다등급 보안 자료기지 체계에서 접근 제어를 위한 질의 제한 기법

주 영 중　　문 송 천
한국과학기술원 정보및통신공학과

QUERY RESTRICTION SCHEME FOR ACCESS CONTROL IN MULTILEVEL SECURE DATABASE SYSTEMS

Young- Joong Joo　　Song-Cheon Moon
Department of Information and Communication Engineering , KAIST

요약 다등급 보안 자료기지 체계에서는 보안성과 더불어 가용성을 보장해 주어야 한다. 본 논문에서는 보안 메커니즘인 전위 프로세스가 고수준의 보안성을 유지하면서 동시에 가용성을 최대한 보장해 줄 수 있도록 하는 질의 제한 기법을 제안하고자 한다. 기존의 접근제어가 질의에 대한 최종 응답의 유무에 관계없이 질의를 획일적으로 처리함으로써 응답 대기시간의 지연을 가져오는 반면 제안한 질의 제한 기법은 최종 응답이 존재하지 않는 질의를 선별하여 원천적으로 그 처리를 거부하도록 한다. 또한 최종응답이 존재한다해도 자료기지의 모든 자료를 판독할 수 있는 사용자인 경우에는 상향판독 불가 원칙을 점검하는 응답여과를 생략하도록 한다. 이러한 질의거부와 여과생략을 통해 신 접근제어 정책은 자료기지 관리체계의 질의처리에 따른 시공간적인 부담을 최대한으로 줄임으로써 응답 대기 시간을 단축시키고 다수 사용자가 공유해야 하는 제한된 시스템 자원을 최종 응답을 갖지 않는 사용자의 질의 처리에 할당하지 않음으로써 가용성을 향상시키게 되는 것이다.

1. 서 론

자료기지 체계에서 불법적 정보 유출을 막기 위해서는 자료에 대한 접근 시도가 적법한지를 검증할 수 있는 접근 제어가 우선적으로 요구된다. 이러한 접근제어는 질의를 통해 자료기지에 접근하고자 할 때마다 활성화되어 사용자가 판독/기록 가능한 자료에만 접근하도록 제한한다. 기본적인 자료기지 관리체계의 질의처리 시간과 더불어 이와 같은 접근 요구의 적법성을 검증하기 위한 시간을 부가적으로 소요하기 때문에 접근 제어는 응답 대기 시간의 지연을 가져온다. 또한 다수의 사용자가 공유하고자 하는 제한된 시스템 공간상에서 사용자가 요구한 자료에 대하여 접근 권한 여부를 검증하기 위해 별도의 작업 공간을 필요로 하게 되는 것이다.

접근 제어를 위한 추가적인 시간 소요와 공간 확보에 따른 응답 대기 시간의 지연에도 불구하고 접근 제어에 대한 대부분의 선행 연구는 보안성만을 강조하는데 초점을 맞추어 왔다. 특히 군사환경에서 사용되어온 강제적 접근제어(mandatory access control: MAC)[1] 정책을 도입함으로써 고수준의 보안성을 유지하려는 시도가 무결성 잠금[2], 최대 권한 뷰[3], 상호 여과기[4]등에서 이루어졌다. 이들은 모두 사용자와 자료기지 관리체계 사이에 위치하는 전위 프로세스라는 보안 메커니즘을 채택하고 있다. 전위 프로세스는 기존 시스템의 변화를 최소화하자는 간결성을 목적으로 기존의 운영체계나 자료기지 관리체계를 변화시키지 않고 프로세스 단위의 접근 제어 모듈을 이용하여 고수준의 보안성을 유지하고자 한다. 또한 기본적으로 하드웨어에 의존하지 않는 소프트웨어를 이용한 구현 형태를 갖도록 설계되었기 때문에 보안 컴파일러[5], 보안 운영체계[6], 보안 자료기지 관리체계[7]등의 보안 메카니즘에 비해 보안성 검증과 관리가 용이하며 이식성이 높다.

이상의 장점에도 불구하고 전위 프로세스는 다른 보안 메커니즘과 마찬가지로 보안성에만 초점을 맞추었기 때문에 접근 제어시의 시공간적 부담으로 인해 사용자의 가용성 저하를 막지 못하고 있다. 따라서 본 논문에서는 전위 프로세스의 접근 제어 모형을 재설계하여

가용성을 향상시키기 위한 질의 제한 기법을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 제 2장은 관련연구로서 전위 프로세스의 문제점을 기술하고 제 3장은 접근 제어 모형을 보여준다. 그리고 제 4장은 질의 여과의 개념을 제시하고자 한다. 제 5장은 결론으로 끝맺는다.

2. 관련 연구

전위 프로세스는 기본적으로 벨/라파듈라 모형[8]의 하향 기록 불가/상향판독 불가 원칙에 따라 접근제어가 이루어진다. 즉, 사용자의 비밀취급 인가등급이 자료의 비밀등급보다 높은 경우에는 기록 접근이 허용되지 않으며, 낮은 경우에는 판독 접근이 허용되지 않는다. 하향 기록 불가 원칙은 자료 입력시에 적용되며 사용자에게 돌려줄 응답이 없기 때문에 질의 수행과 동시에 접근 제어가 완료된다.

이에 반해 상향 판독 불가 원칙은 전위 프로세스가 자료기지 관리체계의 질의 처리 결과를 사용자에게 돌려주기 전에 이를 여과할 때 적용된다. 그러므로 자료 판독을 요구하는 사용자의 질의는 자료기지 관리체계로 무조건 전달되어 처리되어야만 하는 것이다. 다음 예 1을 통해 무조건적 질의 전달로 인한 사용자 응답 대기 시간의 지연 부담을 살펴보기로 한다.

예1(무조건적 질의 전달로 인한 응답대기 시간의 지연)

자료의 비밀등급이 상위 등급에 편중된 자료기지에 대해 상위 등급 사용자 A와 하위 등급 사용자 B가 동시에 동일 자료를 요구하지만, B는 낮은 비밀취급 인가등급에 의해 자료기지에 판독할 수 있는 자료가 존재하지 않는다라고 가정한다(그림 1). 시간 공유 체계에서 스케줄러에 의해 각 프로세스에게 할당되는 시간 간격은 100msec, 자료기지 관리체계가 질의를 처리하는데 소요되는 시간은 200 msec, 전위 프로세스가 질의 처리 결과를 전달받아 이를 여과하고 최종적으로 사용자에게 여과된 응답을 돌려주는데 소요되는 시간은 100msec라고 가정한다. 즉 사용자의 질의 수행을 완료하는데 총 300msec의 시간이 소요된다.

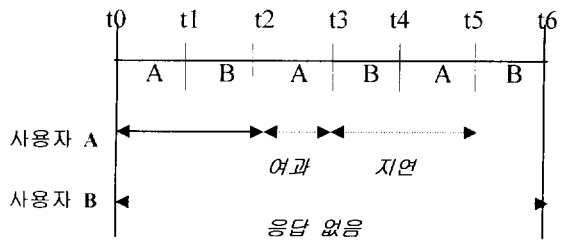

그림 1 상위등급 편중 자료기지에서의 응답 대기시간

A와 B가 스케줄러에 의해 교대로 수행됨에 따라 A의 응답 대기시간은 t0~t5(500 msec)가 소요되고 B의 응답 대기시간은 t0~t6 (600 msec)가 소요된다. 이때 전위 프로세스는 최종 응답이 존재하지 않는 B의 질의 수행 요구를 거부할 수 없기 때문에 B에게 A와 동일한 접근 제어를 적용해야만 한다. 결국 A는 B로 인해 t3에 돌려받을 수 있는 응답을 *지연*(200msec)만큼 지연된 t5에 돌려받게 된다. 게다가 A는 자료기지의 모든 자료를 판독할 수 있음에도 불구하고 전위 프로세스의 접근제어 정책상 자료기지 관리체계의 질의 처리 결과를 여과한 최종 응답을 돌려받아야 하기 때문에 t2에 돌려받을 수 있는 응답을 *여과*(100msec)만큼 지연된 t3에 돌려받게 되는 것이다. 결국 A는 응답 대기 시간이 300 msec 나 지연된 것이다.

끝(예 1).

전위 프로세스의 획일적인 접근 제어는 시간적 부담뿐만 아니라 공간적 부담을 유발시킨다. 이는 전위 프로세스가 자료기지 관리체계의 질의 처리 결과를 여과하기 위해 자신의 임시 기억 공간으로 이들을 모두 옮겨 놓아야 하기 때문이다. 대부분의 시스템은 주기억장치가 충분히 크지 않기 때문에 이러한 전위 프로세스의 공간 점유는 페이지 부재로 인한 기억 장치간 입출력 횟수를 증가시켜 사용자 응답 대기 시간을 더욱 더 지연시키게 된다.

3. 접근 제어 모형

시스템에 보안 정책을 반영하기 위한 접근 제어 모형을 설계하기 위해 다음과 같은 가정을 두고자 한다.

① **(전위 프로세스의 신뢰성):** 접근 제어의 주체인 전위 프로세스는 보안상 신뢰할 수 있다.

② **(접근제어를 위한 폐쇄모형):** 사용자는 명시적으로 비밀취급 인가등급을 부여받아야만 자료기지의 객체에 접근할 수 있다.

③ **(다등급 자료기지의 원소 단위 조밀도):** 다등급 자료기지는 속성 값마다 비밀등급을 갖는 원소 단위의 조밀도(granularity)를 갖는다.

④ **(자료기지 관리체계의 휘발성 서비스):** 자료 기지 관리체계는 사용자 질의를 처리한 후 주기억장치의 대상 자료를 제거하도록 한다.

전위 프로세스는 작업을 관리해야 할 책임이 있으며 위치상 중개자의 역할을 해야 한다. 이러한 중개 과정에서 전위 프로세스는 보안성을 유지하면서 동시에 가용성을 보장해주어야 하는 것이다. 다음 그림 2는 이를 위해 기존의 접근 제어 모형을 재설계한 것이다.

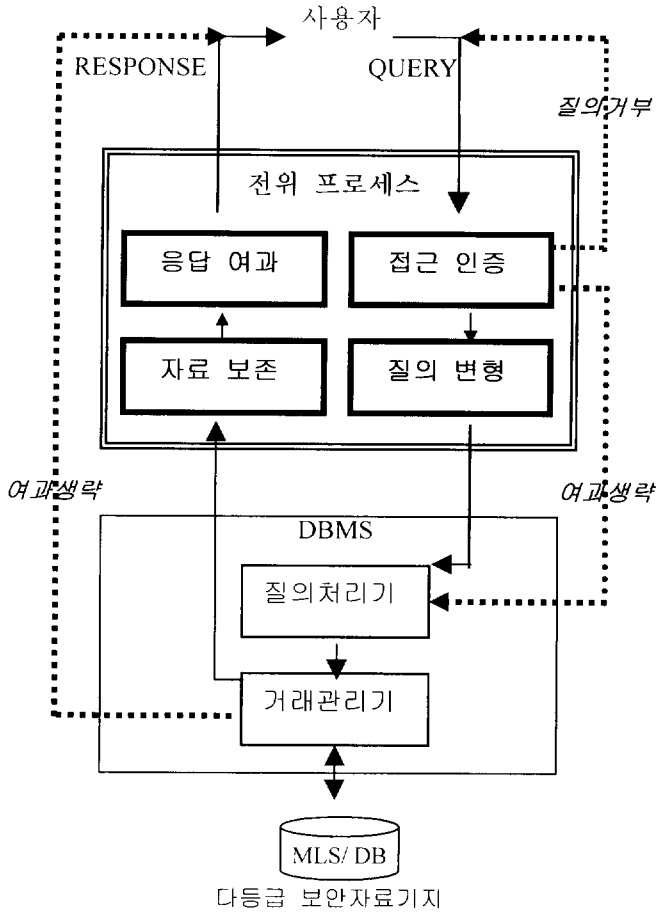

그림 2 접근 제어 모형

4. 질의 여과의 개념

사용자의 가용성을 보장해 주기 위해 전위 프로세스는 **질의 여과**의 개념을 기반으로 하는 접근제어를 수행해야 한다. 이는 다음과 같은 두가지 이유에 기인한다. 첫째, 자신의 등급보다 상위 등급의 자료를 판독하려는 사용자에게 최종 응답은 존재하지 않는다. 둘째, 질의 여과에 의해 모든 사용자의 응답 대기 시간을 단축시킬 수 있다. 이때 질의 여과란 상향 판독하려는 질의를 여과하여 자료기지 관리체계의 질의 처리 대상에서 제외시키는 것을 일컫는다.

전위 프로세스가 질의 여과의 개념을 기반으로 접근 제어를 수행하기 위해서는 자료기지의 등급 분포를 나타내는 별도의 자료구조를 필요로 한다. 본 논문에서 이를 등급 분포도 표라 칭하겠다. 전위 프로세스는 이 표를 근거로 접근 제어를 수행하게 되는 것이다.

사용자가 생성한 표 1 의 EMPLOYEE 라는 자료 릴레이션에서 성명, 부서, 급여란은 객체의 내용을 담고 있으며 $C_{성명}$, $C_{부서}$, $C_{급여}$란은 각 속성란에 입력된 객체의 비밀등급을 나타낸다. 그리고 TC 는 이들중 가장 상위 등급의 비밀등급을 나타내며 사용자가 레코드 단위의 자료를 요구할 때 사용된다.

표 1 사용자가 생성한 자료 릴레이션
EMPLOYEE

성명	$C_{성명}$	부서	$C_{부서}$	급여	$C_{급여}$	TC
박	2	전산실	3	5000	3	2
이	2	비서실	2	3000	1	1

전위 프로세스는 표 1 의 EMPLOYEE 가 생성되면 표 2 와 같은 등급 분포도 표인 EMPLOYEE_CLASS 를 생성하게 된다. 등급 분포도 표는 각 속성의 최상위 등급과 최하위 등급을 나타내는 속성_H 와 속성_L 란으로 구성되어 있으며 자료가 새로 입력되는 경우에만 그 내용이 갱신된다.

표 2 전위 프로세스가 생성한 등급분포도 표
EMPLOYEE_CLASS

성명 _H	성명 _L	부서 _H	부서 _L	급여 _H	급여 _L	TC_ H	TC_ L
2	2	2	3	1	3	1	2

또한 등급 분포도 표는 자료 릴레이션의 크기가 증가해도 각 속성의 최상위/최하위 등급 정보만을 유지하면 되기 때문에 자료 릴레이션이 N 개의 속성을 가질 경우 N+1 byte 의 고정 크기를 갖는다. 등급 분포도 표를 참조하여 접근 제어를 수행하게 되는 질의 제한 기법의 알고리즘은 다음 알고리즘 1 과 같다. 이때 등급분포도 표(Class Distribution Table)는 CDT, 사용자의 비밀취급 인가등급은 User_Clearance 로 표기하기로 한다.

알고리즘 1 질의 제한 기법의 알고리즘

```
1   Algorithm Query_Restriction_Scheme(QRS)
2   Input: Query
3   Output:prediction result; FILTER, FILTERLESS, REJECT
4           Boolean value; success, failure
5   {
6       relation_name=abstract(Query)
7       attribute_list=abstract(Query)
8       CDT=relation_name+_CLASS
9       While(all attribute_list){
10          IF(User_Clearance<CDT.attribute_L)
11              THEN result=REJECT
12          ENDIF
13      }
14      IF(result=REJECT) THEN return (failure)
15      ENDIF
```

```
16      While(all attribute_list){
17          IF(User_Clearance>CDT.attribute_H)
18              THEN result=FILTERLESS
19              ELSE {result=FILTER
20                  break
21              }
22          ENDIF
23      }
24      IF(result=FILTERLESS)
25          THEN{send_query_to_DBMS(Query)
26              pass_response_to_user(Response)
27           }
28           ELSE{ Query'=query_modification(Query)
29                send_query_to_DBMS(Query')
30                storage_response_of_DBMS(Response)
31                Response'=filter(Response)
32                pass_response_to_user(Response')
33           }
34      ENDIF
35      return(success)
36  }
```

전위 프로세스는 가장 먼저 사용자의 질의에서 자료 릴레이션의 이름과 속성 리스트를 추출해낸다. 추출해낸 자료 릴레이션의 이름에 _CLASS를 덧붙여 등급 분포도 표의 이름을 알아낸다. 그리고 모든 속성 리스트에 대하여 속성의 최하위 등급을 나타내는 속성_L 중 하나라도 사용자 비밀취급 인가등급보다 낮은 것이 있다면 원천적으로 질의처리를 거부(REJECT)하도록 한다.

전위 프로세스는 거부되지 않은 질의에 대해서 다시 여과 생략의 필요성을 판단한다. 모든 속성 리스트에 대하여 속성의 최상위 등급을 나타내는 속성_H가 사용자 비밀취급 인가등급보다 모두 낮다면 여과를 생략(FILTERLESS)하고, 그렇지 않은 경우에는 반드시 여과(FILTER)를 거치도록 한다.

후자의 경우 전위 프로세스는 여과할 때 자료의 비밀등급을 참조하기 위해 사용자의 질의에 자료의 비밀등급 요구를 추가한다. 이와 같이 변형된 질의는 자료기지 관리체계로 전달되어 처리된다. 자료기지 관리체계의 질의 처리 결과는 전위 프로세스의 임시 기억 공간에 저장되며 그 안에는 자료와 그 자료의 비밀등급이 함께 위치한다. 전위 프로세스는 최종적으로 질의 처리 결과에 대해 자료의 비밀등급을 비교하여 사용자의 비밀취급 인가등급보다 높은 등급의 자료를 여과하고 여과된 최종 결과만 사용자에게 돌려주게 되는 것이다. 이상의 질의 거부(REJECT), 여과 생략(FILTERLESS), 여과(FILTER)를 결정짓는 주체는 바로 전위 프로세스의 핵심 모듈인 접근 인증 모듈이다.

5. 결 론

다등급 보안 자료기지 체계에서는 보안성의 유지와 더불어 사용자의 가용성을 보장해 주어야 한다. 한정된 자원을 공유하려는 다수의 사용자는 최종 응답을 갖지 않는 일부 사용자에 의해 응답 대기 시간이 지연됨으로써 가용성의 저하를 감수하게 된다. 본 논문에서는 이러한 문제점을 해소하기 위해 최종 응답을 갖는 질의만 선별하여 자료기지 관리체계에 전달함으로써 가용성을 향상시키기 위한 질의 제한 기법을 제안하게 된 것이다.

이 기법을 제안하게 된 근본적인 배경은 자료기지의 자료가 항상 상위등급에서 하위등급까지 고루 분포되어 있지 않다는 사실이다. 군대와 같은 보고 위주의 환경에서 자료기지의 비밀 등급 분포는 해당 업무의 성격이나 기밀도에 따라 상위 또는 하위 등급으로 자연스럽게 편중 분포되는 경향을 보인다. 이는 군대가 조직 구성원의 비밀 자료 생산을 엄격하게 통제하기 때문이다. 이러한 성향은 상업 환경에서도 마찬가지이다. 이와 같이 편중 분포된 자료기지에 균등 분포된 자료기지를 가정한 기존의 획일적인 접근제어를 적용한다는 것은 매우 부적절하다. 따라서 본 논문에서는 질의 제한 기법을 통해 이러한 편중 성향을 반영하고자 한 것이다.

참고 문헌

[1] Department of Defense, "DoD Trusted Computer Evaluation Criteria," DoD Computer Security Center, CSC-STD-001-83, 1983.

[2] Richard Graubart, "The Integrity-Lock Approach to Secure Database Management," In Proc.of Symp. on Security and Privacy, IEEE computer society, pp. 62 - 74, 1984.

[3] D.Downs and G.J.Popek, "A Kernel Design for a Secure DBMS," In Proc. 3rd conf. On Very Large Data Bases, 1977.

[4] Dorothy E.Denning, "Commutative Filters for Reducing Inference Threats in Multilevel Database Systems," In Proc. Of Symposium on Security and Privacy, IEEE Computer Society, pp. 134 - 146, 1985.

[5] Dorothy E.Denning, "A Lattice Model of Information Flow," comunication of The ACM, Vol 19, pp. 236 - 243, 1976.

[6] E.McCauley and P.Drongowski, "KSOS- The Design of a Secure Operating System," AFIPS Conf, Proc. 48, pp. 345 - 351, 1979.

[7] C.Wood, R.C.Summers, E.B.Fernandez, "Authorization in Multilevel Database Models," Information Systems, Pergamon Press, 1979.

[8] D.E.Bell and L.J.La Padula, "Secure Computer Systems: Mathemetical Foundations ," ESD-TR- 73 -278, vol. 1, MITRE corp., 1973.