通信情報保護學會誌
第2卷 第4號, 1992. 12

데이타베이스 시스템의 보안평가 기준

신 장 균*

1. 개 요

컴퓨터 보안의 주요 목적은 정보의 비밀성(secrecy), 무결성(integrity), 그리고 가용성(availability)을 보장하는데 있다. 정보의 비밀성은 컴퓨터 시스템내에 저장된 정보의 불법적인 노출로 부터 보호하는 것이고, 정보의 무결성은 정보가 불법적으로 변경되지 않도록 보호하는 것이며, 정보의 가용성은 서비스 부인 공격으로부터 보호하는 것이다. 이러한 컴퓨터 보안문제는 정보를 어떻게 통제하여 보호하는가라는 보호 메카니즘의 설계와 구현의 문제와, 그리고 구현된 보호 메카니즘을 어느 정도 신뢰할 수 있는가라는 보안의 평가 및 검증의 문제로 분류할 수 있다.

본고에서는 비밀정보를 적절하게 보호할 수 있는 대책이 요구되고 있는 데이타베이스 시스템의 보안평가 기준을 살펴보기 위해 먼저 컴퓨터 보안 평가의 주도적 역할을 하고 있는 미국의 컴퓨터 보안평가 지침서인 TCSEC(Trusted Computer System Evaluation Criteria)의 보안 요구사항과 평가등급 내용을 살펴보고, 이 기준을 데이타베이스 시스템에 적용하기 위한 TDI(Trusted Database Management System Interpretation of the TSCEC)를 분석하여 데이타베이스 보안 요구사항을 제시하였다.

2. 컴퓨터의 보안평가기준

미국의 NCSC(National Computer Security Center)는 1985년에 안전한 컴퓨터 시스템을 위한 평가 지침서인 TCSEC(일명"Orange Book")을 발간하였다. 안전한 컴퓨터 시스템은 인가된 사용자나 사용자 그룹을 식별하고, 정보에 대한 읽기, 쓰기, 삭제등에 대한 엑세스 요구를 통제한다. 컴퓨터 보안의 절대적인 보증을 기대하는 것은 비효율적이기 때문에 어떤 종류의 보안측정 도구들이 컴퓨터 시스템의 보안을 평가하는데 적절한지 식별되어야 한다. TCSEC은 컴퓨터 시스템의 보안을 효과적으로 평가하기 위해 6개의 기본 요구사항을 정의하였으며, 그 기본 요구사항을 만족시키는 수준에 따라 7가지의 평가등급을 제시하고 있다.

2.1. 보안 요구사항

기본적인 보안 요구사항은 보안정책(security policy), 표시(marking), 식별(identification), 기록성(accountability), 보증(assurance), 연속적 보호(continuous protection)이다. 이러한 요구사항 중에서 보안정책, 표시, 식별, 기록성은 정보에 대한 엑세스를 통제하기 위한 사항이고, 보증과 연속적 보호는 신뢰성 있는 컴퓨터를 제공하기 위한 보안

* 육군사관학교 부교수, 종신회원.

검증에 관한 사항이다.

1) 보안정책

컴퓨터 시스템에는 명시적이고 잘 정의된 보안정책이 있어서 주체와 객체가 식별되고 주체에 의한 객체에 대한 엑세스 요구를 인가해 줄 것인가에 대한 보안규칙을 적용해야 한다.

2) 표 시

모든 객체는 그 객체의 보안등급을 나타내는 "레이블"을 갖고 있어야 하는데 객체와 보안 레이블의 연관을 표시(marking)라고 한다. 이러한 레이블들은 객체에 대한 엑세스 요구시마다 비교를 위해 사용가능해야 한다.

3) 식 별

모든 주체들은 유일하고 분명하게 식별되어야 한다. 컴퓨터 시스템은 엑세스하는 주체가 누구인지 식별 가능해야 하며, 이와 관련된 인증정보는 안전하게 관리되어야 한다.

4) 기 록 성

시스템 보안에 영향을 미치는 동작에는 새로운 가입자의 가입, 주체나 객체의 보안 등급변화, 새로운 주체나 객체에 대한 보안등급 부여, 비인가된 엑세스 요구 등이 있는데 시스템은 이러한 동작들에 대한 안전하고 완벽한 기록들을 유지해야 한다.

5) 보 증

보안정책, 표시, 식별, 기록성이 시스템에 의해 적용된다는 것을 보증하기 위한 메카니즘을 포함해야 하며, 메카니즘의 효율성을 평가할 수 있어야 한다.

6) 연속적 보호

보안을 구현한 메카니즘은 비인가된 변화나 침투에 의한 방해로부터 계속적으로 보호되어야 한다.

2.2. 보안 평가등급

NCSC는 6개의 기본 요구사항을 만족하는 정도에 따라 크게 D분류, C분류, B분류, A분류를 구분한 다음 각 분류에 대해 세분하여 7가지 보안등급을 제시하였는데 낮은 보안수준으로부터 높은 보안수준으로 각 등급을 나열하면, C, C1, C2, B1, B2, B3, A1이다. 각 등급은 서로 독립적인 것이 아니고 서로 연관되어 있으며 상위 등급은 하위 등급에 보다 많은 보안 요구사항들을 추가시킨 것으로 정의된다. 실제로 이 등급들은 D, C, B, A, 의 4가지 분류와는 다른 4개의 집합으로 구분할 수 있다 : 집합 D는 요구사항이 없는 등급이다 ; 집합 C1/C2/B1은 많은 상업적 운영체제에 대한 일반적인 보안특성을 요구하는 등급들이다 ; 집합 B2는 사용하고 있는 모델의 보안에 대한 정확한 증명과 TCB의 서술적인 명세서를 요구하는 등급이다 ; 집합 B3/A1은 TCB에 대해 더욱 정확하게 증명된 명세서와 공식 설계를 요구하는 등급들이다 ; 이와 같은 각 보안등급에서 요구하는 보안특성들은 다음과 같다.

1) 등급 D : Minimal Protection

요구되는 보안특성이 없는 등급으로 보안평가가 실패한 시스템이 포함된다.

2) 등급 C1 : Discretionary Security Protection

C1 등급은 동일 수준의 기밀성을 갖는 데이타를 처리하는 사용자들의 환경을 위한 등급으로 시스템은 데이타로부터 사용자들의 격리(separation)를 제공한다. 사용자들이 그들 자신의 데이타를 보호할 수 있는 엑세스 제한을 구현하기에 충분한 엑세스 제어 메카니즘이 있어야 한다. C1 등급으로 분류되기 위해서는 시스템은 보안기능을 포함하는 보안 영역(domain)을 가져야 하는데 이 영역들은 비인가된 변경(tampering)으로부터 보호되어야 한다.

C1등급에서의 가장 중요한 개념은 "discretionary" 제어이다. 모든 사용자 그룹은 확인되어야 하며, 각 사용자 그룹은 다른 사용자 그룹의 엑세스 요구를 허락 또는 거부할 수 있는 권한을 갖는다. 즉 사용자 그룹의 식별에 근거하여 객체에 대한 엑세스 요구를 통제하게 된다. 또한 시스템 보안을 보증하기 위해서는 침투시험(penetration testing)과 같은 방법을 수행하여 비인가된 사용자 그룹이 보호 메카니즘을

우회하거나 파괴하는 방법이 없다는 것을 보여야 한다. 이러한 C1 등급에 요구되는 보안기준은 다음과 같다.

- 보안정책(Security policy)
  - Discretionary 엑세스 제어
- 기록성(Accountability)
  - 식별(identification)과 인증(authentication)
- 보증(Assurance)
  - 시스템 구조(system architecture)
  - 시스템 무결성(system integrity)
  - 시스템 시험(system testing)
- 문서화(Documentation)
  - 사용자 보안 가이드(security feature user's guide)
  - 신뢰기능 메뉴얼(trusted facility manual)
  - 시험문서(test documentation)
  - 설계문서(design documentation)

3) 등급 C2 : Controlled Access Protection

C2 등급은 보호기능이 개인 사용자 수준으로 구현되는 discretionary 엑세스 제어를 제공한다. 시스템의 감사추적(audit trail)은 각 객체에 대한 각 개인들의 엑세스를 추적할 수 있어야 한다. C2 등급에 부과된 추가의 규제는 잔여정보(residure) 노출의 제거이다. 잔여정보란 한 프로세스가 실행이 종료된 후 레지스터, 메모리, 디스크에 남아있는 데이타이다. 즉 프로세서 종료시에 기억장소에 남아있는 것 뿐 아니라 보조기억 장치에 쓰여진 데이타를 포함한다. C2 등급은 잔여정보인 한 객체(object)가 다른 사용자에 의해 재사용될 수 있기전에 0으로 쓰기를 하는 등의 방법으로 제거되어야 하는 요구사항을 포함한다. C2 등급의 시스템을 예를들어 보면 IBM MVS 운영체제와 DEC VAX/VMS 운영체제가 있다.

4) 등급 B1 : Labeled Security Protection

모든 B 등급은 nondiscretionary 즉, 강제적인 엑세스 제어인 mandatory 엑세스 제어(MAC)를 포함한다. B1 등급에서 제어되는 모든 주체와 객체들은 각각 하나의 보안수준(security level)을 할당받아야 한다. 제어되는 각 객체는 개별적으로 보안수준에 의해 레이블이 붙여지고 이 레이블들이 기본적으로 엑세스 제어 결정에 사용된다. 엑세스 제어는 계층적 등급(hierachical level)과 비계층적 범주(nonhierachical categories)를 모두 포함하는 보안모델(security model)에 기초로 하고 있다. 계층적 등급을 갖는 시스템의 예로는 unclassified, classified, secret, top secret의 계층적 등급을 갖는 군사적 등급을 들 수 있고 비계층적 범주는 최소 권한(need-to-know) 범주 집합을 의미한다. 이러한 mandatory 엑세스 제어 정책을 포함하고 있는 대표적인 보안 모델은 Bell-Lapadula 모델이다. 따라서 B1 등급은 DAC 통제를 포함하며, 나아가 Bell-Lapadula 모델의 모든 통제를 포함해야 한다.

5) 등급 B2 : Structured Protection

B2 등급의 주요한 개선은 설계 요구사항이다 : B2 시스템의 설계와 구현은 더욱 철저한 테스트와 조사가 가능해야 한다. 검증 가능한 설계가 제시되어야 하며, 테스트는 시스템이 제시된 설계를 구현했음을 확인할 수 있어야 한다. 따라서 시스템의 모든 주체와 객체들에게 적용되는 DAC와 MAC 통제가 명확하게 정의되고 문서화된 공식적인 보안모델을 기초로 구성되어야 한다. B2 등급의 또 다른 특성은 Covert 채널의 분석이 요구되는 점이다. Covert 채널은 서로 통신할 수 없는 프로세스들이 비정상적인 방법으로 정보를 누출시키는 채널이다. 즉 직접적으로 통신을 하는 것이 아니라 제 3 의 객체를 통해 간접적으로 통신을 하거나, 또는 한 프로세스의 실행동작으로부터 다른 프로세스가 정보를 획득하는 가상적인 채널이다.

6) 등급 B3 : Security Domains

B2 등급은 주체의 객체에 대한 모든 엑세스를 통제하는 조회 모니터(reference monitor) 요구사항을 만족해야 한다. 조회 모니터는 시스템의 모든 엑세스 메카니즘을 포함하고 있는 부분으로 엑세스 권한집합이 데이타베이스로 구성되어 있으며, 활동중인 모든 주체가 객체에 대한 엑세스 권한을 얻기 위해

서나 엑세스 권한을 변경하기 위해서는 반드시 조회 모니터에 요구하여 승인을 받아야 하는 규칙이 적용된다. 이러한 조회 모니터는 분석과 테스트가 용이하도록 충분히 작아야 하며, 침투로 부터 완전히 보호(tamperproof) 되어야 한다. 이러한 tamperproof 시스템은 침투에 대해 매우 민감하게 저항하는 시스템이다. 따라서 시스템 보안에 관한 위반 사건이 발생했을 때 즉시 식별할 수 있는 감사(audit) 능력과 시스템 회복능력이 요구된다.

7) 등급 A2 : Verified Design

A1 등급은 공식적으로 검증된 시스템 설계를 요구한다. A1 시스템의 보안능력은 B3 등급의 능력과 같다. A1 등급은 trusted computing base가 정확하게 구현되었다는 높은 수준의 보증(assurance)을 요구하는데 A1 등급 검증(certification)을 위한 5가지 중요한 기준이 제시되고 있다.

i) 보호 시스템의 공식적인 모델과 그 모델의 일관성 및 적절성에 대한 증명

ii) 보호 시스템의 공식적인 최상위 명세(top-level specification)

iii) 최상위 사양이 보호 모델과 일치한다는 것을 증명

iv) 명세와 일치하는 구현

v) Covert 채널의 공식적인 분석

이러한 A1 등급으로 분류된 시스템에는 Honeywell SCOMP가 있으며 SRI의 PSOS(Provably Secure Operating System), IBM의 KVM/370 (Kernelized VM/370), 그리고 Ford aerospace의 KSOS(Kernelized Secure Operating System)이 A1 등급을 목표로 연구 개발되고 있다.

3. 보안평가 기준의 DB 적용

3.1. TDI의 보안 요구사항

미국의 NCSC(National Computer Security Center)는 1991년에 보안 평가 기준의 데이타베이스 적용인 TDI(Trusted Database Management System Interpretation of TCSEC)을 발간하였다. TDI는 TCSEC의 보안 요구사항을 기반으로 DBMS에 적용하는 경우에 필요한 특정한 보안요구사항을 명시한 것으로 TCSEC의 DBMS 응용에 대한 해석된 보안요구사항을 포함하고 있다. 이러한 해석된 요구사항(interpreted requirements)은 보안정책(Security Policy), 기록성(Accountability), 보증(Assurance), 그리고 문서화 (Documentation)로 구분되어 있는데 이를 요약하면 표 1과 같다.

표 1. 해석된 요구사항

구분	세 부 항 목	보 안 요 구 사 항
보안정책	Discretionary 엑세스 제어	TCSEC의 요구사항과 동일
	객체 재사용	TCSEC의 요구사항과 동일
	레이블(Labels)	변경된 요구사항 제정
	Mandatory 엑세스 제어	TCSEC의 요구사항과 동일
기록성	식별과 인증	TCSEC의 요구사항과 동일
	감사(Audit)	변경된 요구사항 제정
보증	운영적 보증 (Operational Assurance)	시스템 구조 요구사항만 변경하여 제정(기타요구 사항은 TCSEC과 동일)
	생명주기 보증(Lift Cycle Assurance)	설계사양과 검증 요구사항만 변경하여 제정(기타 요구사항은 TCSEC과 동일)
문서화	메뉴얼과 사용자 지침서	TCSEC의 요구사항과 동일
	시험(Test) 문서	TCSEC의 요구사항과 동일
	설계(Design) 문서	변경된 요구사항 제정

1) 레이블(Labels)

TCSEC의 레이블 요구조건은 전부가 데이타베이스 관리 시스템에 적용될 수 있다. TCSEC의 레이블 요구조건과 DBMS의 레이블 요구조건과의 기본적인 차이점은 레이블이 어떻게 처리되는가라는 문제가 아니고 어떠한 저장객체에 레이블을 붙이는가 하는 문제이다. B1 평가등급에서 시작하여 상위등급으로 안전한 데이타베이스 관리 시스템은 모든 저장 객체에 제어하기 위한 레이블을 연관 시키는데 보호해야 할 저장 객체의 단위(granularity)는 DBMS 설계자에 의해 선택될 수 있다.

TCB(Trusted Computing Base) 경계에서 보여질 수 있는 저장된 뷰(view) 정의들은 반드시 레이블이 붙은 객체로 저장되어야 한다. TCB는 뷰 정의와 뷰 객체(instantiation)에 대한 엑세스를 제어해야 한다. TCB 설계자와 평가자는 명시적으로 레이블된 객체와

묵시적으로 레이블된 객체를 구분할 수 있으며 그러한 구분은 TCB의 한계(confines) 내에서만 의미가 있다.

데이타베이스 관리 시스템의 경우 화일, 레코드, 릴레이션 그리고 튜플과 같이 데이타베이스의 기본 데이타를 저장하는 객체와 디렉토리, 인덱스, 스키마, 데이타 사전, 트랜잭션 로그등과 같은 메타데이타(metadata)를 저장하는 객체는 반드시 레이블을 붙여야 한다. 레이블이 필요없는 객체에는 프린터 데몬(daemon), 자원 할당 테이블과 같은 사용자에게 보여지지 않는 내부자원이 포함된다.

2) 감사(Audit)

TCSEC의 감사 요구조건도 데이타베이스 관리 시스템에서 적용될 수 있다. TCB는 mandatory 보안정책과 discretionary 보안정책에 의해 보호되는 객체에 대한 모든 엑세스 기도를 감사 기록 유지할 수 있어야 한다. TCB 내부에 국한된 감사 연산(audit operation)은 필요하지 않으나 운영체제나 데이타베이스 관리 시스템에 의해 보안 감사기록이 별도로 각각 유지될 수도 있다. 운영체제의 감사기록과 데이타베이스 관리 시스템의 감사기록간의 상관분석은 항상 이루어질 수 있어야 한다. 이러한 감사기준의 초점은 사용자의 작동에 대한 개별적인 기록성을 제공하는 것으로 이 목표는 백업이나 복구기록(recovery log)의 경우와는 같지 않다. 백업이나 복구기록과의 통합된 기록을 유지하는 것은 금지되어 있지는 않으나 요구사항에는 포함되어 있지 않다.

3) 시스템 구조

TCSEC의 시스템 구조 요구조건도 데이타베이스 관리 시스템에 적용될 수 있다. 이러한 해석은 DBMS 평가가 때때로 복수의 TCB 부분집합(subsets) 들을 포함하기 때문에 부분적인 평가에 적용될 수 있는, 일반적으로 해석된 요구사항의 복수(duplication)를 제공하고 있다.

4) 설계 사양과 검증

TCSEC의 설계 사양(design specification)과 검증(verification) 요구조건은 관계된 문서화 요구조건과 함께 데이타베이스 관리 시스템에 적용될 수 있다. 데이타베이스 환경에서 주체(subject)와 객체(object)에 대한 집합은 안전한 운영체제 환경에서 보다 훨씬 크게 형성된다. 데이타베이스 시스템은 안전한 운영체제를 기반으로 하여 구축되기 때문에 TCB 부분집합에 대한 주체들의 집합으로 운영체제에 의해서 생성되는 활동적인 개체(active entities)와 DBMS의 안전한 부분에 의해서 생성되는 활동적인 개체가 포함될 수 있다. 객체들에 대한 후보들의 집합은 매우 크게 형성 되는데 예를 들어 화일(files), 세그먼트(segment), 버퍼(buffers), 페이지(pages), 관계(relations), 테이블(table), 튜플(tuples), 행(rows), 열(columns), 원소(elements), 개체(entities), 관계성(relationship), 프로시쥬어(procedures), 메타데이타(metadata), 질의어트리(query tress), 록킹 메카니즘(locking mechanism), 복귀 메카니즘(rollback mechanisms), 인덱스 (indices), 뷰정의(view definition), 뷰 객체(view instantiation), 인증 테이블(authorization tables), 데이타 사전 테이블(data dictionary tables), 그리고 감사기록(audit logs), 등이 있다.

여러개의 TCB 부분집합으로 구성되는 TCB 경우의 보안정책에서 구현으로의 사상(mapping)에 관한 TCSEC 요구조건은 다음 3가지 문제를 포함하고 있다.

- TCB 부분집합에 대한 보안 정책의 할당 (allocation)
- 전체 보안 정책을 위한 각각의 TCB 부분집합에 대한 모델들의 관계
- 전체 보안정책을 위한 각각의 TCB 부분집합의 최상위 사양(top level specification)들의 관계

이러한 문제는 첫번째로 전체 시스템의 보안정책을 각각의 TCB 부분집합으로 정확히 구분하여 할당하고, 둘째는 각각의 TCB 부분집합의 보안정책을 나타내는 모델들의 집합이 전체 시스템에서 요구되는 보안정책을 표현할 수 있어야 한다는 문제이며, 셋째로 각각의 TCB 부분집합에 대한 최상위 사양의 집합이 예외(exception), 오류(errors), 그리고 효과(effects) 측면에서 복합적인 TCB 인터페이스를 구성하는 방법의 문제로서 전체 시스템의 최상위

사양을 만족해야 하는 문제이다.

한편 각각의 TCB 부분집합에 대한 보안정책에서 구현으로의 사상(mapping)은 단일의 TCB를 구현하는 기법을 동일하게 적용할 수 있다. 각각의 TCB 부분집합에 대해 설계자와 평가자는 보안정책, 모델 그리고 사양이 TCSEC 요구조건을 만족함을 명시적으로 보여야 하며 나아가 TCB 부분집합의 모임들이 어떻게 복합적인 TCB의 보안정책을 구현할 수 있는지에 대한 비공식적인 언급이 있어야 한다. 이와 같은 보안정책에서 구현으로의 사상과정을 도식화하면 그림 1과 같다.

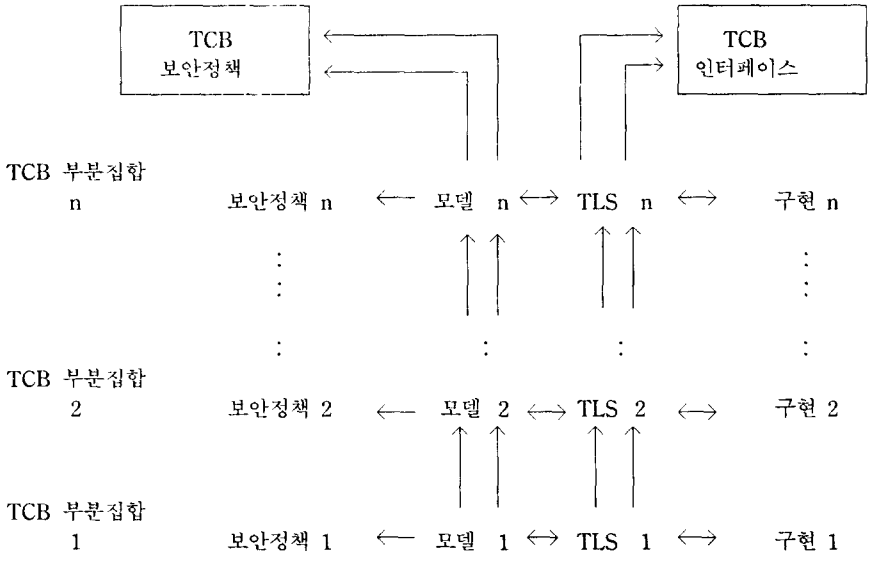

표 1. TCB 부분집합 구현

즉 각각의 TCB 부분집합에 대해 보안정책이 할당되어 명시되고 이를 구현하는데 소요되는 보안모델이 개발되고 유지되어(사용되어) 보안정책을 실현하는데 충분하다는것을 보인 다음 최상위 사양(TLS)를 제정하여 보안모델과 실제 TCB 구현이 일치함을 보여야 한다.

5) 설계 문서화

TCSEC의 설계 문서화(design documentation) 요구조건도 데이타베이스 관리 시스템에 적용될 수 있다. 이러한 해석은 DBMS 평가가 때때로 복수의 TCB 부분집합들을 포함하기 때문에 부분적인 평가에 적용될 수 있는, 일반적으로 해석된 요구사항의 복수(duplication)를 제공하고 있다.

3.2. 일반적 보안 요구사항

데이타베이스 시스템의 보안 요구사항은 운영체제의 보안 요구사항과 비교할 때 기본적인 수준에서 동일한 내용을 포함하고 있으며 다음과 같이 분류할 수 있다. 즉 외부적인 재해나 공격으로부터 데이타베이스의 값이 보호되고 유지되어야 하는 데이타베이스 무결성, 각 원소에 포함되어 있는 데이타가 정확해야 하는 원소 무결성, 모든 엑세스 기록을 유지하여 추적할 수 있어야 하는 엑세스 제어, 모든 사용자는 정확하게 식별되어야 하는 사용자 인증, 그리고 적법한 사용자는 항상 데이타베이스를 엑세스할 수 있어야 하는 가용성의 요구사항이 있다.

1) 데이타베이스의 무결성(integrity)

사용자는 데이타 값의 정확도를 신뢰할 수 있어야 하는데 이를 위해 데이타베이스 수정(update)이 적법한 인가자에 의해서만 이루어진다는 것을 보증해야

한다. 또한 데이타는 외부의 불법적인 프로그램 작동이나 화재, 전원고장등의 물리적인 재해로 인한 훼손으로부터 보호되어야 한다. 데이타베이스의 무결성에 영향을 주는 상황을 다음 2가지 경우로 분류할 수 있다.

- 전체 데이타베이스가 손상을 입은 경우
- 각각의 데이타 항목(data item)을 읽을 수 없는 경우

운영체제의 관점에서 보면 데이타베이스는 화일이고 DBMS는 프로그램이다. 따라서 데이타베이스 전체에 대한 한가지 보호방법은 시스템의 모든 화일에 대한 정기적인 백업(backup) 복사를 유지하는 것이다.

2) 원소 무결성(Element integrity)

데이타베이스의 원소 무결성은 원소의 정확성(accuracy)을 의미한다. 궁극적으로 권한을 부여받은 사용자가 데이타베이스에 정확한 데이타를 입력하는 책임을지고 있다. 그러나 사용자는 데이타를 수집하거나, 결과를 계산하거나, 값을 입력하면서 실수를 범할 수 있다. 따라서 DBMS는 사용자가 틀린 값을 입력할 때는 이를 경고해 주고, 틀린 값이 입력된 후에는 이를 수정할 수 있도록 도움을 주는 기능을 포함해야 한다. DBMS는 데이타베이스의 각 항목의 무결성을 유지하기 위해 필드 체크(field check)를 수행한다. 필드 체크는 해당 위치의 적절한 값에 대한 검사(test)로서 숫자(numeric), 대문자, 허용문자집합등의 확인을 하여 데이타가 입력될 때 간단한 오류를 방지해 준다.

3) 감사성(Auditability)

데이타베이스에 대한 모든 엑세스(판독 및 기록)의 감사기록을 유지하는 것이 바람직하다. 이러한 감사기록은 데이타베이스의 무결성을 유지하는데 도움을 주며 적어도 데이타 값에 어떤 변화가 언제 있었느지를 발견할 수 있게 해 준다. 감사성의 가장 중요한 문제중의 하나는 감사대상이 되는 단위(granularity)이다. 운영체제의 감사대상은 화일(open file) 또는 프로시쥬어(call procedure)이나 레코드 기록이나 명령어의 실행과 같이 구체적인 사건이 될 수 없다. 데이타베이스의 감사기록이 실용적이기 위해서는 레코드(record), 필드(field), 원소(element) 수준의 모든 엑세스를 포함해야 한다. 나아가 이러한 감사기록은 일반 사용자로부터 그 엑세스가 제한적이어야 한다.

4) 엑세스 제어(Access control)

데이타베이스는 흔히 사용자 엑세스 권한(access privilege)에 의해 논리적으로 분리된다. 데이타베이스는 물리적인 데이타의 저장과 관리를 중앙 집중식으로 처리할 수 있기 때문에 유용하다. 따라서 제한된 엑세스는 이러한 중앙 집중화의 책임이며 권한이다. 데이타베이스 관리자는 누가 어떤 데이타를 필드, 레코드, 원소 수준에서 엑세스 할 수 있는가를 규정해야 한다. 엑세스의 권한 모드는 다양하게 정의될 수 있다. 사용자나 프로그램은 어떤 값을 추가, 삭제, 변경 또는 판독을 할 수 있는 권한을 갖거나, 전체 필드나 레코드를 삽입, 삭제할 수 있는 권한을 갖거나 또는 전체 데이타베이스를 처리(재구성)할 수 있는 권한을 갖을 수 있다.

5) 사용자 인증(User authentication)

모든 사용자는 감사기록과 데이타에 대한 엑세스 허가를 위해 정확하게 식별되어야 한다. 일반적으로 DBMS는 운영체제 위에서 수행되고 있는 응용프로그램이므로 운영체제와의 안전한 통로(trusted path)를 갖고 있지 못하다. 따라서 사용자 인증정보를 포함하여 DBMS가 받는 모든 정보는 의심의 대상이 되며 DBMS는 별도로 사용자 인증을 수행해야 한다.

6) 가용성(Availability)

DBMS는 프로그램과 시스템의 양쪽 측면을 갖고 있다. DBMS는 다른 하드웨어와 소프트웨어 자원을 사용하는 시스템이며 많은 사용자에게는 응용프로그램이기도 하기 때문에 매우 높은 수준의 가용성 요구조건을 필요로 한다. 사용자는 일반적으로 엑세스 권한을 부여받은 데이타베이스를 엑세스할 수 있어야 한다. 두명의 사용자가 동시에 같은 레코드를 엑세스 했을 때 이를 중지해야 하며 비밀 데이타를

보호하기 위해 보호될 필요성이 없는 데이타의 엑세스를 제한하는 문제를 해결해야 한다.

4. 결 론

본고에서는 비밀정보를 적절하게 보호할 수 있는 대책이 요구되고 있는 데이타베이스 시스템의 보안 평가 기준을 살펴보기 위해 먼저 컴퓨터 보안 평가의 주도적 역할을 하고 있는 미국 NCSC의 컴퓨터 보안평가 지침서인 TCSEC인 보안 요구사항과 평가 등급 내용을 살펴보고, 이 기준을 데이타베이스 시스템에 적응하기 위한 TDI를 분석하여 일반적인 데이타베이스 시스템의 보안 요구사항을 제시하였다. 컴퓨터 보안에 대한 국내의 요구가 급증하고 있는 현재 컴퓨터 시스템을 보안측면에서 분류하고 평가할 수 있는 국가 표준을 제정하고 이를 바탕으로 데이타베이스 시스템의 보안 평가 기준을 제정하는 것은 시급한 과제이다. 일반적인 데이타베이스 보안 요구사항에는 데이타 값이 보호되고 그 구조가 유지되어야 하는 데이타 무결성, 각 원소에 포함되어 있는 데이타가 정확해야 하는 원소 무결성, 모든 엑세스 기록을 유지하여 추적할 수 있어야 하는 감사성, 모든 사용자는 정확하게 식별되어야 하는 사용자 인증, 그리고 적법한 사용자는 항상 데이타베이스를 엑세스할 수 있어야 하는 가용성의 요구사항이 있다.

참 고 문 헌

1. Abrams M.D. and G.W. Smith, "A General Framework for Database Access Control", Database Security iv : Status and Prospects, IFIP, 1991, pp.171-178.

2. DoD, Trusted Computer System Evaluation Criteria, DoD 5200.28 STD, Dec. 1985.

3. Lewis S.R., "The Front End Approach to Database Security", Information Security, IFIP, 1991, pp.449-460.

4. NCSC, Trusted Database Management System Interpretation of the TCSEC, NCSC-TG-021 Version 1, Aprill 1991.

5. Pfleegr C.P., Security in Computing, Prentice-Hall, 1989.

6. Wiseman S., "Audit Control in Databases", Information Security, IFIP, 1991, pp.99-110.

□ 著者紹介

申 壯 均(종신회원)

1974년 육군사관학교 졸업
1979년 서울대 산업공학과 졸업
1983년 미 Wisconsin대(전산학 석사)
1989년 고려대 대학원(전산학 박사)

현재 : 육군사관학교 부교수
관심분야 : 운영체제 보안, 분산 시스템