通信情報保護學會誌
第7卷 第2號, 1997. 6

보안 지식 베이스 관리 시스템에서의 질의 처리

조 일 래*, 김 원 중**, 심 갑 식***

Abstract

This paper describes the notion of a Multilevel Secure Knowledge Base Management System(MLS/KBMS). It states a security policy and security constraints. A design for query operation introduced cover story in a MLS/KBMS is discussed.

Query processing approach is to provide cover stories that lead to alternative explanations for readily available information. Therefore such cover stories prevent an unauthorized user from inferring high-level information from low-level data.

1. 서 론

인공지능과 데이타베이스 기술이 통합되어 지식베이스 관리시스템이 출현하였다. 지식베이스 관리시스템(Knowledge Base Management System)의 장점은 인공지능과 데이타베이스 분야에서의 기능들을 모두 이용할 수 있다는 것이다. 즉, 인공지능 분야는 연역(reasoning), 추론(inferencing), 문제해결(problem solving) 분야에서 뛰어난 기능을 발휘하고, 데이타베이스 분야는 방대한 분량의 데이타를 효율적으로 처리할 수 있는 능력을 가지고 있다.

지식베이스 관리시스템에 대한 보안성 첨가는 기존의 데이타베이스 관리시스템보다 훨씬 복잡하다. 왜냐하면 지식베이스 관리시스템은 질의-응답 시스템일 뿐만 아니라 문제해결 시스템이기 때문이다. 데이타와 지식 그 자체의 무결성과 데이타와 지식을 조작하는 타스크(task)의 수행 후에도 무결성(integrity)이 유지된다는 것을 보장하기 위해서는 접근 권한이 없는 사용자로부터 데이타와 지식을 보호하는 것은 매우 중요하다.

지식베이스 관리시스템에 보안성을 제공할 때 발생되는 문제점 중 하나는 추론 기능이다. 지식베이스 관리시스템에서는 추론 기능이 시스템에 내재되어 있기 때문에 사용자로부터 질의가 들어오면 명시적(explicit) 정보로부터 연역할 수 있는 모든 정보를 시스템 자신이 추론할 것이다. 그러므로 질의어에 대한 결과는 명시적 정보뿐만 아니라 암시적(implicit) 정보도 포함하게 될 것이다. 따라서 보안 지식베이스 시스템에서는 데이타와 지식이 해답되어지기 전에 사용자가 이 정보를 볼 수 있는 권한을 가지고 있는지의 여부를 검사할 수 있어야 한다. 데이타베이스 관리시스템의 경우는

* 순천공업전문대학 조교수
** 순천대학교 조교수
*** 진주산업대학교 조교수

고유의 추론 기능을 가지고 있지 않기 때문에 데이타베이스 관리시스템에 추론 엔진이 추가되지 않는다면 데이타베이스 관리시스템은 사용자에게 명시적 데이타만을 제공하는 지식베이스 관리시스템의 특별한 형태가 될 것이다. 물론 사용자는 명시적 데이타들을 계속 축적함으로써 접근 권한이 없는 데이타를 추론할 수도 있지만 추론 엔진에 의하지 않고 기밀 데이타를 연역하는 데는 많은 시간이 걸릴 것이다.

인공지능 시스템에 보안성을 통합하려는 시도는 있었으나 이런 연구들은 대부분 전문가 시스템에 보안성을 제공하려는 데 집중하였다[1,2]. 그리고 지식베이스 관리시스템에서의 다단계 보안에 대한 연구가 있었으나 이들 연구에서는 어떤 사용자가 비권한 데이타와 지식을 아예 얻지 못하게 하는 방식이었다[3]. 그러나 이는 효과적이지 못한 보안기법이다. 왜냐하면, 한 사용자가 질의를 해서 아무 해답이 나오지 않는다면 이것은 어떤 중요한 정보가 있다는 의미가 되고, 이 자체가 정보 유출이 되기 때문이다. 권한이 없는 사용자가 높은 보안등급의 데이타에 접근하기 위한 비정상적인 여러 경로가 있을 수 있다. 즉, 아무 해답도 얻지 못한 질의자는 많은 시간이 걸리겠지만, 추론 방법이나 다른 어떤 방법으로 높은 보안등급의 정보를 얻을 수도 있다. 이는 강제적 접근제어(Mandatory Access Control:MAC)가 정보의 불법적 유출은 방지할 수 있다고 할지라도 비권한 사용자로부터 낮은 등급의 데이타에서 높은 등급의 정보를 추론하는 것을 완전하게 방지할 수 있는 메카니즘을 가지고 있지 않기 때문이다.

강제적 접근제어는 시스템내에 있는 주체(subject)와 객체(object)의 보안등급에 따라 제어를 통제한다. 객체는 릴레이션(relation), 레코드, 레코드내의 필드값 등을 의미하며, 주체는 객체에 접근을 요청할 수 있는 프로세스이다. 보안등급들의 집합은 부분순서 격자(TopSecret(TS) 〉 Secret(S) 〉 Confidential(C) 〉 Unclassified(U))를 형성한다. 여기서 기호(〈, 〉, ≤ 그리고 ≥)는 격자 모델에서 보안등급들 사이의 지배(dominate)관계를 나타낸다.

본 논문에서는 데이타베이스 보안을 위한 커버 스토리(cover story) 개념을 지식베이스 관리시스템에 도입하여 위의 문제점을 해결하려는 시도이다[4]. 커버 스토리는 높은 보안등급의 정보에 대한 또 다른 설명이며, 이것은 누구나 쉽게 접근할 수 있는 정보이다. 이것은 보안등급이 낮은 사용자의 질의에 대해 전혀 해답을 주지 않는 것보다 그 사용자에게 커버 스토리를 이용하여 적절한 수준의 유사한 정보를 제공해 줌으로써 추론채널을 사전에 방지하고자 하는 것이다.

본 논문의 구성에서 1장은 논문의 연구배경인 서론이며, 2장에서는 보안정책 및 보안 제약조건을 설명한다. 지식베이스 관리시스템에서도 데이타베이스 관리시스템의 보안 정책과 보안 제약조건을 따르므로 다단계 보안 데이타베이스에 대한 보안 정책과 보안 제약조건도 함께 살펴본다. 그리고 3장에서 다단계 보안 지식베이스 관리시스템에 대해 서술하고, 4장에서 결론 및 추후 연구과제를 제시한다.

2. 데이타베이스 보안

2.1 보안 정책

다단계 보안 데이타베이스 관리시스템에 대한 보안 정책(security policy)에서 설명되어야 할 사항은 강제적 접근, 문맥, 내용, 시간에 의한 보안등급, 함수적 조작, 집단화, 추론, 보안등급 강하, 임의적 접근(discretionary access), 무결성 등이다.

강제적 접근 제어에서는 사용자가 자신의

권한등급에 따라 데이타를 접근하며, 내용기반 보안등급은 데이타 내용에 따라 데이타에 보안등급을 할당한다. 문맥기반 보안등급은 검색될 데이타의 "특정문맥에 따라 데이타에 보안등급을 할당하는 것이다. 시간에 의한 보안등급은 외부조건을 의미하며 "비행 목적지는 출발 시각까지 보안사항이다"는 것과 같은 것이다. 데이타의 함수적 조작은 개수, 합계, 평균 등과 같은 함수와 관련이 있다. 집단화 데이타의 보안등급에서 집단화를 구성하는 개개 원소의 보안등급은 서로 달라야 한다. 낮은 보안등급의 데이타들로부터 더 높은 보안등급의 데이타를 추론할 때 추론 위반이 발생한다. 보안등급 강하는 데이타의 보안등급을 낮추는 과정이다. 임의적 접근제어 메카니즘에서는 자신이 생성한 데이타에 대한 접근권한을 다른 사용자에게 넘겨 줄 수 있다. 무결성 제어는 데이타가 일관성 있고 올바르다는 것을 보증한다.

아래에 설명될 보안정책은 위에서 설명한 것의 일부가 될 것이다. 왜냐 하면, 특정 보안등급의 사용자는 자신 이하의 보안등급 정보를 접근한다는 것을 보증하는 것이 주된 목적이기 때문이다. 그러므로 임의적 접근 제어와 무결성은 이 정책에서 설명되지 않는다. 따라서 보안정책은 다음과 같이 정의할 수 있다.

① 모든 사용자는 최대 보안등급을 부여받는다. 사용자들은 최대 보안등급 이하인 보안등급으로 로그할 수 있다. 사용자가 로그한 보안등급으로 사용자의 행위를 주체가 수행한다.
② 객체는 데이타베이스에 있는 데이타이다. 데이타의 문맥, 내용, 집단화, 시간에 근거해서 데이타에 보안등급이 부여된다.
③ 주체의 보안등급이 객체의 보안등급 이상일 때만 주체는 객체를 판독한다.
④ 주체의 보안등급이 객체의 보안등급 이하일 때만 주체는 객체를 기록한다.
⑤ 어떤 주체가 전에 응답된 해답을 결합하여 자신의 보안등급 이상의 데이타를 연역할 수 있다면 그런 해답은 주체에게 양도(release)되지 않아야 한다.

하나의 질의 응답이 어떤 주체에게 양도되었을 때, 그 주체 보안등급 이상의 모든 주체는 그 질의 응답을 판독할 수 있다고 가정한다. 위의 ③과 ④는 대부분의 TCB(Trusted Computing Base)에서 사용되는 BLP(Bell-LaPadula) 정책의 단순성질(simple property)과 *-성질(star- property)이며, ⑤는 참고문헌 [6]에서 설명된 것과 같은 추론 문제의 변형이다[5].

2.2 보안 제약조건

위에서 설명된 보안 정책을 구현하는 메카니즘은 분류규칙(classification rule)이라는 보안 제약조건[7,8]이다. 보안 제약조건은 강력한 분류 정책의 토대가 된다. 왜냐 하면 데이타의 어떤 부분 집합이라도 정적으로나 동적으로 보안등급을 할당할 수 있기 때문이다.

단순 제약조건은 전체 데이타베이스, 릴레이션, 속성의 분류이다. 내용기반 제약조건은 튜플이나 원소 값을 분류한다. 문맥기반 제약조건은 데이타 간의 관련성을 분류한다. 하나의 속성에 합계, 평균, 개수와 같은 함수를 적용한 결과의 분류 등급은 원래 데이타의 분류 등급과 다르게 할당될 수 있다. 마지막으로 데이타의 분류 등급은 시간, 문맥, 내용의 변화에 따라 동적으로 바뀔 수 있다.

제약조건은 데이타 사양과 등급 분류로 구성된다. 데이타 사양은 관계대수를 사용하여 데이타베이스의 부분집합을 정의하고, 등급 분류는 이 부분집합의 보안등급을 정의한다[9]. 예를 들면 릴레이션 고용인(주민등록번호, 이름, 봉급)으로 구성된 데이타베이스를 생각해

보자. 릴레이션에서 밑줄은 키를 의미한다. 2,000,000원 이상인 소득자의 모든 이름을 S 등급으로 분류하는 내용기반 제약조건은 보안등급(PROJECT[이름](SELECT[봉급 > 2000000] 고용인)) = S 이다. 그리고 모든 이름과 봉급을 함께 취급하여 S 등급으로 분류하는 문맥기반 제약조건은 보안등급[PROJECT[이름, 봉급] 고용인) = S로 표현 할 수 있다. 모든 이름과 봉급 각각을 S 등급으로 분류하는 단순 제약조건은 보안등급(PROJECT[이름] 고용인) = S 그리고 보안등급(PROJECT[봉급] 고용인) = S 으로 표현된다. 여기서 SELECT와 PROJECT는 관계 대수 연산자이다.

메타 데이타나 제약조건 자체에 대해서도 보안 제약조건을 적용할 수 있지만 본 논문에서는 언급하지 않을 것이다. 보안 제약조건은 스키마 조작 연산, 질의 연산, 갱신 연산에서 사용된다. 여기서 갱신 연산에 대한 논의는 하지 않고 나머지 것들에 대해서만 언급할 것이다. 스키마를 조작 연산할 때의 보안 제약조건은 특정 릴레이션을 저장하고 있는 화일의 보안등급을 결정한다. 화일은 하나의 보안등급을 갖는다고 가정하자. 그러면 다단계 릴레이션에서 서로 다른 보안등급을 갖는 데이타는 하나 이상의 화일에 저장된다.

예를 들면 봉급이 2,000,000원 이상인 이름을 S 등급으로 하는 내용기반 제약조건이 실행된다면 릴레이션 고용인은 두 화일에 저장될 것이다. 봉급이 2,000,000원 이상인 튜플들은 S 등급 화일에 저장될 것이고 나머지 튜플들은 U 등급 화일에 저장될 것이다. 이름과 봉급 각각의 속성은 U 등급이지만 묶어서는 S 등급으로 하는 문맥기반 제약조건이 실행된다면 주민등록번호, 이름, 봉급 각각을 서로 다른 U 등급 화일에 저장하는 것이다. 이 의미는 U 등급 주체가 고용인의 이름과 봉급을 얻지 못하도록 보안제어가 실행되어야 한다는 것을 뜻한다. 즉, 이름이 U 등급 사용자에 의해 판독된 후 동일한 사용자의 행위를 수행하는 주체가 봉급 화일을 개방할 수 없도록 보안제어가 실행될 수 있다는 것이다.

질의 처리에서 보안 제약조건은 질의를 수정하는데 사용된다. 그래서 수정 질의가 제출되었을 때 생성된 해답의 보안등급은 질의한 주체의 보안등급 이하일 것이다. 이와 같은 질의 수정 기법의 변형이 다른 데이타베이스 문제점을 해결하기 위해 과거에 제안되었다[10]. 이런 기법을 간단한 예로 설명하겠다. U 등급 사용자가 고용인의 모든 이름을 검색하는 질의를 하고 봉급이 5,000,000원 이상인 고용인 이름을 S 등급으로 하는 내용기반 제약 조건이 실행된다고 가정하자. 그러면 봉급이 5,000,000원 이하인 모든 이름을 검색하기 위해 질의가 수정된다. 이런 질의 수정 알고리즘의 정형화된 설명은 참고문헌 [8]에 나와 있다. S 등급 사용자가 같은 질의를 한다면 어떤 질의 수정도 수행되지 않는다. 대신에 두 화일에서 튜플이 판독되어 해답을 얻기 위해 합쳐진다.

3. 다단계 보안 지식베이스 관리시스템

3.1 지식베이스의 구성

지식베이스는 명시적 사실과 추론 엔진이 새로운 정보를 연역하게 하는 규칙들로 구성된다. 명시적 사실들은 데이타베이스를 형성한다. 즉, 지식베이스는 데이타베이스와 규칙 베이스로 구성된다. 이런 스킴(scheme)은 지식베이스 관리시스템에서 보안성 문제의 이해에 도움을 줄뿐만 아니라 데이타베이스 관리시스템에서 추론 문제를 서술하기 위한 토대를 마련해 준다. 이것은 데이타베이스 관리시스템의 보안성 문제와 지식베이스 관리시스템의 보안성 문제 사이의 연계를 형성한다.

데이타베이스는 관계형 모델을 사용하고 규칙 베이스는 혼절(Horm-clause)논리 프로그래

밍 문장으로 구성된다고 가정한다. 이런 선택의 이유는 관계형 데이타베이스와 혼절 논리 프로그래밍 시스템 사이의 관련성 때문이다. 즉, 모든 관계형 데이타베이스는 혼절 논리 프로그래밍 시스템이다. 데이타베이스 보안성에 대한 논의는 관계형 모델에 집중한다. 또한 규칙 베이스가 혼절 논리 프로그래밍 문장이라는 데는 이론의 여지가 없다. 혼절 논리가 제 1계 논리를 완전히 표현할 수는 없지만 우리가 표현 하고자 하는 많은 규칙과 제약조건들을 혼절 논리의 일부로도 표현할 수 있다. 그리고 혼절 논리 프로그래밍 시스템에서 사용되는 추론 메카니즘인 분해 원칙은 완전하다. 그러므로 그런 메카니즘은 추론에 의한 보안성 위반을 탐지하는데 사용된다.

지식베이스의 규칙 베이스 구성은 보안 제약조건, 각 보안등급에 대한 환경, 무결성 제약조건, 추론 규칙, 실세계 정보 등이다. 보안 제약조건은 2장에서 설명된 분류 규칙이다. 이들 제약조건들은 데이타베이스에 있는 데이타와 규칙 베이스에 있는 규칙들에 대해서 실행되며, 보안등급과 관련된 환경은 그 보안등급으로 분류된다. 예를 들면, S 등급의 환경은 S 등급으로 분류된다는 것이다. 무결성 제약조건은 데이타 값이나 속성들 사이의 관련성에 적용될 제약조건이며, 추론 규칙은 암시적 데이타를 연역하는데 사용된다. 실세계 정보는 데이타베이스의 일부가 아닌 사실들이다.

3.2 지식베이스 관리시스템에서 질의어 처리

보안 지식베이스 관리시스템의 구성도는 (그림 1)과 같다. 질의어는 혼절 문장으로 기술되며, 외부 주체와 지식베이스 관리시스템 사이의 인터페이스인 사용자 인터페이스 관리자는 질의어를 받아들여 그것을 요청 처리기에게 넘겨준다. 요청 처리기의 기능은 다음과 같다.

① 규칙 베이스 조사만으로 질의어가 해답되어 지는가 혹은 데이타베이스를 접근해야 하는지를 결정한다. 데이타베이스를 접근하기 전에 질의어가 수정되어야 되는 경우가 있을 수 있다.
② 규칙 베이스만을 조사함으로써 얻어진 해답들을 결합한다.
③ 데이타베이스를 접근하기 전에 질의어가 수정되어야 할 필요성이 있다면 질의어 수정을 한다.

추론 엔진은 추론 규칙을 적용하거나 질의어를 처리하는 동안 기존 정보에서 새로운 정보를 연역하며, 규칙들은 단일 보안등급 화일에 저장되어 있다. 더욱이 TCB가 수행하는 BLP 정책은 낮은 보안등급의 주체가 더 높은 보안등급의 화일을 판독하지 못하게 한다. 그러나 추론에 의한 보안성 위반은 이 단계에서 탐지되지 않는다. 요청 처리기의 기능은 보안성과 밀접한 관계가 없으며, 보안 제약조건과 환경은 이 단계에서 조사되지 않는다. 요청 처리기의 중간 결과는 다음의 경우로 나누어진다.

① 중간 결과가 없는 경우
② 규칙 베이스에서 생성된 응답인 경우
③ 원래의 질의어 또는 데이타베이스 관리 시스템이 처리할 수정된 질의어인 경우

데이타베이스 관리시스템이 질의어를 처리하기 전에 먼저 적당한 관계형 질의어로 변환되어 데이타베이스 관리시스템에 의해 처리된다. 데이타베이스는 하나 혹은 그 이상의 단일 보안등급 화일에 저장되고 BLP 정책에 의해 화일들의 접근이 제어된다. 데이타베이스 관리시스템이 생성한 해답은 적당한 형식으로 변환되어 응답 처리기로 송신된다. 뿐만 아니라 해답을 만들어 내는데 사용된 릴레이션, 속성, 화일들에 대한 정보 역시 응답 처리기로 보내

진다. 유사하게 요청 처리기는 생성할 해답과 해답을 만들어 내는데 사용할 규칙과 화일에 관한 정보를 응답 처리기로 보내며, 응답 처리기는 두 해답을 결합한다. 사용자가 제시한 질의어는 응답 처리기로 전달되는데 이때 응답 처리기는 생성될 해답이 의미가 있는지를 결정할 수 있다.

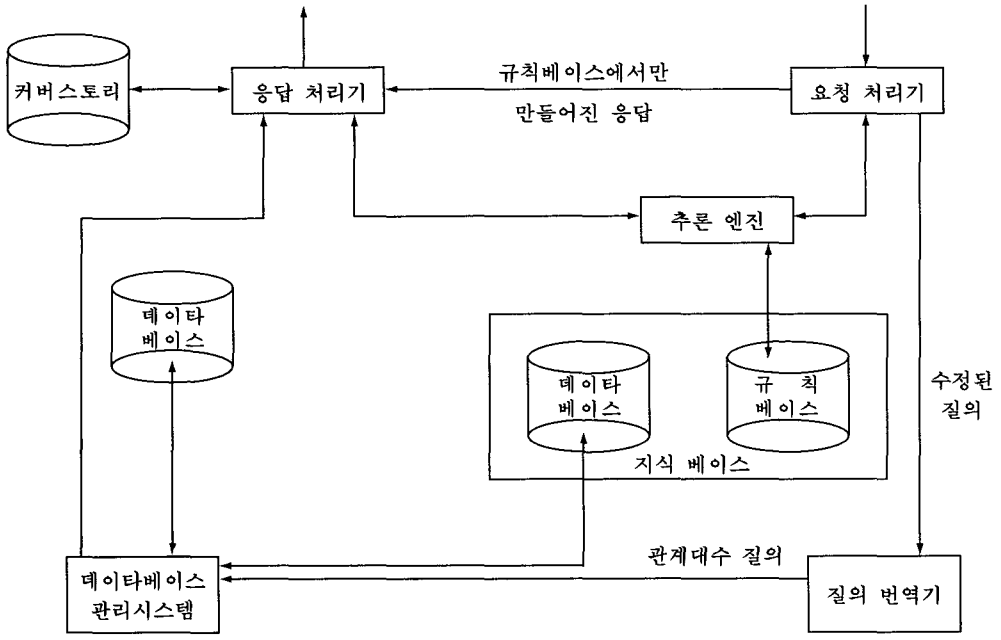

그림 1 보안 지식 베이스 관리 시스템의 구성도

응답 처리기는 보안성에 대한 중요한 기능이 있다. 요청 주체에게 해답을 줄 것인가를 결정하기 위해서 보안 제약조건과 환경조건이 조사되는 것은 바로 이 시점이다. 다른 구성요소가 응답 처리기로 전달한 정보는 반드시 올바른 것이어야 한다. 그러므로 이런 전달 기능은 역시 보안성에 결정적 영향을 미친다.

이제까지의 전체 처리는 질의를 요청한 주체의 보안등급에서 이루어 졌다. 그러나 어떤 해답이 특정 보안등급으로 양도되었다면 추론에 의한 보안 위반이 발생하는지를 결정하기 위해 그 보안등급보다 더 높은 보안등급의 모든 환경이 조사되어야 한다. 그러나 BLP 정책에서는 주체의 보안등급보다 더 높은 보안등급의 환경이 판독 연산을 위해 접근하는 것을 허용하지 않을 것이다. 그러므로 설계에서도 각 환경은 환경 보안등급으로 서버동작을 한다. 한 환경이 판독되어야 할 때 메세지가 이 서버에 보내지며, 서버는 요구 주체의 보안등급 이상에서 동작할 것이다. 서버는 환경을 조사하고 해답이 양도될 때 추론에 의한 어떤 보안 위반이 발생하는지를 결정하며, 연역은 추론엔진이 수행한다. 그런 후 적절한 메세지가 초기 메세지를 발원한 주체에게 보내질 것이다. 이것은 하향 기록 연산이 될 수도 있으므로 신뢰성이 있어야만 한다. 어떤 보안 위반도 없다면

해답은 요구 주체에게 양도되고, 그렇지 않다면 양도되지 않을 것이다.

3.3 예제

앞에서 설명한 지식베이스 관리시스템에 의해 질의가 처리되는 방법을 예제를 통해 살펴보자.

〈 예제 1 〉 규칙 베이스가 아래와 같다고 가정하자.

[규칙1] 이름(X) :- 고용인(X, Y, Z)

[규칙2] 봉급(Y) :- 고용인(X, Y, Z)

[규칙3] 주민등록번호(Z) :- 고용인(X, Y, Z)

[규칙4] 보안등급(X, Secret) : 고용인(X, Y, Z) ∧ GREATER(Y, 8000000)

[규칙5] 중견고용인(X) :- 고용인(X, Y, Z) ∧ GREATER(Y, 5000000)

[규칙6] 중견고용인(신이언).

여기서 규칙1, 규칙2, 규칙3은 무결성 제약조건인데 이는 고용인(X, Y, Z)이 참일 때, X는 이름, Y는 봉급, Z는 고용인의 주민등록번호를 나타낸다. 규칙4는 8,000,000 이상 소득의 모든 고용인 이름을 S 보안등급으로 분류하는 내용기반 제약조건이다. 규칙5에서는 5,000,000 이상 소득의 고용인은 중견고용인이라는 추론규칙이다. 규칙6에서는 신이언이 중견고용인이라는 것이다. 이 모든 규칙들은 U 보안등급이라고 가정하고, 데이타베이스는 다음과 같은 릴레이션 고용인의 튜플들로 구성되어 있다고 하자.

튜플1 : (홍길동, 6000000, 11)

튜플2 : (서재일, 3000000, 22)

튜플3 : (김영재, 9000000, 33)

튜플4 : (이일등, 10000000, 44)

튜플5 : (신 설, 2000000, 55)

튜플3과 튜플4는 S 보안등급 화일에 저장될 것이고, 나머지 튜플들은 U 보안등급 화일에 저장될 것이다. 만약 U 보안등급 사용자가 모든 중견고용인의 이름을 검색하는 질의를 한다면 그 질의는 '중견고용인(X).' 형태일 것이다. 요청 처리기는 먼저 질의를 부정(← 중견고용인(X).) 할 것이며, 부정된 질의는 규칙들로 분해된다. 요청 처리기의 출력은 신이언이고 역시 "Y, Z(고용인(X, Y, Z) ∧ GREATER(Y, 5000000))." 과 같은 수정 질의이며, 이 수정 질의는 관계대수와 같은 관계 언어로 변환된다. 동치 관계대수 형태는 "PROJECT[이름](SELECT[봉급 〉 5000000] 고용인)." 이다.

데이타베이스 관리시스템은 이 질의를 처리할 것이다. U 보안등급 주체는 U등급 화일을 접근하여 판독만 할 수 있다. 그러므로 이 질의가 생성한 응답은 리스트(홍길동)이다. 신이언, 홍길동 그리고 질의를 처리하는데 사용된 릴레이션, 규칙, 화일에 관한 정보와 질의 자체도 응답 처리기로 보내진다. 응답 처리기는 U 보안등급 이상의 모든 환경을 조사해서 양도될 리스트 (신이언, 홍길동)가 어떤 보안 위반을 발생시키는가를 알아본다. 이 예제에서 환경이 초기에는 아무 것도 없다고 가정하였으며 문맥 혹은 집단화 제약조건이 없을 때, U 보안등급의 환경에 이 리스트를 양도하는 것은 어떤 보안 위반도 발생하지 않을 것이다. 그러므로 리스트 (신이언, 홍길동)이 해답이 된다. 그리고 아래의 규칙이 U 보안등급의 환경에 첨가될 것이다.

[규칙6] 중견고용인(신이언).

[규칙7] 중견고용인(홍길동).

그리고 다음 규칙이 규칙 베이스에 삽입될 것이다.

[규칙8] 양도(신이언, Unclassified) :- 중견고용인(신이언)

[규칙9] 양도(홍길동, Unclassified) :- 중견고용인(홍길동)

〈 예제 2 〉 규칙 베이스가 아래 규칙들로 구성되어 있다고 하자.

[규칙1] 이름(X) :- 고용인(X, Y, Z)

[규칙2] 봉급(Y) :- 고용인(X, Y, Z)

[규칙3] 주민등록번호(Z) :- 고용인(X, Y, Z)

[규칙4] 보안등급(X, Secret) :- 고용인(X, Y, Z) ∧ 양도(Y, Unclassified)

[규칙5] 보안등급(Y, Secret) :- 고용인(X, Y, Z) ∧ 양도(X, Unclassified)

위에서 규칙1, 규칙2, 규칙3은 예제1과 같고 규칙4와 규칙5는 고용인의 이름과 봉급을 함께 S 보안등급으로 하는 문맥기반 제약조건의 변형이다. 즉, 일단 이름이 양도되면 대응 봉급은 S 보안등급이다. 유사하게 봉급이 일단 양도되면 대응 이름은 S 보안등급이다. 데이타베이스는 예제1과 같다. 데이타베이스 관리시스템이 보안성과 일관성을 유지할 수 있도록 하기 위해서 릴레이션 고용인은 3개(이름, 봉급, 주민등록번호)의 U 보안등급 화일에 저장된다. 튜플 식별자가 화일에 있는 각 원소와 연관되어 있어서 이름, 봉급, 주민등록번호는 서로 연관되어 질 수 있다.

만약 U 등급의 사용자가 두 개의 질의(이름 검색, 봉급 검색)를 한다고 가정하자. 이름 검색 질의 처리는 예제1과 유사하다. 모든 U 보안등급의 이름이 질의한 U 등급 사용자에게 양도되고, U 보안등급 환경은 양도된 모든 이름들을 삽입함으로써 갱신되어, 다음 규칙이 삽입될 것이다.

[규칙6] 양도(X, Unclassified) :- 고용인(X, Y, Z)

이제 모든 봉급을 검색하는 질의가 처리되고, 어떤 질의 수정도 요청 처리기에 의해 수행되지 않는다. 다시 말해서 질의는 관계대수로 변환되고 데이타베이스 관리시스템에 의해 처리된다. 그리고 관련된 화일 릴레이션에 대한 정보와 봉급값이 응답 처리기로 송신되어 U 보안등급 환경과 규칙1에서 규칙6까지를 검사함으로써 봉급값이 S 등급이라는 것을 결정할 것이다. 그러므로 봉급값은 사용자에게 반환되지 않을 것이다. 이 때 U 등급의 사용자에게 아무런 봉급값을 반환하지 않는다면 그 사용자에게 어떤 중요한 정보가 있다는 사실이 노출되게 마련이고, 사용자는 어떤 방법으로든지 해답을 찾으려고 할 것이다. 이를 방지하기 위해 커버 스토리 데이타베이스에 적절한 가상의 데이타를 저장해 놓고 이와 같은 현상이 발생했을 경우에 질의한 사용자의 보안등급에 맞는 정보를 해답해 주는 것이 훨씬 보안성 면에서 안전하다.

사용자가 이름과 봉급을 동시에 요청하면 이름 화일과 봉급 화일이 개방되고 판독될 것이다. 그러나 응답 처리기는 이름과 봉급이 양도될 수 있는 지를 검사해야 한다. 먼저 이름이 양도된다는 사실을 삽입함으로써 규칙 베이스를 임시적으로 갱신한 후 봉급값이 양도될 수 있는지를 검사해야 한다. 앞의 예제에서는 두 가지 경우 모두 양도할 수 없다. 그러므로 규칙 베이스의 갱신은 완료되지 않고 커버 스토리 데이타베이스에 있는 적절한 수준의 유사한 정보를 사용자에게 반환하면 된다.

4. 결 론

본 논문은 지식베이스 관리시스템에서 보안

성 첨가에 대한 연구이다. 보안 제약조건과 보안 정책을 설명하고 질의 처리를 위한 구성도를 설계하였다. 보안 제약조건과 보안정책은 일반 데이타베이스 관리시스템과 유사하며, 질의 처리에서는 어떤 데이타와 지식에 접근 권한이 없는 사용자에게 아무런 응답을 주지 않는 대신에 가상의 데이타와 지식을 응답해 주는 커버 스토리 개념을 도입하여 보안성을 유지할 수 있도록 하였다. 커버 스토리 개념은 비권한 사용자가 가상의 정보를 진정한 값으로 인식하도록 하여, 비권한 사용자가 아무런 값을 보지 않는 것보다 보안성 면에서 훨씬 안전하다. 이에 대한 간단한 예제로써 질의처리 과정을 보여 주었다.

본 논문의 질의 처리기 설계에서는 데이타베이스에 있는 데이타와 규칙 베이스에 있는 규칙들은 서술된 보안 제약조건에 의해서 단일 보안등급 화일에 저장된다고 가정하였다. 그러나 규칙과 릴레이션들의 분할 방법, 그리고 지식베이스 관리시스템에서 갱신기의 설계는 추후 연구과제이다.

참 고 문 헌

[1] T.F. Lunt and M. B. Thuraisingham, "Security in large AI systems", AAAI Conference Workshop on Databases in Large AI Systems Proceedings, 1988.

[2] T. Berson and T.F. Lunt, "Multilevel security in knowledge-based systems", IEEE Symposium on Security and Privacy Proceedings, pp.235～242, 1987.

[3] M.B. Thuraisingham, "Towards the design of a secure data/knowledge base management system", Data & Knowledge Engineering 5, North-Holland, pp.59～72, 1990.

[4] T.D. Garvey and T.F. Lunt, "Cover Stories for Database Security", DATABASE SECURITY, V : Status and Prospects, North-Holland, pp.363 ～ 380, 1992

[5] D.E. Bell and L.J. La Padula, "Secure Computer System : Unified Exposition and Multics Interpretation", Tech. report MTR-2997, MITRE Corporation, 1975.

[6] M. Morgenstern, "Security and inference in multilevel database and Kowledge-based systems", ACM SIGMOD Conference Proceedings, pp.357～373, 1987.

[7] D.E. Denning, S.K. Akl, M. Morgenstern, P.G. Neumann, R.R. Schell and M. Heckman, "Views for multilevel database security", IEEE Symposium on Security and Privacy Proceedings, pp.156～172., 1986

[8] P.A. Dwyer, G. Jelatis and M.B. Thuraisingham, "Multilevel security in Database Management Systems", Computers and Security Vol. 6, No. 3, pp.252～260, 1987.

[9] J.D. Ullman, Principles of Database Systems, Computer Science Press, 1982.

[10] M. Stonegraker, " Implementation on Integrity Constraints and Views by Query Modification", ACM SIGMOD Conference Proceedings, 1975.

□ 著者紹介

조 일 래

1984년 전남대학교 계산통계학과 졸업
1986년 전남대학교 대학원 계산통계학과 이학석사
1993년 전남대학교 대학원 계산통계학과 박사과정 수료
1989년 ~ 현재 순천공업전문대학 전자계산과 조교수

※ 관심분야 : 데이타 마이닝, 이력 데이타베이스, 데이타베이스 보안

김 원 중

1987년 전남대학교 계산통계학과 졸업
1989년 전남대학교 대학원 계산통계학과 이학석사
1991년 8월 전남대학교 대학원 계산통계학과 이학박사
1992년 3월 ~ 현재 순천대학교 전자계산학과 조교수

※ 관심분야 : 소프트웨어 공학, 데이터 모델링, 객체 지향 시스템 등

심 갑 식

1985년 전남대학교 계산통계학과 졸업
1987년 전남대학교 대학원 계산통계학과 이학석사
1993년 전남대학교 대학원 전산통계학과 이학박사
1993년 ~ 현재 진주산업대학교 교양과정부 조교수

※ 관심분야 : 데이타베이스 보안, 연역 데이타베이스, 객체지향 데이타베이스