通信情報保護學會誌
第6卷 第1號, 1996. 3

# 데이타베이스 보안을 위한 모델

## (Models for Database Security)

박 석*, 양 지 혜*

## 요 약

이제는 암호 체계 또는 운영체제 보안등을 이용하여 데이타베이스 내의 정보를 보호하기에는 불충분하기 때문에 데이타베이스를 위한 보안 정책이 필요하다. 데이타베이스 보안은 어떤 모델을 사용하느냐에 의해 보안의 유지 정도, 사용자의 표현 의도, 연산 수행 결과 등이 결정되기 때문에 모델의 결정이 데이타베이스 보안과 직접적인 관련을 갖는다. 본 논문에서는 주요한 데이타베이스 보안 모델의 특징을 분석하고, 앞으로의 연구 방향에 대해서 살펴본다.

## 1. 서 론

요즘은 널리 보급된 통신망을 이용하여 여러 사용자들이 데이타베이스 내의 데이타를 사용하고 있다. 지금까지 데이타베이스 시스템 보안을 위해서 사용되었던 기법은 사용자 인증을 통해 데이타베이스 접근을 제한하거나, 운영 체제 단계에서 지원하는 보안 정책 수행이 대부분이었다. 따라서, 사용자에 따라 보안 데이타베이스 시스템이 허용하는 데이타베이스 정보만을 제공하는 보다 세분화된 보안 유지가 필요하다.

이러한 보안 요구 사항을 만족시키기 위하여 다음 조건을 만족하는 보다 정확한 데이타베이스 보안 모델이 필요하다. 보안 모델은 보안 데이타베이스 시스템이 갖추어야 할 기능적이고 구조적인 속성을 표현할 수 있고, 또한 사용자의 의도를 충분히 표현할 수 있어야 한다. 데이타베이스에서 모델링이란 개체와 관련된 정보를 어떻게 표현할 것인가와 관련된 부분인데, 이러한 모델에 따라 데이타베이스 시스템의 연산 수행과 병행 수행, 회복 수행 등에 직접적인 영향을 미친다. 또한, 보안 모델은 보안 데이타베이스 시스템이 갖추어야 할 특성을 만족해야 하며, 개념적인 모델에 상응하고 이에 따라 구현되고 있는지가 증명되어야 한다.

* 서강대학교 전자계산학과 데이타베이스 연구실

이 연구는 1994년도 한국과학재단 연구비 지원에 의한 결과임(과제번호:941-0900-038-2)

## 2. 기본적인 보안 모델

데이타베이스 보안 모델은 크게 임의적 보안 모델(discretionary security model)과 강제적 보안 모델(mandatory security model)로 구분할 수 있다[1].

임의적 보안 모델은 사용자들이 정보에 접근하기 위한 정책이 사용자들의 신분 (identity)과 사용자들에게 허용된 권한에 따라 결정이 된다. 임의적 보안 모델에 사용되는 기본 정책은 소유자 권한 정책(ownership policy)인데, 이러한 정책에 따라 객체를 생성한 사용자가 다른 사용자에게 권한을 부여하거나 취소시킬 수 있다. 그러나, 임의적 보안 모델은 이러한 권한의 이동으로 인해 정보가 누출되거나 파괴될 수 있다는 단점을 가진다. 비교적 초기의 데이타베이스 보안 모델들이 여기에 속하는데, 접근 행렬 모델(Access Matrix Model), 선취-허가 모델(Take-Grant Model), 우드 모델(Wood et al. Model) 등이 있다.

강제적 보안 모델은 데이타베이스를 구성하는 데이타와 이를 접근하는 사용자에게 각각 객체 등급(classification)과 주체 등급(clearance)을 부여하고 특정한 보안 정책에 따라 주체의 객체로의 접근 여부를 결정한다.

강제적 보안 모델은 관계형 데이타베이스 시스템에서 다단계 보안 관계형 데이타베이스 모델로 표현되는데, 각 튜플은 키, 키 등급, 속성 (속성 등급), 튜플 등급의 구조를 갖는다. 관계형 데이타베이스에서는 기본적으로 같은 이름을 가진 키를 허용하지 않기 때문에, 키 등급이 다르고 같은 이름을 갖는 키에 대한 보안을 유지하면서 연산을 처리해 주어야 한다. 이처럼 같은 이름의 개체가 서로 다른 등급을 갖는 데이타가 발생하는데, 이를 다중 인스턴스(polyinstantiation)[4][6]라고 한다. 다중 인스턴스는 다중 튜플(polyinstantiated tuple)과 다중 원소(polyinstantiated element)로 구별되는데, 보안 모델은 이들의 무결성을 유지해 주어야 한다. 이러한 다중 인스턴스를 다루는 방법이 보안 모델들간의 주요 차이점인데, 주요한 강제적 접근 모델들은 다음과 같다.

## 2.1 벨-라파둘라 모델 (Bell-Lapadula Model)

대표적인 강제적 보안 모델로는 1970년대에 발표된 군사 보안을 위한 벨-라파둘라 모델이 있다. 이 모델에서는 보안 정책에 의해 정보가 낮은 등급 쪽으로 흐르지 않도록 하기 위해, 다음과 같은 특성을 가진다.

- 단순 보안 속성 : 객체를 읽기 원하는 주체는 주체의 등급이 객체의 등급과 같거나 객체의 등급보다 높아야 한다.
- *-속성 : 한 주체는 자신과 같거나 높은 등급을 가진 객체에 쓰기를 할 수 있다.

즉, 이 모델에서는 보안 정책에 의해 정보가 낮은 등급 쪽으로 흐르지 않도록 하기 위해, 아래로 읽기(read down), 위로 쓰기(write up) 특성을 가진다.

## 2.2 비바 모델(Biba Model)

벨-라파둘라 모델은 정보의 보안만을 고려하기 때문에 정보가 낮은 보안 등급 쪽으로 흐르는 것을 막을 수 있지만 무결성을 보장하지는 못한다. 즉, 보안 등급이 낮은 사용자가 자신보다 상위 등급의 데이타에 쓰기를 수행할 수 있는데, 이 과정에서 상위 등급 데이타의 무결성이 깨어질 수 있다. 이러한 문제점을 개선한 모델이 비바 모델이다. 이 모델은 벨-라파둘라 모델의 보안 등급은 그대로 유지하면서, 사용자에게 무결성 등급을 부여하였다. 따라서, 무결성 등급이 낮은 사용자는 무결성 등급이 높은 데이타를 수정하지 못하게 함으로써 데이타의 무결성이 유지되도록 한다. 비바 모델의 무결성 등급은 벨-라파둘라 모델의 등급과 유사한 범주(Category) 집합과 C(Crucial), VI(Very Important), I(Important) 로 이루어진 계층 등급

으로 이루어져 있다. 즉, 사용자는 자신의 보안 등급 뿐 아니라 무결성 등급으로 데이타로의 접근이 결정되기 때문에, 이 모델에서는 보안 뿐만 아니라 데이타의 무결성도 유지하고 있다.

## 3. 다단계 보안 모델

### 3.1 Sea View 모델

1980년 대 후반에 Stanford Research Institute(SRI)는 관계형 데이타베이스 시스템의 보안을 위해 Sea View(SEcure dAta VIEW) 모델을 개발하였다[1]. Sea View 모델은 강제적 보안 모델과 TCB(Trusted Computing Base) 모델로 구성되어 있다. 강제적 보안 모델은 벨-라파둘라 모델의 정책을 수행하는 참조 모니터 역할을 하고, TCB 모델은 다단계 릴레이션들의 개념을 정의하고, 이를 위한 임의적 보안 정책을 지원한다. TCB의 모든 정보는 참조 모니터가 관리하는 객체들에 저장되어 있는 강제적 보안 모델의 상위에 존재한다고 할 수 있다.

Sea View 모델에서 접근을 제어하는 강제적 보안 모델은 사용자가 데이타 접근을 원할 때, 각 데이타에 필요한 보안성과 무결성 인증을 갖추어야만 접근을 허용하는 작업을 수행한다. 이 과정에서 벨-라파둘라의 공리가 주체, 객체 그리고 접근 방법에 적용된다. 그러나, 상위 등급 데이타에 대한 쓰기는 허용하지 않는다. 모델링에서의 주요 문제점은 데이타 무결성 유지와 다중 인스턴스 관리에 있는데, Sea View 모델에서는 다중 인스턴스와 관련하여 갱신 연산이 다음과 같은 문제점을 갖는다. $C_{name}$, $C_{department}$, $C_{salary}$는 각 속성 값의 등급을 나타내고, TC는 튜플의 등급을 나타낸다. 본 논문에서 등급간의 순위는 내림차순으로 TS 〉 S 〉 C 〉 U인 것으로 가정하였다.

| Name | $C_{name}$ | Department | $C_{department}$ | Salary | $C_{salary}$ | TC |
|---|---|---|---|---|---|---|
| Bob | S | Dept1 | S | 10K | S | S |
| Ann | S | Dept2 | S | 30K | TS | TS |
| Ann | S | Dept2 | S | 20K | S | S |
| Sam | TS | Dept2 | TS | 30K | TS | TS |

그림 1. TABLE : Employee

| Name | $C_{name}$ | Department | $C_{department}$ | Salary | $C_{salary}$ | TC |
|---|---|---|---|---|---|---|
| Bob | S | Dept1 | S | 10K | S | S |
| Ann | S | Dept2 | S | 30K | TS | TS |
| Ann | S | Dept2 | S | 20K | S | S |
| Ann | S | Dept1 | TS | 30K | TS | TS |
| Ann | S | Dept1 | TS | 20K | S | S |
| Sam | TS | Dept2 | TS | 30K | TS | TS |

그림 2. 갱신 후의 Employee

그림 1의 테이블에 등급이 TS인 주체가 다음과 같은 연산을 수행하면,

```
UPDATE Employee
SET Department = "Dept1"
WHERE Name = "Ann"
```

결과는 그림 2와 같다.

위의 예에서 알 수 있듯이, 다중 인스턴스를 다룰 때 각 속성을 단위로 연산이 발생하도록 하였기 때문에 갱신 연산에 의해 의미적으로 불명확한 여러 개의 새로운 튜플(그림 2의 진한색 튜플들)이 생성되는 단점이 있다.

### 3.2 Jajodia-Sandhu 모델

Jajodia-Sandhu 모델은 관계형 데이타베이스 시스템에서 강제적 보안 정책을 수행하는 응용을 위해서 개발되었다. 기본적으로 이 모델은 위로 읽거나 아래로 쓰는 것을 허용하지 않는 속성을 갖고, 한 개체는 각 등급에 많아야 한 개만이 존재하도록 관리한다. 또한 Sea View 모델의 문제점인 갱신 연산시에 불필요한 튜플이 생성되는 단점을 개선하기 위해 각 개체를 개체 등급에 의해 구분하여 연산이 발생하도록 하였다. 정보의 흐름을 보다 정확히 제거하기 위하여 필터 함수를 두어 각 속성마다 사용자 등급과 비교하여 보안 정책이 허용하는 정보만 제공하도록 하였다.

### 3.3 Smith-Winslett 모델[5]

관계형 데이타베이스 시스템을 위해 각 등급별로 다른 데이타베이스를 유지하도록 관리한다. 각 튜플은 키, 키 등급, 속성, 튜플 등급으로 구성되어 있고, 각 주체는 자신의 등급과 같은 등급의 객체만을 관리하고(believe), 자신의 등급보다 낮은 데이타를 참조(see)할 수 있다. 따라서, 읽기는 다른 모델과 같지만, 위로 쓰기(write up)는 허용하지 않는다. 즉, 자신과 같은 등급을 가진 데이타만을 갱신할 수 있다.

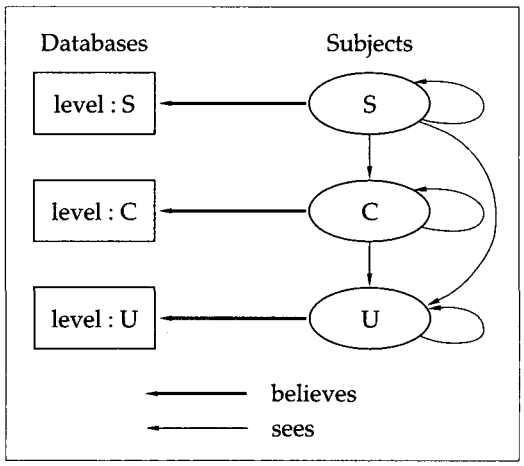


그림 3. 서로 다른 등급간의 주체와 객체와의 관계

위의 "believe" 개념에 의한 해석으로 기존의 보안 모델에서의 문제점인 다중 인스턴스 관리와 해석에 대한 모호성을 해결하고 있다. 그러나, 여러 등급에 걸친 죠인(Join)을 수행할 경우나 하위 등급 데이타들이 변화할 때, 이 모델의 특성으로 인해 하위 등급의 변화가 상위 등급에 즉각 반영되지 않는 문제점이 있다.

### 3.4 다단계 관계형 데이타 모델[3]

다단계 관계형 데이타 모델은 관계형 데이타베이스 시스템에서 강제적 보안 정책을 수행하는 Jajodia-Sandhu 모델을 기반으로 하고 다른 모델들의 장점을 통합한 모델이다. 기본적으로 이 모델에서는 한 개체는 각 등급에 많아야 한 개만이 존재하도록 관리한다. 또한, 갱신 연산 시에 필요 없는 튜플이 만들어지는

Sea View 모델의 문제를 개선하기 위해 각 개체를 개체 등급으로 식별하여 연산이 발생하도록 하였고, 이로 인한 정보의 흐름이 없도록 필터 함수(filter function)를 두어 개체의 각 속성을 사용자 등급과 비교하여 보안 정책이 허용하는 정보만 제공하도록 하였다.

또한, 다단계 관계형 데이타 모델은 LDV (Lock Data View)[2]와는 다른 방법으로 상위 등급 데이타에 대해 쓰기를 허용하고 있는데 이를 비교하면 다음과 같다. 먼저, LDV 보안 모델에서는 하위 등급을 가진 사용자가 상위 등급을 가진 데이타를 자신의 튜플 내에 유지하면서, 하위 등급을 가진 사용자의 읽기를 금할 수 있도록 허용한다. 예를 들면, 테이블 Starship에 대한 등급 S를 가진 사용자의 뷰는 다음과 같다.

| SHIP | OBJ | DEST | TC |
|---|---|---|---|
| Enterprise S | Spying S | Mars S | S |
| Enterprise U | Exploration U | Rigel S | U |

그림 4. S 등급의 사용자의 뷰

등급 U를 가진 사용자의 뷰는 다음과 같다.

| SHIP | OBJ | DEST | TC |
|---|---|---|---|
| Enterprise U | Exploration U | 0 | U |

그림 5. U 등급의 사용자의 뷰

즉, 속성 DEST에 대한 Rigel(S) 정보는 등급 U를 가진 사용자가 상위 등급 사용자를 위해 기록한 데이타이므로 등급 U를 가진 사용자들은 읽을 수 없고, 등급 U를 가진 제한된 사용자들만이 Rigel(S)를 수정할 수 있다.

다단계 관계형 데이타 모델은 "data borrow"라는 개념을 통해서 하위 등급 데이타의 변화가 상위 등급 사용자들에게 전달되도록 한다. 다시 말하면, 임의의 한 등급을 가진 주체가 인정하는 데이타는 같은 등급을 가진 데이타와 낮은 등급으로부터 빌려 온 데이타이다. 이때 낮은 등급으로부터 빌려 온 데이타는 단지 그 하위 등급만이 갱신할 수 있다. 따라서 상위 등급의 주체는 하위 등급 데이타의 변화된 내용을 즉시, 그리고 자동적으로 참조할 수 있게 된다. (즉, 공유하는 데이타의 물리적 주소는 같다.) 또한, 상위 등급이 참조하는 하위 등급 개체에 대한 튜플이 상위 등급에 반드시 존재하도록 관리한다. 위의 정의에 의하여, Table 1과 Table 2는 다른 의미를 갖는다.

| SHIP | OBJ | DEST | TC |
|---|---|---|---|
| Enterprise U | Exploration U | Talos U | S |
| Enterprise U | Exploration U | Talos U | U |

그림 6. TABLE 1

| SHIP | OBJ | DEST | TC |
|---|---|---|---|
| Enterprise U | Exploration S | Talos S | S |
| Enterprise U | Exploration U | Talos U | U |

그림 7. TABLE 2

Table 1에서 S 등급의 주체가 소유하고 있는 모든 데이타는 등급 U의 주체가 소유하고 있는 데이타를 빌려 온 것이기 때문에 등급 U를 가진 주체에 의해서만 수정 가능하다. Table 2의 첫 번째 튜플은 등급 U에 존재하는 개체에 대한 정보이지만, 등급 S의 데이타이기 때문에 등급 S를 가진 주체에 의해서만 수정 가능하다. 따라서, 속성 OBJ와 DEST의 값이 같은 것은 우연한 일이다.

상위 등급 사용자가 참조하는 하위 등급 개체가 있다면 그 개체에 대한 튜플이 하위 등급에 반드시 존재해야 한다는 것이 data-borrow 성질이다. 이것은 data-borrow로 인한 다단계 관계형 모델 내에서 정보가 누출되는 것을 방지하도록 보장해 주고, 하위 등급 데이타의 변화가 상위 등급에 자동적으로 반영된다. 다단계 관계형 데이타 모델은 등급간의 간섭이 없으며 보안 다단계 데이타베이스 모델로서의 공식적인 증명을 갖추고 있다. 지금까지의 데이타베이스 보안 모델들의 특징을 비교하면 표 1과 같다. 초기에는 운영체제 보안과 데이타베이스 보안을 동시에 만족하는 모델들이 설계되었다가 점차 데이타베이스 보안만을 위한 모델들로 발전하게 된다. 또한, 초기의 모델들은 임의적 보안 정책들을 지원하지만, 점차 강제적 보안 정책을 지원하고 있다.

## 4. 능동 데이타베이스와 객체지향 데이타베이스의 보안 모델

능동 데이타베이스란 지식 기반 시스템과 규칙(rule)으로 데이타베이스 내의 사실을 관리한다. 따라서, 능동 데이타베이스에서는 데이타의 무결성을 유지하고, 감사(audit) 기능을 수행을 위하여 규칙을 사용한다. 다음은 POSTGRES에서 감사의 기능을 수행하는 규칙의 예이다.

```
on retrieve to EMP.salary
then do append to AUDIT
(name=current.name,
 salary=current.salary, user=user())
```

즉, 데이타베이스 사용자가 다른 사람의 봉급에 대한 정보를 접근하였을 때, 위의 규칙에 의하여 AUDIT 화일에 기록된다. 3.3절에서 이미 설명한 개체 모델이 능동 데이타베이스에 사용되고 있는데, 강제적 보안 접근 정책이 접근 권한, 연산 수행 등이 규칙을 통해 제어된다.

객체지향 데이타베이스는 복잡한 응용에 적합하기 때문에 최근 많은 관심을 받고 있는데, 객체지향 데이타베이스의 보안을 위해 임의적 보안 정책을 사용하는 시스템으로는 ORION과 IRIS가 있다. ORION에서는 주체와 객체들간

표 1. 보안 모델의 특징

| 모델 | 특징 | | | | |
|---|---|---|---|---|---|
| | OS 보안 | DB 보안 | 임의적 정책 | 강제적 정책 | |
| | | | | 보안 | 무결성 |
| Access Matrix | o | o | o | | |
| Take-Grant | o | o | o | | |
| Wood et al. | | o | o | | |
| Bell-La Padula | o | | o | o | |
| Biba | o | | o | o | o |
| Sea View | | o | o | o | o |
| Jajodia | | o | | o | |
| Smith-Winslett | | o | | o | |

의 관계를 먼저 정의해 두고, 이들간의 계층 구조 등을 고려하여 보안을 유지하고 있다.

객체지향 데이타베이스에서 강제적 접근 정책을 적용하여 상위 정보가 하위 등급 쪽으로 흐르지 않도록 하기 위해서 메시지 필터(message filter)를 둔 모델이 있다. 또한, ORION 모델을 확장하여 강제적 접근 정책을 수행하는 SORION 모델에서는 객체(object), 클래스(class), 메소드(method)에 등급을 부여한다. 만약, 하나 이상의 클래스로부터 속성들을 계승(inheritance)받은 하위 클래스(subclass)내에서 계승된 변수들간의 충돌이 발생하면 가장 높은 등급 클래스의 변수로 결정된다.

한 객체 내의 속성들이 서로 다른 등급을 가질 때, 다단계 개체(multilevel entity)라고 하는데, 이러한 개체를 모델링하는 방법에는 다음과 같다.

첫째, 한 객체에는 같은 등급의 속성만을 유지하는 방법이다. 이 경우 다단계 개체가 여러 개의 객체로 표현되어야 하기 때문에 복잡성이 증가한다는 단점을 가진다. 둘째, 다단계 개체를 등급이 다른 속성들을 갖도록 하기 위해서는 복합 객체(composite object)를 이용한다. 이 방법은 한 객체에 대해 같은 이름의 속성이지만 등급이 다른 값(multivalued attribute)을 표현할 수 있다. 이러한 표현은 첫번째 방법보다 표현력은 우수하지만, 다단계 개체의 경우 하나 이상의 객체를 접근해야 한다는 단점이 있다.

## 5. 결 론

지금까지 데이타베이스에 따라 이에 적합한 보안 모델들에 관하여 소개하였다. 초기에는 객체와 주체의 관점에서 보안을 유지하기 위한 모델들이 제안되었으나, 점차 기존의 데이타베이스의 보안을 위한 모델들이 발표되고 있음을 알 수 있었다. 고유한 장점을 가진 이러한 모델들은 데이타베이스의 보안을 위한 것이지만, 사용자의 표현 의도나 연산 결과와 직접적인 관련이 있기 때문에 좀더 무결성을 가지는 강력한 보안 모델이 요구된다.

앞으로의 연구 방향은 사용자의 의도를 좀더 정확하고 자유롭게 표현하며, 보안을 유지하는 데이타베이스 모델이 개발되어야 할 것이다. 또한 등급간의 간섭이 없고, 데이타의 변화에 능동적으로 반응하며 시스템 가용성이 보장되는 보안 데이타베이스 모델이 필요하다.

## 참 고 문 헌

[1] S.Castano, M.Fugini, G.Martella and P.Samarati, Database Security, Addison-Wiesly, 1995.

[2] T.F.Keefe, W.T.Tasi and J.Srivastava, "Multilevel Secure Database Concurrency Control," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp.337-344, 1990.

[3] F. Chen and R. Sandhu, "The Semantics and Expressive Power of the MLS Data Model," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp.128-142, 1995.

[4] T.F. Lnut and D. Hsieh, "Update Semantics for a Multilevel Relational Database System," DATABASE SECURITY IV, pp281-296, 1991.

[5] K. Smith and M. Winslett, "Entity Modeling in the MLS Relational Model," Proceedings of the 18th VLDB Conference, pp199-210, 1992.

[6] D. Denning, "Lessons Learned from Modeling a Secure Multilevel Relational Database System," DATABASE SECURITY, pp35-43, 1988.

## □ 著者紹介


**박 석**

1978년 서울대학교 계산통계학과 학사
1980년 한국과학기술원 전산학과 석사
1983년 한국과학기술원 전산학과 박사
1983년 ~ 현재 서강대 전자계산학과 교수
1989년 ~ 1991년 University of Virginia 방문교수
1992년 ~ 현재 한국정보과학회 데이타베이스 연구회 부위원장
1993년 ~ 1994년 한국정보과학회 논문지 편집위원
1995년 ~ 현재 통신정보보호학회 논문지 편집위원
1996년 ~ 현재 한국정보과학회지 편집위원

※ 주관심 분야 : 실시간 데이타베이스, 보안 데이타베이스, 주기억장치 데이타베이스, 멀티미디어 데이타베이스 시스템, 트랜잭션 관리, 병행수행 제어

**양 지 혜**

1994년 서강대학교 전자계산학과 학사
1994년 ~ 1996.1 서강대학교 대학원 전자계산학과 석사 과정
1996년 ~ 현재 한국오라클(주)

※ 주관심 분야 : 보안 데이타베이스 모델링 및 병행수행, 객체지향 데이타베이스, 주기억장치 데이타베이스