2000 년 한국정보처리학회 추계 학술발표논문집 제 7 권 제 2 호

이중 보안 레벨 기반의 다단계 관계형 모형

김상석*, 김응모*
*성균관대학교 전기전자컴퓨터 공학부
e-mail : upstone@ece.skku.ac.kr

Multilevel Relational Model based on Double Security Model

Sang-Suk Kim*, Ung-Mo Kim*
*Dept. of Electronic & Computer Engineering , SungKyunKwan University

요 약

DAC 정책을 기반으로 하는 DBMS에서 데이터에 대한 사용자의 접근 통제는 접근 규칙 데이터베이스에 저장된 접근 규칙을 바탕으로 이 사용자가 접근 하려는 데이터에 접근 권리가 명시적으로 기술되었는지를 확인하므로 써 수행된다. MAC 정책은 각 시스템의 주체와 객체에게 보안 등급을 부여하고, 등급별로 분리된 정보의 보안을 유지하기 위해서 다중 보안 단계에서 정보를 처리하는 강제적 접근 권한을 제공한다. 본 논문에서는 실제 MAC 정책을 기업 환경에 적용시키는데 있어서는 많은 제약사항이 존재하고 있으며, 이러한 제약사항 중에 레벨별로 정보의 공유가 필요할 경우에 레벨간에 최대, 최소를 둠으로써 레벨간의 정보 공유를 가능하게 만들고자 하는 모델을 제안하고자 한다.

1. 서론

급격한 정보화 추세에 따른 컴퓨터의 대량 보급과 통신망의 확대는 사용자의 편리성과 효율성을 극대화 시키며 국가 산업 경쟁력의 바탕이 되고있으나, 컴퓨터 시스템의 장애 또는 부정한 방법으로 피해를 일으키는 컴퓨터 범죄와 개인의 사생활 침해, 그리고 컴퓨터 바이러스 등 역기능적인 부작용도 중요한 문제가 되고 있다. 컴퓨터 시스템에서 보안의 필요성은 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 판독하거나 또는 부적절하게 기록하는 것을 방지하며, 그리고 정당한 권한을 갖는 사용자의 정보 처리 서비스를 컴퓨터 시스템에서 거부하지 않도록 보호하기 위한 것이다.

본 논문에서는 데이터베이스 관리 시스템(database management system : DBMS) 이 보안성이 제공될 수 있도록 현재까지 관계형 DBMS 에 대해 연구 개발된 기본적인 보안 접근 제어 기술과 MAC 정책에 해당하는 SeaView 모델에서 레벨별로 정보의 공유를 위해 레벨들의 집합에 대해 설명한다.

2. Relational DBMS 를 위한 보안 모델

관계형 DBMS 에서 데이터의 보호는 DAC 정책과 MAC 정책에 해당하는 보안 모델을 기초로 하여, 이를 관계형 데이터베이스에 적합하도록 확장한 접근 제어 모델에 의해 이루어진다.

2.1 DAC 정책

DAC 정책을 기반으로 하는 DBMS 에서 데이터에 대한 사용자의 접근 통제는 접근 규칙 데이터베이스에 저장된 접근 규칙을 바탕으로 이 사용자가 접근 하려는 데이터에 접근 권리가 명시적으로 기술되었는지를 확인하므로써 수행된다. 따라서, 접근 모델은 접근 규칙의 구조를 기술하고, 그리고 접근 규칙을 생상하고 삭제 시키는 접근 규칙의 관리방법이 정의 되어야

한다.

DBMS 가 유지하는 접근 제어 규칙 데이터베이스에서 특정 접근 규칙을 삭제 시키는 것은 특정 사용자에게 부여된 접근 권리를 철회 시킴으로써 수행되며, 이때 사용하는 방법으로 cascading revoke 와 noncascading revoke 가 있다.

cascading revoke 는 사용자 A 에게서 특정 테이블 T 에 대한 권리 P 를 사용자 X 가 철회하면 그 결과는 A 에 부여된 권리가 부여되지 않은 상태로 된다. 다시 말해서, 특정 권리를 철회하면 다른 사용자에게 접근 권한을 부여한 규칙들이 모두 연쇄적으로 제거되는 효과를 갖는다.

noncascading revoke 는 X 가 권한을 철회할 경우 X 의 권한만 철회되고, 다른 사용자의 권한을 철회되지 않는다. 다시 말해 noncascading revoke 는 자신이 권한을 철회하면 다른 사용자에게 부여된 권한은 철회시키지 않고, 그 사용자에게 주어진 권한만 철회시키는 방법이다.

대부분의 관계형 DBMS 는 명시적인 접근 규칙에 기초한 문맥 기반(context based) 보안을 시행하고 있으나, 데이터 내용에 기반한 접근 제어를 시행할 수 있다. 예를 들어 사용자가 하나의 테이블을 생성하고, 테이블의 속성값이 100 이하인 튜플에 대해서만, 읽기 권한을 주려고 할 경우에, 하나의 뷰를 정의한 후 이 뷰에 대해서 읽기 권한을 부여하면 내용 기반 접근 제어가 시행 될 수 있다.

2.2. Multilevel Security 모델

MAC 정책은 데이터베이스의 테이블과 튜플, 필드에 보안등급을 결합시키는 방법을 사용하고 있다. 다단계 보안 모델인 SeaView 는 MAC 정책을 시행하여 데이터 접근을 통제하고, 데이터의 보안 등급을 결정하는 TCB(Trusted Computing Base) 모델로 구성된다.

MAC 모델의 구성은 주체, 객체, 접근 권리, 보안등급(classification)으로 이루어 진다. 보안 등급은 BLP 와 Biba 모델의 보안 등급과 무결성 등급을 통합한 구조를 갖는다.

다단계 릴레이션은 기존의 단위 릴레이션이 여러 수준의 보안 등급을 포함하도록 확장 시킨 구조이며, 튜플의 모든 항목과 튜플 전체에 대한 보안 등급이 결합된 형태를 갖는다. 이러한 다단계 릴레이션에는 이 릴레이션이 MAC 정책에 위배되지 않도록 반드시 만족해야 하는 여러 형태의 무결성 제약 조건들이 다단계 보안 모델별로 다양하게 정의한다.

STARSHIP	OBJECTIVE	DESTINATION
Voyger	Exploration	Talos
Explorer	Spying	Rigel

<표 1. 단일 값 릴레이션>

STARSHIP	K_C	OBJECTIVE	DESTINATION	T_C
Voyger	U	Exploration	Talos	U
Explorer	S	Spying	Rigel	S

<표 2.다단계 릴레이션>

- Multilevel entitiy 무결성

주키(primary key)를 구성하는 속성들의 값은 어떤 튜플 내에서도 동일한 보안 등급을 갖으며, 주키 속성 값의 보안 등급은 튜플에 존재하는 다른 모든 속성들 값의 보안 등급에 의해 dominate 된다.

- Multilevel referential 무결성

외래키가 존재하면, 참조되는 주키를 포함하는 튜플 또한 그 보안 등급에서 반드시 접근해야한다.

주키의 값이 동일하지만 키값의 보안 등급이 서로 다른 여러 개의 튜플들이 동시에 존재할 수 있다. 이 경우를 다중 인스턴스이라 한다. 예를 들면 한 사용자가 특정 릴레이션에 동일한 값을 갖는 데이터가 높은 보안 등급에 이미 존재할 때 낮은 등급의 보안 등급을 갖는 사용자가 높은 등급의 보안 등급을 갖는 데이터가 존재한다는 사실을 추론 할 수 있으므로 이 연산을 거부 할 수 없다. 이 경우에 다중인스턴스가 발생한다. 또한 높은 등급의 사용자가 데이터를 update 할려고 했을 때 낮은 등급의 데이터에 이러한 사실이 반영되므로, 이러한 경우를 막기 위하여 다중 인스턴스를 발생시킨다.

STARSHIP	K_C	OBJECTIVE	DESTINATION	T_C
Voyger	U	Exploration	Talos	U
Explorer	S	Spying	Rigel	S
Explorer	U	Exploration	Rigel	U

< 표 3.다중 인스턴스 >

3. 이중 보안 레벨 기반의 다단계 관계형 모델

이 모델은 SeaView 모델을 기초로 하여 레벨별로 정보의 공유가 이루어질 수 있는 모델이다.

이모델에서 데이터베이스 접근 제어를 위한 모델의 구성 요소로는 주체, 객체, 주체와 객체의 보안 등급 (기존의 단일 보안 등급에서 보안 등급에 최대, 최소값으로 확장), 보안 등급의 제약 조건이 있다.

제안한 모델의 특징은 객체의 보안 레벨이 최대, 최소값을 갖는 레벨의 리스트로 표현하여 정보를 공유하고 싶은 레벨들이 접근을 보장하고 공유하고 싶지 않은 레벨에 정보의 노출을 막기 위해서 제약조건이 존재한다.

- security labels

L_0 : the set of security levels

각 subjects 는 clearance level $l \in L_0$ 을 가지고 있다.

security labels L 을 정의하면

if $l \in L_0$, then $l \in L$

if $l_i, l_j \in L$, then $l_i \cup l_j \in L$

$L=\{l_1 \in L, l_2 \in L, .., l_n \in L \mid l_1, l_2, .., l_n\}$

$\leq$: the dominate relation

$L=[l_i, l_j]$: l_i 와 l_j 를 최대 최소로 하는 level 들의 집합이다.

예를들면 B-L 모델의 보안 등급(" unclassified" ≤" classified" ≤ " secret" ≤" top-secret")에서
L = [U, S] 는
L = {U ∈ L, C ∈ L, S ∈ L | U, C, S}를 의미한다.

● 키 제약 조건

K : the set of key attributes
$A_1, A_2, \cdots, A_n$: all nonkey attributes
Kc : A key classification level
Tc : A tuple classefication level

1. K, Kc, Tc → $A_1, A_2, \cdots, A_n$
2. Kc_i: I 번째 tuple 의 key classification level
   Kc_j: j 번째 tuple 의 key classification level
   K_i: I 번째 tuple 의 key attribute
   K_j: j 번째 tuple 의 key attribute
   If $K_i = K_j$, then $Kc_i \cap Kc_j = \emptyset$
3. 어떤 tuple 안에서 Kc 와 Tc 의 관계는 Tc ∈ Kc 을 만족해야 한다.

● operations

access property : 특정 레벨에 있는 데이터를 read, update 하기 위해서는 그 레벨에 있는 user 만이 할 수 있다.

OPERATION	SUBJECT LEVEL	OBJECT LEVEL	CONDITION
Read	l	$L = [l_i, l_j]$	$LL(L) \le l \le GL(L)$
update	l	$L = [l_i, l_j]$	$LL(L) \le l \le GL(L)$

GL(Greatest Level) : GL(L)은 L 의 레벨 집합 중 가장 상위 레벨을 의미한다.
LL(Lowest Level) : LL(L)은 L 의 레벨 집합 중 가장 하위 레벨을 의미한다.
예를 들면 L = [C, TS]
GL (L) = TS
LL(L) = C
Subject 의 보안 등급이 l 이고 object 의 보안 등급이 L 일때 subject 는 $LL(L) \le l \le GL(L)$만 read , update 가 가능하다.

<BASE TABLE>

STARSHIP	Kc	OBJECTIVE	DESTINATION	Tc
Voyger	[U,C]	Exploration	Talos	[U,U]
Explorer	[S, TS]	Spying	Rigel	[S,TS]
Voyger	[S,S]	Exploration	Talos	[S,S]

<TS - INSTANCE>

STARSHIP	Kc	OBJECTIVE	DESTINATION	Tc
Null	Null	Null	Null	Null
Explorer	[S, TS]	Spying	Rigel	[S,TS]
Null	Null	Null	Null	Null

<S - INSTANCE>

STARSHIP	Kc	OBJECTIVE	DESTINATION	Tc
Null	Null	Null	Null	Null
Explorer	[S, TS]	Spying	Rigel	[S,TS]
Voyger	[S,S]	Exploration	Talos	[S,S]

<C - INSTANCE>

STARSHIP	Kc	OBJECTIVE	DESTINATION	Tc
Voyger	[U,C]	Null	Null	Null
Null	Null	Null	Null	Null
Null	Null	Null	Null	Null

<U - INSTANCE>

STARSHIP	Kc	OBJECTIVE	DESTINATION	Tc
Voyger	[U,C]	Exploration	Talos	[U,U]
Null	Null	Null	Null	Null
Null	Null	Null	Null	Null

4.결론

본 논문에서는 관계형 데이터베이스에서 보안 모델을 적용하기 위한 보안 모델을 MAC 정책의 한 모델인 SeaView 모델에서 레벨들간에 정보를 공유하기 위한 방법을 제시하였다. 이 방법은 기존의 단일 레벨에서 최대, 최소를 이용한 복수개의 레벨을 사용함으로 써 레벨별로 데이터의 공유가 이루어지는 방법을 살펴보았다. 그러나 이 방법은 실제 기업 환경에서 적용하기 위해서는 레벨들의 세분화가 필요하고, 세분화된 레벨들의 관계를 규명하는 연구가 향후에 이루어져야 한다.

참고문헌

[1] Bell D.E. and La Padula L.J.(1973). Secure Computer Systems:mathematical foundations. ESD-TR-73-278, vol.1-2 ESD/AFSC, Hanscom AFB, Bedford, MA, November 1973(MTR-2547, vol. 1-2 . MITRE Corp., Bedford, MA

[2] Bertino E., Samarati P. and Jajodia S. (1993) High assurance discretionary access control in object bases. In Proc. First ACM Conf. On computer and Communications Security, Fairfax, VA, November 1993

[3] Biba K.J.(1977). Integrity considerations for secure computer systems. ESD-TR-76-372, ESD/AFSC, Hanscom AFB, Bedford, MA, April 1977(The MITRE Corp., MTR-31530

[4] Denning D.E.(1976). A lattice model of secure information flow. Comm. ACM, 19(5)

[5]Denning D.E. et al(1988). The SeaView security model. In Proc. IEEE Symp. On Security and Privacy, Okland, CA, April 988
[6]Jajodia S. and Sandhu R.(1990). Polyinstantiation integrity in multilevel relations. In Proc. IEEE Symp. On Security and Privacy, Oakland, CA, May 1990
[7] Jajodia S. and Sandhu R.(1991a). Toward a multilevel relational data model. In Proc. ACM-SIGMOD Conf., Denver, CO, May 1991
[8] Jajodia S. and Sandhu R.(1991b). Enforcing primary key requirements in multilevel relations. In Proc. 4th RADC Workshop on Multilevel Database Security, Little Compton, Rhode Island, April 1991