통합 직무기반 접근제어 모델 설계

박 진 호* 안 성 진**
*송호대학 정보산업계열 교수
**성균관대학교 컴퓨터교육학과 교수

요 약

본 논문에서는 접근제어 요구 사항의 복잡한 문제를 해결하기 위한 직무기반 접근제어 모델을 설계하였다. 본 논문에서 설계한 접근제어 모델은 직무기반 접근제어를 이용하여 권한을 효과적으로 통제하고, 신분 및 규칙기반 접근제어를 이용하여 정보의 비밀성, 무결성 및 가용성의 보장과 불법적인 유통을 방지할 수 있다. 설계된 접근제어 모델은 직무, 보안등급, 무결성 등급 및 소유권 등의 다단계 보안 정책을 기반으로 하여 자원에 대한 불법적인 접근을 방어 할 수 있다.

Design of Integrated Role-Based Access Control Model

Park Jin Ho* Ahn Seong Jin**

ABSTRACT

This paper design a role-based access control model that can resolves the complicated problems of access control requirements. In this paper, we designed an access control model which can control a permission making use up role-based access control, can guard the confidentiality, integrity and availability of information and can control illegal information flow. The designed access control model can protect resources from unauthorized accesses based on the role, multi-level security policies of security level, integrity level and ownership.

1. 서 론

컴퓨터와 정보통신망의 사용이 확대됨에 따라 컴퓨터 시스템은 다양한 응용과 사용자를 지원하며, 데이터의 보안에 대한 관심이 증가되었다. 시스템관리자와 프로그램 개발자들은 특정한 데이터와 자원에 대하여 정당한 사용자만 접근할 수 있도록 하기 위한 여러 종류의 접근제어 모델에 관심을 가지게 되었다.

접근제어의 목적은 컴퓨팅 자원, 통신 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다[1][2]. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령어의 실행 등을 포함한다. 즉, 접근제어는 각 자원에 대한 비밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며, 이러한 서비스들의 권한 부여를 위한 수단이 된다[3][4].

개방형 정보 통신망에서 접근제어는 실제의 어떤 개방 시스템에 있는 물리적 실체, 파일과 같은 논리적 실체, 그리고 일반적 사용자와 같은 다양한 형태의 실체들과 연관된다[5]. 접근제어의 결정은 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고, 어떤 조건하에서 접근할 수 있는지를 다루는 문제이다. 즉, 이러한 결정은 접근제어 정책에 반영이 되고, 접근 요청은 접근 정책을 시행하는 접근제어 메커니즘을 통하여 시행된다[2].

현대의 복잡한 정보 통신 응용에서 한가지 정책이나 모델이 필요한 접근제어 요구사항을 모두 만족시킬 수 없다. 또한, 다양한 정책들을 배타적인 관계가 아니라 공통의 목적을 위하여 상호 보완적으로 사용 할 수 있다.

따라서, 본 논문에서는 직무기반 접근제어를 이용한 권한의 통제와 사용자의 신분 및 규칙기반 접근제어를 이용한 비밀성과 무결성 보장 및 정보의 흐름제어를 할 수 있는 직무기반 접근제어 모델을 설계하고자 한다.

2. 직무기반 접근제어

직무는 접근제어 정책의 기본규칙을 작성하기 위한 의미론적 구성개념이다. 시스템관리자는 직무기반 접근제어에 의해 회사나 조직에서 수행되는 일의 기능에 따라 직무를 만들고, 이러한 직무에 대하여 권한을 부여하며, 사용자를 자신의 일에 대한 특정한 책임과 자격을 기본으로 하여 작성된 직무에 부여한다.

직무는 특정한 일에 대한 자격을 나타내며 권한과 책임이 함께 통합된 것이다. 권한과 책임은 자격과는 별개의 것이다. 한 사람이 여러 부서를 관리할 자격은 가질 수 있지만, 책임은 실제적으로 관리하는 하나의 부서에 대하서만 가진다. 직무는 또한 특정한 의무가 여러 사람에게 분산되어지는 것도 반영할 수 있다. 직무기반 접근제어는 직무 개념의 모든 표현에 쉽게 적응시킬 수 있다.

직무는 자원을 접근하도록 허락된 특정 개인과 접근할 수 있는 자원의 범위 모두를 정의한다. 예로, 운영자 직무는 모든 컴퓨터 자원에 접근할 수 있지만 접근 권한을 변경할 수 없고, 보안관리자 직무는 권한을 변경할 수 있지만 자원에 대한 접근은 할 수 없고, 보안 감사 직무는 감사자료에만 접근할 수 있다. 직무는 Novell NetWare, MS Windows 2000등의 시스템 관리를 위한 사용되고 있으며 직무기반 접근제어는 표준화 영역에서도 강한 관심을 보이고 있다. Oracle v7.0에서의 직무 구현을 기초로 하여 database management system을 위한 SQL3 표준의 한 부분으로 고려되고 있다.

사용자와 권한에 대한 특정한 결합은 시간에 따라 변하는 직무와 함께 수행됨으로 직무와 관련된 권한은 더욱 안정적이다. 즉, 직무가 나타

내는 일의 기능을 수행하는 사람보다 직무는 변화의 빈도가 작기 때문에 직무를 기반으로 하는 보안관리가 권한을 기반으로 하는 것보다는 더 간단하다. 사용자는 변화가 필요할 경우 단순히 다른 직무에 배정되기만 하면 된다. 조직에서 새로운 응용이나 시스템이 필요한 경우, 직무는 새로 부여되는 권한만 부여받으면 된다.

직무기반 접근제어가 유용하다고 널리 알려졌지만, 실제 사용하는 것에 대해서는 호응도가 작다. 이러한 결과로, 직무기반 접근제어는 연구자와 시스템 개발자에 의해서 자주 연구되고 있다. 직무기반 접근제어의 최적의 변화는 직무간, 권한과 직무간, 그리고 사용자와 직구간의 관계 확립을 위한 능력을 포함한다. 예로, 한 사람의 사용자가 두 개의 직무를 모두 수용할 수 없는 상호 배타적인 직무가 형성될 수 도 있다. 직무들은 상속관계를 얻을 수도 있고, 반면에 다른 직무에 정해진 권한을 상속시킬 수도 있다. 이러한 직무와 직무간의 관계는 의무의 분산과 저작권의 위임을 통하여 보안 정책을 강화시킬 수도 있다.

직무기반 접근제어에서는 직무권한 관계가 미리 정의되어질 수 있다. 이러한 것은 미리 정해진 직무에 사용자를 할당하는 것을 쉽게 만든다. 직무에 권한을 할당하는 것은 직무에 사용자를 할당하는 것 보다 비교적 적게 일어난다. 이러한 것은 보안관리자가 새로운 직무를 만들거나 직무에 대한 권한을 변형시키지 않고 사용자에게 이미 만들어진 직무를 수여할 수도 취소할 수 있게 하는 것이 바람직하다. 사용자를 직무에 할당하는 것이 직무에 권한을 할당하는 것보다 기술적으로 단순하다. 직무기반 접근제어가 아니면 어떠한 권한을 어떤 사용자에게 부여할 것인가를 결정하기가 매우 어렵다.

접근제어 정책은 직무에 대한 권한, 사용자와 직무 및 직무와 직무간의 관계와 같은 요소들로 직무기반 접근제어에 포함되어진다. 이러한 요소들이 종합적으로 시스템내의 특정 정보에 대한 특정한 사용자의 접근을 허락할 것인가에 대한 결정을 할 수 있다. 직무기반 접근제어의 요소들은 시스템관리자에 의해서 직접적으로 또는 시스템관리자가 권한을 위임한 적절한 직무에 의해서 간접적으로 구성될 수 있다. 시스템에서 시행되는 정책은 시스템관리자에 의해서 수행된 직무기반 접근제어 요소의 특정 구성의 결과이다. 접근제어 정책은 시스템 생명주기에 따라 변하기 때문에 직무기반 접근제어는 조직의 변화되는 필요성을 충족할 수 있도록 접근제어를 변경할 수 있도록한 기능을 통해서 중요한 장점을 제공한다.

3. 통합 직무기반 접근제어 모델 설계

규칙기반 접근제어는 신분기반 접근제어를 완전히 대체할 수 없으며 또한, 직무기반 접근제어가 신분기반 접근제어와 규칙기반 접근제어를 완벽하게 병합한 것이 아닌 상호보완의 관계이다. 이러한 3가지의 접근제어에 기초한 새로운 접근제어 모델을 수립하고 적용할 환경에 적합한 모델로 발전시킬 필요가 있다.

본 논문에서는 3 가지 접근제어가 상호 보완적인 관계에서 작용하도록 접근제어 모델을 설계하고자 한다. 비밀성 보장을 위해서 BLP 모델의 기본 원리인 No Read-Up Secrecy와 No Write-Down Secrecy를 만족시키는 단순-보안성질(simple - security property), 임의-보안 성질(discretionary-security property)과 스타-보안 성질(*-security property)을 이용하고, 무결성 보장을 위해서는 Biba 모델의 엄격한 무결성 정책(strict integrity policy)과 접근제어 리스트(access control list)를 이용하여 비밀성과 무결성 및 정보의 흐름제어가 가능한 직무기반 접근제어 모델을 설계한다.

3.1 기본 설계 개념

망 객체(network object)는 컴퓨터 자원을 사용하고, 데이터를 저장하고, 특정 서비스를 수행할 수 있는 망상의 모든 실체(entity)를 의미한다. 실체는 인간과 같은 능동적 실체와 웹 서버나 데이터베이스 서버와 같이 수동적 실체일 수도 있다. 망 객체는 망상에서 유일한 구분자를 가지고 있고, 각각의 구분자에는 자신이 망상에서 수행할 수 있는 작업에 대한 할당된 권한을 가지고 있다. 이러한 모든 망 객체는 접근제어를 위한 기본적인 정보를 제공하는 ACI(Access Control Information)에 존재한다<표 1>.

<표 1> Access Control Information

object-ID	security -level	integrity -level	owner	role
o1	Top Serect	Crucial	o2	r1
o2	Secret	Important	o2	r2

<표 2> Role-Table

role	permission	access control list
r1	crw--	mail server, web server
r2	-rwxd	C++, mail server

비밀성 등급(security level)은 실체의 비밀성 수준을 나타내는 계층적 분류 체계로서 Top Secret > Secret > Confidential > Unclassified와 같이 분류하고, 무결성 등급(integrity level)은 실체가 소유하는 정보의 수정에 관한 권한의 수준을 나타내는 계층적 분류 체계로서 Crucial > Very Important > Important와 같이 분류한다.

직무(role)는 망 객체가 수행할 수 있는 작업을 말한다. 이것은 하나의 망 객체 또는 여러 개의 망 객체와 관련되고 각각 다른 권한을 부여받는다. 모든 직무와 권한 및 접근 가능한 망 객체는 role-table에 명시되어 있다<표 2>.

직무의 계층적 표현은 더욱 명확한 구조적인 권한부여를 한다. 직무의 계층적 구조는 조직내의 논리적 권한과 책임의 구조와 동일하다. 직무는 상위 직무가 하위 직무를 지배하는 구조로써 하위 직무의 모든 권한을 상위 직무가 상속한다.

권한(permission)은 망상의 객체들이 수행할 수 있는 동작의 종류를 의미하며, 보안관리자가 망상의 객체에 이러한 권한을 부여한다. 본 논문에서 설계하고자 하는 모델에서는 create, read, write, execute, delete 등의 권한을 정의한다.

3.2 접근제어 규칙 설계

3.2.1 접근제어 규칙 표기법 정의

접근제어 규칙의 표현에서 사용된 표기법을 정의한다. 집합 표현에서의 대소문자는 집합과 원소를 나타내며, 함수 표현에서의 매개 변수들은 실체를 나타낸다.

- S : 접근제어의 주체 집합, s∈S
- O : 접근제어의 객체 집합, o∈O
- P : 접근 권한 집합, P={c, r, w, x, d} p∈P, (c ; create, r ; read, w ; write, x ; execute, d ; delete)
- S_Level(a) : 비밀성 등급 함수
- I_Level(a) : 무결성 등급 함수
- PERMISSION(role, a) : role의 a에 대한 권한 검색 함수
- owner(a) : 소유권자 함수
- get_ACI(a) : ACI 요구 함수
- exist_ACI(a) : ACI에 대해서 a의 존재 여부 확인 함수

3.2.2 직무기반 접근제어 설계

직무기반 접근제어 모델의 보안 특성을 이용한 규칙으로서 주체(s)가 객체(o)에 대하여 수행

체는 ACI에 존재해야 하며, 주체는 객체에 대한 적절한 접근권한을 소유해야 하고 있어야 한다.

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

3.2.3 규칙기반 접근제어 설계

강력 접근제어 규칙은 비밀성 보장을 위하여 주체의 비밀성 등급이 객체의 비밀성 등급을 지배할 때는 read와 execute 권한을 허용하고, 주체의 비밀성 등급이 객체의 비밀성 등급이 동일할 때는 create와 delete권한을 허용한다. 무결성 보장을 위해서는 주체의 무결성 등급과 객체의 무결성 등급이 일치할 때만 create, write, execute 및 delete 권한을 허용한다.

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

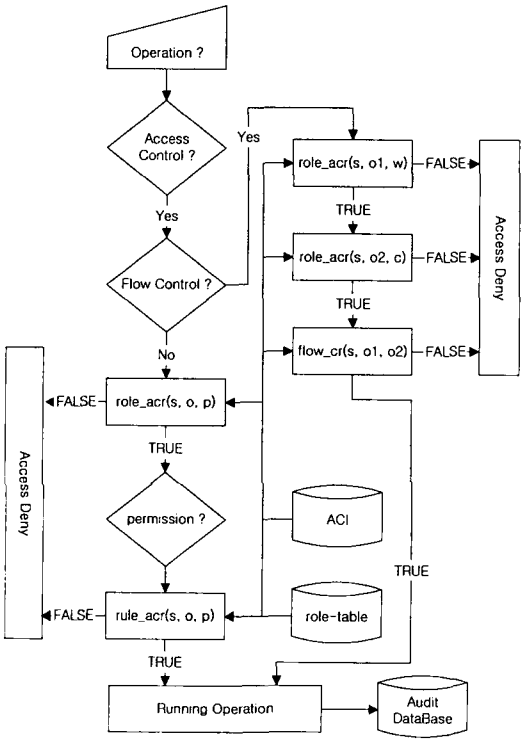
3.2.4 흐름제어 설계

흐름 제어 규칙은 상위의 보안 레이블을 가진 실체가 하위 보안 레이블을 소유한 실체로의 상위 보안 레이블 정보를 전달해 주는 것을 방지하기 위한 규칙이다. 즉, 하위의 보안 레이블을 소유한 실체가 제3자인 상위 보안 레이블의 실체로 가장하거나 결탁하여 정보를 observe할 수 없게 하기 위한 것이다. 주체(s)가 한 객체가 소유한 정보(o1)를 다른 객체(o2)로 전달하기 위한 move 오퍼레이션은 주체가 두 객체에 대하여 보안 레이블이 지배 관계에 있어야 하고, 두 객체간에는 보안 레이블과 무결성 등급이 일치해야만 한다.

```
flow_cr(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
```

3.3 접근제어 모델 구성

앞에서 설계한 접근제어 규칙을 사용한 접근제어 모델의 구성은 (그림 1)과 같다.



(그림 1) 직무기반 접근제어 모델 구성도

4. 결 론

본 논문에서는 조직내의 직무를 사용하여 권한을 엄격히 통제할 수 있도록한 직무기반 접근제어, 보안등급, 무결성 등급 및 소유권 등을 이용하는 다단계 보안 체계를 이용하여 권한의 불법적 사용을 방지할 수 있도록한 규칙기반 접근제어 및 다단계 보안 체계를 이용하여 각 보안등급간의 정보의 흐름을 제한함으로써 정보의 불법적 유통을 차단할 수 있도록한 흐름제어 방법 등을 설계하였다.

본 논문에서 설계한 직무기반 접근제어 모델은 각 조직내의 서로 다른 보안 요구사항을 효과적으로 충족시키기 위해서 조직내의 직무를 기반으로 하여 각 직무에 따라 권한을 부여함으로써 융통성을 제공한다.

참고문헌

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

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

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

[4] Wen-Pal Lu, Maluk K. Sundareshan, "A Model for Multilevel Security in Computer Networks", IEEE Transactions on Software Engineering, Vol. 16, No. 6, pp.647-659, June 1990.

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

[6] McLean J., "The Specification and Modeling of Computer Security", IEEE Computer, Vol. 23, pp.9-16, 1990.

[7] Gregory B. White, Eric A. Fisch , Udo W. Pooch, "Computer System and Network Security", CRC Press, Inc., 1996.

[8] Ravi S. Sandhu, Hal Feinstein, "A Three

Tier Architecture for Role-based Access Control", In 17th NIST-NCSC National Computer Security Conference, Baltimore, MD., pp.34-46, Oct. 1994.

[9] Silvana C., Maria G. F., Giancarlo M., Pierangela S., "Database Security", ACM Press, 1995.

[10] Harrison M.A., Ruzzo W.L., Ullman J.D., "Protection in operating systems", Comm. ACM, 19(8), pp.461-471, 1976.

[11] Clark D. D., Wilson D. R., "A Comparison of Commercial and Military Computer Security Policies", IEEE Symp. On Security and Privacy, New York, pp.184-194, 1987.

[12] Ravi S. Sandhu, "Lattice-Based Access Control Models", IEEE computer, pp.9-19, Nov., 1993.

[13] Roos Lindgreen, Herschberg I. S., "On the Validity of the Bell-LaPadula Model", Computer & Security, Vol. 13, pp.317-338, 1994.

[14] Biba K. J., "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, The MITRE Corp., 1977.

[15] Denning D.E., "A Lattice Model of Secure Information Flow", Comm. ACM, 19(5), pp.236-243, May, 1976.

[16] Silberschatz Galvin, "Operating System Concepts", Addison-Wesley, 1994.

[17] Ian M. Symonds, "Security in Distributed and Client/Server Systems - A Management Views", Computer and Security, Vol. 13, pp.473-480, 1994.

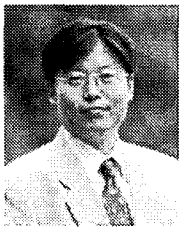
[18] Simson Garfinkel, Gene Spafford, "Practical UNIX Security", O' Reilly and Associates, 1994.

[19] R.S. Sandhu and E.J. Conyne, "Role-Based Access Control Models", Computer, pp.38-47, Feb. 1996

박 진 호

1995년 대전대학교 전자계산학과(공학사)
1997년 대전대학교 컴퓨터공학과(공학석사)
1997년 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부(박사수료)
2000년 ~ 현재 송호대학 정보산업계열 전임강사
관심분야 : 네트워크 관리, 보안

안 성 진



1988년 성균관대학교 정보공학과 졸업(공학사)
1990년 성균관대학교 대학원 정보공학과 졸업 (공학석사)
1998년 성균관대학교 대학원 정보공학과 졸업 (공학박사)
1990년 ~ 1995년 한국전자통신연구원 연구 전산망 개발실 연구원
1996년 정보통신 기술사 자격 취득
1999년 ~ 현재 성균관대학교 컴퓨터교육과 조교수
관심분야 : 네트워크 관리, 트래픽 분석 , 보안관리