通信情報保護學會誌
第5卷 第3號, 1995. 9

다단계 보안 데이타베이스 관리시스템에서의 고수준 보안성을 제공하는 거래관리

Tightly Secure Transaction Management in Multi-Level Secure Database Management Systems

손 용 락*, 문 송 천**

요 약

다단계 보안 데이타베이스 관리체계(Multi-Level Secure Database Management System: MLS/DBMS)에서 모든 거래와 데이타는 각각 유일한 보안성을 가지고 있다. MLS/DBMS 상에서 동시수행중인 거래들은 공유 데이타를 접근하는 과정에서 충돌가능성을 항시 지니고 있다. 이러한 충돌을 해결하는 과정에서 만약 낮은 보안등급을 가지는 거래가 지연되는 현상이 발생하였을 경우, 높은 보안등급의 정보가 낮은 보안등급의 거래로 유출되어 결과적으로 보안정책을 위반하게 된다. 이러한 종류의 통신경로를 비밀경로라고 한다.

비밀경보 문제를 해결하기 위한 몇몇 종류의 거래관리 기법들이 제시되었다. 이들 기법들은 비록 비밀경로 문제를 해결하였지만, 불행하게도 이들은 보안의 또 다른 측면인 무결성에 대한 고려를 간과하고 있다. 본 논문에서 제안하는 고수준 보안 거래 관리기는 동시에 수행중인 거래들을 스케줄링하는 과정에서 정보의 기밀성 유지를 무결성의 손실없이 이루고 있다. 기밀성을 위하여 고수준 보안 거래관리기는 비완료된 데이타의 은닉에 방법적 기반을 두고 있다. 또한, 무결성을 얻기 위하여 데이타의 적절성을 판단하는 과정에서 데이타의 신뢰성을 최신성과 함께 고려하고 있다.

1. 서 론

다단계보안 체계는 조직의 주요정보를 보호하기 위한 엄격한 통제방법을 제공하고 있다. 다단계보안 데이타베이스 관리체계는 다단계 보안 체계의 접근통제 방법을 데이타베이스에 적용하고 있다. 이러한 접근통제는 조직의 주요정보를 비인가된 사용자로부터 보호하는데 그 목적이 있다.

다단계보안 데이타베이스 관리체계는 다음과 같은 측면에서 일반적인 데이타베이스 관리체계과 차별성을 가진다.

- 다단계보안 데이타베이스 관리체계에 의해 통제되는 모든 데이타와 사용자는 각각 유일한 보안등급을 가진다.
- 데이타에 대한 사용자의 접근은 사용자에게 부여된 보안등급과 데이타의 보안

* 서경대학교 전산통계학과
** 한국과학기술원 정보 및 통신공학과

등급에 기반을 두고 통제 되어진다.

위와 같은 특성을 가짐에 따라 조직의 보안정책은 보안등급에 기반을 두고 이루어지게 된다. 일반적으로 보안정책은 조직의 정보흐름이 항상 하위 보안등급의 사용자나 데이타로부터 상위 보안등급의 사용자나 데이타에게로 향하도록 하고 있다[2].

하지만, 이러한 보안정책이 데이타를 접근하는 과정에서의 하위 보안등급의 데이타나 사용자에게로 향하는 정보흐름을 불허하고 있음에도 불구하고, 이를 위반하는 통신 경로가 여전히 존재하게 되는데 이러한 통신경로를 비밀경로라고 한다[7]. 즉, 비밀경로는 정보시스템내에 존재하는 비인가된 통신경로라고 정의할 수 있다. 이러한 비밀경로를 통한 통신은 CPU 사용시간이나 메모리 블록, 디스크 섹터, 데이타베이스의 특정 데이타 항목 등의 공유자원을 여러 사용자가 동시에 접근하는 과정에서 쉽게 생성되어질 수 있다. 이들 공유자원들을 이용하여 송신측에서는 공유자원의 상태를 변경시키고, 수신측에서는 그 공유자원의 변경된 상태를 감지함으로써 통신이 이루어진다. 이러한 비밀경로를 이용한 통신은 운영체계나 데이타베이스 관리체계와 같은 시스템 소프트웨어들이 공유자원에 대하여 사용적인 측면에 대한 제어만을 하고 있음에 그 원인이 있다.

본 논문은 다단계 보안 데이타베이스 관리체계에서 동작중인 거래관리기가 동시에 수행중인 거래들을 스케줄링하는 과정에서 비밀경로를 제거하는 방안에 기본적인 촛점을 맞추고 있다. 거래는 데이타베이스상에서 원자적으로 수행되는 판독과 갱신연산들의 순서화된 집합으로 이루어져 있다. 동시수행중인 거래들은 데이타베이스의 공유된 데이타항목을 접근하는 과정에서 불가피하게 충돌을 야기시키게 된다. 거래관리기가 거래들간의 이러한 충돌을 발견하게되면 거래 및 데이타베이스의 정확성을 위하여 몇몇 거래들의 수행을 불가피하게 지연시킨다[1]. 이 경우 지연되는 거래가 충돌이 발생한 거래의 보안등급보다 상대적으로 낮은 보안등급을 부여 받았다면 낮은 보안등급의 거래로의 정보흐름이 발생하게 된다. 만약 충돌하는 이러한 거래들을 제기한 사용자들이 서로 공모를 하고 있었다면, 비인가된 기밀정보가 누출되게 된다.

예 1 (비밀경로 생성) :

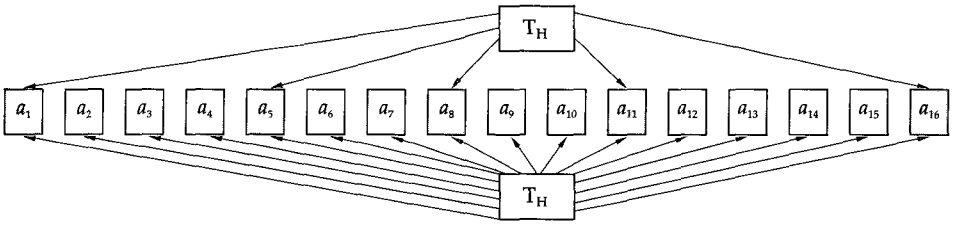


그림 1 T_H와 T_L사이의 비밀경로

동시수행중인 거래 T_H와 T_L은 각각 상위 보안등급과 하위 보안등급을 부여받고 있으며 이들에 대한 스케줄링은 잠금기법[1]을 사용하고 있다고 가정한다(그림 1). 또한, T_H와 T_L은 데이타항목 a_1, a_2, …, a_{16}을 공유하기로 약속을 하였다고 가정한다.

T_L은 자신의 부거래 T_{L1}, T_{L2}, ···, T_{L16}을 생성하고 이들 부거래들로 하여금 공유하기로 한 데이타들을 접근하도록 한다. 예를 들면, T_{L1}은 a_1을, T_{L2}는 a_2를 접근한다. 만약, T_H가 a_1, a_5, a_8, a_{11}, a_{16}을 판독하기 위해 접근하고 T_L은 모든 공유데이타들을 갱신하기 위해 접근할 경우, a_1, a_5, a_8, a_{11}, a_{16}을 T_H와 T_L이 동시에 접근하는 과정에서 충돌이 발생하게 된다. T_H의 모든 판독연산이 T_L의 모든 갱신연산들 보다 선행하여 제기된다면, 거래 관리기는 거래의 정확성을 위하여 충돌이 발생하는 데이타들에 대한 T_L의 갱신연산들을 지연시키게 된다. 결국 T_H는 T_L의 갱신연산을 지연 혹은 즉시 수행시키는 것을 선택적으로 제어할 수 있게 된다. 그러므로, T_H와 T_L이 공모를 하게 되면 T_H는 T_L과 공유하고 있는 데이타들 중 일부에 대하여 선택적으로 판독연산을 제기함으로써 의도한 형태의 비트열을 T_L로 보낼 수 있다. T_L 또한 자신의 지연된 갱신연산들을 판별함으로써 T_H로 부터 전하여진 비트열을 수신할 수 있다. 그림 1에서는 T_H가 T_L로 '1000100100100001'을 전송하는 경우를 나타내고 있다.

→ 예 1 끝 ■

이러한 비밀경로에 관한 선행 연구결과들은 크게 2가지 종류로 구분할 수 있다. 즉, 무조건적 우선방법[3, 4]와 순서판 방법[5, 6]이 그것이다. 무조건적 우선방법은 서로 다른 보안등급을 가지는 거래들 사이에 충돌이 발생하였을 경우 하위 보안등급의 거래가 제기한 연산에 대하여 무조건적으로 우선순위를 부여하여 처리하는 방식이다. 이에다라 하위 보안등급 거래는 상위 보안등급 거래에 의한 수행상의 간섭을 전혀 받지 않게 됨으로써 정보의 기밀성을 유지하게 된다. 순서판 방법은 정보의 기밀성을 획득하기 위하여 공유되는 데이타를 접근하는 거래들이 서로 다른 버전의 데이타를 생성하고 판독하도록 함으로써 거래들간에 발생할 수 있는 간섭을 배제시키고 있다.

비록, 이들 선행 연구결과들이 기밀성을 획득하고 있지만, 이들은 보안의 다른 한편의 중요한 측면인 무결성에 대하여는 간과를 하고 있다. 또한, 무조건적 우선방법에 의한 거래 스케줄링 과정에서 발생하는 불공정성으로 말미암아 상위 보안등급 거래들이 기아현상에 봉착할 수 있다. 이와 더불어, 무조건적 우선방법은 거래들 사이에 교착상태를 발생시킬 수 있다. 이러한 현상들은 시스템의 성능을 저하시키는 요인으로 작용하게 된다. 교착상태 문제는 순서판 방법에서도 발생할 수 있는 것으로써, 이로 인하여 이 방법 또한 시스템의 성능저하를 초래하게 된다. 이와 더불어, 선행 연구결과들이 가지고 있는 공통된 문제점은 무결성의 중요한 측면인 데이타의 신뢰성에 대한 고려를 간과하고 있다는 것이다. 이들 연구결과들은 데이타의 최신성만을 데이타의 무결성을 판단하는 기준으로 삼고 있다. 이에따라, 데이타의 신뢰성에 대한 무시는 거래관리에 있어서 보안상의 취약성을 노정시킬 수 있다.

선행 연구결과들이 무결성과 시스템의 성능을 희생시킴에 따라, 이들 연구결과로는 고수준의 거래관리기를 구성하기에는 어려움이 있다. 본 논문에서는 기밀성과 무결성을 함께 획득하는 새로운 거래관리기를 제안하고자 한다.

2. 모 델

2.1 거래 모델

거래 T_i에 의해 데이타 x에 수행되는 판독(갱신)연산은 $R_i[x]$($W_i[x]$)로 표시된다. T_i의 완료는 C_i로 표시되며, 완료 후에는 T_i가 행한 모든 갱신결과를 데이타베이스에 반영하게 된다. 이와 반대로, A_i로 표시되는 T_i의 철회는 T_i가 행한 모든 갱신결과를 취소시키게 된다. 거래들의 집합을 $T = \{T_1, T_2, \cdots, T_n\}$으로 정의

할 때 T에 속한 거래들의 데이타베이스상에서의 수행궤적은 거래이력(history), H, 라고 표시되는 구조를 가지게 된다.

일반적으로 단일버전을 기반으로 하는 보안 거래관리는 데이타베이스 시스템의 성능에 대한 공격에 매우 취약한 특성을 가지고 있다. 이에따라 다중버전을 기반으로 하는 보안 거래관리가 불가피하다. 다중버전 데이타베이스에서는 데이타에 대한 모든 판독연산은 그 데이타에 대한 새로운 버전을 생성하게 된다. 다중버전 거래이력(H)은 데이타의 버전들에 대한 연산들의 순서를 나타낸다. 그러므로 다중버전 거래이력에서의 $W_i[x]$는 $W_i[x_i]$로, $R_i[x]$는 $R_i[x_j]$로 사상되어 진다. 거래집합 T에 대한 두가지 이상의 다중버전 거래이력들은 그들이 동일한 거래들로 구성되어 있다면 동등하다고 한다. 다중버전의 거래이력들은 그들이 동일한 거래집합에 대한 순차적인 거래이력과 동등하다면 '단일버전 순서화 가능하다(One-copy serializable : ISR)'라고 일컬어지며 이는 거래이력이 정확함을 결정적으로 판단하게 한다[1].

다중버전 거래이력이 1SR 인지에 대한 여부를 판단을 하기 위하여 다중버전 순서화 가능 그래프(Multiversion serialization graph : MVSG(H))가 사용되어진다. MVSG(H)의 구성에 대한 제한사항을 다음과 같다.

- 각 데이타 x에 대하여, MVSG(H)는 x의 모든 버전들에 대하여 순서 ($\ll_x$로 표기됨)를 가지도록 한다.
- 각 데이타 x에 대하여, T_j가 T_i로 부터 x를 판독하고 $x_i \ll_x x_k$이면 MVSG(H)는 $T_i \rightarrow T_j$라는 연결선을 가지게 된다. 이와 반대로, $x_k \ll_x x_i$이면 MVSG(H)는 $T_k \rightarrow T_i$라는 연결선을 가지게 된다.

정확한 결과를 생산하는 거래이력에 대한 MVSG(H)는 비순환성을 가지는데, 다중버전 거래이력 H가 단일버전 순서화 가능하다면 MVSG(H)는 비순환성을 가진다[1].

2.2 거래관리에서의 보안모델

보안등급 사상함수 SL은 데이타와 거래들을 보안등급에 사상시켜 주는 역할을 한다. 이러한 보안등급 사상함수를 적용함에 따라 거래들의 연산들은 정의 1에서 나타나는 제한사항을 준수하여야 한다.

정의 1(거래 접근통제 정책)

① 모든 거래들은 단일 보안등급을 부여받는다.

② $SL(T_i)$와 $SL(x)$는 일반 사용자에 의해서는 수정이 불가능 하다.

③ $SL(T_i) > SL(x)$인 경우, T_i는 x에 대한 갱신을 불허한다.

④ $SL(T_i) < SL(x)$인 경우, T_i는 x에 대한 판독을 불허한다.

이러한 보안성을 모델링하는 과정에서 두가지 종류의 등급이 필요하게 되는데, 기밀등급(Confidentiality level)과 무결등급(Integrity level)이 그것이다. 이들에 대한 등급 사상함수로는 CL과 IL을 각각 사용하도록 한다.

정의 2(기밀성 획득) 기밀성을 획득하기 위하여 보안 거래관리기는 다음의 제한사항들을 준수하여야 한다.

① 동시에 수행되는 거래 T_1과 T_2에 대하여, $CL(T_1)$과 $CL(T_2)$는 각각 $SL(T_1)$과 $SL(T_2)$의 값을 갖게된다. 즉, $CL(T_1) = SL(T_1)$이며 $CL(T_2) = SL(T_2)$이다.

② 만약 $CL(T_1) > CL(T_2)$이면, 보안 거래관리기는 T_1이 T_2를 간섭하는 것을 방지하여야 한다.

기밀성을 획득함으로써 하위 기밀등급 거래에 대한 상위 기밀등급 거래의 간섭이 배제되게 된다. 이에따라 이러한 거래들간의 비밀경로도 제거되게 된다.

시스템이 보안성을 가지는 과정에서의 성능 저하를 방지하기 위하여 다중버전을 기반으로 하고 있지만, 1장에서 언급하였듯이 버전의 최신성만으로는 그 버전에 대한 무결성의 정도를 파악하기에는 부족하다. 그러므로, 데이타 버전의 무결성을 보다 정확히 판단하기 위하여 신뢰성을 최신성과 함께 고려하도록 한다.

데이타 버전의 신뢰성은 일반적으로 그 버전을 생성하는 거래의 정보처리 능력에 따라 달라질 수 있다고 할 수 있다. 거래의 이러한 정보처리 능력은 두가지 측면에서 파악될 수 있는데, 해당 거래가 참조가능한 데이타들의 다양성의 정도에 대한 측면과 그 거래에 의하여 참조되는 데이타의 신뢰성에 대한 측면이 그것이다.

■ **정의 3(무결성 획득)** 무결성을 획득하기 위하여는 보안 거래관리기는 다음의 제한사항을 준수하여야 한다.

① 거래 T_i가 시작될 때, $IL(T_i) = SL(T_i)$

② 데이타 x의 최초버전 x_0에 대하여, $IL(x_0) = SL(x)$

③ T_i가 $W_i[x]$에 의해 x의 새로운 버전 x_i를 생성하면 $IL(x_i) = IL(T_i)$

④ T_i가 $R_i[x_j]$에 의해 x_j로 부터 값을 참조하게 되면, $IL(T_i) = \max\{IL(a), IL(b), \ldots, IL(x_j)\}$. 이때 a와 b는 T_i가 x_j를 판독하기전에 판독한 버전들이다.

⑤ T_i가 y_i를 판독할 경우, $IL(y_j) = \max\{IL(y_1), IL(y_2), \ldots, IL(y_j), \ldots, \}$ 이어야 한다. 또한 두개이상의 버전이 최상의 무결등급을 가지면 가장 최근에 생성된 버전을 선택한다.

■ **정의 4(고수준 보안성 획득)** 거래관리기가 기밀성과 무결성을 동시에 획득할 경우 이 거래관리기는 고수준의 보안성을 획득하게 된다.

3. 고수준 보안 거래 관리기 (Tightly Secure Transaction Scheduler : TS²)

TS²의 목적은 동시에 수행되는 거래들을 스케줄링하는 과정에서 고수준의 보안성을 획득하는데 있다. TS²는 이러한 고수준 보안성을 획득하기 위하여 다음과 같은 전략을 채택하고 있다.

- 비완료된 데이타들을 은닉시킴으로써 기밀성을 획득함
- 데이타의 신뢰성을 최신성과 함께 고려함으로써 무결성을 획득함

3.1 비완료된 데이타의 은닉

다중버전 스케줄링 기법에 기초를 하고 있는 TS²는 비완료된 버전의 은닉을 위하여 두개이상의 거래들간의 통신은 반드시 완료된 데이타 버전을 이용함으로써 이루어지도록 제한하고 있다[8]. 이에따라 비완료된 거래들간에는 결코 통신이 이루어지지 않는다. 그 결과, 비완료된 거래들간의 간섭은 발생하지 않으며, 이에따라 비완료된 거래들간에 비밀경로가 발생하는 것이 불가능하게 된다. 또한 데이타 버전들이 그들의 생성자가 완료된 후에만 참조가능하게 되므로 비완료된 거래의 갱신연산은 다른 비완료된 거래의 연산수행을 방해하지 못하게 된다. 그러므로 모든 거래들은 다른 거래로 부터 제기될 수 있는 간섭을 전혀 겪지 않고 수행되어진다.

3.1.1 비완료된 데이타의 은닉을 위한 특성

비완료된 데이타의 은닉을 위하여 TS²는 다음과 같은 특성들을 지니고 있다.

- 순서상의 특성 : 거래 T_i가 시작될때 TS²는 T_i에 대하여 시작판(begin-stamp :

$bs(T_i)$)을 배정한다. $bs(T_i)$는 이미 완료된 모든 거래의 시작판보다는 항상 큰 값을 갖고, 향후 제기될 거래들의 시작판 보다는 같거나 작은 값을 갖게 된다.

- 공개상의 특성 : 거래 T_i가 비완료된 상태에서는 T_i가 제기한 갱신연산의 결과는 다른 거래에 공개되지 않으며 T_i가 완료된 후에 비로소 공개된다.
- 판독상의 특성 : 거래 T_i가 x_j를 판독하기 위하여는 x_j의 갱신판(write-stamp : $ws(x_j)$)이 $bs(T_i)$보다 작거나 같은 경우에만 가능하다.
- 비간섭 갱신특성 : 갱신연산은 다른 거래가 제기한 갱신연산과는 무관하게 수행되어진다.

이러한 특성은 TS^2가 1SR이라는 것을 증명하기에 충분한 것들이다. 더우기 이러한 특성을 가짐에 따라 TS^2는 비밀경로 문제를 해결할 수 있으며 낮은 보안등급을 가지는 거래가 시도하는 악의적인 보안침해 행위를 방지할 수 있다. 이러한 것들에 대한 증명은 4장에서 하도록 한다.

3.1.2 은닉특성의 실현

비완료된 버전들에 대한 은닉을 실현하기 위하여 참조계수기(Visible counter : VC)라는 공유변수를 사용한다. 거래 T_i가 시작될때 (이를 B_i로 표시함) TS^2는 $bs(T_i)$를 VC값을 가지도록 하며 VC는 거래가 완료될 때 마다 1씩 증가하게 된다. 거래들에 대한 시작판들의 순서가 반드시 그들이 완료되는 싯점들의 순서와 동일할 필요는 없으므로 이러한 방식은 타당한 것이 된다.

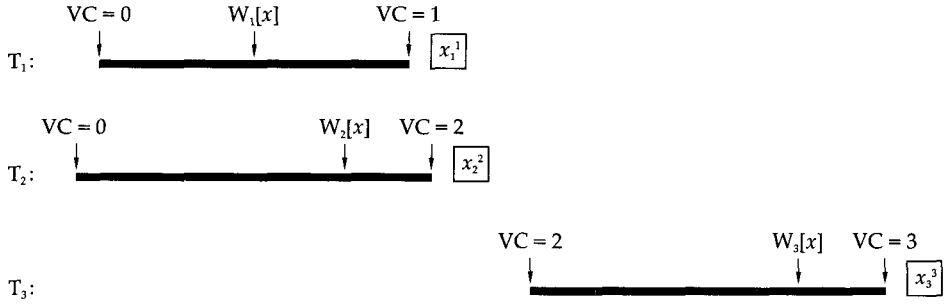


그림 2 새로운 버전 생성

TS^2는 $W_i[x]$를 처리한 후 $ws(x_i)$가 ∞값을 갖도록 한다. 그러나 T_i가 완료할 때 TS^2는 $ws(x_i)$의 값을 T_i가 완료함에 따라 증가되어진 VC의 값으로 변경한다. 그래서 $ws(x_i)$는 항상 $bs(T_i)$보다는 큰 값을 갖게 된다. 그림 2는 VC, 거래들의 시작판 값, 데이타버전들의 갱신판들의 변이과정을 보여주고 있다. 각 버전의 아랫첨자와 윗첨자는 각각 그 버전의 생성자의 시작판 값과 생성자가 완료될 때의 VC 값을 나타내고 있다.

만약 일반적인 다중버전 시간판 순서기법(Multiversion timestamp ordering)을 이용하는 거래관리기가 '$B_3B_2W_2[x_2]C_2B_1R_1[x]W_3[x_3]C_3R_1[x]$' 형태의 연산요구를 받았다면, 그 거래관리기는 두번째의 $R_1[x]$가 첫번째의 $R_1[x]$와 동일한 버전을 읽도록 하기 위하여 $W_3[x_3]$의 수행을 거부할 것이다. 그러나 만약 $SL(T_1) > SL(T_3)$일 경우, 이러한 거부는 보안정책을 위반하는 정보의 흐름을 유발시킬 것이다. 그러나, 그림 3에서 나타나듯이 TS^2는 하위 보안등

급 거래가 제기한 판독연산을 거부하지 않은 채 첫번째와 두번째의 $R_2[x]$들이 동일한 버전을 판독할 수 있도록 한다.

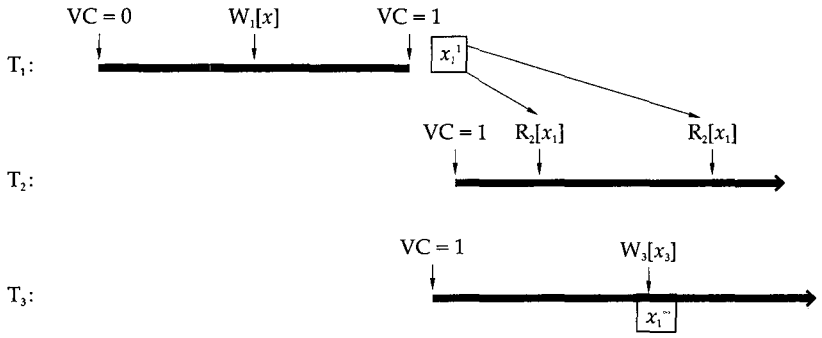


그림 3 동일한 버전에 대한 판독

$ws(x_1) = bs(T_2)$이므로 첫번째 $R_2[x]$는 T_1에 의해 생성된 버전(x_1)을 판독한다. $W_3[x]$연산의 요구를 받았을때, TS^2는 $W_3[x]$를 거부하는 대신에 $ws(x_3)$이 ∞값을 갖도록 하여 x_3가 T_2에 의해 참조되는 것을 방지한다. $ws(x_3)$가 항상 $bs(T_2)$보다 큰 값을 가지고 있기 때문에 두번째 $R_2[x]$는 x_3대신에 x_1을 판독하게 된다. 이로써 TS^2는 두개의 $R_1[x]$가 일관성이 있는 값을 얻도록 함에 따라 $W_3[x]$를 T_2의 간섭없이 수행시킬 수 있다. 이에따라 만약 $SL(T_2) > SL(T_3)$일 경우에도 TS^2는 보안정책을 위반하는 정보유출을 발생시키지 않으면서 T_2와 T_3를 스케줄링할 수 있게 된다.

거래와 데이타들의 보안등급들이 $SL(T_1) = SL(T_2) = SL(x) = SL(y)$, $SL(T_3) \leq SL(T_1)$ 그리고 $SL(T_4) < SL(T_2)$의 형태를 가진다고 가정한다(그림 4). 만약 T_1과 T_2가 순서판 방법에 따라 스케줄링되어 진다면 이들 거래들은 자신들의 대응거래들이 완료될 때까지 서로 기다리게되는 교착상태에 빠지게 된다. 그러나, 만약 이들 거래들이 TS^2에 의해 스케줄링되어진다면 이들은 교착상태를 발생시키지 않고 스케줄링되어질 수 있다.

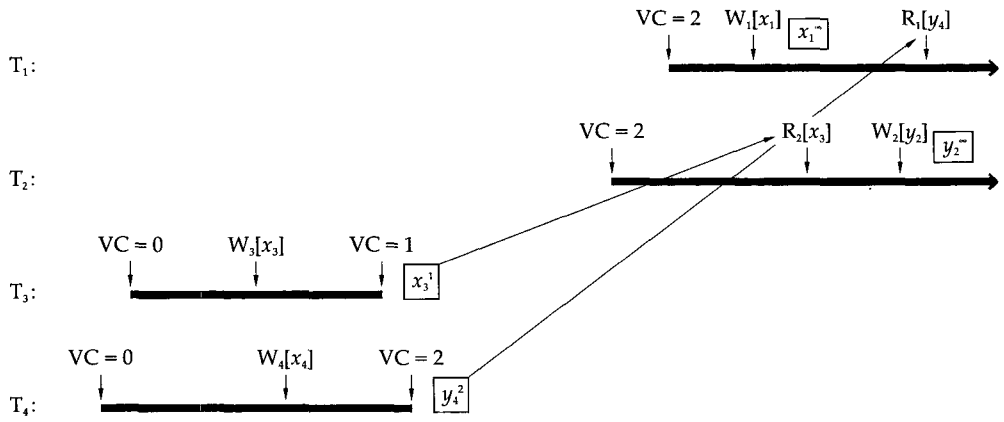


그림 4 비완료된 버전의 판독방지

TS²는 $ws(x_1)$과 $ws(y_2)$를 각각 ∞의 값을 갖도록 함으로써, $R_2[x]$와 $R_1[y]$가 각각 x_1과 y_2를 참조하는 것을 방지한다. 이에따라 TS²는 $R_2[x]$와 $R_1[y]$로 하여금 각각 완료된 버전인 x_3와 y_4를 판독하도록 한다. 그 결과 T_1과 T_2는 더이상 상대편이 완료되기를 기다릴 필요가 없게 된다. 따라서 TS²는 비완료된 버전을 은닉시킴으로써 교착상태를 야기시킬 수 있는 모든 수단을 제거하고 있다.

3.2 신뢰성 있는 버전의 선택

이미 언급한 것처럼 데이타 버전의 최신성은 인가된 모든 거래들에 의하여 쉽게 변경가능함에 따라 버전의 무결성의 정도를 판단하는 데에는 부족하다. 그래서 판독연산을 요구받게 되면, TS²는 버전에 대한 무결성의 정도를 판단하는데 있어서 최신성과 더불어 버전의 신뢰성도 함께 고려한다. 이를 위하여 TS²는 후보리스트(canididate-list)라고 하는 특별한 리스트를 유지한다. TS²가 $R_i[x]$연산을 요구를 받았을때, x에 대한 적절한 버전을 찾기 위하여 x의 버전들로 구성된 후보리스트($cand_i[x]$)를 구성한다. $ccand_i[x]$의 각 원소들은 후보판(candidate-stamp)를 가지게 되는데 x_j의 후보판은 $cs(x_j)$로 표시된다. $cs(x_j)$는 [$IL(x_j)$, $ws(x_j)$]의 순서를 구성되는데, 이는 x_j의 무결등급이 갱신판 값에 대하여 항상 우선적으로 취급되도록 하기 위함이다. TS²가 $R_i[x]$ 요구를 받게 되면, TS²는 $cand_i[x]$에 존재하는 버전들 중 최대값의 후보판을 가지고 있는 버전을 가장 적절한 버전으로 선택한다.

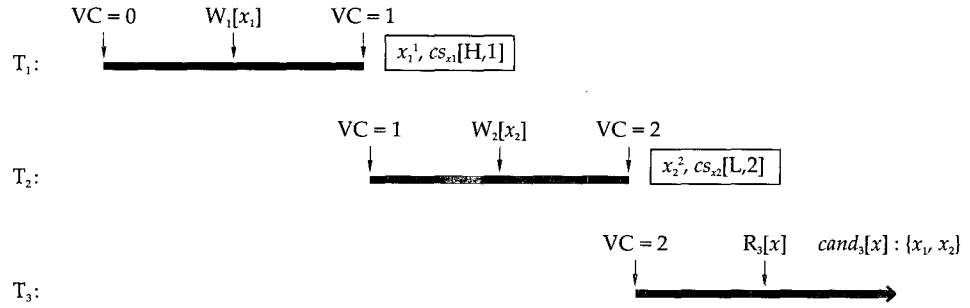


그림 5 신뢰성 있는 버전의 판독

그림 5에서 $SL(T_1) = IL(T_1) = H$, $SL(T_2) = IL(T_2) = L$, 그리고 $H > L$이라고 가정한다. $R_3[x]$ 요구에 대하여 $ws(x_1) < bs(T_3)$이고 $ws(x_2) = bs(T_3)$이므로 TS²는 $cand_3[x]$를 $\{x_1, x_2\}$로 구성한다. $R_3[x]$ 요구에 대하여 비록 x_1이 x_2보다 먼저 생성되었지만 $cs(x_1) > cs(x_2)$이므로 TS²는 x_1을 적절한 버전으로 선택한다. 즉, TS²는 높은 무결등급 거래에 의해 생성된 버전을 낮은 무결등급 거래에 의해 생성된 버전보다 더 적절한 것으로 판단한다. 그러나 만약 H = L 인 경우, $cs(x_2) > cs(x_1)$이므로 TS²는 x_2를 더 적절한 버전으로 판단한다. 즉 TS²는 동일한 무결등급 거래들에 의해 생성된 버전들에 대하여는 최근에 생성된 버전을 더 적절한 버전으로 판단한다.

4. 정확성과 보안성에 대한 증명

TS²에 의한 스케줄링의 결과가 정확성을 가지려면 스케줄링의 결과로 나타나는 거래이력이 1SR이어야 한다.

❖ 정리 1(정확성 획득)

판독상의 특성과 공개상의 특성에 의거하여, TS²는 동시 수행되는 거래들을 1SR의 결과를 갖도록 스케줄링한다.

증명 : TS²가 생성한 거래이력 H에 대한 정확성을 증명하기 위하여, MVSG(H)에 연결선을 추가하는 모든 경우에 대한 고찰을 한다.

■ 경우 1 $SL(T_i) > SL(T_j)$이고 T_i와 T_j사이에 판독/갱신의 연관성이 존재하는 경우.

만약 $R_i[x_j] \in H$이면 $T_i \rightarrow T_j$가 MVSG(H)에 추가된다. $R_j[y_i]$ 요구에 대하여, 거래 접근 통제 정책에 의거하여 $SL(T_j) \geq SL(y)$이고 $SL(y) \geq SL(T_i)$이다. 따라서 TS²는 절대 $R_i[x_i]$ 요구를 받지 않는다. 이에따라 $T_i \rightarrow T_j$는 결코 MVSG(H)에 나타나지 않게 된다. 그러므로 이 경우에는 MVSG(H)는 사이클을 가지지 않는다.

■ 경우 2 $SL(T_i) = SL(T_j)$이며 T_i와 T_j 사이에 판독/갱신 연관성이 존재하는 경우

만약 $R_i[x_j]$이면 $T_i \rightarrow T_j$가 MVSG(H)에 추가되고, 이에따라 $bs(T_j) < bs(T_i)$가 된다. $R_j[y_i]$ 요구에 대하여, 공개상의 특성에 의거하여, T_j는 T_i가 완료된 후에 y_i를 판독하는 것이 허용된다. 이때 T_i가 완료된 후에는 $bs(T_i) < ws(y_i)$가 된다. 그러나 $bs(T_j) < bs(T_i)$이므로 $bs(T_j) < ws(y_i)$이다. 이에따라 판독상의 특성에 의거하여 T_j가 y_i를 판독하는 것은 불가능하게 됨에 따라 $T_i \rightarrow T_j$는 결코 MVSG(H)에 나타나지 않게 된다. 그러므로 이 경우에도 MVSG(H)는 사이클을 가지지 않는다.

■ 경우 3 $SL(T_i) \geq SL(T_j)$이고 T_i와 T_j사이에 갱신/갱신 관련성이 존재하는 경우

$x_i \ll_x x_j$일때, 비간섭 갱신특성에 의거하여, TS²는 x_i에 대한 고려가 필요하지 않은채 $W_i[x]$ 요구를 처리할 수 있다. 이에따라 비록 $x_i \ll_x x_j$일지라도 T_i와 T_j 사이에는 실제적으로 관련성이 존재하지 않게 됨에 따라 MVSG(H)에 $T_i \rightarrow T_j$가 나타나지 않는다. 그러므로 이 경우에는 MVSG(H)는 사이클을 가지지 않는다.

이상과 같이 MVSG(H)에 연결선을 추가할 수 있는 모든 경우를 고찰한 결과 TS²에 의해 생성되어진 거래이력 H에 대한 MVSG(H)는 사이클을 가지지 않으므로 H는 1SR이며, 이에따라 TS²는 정확한 거래이력을 결과로 낳게 된다.

❖ 정리 2(고수준 보안성 획득)

동시에 수행중인 거래들을 스케줄링하는 과정에서 TS²는 기밀성과 무결성에 대한 손실을 발생시키지 않는다.

증명 : 고수준 보안성의 획득을 증명하기 위하여 거래들을 스케줄링하는 과정에서 TS²가 기밀성과 무결성을 획득하는 경우를 고찰한다.

■ 경우 1 기밀성 획득

$CL(T_i) > CL(T_j)$, $CL(x) > CL(T_i)$, $CL(T_i) = CL(y)$ 그리고 $CL(T_j) = CL(z)$라고 가정한다. 거래 접근통제 정책에 의거하여, '$R_i[y]W_j[y]$', '$R_j[z]W_i[z]$', '$W_i[x]W_j[x]$', 그리고 '$W_i[y]W_j[y]$'와 같은 연산요구 순서들은 보안정책을 위반하는 정보흐름을 야기 시킬 수 있다. 그러나 공개상의 특성에 따라 TS²는 $R_i[y]$와 $R_j[z]$와 각각 충돌하는 $W_j[y]$와 $W_i[z]$ 요구를 거부하지 않는다. 또한 비간섭 갱신 특성에 의거하여, TS²는 $W_i[x]$ 및 $W_i[y]$와 각각 충돌하는 $W_j[x]$와 $W_j[y]$ 요구를 거부하지 않는다. 따라서 $W_j[x]$, $W_j[y]$ 그리고 $W_j[z]$를 이용하여서는 T_j는 T_i로 부터 어떠한 정보도 받지 못한다. 결국, 공유데이타를 동시접근하는 과정에서 발생하는 충돌에 따른 거래의 지연을 이용하여서는 T_j는 T_i로 부터 아무런 정보를 받지 못한다. 그러므로 TS²는 거래들을 스케줄링과정에서 비밀경로를 발생시키지 않으며, 그 결과 기밀성을 획득하게 된다.

■ 경우 2 무결성 획득

거래 T_i가 $W_i[x]$ 요구를 제기하여 새로운 버전 x_i를 생성하고자 할때, TS²는 이 요구가 있기까지 수행된 모든 판독연산들에 대하여 항상 최상의 무결등급을 가지는 버전들을 제공하였다. 이에따라 T_i가 새로운 버전을 생성하는 싯점에서는 최상의 무결등급을 가지는 정보들을 이용한 정보처리과정을 수행한 상태이므로 T_i가 생성하는 버전 또한 T_i가 생성할 수 있는 최상의 무결등급을 갖게 된다. 또한 TS²는 x_i의 무결등급 $IL(x_i)$이 T_i가 $W_i[x]$ 요구를 제기하는 싯점에서의 $IL(T_i)$값을 갖도록 함으로써, T_i가 x_i를 생성하기까지 습득한 최상의 무결성을 x_i에 반영할 수 있도록 한다. 이에따라 새로운 버전의 생성에 필요한 정보처리과정에서 참조되는 버전들의 무결성 정도가 최상의 상태에 있으며, 이러한 최상의 무결성 정도가 새로운 버전에 반영되고 있으므로 TS²는 거래들을 스케줄링하는 과정에서 무결성을 획득한다.

이상과 같이 TS²가 거래들을 스케줄링하는 과정에서 기밀성과 무결성을 함께 획득하고 있으므로 TS²는 고수준의 보안성을 획득하고 있다.

5. 결 론

본 논문은 거래들을 스케줄링하는 과정에서 기밀성과 무결성을 함께 획득함으로써 고수준의 보안성을 얻는 것이 가능함을 제시하고 있다. 고수준의 보안성을 획득하는 과정에서 TS²는 기밀성의 획득을 위하여 거래들간의 통신이 완료된 버전들만을 이용하도록 제한하고 있다. 무결성을 획득하기 위하여 TS²가 채택하고 있는 정책은 정보의 무결성의 정도가 그 정보를 생성하는데 참조된 정보들의 무결성 정도와 그 정보를 생성하는 거래의 정보처리능력에 따라 결정된다는 사실에 근거를 두고 있다.

TS²가 가질 수 있는 문제점으로는 거래들로 하여금 어느정도 오래된 버전들을 판독하게 한다는 것이다. 이 문제에 대한 해결방안이 향후 연구과제로 남을 것이다. 또한 보안모델의 단순화를 위하여 TS²는 기밀등급과 무결등급이 동일한 형태를 가지는 것으로 상정하고 있다. 보다 더 융통성있는 보안정책이 운영되도록 하기 위하여 이들 등급들이 서로 독립적으로 존재하는 경우에 대한 연구결과도 향후의 확장된 형태의 TS²에서 제시될 것이다.

참 고 문 헌

[1] P. A. Bernstein, V. Hadzilacos and N. Goodman, Concurrency Control and Recovery in Database Systems, Addison-Wesley, 1987. Control and Recovery in Database Systems, Addison-Wesley, 1987.

[2] Ravi Sandhu, "Mandatory Controls for Database Integrity", DATABASE SECURITY, Ⅲ : Status and Prospects, ed. David L. Spooner, Carl Landwehr, Elsevier SCience Publishers B. V., 1990, pp. 143-150.

[3] John McDermott and Sushil Jajodia, " Orange Locking : Channel-Free Database Concurrency Control via Locking", DATABASE SECURITY, VI : Status and Prospects, ed. Bhavani M. Thuraisingham, Carle. Landwehr, Elsevier Science Publishers B.V., 1993, pp. 267-284.

[4] Oliver Costich and Sushil Jajodia, "Maintaining Transaction Atomicity in MLSDatabase Systems With Kernalized Architecture", DATABASE SECURITY, VI : Status and Prospects, ed. Bhavani M. Thuraisingham, Carle. Landwehr, Elsevier Science Publishers

B. V., 1993, pp. 249-265.

[5] T.F. Keefe, W. T. Tsai and J. Srivastava, "Multilevel Secure Database Concurrency Control", Proceedings of IEEE Symposium on Security and Privacy, 1990,pp.337-344.

[6] Sushil Jajodia Vijayalakshmi Atluri, "Alternative Correctness Criteria for Concurrent Execution of Transactions in Multilevel Secure Database", Proceedings of IEEE Symposium on Security and Privacy, 1992, pp. 216-224.

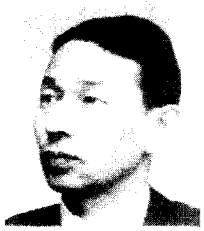
[7] Charles P. Pfleeger, Securtiy in Computing, Prentic-Hall International, Inc., 1989. pp. 299-345

[8] Yonglak Sohn, Sukhoon Kang, and Songchun Moon, "Concurrency Control Scheme in Multi-Level Secure Database Management Systems", The EUROMICRO Journal, 40, 1994

□ 著者紹介

손 용 락(孫 用 洛)

1986년 경북대학교 전자공학과 전산전공 학사
1988년 고려대학교 전자공학과 정보처리전공 석사
1992년 9월 ~ 현재 한국과학기술원 정보 및 통신공학과 컴퓨터공학전공 박사과정
1988년 9월 ~ 1995년 3월 (주) 데이콤
1994년 11월 ~ 현재 한국통신정보보호학회 회원
1995년 3월 ~ 현재 서경대학교 전산통계학과 전임강사
※ 주관심분야 : 데이타베이스 보안, 동시성제어, 정보검색시스템



문 송 천(文 松 天)

1975년 숭전대학교 전산학과 학사
1977년 한국과학기술원 전산학과 석사
1985년 University of Illinois at Urbana-Champaign 전산학과 박사
1977년 3월 ~ 1985년 4월 숭전대학교 전산학과 조교수
1981년 9월 ~ 1984년 8월 미국육군연구소(CERL) 연구원
1985년 ~ 현재 한국과학기술원 교수
1989년, 1994년 영국 에딘버러대학, 캠브리지대학 객원교수
1990년 ~ 1992년 한국정보과학회 데이타베이스 연구회 회장
1991년 미국정보과학회(ACM) DB연구회 학술위원
1991년 4월 ~ 1993년 4월 DASFAA93 국제학술대회 학술의장
1991년 9월 ~ 현재 유럽정보과학회(EUROMICRO) 상임이사
1991년, 1995년 니카라과정부 외무부 자문역, 루마니아정부 산업부 자문역
1994년 헝가리 과학원 초청 저명과학자
1994년 10월 ~ 현재 한국정보과학회 이사