2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

다단계 데이터베이스 역할기반 제어 보안 모델

조준호*, 김응모*
*성균관대학교 전기전자 및 컴퓨터공학과
e-mail:sting333@chollian.net

Security Model Using Role-Based Access Control in Multi-Level Database System

Jun-Ho Jo*, Ung-Mo Kim*
*Dept of Electronic & Computer Engineering,
Sung-Kyun-Kwan University

요약

역할 기반의 접근제어 시스템은 응용에 따라 보호 객체들에 대한 접근을 역할들로 분류하고 이를 책임 있는 사용자에게 할당함으로써 개개의 사용자들에게 권한을 할당, 회수하는 전통적인 기법에 비해 단순하고 편리한 권한 관리를 제공한다. 다단계 보안 시스템은 각 시스템의 주체와 객체에게 보안 등급을 부여하고, 등급별로 분리된 정보의 보안을 유지하기 위해서 다중 보안 단계에서 정보를 처리하는 강제적 접근 제어를 제공한다. 본 논문에서는 MAC 기반의 데이터베이스 환경에서 최소 권한 정책을 반영하기 위하여 역할 기반의 접근 제어 기법을 적용한다. 따라서 같은 등급 혹은 그 이상의 등급을 가진 사용자라 할지라도 실제 데이터베이스 내에 저장된 데이터에 대한 권한 없는 접근, 고의적인 파괴 및 변경을 방지함으로써 실제 기업 환경에 적합한 다단계 역할기반 보안 모델을 제시한다.

1. 서론

최근 컴퓨터 기술의 급격한 발전과 컴퓨터 사용자들의 기하 급수적인 증가로 인한 방대한 정보의 보안 문제가 심각하게 대두되고 있다. 또한 컴퓨터 시스템과 정보 시스템들이 네트워크를 통해 서로 연결되고 정보 공유가 이루어짐에 따라 보안의 중요성은 더욱 커져가고 있다. 컴퓨터 보안의 주목적은 컴퓨팅 자원, 통신 자원 및 정보자원 등에 대하여 허가되지 않은 접근을 방지하는 것이다. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령의 실행을 의미한다. 즉, 컴퓨팅 자원에 대한 적절한 통제를 통해 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한부여를 제공할 수 있다. 본 논문에서는 See View 모델을[5] 바탕으로 한 강제적 접근제어(이하 MAC : Mandatory Access Control) 기반의 데이터베이스 환경에서 등급이 부여된 데이터들을 역할로 구성하고 주체(subject)에게 할당함으로써 같은 등급 혹은 그 이상의 등급을 가진 주체에게 최소 권한 정책을 제공하는 방법에 대해 언급한다. 데이터베이스 보안을 위한 접근 방법으로는 엄격한 보안 정책에 적합한 다단계 데이터베이스 보안 시스템과 최소 권한 정책에 적합한 역할 기반의 데이터베이스 보안 시스템을 들 수 있다. 다단계 데이터베이스 보안 시스템은 각 시스템의 주체와 객체에게 보안 등급(security level)을 부여하고, 등급별로 분리된 정보가 하위 등급으로 흘러 내려가는 것을 방지하는 보안 시스템이다.[1] 즉, 이는 사용자를 위한 하나 이상의 보안인가 등급(security clearance level)과 시스템 내의 데이터들을 위한 하나 이상의 분류 등급(classification level)을 가진 시스템을 말하며, 이러한 등급을 이용하여 인가 받지 않은 사용자로부터 기밀정보의 유출을 제어하는 기법들을 제공함으로써 수직적 보안을 유지한다. 역할 기반의 데이터베이스 접근 제어 시스템에서는 사용자에게 직접 객체에 대한 접근 권한을 부여하기보다는, 조직 내에서 책임과 자격에 근거하여 역할에 사용자들이 부여된다. 따라서 역할에 할당된 사용자들만이 그 역할이 포함

하고 있는 권한을 행사할 수 있다. 따라서 조직상 기능들의 변경에 의해 새로운 권한이 추가되고, 더 이상 필요 없는 권한들이 삭제될 때, 혹은 역할에 대한 사용자가 취소되거나 추가될 때 권한관리와 유지보수가 단순화되는 장점이 있다. 본 논문에서는 MAC 기반의 데이터베이스 환경에서 최소 권한 정책을 적용하기 위해 역할 기반 접근 제어 기법을 적용함으로써 등급간의 수직적 보안과 더불어 같은 등급 혹은 그 이상의 등급을 가진 사용자들간의 수평적 보안을 제공하는 기법에 대해 소개하고자 한다.

2. 역할기반 접근제어 (Role-Based Access Control)

역할기반 접근제어(이하 RBAC) 기법의 개념은 1970년대에 온라인 시스템 상에서 다중 사용자와 다중 응용으로부터 시작되었다.[2] RBAC의 기본개념은 역할과 권한이 관련되고, 사용자는 적절한 역할에 지정된다는 것이다. 역할은 조직 내에 다양한 작업 함수에 따라 생성되고, 사용자는 그들의 자격과 책임에 기초하여 역할에 지정된다. 사용자는 하나의 역할에서 다른 역할로 쉽게 재 지정될 수 있고, 역할은 새로운 응용으로써 새로운 권한을 부여받을 수 있다. 또한 필요에 의해 권한이 역할로부터 회수될 수도 있다. 이는 권한관리에 있어서 유연성과 편리함을 제공한다. RBAC 기법의 중요한 특징은 권한의 남용을 방지하기 위한 최소 권한 정책을 실현하고 역할에 대한 책임을 분명히 구분할 수 있는 의무분리 정책을 제공하는 것이다.

역할은 자신의 이름과 자신에 포함된 특권(Privilege)들의 집합으로 구성된다. 특권은 객체와 객체상의 접근 모드의 쌍으로 구성되는데, 일반적으로 다음과 같이 정의한다.

● 특권(Privilege) : (o,m) [단, o는 object를 뜻하고 m은 해당 object의 접근모드를 뜻한다.]
● 역할(Role) : (rname,rpset) [단, rname은 역할의 이름을 뜻하고 rpset은 특권들의 집합을 뜻한다.]
● 안전한 역할(Secure Role) : (ranme,rpset,racl) [한 시스템에서의 역할의 이름은 유일하며 역할마다 racl(role access control list)를 등록함으로써 사용자에게 할당된다.]

본 논문에서는 기존의 역할개념을 MAC에 적용하기 위해서 보안 정책에 위배되지 않는 형태로 역할을 표현한다. 이는 역할을 구성하고 있는 특권(Privilege)의 등급을 바탕으로 역할의 등급을 부여하는 것인데, 이는 4절에서 소개한다.

3. 강제적 접근제어 (Mandatory Access Control)

TCSEC[3]에서 정의한 MAC의 개념을 살펴보면 주체와 객체에 각각 인가등급(clearance)과 분류 등급(classification level : Top-Secrete[TS], Secrete[S], Confidential[C], Unclassified[U])을 부여하고 각 등급간의 관계 및 접근 정책을 명시한다. 즉, 객체에 포함된 정보의 비밀성(레이블로 표현된 보안등급)과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 인가등급에 근거하여 객체에 대한 접근을 제한하는 방법을 의미한다. MAC의 핵심은 보안등급이 높은 정보가 낮은 등급으로 흘러 내려가는 방지하는 것이다. 이는 주체와 객체, 그리고 보안등급을 정의하고 이들간의 관계에 있어서 일정한 규칙을 적용함으로써 정보의 흐름을 제어한다. MAC 기반의 시스템에서는 모든 주체와 객체는 보안등급이 부여되는데, 시스템에서의 주체는 사용자, 응용 프로그램 등의 능동적인 행위를 하는 대상이 되며 객체는 시스템상의 자원 등과 같은 수동적인 대상이 된다.[4] 본 논문에서는 MAC에서 가장 일반으로 알려진 Bell-Lapadula(이하 BLP) 모델을 적용하고 이 모델에서 정의한 Simple Security Property와 *-Property를 준수한다.

● Simple Security Property : Subject s can read object o only if $L(s) \geq L(o)$
● *-Property : Unstrusted subject s can write object o only if $L(s) \leq L(o)$

이 두 가지 규칙에서 전자는 "no read up", 후자는 "no write down" 규칙을 의미한다. 이 규칙을 데이터베이스 환경에서 준수하기 위해서는 See View 모델에서 소개한 Polyinstantiation 기법을 사용한다.[5]

4. 다단계 데이터베이스 시스템에서의 역할 구성

BLP 모델에서 상위등급의 정보가 하위등급으로 흘러 내려가는 것을 막기 위해 두 가지 규칙을 정의하였다. 하지만 이 개념만으로 데이터베이스 환경에 적용하기 위해서는 많은 제약사항들이 존재한다.[5] 이를 해결하기 위해 See View 모델에서는 TCB를 기반으로 한 MAC 환경에 다단계 데이터베이스를 구축하고 BLP 모델의 규칙을 준수하기 위한 여러

가지 기법이 소개되었다.[5] 사용자들은 자신에게 부여된 등급의 인스턴스(instance)를 접근하게 되는데 자신이 가지고 있는 등급 이하의 정보들만 인스턴스에 나타나며 상위 등급의 데이터들은 NULL값으로 표시된다. 또한 Polyinstantiation을 이용하여 하위 사용자가 상위 데이터를 무단으로 변경하거나 상위 사용자가 하위 데이터영역에 정보를 유출하는 것을 방지하였다. 본 논문에서는 이러한 개념을 바탕으로 다단계 데이터베이스 시스템이 갖는 문제점을 지적하고 새로운 관점에서 이를 보완하는 방안을 제시하였다.

다단계 데이터베이스 시스템에서의 문제점은 사용자가 자신이 가진 등급이하의 모든 정보에 대한 접근 권한을 가지고 있는데서 비롯된다. 예를 들어 S-등급의 사용자가 테이블을 생성하면 S-등급 혹은 그 이상의 사용자에게 모든 정보가 공개된다. 이는 실제 조직이나 기업환경에서 개인간 혹은 부서간의 심각한 정보의 유출을 초래한다. 또한 같은 등급 혹은 그 이상의 등급을 가진 모든 사용자들이 접근할 수 있기 때문에 수 많은 Polyinstantiation을 발생시킨다. 이는 저장공간의 낭비 및 어떠한 정보가 사실인가를 결정하는 문제를 야기시킨다. 따라서 다단계 데이터베이스 시스템에 역할을 이용한 최소 권한 정책을 적용함으로써 등급간의 보안과 등급내의 보안을 제공하는 것이 본 논문에서 제안하는 바이다. 역할개념을 도입함으로써 역할에 할당된 사용자들에 근거하여 책임자를 선별하는 것이 가능하고 일반 조직이나 기업환경에서 직무기반의 접근 통제를 제공한다. 역할은 임의적 접근제어(이하 DAC : Discretionary Access Control)의 성격을 포함하고 있는데 MAC 정책에 위배되지 않는 범위 내에서 권한의 전파를 통해 유연성을 제공한다. 또한 객체에 접근하는 사용자의 수를 제한하기 때문에 Polyinstantiation을 감소시킨다. 실제로 다단계 데이터베이스 환경에서 역할을 구성하는 방법은 다음과 같다.

Table1[U]: U등급을 가진 사용자 u에 의해 생성
Table2[C]: C등급을 가진 사용자 c에 의해 생성
Table3[S]: S등급을 가진 사용자 s에 의해 생성
Table4[TS]: TS등급을 가진 사용자 ts에 의해 생성

위의 테이블들은 각각 등급이 부여되어 있기 때문에 DAC에서 역할을 구성하는 방법과 차이가 있다. 역할을 구성하고 역할이 포함하고 있는 등급들을 바탕으로 역할의 등급을 부여하는 방법은 다음과 같다.

● L(Role)=[Null] (단, 특권집합이 공집합일때)
● L(Role)=[Min $L(o_i)$, Max $L(o_j)$]{$L(o_k)$} (단,$k \geq 1$)
: 역할이 포함하고 있는 특권들의 집합 중에서 최소, 최대 등급으로 역할의 등급을 나타낸다. 단, 여기서 L(s), L(o), L(Role)은 각각 주체, 객체, 역할의 등급을 의미한다.

역할 이름	특권 집합(Privilege Set)	등급
RoleA	(T1[U],r/w),(T2[C],r/w),(T3[S],r)	U,S
RoleB	(T1[U],r/w),(T2[C],r)	U,C
RoleC	(T1[U],r/w),(T2[C],w),(T3[S], r)	U,S
RoleD	(T1[U],r/w),(T2[C],r/w),(T4[TS],r/w)	U,TS
RoleE	(T1[U],r/w],(T2[C],r/w),(T3[S]r/w) (T4[TS],r/w)	U,TS
RoleF	$\emptyset$	Null

[표 1 역할 등급]

[표1]에서는 역할 구성하고 그것의 등급을 나타내었다. 역할F는 최소 역할(MinRole)을 나타내며 특권을 포함하고 있지 않기 때문에 등급을 Null로 표시하였다. 역할E는 모든 역할의 특권을 포함하고 있으므로 최대 역할(MaxRole)이 된다. 역할을 주체에게 할당할 때에는 다음과 같은 규칙을 따른다.

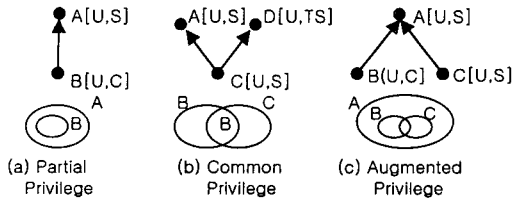
● L(s) ≥ L(Min L(o)) : 주체의 보안등급은 역할의 최소 등급과 같거나 크다.

주체 s의 등급은 S이므로 s를 RoleD[U,TS]에 할당하는 것이 가능하다. 그러나 s가 RoleD에서 사용할 수 있는 특권은 s의 등급보다 같거나 작은 등급의 특권들로 제한된다. 따라서 주체가 같은 역할을 할당받았다고 하더라고 주체의 등급에 따라 특권을 사용하는 것이 차별화 된다. 즉, 주체가 역할이 포함하고 있는 특권들을 사용할 수 있는 조건은 자신에게 부여된 등급 이하의 특권들만 사용할 수 있다는 것이다. 이는 주체와 역할이 세션에 의해 연결될 때 참조 모니터(reference monitor)를 두어 감시한다.[6]

5. 역할 계층 (Role Hierarchy)

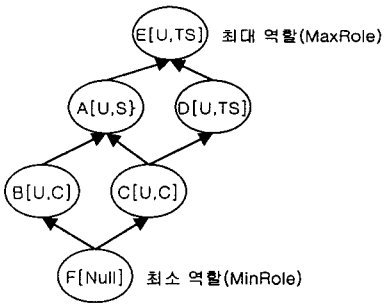
시스템 상에 존재하는 역할들은 자신이 포함하고 있는 특권에 따라 계층을 형성한다. 이러한 계층 구조를 그래프 형태로 표현하는 것이 가능한데, 역할은 그래프 상위 노드(node)로, 역할간의 관계는 단

방향의 단선(edge)으로 표현된다.[7,8]



[그림 1] 역할 관계의 3가지 종류

[그림1]은 기본적인 역할 관계의 3가지 종류를 나타내고 있다. 이러한 종류의 관계를 바탕으로 역할 그래프(Role graph)를 형성하게 되는데 [표1]은 이러한 3가지 종류의 역할 관계를 모두 반영하고 있다. [그림1]의 [a]를 보면 역할A는 역할B의 특권들을 모두 포함하고 있기 때문에 B→A로 표현하였다. 다시 말해 B는 A의 하위역할(junior role)이라 불리고 역할A는 역할B의 상위역할(senior role)이라 불린다. 따라서 역할 그래프를 참조하면 역할간의 포함관계 및 전체적인 구조를 쉽게 파악할 수 있다.



[그림 2] 표1의 역할 그래프(Role graph)

[그림2]는 [표1]의 역할들의 관계를 그래프 형태로 나타낸 것인데 이는 *Role Graph Property*를 모두 만족한다.[7,8]

6. 결론 및 추후 연구과제

본 논문에서는 See View 모델에서 제안한 MAC 기반의 다단계 데이터베이스 환경에서 역할이 부여된 객체들에 대한 특권들을 역할로 구성하고 이를 사용자에게 할당함으로써 최소 권한 정책을 실현하였다. 역할은 등급이 부여된 객체를 포함하기 때문에 역할에 등급을 부여하는 방법을 소개하였으며 주체에게 할당하기 위한 조건 및 주체가 실제로 사용가능한 역할내의 특권들에 대해 알아보았다. 또한 역할간의 관계를 그래프로 표현함으로써 관리자에 의한 중앙 관리가 용이하다는 것을 살펴보았다.

추후 연구 과제는 제안한 모델을 보다 정형화된 방식으로 기술하고 실제 조직이나 기업환경에서 필요로 하는 정책에 따라 역할에 등급을 부여하고 주체에게 할당하는 방법을 좀더 세분화하고 다양화하여 좀더 유연한 다단계 데이터베이스 보안 모델을 제시하는 것이다.

7. 참고 문헌

[1] R.S. Sandhu. Lattice-based access control models. *Computer*, 26:9-19, Nov.1993

[2] Ravi Sandhu, Qamar Munawer, "How to do Discretionary Access Control Using Roles", *Proceeding of 3th Workshop on Role-Based Access Control*, Fairfax, Virginia, October 22-23, 1998

[3] U.S. Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200. 28-STD, National Computer Security Center, 1985

[4] S. Castano, M. Fugini, G. Martella, and P. Samarati. *Database Security*. Addison Wesley, 1994

[5] TERESA F. LUNT, DORTHY E. DENNING, ROGER R. SCHELL, MARK HECKMAN, and WILLIAM R. SHOCKLEY, "The See View Security Model", *IEEE TRANSATION ON SOFTWARE ENGINEERING*, VOL. 16, NO. 6, JUNE 1990

[6] Nat. Comput. Security Center, Dep. Defense Trusted Computer system Environment Criteria, Tech. Rep. DOD 5200.28-STD, Dec. 1985.

[7] R.S Sandhu. Role hierarchies and contraints for lattice-based access controls. In *Compter Security - ESORICS 96*, page 65-79. Springer Verlag, 1996. Lecture Notes 1146.

[8] M. Nyanchama and S. L. Osborn. Access rights administration in role-based security systems. In J. Biskup, M. Morgenstern, and C. E. Landwehr, editors, *Database Security, VIII, Status and Prospects, Proceedings of the IFIP WG11.3 Working Conference on Database Security*, pages 37-56. North-Holland, 1994.