通信情報保護學會誌
第2卷 第3號, 1992. 9

다단계 보안 데이타 모델

심갑식* · 노봉남**

1. 서 론

과거 수년 동안 대부분 컴퓨터 보안 연구자들은 안전한 운영체제 설계와 구현에 집중하여 왔다. 그러나 이런 노력들은 접근제어(access control) 지향적이어서 운영체제 수준의 객체에 사용자의 접근을 제어하는 것에 관심이 집중되었다. 이들 개념을 데이타베이스 영역으로 확장할 때, 운영체제는 높은 수준(화일 또는 사용자)에서 서비스를 제공할 수 있었지만 데이타베이스 시스템은 더 낮은 수준의 데이타 크기 단위(튜플, 레코드, 필드 등)를 취급해야 하므로 새로운 해결책이 제시되어야 한다.

데이타베이스 보안에서는 보안정책을 실행하는 시스템의 수행능력과 관계되며, 보안정책은 정보의 유출, 수정, 파손 등을 다룬다. 예를 들면, 미국방부의 강제적 보안(다단계 보안) 정책은 인가된 개인에 따라 비밀정보의 접근을 제한한다. 비밀 데이타는 비권한 사용자로부터 직접 접근을 보호해야할 뿐만 아니라, 추론과 같은 간접 수단을 통한 유출을 보호하는 것이 강제적 보안에서는 요구된다. 다단계 데이타베이스 시스템에 대한 요구조건은 특정 응용분야에 따라 다를 수 있으나 다음 특징은 공통적으로 가지고 있다.

(1) 강제적 보안(mandatory security)

컴퓨터 시스템이 다양한 보안등급을 가진 정보를 포함하고 있고 시스템에 포함된 가장 높은 보안등급의 데이타를 접근해서는 않될 사용자가 있을 때 다단계 보안의 필요성이 있다. 보안 등급은 Top Secret(TS) > Secret(S) > Confidential(C) > Unclassified(U)로 나누어진다. 보호되어야 할 정보의 보안등급(classification)은 정보의 비인가된 유출(unauthorized discloure)에서 기인될 수 있는 잠재적 피해에 따라 구별된다. 사용자에게 할당된 보안등급은 기밀 정보를 유출하지 않을 사용자의 신용도를 반영한다.

다단계 데이타베이스 시스템은 다양한 보안등급을 가지는 데이타와 인가등급을 가지는 사용자를 유지하여야 한다. 가장 일반적인 경우라면 데이타베이스에서 원자적 사실(fact)에 각각 보안등급의 부여가 필요하다. 강제적 접근제어의 요구조건은 두 규칙으로 형식화 된다. 첫째는 비권한자에 의한 데이타의 유출을 막는 것이고, 두번째는 데이타의 불법적인 수정을 방지하는 것이다.

첫째, 단순 성질(simple property)

주체 S의 보안등급이 객체 O의 보안등급 보다 같거나 높을 때 주체 S는 객체 O를 판독(read) 할 수 있다.

둘째, *-성질(star-property)

* 통신정보보호학회 정회원, 전남대학교 전산학과 박사과정
** 통신정보보호학회 종신회원, 전남대학교 전산학과 부교수

주체 S의 보안등급이 객체 O의 보안등급보다 같거나 낮을 때 주체 S는 객체 O를 기록(write)할 수 있다.

위 규칙에서 주체는 사용자의 행위를 수행하는 프로세스이고 프로세스는 사용자의 보안등급에서 나온 보안등급를 갖는다. 다단계 보안이라는 것은 서로 다른 보안등급을 가진 사용자마다 접근하는 데이타 집합이 다른 다단계로 되어 있다는 것을 의미한다.

(2) 원자값의 보안등급(classification of atomic facts)

데이타베이스에 있는 각각의 원자값에 보안등급을 부여하는 능력을 말한다. 릴레이션 모델에서 이 요구조건의 의미는 속성값 수준으로 보안등급을 가진 다단계 릴레이션을 유지해야 한다는 뜻이다.

(3) 다단계 뷰(multilevel view)

모든 데이타가 서로 다른 보안등급을 갖는 데이타의 뷰를 가지는 능력이다. 뷰는 유도(derived) 데이타이기 때문에 보안등급을 유도할 능력이 필요하다.

(4) 다단계 삽입과 갱신(multilevel entry and update)

다양한 보안등급을 가진 속성들로 구성된 레코드를 삽입하는 능력과 단일 트랜잭션에서 다양한 보안등급을 가진 속성값을 갱신하는 능력을 말한다.

(5) 각 보안등급의 일관성(consistency at each access class)

어떤 데이타가 모든 보안등급에서 숨겨질지라도 다양한 보안등급에서 연산하는 주체에게 데이타베이스의 일관된 상태를 유지하는 능력이 있어야 한다.

(6) 규칙기반 보안등급(rule-base classification)

데이타에 할당된 보안등급에 대한 데이타베이스 무결성 제약조건을 정의하는 능력이다.

(7) 보안등급에 근거한 검색(retrievals based on access class)

보안등급에 따라서 검색하기 위해 데이타를 선택하는 능력이다.

다단계 데이타베이스 시스템에 대한 위의 요구조건들은 관계형 모델, 개체-관련성 모델, 객체지향 데이타 모델 등에 영향을 미쳤다.

2. 다단계 관계형 모델

2.1 기본 개념

다단계 데이타를 취급하기 위해, 릴레이션 보안수준에서 속성값 수준의 보안등급을 포함하도록 해야 한다. 속성, 튜플 수준의 보안등급은 속성값 수준의 보안등급에 의해서 정의될 수 있다. 릴레이션 스키마에서 보안등급 레이블(label)을 속성으로 모델링 한다. 이런 방법으로 새로운 데이타를 레이블링하기 위한 분류 규칙이 보안등급 속성에 대한 무결성 제약조건으로 표현된다. 그리고 검색은 보안등급 속성 뿐만 아니라 데이타 속성에 대한 값을 선택할 수 있다.

스키마는 각 데이타 속성 Ai에 대한 보안등급 Ci를 포함하도록 확장된다. Ci의 도메인(domain)은 [Li, Hi]로 정의되고 이것은 가장 낮은 보안등급 Li에서 가장 높은 보안등급 Hi 범위의 부분격자(sublattice)를 나타낸다. 튜플에서 속성값 ai의 보안등급은 대응값 ci로 한다. 다단계 릴레이션 R은 각각 데이타 속성 Ai에 대해서 보안등급 Ci가 존재하는 릴레이션으로 정의된다.[2)]

R(A1, C1, … , An, Cn)

스키마에서 보안등급 레이블을 속성으로 취급할 때의 장점은 릴레이션 질의어에서 보안등급에 근거한 선택(selection)을 간단히 공식화하는 방법을 제공한다. 그림 1은 세가지 데이타 속성을 가지는 다단계 릴레이션을 보여주고 있다. 여기서 속성 A1은 주키이다. 각 보안등급 속성의 범위는 [S, TS]이다. 전체 릴레이션의 보안등급은 S이다.

다단계 릴레이션 R에 대한 스키마도 보안등급을

이름	보안등급1	나이	보안등급2	기술	보안등급3
심갑식	S	17	S	정보처리	S
이영록	S	34	S	암호분석	TS
노봉남	TS	5	TS	암호관리	TS

그림 1. 다단계 릴레이션 R

할당하고 class(R)로 표기 한다. 이 클라스는 릴레이션 이름, 모든 속성 이름 그리고 스키마를 위한

타입 정의에 적용된다. 스키마에 단일 보안등급을 할당하는 것은 구현을 매우 단순화시킨다. 왜냐하면 데이타의 어떤 부분을 접근하는 모든 주체는 전체 릴레이션 구조를 알 수 있기 때문이다. 만약 스키마가 어떤 속성이 어떤 주체에게 보이지 않는 다단계이라면 어떤 단일 주체도 완전한 튜플을 삽입하거나 삭제할 수 없다. 왜냐하면 주체는 전체 레코드 구조를 판독(read)하고 기록(write)할 수 없기 때문이다.

class(R)은 보안등급 속성 C1, … , Cn의 하계(lower bounds) (L1, … , Ln) 이하이어야 한다. 이 성질은 릴레이션의 어떤 주어진 인스턴스의 모든 데이타 속성값 보안등급에 의해 스키마 보안등급이 지배되는 것을 의미한다. 만약 이 성질이 만족하지 않는다면 스키마 보안등급 보다 더 낮은 보안등급을 가진 데이타는 낮은 보안등급의 주체가 이용할 수 없다. 왜냐하면 이들 주체는 릴레이션을 참조할 방법이 없기 때문이다. 그림 1의 다단계 릴레이션에 주체 보안등급이 S인 릴레이션은 그림 2와 같다. 여기서 S보다 높은 등급을 갖는 속성값은 널값을 가지며, 그 보안등급은 S이다. 왜냐하면 이영록이 암호분석 기술을 가지고 있다는 것은 Top secret 사항이기 때문이다.

이 름	C1	나 이	C2	기 술	C3
심갑식	S	17	S	X	S
이영록	S	34	S	null	S

그림 2. 여과된 secret 릴레이션

2.2 다단계 릴레이션 무결성 규칙

무결성 제약 조건의 목적은 데이타베이스를 일관된 상태로 유지하기 위한 것이다. 여과(filtering)는 다양한 보안등급의 주체들에게 데이타베이스의 다양한 뷰를 제공하기 때문에 각 보안등급에서 보이는 데이타의 일관성을 보장하기 위해 릴레이션 모델의 응용 독립적인 무결성 규칙 즉, 개체 무결성과 참조 무결성이 확장되어야 한다.

여과(filtering)는 응용에 따른 무결성 제약조건에 영향을 준다. 그리고 응용에 따른 무결성 제약조건이 전체(global) 일관성을 보장하는 것이라면 각 보안등급에서 일관성을 보장하는 방식으로 그들이 공식화되어야 한다.

새로운 튜플이 단단계 릴레이션에 삽입될 때마다 데이타 속성값은 응용 독립과 응용 종속 무결성 규칙에 제약 받는다. 뿐만 아니라, 튜플의 속성값에 대한 보안등급도 분류 제약조건[3]이라는 응용 종속 무결성 규칙에 의해 제약받는다.

2.2.1 다단계 개체 무결성

개체 무결성이란 릴레이션에 있는 어떤 튜플도 주키 속성들에 대하여 널값을 갖을 수 없다는 것을 말한다. 주키는 특정 튜플을 유일하게 구별하는 것이다. 주키를 구성하는 속성값 모두는 같은 보안등급을 가져야 한다. 그렇지 않으면, 가장 높은 키 속성값의 보안등급보다 더 낮은 보안등급인 주체는 키를 형성하는 어떤 속성값에 대해서는 널값으로 보이는 경우가 있다. 뿐만 아니라, 주키의 보안등급은 튜플에 있는 모든 다른 속성값들의 보안등급들 중 가장 낮은 보안등급을 가져야 한다. 이 요구사항의 이유는 주키는 한 튜플과 대응 속성값을 유일하게 선택하는데 필요하기 때문이다. 만일 주키가 튜플에 있는 어떤 속성값의 보안등급에 의해 지배되지 않는다면 속성값의 보안등급에서 운영하고 있는 주체는 그 속성값을 유일하게 선택할 수 없다. 이들 요구사항은 개체 무결성에 대한 다음의 확장된 제약조건을 이끌어 낸다.

성질1 〈다단계 개체 무결성〉

Ak를 릴레이션 R의 주키를 형성하는 데이타 속성들의 집합이라 하자. 데이타 속성 Ai∈Ak에 대응하는 모든 보안등급 속성들 Ci는 R의 어떤 주어진 튜플에서 같은 값을 갖는다. 그리고 보안등급 속성 Ci는 데이타 속성 Aj ∉Ak에 대응하는 각각 보안등급 속성 Cj의 값에 의해 지배된다. R의 인스턴스에 있는 어떤 튜플도 어떤 주키 속성들에 대해서도 널값을 갖을 수 없다.

주키 보안등급에 대한 제약조건은 다른 실제적 이유가 있다. 만일 주키 보안등급이 일정하게 할당되지 않으면 튜플이 생성될 때 키가 완전하게 정의되도록 다단계 주체는 릴레이션에 튜플을 첨가시킬

필요가 있다. 주키 참조없이 갱신하기 위해 튜플이 선택될지라도 갱신하기 위해 주키를 선택하는 것은 필수적이다.

2.2.2 다단계 참조 무결성

참조 무결성이란 모든 외래키(foreign key)는 그 키가 주키가 되는 어떤 다른 릴레이션에 존재하는 튜플을 참조해야 한다는 뜻이다. 다단계 데이타베이스에서 이 의미를 보면 외래키 속성값은 더 높은 혹은 비교할 수 없는 보안등급을 가진 튜플은 참조의 보안등급에서 존재하지 않는 것으로 나타나기 때문에 참조 무결성에 대해 다음의 확장된 규칙을 이끌어 낸다.

성질 2 〈다단계 참조 무결성〉

참조될 릴레이션에 대응 주키를 가진 튜플이 존재하지 않는한 릴레이션에 있는 어떤 튜플도 널값이 아닌 외래키를 갖을 수 없다. 한 튜플에서 외래키를 구성하는 각각의 속성값 보안등급은 동일해야 한다. 다시 말해서, 외래키 속성들은 일정하게 분류되어야 한다. 그리고 참조될 튜플에 있는 주키 속성값의 보안등급을 지배해야 한다.

참조될 튜플의 보안등급을 외래키 보안등급이 엄밀하게 지배할 때 참조 무결성이 필요성에 대한 의문이 일어난다. 이런 상황에서 참조될 튜플의 보안등급에서 연산하는 주체는 허상참조(dangling reference)를 모르고 튜플을 삭제할 수 있다. 여과(filtering) 때문에 주체는 참조의 존재를 모르기 마련이다. 이런 이유 때문에 공통 보안등급을 가지는 데이타에 대해서만 참조 무결성이 의미있다고 주장한다. 더 높은 보안등급으로부터 참조되는 튜플을 삭제하는 경우에는 무결성 위반으로 간주되지 않는다. 그러나 어떤 하향 참조에도 의존하지 않기 때문에 이런 접근방법은 높은 수준의 일관성을 제공하지 못한다.

다단계 릴레이션 모델에서 모든 데이타는 보안등급을 할당 받는다. 그리고 릴레이션 스키마, 뷰, 무결성 제약조건, 분류 제약조건을 정의하는 정보도 포함한다. 만일 모든 구조적 정보가 릴레이션과 같은 다단계 시스템 릴레이션에 위치한다면 릴레이션 스키마를 명시하는 속성값들에 할당된 보안등급들은 앞의 무결성 규칙들에 의해 제약된다. 예를 들면, 뷰 정의에 할당된 보안등급은 그 뷰에서 참조된 각 릴레이션의 보안등급과 같아야 한다. 이것은 참조 무결성 때문이다.

2.3 다중 인스턴시에이션

다중 인스턴시에이션(polyinstanciation)은 같은 이름으로 많은 데이타 객체의 동시 존재를 의미한다. 여기서 많은 인스턴시에이션들은 그들의 보안등급으로 구별된다. 이것은 다단계 보안의 불가피한 결과이고 데이타베이스, 릴레이션, 튜플 그리고 데이타 속성값에 영향을 준다.

(1) 다중 인스턴시에이션 릴레이션(PIR)들은 릴레이션 이름 R과 스키마 보안등급 (R)에 의해 구별되는 릴레이션들이다. 그래서 동일 이름 R이지만 다른 class(R)을 가진 몇개의 릴레이션들이 존재할 수 있다.

(2) 다중 인스턴시에이션 튜플(PIT)들은 주키와 관련키 보안등급에 의해 구별되는 튜플이다. 그래서 같은 다단계 릴레이션에는 주키 값은 같지만 서로 다른 보안등급인 몇개의 튜플 인스턴스들을 포함할 수 있다.

(3) 다중 인스턴시에이션 속성값(PIE)들은 주키, 키 보안등급, 그리고 속성값 보안등급(속성 이름을 첨가해서)에 의해 구별되는 속성값들이다. 그래서 다른 보안등급이지만 같은 (주키, 키 보안등급)의 쌍과 연관되는 속성에 대하여 많은 속성값들이 존재할 수 있다.

개체 무결성에 대한 규칙은 키내의 다중 인스턴시에이션을 금지한다. 다시 말해서 주키 속성에 대한 다중 인스턴시에이션 속성값들을 금지한다. 튜플이 릴레이션에 첨가될 때 모든 주키 속성들은 완전하게 정의되어야 하므로 널값이어서는 안된다. 그리고 키 속성들은 키 정의에 의하여 갱신할 수 없다.

다중 인스턴시에이션은 다단계 릴레이션, 강제적 보안, 여과(filtering)의 자연스런 결과이다. 다중 인스턴시에이션 데이타를 주체가 완전히 알아채지 못하는 방법으로 다중 인스턴시에이션을 유지해야 한다.

3. 다단계 개체-관련성 모델

3.1 기본 개념

개체(entity)는 구별되는 사물이나 개념인 데이타 객체(object)이다. 구별성(distintness)의 의미는 객체에 이름을 붙일 수 있다는 뜻이다. 모델에서 개체와 그 대응 이름은 서로 다른 데이타 객체로 취급한다.

관련성(relationship)은 두개 이상의 개체를 연관시키는 데이타 객체이다. 개체-관련성 그림표에서 개체는 사각형으로 표시하고 관련성은 다이아몬드형으로 표시한다.

개체-관련성 항목(item)은 개체와 관련성의 일반화이다. 개체-관련성 그림표에서 모든 다각형은 개체-관련성 항목이다. 각각의 개체-관련성 항목은 단일 타입(type)을 갖는다. 일반형 개체-관련성 모델(GTERM : Generalized Typed Entity-Relationship Model)은 어떤 타입의 서브타입(subtype)을 수용하지 않기 때문에 일반형 개체-관련성 모델은 완전히 일반화된 것이 아니다.

참조(reference)는 참여 개체를 확인하는 관련성의 기본 구성요소(primitive component)이다. 참조는 개체 이름의 복제가 아니라 포인터(pointer)로 생각할 수 있다. 개체-관련성 그림표에서 참조는 관련성에서 개체로의 화살표로 표현한다.

한편, 역할(role)은 관련성내의 참조들 사이의 식별자(discriminant)이다.

참조 집합(reference-set)은 특정 역할을 갖는 개체-관련성 항목의 모든 참조의 집합이다. 각각의 참조 집합은 단일 타입을 갖는다. 각 참조 집합 타입은 참조 집합을 포함하는 개체-관련성 항목의 타입과 그 참조 집합에 대한 역할(role)에 의해서 결정된다. 참조 집합 타입은 관련성내에서 특정 역할을 하는 개체 타입을 명시한다. 그들은 대응수(cardinality) 제약조건을 명시한다. 필수적(mandatory) 참조는 대응 참조 집합 타입에 대해 양의 최소 대응수 제약조건(positive minimum cardinality constraint)으로 정의된다. 선택적(optional) 참조는 최대와 최소, 대응수 제약 조건으로 정의된다.

속성(attribute)은 한 개체, 개체의 이름 혹은 관련성의 구성요소인 값의 순서화되지 않은(unordered) 집합이다. 각 속성은 하나의 대응되는 타입을 가진다. 속성을 값의 집합으로 취급하는 이유는 2가지이다.

첫째, pascal, Ada같은 프로그래밍 언어는 집합 데이타 타입들을 지원한다. 이 데이타 타입들은 단일값(single-valued) 데이타 타입으로 서술될 특징보다 훨씬 더 복잡한 특징들을 서술할 수 있다. 일반형 개체-관련성 모델은 직접적으로 모든 속성을 값의 집합으로 서술하는 데이타 타입들을 지원한다.

둘째, 속성에서 널(null) 값은 전적으로 회피된다. 널 속성은 널 집합이다.

속성에 대한 필수/선택 제약조건은 간단한 대응수 제약조건으로 표현될 수 있다. 각 속성 타입은 최소와 최대 대응수를 할당받는다. 선택적인 속성은 그 타입의 최소 대응수가 0인 단순한 속성이다. 필수적인 속성은 그 타입이 양의 최소 대응수를 갖는 속성이다.

3.2 다단계 보안 특징

다단계 보안과 관련된 일반형 개체-관련성 모델의 기본 공리는 꽤 간단하다. 각 개체-관련성 항목은 다음 제약조건을 따르는 다단계 자료구조이다.[4]

〈공리 1〉 각 개체-관련성 항목은 최소 보안등급을 갖는다. 개체-관련성 항목을 이루는 각각의 구성요소의 보안등급은 개체-관련성 항목의 최소 보안등급을 지배하므로 이 최소 보안등급을 개체-관련성 항목의 보안등급으로 한다.

〈공리 2〉 각 이름은 보안등급을 갖는다. 이름의 구성요소는 이름과 동일한 보안등급을 일정하게 한다.

〈공리 3〉 개체의 보안등급은 그 이름의 보안등급과 같다. 이것에 대한 이유는 간단하다. 객체 이름을 안다는 것은 객체 자체를 안다는 것과 동일하기 때문이다.

〈공리 4〉 관련성의 보안등급은 각각 참조될 개체의 보안등급을 지배한다. 관련성은 참여 객체들에 대한 언급이므로 어떤 사실(fact)로 볼 때 관련성의 존재는 참여 개체의 존재를 예상할 수 있으므로 관련성은

참여 개체들을 안다고 가정한다. 그래서 관련성의 보안등급은 그것에 참여하는 개체들의 보안등급 보다 더 낮을 수 없다. 더우기 관련성은 각각의 참여 개체들에 대한 부가적 정보를 표현하기 때문에 관련성 보안등급은 어떤 참여 개체들의 보안등급보다 높아야 한다.

〈공리 5〉 참조의 보안등급은 참조를 포함하는 개체-관련성 항목의 보안등급과 같다.

이 공리에 대한 근거는 참조가 관련성 의미의 중심이 된다는 것이다. 만약 참조가 관련성에 첨가되거나 제거된다면 관련성의 의미도 변화 되어야 한다.

3.3 연구 결과

보안 개체-관련성 모델 연구는 다단계 보안 자료구조의 규칙에 대한 근거를 제공한다. 그 근거는 다단계 데이타베이스를 단순히 사실(fact)의 집합으로 간주하는 데에 있다. 이런 추상화는 개체-관련성 모델 뿐만 아니라 다른 모델에도 적용시킬 수 있다. 둘째로, 이 추상화는 다단계 보안 데이타베이스를 위한 데이타 모델의 3가지 원칙인 정보크기 단위 원칙, 종속성 원칙, 결정성 원칙을 제안한다. 세째로, SeaView 데이타 모델과 비교하면, SeaView 모델[5]이 결정성 원칙을 위반한다는 것을 알 수 있다.

3.3.1 기본 추상화

일반형 개체-관련성 모델에서 다단계 데이타 구조에 대한 공리들에서 볼 수 있었던 것처럼 우리는 다단계 보안 데이타베이스를 연관된 사실(fact)의 집합으로 간주하였다. 여기서 하나의 사실은 단순히 정보의 캡슐화 단위이다. 데이타베이스에서 어떤 사실은 다른 사실들을 참조한다. 다른 사실들을 참조하는 하나의 사실은 각각 참조될 사실에 논리적으로 종속한다.

이 추상화의 장점 중 하나는 그래픽 해석과 일치한다는 것이다. 만일 사실이 그래픽 노드(node)로 표현될 때 논리적 종속성은 의존 사실에서 기본사실(base fact)로의 화살표이다. 이런 방식으로 해석되는 잘 정의된(well-defined) 데이타베이스는 비환형 방향 그래프를 생성해야 한다.

3.3.2 다단계 데이타베이스의 원칙

데이타베이스에 대한 위의 간단한 추상화를 사용하여 우리는 다단계 데이타베이스를 관련된 사실들의 집합으로 간주한다. 여기서 각각의 사실들은 각각의 보안등급(access class)을 가진다. 이것은 잘 정의된 다단계 데이타베이스의 기준을 제공하고 있다. 다단계 데이타베이스에 대한 3가지 원칙은 다음과 같다.

(1) 정보크기 단위 원칙(the granularity principle)

다단계 보안 데이타베이스에서 보호 목적을 위해 가장 미세한 수준의 정보단위가 원자값에 해당하는 자료구조여야 한다. 만약 이것을 SeaView 모델에 적용한다면 튜플내에 있는 키는 원자값으로 취급되어야 한다. 다시 말해서 튜플에서 주키의 모든 속성값은 동일한 보안등급을 할당받아야 한다. 관련성에서 외래키의 모든 속성값도 역시 같은 보안등급을 가져야 한다.

정보크기 단위 원칙 적용에서 데이타의 객체 관련성의 모든 참조를 관련성을 표현하기 위해 필수 불가결한 것으로 간주한다. 결과적으로 모든 참조는 같은 보안등급을 할당 받는다.

(2) 종속성 원칙(the dependency principle)

관련되지 않는 사실의 데이타베이스는 관심이 없다. 종속성 원칙에는 다단계 데이타베이스를 논리적 종속성에 의해 연관된 사실들의 집합으로 볼 수 있다. 종속성 원칙이 설명하는 것은 한 사실의 보안등급은 그 사실이 종속하는 다른 사실의 보안등급을 지배한다는 것이다.

일반형 개체-관련성 모델에 적용할 때 종속성 원칙 관점에서 관련성의 보안등급은 참여 개체들의 보안등급을 지배한다.

종속성 원칙의 결과로 한 사실이 데이타베이스에서 제거되면 논리적 일관성 때문에 모든 종속 사실들을 제거하거나 확장하게 한다. 종속 사실의 삭제나 갱신은 비밀성에 대하여 "상향기록(write-up)"이고 무결성에 대하여 "하향기록(write-down)"이므로 이것이 허용된다.

(3) 결정성 원칙(the determinacy principle)

이것은 사실적인 종속성(factual dependency)이 모호하지 않아야 한다는 것을 의미한다. 이것은 데이타베이스를 관련된 사실들의 저장소로 보는 관점이다.

참조 무결성은 한 릴레이션에서 하나의 튜플에 있는 외래키는 다른 튜플에 있는 키와 동일하다는 것을 말한다. 키는 릴레이션내에서 유일하므로 단 하나의 튜플만이 확인된다. 그래서 외래키를 포함하는 튜플은 사실들의 집합으로 볼 수 있으며, 이 사실들 각각은 외래키에 의해 확인된 다른 사실에 의존한다.

그러나 다단계 데이타베이스는 다중 인스턴시에이션(polyinstantiation)이라는 문제점을 나타난다. 다중 인스턴시에이션은 기본적으로 다양한 보안등급인 사실들의 복제이다. 그런 복제가 발생했을 때 그 해석이 중요하다. 결정성 원칙이 다중 인스턴시에이션을 제거하지 않는다. 그러나 결정성 원칙은 혼돈을 야기시킬 수 있는 문제점을 해결해준다.

4. 다단계 보안 객체지향 모델

여기서는 객체지향 데이타베이스 시스템을 위한 강제적 보안 모델을 설명하여 일반 객체지향 데이타 모델에 보안 성질을 통합하는 방법을 보여준다.

이들 성질들을 설명하기 전에 다음 두가지 점을 강조하는 것은 중요하다. 첫째, 다단계 객체지향 데이타베이스 시스템의 설계는 강제적 보안 성질들을 실현하기 위해 기본 강제적 보안커널에 의존해야만 한다. 기본 강제적 보안커널을 이용한다는 것은 보장(assurance)을 얻기 위한 실제적인 방법이다. 둘째, 객체가 분류될 때 그 의미를 먼저 정의해야 한다.

여기에서 언급한 내용은 다단계 객체지향 시스템 모델링의 기초적인 것이다. 객체를 다단계로 하는 것은 매우 복잡하고 어려운 문제를 초래한다.

4.1 보안의 의미

객체 모델에서 보안등급은 객체(또는 클라스)와 객체의 구성요소와 관련된다. 가장 일반적이기 위해서는 객체가 다단계가 되어야 한다. 즉, 클라스 이름, 인스턴스 변수이름, 메소드와 같은 객체의 다양한 부분들은 서로 다른 보안등급을 갖을 수 있다.

객체(혹은 클라스)가 보안등급 C를 갖는다는 의미는 객체(혹은 클라스)가 존재한다는 사실이 보안등급을 갖는다는 뜻이다. 객체가 존재한다는 사실을 보호하는데 사용되는 메카니즘은 객체이름에 보안등급 C를 할당하는 것이다. 객체 0의 구성요소가 보안등급 C를 가진다는 것은 그 요소와 객체 0의 연관성이 C로 분류된다는 것을 의미한다. 객체 0가 요소 V를 가진다는 사실을 보호하는데, 사용되는 메카니즘은 객체의 요소 이름에 보안등급 C를 할당하는 것이다. 이것은 객체와 요소 사이의 연관성을 보호한다.

예를 들면 인스턴스 변수 WORK-ON을 생각해 보자. 이 변수는 '직원' 객체와 '프로젝트' 객체 사이의 관련성을 나타내는데 사용된다. 직원 객체의 인스턴스 변수 '작업'을 C등급으로 분류함으로써 이런 관련성에 보안등급 C를 할당할 수 있다.

일반적으로 객체 A가 객체 B에 관련될 때, B는 A보다 더 높거나 낮게 분류될 수 있다. 만약 B가 A보다 더 높다면 B와 같은 등급의 주체는 관련성을 볼 수 있지만 A와 동일한 등급의 주체는 볼 수 없다. 아래에서 모델의 응용독립 분류 규칙을 열거한다.

4.2 보안등급 계층

'is-a' 클라스 계층과 관계된 보안 성질은 대응되는 보안등급 계층이 필요하다.[7] 객체지향 시스템은 시스템에 정의된(system-defined) 클라스를 갖는다. 이것은 어떤 보안등급의 주체도 이용가능해야 하므로 시스템에서 가장 낮은(system-low) 등급이어야 한다. 클라스의 보안등급을 언급할 때는 클라스 이름의 보안등급을 의미한다. 이것은 클라스가 존재한다는 사실의 보안등급과 일치한다.

성질 1 〈기본 클라스 성질〉

시스템에서 기본으로 정의된 클라스는 시스템에서 가장 낮다.

예를들면 INTEGER, STRING, BOOLEAN과 같은 기본 클라스와 최상위 클라스 OBJECT는 시스템에서 가장 낮은 보안등급을 갖는다.

하위 클라스(subclass)는 한 클라스의 특수화(specialization)이거나 인스턴스이다. 예를 들면, 자전거는 산악자전거라는 하위 클라스(혹은 인스턴스)를 갖을 수 있다. 하위 클라스는 상위 클라스로부터 그의 정의를 유도해 낸다. 그래서 하위 클라스 이름의 보안등급은 그의 상위 클라스 이름의 보안등급보다 같거나 높아야 한다. 이것은 다음 성질에서 표현된다. 여기서 L은 보안등급을 나타낸다.

성질 2 〈계층 성질〉

O_1이 O_2의 상위 클라스일 때, 모든 O_1과 O_2에 대하여 $L(O_2) \geq LO_1$이다.

예를 들면 쓰레기차가 트럭의 하위클라스이라면 L(쓰레기차) ≥ L(트럭)이다.

4.3 다단계 객체와 관련된 성질

모델이 다단계 객체를 지원한다면 여기서 열거한 성질들이 더 필요하다. 객체이름이 보호되면 그 요소와의 연관성은 그 보안등급 이상이다. 그래서 한 객체의 요소(즉, 그들의 이름)의 보안등급은 객체이름의 보안등급 이상이어야 한다. 이것은 다음 성질로 표현된다. 아래에서 L(V)는 요소의 보안등급을 나타내고 L(O)는 객체이름의 보안등급을 의미한다.

성질 3 〈계층 성질〉

V가 O의 구성요소라면 모든 V와 O에 대해 L(V) ≥ L(O)이다.

예를 들면, SECRET 클라스 '첩보비행기'는 SECRET 인스턴스 변수 '제작사'와 TOP-SECRET 인스턴스 변수 '임무'를 가질 수 있다. 그래서 SECRET 사용자는 클라스 첩보비행기가 인스턴스 변수 임무를 가진다는 것을 모른다. 그리고 임무는 인스턴스 변수와 관련된 데이타가 SECRET나 그 이하로 분류되었다 할지라도 SECRET 사용자는 그 어떤 데이타도 검색할 수 없다. 위의 예에서 인스턴스 변수 제작사는 클라스 '회사'이어야 한다. 즉, 그 값은 클라스 회사라는 객체의 객체식별자이어야 한다. 여기서 클라스 회사는 UNCLASSIFIED이다. 그러면 인스턴스 변수 제작사를 SECRET 등급으로 한다는 의미를 보면 첩보비행기의 제작사를 요청하는 질의어로 검색될 때 회사이름은 자동적으로 SECRET로 할당된다는 뜻이다. 다른 관점에서 회사이름이 검색될 때는 UNCLASSIFIED이다.

메소드의 보안등급은 메소드가 객체와 관련되어 있다는 사실의 보안등급이지 실제 코드의 보안등급이 아니다. 예를들어 은행구좌는 구좌의 하위클라스이고 은행구좌는 SECRET이며 구좌는 UNCLASSIFIED이라고 하자. 은행구좌는 구좌로부터 메소드 예금, 출금, 질의를 상속받는다. 은행구좌에서 메소드는 SECRET이고 구좌에서의 메소드는 UNCLASSIFIED이다. 메소드를 구현하는 코드는 저장(storage)객체에 저장되므로 보안등급을 갖는다. 메소드를 구현하는 코드는 객체에서 가장 낮은 보안등급 이상으로 분류되어야 한다. 그렇지 않으면 메소드가 수행될 수 없다. 위의 예에서 메소드 출금을 구현하고 있는 코드는 UNCLASSIFIED보다 더 높을 수 없다.

한 객체는 그 객체 클라스의 구성요소를 상속받는다. 예를 들면, 산악자전거는 그의 클라스 자전거에서 인스턴스 변수 색깔을 상속받는다. 값도 역시 상속 받는다. 예를 들면 빨강 산악자전거는 값 '빨강'을 가진 인스턴스 변수 색깔을 상속받는다. 하위 클라스는 상위 클라스 이상으로 비밀이고, 하위 클라스의 구성요소도 상위 클라스 구성요소 이상으로 보호해야 한다. 이것은 다음 성질로 표현된다.

성질 4 〈상속 성질〉

O_2가 O_1에서 상속 받은 구성요소 V_2는 O_1의 대응 구성요소 V_1이상으로 분류된다.

즉, $L(V_2) \geq L(V_1)$이다.

한 객체가 다중 클라스를 가져서 각각의 클라스들로부터 구성요소를 상속받을 때 이름 충돌(name conflict)이 발생할 수 있다. 그러나 보안모델에서는 다음 성질이 충돌을 해결할 수 있다.

성질 5 〈다중 상속 성질〉

두개 이상의 객체 클라스가 V라는 구성요소를 가

질때, 객체는 가장 낮은 보안등급을 가진 구성요소 V를 상속 받는다.

주체가 한 객체에 메시지를 보낼 때 주체는 객체의 보안등급 이상이어야 한다. 그렇지 않으면 주체는 객체의 존재를 모를 것이다. 주체의 보안등급은 또한 활성화될 메소드의 보안등급 이상이어야 한다. 그렇지 않으면, 주체는 객체와 메소드의 연관성을 모를 것이다. 이들 요구 사항은 다음 성질로 요약된다.

성질 6 〈주체의 보안등급 성질〉

만약 주체 S가 메소드 M을 수행하기 위해 객체 O에 메세지 m을 보낸다면

* $L(S) \geq L(M) \geq L(O)$이고 $L(S)=L(m)$이다.

예를 들면, L(S)가 은행구좌에 메세지 잔액조회의 보안등급 이상일 때만 주체 S는 은행 계좌 잔액에 질의할 수 있다. 〈성질 6〉에서 $L(S)=L(m)$은 강제적 보안의 *-성질의 결과이다. 왜냐하면 주체 S는 메시지를 생성(create) 혹은 기록(write)하기 때문이다.

4.4 다단계 객체의 문제점

객체가 다단계일 때 일어나는 몇가지 문제점들이 있다. 만약 객체가 다단계이라면 새로운 인스턴스를 생성하는 것이 어렵다. 예를 들면, 만일 객체 O가 변수 V_1과 V_2를 갖고 여기서 $L(O)=L(V_2)=$ UNCLASSIFIED이고 $L(V_2)=$SECRET일 경우 UNCLASSIFIED 주체가 O의 새로운 인스턴스를 생성한다면 어떻게 되겠는가? 주체는 변수 V_2를 모르므로 인스턴스는 변수 V_1만으로 생성될 것이다.

그러나 이제 UNCLASSIFIED 주체가 새로운 객체를 보고 V_2와 함께 새로운 변수를 첨가 한다면 결국 다중 인스턴시에이션이 발생한다.

지금까지의 성질들로는 다음 사항을 금지시킬 수 없다. 객체 O_1은 변수 V_1과 V_2를 상속한다. 이제, 그림 3에서 처럼 $L(O_1)=$UNCLASSIFIED이고, $L(V_1)$ 와 $L(V_2)$는 O_1에서 UNCLASSIFIED, $L(O_2)=$SECRET, $L(V_1)$은 O_2에서 SECRET 그리고 $L(V_2)$는 O_2에서 TOP-SECRET이라고 가정하자.

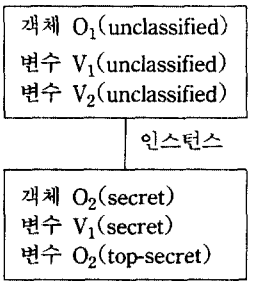


그림 3. TOP-SECRET 주체의 뷰

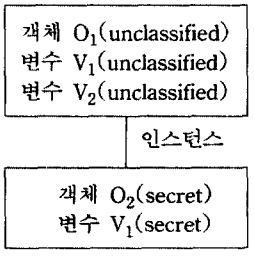


그림 4. SECRET 주체의 뷰

그림 4에서 보여진 것처럼 SECRET 주체는 두개의 객체를 볼 수 있고, 또 O_2는 변수 V_2를 상속받았지만 보이지 않는다. 그래서, SECRET 주체는 변수 V_2가 더 높은 등급으로 존재한다는 것을 추론할 수 있다. 이런 문제는 다음 성질을 도입하여 해결할 수 있다.

성질 7 〈한계 성질〉

객체 O_2가 클라스 O_1에 속하고 O_1은 구성요소 V를 갖는다면 그리고 O_1에 있는 V의 보안등급이 $L(O_2)$ 보다 낮다면 O_2에 있는 V의 보안등급은 $L(O_2)$ 보다 낮다.

5. 결 론

지금까지 각 데이타 모델에서의 보안성 연구 방향에 대해 알아보았다. 그러나 앞으로 연구해야 할 많은 문제들이 산적해 있다. 다단계 보안 데이타베이스 관리 시스템에서 자신의 보안등급으로 신분이 확인된 사용자는 다양한 분류 등급의 데이타로 구성된 데이타베이스를 접근한다. 다단계 데이타베

이스 보안의 연구 방향은 아래와 같다

(1) 보안등급 제약조건(classification constraints) 관리

보안등급 제약조건은 데이타베이스 무결성 제약조건과 유사하지만 그것은 데이타 값이라기 보다는 데이타에 할당될 보안등급을 관리하는데 사용된다는 것이 다르다. 무결성 제약조건은 타당한 데이타가 데이타베이스에 들어가는 것을 보장하기 위해 사용된다. 예를 들면, 이들 제약조건은 속성값의 범위라든지 여러 데이타 속성값 사이의 관련성을 정의할 수 있다. 보안등급 제약조건은 데이타베이스에 들어갈 데이타에 보안등급을 할당하는데 사용한다. 이들 규칙은 데이타 값에 따라서 또는 데이타베이스에 있는 다른 데이타와의 관련성에 따라서 보안등급을 할당할 수 있다.

(2) 바람직하지 않는 추론 방지

어떤 데이타를 사용하여 보안등급이 더 높은 데이타에 대한 부분 혹은 전체 정보를 유도해낼 때 다단계 추론 문제가 일어난다.[8,9] 어떤 경우에는 정보의 존재를 아는 것조차 보안되어야 할 경우가 있다. 개개의 데이타 항목은 낮게 분류되고 데이타 항목사이의 관련성이 높은 비밀성이 있을 때 이런 문제가 일어난다. 집단화(aggregation) 문제 역시 데이타 사이에 보호해야 할 관련성이 있을 때 이를 보호해야 한다.

(3) 다단계 데이타베이스 연산의 의미 정의

속성값 수준이 보안등급을 가진 다단계 데이타베이스 시스템에서 기본 데이타 조작연산인 삽입, 삭제, 갱신에 대한 의미를 정의할 필요성이 있다.[10] 예를 들면, 갱신연산으로 얼마의 다중 인스턴시에이션이 일어나며 삭제연산에서 어느 다중 인스턴시에이션 인스턴스를 삭제할 것인가 하는 문제가 발생된다.

(4) 다단계 보안 모델 연구

데이타베이스 보안에 대한 대부분의 연구는 Woods Hole Study[17]에 근거하며 이것은 데이타베이스 보안에 대한 연구 안건을 설정했다. 처음에는 데이타 암호화, 여과기(filter)나 무결성 록(intergrity lock) 메카니즘[18] 사용에 집중했으나, 최근 연구는 관계형 데이타 모델에 기초한 보안 데이타베이스 시스템을 제공하기 위한 다양한 기법과 접근 방법들을 소개하고 있다.[11,12,13,14,15] 또한 객체지향 시스템, 개체-관련성 시스템, 지식베이스 시스템 등과 같은 시스템에서도 보안성 문제가 연구되고 있다.

(5) 다단계 보안 분산 데이타베이스 시스템 연구

연구자들은 보안 분산 데이타베이스 시스템을 위한 구조(architecture) 연구를 시작하고 있고 분산 데이타의 보안성, 일관성, 가용성의 균형에 촛점을 맞추고 있다. 매우 복잡한 네트워크 그리고 분산 정보처리에서는 보안성을 보증해 주기 위한 많은 방법들이 필요하다. 분산 시스템 내에서의 보안 목적은 네트워크 시스템과 유사한 목적이다. 보안성의 구성요소는 보안정책, 보안영역 그리고 보안관리 등이 있다.[16]

참 고 문 헌

1. D.E. Denning, Cryptography and Data Security, Addison-Wesley, Reading, Ma, 1982.

2. D.E. Denning and T.F. Lunt, "A Multilevel Relational Data Model", Proceedings 1987 IEEE Symposium On Security and Privacy, 1987, pp. 220-234

3. R.W. Conway, W.L. Maxwell and H.L. Morgan, "On the Implementation of Security Measures in Information Systems", Communications of the ACM, 15(4), April 1972.

4. G. Gajnak, "Some Results from the Entity Relationship Multilevel Secure DBMS Project", 4th Aerospace Computer Security Applications Conference, IEEE, December 1988, pp.66-71.

5. D.E. Denning, T.F. Lunt, R.R. Shell, W.R. Shockely and M. Heckman, "The SeaView Security Model", IEEE Transactions On Software Engineering, Vol. 16, No. 6, June 1990, pp. 593-607.

6. J.K. Millen and T.F. Lunt, "Security for Object-Oriented Database Systems", Proceedings 1992 IEEE Symposium On Security and Privacy, 1992, pp.260-272.

7. T.F. Lunt, "Multilevel Security for Object-Oriented Database Systems", Database Security III : status and perspects, IFIP, 1990, pp. 199-209.

8. T.D. Garvey, T.F. Lunt and M.E. Stickel, "Abductive and Approximate Reasoning Models for Charecterizing Inference Channels", Proc. Fourth Workshop on the Foundations of Computer Security, June 1991, pp. 118-126.

9. T.F. Lunt, "Aggregation and Inference : Facts and Fallacies", Proc. 1989. IEEE Symp. on Research in Security and Privacy. May 1989, pp. 102-109.

10. T.F. Lunt and D. Hsieh, "Updata Sema ntics for a Multilevel Relational Database System", In Proceedings of the 4th IFIP WG11.3 Workshop on Database Security, September 1990, pp. 281-296.

11. T.D. Garvey and T.F. Lunt, "Multilevel security for Knowledge-based Systems", Proc. EISS Workshop on Database Security European Institute for System Security, April 1990.

12. S. Jajodia and B. Kogan, "Integrating an Object-Oriented Data Model with Multievel Security", Proc. 1990 IEEE Symp. on Security and Privacy, May 1990, pp. 76-85.

13. T.F. Keefe, W.T. Tsai and M.B. Thuraisingham, SODA : A Secure Object-Oriented Database System, Technical Report TR89-12, University of Minnesota, Computer Science Department, 1989.

14. T.F. Lunt, "The True Meaning of Polyin stantiation : Proposal For an Operational Semantics For a Multilevel Relational Database System", Proc. Third RADC Database Security Workshop, June 1990.

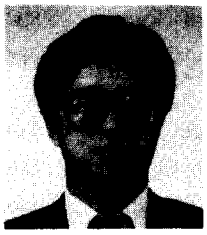
15. T.F. Lunt, R.R. Schell, W.R. Shockley, M. Heckman and D. Warren, "Toward a Mul tilevel Relational Data Language", Proc. Fourth Aeropace Compter Security Applications Conf., December 1988, pp. 72-79.

16. A. Downing, I. Greenberg and T.F. Lunt, "Issues in Distributed Database Security," Pro ceedings of the 5th Aeropace Computer Security Conference, December 1989.

17. Air Force Studies Board Committe on Data Management Security, Multilevel Data management Security, National Academy Press, 1983.

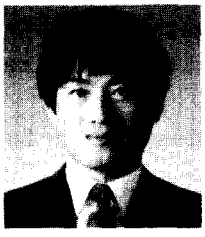
18. R.D. Graubart, "The Integrity-Lock Approach to Secure Database Management", Proceedings of the IEEE 1984 Symposium on Security and Privacy, April 1984, pp. 62-71.

□ 著者紹介



심 갑 식

1985년 전남대학교 계산통계학과 이학사
1987년 전남대학교 대학원 전산통계학과 이학석사
1990년－현재 전남대학교 전산학과 박사과정
관심분야 : 데이타베이스 설계, 객체지향 시스템, 컴퓨터 보안, 지식베이스 시스템



노 봉 남

1978년 전남대학교 수학교육과 졸업
1982년 한국과학기술원 전산학과 졸업
1982년～현재 전남대학교 전산학과 부교수
저 서 : 운영체제 입문, 시스템언어 입문, 객체지향 파스칼, 컴퓨터와 정보사회, 객체지향 시스템
관심분야 : 데이타 모델링, 객체지향 시스템, 정보통신보안, 정보사회론