通信情報保護學會誌
第2卷 第3號, 1992. 9

데이타베이스 보안에 대한 최신 연구 동향

강석훈* · 문송천*

1. 개 요

정보는 기관의 전략과 운용에 관련된 중요한 자산이며, 따라서 기밀 정보를 보호할 수 있는 적절한 보안대책이 요구된다. 정보보호의 중요성에도 불구하고 보안에 관한 연구분야는 데이타베이스 연구자들에게 상대적으로 등한시 되어 왔다. 본 고에서는 데이타베이스 보안에 대한 최신 연구동향을 조사하고 부분적나마 중요한 향후 연구과제들을 소개한다.

데이타베이스 보안이라 하면, 데이타베이스에 저장된 데이타에 대한 권한이 없는 액세스, 고의적인 파괴 혹은 변경 그리고 비일관성을 발생시키는 우발적인 사고로부터 데이타 또는 데이타베이스를 보호하는 의미로 정의할 수 있다. 액세스 제어를 위한 보안 정책은 임의적 액세스 제어(discretionary access control: DAC)정책과 강제적 액세스 제어(mandatory access control: MAC)정책으로 크게 구분할 수 있다[Lunt 89]. DAC정책은 주체나 주체가 속해있는 그룹들의 식별자를 근거로 객체에 대한 액세스를 제한하는 방법이며, MAC 정책은 객체에 포함된 정보의 비밀 등급(sensitivity)과 주체에 부여된 등급별 비밀 취급 인가(clearance)를 기반으로 하여 객체에 대한 액세스를 제어하는 방법이다. MAC 정책은 비밀 등급별 보안(multilevel security: MLS)기법 구현을 위한 방법론의 핵심이 된다.

대부분의 상용 데이타베이스 관리 시스템들이 채택하고 있는 보안 유지 방법은 데이타에 대한 사용자들의 사용 권한을 제어하는 임의적 액세스 제어 방식들이다[Slom 88]. 임의적 액세스 제어 방식이라고 명명된 이유는 데이타에 대한 사용 권한을 사용자 임의대로 다른 사용자들에게 넘겨줄 수 있는 액세스 제어 방식이기 때문이다. 이러한 DAC 방식은 대부분의 정직한 내부 사용자들에 대한 정보의 누출을 방지하는 경우에는 적합할 수 있으나, 악의적인 침입자들의 트로이 목마를 이용한 데이타의 액세스 또는 컴퓨터 바이러스에 의한 데이타의 액세스는 반드시 제한되고 방지되어야 함에도 불구하고 원천적으로 방지할 수 없는 결함을 가지고 있다. 트로이 목마는 프로그램 내에 인가되지 않은 사용자에게 정보를 누출시키는 악의의 코드를 수록한 것이다. 예를 들어, 유틸리티 프로그램 중의 정렬 프로그램에 트로이 목마가 감춰져 있다면, 사용자가 정렬 프로그램을 불러 자신의 화일들을 정렬시키고자 할 경우마다 인가 받지 못한 사용자에게 자신의 화일들을 통채로 복사시킬 수가 있는 것이다.

따라서, DAC 방식의 결점을 극복하기 위한 강제적인 액세스 제어 방식이 개발되었다. MAC 방

* 한국과학기술원 서울캠퍼스 정보 및 통신공학과

식은 주체와 객체라는 용어에 의해 기술된 Bell-LaPadula 모델에 기초한다[Lunt 90]. 객체는 데이타 화일, 레코드 또는 레코드 내의 필드로 이해될 수 있으며, 주체는 객체들에 대한 액세스를 요청할 수 있는 활성화된 프로세스이다. 모든 객체는 비밀등급이 할당되며, 각각의 주체도 등급별 비밀취급 인가가 되어야 한다. 비밀 등급은 아래에 기술한 두개의 구성 요소들로 이루어진다.

첫째, 계층적 등급으로서 통상 1급 비밀(top secret), 2급 비밀(secret), 3급 비밀(confidential), 그리고 비밀 해당사항 없음(unclassified)들로 구분된다.

둘째, 취급 분야 집합으로서 예를 들면 국방, 행정, 외교 분야등을 들 수 있다.

Bell-LaPadula 모델은 데이타 액세스를 할 경우, 아래의 제약조건을 부가한다. (1) 단순 특성(Simple Security Property, 상향열람 금지): 주체의 비밀등급이 객체의 비밀 등급 보다 동일하거나 높을 경우에만 객체의 읽기 액세스가 허용된다. (2) 복합 특성(*-Property, 하향 기록 금지): 주체의 비밀등급이 객체의 비밀등급 보다 동일하거나 낮을 경우에만 객체에 기록 액세스가 허용된다.

위에서 기술한 두개의 제약조건들은 상위 비밀 취급 인가자로 부터 하위 비밀 취급인가자에게로의 정보 누출이 없도록 고안된 것이다. 이러한 제약조건들은 강제적이고 시스템에 의해 모든 읽기와 기록 연산에 대해 자동적으로 실행되기 때문에 트로이목마에 의한 침투를 점검하고 방지할 수 있다.

그러나 최근에 밝혀진 바로는 Bell-LaPadula의 제약 조건들을 항상 올바르게 실행할지라도 보안상의 문제가 발생할 수 있음이 판명되었다[Koga 90].

안전한 시스템은 데이타에 대한 직접적인 비밀 누출 뿐만 아니라 간접적인 비밀 누출을 통한 불법적인 정보의 흐름을 차단할 수 있어야 한다. 비밀 채널(covert channel)이 후자에 속하는 간접적인 비밀 누출의 형태이다. 비밀 채널은 상위 비밀 취급인가자가 하위 비밀 취급인가자에게 정보의 양에 관한 다소를 불문하고 간접적인 정보 누출 수단을 제공할 수 있다[Lamp 73].

예를 들어, 트랜잭션을 종료시키기 위한 이단계 종료규약(two-phase commit protocol)을 사용하는 데이타베이스가 있다고 가정한다. 또한 임의의 트랙잭션이 2급 비밀 프로세스와 3급 비밀 프로세스와 함께 종료하기 위해 종료 준비완료(ready-to-commit) 메세지를 양쪽으로 부터 모두 받아야 하고 받지 못할 경우 취소(abort)된다고 가정할 경우, 순수한 데이타베이스 관점에서는 아무런 문제를 야기하지 않으나 보안상의 관점에서는 기밀 누출이 충분히 가능하다고 볼 수 있다.

2급 비밀 프로세스가 트랙잭션 종료에 동의하거나 동의하지 않거나를 결정하여 한개의 비트 정보를 전송할 수 있기 때문에 2급 비밀 프로세스로부터 3급 비밀 프로세스에게 서로 약속된 아래와 같은 방법으로 기밀 정보를 누출 시킬 수가 있다. 즉, 3급 비밀 프로세스가 다수의 트랜잭션들을 생성한 이후 3급 비밀 프로세스는 항상 트랜잭션의 종료에 동의하도록 한다면 2급 비밀 프로세스는 선별적으로 트랜잭션의 취소들을 야기시켜 3급 비밀 프로세스의 비밀 채널을 설치할 수가 있는 것이다.

MLS-DBMS 측면에서 언급해야 할 또다른 관점이 있다. 미 국방성의 요구 사항을 만족하기 위해서는 시스템이 안전하다고 것을 반드시 증명할 수 있어야 한다. 이러한 목적으로 정보 보호용 DBMS 설계자들은 TCB(trusted computing base, 보안커널 또는 참조 모니터) 개념을 준수하여 설계한다. TCB는 시스템 내의 모든 보안 관련 행위들에 대해 책임이 있어서 데이타베이스에 대한 모든 액세스들이 우회 통과될 수 없도록 하고 적절한 조치를 취한다. TCB는 보안 규격을 올바르게 실행하고 있음을 증명할 수 있도록 간단 명료하게 설계되어야 하며, 외부 침투가 불가능한 안전함이 증명될 수 있도록 TCB 이외의 다른 시스템 구성 요소들과 격리 되어야 한다.

미 국방성의 TCSEC에는 각종 컴퓨터 시스템의 보안 기준을 평가할 수 있는 평가기준 행렬표가 기술되어 있다. A1, B3, B2, B1, C2, C1, 그리고 D와 같은 등급이 부여되며, 각 등급별로 시스템이 해당 등급에서 반드시 보유해야 하는 요구사항들을 기술하고 있다[DOD 83].

간단히 요약하면, C1과 C2등급의 시스템은 데이타에 대한 DAC 기법을 제공해야 하며, B1 등급의

시스템은 MAC 기법을 제공해야 한다. B2 또는 B3, A1와 같은 상위 등급의 시스템은 특히 비밀 채널에 대한 보다 향상된 보증이 제공되어야 한다. A1등급에서는 가장 엄격한 정보보호 기준이 제시된다. D등급은 A, B 또는 C등급등으로 평가될 필요가 없는 보안 요구가 필요하지 않은 모든 시스템들로 구성된다.

지난 십수년간 데이타베이스 보안에 관한 문제들은 끊임없이 대두되었으며, 몇몇 훌륭한 제어기법들이 연구 개발되었다. 그러나 이들 이용 가능한 제어 방법들 보다 더 많은 보안문제들이 아직 남아 있다. 미국의 경우를 보더라도 1981년에서야 미국방성은 NCSC(National Computer Security Center)를 설립하여, 컴퓨터 시스템에 대한 보안성 평가의 기준이 되는 TCSEC(Trusted Computer Evaluation Criteria)를 제정하여 1983년에 초판, 1985년에 개정판을 발간하였고, 1985년 5월 이후로 NCSC는 데이타베이스 시스템에 TCSEC을 확장 적용하기 위한 TDI(Trusted DBMS Interpretation)을 준비하여 1988년 11월에 초고가 나왔다고 한다.

2. 비밀 보안용 DBMS 요구사항 분석

본 고에서 다룰 엄격한 비밀 보안용 데이타베이스 관리 시스템(multilevel secure database management system: MLS-DBMS)은 적어도 두가지 측면에서 기존의 상용 DBMS와는 크게 구분된다[Thur 90]. 첫째, 데이타베이스 내의 데이타 항목은 여러 단계의 비밀 등급을 가지며, 비밀 등급의 변경이 동적으로 이루어질 수 있어야 한다. 둘째, 데이타에 대한 사용자의 액세스 제어는 사용자에 부여된 등급별 비밀 취급 인가 여부에 반드시 의거해야 한다. MLS 기법 또는 MAC 정책은 Bell-LaPadula 모델에 기초하고 있다. 즉, 주체의 비밀 등급보다 높은 객체에 대한 읽기는 허용되지 않으며, 쓰기는 허용된다. 이러한 제약조건을 준수하면 비밀 등급이 높은 객체로 부터 낮은 객체로의 정보의 흐름이 차단될 수 있다. 따라서, 이들 제약사항들이 강제적이고 자동적으로 실행되기 때문에 트로이목마로 부터 보호될 수 있다.

2.1 기밀 데이타

몇몇 데이타베이스들은 기밀 데이타라는 것을 포함한다. 기밀 데이타는 공개적으로 만들어지지 않는 데이타를 말한다. 데이타 항목이 비밀인지 여부의 결정은 개개의 데이타베이스의 속성에 의존한다. 명백히 공중 도서 목록 데이타베이스는 기밀 데이타를 포함하지 않지만, 국방 데이타베이스는 전부 기밀이라고 볼 수 있다. 이러한 두 가지 경우는 전부가 기밀 내용을 갖지 않거나 전부 기밀이기 때문에 비교적 용이한 기법이 적용될 수 있다. 더욱 흥미롭고 어려운 문제는 데이타베이스의 일부가 극비인 MLS-DBMS 경우에 발생한다. 예를들어, 학교내의 학생 화일에서 학생의 성적 내용은 인증된 사람만이 액세스할 수 있도록 해야 한다. 사용자에 부여된 비밀 취급 인가가 인증된 사람만이 이러한 기밀 데이타 액세스할 수 있도록 하는 것이 MLS 액세스 제어 문제에서 상당히 중요하다.

아래 요인들이 데이타를 기밀로 만든다.

1) 원천적인 기밀성 : 값 자체가 원천적으로 극비라는 것을 드러낸다. 예들 들어, 방위 미사일이 설치된 위치 등이다.

2) 기밀 근원으로부터의 기밀성 : 데이타의 근원이 기밀과 관련된 수단이 될 수 있다. 예를 들어, 범죄자가 누설한 특별한 정보가 이에 해당된다.

3) 선언된 기밀성 : 데이타베이스 관리자나 데이타의 소유자는 데이타가 기밀이라고 선언할 수 있다. 예를 들어, 군사 정보 데이타나 미술품의 기증자 이름 등이다.

4) 특정 속성이나 레코드의 기밀성 : 데이타베이스에서 특정 속성이나 레코드는 기밀로 분류될 수 있다. 예를 들어, 인사 데이타베이스에서 봉급과 같은 것이 이에 해당된다.

5) 이미 드러난 정보와 관련된 기밀성 : 몇몇 데이타는 다른 데이타의 존재에 의해 기밀로 되어진다. 예를 들어, 어떤 금이 발견된 곳의 경도만이 알려지고 위도는 알려지지 않을 경우의 좌표이다.

2.2 기밀 데이타의 노출 형태

데이타뿐만 아니라 데이타의 특성도 기밀을 가질 수 있다. 이런 기밀 데이타는 더욱 철저한 보안을 요구하지만 때로는 비인증된 사용자에게 쉽게 노출되기도 한다. 여기서는 노출의 여러가지 형태에 대해 알아보기로 하자.

1) 정확한 데이타값의 노출 : 가장 심각한 노출은 기밀 데이타 본래의 정확한 값이 노출되는 것이다. 사용자는 데이타가 기밀 데이타인지 모르고 일반적인 데이타 요청처럼 데이타를 요구하게 된다. 이 경우 우연히 기밀 데이타가 보호받지 못하고 전달될 수 있다면 이 기밀 데이타의 보안은 파괴된다.

2) 영역의 노출 : 기밀 데이타의 영역이 노출되는 것으로 기밀 데이타의 값 y가 L과 H라는 두 값 사이에 있음을 알게 된 경우이다. 이진 탐색(binary search)과 같은 방법을 이용하여, 실제의 값이 노출될 수 있다.

3) 부정 결과에 의한 노출 : 부정 결과를 결정하는 질의가 있을 수 있다. 즉, x는 y의 값이 아니다라는 형태이다. 예를 들어, 어느 비밀 요원의 성별이 무엇인가라는 질의에 대하여 남자가 아니다라는 응답에 의하여 여자라는 정보를 알 수 있다. 이와 같이 부정 결과를 산출하는 질의를 통하여 원하는 정보가 노출될 수 있다.

4) 존재성의 노출 : 어떤 경우 데이타의 존재 자체가 데이타 값에 관계없이 비밀이 될 수 있다. 예를 들어, 사업자가 종업원들의 시외전화 사용을 감시하고 있다면, 개인 화일의 장거리 전화 필드 존재 자체가 기밀 데이타로 분류된다.

5) 확률값에 의한 노출 : 마지막으로 어떤 원소가 어떤 값을 갖고 있는지 확률적으로 결정할 수 있다.

3. 향후 연구 방향

3.1 보안유지 기능을 갖는 트랜잭션 관리

MLS-DBMS는 기밀 데이타에 대한 직접적인 노출뿐만 아니라 불법적인 정보의 흐름을 초래하는 간접 노출 방법인 비밀 채널(covert channel)에 대해서도 대비책이 있어야 한다[Tsai 90]. 비밀 채널은 비밀 등급이 높은 사용자가 비밀 등급이 낮은 사용자에게 정보를 제공하는 간접 수단을 지칭한다.

동시성 제어는 데이타베이스 관리 시스템(DBMS)의 기본적인 요구 중에 하나이다. 동시성 제어의 목적은 동시에 수행하는 트랜잭션이 충돌과 틀린 결과를 만들지 않도록 하는 것이다[Bern 87]. MLS-DBMS내에 동시성 제어 기법은 또한 보안 요구를 위반하지 않아야 한다. 특히 강제적 보안 규정을 준수해야 하며, 비밀 채널을 도입해서는 않된다.

MLS-DBMS에서의 동시성 제어는 직렬성은 물론 보장하여야 하며 보안성도 보장될 수 있어야 한다. 그러나 기존의 동시성 제거 기법을 MLS 환경에 수정없이 적용할 경우 보안성이 보장되지 않는 문제가 발생될 수 있다.

낙관적인 방법[Kung 81]의 경우 무한정 기다림(starvation)현상이 발생할 수 있다. 예를 들어, 임의의 트랜잭션이 자신의 보안 등급보다 더 높은 데이타를 읽을려고 할 경우 판독 단계, 검증 단계를 거쳐 기록 단계에 도달되었을 때에 비로소 철회되고, 재시작된 후 다시 위의 단계를 거쳐 철회되는 과정을 반복하게 된다.

이단계 로킹 기법(2PL)의 경우는 보안성이 보장되지 않는다. 예를 들어, 아래와 같은 입력을 생각할 경우:

```
T1(S): R(y, U)          R(z, U)
T2(U):        W(y, U)
```

이러한 입력은 2PL 규약에 의해 아래와 같이 스케쥴이 조정된다.

```
T1(S): R(y, U)  R(z, U)
T2(U):                  W(y, U)
```

이때, T2(U): W(y, U)는 T1(S): R(y, U)에 대해 지연이 되었다. 이러한 지연시간을 T2와 T1이 감지할 수 있다면, T1(S)와 T2(U) 사이에 시간지연 비밀 채널(timing covert channel)이 설치될 수 있는 것이다.

동시성 제어 스케쥴러를 구현한 적법한 사용자 주체(trusted subject)를 사용할 때의 문제점은 동시성 제어 스케쥴러의 보안성의 평가가 매우 어렵다는 것이다. 검증 가능 여부는 심지어 단순한 프

로그램에서도 어려운 문제이며, 복잡한 프로그램인 동시성 제어 스케쥴러의 구현에 대한 검증은 대단히 어렵게 여겨진다. 더우기, DBMS 스케쥴러는 때때로 버퍼 관리와 회복과 같은 복잡한 DBMS 구성 요소와 연관 되어 있어 스케쥴러만 따로 분리하여 평가하기란 불가능하다. 기본적인 DBMS 구성 요소에 관한 보안 관련 특성은 아직까지 기출판된 문헌들에서는 언급되지 않았다. MLS-DBMS는 trusted computing base(TCB)상에 위치하고 있다는 것을 전제로 한다.

3.2 객체 지향 데이타베이스 시스템을 위한 MAC보안 기법

객체 지향 데이타베이스 시스템(OODBS)에서는 실세계의 모든 개념적 개체가 단일 개념의 객체로서 모델링될 수 있다. 또한 객체는 데이타를 저장하고 그 데이타에 대한 연산을 제공하는 독립적인 단위이기 때문에 데이타 추상화 개념을 잘 지원해 준다. 뿐만 아니라 데이타 사이에 존재하는 복잡한 의미관계(semantic relationship)인 일반화(generalization)와 통합(aggregation)을 쉽게 나타낼 수 있다. 일반화는 둘 또는 그 이상의 하위 단계의 개체 집합을 합하여 더 높은 상위 단계의 개체 집합을 생성하는 것으로 하위 단계에 있는 개체 집합들 사이의 차이점을 감추고 유사점을 강조하기 위해 사용된다. IS-A 계층관계가 일반화의 예이다. 통합은 관계를 상위 단계의 개체로 취급하는 추상화이다. IS-PART-OF 계층관계가 통합의 예이다.

현재까지 OODB 시스템에 대한 데이타 모델의 표준화는 아직 이루어지지 않고 있다[Atki 89]. 따라서, MCC에서 개발한 ORION 객체 모델을 우선적으로 고려하도록 하겠다. ORION 객체 모델은 객체 지향 모델의 범용적인 공통요소들을 많이 보유하고 있으며, 그 응용분야가 상대적으로 크다고 볼 때 MLS-OODBS를 위한 객체 모델의 대상으로 선택 가능하다고 볼 수 있기 때문이다.

MLS-OODBS에 기초한 보안 정책은 아래와 같은 특성들을 가진다. 객체 지향 데이타베이스의 객체와 보안 정책에서의 객체와의 혼동을 피하기 위해서 본 절에서는 객체 대신 개체로 표기하도록 한다.

(i) 주체와 개체는 보안등급이 할당된다.

(ii) 주체는 주체의 보안등급이 개체의 보안등급을 지배하면 개체에 대한 읽기 액세스를 가진다.

(iii) 주체는 주체의 보안등급이 개체의 보안등급과 동일할 경우 개체에 대한 쓰기 액세스를 가진다. BellLaPadula *-특성과는 보안등급이 높은 개체로 쓰기를 허용하지 않는 점이 다르다. *-특성을 따를 경우 주체가 임의의 데이타를 쓰고 난 후, 나중에 읽을 수가 없다는 것으로도 해석되며 일반적인 응용의 경우에는 너무 엄격하거나 자연스럽지 못한다고 여겨지기 때문이다.

(iv) 주체는 주체의 보안등급이 방법의 등급과 방법이 정의된 형의 등급 모두를 지배하면 방법을 실행시킬 수 있다.

(v) 방법은 실행을 개시시킨 주체의 보안등급으로 실행한다.

(vi) 방법 m1이 실행중에 또 다른 방법 m2가 실행되어져야 한다면 m2는 m1의 실행등급이 m2의 보안등급과 m2가 정의된 형의 보안등급 모두를 지배하는 경우에만 실행할 수 있다.

(vii) 새로운 객체가 방법의 실행 결과로 생성되어져야 한다면 객체는 방법의 실행을 개시시킨 주체의 보안등급에서 생성된다.

다중인스턴스(polyinstantiation) 처리[Jajo 90]는 실세계에서 서로 보안등급이 다른 주체들로 하여금 단일 개체에 대해 서로 다른 뷰를 가지도록 할 때 발생한다. 객체 지향 시스템에서는 서로 다른 뷰는 서로 다른 객체 값, 서로 다른 클래스 구조, 서로 다른 클래스 방법과 서로 다른 방법의 정의등과 관련지울 수 있다. 다중인스턴스 처리의 유형은 아래와 같다.

1) 객체 값의 다중인스턴스 처리 : 객체 o에 대한 보안등급이 2급비밀인 주체의 뷰는 제대로 된 값을 보여 주지만, 보안등급을 부여받지 못한 사용자에게는 허위정보를 보여준다.

2) 클래스 구조의 다중인스턴스 처리 : 고용인 클래스(성명, 주민등록번호, 급여액)에 대한 보안등급을 부여 받지 못한 사용자의 뷰는(성명, 주민등록번호)로 급여액 인스턴스 변수가 생략되어야 한다.

3) 클래스 방법 다중인스턴스 처리 : 고용인 클래스에 대해 보안등급을 부여받지 못한 사용자는 get-성명, change-성명의 방법들에 의한 뷰를 가지지만 2급 비밀취급인가를 받은 주체는 get-성명, change-성명 뿐만 아니라 get-급여, change-급여액의 방법들을 포함한 뷰를 가진다.

4) 방법의 다중인스턴스 처리 : update-급여액의 방법에 대한 비인가자의 뷰는 인상분이라는 한개의 매개변수만을 갖지만, 인가자의 뷰는 인상분과 새로 인상된 급여총액과 같이 두개의 매개변수를 가진다.

3.3 객체 지향 데이타베이스 시스템을 위한 권한 모델

권한 모델(authorization model)은 데이타베이스에서 지원되는 데이타 모델과 서로 일관성있게 설계되어야 한다. 현재 존재하는 데이타베이스 시스템에서 지원되는 권한 모델은 모두 관계형(relational), 계층형(hierarchical), 망형(network) 데이타 모델에 맞게 개발되었다. 몇몇 데이타베이스 전문가들은, 이 권한 모델들이 객체지향 데이타 모델(object-oriented data model)이나 의미적 데이타 모델(semantic data model)과 같은 차세대의 데이타 모델에는 적합하지 않은 몇가지 중요한 단점을 지적하면서, 그러한 결점을 제거하는 시도로서 새로운 권한 모델을 제시하였다[Rabi 88]. 현재 존재하는 권한 모델들은 권한의 단위를 릴레이션(relation) 또는 릴레이션의 속성(attribute)으로 가정하고 있다. 더우기 이 모델들은 클래스 계층 구조와 방법, 또는 복합 객체(composite objects) 버전(version)과 같은 의미적 모델링 개념(semantic modeling con-cepts)등 객체 지향 개념의 의미를 반영하지 않는다.

[Rabi 88]의 모델은 [Fern 75]에서 처음 정형화된 암시된 권한(implicit authorization)의 개념을 발전시킨 것이다. 그리고 그것을 객체 지향 개념과 의미적 모델링 개념으로 확장한 것이다. 암시된 권한의 발상은, 어떤 데이타베이스 객체에 대하여 한 사용자에게 특정한 권한을 부여하는 것이 다른 권한을 유도할 수 있다는 것이다. 권한은 권한의 주체(사용자 또는 사용자 집단), 권한의 종류(참조, 갱신, 생성) 그리고 권한의 객체(단일 객체, 객체 집단, 데이타베이스 전체)로 구성된다. 명시된 권한(explicit authorization)은 권한 정의의 3차원, 즉 권한 주체, 권한 종류, 권한 객체의 임의의 조합에 의하여 다른 권한을 유도할 수 있다. 예를 들어, 어떤 객체 집단(여기서 객체는 클래스, 릴레이션 또는 레코드형이 될 수 있다)에 대하여 한 사용자 집단에 갱신 권한을 부여했다면, 그 권한은 다음과 같은 권한들을 유도할 수 있다: 그 객체 집단을 구성하는 임의의 구성 객체에 대한, 그 사용자 집단의 임의의 구성원의 갱신 권한, 그 객체 집단 또는 그 구성 객체에 대한 그 사용자 집단의 임의의 구성원의 참조 권한 등. 암시적 권한 개념의 도입은 모든 권한들을 명시할 필요를 없애 준다. 시스템으로의 침입을 감시하기 위하여, 권한 메카니즘이 명시적으로 저장된 권한들의 최소한의 집합으로부터 필요한 권한의 여부를 계산해 낼 수 있기 때문이다. 물론 암시된 권한으로 인한 계산 부담은, 특정한 응용 환경에서 줄어드는 권한에 대한 기억 장소의 양과 반드시 비교해 보아야 한다.

3.4 이질형 분산 데이타베이스 시스템에서의 보안

이질형 분산 데이타베이스 시스템(Heterogeneous Distributed Database System : HDDBS)은 개별 데이타베이스 관리 시스템에 의해 자치적으로 관리되는 개별 데이타베이스 시스템(DBS) 사이에 상호 연산을 지원하는 시스템이다. 개별 DBS는 전역 스키마가 없는 약한 결합을 형성하거나 연합 DBS를 형성하는 강한 결합을 이룬다. HDDBS 시스템에서 데이타베이스 보안은 매우 중요한 기능이나 구현에 있어 아래에 기술한 이유들로 대단히 복잡하고 어려운 일로 예측된다.

첫째, HDDBS는 개별 DBS 보다 훨씬 많은 사용자 그룹이 있고 이들 다수의 사용자에 대해 보다 정밀한 액세스 제어가 필요하다.

둘째, 개별 DBS는 각기 다른 사용자들의 그룹에 의해 저장된 데이타의 상이한 부분만을 공유하려는

것이 통상적인 경우이다.

셋째, HDDBS에서 개별 DBS를 동시에 액세스가 가능하여 권한 없는 사용자에 의한 정보 유출의 위험이 단일 DBS에 비해 매우 높다.

넷째, 개별 DBS들은 서로 다른 DBMS에 의해 자치적으로 운용되며, 각기 다른 MAC 및 DAC 기법들이 사용될 수 있다.

대부분 관계형 DBMS는 현재 액세스 제어와 뷰 기능으로 보안 기능을 지원한다. 사용자는 SQL의 GRANT 문장을 사용하여 릴레이션을 생성, 변환, 수정 그리고 선택하는 권한을 부여 받는다. 사용자는 또한 부여된 권한을 다른 사용자에게 전파하는 특권을 보유할 수 있다. 이 특권은 시스템 보안 책임자가 REVOKE 문장을 사용함으로써 취소될 수 있다. 관계형 DB 시스템에서 뷰 기능은 시스템 관리자 또는 보안 책임자에게 융통성을 부여하여, 기저 릴레이션으로부터 유도된 어떠한 릴레이션도 될 수 있는 뷰에 대한 권한을 허용할 수 있다. 다단계 보안등급을 갖는 MLS-DBMS는 다양한 보안등급으로 분류된 데이타를 저장하고, 사용자의 비밀 취급 등급 변경이 가능하면서도 비밀 취급 인가가 되지 않은 사용자들로 하여금 비밀 데이타가 유출되는 것을 방지할 수 있어야 한다. 이러한 보안 기법은 보다 융통성이 있고, 보호의 단위는 튜플 또는 속성의 단위까지 세분화 될 수 있다. 비록 HDDBS와 같이 TCB를 요구하는 진정한 의미의 다단계 보안 시스템과 같은 방대한 소프트웨어 시스템을 만드는 것은 대단히 어려운 작업임에는 틀림없으나 결코 불가능한 것은 아니다. MAC 기법의 개념은 HDDBS에서도 적용될 수 있다[Kang 92].

국내 연구동향 중 현재 한국과학기술원 문송천 교수 실험실에서 진행 중인 확장 연구과제로서 국내 최초 연구 개발된 관계형 데이타베이스 시스템인 IM의 차기 버전인 상용 IM에 보안기능을 구현시키는 연구활동이 내년 초 완료될 예정이며, 역시 KAIST에서 제작된 분산 데이타베이스 관리체계인 DIME(Distributed Information Management)에 다단계 보안기능을 설계 및 구현하는 연구가 1994년에 완료될 예정이다.

4. 결 론

데이타베이스 보안에 관한 연구의 역사적 진행 과정을 돌이켜 보면 데이타베이스의 완벽한 보안유지란 매우 힘든 문제임을 알 수가 있다. 가장 주된 이유는 데이타베이스의 기본 기술이 먼저 개발된 이후에 보안 문제를 고려해 왔었기 때문이다. 즉, 데이타베이스 기술이 데이타베이스 보안 기술보다 훨씬 앞서 갔었다. 이러한 기술 격차를 줄여나가는 방법으로 새로운 데이타베이스 기술을 보안 관련 기술과 병행하여 연구하는 것이 국내의 현실에서 볼 때 가장 바람직할 것이다.

비밀 보안용 MLS-DBMS에 관한 연구분야는 광범위하고 해결 해야할 문제들이 산적해 있다. 본고에서는 제시된 문제들을 중심으로 보다 철저한 분석과 집중적인 연구가 시급히 요청된다.

참 고 문 헌

[Atki 89] M. Atkinson et al., "The Object-Oriented Database System Manifesto," Proc. of Deductive and Object-Oriented Databases, 1989, pp.40-57.

[Bern 87] P.A. Bernstein, V. Hadzilacos, and N. Goodman, "Concurrency Control and Recovery in Database Systems," Addison-Wesley, Reading, MA, 1987.

[DOD 83] "Department of Defense Trusted Computer System Evaluation Criteria," Department of Defense, National Computer Security Center, 1983.

[Fern 75] E.B. Fernandez, R.C. Summers, and C.D. Coleman, "An Authorization Model for a Shared Database," In Proceedings of the 1975 ACM-SIGMOD International Conference. ACM, New York, 1975.

[Jajo 90] S. Jajodia and R. Sandhu. "Polyinstantiation Integrity in Multilevel Relations," Proc. IEEE Symp. on Research in Security and Privacy, May 1990, pp.104-115.

[Kang 92] Sukhoon Kang and Songchun Moon, "An Integrated Access Control in Heterogeneous Distributed Database Systems," Journal of Microprocessing and Microprogramming, Vol. 35, No. 1-5, 1992, pp.429-436.

[Koga 90] B. Kogan and S. Jajodia, "Concurrency Control in Multilevel-secure Databases Using Replicated Archiecture," Proc. ACM SIGMOD Int'l. Conf. on Management of Data, May 1990, pp. 153-162.

[Kung 81] H.T. Kung and J.T. Robinson, "On Optimistic Methods for Concurrency Control," ACM trans. on Database Systems, Vol. 6, No. 2, Jun. 1981, pp.213-226.

[Lamp 73] B.W. Lampson, "A Note on The Confinement Problem," CACM, Vol. 16, No. 10, Oct. 1973, pp.613-615.

[Lunt 89] T.F. Lunt, "Access Control Policies for Database Systems," In C.E. Landwehr, Editor, Database Security II: Status and Prospe cts, North Holland, 1989.

[Lunt 90] T.F. Lunt, D.E. Denning, R.R. Schell, M. Heckman, and W.R. Schockley, " The SeaView Security Model," IEEE Trans. on Software Engineering, Vol. 16, No. 6, Jun. 1990, pp.593-607.

[Rabi 88] F. Rabitti, D. Woelk, and W. Kim, "A Model of Authorization for Object Oriented and Semantic Databases," In Proceedings of the International Conference on Extending Database Technolgy(Venice, Italy), Mar. 1988.

[Slom 88] M.S. Sloman and J.D. Moffet, "The Source of Authority for Commercial Access Control," Computer, Vol. 21, No. 2, Feb. 1988.

[Thur 90] B. Thuraisingham and P.D. Stachour, "Design of LDV: A Multilevel Secure Relational Database Management Systems," IEEE Trans. on Knowledge and Data Engineering, Vol. 2, No. 2, Jun. 1990, pp.190-209.

[Tsai 90] W.T. Tsai and T.F. Keefe, "Multiversion Concurrency Control for Multilevel Secure Database Systems," Proc. IEEE Symp. on Research in Security and Privacy, May 1990, pp. 369-383.

□ 著者紹介

강 석 훈

한양대학교 전자공학 학사
한국과학기술원 전산학 석사
현재 한국과학기술원 전산학 박사과정
현재 금성정밀(주)기술 연구소 선임연구원

문 송 천

한국과학기술원 전산학 박사
미국 일리노이(어바나)대학교 전산학 박사
숭실대학교 전산학과 교수
영국 에딘버러대학교 전산학과 교환교수
한국정보과학회 데이타베이스 연구회 회장
현재 한국과학기술원 정보 및 통신공학과 교수
현재 유럽 정보과학회 이사
국내 및 아시아권 최초로 다수사용자 관계형 DBMS 'IM' 개발(1990. 5)