通信情報保護學會誌
第8卷 第2號, 1998. 6

DBMS 보안 기술 동향

오 경 희*, 구 자 동*, 홍 기 웅*

요 약

중요한 정보가 컴퓨터를 통하여 저장·처리되면서 이들을 안전하게 유지·관리하여야 할 필요성이 크게 부각되고 있다. 본 고에서는 다양한 정보를 안전하게 유지·관리하기 위한 보안 모델을 소개하고 이를 기반으로 안전한 DBMS의 설계를 위한 커널 구조, 중복 구조, 분산 구조 등의 구축 기술과 상용 DBMS 보안제품의 평가 동향을 소개하고자 한다.

1. 서 론

여러 분야의 다양한 요구에 따른 데이터베이스의 발달과 더불어 개인정보의 보호 및 기밀문서 관리의 문제가 중요시되자, 데이터 보안에 대한 새로운 인식과 필요성이 대두되었다. 이에 따라 1970년대부터 데이터 보안을 위해 안전한 DBMS 구축 및 트랜잭션 처리방법에 대한 많은 연구가 진행되었고 이러한 연구의 결과로 1980년대 중반부터 상용 DBMS 보안제품이 나오게 되었다. 또한 1991년에는 미국의 국방성에서 안전한 DBMS의 평가를 위한 TCSEC의 해석[1]을 발표하였으며 유럽에서도 ITSEC[2]에 따라 DBMS 보안제품을 평가하는 등 현재는 많은 상용 DBMS 보안제품이 평가되어 각국의 평가된 제품목록에 등재되어 있다.

본 고에서는 DBMS 보안의 기술동향에 대해 살펴보고자 한다.

*한국정보보호센터

2. DBMS 보안에서 사용되는 보안 모델

데이터 보안에 관한 연구가 계속되면서 다양한 방법들이 제시되었는데, 이 중 사용자와 데이터에 비밀등급을 두어 기밀정보의 보안을 유지하는 다단계 보안 시스템(Multilevel secure system, MLS)이 제시되었고 현재 가장 널리 사용되고 있다. 다단계 보안 시스템은 사용자를 위한 하나 이상의 보안 등급(security clearance level)과 시스템 내의 데이터를 위한 하나 이상의 분류 등급(classification level)을 가진 시스템을 말하며 이러한 등급을 이용하여 기밀정보의 노출을 제어하는 방법을 제공한다.

다단계 안전한 데이터베이스 관리시스템(MLS/DBMS)은 이러한 다단계 보안 시스템의 접근통제를 데이터베이스 관리시스템에 적용한 것이다. 이러한 시스템의 목적은 기밀 정보를 인가되지 않은 사용자로부터 보호하는 것이다. 이를 위해 MLS/DBMS에서는 통제하

는 모든 데이터 항목에 대해 고유한 등급을 가져야 하며, 사용자가 데이터에 접근하는 것은 사용자의 인가등급과 데이터의 보안 등급에 의해 통제되도록 하고 있다.

사용자의 데이터 접근을 통제하기 위한 접근통제방법으로는 강제적 접근통제방법(Mandatory Access Control, MAC)과 임의적 접근통제방법(Discretionary Access Control, DAC)으로 나누어 볼 수 있다. 이러한 접근통제방법을 기반으로 하여 실제 구현을 위한 보안모델을 연구하기 시작하였다. 이러한 보안모델은 시스템이 원하는 보안 요구사항에서 특정 소프트웨어에 국한되지 않는 상위수준의 개념모델 구축을 가능하게 만들었다. 1978년부터 많은 보안모델이 연구되었는데, 크게 두가지로 나누어보면, 임의적 보안모델(Discretionary security model)과 강제적 보안모델(Mandatory security model)로 나누어볼 수 있다. [표 1]은 대표적인 보안모델의 특성을 표로 정리한 것이다.[3]

표 1. 보안모델의 특성

	임의적 정책	강제적정책		간접접근 또는 정보흐름통제	접근통제
		비밀성	무결성		
Bell-LaPadula	◎	◎		◎	◎
Biba	◎		◎	◎	◎
Dion		◎	◎	◎	◎
Sea View		◎	◎	◎	◎
Jajodia-Sandhu	◎	◎		◎	◎

데이터의 비밀성에 중점을 둔 대표적인 보안모델로는 BLP 모델을 들 수 있고, 데이터의 무결성에 중점을 둔 보안모델로는 비바모델을 들 수 있다. 또한 현재 초고속 전산망 정보보호 기술로서 SRI의 Seaview DBMS 정보보호 모델이 주목받고 있으며 Secure ORACLE 등으로 제품화되고 있다. DB를 관리하는 DBMS에 대한 정보보호 기술은 DBMS가 컴퓨터 운영체제와 유사한 독립된 응용 운영체제이므로 DBMS의 특성을 고려한 별도의 정보보호 기술로써 연구되고 있다.

3. 안전한 DBMS의 구조

다양한 보안모델을 사용하여 안전한 DBMS를 구축할 수 있는데, 구조상으로 크게 세 분야로 나눌 수 있으며, 각 분야별로 많은 연구가 이루어지고 있다. 안전한 DBMS를 구조별로 나누어보면 다음과 같다.

3.1 커널구조

커널구조(Kernelized Architecture)에 관한 연구는 1974년부터 시작하여 현재까지 계속되고 있다. 커널구조는 서로 다른 보안등급간에 자원을 공유하기 위해 연구가 시작되었으며, 자원공유면에서는 DBMS 구조중에서 가장 쉽게 구축할 수 있으므로 많은 연구가 진행되었다.[4] 1983년 Air Force Studies Boards에서 커널구조를 구축하면서부터 연구가 활발해졌다.

커널 구조는 자원을 공유함으로써 시스템 효율면에서 많은 향상을 가져올 수 있으나 이로 인해 상위등급 사용자의 보안유지면에서 많은 어려움을 가지게 된다. 다음은 커널구조를 그림으로 나타낸 것이다

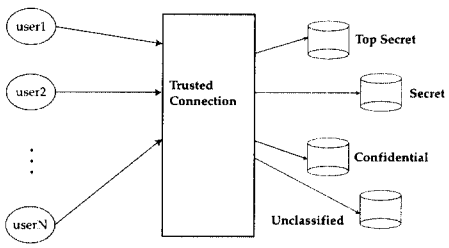


그림 1. 커널구조

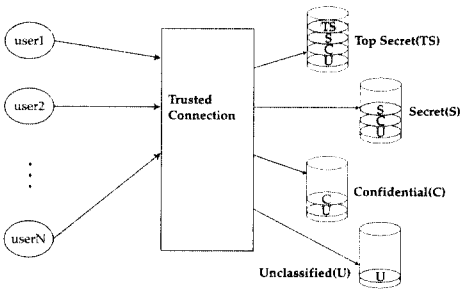


그림 2. 중복구조

중복구조(Replicated Architecture)는 1983년부터 연구가 시작되어 현재까지 많은 논문이 발표되면서 활발한 연구가 진행 중에 있다. 중복구조를 연구하게 된 배경은 기존의 데이터베이스를 변형없이 그대로 사용하고자 하는데 있다. 그러기 위해 기존의 보안개념이 없는 데이터베이스에 TCB(Trusted Computing Base)를 붙임으로서 보안기능을 제어하게 된다.

중복구조의 장점은 하위등급 데이터의 내용을 상위등급 사용자가 복사본을 통해 모니터하게 되므로 하위등급 작업에 아무런 영향을 미치지 못한다는데 있으나 이러한 복사본을 유지하기 위한 노력이 단점으로 작용한다. 1993년 미국 해군 연구소(Naval Research Laboratory)에서는 'SINTRA'라고 명명한 중복구조를 이용한 안전한 DBMS 프로토타입을 발표하였고 이후 SINTRA의 성능평가 및 향상을 위한 연구가 계속 진행중이며, SINTRA를 이용한 추가적인 개발에 노력중이다.[5][6] SINTRA 구축시 상용 DBMS로는 Oracle을 사용하였고 기존의 여러 알고리즘을 사용한 성능분석은 이미 학계에 발표된 바 있다.

다음은 중복구조를 그림으로 간단히 나타낸 것이다.

3.3 분산구조(Distributed Architecture)

네트워크가 점점 발달함에 따라 DBMS 또한 중앙집중환경에서 분산환경으로 바뀌는 추세이다. 분산 데이터베이스 시스템 설계 및 트랜잭션 처리에 관한 연구는 일찍 시작되어 현재 많은 분야에서 활발히 연구가 진행되고 있으나 분산 환경하에서의 보안 데이터베이스 관리시스템 구축 및 트랜잭션 처리방법에 관한 연구는 '90년대에 들어오면서 시작되었다. 1993년 Jajodia와 McCollum으로 시작하여 분산 보안 데이터베이스 관리시스템상에서 트랜잭션 처리방법에 관한 연구가 시작되었다.[4] 현재 많은 연구가 진행된 것은 아니나 앞으로의 발전전망을 볼 때 가장 중요한 분야가 될 것이다. 다음은 분산 데이터베이스 시스템을 그림으로 간단히 도식화한 것이다.

4. 각국의 평가된 제품 현황

상용의 DBMS 보안제품이 출시되기 시작하자 이미 안전한 컴퓨터시스템에 대한 평가를 진행중이던 미국에서는 TCSEC을 DBMS에 맞게 해석한 기준인 TDI(Trusted DBMS Interpretation of TCSEC)[1]를 개발하여 이에 따라 현재까지 DBMS 보안제품을 평가하고 있으며 유럽은 유럽 4개국의 공통기준인 ITSEC[2]

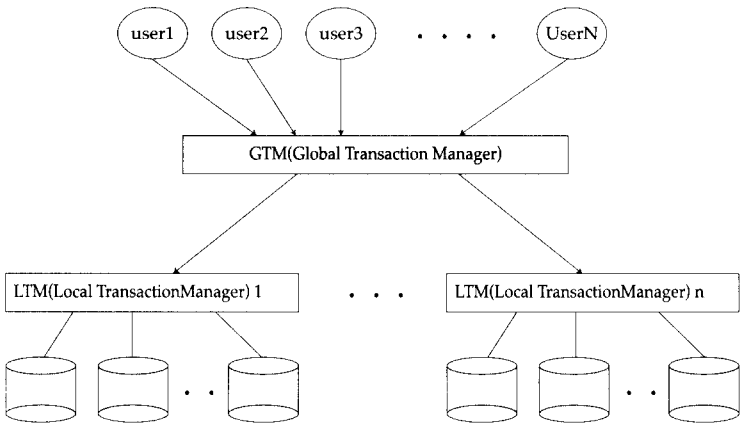


그림 3. 분산구조

에 기반하여 DBMS 보안제품을 포함한 각종의 보안제품을 평가하고 있다.

각국의 평가목록을 살펴보면 DBMS 분야를 포함하고 있는 경우는 매우 드물며 현재 사용되고 있는 DBMS 제품중 평가를 받은 제품은 몇몇에 불과하다. 미국의 TDI와 영국의 ITSEC으로 몇몇 DBMS 제품을 평가하고 있는 것을 볼 수 있으며 프랑스나 독일 등 유럽지역에서 평가된 DBMS 제품은 아직 없다. 미국과 영국에서 평가된 상용 DBMS 제품은 [표 2][표 3]과 같다.[7]

5. 결 론

현재 안전한 DBMS 기술은 기존의 DBMS에 보안기능만을 추가하는 방향으로 발전하였기 때문에 기존의 기술과 보안기능과의 충돌로 인해 발생되는 많은 문제들을 해결하기 위해 노력해왔다. 데이터 보안모델, 트랜잭션 처리, 다양한 환경에서의 안전한 DBMS 구축 등에서는 꾸준한 발전이 있었고 상용 DBMS에도 많이 반영되었다. 현재 연구가 미비한 분야는 다단계 보안 데이터베이스 시스템의 성능향상과

표 2. 미국의 안전한 DBMS 제품 평가목록

제품명	등급	업체명	날짜
INFORMIX-OnLine/Secure 4.1	B1	Informix Software, Incorporated	'94.3.21
INFORMIX-OnLine/Secure 5.0	B1	Informix Software, Incorporated	'94.11.15
Trusted Oracle7	B1	Oracle Corporation	'94.4.5
Secure SQL Server Version 11.0.6	B1	Sybase, Inc.	'97.1.7
INFORMIX-OnLine/Secure 4.1	C2	Informix Software, Incorporated	'94.11.15
INFORMIX-OnLine/Secure 5.0	C2	Informix Software, Incorporated	'94.11.15
Trusted Oracle7	C2	Oracle Corporation	'94.4.5
Secure SQL Server Version 11.0.6	C2	Sybase, Inc.	'97.1.7

표 3. 영국의 안전한 DBMS 제품 평가목록

제품명	등급	업체명	날 짜
Informix Online/Secure B1 and C2 version 5.0	E3	Informix Software Ltd	'95.4
Oracle 7 and Trusted Oracle 7 Release 7.0.13.6	E3	Oracle Corporation	'95. 9

시스템 회복시 발생하는 보안문제 해결, 데이터베이스의 무결성 분야, 분산 안전한 DBMS 상의 트랜잭션 처리방법 등이다.[4]

성능향상면에서는 Seaview 모델의 경우, 관계의 수직 혹은 수평분할을 허용하고 있으나, 다단계 관계일 경우 단일 관계에 비해 오버헤드가 너무 크다는 지적과 함께 1991년 Jojodia와 Sandhu가 새로운 분할법을 제시하면서 현재 계속 연구가 진행되고 있는 중이다.[8] 시스템 회복시 보안문제는 1992년부터 관심을 가지기 시작하여 아직 미비한 수준에 있으며, 연구된 부분이 매우 적다. 분산 안전한 DBMS 상에서의 트랜잭션 처리방법에 관해서는 일찍이 논의된 바 있으나, 현재 기술수준은 아직 미비하다.

또한 1997년 IFIP WG11.3 Workshop on Database Security 패널과 IEEE Symposium on Security and Privacy 에서는 의사결정 지원을 위한 방대한 데이터 처리를 위해 기존의 관계형 데이터베이스에서 관계형-객체 데이터베이스나 객체 지향 데이터베이스로의 이전이 이루어지고 있는 가운데 중요하게 부각되고 있는 분야인 데이터웨어 하우징과 데이터마이닝 분야에서의 보안문제가 큰 주제로 다루어졌고, 앞으로 활발히 연구될 전망이다.

참 고 문 헌

[1] National Computer Security Center, *Trusted DataBase Management System Interpretation of the TCSEC*, NCSC-TG-02, Apr., 1991.

[2] Harmonised Criteria of France, Germany, the Netherlands, and the United Kingdom, *Information Technology Security Evaluation Criteria(ITSEC)*, June 1991, Version 1.2 (Provisional).

[3] S. Castano, M. Fugini, P. Samarati, *Database Security*, 1994.

[4] S. Jajodia, T. F. Thomas, R. Mukkamala, " Multilevel Secure Transaction Processing : Status and Prospects", IFIP WG11.3 Workshop in Database Security, 1996.

[5] R. Mukkamala, M. H. Kang, J. H. Froscher, "Architectural Impact on Performance of a Multilevel Database System," Proceedings of the tenth Annual Computer Security Applications, 1994.

[6] M. H. Kang, J. N. Frocher, J. McDermott, " Achieving Database Security through Data Replication : The SINTRA prototype," Proceedings of the 17th National Computer Security Conference, 1994.

[7] http://www.radium.ncsc.mil/tpep/epl/

[8] T. Lunt, "The SeaView security model," IEEE Transactions on Software Engineering, 1990.

□ 著者紹介

오 경 희

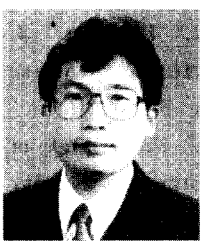
1988년 2월 서강대학교 전자계산학과(학사)
1992년 2월 한국과학기술원 전자계산학과(석사)
1995년 11월 CISA
1992년 10월 - 1996년 12월 한국통신 멀티미디어연구소 전임연구원
1996년 12월 - 현재 한국정보보호센터 주임연구원

※ 주관심분야 : 정보보호시스템 평가체계, 정보시스템 감사, 위험분석 및 관리

구 자 동

1996년 2월 아주대학교 컴퓨터공학과(학사)
1998년 2월 아주대학교 대학원 컴퓨터(석사)
1998년 3월 - 1998년 7월 삼성전자 정보통신 개발센타
1998년 7월 - 현재 한국정보보호센터 연구원

※ 주관심분야 : 정보보호시스템 평가체계, 이동통신 보안, 침입탐지시스템



홍 기 웅

1985년 2월 전남대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산과(석사)
1994년 4월 정보처리기술사
1996년 2월 아주대학교 컴퓨터공학과(박사)
1985년 9월 - 1995년 10월 한국전자통신연구소 선임연구원
1992년 - 1993년 이태리, Alenia Spazio사 Senior Researcher
1995년 10월 - 1996년 4월 한국전산원 선임연구원
1996년 4월 - 현재 한국정보보호센터 책임연구원, 평가체계팀장/기술표준팀장

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보시스템 위험분석 · 평가, 정보보호 표준화