근 제어 시뮬레이션 모델은 컴퓨터 시스템에서 실제로 접근 제어를 구현하는 경우에 사전 시뮬레이션을 위해 사용할 수 있는 모델 역할을 할 수 있을 것으로 판단된다. 향후에는 본 논문의 시뮬레이션 모델을 기반으로 하고, 윈도우즈 서버 2003의 웹서버를 이용하여, 직무 계층상의 직무를 해당 직무 계정에 맵핑하는 방법을 통해서 실제의 컴퓨터상에서 동작하는 시뮬레이터를 개발하는 연구를 계속하고자 한다.

참고문헌

[1] Ravi S. Sandhu, Edward J. Coyne, "Role-Based Access Control Models", IEEE Computer, pp.8-47, Feb., 1996.

[2] Warwick Ford, "Computer Communications Security-Principles, Standard Protocols and Techniques", Prentice Hall, pp. 149-176, 1994.

[3] Shari Lawrence Pfleeger, "A Framework for Security Requirements", Computer & Security, Vol. 10, pp. 511-523, 1991.

[4] ISO, "OSI-Security Frameworks in Open Systems -Part 1: Security Frameworks Overview", ISO/IEC DIS 10181-1, 1993.

[5] ISO, "OSI-Security Frameworks in Open Systems-Part 3: Access Control", ISO/IEC DIS 10181-3 , 1993.

[6] Ingrid M. Olson, Marshall D. Abrams, "Computer Access Control Policy Choices", Computer & Security, Vol. 9, pp. 699-714, 1990.

[7] Ravi Sandhu, Qamar Munawer, "How to do Discretionary Access Control Using Roles", In Proc. of ACM 3rd Workshop on RBAC, pp. 47-54, 1998.

[8] Gail-Joon Ahn, Ravi Sandhu, Myong Kang, Joon Park, "Injecting RBAC to secure a Web-based Workflow System", In Proc. of ACM 5th Workshop on RBAC, pp. 1-10, 2000.

[9] Elisa Bertino, Piero Andrea Bonatti, Elena Ferrari, "A Temporal Role-based Access Control Model", In Proc. of ACM 5th Workshop on RBAC, pp. 21-30, 2000.

[10] 이호, "웹 기반 응용을 위한 직무 기반 접근 제어 모델의 설계", 한국 사이버테러 정보전 학회 논문지, Vol. 2, No. 2, pp. 60-62, 2002

[11] 이호, "안전한 직무 기반 접근 제어에 대한 연구", 한국 OA 학회 논문지, Vol. 6 No. 4, pp. 119-124, 2001.

[12] 이호 "웹 기반 응용 시스템을 위한 안전한 직무 기반 접근 제어 모델에 관한 연구", 박사 학위 논문, 성균관 대학교 대학원 정보공학과, 2002

[13] 이호, "웹 기반 응용을 위한 직무 기반 접근 제어 시스템 모델 설계", 한국 컴퓨터 정보학회 논문지, Vol. 9, No. 3, pp. 67, 2004

저 자 소 개

이 호

1989년 벨기에 VUB 대학원 정보공학과 공학 석사

2002년 성균관 대학교 대학원 정보공학과 공학 박사

1982년~1991년 한국전자통신연구원 선임 연구원

2002년부터 국립 한국재활복지대학 정보보안과 부교수