韓國컴퓨터情報學會 論文誌
第14卷 第6號, 2009. 6.

2009-14-6-3-3

비밀성과 무결성을 보장하는 격자개념의 역할그래프 보안 모델

최 은 복*

A Lattice-Based Role Graph Security Model ensuring Confidentiality and Integrity

Eun-Bok Choi *

요 약

본 논문에서는 정보의 중요도나 관련성의 정보에 기반한 퍼지함수를 적용하여 강제적 접근통제정책의 비밀성과 무결성을 보장하였으며, 보안등급을 이용하여 접근권한의 흐름을 통제할 수 있는 흐름정책과 역할그래프 생성 알고리즘을 제시하여 상속특성으로 인한 권한남용문제를 해결하였다. 또한, 상업적인 환경에 적용이 가능하도록 정보특성별로 역할을 그룹핑하여 역할계층을 구성함으로써 새로운 역할을 추가하는 것이 용이하여 다단계 보안시스템에서도 효과적으로 접근통제를 할 수 있을 뿐만 아니라 대규모 보안시스템으로 확장할 수 있는 장점을 갖는다.

Abstract

In this paper, this model ensures confidentiality and integrity of mandatory access cotrol policy which based on fuzzy function with importance of information. And it solves authorization abuse problem through role graph creation algorithm and flowing policy that security grade is applied. Because this model composes role hierarchy which bind similar role concept to apply to commercial environment, it has expansile advantage by large scale security system as well as is easy that add new role.

▸ Keyword : 격자모델(Lattice Model), 접근통제(Access Control), 역할그래프(Role Graph)

• 제1저자 : 최은복
• 투고일 : 2009. 05. 15, 심사일 : 2009. 05. 19, 게재확정일 : 2009. 06. 09.
* 전주대학교 미디어정보학부 교수

Ⅰ. 서 론

오늘날 컴퓨터와 정보통신의 결합으로 구성된 유비쿼터스 네트워크 환경에서 정보시스템은 의사결정에 필요한 정확하고 다양한 정보를 위치와 시간에 관계없이 접근하는 것이 훨씬 쉬워졌다. 이러한 정보시스템에 존재하는 정보자원에 대한 접근은 사용자의 기본적인 활동이며 사용자의 자원에 대한 접근을 효율적으로 통제하는 것은 보안기술의 가장 중요한 영역이다.

그러나 정보 시스템은 사용자들에게 정보자원을 제공하는 과정에서 사용자들의 무책임한 자원 공유와 불법적인 자원접근으로 보안문제들이 발생되고 있는데, 이러한 보안문제를 해결하기 위해서는 정당한 접근권한을 소유한 사용자만이 규정된 절차에 따라 자원을 활용할 수 있도록 접근을 통제하는 방안이 필요하다. 이러한 이유로 1985년 미 국방성에서는 컴퓨터 보안 평가 지침서(Trust Computer System Evaluation Criteria : TCSEC)이라는 정보 보호 규정을 제정하였는데, 여기에 강제적 접근통제와 임의적 접근통제에 대한 규정내용이 명시되어 있다[1].

강제적 접근통제 모델중 BLP모델은 정보 흐름을 상향흐름에 초점을 맞춤으로서 정보의 보안성에 치우치므로 군대와 같은 제한적인 환경에만 적용되는 단점을 갖고 있으며 Biba 모델은 비밀성보다는 무결성에 초점을 맞춤으로서 과다한 정보 제공으로 인한 정보 관리에 문제점을 갖고 있다. 또한, 임의적 접근통제의 역할기반 접근통제모델의 경우 역할계층에 의한 상속 특성으로 상위 역할을 수행하는 사용자의 경우 하위 역할의 사용자의 모든 역할과 권한을 상속받음으로서 야기되는 권한 남용 등의 문제점이 대두되고 있다.

본 논문에서는 이와 같은 기존의 모델에서 제기되는 비밀성과 무결성문제를 해결하기 위하여 중요도 퍼지 함수인 $H(N, \alpha, \beta) = \alpha T(N) - \beta I(N)$을 계산하여 H값이 양수인경우에는 비밀성 기반 보안흐름정책을 적용하고 음수인 경우에는 무결성 기반 보안흐름정책을 적용하도록 하였다. 특히, TCSEC에 명시된 등급에 기반하여 주체나 객체의 비밀성 및 무결성 등급별 정수값을 적용하였으며, 정보의 비밀성과 무결성에 대한 α, β값을 보안관리자에 의해 적용하도록 함으로써 함수값의 신뢰도를 높였다. 또한, 다양한 보안 요구사항과 정책들이 반영된 격자개념의 역할그래프 보안모델에서 보안등급(주체/객체등급, 주체/객체범위)을 이용하여 접근권한의 흐름을 통제할 수 있는 흐름정책과 역할그래프 생성 알고리즘을 제시하여 상속특성으로 인한 권한남용문제를 해결하였다. 그리고 상업적인 환경에 적용이 가능하도록 정보특성별로 역할을 그룹핑하여 역할계층을 구성함으로써 새로운 역할을 추가하는 것이 용이하여 다단계 보안시스템에서도 효과적으로 접근통제를 할 수 있을 뿐만 아니라 대규모 보안시스템으로 확장할 수 있는 장점을 갖는다.

Ⅱ. 관련연구

1. 접근통제 정책

강제적 접근통제 정책은 군사환경이나 매우 제한적인 환경에서 제한된 수의 보안 관리자들에 의해 일정한 규칙에 따라 사용자의 정보에 대한 접근을 통제하고, 보안등급이 결정되는 정책으로 규칙기반(Rule-based)기법과 관리기반(Administrative-based) 기법이 통제기법으로 이용되며, 대표적인 모델로는 비밀성을 중요시하는 BLP(Bell-LaPadula) 모델과 정보의 무결성을 강조하는 Biba 모델이 있다[2].

반면에 임의적 접근통제 정책에서는 정보의 소유자들이 임의적으로 접근권한을 다른 사용자에게 위임할 수 있게 하는 정책으로, 신분기반(Identity-based)기법과 사용자 기반(User-based)기법이 접근통제 기법으로 이용되며, 접근을 요청한 주체가 객체에 대한 권한을 자율적으로 다른 주체에게 권한을 부여하거나 철회할 수 있다. 이 정책에는 접근통제행렬(Access Control Matrix), 접근통제리스트(Access Control List), 능력리스트(Capability List) 등이 있다[3].

비 임의적 접근통제 정책은 상업적인 환경에서는 기업마다 서로 다른 보안 요구사항과 정책들을 반영해야하기 때문에 강제적 접근통제나 임의적 접근통제만으로 이러한 요구를 만족시킬 수 없기 때문에 제시된 정책으로 역할기반(Role-based) 기법과 격자기반(Lattice-based) 기법이 이용되며, 대표적인 모델인 역할기반 접근통제모델은 주체가 가지는 역할에 따라, 접근할 수 있는 정보가 결정되고 사용할 수 있는 정보의 한계가 결정된다. 그리고 역할과 역할에 대한 권한을 정적으로 부여하므로서 수많은 접근권한을 관리하는데 융통성을 제공한다. 또한 역할이 조직이나 환경에 따라 자연스럽게 생성되고 재구성될 수 있는 유연성을 갖는다[4].

접근통제 시스템에서 역할기반 기법을 적용한 기존의 역할기반 접근통제 모델은 역할, 사용자, 접근권한 할당, 접근권한의 상속성의 관계에 의해 사용자의 자원에 대한 접근을 통제한다. 이때, 하위역할에 할당된 사용자의 모든 접근권한은 상위역할에 할당된 사용자의 접근권한에 상속됨으로서 접근권한의 집중에 의한 기밀성보호가 어렵고 최소권한정책을 위배함으로서 권한의 남용 문제

가 발생한다. 또한 격자기반 기법의 경우 정보의 흐름이 정보가 가지고 있는 기본 특성과 흐름정책에 따라 정보의 권한이 달라진다 [5].

2. 격자모델

Denning의 정보 흐름(FM:Flow Model) 모델은 FM=〈N, P, SC, ⊕, →〉에 의해 정의되어진다[6]. 여기서 N은 객체의 유한집합이며 P는 유한 프로세스 집합(주체 집합), SC는 보안등급 집합, 등급조합 연산자인 ⊕는 결합 및 교환법칙 특성을 갖는 이진 연산자, 흐름 관계인 →는 보안등급의 쌍으로 표현된다. 예로, 등급 A와 B에 대해 A→B는 만약 A등급의 정보가 B등급의 정보로의 흐름을 허가된다면 우리는 A→B로 쓰며, 정보는 A등급에서 B등급으로 흘러간다고 말한다.

모델의 보안 요구조건은 흐름 모델 FM이 만약 연산순서의 수행 관계 →를 침범하는 흐름이 발생하지 않는다면 FM은 안전하다고 정의된다.

다음과 같은 가정하에 〈SC, →, ⊕〉은 유한 격자를 형성한다.

(1) 〈SC, →〉은 부분 순서 집합이다.

(2) SC는 유한하다.

(3) SC는 ∀A□SC, L→A인 하한경계값(lower bound)를 갖는다.

여기에서 ∀A□SC, L→A의 의미는 'SC에 포함되는 모든 보안등급 A는, lower bound L에서 보안등급 A로의 정보흐름 관계→를 갖는다'것을 의미한다.

(4) 등급조합연산자인 ⊕는 SC에서 최소 상한 경계값 연산자(least upper bound operator)이며, 다음과 같은 특성을 갖는다.

(a) $A \rightarrow A \oplus B$ and $B \rightarrow A \oplus B$

(b) $A \rightarrow C$ and $B \rightarrow C \Rightarrow A \oplus B \rightarrow C$

3. 역할기반 접근통제모델(RBAC)

RBAC0는 역할기반 접근통제 정책에서 최소한의 요구조건을 갖는 기본 모델이며 RBAC1은 역할 계층성을 첨가한 개념이다. 반면 RBAC2는 제약조건을 첨가한 모델이며 통합 모델인 RBAC3는 RBAC1과 RBAC2를 통합한 모델이다 [7].

□ 기본모델 - RBAC0

RBAC0는 4가지 개체인 사용자(U), 역할(R), 허가사항(P), 그리고 세션(S)으로 구성된다. 허가사항은 한 개 이상의 객체에 적용되는 접근 모드를 의미하며 이는 권한을 부여하는 양성적 측면을 가진다. 허가사항의 연산은 read, write, execute뿐만 아니라 상업적인 측면에서 추상적인 데이터를 처리할 수 있는 연산인 select, update, delete, debit, credit 등이 있다. 사용자는 역할을 수행하기 위해서는 트랜잭션에 해당하는 세션을 설정한다. 하나의 사용자가 여러 개의 역할을 동시에 수행할 수 있는 일 대 다 구조를 가질 수 있으며 사용자에 의해 자율적으로 생성, 변경, 소멸될 수 있다.

□ 역할 계층성 모델 - RBAC1

계층성은 권한과 책임을 수반하는 구조적 역할이라 할 수 있다. 권한은 단계별로 해당역할을 계층성에 부여하며, 역할

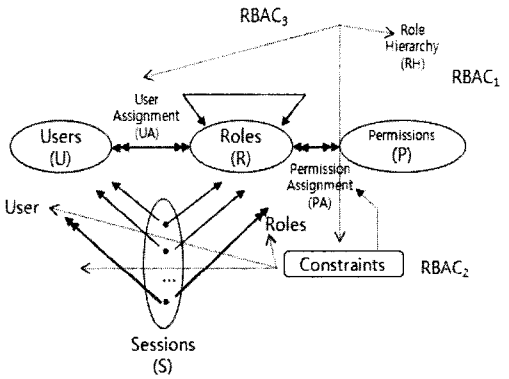

그림 1. 역할기반 접근통제 모델
Fig. 1. Role Based Access Control Model

에 대한 감사 추적시 계층구조를 이용한다. 하위역할은 상위역할에 모든 허가사항을 상속하므로 상위역할은 자신의 허가사항 뿐만 아니라 하위 역할의 허가사항도 포함하게 된다. 때때로 상속성의 범위를 제한할 필요가 있는데, 하위 역할이 상위 역할에 허가사항을 상속할 때 비밀을 요하는 경우에는 사설 비밀 역할(private Role)을 생성하여 상속한다.

□ 제약조건 모델 - RBAC2

가장 일반적인 RBAC의 제약조건은 상호 배타적인 역할(임무분리)이다. 예를 들어 회계관리자와 구매 관리자는 서로 배타적인 관계에 있으므로 임무를 분리시켜야 하는 제약조건을 두어야 한다. 둘째, 사용자가 가질 수 있는 역할의 개수(cardinality)를 제한할 수 있어야 한다. 이는 한 사용자가 수행할 수 있는 최대 역할개수와 최소 역할개수를 정의함을 의미한다. 셋째, 조건의 역할로 한 사용자에게 꼭 필요한 역할은 선결조건으로 부여가 되어야 함을 의미한다. 기타 고려해야 할 사항으로 동적 임무 분리정책은 사용자와 역할이 설정은 되어있으나 세션이 수행될 때는 어느 하나만 수행되도록 해야한다는 것을 의미한다. 또한 세션 제약조건으로, 동시에

수행할 수 있는 사용자의 세션의 수를 제한해야 한다.

□ 통합 모델 - RBAC3

RBAC3 모델은 역할 계층성 모델인 RBAC1과 제약조건 모델인 RBAC2를 결합한 모델이다. 역할 계층 구조에 제약조건이 적용되며 역할 계층은 부분 순서 관계를 갖는다. 단일 시스템에 의한 역할기반 접근통제정책이 아닌 대규모 시스템에서는 역할의 개수가 매우 많아 이를 관리하는 일이 중요하다. 역할기반 접근통제정책의 주요한 장점은 이러한 허가사항 관리를 효율적이고 단순화시킬 수 있다는 점이다.

□ 응용모델 - ARBAC / T-RBAC

행위기반 접근통제(ARBAC)는 워크플로우에 의해서 표현된 공동 작업 환경을 위하여 연구된 것으로 이는 공통 목표를 달성하기 위하여 결합된 활동의 집합으로 정의된다. 강제적접근통제, 임의적 접근통제 및 역할기반 접근통제 모델의 경우는 접근 권한의 부여시점에서 권한이 활성화(activate)되어 임의의 시점에서 사용가능한 반면에 행위기반 접근통제 모델에서는 사용자에 대한 접근권한 할당(access right assignment)과 접근권한 활성화(access right activation)로 분리된다. 어떤 사용자가 워크플로우 내의 과업에 대한 실행권한을 부여 받았다고 하더라도 그 권한의 사용은 워크플로우의 진행상태에 따라 제약을 받는다. 행위기반 접근통제모델은 에플리케이션 레벨 제약을 위한 명세를 제공하고 현실 세계의 무결성 규칙의 구현을 지원한다. 그러나 행위기반 접근통제는 기업 환경에서 워크플로우에 속하지 않는 많은 작업들을 다루지 않고 있어 사용이 제한적이다[8].

과업 역할기반 접근통제 모델(Task-Role-Based Access Control : T-RBAC)은 역할기반 접근통제 모델을 기초로하여 행위기반 접근통제 모델을 통합한 모델이다. 과업 역할기반 접근통제 모델과 역할기반 접근통제 모델의 가장 큰 차이점은 접근권한을 부여하는 방법이다. 역할기반 접근통제에서는 접근권한이 직접 역할에 부여되나, 과업 역할기반 접근통제 모델에서는 접근권한이 그 역할이 수행하는 과업(task)을 통해 부여된다는 점이다. 과업 역할기반 접근통제 모델에서 과업은 3개의 클래스로 분류된다. 클래스 S에 속하는 과업은 계승시킬 수 있으며, 그들의 접근권한은 역할계층에서 더 높은 역할로 상속된다. 클래스 P에 속하는 과업은 단일 역할에 할당 가능한 과업으로 역할계층에서 상위의 역할로 상속되지 않는다. 클래스 W에 속하는 과업은 활동적인 보안 정책으로 워크플로우 메커니즘에 의해서 관리된다. 그래서 과업역할기반 접근통제 모델은 기업환경에 대하여 행위기반 접근통제 모델과 역할기반 접근통제 모델의 제한사항들을 해결한다. 그러나 과업 역할기반 접근통제 모델은 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한하여 최소권한 원칙을 이행할 수 있는 방법을 제공하지 않아 최근의 변화하는 기업 환경에 적용하기에는 무리가 따른다[9,11].

강제적 접근통제 모델중 BLP모델은 권한을 갖지 않은 사용자에게 정보가 흐르는 것을 방지하는 정보의 비밀성을 보장하는데는 효과가 있지만 보안등급이 낮은 주체가 보안등급이 높은 객체를 부당하게 훼손하거나 변경할 우려가 있어 정보의 무결성을 보장하지 못한다. Biba 모델은 비밀성보다는 무결성에 초점을 맞춤으로서 과다한 정보 제공으로 인한 정보 관리에 문제점을 갖고 있다. 또한, 임의적 접근통제의 역할기반 접근통제모델은 사용자들이 수행하는 공통적인 기능들에 기반을 둔 그룹들인 역할로 구성되며 조직이나 환경에 따라 역할이 자연스럽게 생성되고 재구성될 수 있는 유연성을 갖는다. 그렇지만 역할계층의 경우 부분순서 지배관계에 따라 상위역할의 경우에 하위역할의 모든 권한을 상속받으므로 권한간의 충돌 및 남용문제가 발생된다. 또한, 역할을 수행하는 관리자와 객체에 대한 접근통제 방법이 제공되지 않아 정보의 무결성을 해칠 우려가 있다[10].

III. 본 론

1. 격자개념의 역할 그래프 보안 모델

1.1 보안 모델의 특성 정의

본 역할그래프 보안 모델은 등급을 갖는 주체와 객체, 권한특성, 역할 그리고 정보보호의 비밀성, 무결성에 관한 중요도와 관련성의 방법을 반영하여 조직적으로 조합한 새로운 정보보호기능을 기반으로 하는 모델이다.

권한특성은 주체와 객체, 객체에 대한 연산의 집합, 객체의 중요도 퍼지값인 (s, o, m, α, β)으로 구성되는데, s는 주체, o는 객체, m은 주체에 대한 객체의 접근모드, α, β는 정보보호의 비밀성이나 무결성의 중요단계를 기술하는 퍼지값으로 비밀성은 α, 무결성은 β로 기술된다. 만약 이 두 값이 0이나 1인 값을 가지면 중요도가 해당 특성에 대해 무관하거나 완전 관련성을 의미한다. 또한 α=β는 비밀성과 무결성에 대해 동일한 중요도를 의미한다. 또한, α > β는 무결성보다는 비밀성에 더 많은 중요도가 있음을 의미하며 α < β는 비밀성보다는 무결성에 더 많은 중요도가 있음을 의미한다.

역할은 권한특성과 관련되어 명명된 집합인 (r.name, r.pset)

으로 구성되며 r.name은 역할 이름, r.pset은 역할에 대한 권한 특성집합을 의미한다. r.pset은 객체 o와 접근모드집합인 (o, m)으로 구성된다. 역할기반접근통제모델에서 사용자에게 권한부여는 사용자/그룹 권한부여, 역할/역할 권한부여, 역할/권한 권한부여로 나눌 수 있고 이러한 관계를 통해 사용자는 권한의 투명성을 제공받는다. 역할 관계는 is-junior 관계로 표현되는데 부분권한과 공통권한, 증강권한으로 나뉜다. 부분권한은 역할A가 역할B의 부분집합 관계(역할A ⊂ 역할B)의 관계를 갖으며, 공통권한은 역할P와 역할Q의 공통집합인 역할R을 갖는 권한(역할R is 역할P ∩ 역할Q)이며 증강권한은 역할X와 역할Y의 합집합이 역할Z의 부분집합이 되는 권한 [(역할X ∪ 역할Y) ⊂ 역할Z]을 말한다. 역할은 역할 그래프의 한 노드를 구성하는데, 만약 R1.pset ⊆R2.pset이면 R1이 R2의 하위역할이 된다.

본 역할그래프 보안 모델을 구성하기 위해서 다음과 같은 몇가지 전제조건을 정의하였다.

- 하나의 최대역할과 최소역할을 가질 수 있다.
- 주체는 객체의 집합으로 그룹핑된 역할에 배정된다.
- 주체와 객체는 공백객체와 공백주체를 포함한다.

여기에서 공백객체는 보안함수값을 가지지만 객체의 이름만 가지고 있고 정보의 내용이 없는 객체를 공백객체라 정의한다. 예로 보안등급이 부여된 파일을 갖지않는 공백파일이 이에 해당한다. 공백주체는 공백객체와 연관된 주체를 공백주체라 정의한다.

- 최소 역할에서 모든 ri로 가는 경로가 존재하고, 모든 rj에서 최대 역할로 가는 경로가 존재한다.
- 역할 그래프는 비사이클을 형성해야 한다.
- 두 개의 역할 ri 와 rj에 대하여 만약 ri.pset ⊆ rj.pset이면 ri에서 rj로 가는 경로가 반드시 존재한다.
- 비밀성 α값과 무결성 β는 $0 \le \alpha \le 1$, $0 \le \beta \le 1$의 값을 갖는다.
- 중요도 퍼지 함수 H(N, α, β) = αT(N) - βI(N), 여기에서 N은 주체나 객체, T는 비밀성, I는 무결성 등급값, α는 비밀성 중요도, β는 무결성 중요도를 의미한다.
- 등급 값은 T=T(Si)/T(Oj)값, I=I(Si)/I(Oj)으로 정수값을 갖는다.
- 중요도 퍼지함수값은 α * [(T(Si)/T(Oj)] - β * [I(Si)/I(Oj)]으로 계산되며 중요도 퍼지값인 α와 β 그리고 주체 및 객체의 보안등급은 보안관리자에 의해 배정되어 결정된다.

이 논문에서 주체와 객체의 비밀성 및 무결성은 TCSEC에 언급되는 개념을 사용하며 주체 Si의 등급을 SC(Si)라고 표현하며 객체 Oj의 등급은 SC(Oj)라고 표현하고 〈표 1〉에서 그들을 표기하였다.

특히,비밀성보안등급은 TS(Top_Secret)〉S(Scret)〉C(Classified)〉UC(UnClassified)의관계를갖으며무결성보안등급은 C(Crucial)〉VI(VeryImportant)〉I(Important)〉U(Unclassified)의 관계를 갖는다. 또한 비밀성 및 무결성 등급값인 T값과 I값은 TCSEC의 A등급에서 D등급의 7등급을 비밀성/무결성 등급의 4등급에 맞추어 등급별로 정수값을 할당하였다.

표 1. 등급별 정수값
Table 1. value by security grade

보안등급 (비밀성/무결성)	보안등급 설명	비밀성등급 T값	무결성등급 I값	TCSEC 비교
TS/C	인가(검증)된 보호등급	4	4	A 등급
S/VI	효력을 갖는(강제적) 보호등급	3	3	B3,B2, B1 등급
C/I	자율적 보호등급	2	2	C2,C1 등급
UC/U	비보호등급	1	1	D 등급

O′는 실제적인(현실적인) 객체 집합이며 S′은 실제적인 주체 집합이며 SC′은 실제적인 보안등급이며 유한집합이라 가정하자.

정의 1 : 주체 s의 보안등급인 SCs는 다음과 같다.

SCs ={s| s□S′, H(s, α, β) = αT(s) - βI(s) 이며, 이 등급은 상수값을 갖는다.}

여기서 보안등급은 숫자값으로 표현되며 모든 보안등급에 속하는 실제적인 주체에 대해 H(s′, α, β)= H(s, α, β)이다. 수식으로 표현하면 ∀s′□SCs, H(s′, α, β)= H(s, α, β) 이다.

정의 2 : 객체 o의 보안등급(SCo로 표기함)은 다음과 같다.

SCo ={o| o□O′, H(o, α, β) = αT(o) - βI(o) 이며, 이 등급은 상수 값을 갖는다.}

여기서 보안등급은 숫자값으로 표현되며 모든 보안등급에 속하는 실제적인 객체 o′에 대해 H(o′, α, β)= H(o, α, β) 이다. 수식으로 표현하면 ∀o′□SCo, H(o′, α, β)= H(o, α, β) 이다.

그러므로 주체나 객체의 실제적인 보안등급 SC′ ={SCs|s, SCo|o□SC′, SC′={TS/C, S/VI, C/I, UC/U] }중 하나의 값을 갖는다.

정의 3 : 비밀성 기반 읽기 보안 흐름 정책: H(o1, α, β) ≤ H(o2, α, β)를 갖는다면 곧, 비밀성이 중시되는 특성을 갖는다면 주체의 등급이 두 객체중 중요도 퍼지함수 H()값이 높은 o2객체의 등급을 지배하는 경우에 한하여 객체 o1과 o2를 읽을 수 있도록 한다(no-read-up). 이는 주체 자신의 등급보다 더 높은 객체에 대해서는 읽을 수 없도록 함으로써 비밀을 요하는 정보가 노출되는것을 차단하기 위함이다.

read : H(o1, α, β) ≤ H(o2, α, β) → ∀s□S, o1,o2 □O, SCs ≥ max(SCo1, SCo2))

정의 4 : 비밀성 기반 쓰기 보안 흐름 정책: H(o1, α, β) ≤ H(o2, α, β)를 갖는다면 곧, 비밀성이 중시되는 특성을 갖는다면 주체의 등급이 두 객체중 중요도 퍼지함수 H()값이 낮은 o1객체의 등급에 지배되는 경우에 한하여 객체 o1과 o2를 쓸 수 있도록 한다(no-write-down). 이는 주체 자신의 등급보다 더 높은 객체에 대해서는 무단으로 추가하거나 갱신할 수 없도록 함으로써 정보의 무단변경과 혼란을 차단하기 위함이다.

write : H(o1, α, β) ≤ H(o2, α, β) → ∀s□S, o1,o2□O, SCs ≤ min(SCo1, SCo2))

정의 5 : 무결성 기반 읽기 보안 흐름 정책: H(o1, α, β) ≥ H(o2, α, β)를 갖는다면 곧, 무결성이 중시되는 특성을 갖는다면 주체의 등급이 두 객체중 중요도 퍼지함수 H()값이 낮은 o2객체의 등급보다 낮은 경우에 한하여 객체 o1과 o2를 읽을 수 있도록 한다(no-read-down). 이는 주체 자신의 등급보다 더 낮은 객체에 대해서는 읽을 수 없도록 함으로써 신뢰성이 떨어지는 객체의 부당한 객체등급 상향을 막기위함이다.

read : H(o1, α, β) ≥ H(o2, α, β) → ∀s□S, o1,o2 □O, SCs ≤ min(SCo1, SCo2))

정의 6 : 무결성 기반 쓰기 보안 흐름 정책: H(o1, α, β) ≥ H(o2, α, β)를 갖는다면 곧, 무결성이 중시되는 특성을 갖는다면 주체의 등급이 두 객체중 중요도 퍼지함수 H()값이 높은 o1객체의 등급을 지배하는 경우에 한하여 객체 o1과 o2를 쓸 수 있도록 한다(no-write-up).

write : H(o1, α, β) ≥ H(o2, α, β) → ∀s□S, o1,o2□O, SCs ≥ max(SCo1, SCo2))

1.2 사례 연구

〈표 2〉에서처럼 등급별 주체 곧, 보안등급이 배정된 주체인 사용자에 할당된 테이블이 있다고 하자. 등급별 주체에 대해 읽기 및 쓰기 특성에 대한 접근가능 테이블 리스트는 본론의 1.1에서 정의한 비밀성과 무결성 보안 흐름 정책에 의해 기존에 할당된 테이블뿐만 아니라 상속성으로 권한을 물려받는 테이블까지 포함하게 된다〈표 3〉〈표 4〉. 특히, 음영으로 처리된 테이블이 권한상속에 의한 접근가능한 테이블 리스트이다.

표 2. 등급별 주체에 할당된 테이블
Table 2. Table assigned to subject

주체등급	테이블명-(읽기/쓰기)특성등급
STS/C	T1-RTS/C
SS/VI	T2-RS/VI, T3-WS/VI
SC/I	T4-RC/I, T5-WC/I
SUC/U	∅

표 3. 비밀성 기반 접근가능 테이블
Table 3. confidentiality-based accessible table

주체등급	접근가능테이블 리스트
STS	T1-RTS, T2-RS, T4-RC
SSI	T2-RS, T3-WS, T4-RC
SC	T3-WS, T4-RC, T5-WC
SUC	T3-WS, T5-WC

표 4. 무결성 기반 접근가능 테이블
Table 4. Integrity-based accessible table

주체등급	접근가능테이블 리스트
SC	T3-WVI, T5-WI
SVI	T1-RC, T2-RVI, T3-WVI, T5-WI
SI	T1-RC, T2-RVI, T4-RI, T5-WI
SU	T1-RC, T2-RVI, T4-RI

본 모델은 등급을 갖는 주체가 등급이 배정된 객체 테이블을 접근하고 수행하고자 할 때 보안관리자에 의해 명기된 객체의 중요도에 따른 α, β값과 중요도 퍼지 함수인 H(N, α, β) = αT(N) - βI(N)을 계산하여 H값이 양수인 경우에는 〈정의 1〉과 〈정의 2〉의 비밀성 기반 보안흐름정책을 적용하고 음수인 경우에는 〈정의 3〉과 〈정의 4〉의 무결성 기반 보안흐름정책을 적용함으로서 비밀성과 무결성을 모두 보장받는 〈표 3〉과 〈표 4〉를 생성할 수 있다.

표 5. 보안 흐름 정책 알고리즘
Table 5. Security flowing policy algorithm

```
BEGIN
 IF H(N, α, β) > 0 THEN /*비밀성기반정책
  {
   IF L(S) ≥ L(O) THEN
      READ ACCESS SUCCESS;
        ELSEIF L(S) ≤ L(O) THEN
          WRITE ACCESS SUCCESS;
        ELSE ACCESS FAIL;
   ENDIF
   ROLE_GRAPH_CREATION();
     /*비밀성 기반 역할 그래프 생성
    }

 ELSE  /* 무결성 기반 정책
   {
   IF L(S) ≤ L(O) THEN
      READ ACCESS SUCCESS;
       ELSEIF L(S) ≥ L(O) THEN
          WRITE ACCESS SUCCESS;
        ELSE ACCESS FAIL;
    ENDIF
ROLE_GRAPH_CREATION();
   /* 무결성 기반 역할 그래프 생성
   }
ENDIF
END
```

〈표 5〉와 〈표 6〉은 보안 흐름 정책 알고리즘과 역할그래프 생성 알고리즘으로 특정 주체가 테이블에 해당하는 객체에 읽기나 쓰기 권한을 수행하고자 할 경우 중요도 퍼지함수를 계산하여 양수인 경우 정당한 권한을 갖는 주체에게만 정보가 제공되도록하는 비밀성 기반 정책이 적용되고 음수인 경우 정보의 보안성보다는 이용성 측면을 제공하는 환경으로 무결성 기반의 정책이 적용되도록 함으로서 정보의 특성과 중요도에 따라 비밀성과 무결성을 동시에 보장하도록 하였다.

표 6. 역할그래프 생성 알고리즘
Talble 6. Role graph creation algorithm

```
Role_Graph Creation(RG, nx, xSeniors, xJuniors)
{
Input : RG = ⟨ Px, → ⟩
    /*등급 x를 갖는 보안특성 역할 그래프*/
nx : 추가될 보안 특성 노드(단, x는 등급을 의미)
xSeniors : n의 상위 특성
xJuniors : n의 하위 특성

output : 새로운 노드가 추가된 보안특성 역할 그래프로 그래프의 특성은
유지
method:
 Var px, pxi, pxj, pxs : 보안특성테이블;
Begin
 Px : Px ∪ {nx}; /* RG에 새로운 노드 추가 */
  For all pxs ∈ xSeniors DO add the edge nx → pxs;
  For all pxj ∈ xJuniors DO add the edge pxj → nx;
If RG has cycles then abort;
end.
}
```

그래프 생성 알고리즘의 입력값은 역할 그래프, 보안특성과 등급으로 표현되는 새로 추가할 노드 그리고 인접한 상위, 하위 노드로 구성된다. 여기에서 노드는 테이블명과 등급을 갖는 읽기/쓰기 권한특성으로 구성되며, 알고리즘에 의해 생성되는 출력값은 새로운 노드가 추가된 역할 그래프로 기존의 역할 그래프의 특성은 유지되어야 한다. 새로운 노드가 추가되기 위해서는 새로운 노드와 상위노드 그리고 하위노드간의 에지 생성시 사이클이 생성되어서는 안된다.

〈표 2〉, 〈표 3〉, 〈표 4〉와 알고리즘 〈표 5〉, 〈표 6〉에 기반하여 비밀성과 무결성을 보장하는 역할그래프 보안 모델은 다음 〈그림 2〉와 같이 생성될 수 있다. 여기에서 역할은 최소 역할과 최대역할, 그리고 비밀성 기반_역할_그래프(CONF_ROLE_GRAPH)와무결성기반_역할_그래프(INT_ROLE_GRAPH)로 구성되며 비밀성과 무결성 역할 그래프는 각 등급별 주체가 수행가능한 등급별 권한들의 집합으로 구성된다.

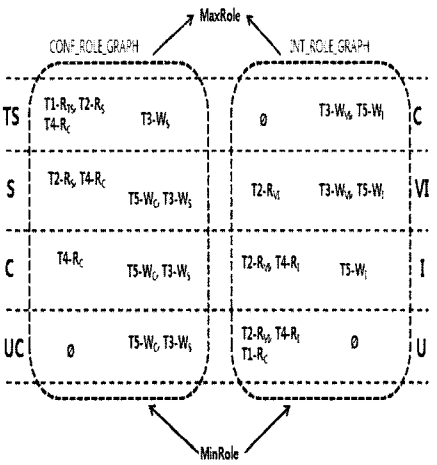

그림 2. 역할 그래프 보안 모델
Fig. 2. Role graph security model

결론적으로 정리하면, 정보보호의 중요한 특성인 비밀성과 무결성은 서로 상충되는 특징으로 인해 별개의 모델로 제시되고 구현되어왔다. 특히, 비밀성에 초점을 맞춘 BLP모델은 정보 흐름을 상향흐름에 초점을 맞춤으로서 군대와 같은 제한적인 환경에만 적용되는 단점을 갖고 있으며 Biba 모델은 비밀성보다는 무결성에 초점을 맞춤으로서 과다한 정보 제공으로 인한 정보 관리에 문제점을 갖고 있었다. 본 논문에서 제시한 보안흐름 정책알고리즘과 역할그래프 생성알고리즘을 통한 역할그래프 보안 모델은 중요도퍼지함수를 적용하여 비밀성과 무결성을 동시에 보장함으로서 정보의 안전성과 상용성을

증대시켰다. 또한 기존의 BLP와 Biba 모델은 보안흐름정책을 주체와 객체의 등급에 의한 격자기반에 의존함으로서 경직된 상하흐름정책에 의존한 반면 본 모델은 역할과 보안등급에 기반한 격자개념을 사용하여 정보흐름정책을 적용함으로서 상업적인 환경에 유연하게 응용할 수 있을 뿐만 아니라 권한간의 충돌 및 남용을 예방할 수 있는 장점을 갖는다.

IV. 결 론

본 논문에서는 강제적 접근통제 정책에서 제기되는 정보의 제한적인 환경에서의 적용문제와 정보관리의 문제점 그리고 역할기반 정책의 하위 역할의 모든 권한을 상위역할이 상속받음으로써 발생되는 권한남용 문제를 해결하고 다양한 보안 요구사항과 정책들을 반영하기 위하여 보안등급을 이용하여 접근권한의 흐름을 통제할 수 있는 보안흐름정책과 역할그래프 생성 알고리즘을 통한 역할그래프 보안모델을 제안하였다.

특히, 정보 중요도 펴지 함수와 주체/객체의 보안등급 비교에 의해서 흐름정책에 합당한 권한만을 상속받도록 함으로써 무분별한 권한남용문제를 해결하였다. 본 모델은 상업적인 환경에 적용이 가능하도록 정보특성별로 역할을 그룹핑한 역할정책을 사용함으로써 새로운 역할의 추가가 용이하여 다단계 보안시스템에서도 효과적으로 접근통제를 할 수 있을 뿐만 아니라 대규모 보안시스템으로 확장할 수 있는 장점을 갖는다.

참고문헌

[1] *http://www.boran.com/security/tcsec.html*

[2] J. Cramption, W. Leung, K. Beznosov, "The Secondary and Approximate Authoriztion Model and Its Application to Bell-LaPadula Policies", Proc. of 11th ACM SACMAT, pp. 111-120, June, 2006.

[3] S. Osborn, R. Sandhu and Q. Munawer, "Configurig Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Polices", ACM Transactions on information and Systems Security, vol.3, no.2, pp. 85-106, 2000.

[4] 김경자, 장태무, "유비쿼터스 환경을 위한 CASA기반의 동적 접근제어 기법", 한국컴퓨터정보학회논문지, 13권 4호, 205-211쪽, 2008.

[5] Vijayalakshmi Atluri and Avigdor Gal, "An authorization model for temporal and derived data : Securing information portals", ACM Trans. Inf. Syst. Secur., vol.5 no.1, pp.63-94, 2002.

[6] D.E. Denning, "A Lattice model of Secure Information Flow", Joural, Commu., ACM, Vol.19, No. 5, pp. 236-243, May, 1976.

[7] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models", COMPUTER SOCIETY, IEEE, pp.38-47, FEB. 1996.

[8] Kaijun Tan, Jason Crampton and Carl A. Gunter, "The Consistency of Task-Based Authorization Constraints in Workflow Sysems", In CSFW, pp.155-162, 2004.

[9] Christian Wolter and Andreas Schaad. "Modeling of Task-Based Authoriztion Constraints in BPMN", In Proceedings of the 5th International Conference on BPM, pp.64-79, 2007.

[10] Hong Chen, Ninghui Li, "Constraint Generation for Separation of Duty", Proc. of 11th ACM SACMAT, 130-138쪽, June, 2006.

[11] 황유동, 박동규, "유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델", 한국컴퓨터정보학회논문지, 10권 3호, 45-54쪽, 2005.

저 자 소 개

최 은 복

1992: 전남대학교 전산학과 이학사.
1996: 전남대학교 전산학과 이학석사.
2000: 전남대학교 전산학과 이학박사
현 재: 전주대학교미디어정보학부 교수
관심분야: 통신망관리, 네트워크 보안 등