제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

상세 접근 제어를 위한 데이터베이스 보안 모델

이금순, 김영호, 원용관
전남대학교 컴퓨터공학과
e-mail:{ks0403, melchi, ykwon}@grace.chonnam.ac.kr

Database Security Model for Detail Access Control

Keum-Soon Lee, Yong-Ho Kim, Yonggwan Won
Dept of Computer Engineering, Chonnam National University

요 약

데이터베이스를 사용하는 정보가 다양해짐에 따라 요구사항 또한 다양해져서 데이터 하나 하나에 대한 접근제어의 필요가 요구되고 있다. 이러한 데이터별 접근제어를 만족하는 보안정책을 정의하고, 정보의 기밀성, 무결성 및 가용성을 유지하는 데이터베이스 보안 모델을 제안한다. 본 논문의 목적은 공통된 data에 대하여 다양한 유형의 접근제어와 지속적으로 변화가 요구되는 접근제어 요구에 대한 해결방법을 제공한다.

1. 서론

다양한 사용자들로 인해 정보를 저장 및 관리하는 데이터베이스에 대한 보안이 필수적인 요소가 되었다. 접근제어의 목적은 컴퓨팅 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다[1]. 정보 생산량의 증가로 인하여 데이터베이스의 규모가 증가하고, 이에 따른 사용자별 정보 접근의 요구사항 또한 다양해져서 이를 효율적으로 관리해 줄 수 있는 보안정책이 필요하다.

기존의 연구된 보안정책들에서는 객체(object: 정보의 집합)에 대한 주체(subject: 정보 접근자), 주체의 역할 또는 보안등급으로 접근제어를 하였다[1]. 그러나, 데이터베이스를 사용하는 영역이 넓어지면서 기존의 방법보다 더욱더 미세한 접근 제어가 필요하게 되었다. 즉, 공통된 하나의 정보에 대하여 사용자별 접근 권한이 보안 등급만으로 정의되기에는 부족한 정도의 세분화가 필요하고, 또한 사용자별 접근권한이 수시로 변동될 필요가 있게 되었다.

본 논문에서는 이러한 데이터 및 사용자별 세밀한 접근제어 권한을 부여하는 보안정책을 정의하고, 정책의 변화를 유연하게 수용하면서 정보의 기밀성, 무결성 및 가용성을 유지할 수 있는 데이터베이스 보안 모델을 제안한다. 제안하는 모델은 임의적 접근제어(DAC: Discretionary Access Control)방식, 강제적 접근제어(MAC:Mandatory Access Control) 방식 및 역할 기반 접근제어 (RBAC: Role Based Access Control)방식을 적절히 조합하여 보안요구사항을 만족토록 하였다.

본 논문의 제2장에는 기존에 연구된 내용을 요약하였고, 3장에서는 사용자 및 데이터의 정의, 접근제어 규칙을 기술하고, 4장에서는 보안정책을 정의하였다. 5장에서는 구현 및 결과를 기술하고, 마지막으로 6장은 본 연구에 대한 결론을 맺었다.

2. 관련연구

2.1 DAC(Discretionary Access Control)

DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공한다. 한 사용자가 객체를 접근할 수 있는 자신의 권한을 다른 사용자에게 허가(grant) 할 수 있다는 면에서 정책은 임의적이다. DAC 정책에는 개인-기반(Individual-Based Policy:IBP)과 그룹-기반(Group-Based Policy:GBP)정책을 포함한다. IBP는 아래의 [표1]과 같이 어떤 사용자가 어떤 객체에 접근할 수 있는지 접근행렬의 열로 표현한다

[표 1] 권한부여 행렬

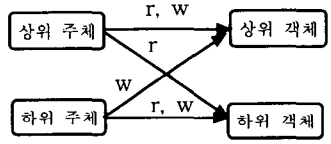
객체 / 주체	파일 1	파일 2	파일 3
사용자 1	r,w	exec	exec
사용자 2	-	-	cr, del
사용자 3	r,w	r	-

r:read, w:write, cr:create,
del=delete, exec:execute

GBP는 다수의 사용자를 그룹으로 묶어 표현함으로 보다 쉽고 효율적인 정책 표현이 가능하다. DAC의 단점은 사용자가 인가 받은 접근이라 할지라도 접근 제한을 우회(bypass)할 수 있다는 것이다[4].

2.2 MAC(Mandatory Access Control)

MAC 정책은 시스템의 주체와 객체의 보안등급에 기초해서 정보에 대한 접근을 통제하는 모델로서, 대표적인 모델은 BLP(Bell-LaPadula) Model[5]을 들 수 있다. BLP Model은 각 보안등급간에 상위등급의 정보가 하위등급으로 유출되는 것을 방지하기 위한 모델이다. 객체와 주체간의 보안등급은 U(Unclassified), C(Classified), S(Secret), TS(Top-Secret)의 4단계로 구분하며, 보안등급은 U에서 TS로 올라 갈수록 높아진다. BLP Model은 No Read-Up Secrecy와 No Write-Down Secrecy 두가지 법칙을 갖는다. 아래의 [그림1]과 같이 No Read-Up 성질은 높은 보안등급의 정보가 하위 보안 등급으로 유출되는 경로는 허용하지 않으므로 정보의 기밀성을 보장하고 있으나 하위등급의 사용자가 상위등급의 객체에 Write를 할 수 있으므로 정보의 무결성은 유지할 수 없다.



[그림1] BLP 보안모델의 성질

2.3 RBAC(Role Based Access Control)

RBAC 정책은 신분-기반 정책과 규칙-기반 정책의 특성을 모두 가진 상업용 환경에 적합한 정책으로서, 자신의 직무에 따라 접근 할 수 있는 정보가 결정되고, 사용할 수 있는 정보의 한계가 정해진다[2][3].

3. 사용자 및 데이터의 정의, 접근제어 규칙

3.1 사용자

사용자는 정보 접근의 주체(subject)로서 데이터베이스의 사용자 또는 사용자 그룹으로 다음과 같이 정의한다. 사용자 집합 $U=\{ u_1, u_2, u_3, \cdots, u_p \}$, p는 사용자의 수. 사용자 소속 그룹 $G=\{ G_1, G_2, G_3, \cdots, G_n \}$, n은 사용자 그룹 수. 사용자의 보안등급에 따라 그룹 $H=\{ H_1, H_2, \cdots, H_m \}$, m은 보안 등급의 수. 사용자 $u_i=\{ u_i \in G_j \} \cap \{ u_i \in H_k \}$, 직무에 따른 사용자 세부 그룹 $G_j=\{ G_{j1}, G_{j2}, \cdots, G_{jq} \}$, $j=\{1,2,\cdots,n\}$, $l=\{1,2,\cdots,q\}$ q은 G_j의 세부 그룹의 수. 사용자 그룹에 속한 사용자의 수: $1 \le N(G_j) \le p$, 직무 그룹에 속한 사용자의 수: $1 \le N(G_{jl}) \le p$ 이다.

3.2 Data

Data는 정보의 집합을 나타내는 객체(object)로서 하나의 Data 또는 Data Group으로 정의한다. 그룹화는 크게 두가지 방법에 준한다. 첫째, 모든 데이터는 Field Name을 기준으로 하여 보안등급으로 그룹화 한다. 둘째, Detail한 그룹화 방법으로 Table Name, Field Name, Record Key의 조합으로 아래의 세가지 단위로 정의된다.

· DtAC(Detail Access Control)의 Group화 단위

① Table 전체, DG_T={Table Name}

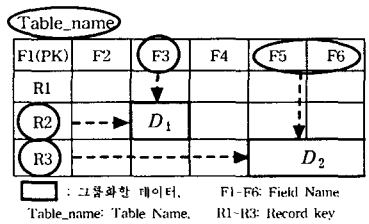
② Table 과 Field

DG_F={Table Name, Field Name}

③ Table 과 Field 와 Record

DG_R={Table Name, Field Name, Record Key}

아래의 [그림2]는 Group화 단위 DG_R에 의해 Group화 한 예이다.



[그림2] DG_R에 의한 Group화

$$D_1=\begin{pmatrix} Table\ Name \\ F3 \\ R2 \end{pmatrix}, \quad D_2=\begin{pmatrix} Table\ Name \\ F5, F6 \\ R3 \end{pmatrix}$$

[수식1] 데이터 그룹 D_1, D_2의 표현식

접근제어를 원하는 데이터 D_1은 Field Name F3과 Record Key R2가 만나는 곳으로 하나의 Data Group으로 [수식1]과 같이 정의하여 접근을 제어 할 수 있다.

3.3 접근제어 규칙

[규칙1] S_level ≥ O_level : 주체의 보안등급이 객체의 보안등급보다 크거나 같으면 주체가 객체를 지배한다고 표현하며 접근이 허용된다.

[규칙2] P(s, d, m) : Detail한 그룹에 대한 접근제어를 표현한다. 이때, $s \in G_j$ 또는 $s \in G_{jl}$

$(j=1,2,\cdots,n\ ;\ l=1,2,\cdots,q)$

$d \in D_r$, $r=\{1,2,\cdots,v\}$ v는 데이터 그룹의 수

$m \in \{r,w,u,d,(r,w),(r,d),\cdots,(r,w,u,d)\}$

만약, $P(G_{jl}, D_r, (r,w))$라면, G_{jl}에 속한 사용자가 D_r 그룹의 데이터에 대하여 Read, Write 권한이 있음을 나타낸다.

4. 보안 정책의 정의

4.1 배경

보안 요구사항을 제시했던 조혈계질환 유전체연구센터의 조직구성은 연구과제에 따라 5개의 그룹으로 구성되었고, 각 그룹은 직무에 의해 소그룹으로 구성되었다. 접근권한은 사용자 등급이 지배하는 객체에 접근하나, 특정 데이터는 관리자가 임의로 권한부여 한 사용자만이 접근을 허용한다.

4.2 보안정책

[정책1] S_level ≥ O_level :주체의 보안등급이 객체의 보안등급을 지배하면 Read, write, update를 할 수 있다.

[정책2] 사용자 u_i 가 $\{u_i \in G_j\}$ 이고 G_{jl} 에 속하는 특정 user는 G_j 에 속한 data에 대해 update가 가능하다.

[정책3] 관리자만이 delete를 허용한다.

[정책4] 권한 관리자가 특정 그룹으로 정의한 data는 접근모드를 허가해 준 user만 접근이 가능하다. P(s, d, m)
단, (S_level≥ O_level)

위의 [정책1]은 MAC의 응용으로 주체와 객체를 보안등급으로 분류하였고, [정책2] [정책3]은 RBAC의 응용으로 특정 Role에 속한 User들에게 권한이 제한되며, [정책4]는 DAC의 응용으로 특정 User에게 접근 권한을 허용하였다.

5. 구현 및 결과

상기와 같은 정의를 기반으로 제안된 방안을 전남대학교병원 조혈계질환 유전체연구센터의 데이터베이스 시스템에 적용하였다.

5.1 사용자 및 데이터

사용자와 모든 데이터 Field는 보안등급이 부여되며 아래의 [표2]와 [표3]과 같은 구조로 정의하였다.

[표 2] Data Security Level

field name	Type(size)	key	nn	description
Field_no	number(10)		not null	auto num
Table_name1	varchar2(30)	primary	not null	physical name
Table_name2	varchar2(50)	primary	not null	logical name
Field_name1	varchar2(50)		not null	physical name
Field_name2	varchar2(50)		not null	logical name
Security_level	varchar2(1)		not null	Security level

[표 3] User Security Level

field name	Type(size)	key	nn	description
User_no	number(10)		not null	auto num
User_id	varchar2(15)	primary	not null	User_id
Password	varchar2(15)		not null	User_password
User_class	varchar2(12)		not null	Group (Gj)
Role	varchar2(1)		not null	Role Group (Gjl)
Security_level	varchar2(1)		not null	Security level(Hk)

Detail Access Control를 위한 Data Group의 구조는 [표4]와 같이 정의하였고 권한관리자에 의해 그룹이 생성된다.

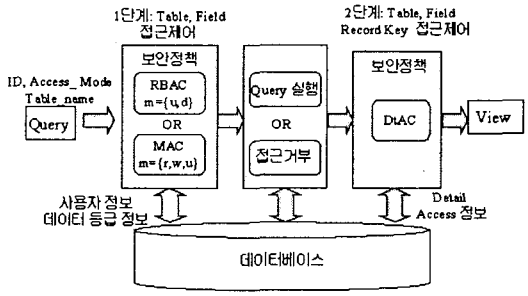
[표 4] Detail Access Permit

field name	Type(size)	key	nn	description
Group_no	number(10)	primary	not null	auto num
Table_name	varchar2(50)		not null	Table name
Field_name	varchar2(50)			Field name
Record_key	varchar2(50)			Record key
Users_id	varchar2(50)		not null	Users
Access_mode	varchar2(10)		not null	Access_mode

5.2 시스템의 구조 및 접근제어

보안정책을 적용한 시스템의 구조를 아래의 [그림3]으로 표현하였다. 제안된 보안정책은 File내의 프로그램으로 설정되었고, Query문이 들어오면 1단계 Module을 include하고 View전에 2단계 Module을 include하여 사용한다. Query문을 통해 ID, Access Mode, Table Name의 정보를 받아 m={r,w,u}이면 MAC Module에 의해 접근가능 한 Field Name과 Field 수를 가져오고 Query문은 재생

성 된 후 실행된다. m={u,d}이면 RBAC Module에 의해 접근제어 되고, Query의 실행 또는 접근거부가 결정된다. 실행된 Query문은 2단계 DtAC Module에서 그룹이 정의되었고, ID가 없으면 Null로 대체되고, ID가 있으면 그대로 View 된다. 보안정책은 1단계에서 Table과 Field 단위로 등급과 Role에 의해 폭넓게 제어하고, 2단계에서는 Record Key에 의해 Detail한 접근제어를 제공한다.



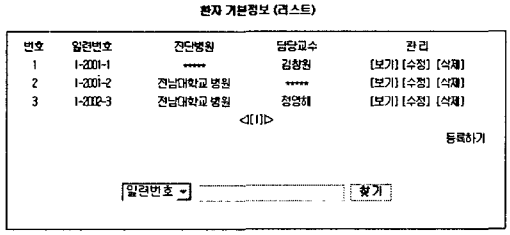
[그림3] 시스템 구조도

5.3 결과

ID가 ks0403인 사용자가 Query문 SELECT * FROM Table_Name;을 던졌을 때 1단계에서 m={r}이므로 사용자 등급이 지배하는 Field Name을 Select하여 Query문은 실행된다. 2단계에서는 [표 5]의 그룹권한 설정에서 ks0403 사용자에게 접근을 허용하고 있지 않는 데이터에 대해 '*****' 문자로 대체되어 출력된다. 그 결과화면은 아래의 [그림4]에 나타내었다.

[표 5] DtAC의 Data Group 설정

Group NO	Table Name	Field Name	Record Key	User_id	mode
1	환자정보	진단병원	1-2001-1	sckim	r
2	환자정보	담당교수	1-2001-2	sckim	r, w



[그림4] 결과 화면

6. 결론

데이터베이스를 활용하는 정보가 다양해짐에 따라 사용자는 데이터 각각에 대해 접근 제어를 요구하는 새로운 요구사항이 도출되어 본 논문에서는 이를 해결하고자 하는 정책기반의 데이터 보안 시스템으로 사용자 및 데이터를 그룹화하고 기존의 보안모델인 MAC, DAC, RBAC의 특성을 조합하여 사용자별 세분화된 데이터의 접근제어를 수행하게 하였다.

보안정책은 주체와 객체의 보안등급으로 분류하여 정보의 기밀성을 유지하고, 하위 주체가 상위 객체에 write를 허용하지 않으므로 정보의 무결성을 보장한다. 또한, 하나의 data에 대한 보안이 필요한 경우 P(s, d, m) 그룹을 정의하여 접근을 제어한다. DtAC는 세부적인 접근제어를 제공하지만 필요한 경우 추가 생성하므로 그룹의 수가 증가하여 시스템의 성능을 저하시킬 우려가 있다. 이러한 문제는 Field Name과 사용자가 같은 그룹을 통합하여 재정의 하는 방법으로 향후 더 연구되어야 할 것이다.

참고문헌

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

[2] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, "Role-Based Access Control Models," IEEE Computer, Vol.29, No.2, pp.38-47, Feb. 1996.

[3] D. Richard Kuhn, "Mutual Exclusion of Role as Means of Implementing Separation of Duty in Role Based Access Control Systems," National Institute of Standards and Technology, Jun. 1996.

[4] Lewis, S.; W iseman, S. Securing an object relational database. Computer Security Applications Conference, 1997.

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