강제적 보안 정책에 기반한 BLP/BIBA 융합 접근 통제 모델

최은복*, 박주기**

요 약

이 논문은 강제적 접근 보안 정책에 기반한 접근통제 모델의 권한에 대한 상반관계를 해결하기 위하여 비밀성과 무결성의 융합 접근통제 모델을 제시한다. 우리는 접근통제 모델의 모든 융합상황을 분석하고 정책의 보안특성에 대한 개념을 진척시키기 위하여 강제적 접근통제 정책내에서 비밀성과 무결성별로 보안 정의, 공리 및 보안 규칙을 기술하고 도출함으로서, 강제적 접근통제 모델의 비밀성과 무결성의 상반관계를 해결함과 동시에 더불어 정보의 가용성을 제공할 수 있는 BLP/BIBA 융합 접근통제 모델을 제시한다.

A BLP/BIBA union access control model based on mandatory security property

Eun-Bok Choi*, Joo-Gi Park**

ABSTRACT

This paper presents union access control model to solve access control model's inconsistency based on the mandatory access control property. We found security definition, rule and axiom by confidentiality and integrity in mandatory access control policy as well as analyzed all union circumstances of access control model. Also, we suggest BLP/BIBA union access control model that can provide mandatory access control model's confidentiality, integrity and availability.

Key Words : access control model, BLP, BIBA

* 전주대학교 미디어정보학부(✉ebchoi@jj.ac.kr)
** KT 중앙연구소
· 제1저자(First Author) : 최은복 · 교신저자(Correspondent Author) : 박주기
· 접수일(2010년 10월 29일), 수정일(1차 : 2010년 11월 26일), 게재확정일(2010년 11월 29일)

Ⅰ. 서 론

유무선 통신 및 컴퓨팅 기술의 급속적인 발전으로 인해 기업과 정부 기관들 뿐만 아니라 개인적으로 소규모 사업을 하는 소호(SOHO)족에도 운영체제의 보안은 정보시스템을 운영하는데 기본이 된다. 더욱이 컴퓨터와 정보통신의 다양한 결합으로 인해 컴퓨터 시스템에 접근하고자 하는 사용자들이 시공을 초월하여 접근함에 따라 인가된 사용자뿐만 아니라 인가된 사용자라고 하더라도 의도적이고 불법적인 자원 접근을 통제하고 관리할 필요성이 있다.

컴퓨터 시스템에서 보안정책을 수립하는데 사용되는 보안모델은 보안 시스템을 설계하는데 있어 중요한 역할을 수행하는데 특히, 높은 수준을 갖는 안전한 운영체제를 갖추기 위해서는 정보 자원에 대한 비밀성과 무결성, 그리고 가용성이 보장되여야 한다. 이중에서 무결성은 데이터의 정확성과 관련되는데, Matt Bishop에 따르면 "무결성은 데이터나 자원의 신뢰성을 의미하며 부당하고 불법적인 변경을 예방하는 용어로 이용된다"라고 언급하면서 무결성의 목표를 다음과 같이 세 가지로 제시하였다[1].

첫째, 불법적인 사용자에 의해 데이터나 프로그램의 수정을 예방하는데 목표가 있다.

둘째, 권한을 소유한 정당한 사용자에 의해 비합리적인 방법에 의한 불법적인 수정을 방지하는데 목표가 있다.

셋째, 내·외적인 데이터나 프로그램의 일관성을 유지하는데 목표가 있다.

하지만 이러한 비밀성과 무결성은 서로 상반되는 개념을 내포하고 있어서 이들 특성을 갖는 모델들은 개별적으로 운영되고 구현되는 한계를 갖고 있다. 그러므로 이러한 상반되는 특성을 다양한 모델 분석과 공리 제시를 통해 해당 모델들을 융합하므로서 정보의 이용성을 제공할 수 있다면 높은 보안성을 유지할 수 있으리라 본다.

본 논문에서는 다양한 모델 분석과 공리 제시를 통해 해당 모델들을 효율적으로 융합함으로서 비밀성과 무결성을 제공함과 동시에 가용성을 높여 높은 보안 수준을 제공할 수 있는 융합 접근통제 모델을 제시한다.

Ⅱ. 관련연구

접근제어 정책은 크게 자율적 접근제어(DAC : Discretionary Access Control)정책, 강제적 접근제어(MAC : Mandatory Access Control)정책, 그리고 역할기반 접근제어(RBAC : Role Base Access Control)정책 등이 있다.

2.1 자율적 접근제어 정책

자율적 접근제어 정책은 접근을 요청한 주체가 객체에 대한 권한을 자율적으로 다른 주체에게 권한을 부여하거나 철회할 수 있음을 의미한다. 여기에 해당하는 접근제어 정책에는 접근제어 행렬(Access Control Matrix), 접근제어 리스트(ACL), 능력리스트(Capability List) 등이 있다.[2]

접근제어행렬은 주체에 해당하는 행과 객체에 해당하는 열, 그리고 행과 열이 교차하는 곳은 연산을 나타낸다. 그러나 대규모 시스템에서는 수많은 주체와 객체가 존재하기 때문에 이들간의 연산을 행렬로 기술하기에는 시스템 공간의 낭비를 초래한다. 따라서 이러한 단점을 해결할 수 있는 접근제어 리스트나 능력리스트를 이용한다.

2.2 강제적 접근제어 정책

강제적 접근제어정책은 시스템 관리자에 의해 보안등급이 결정되는 정책으로 상향의 정보흐름을 유지함으로써 상부보다는 권한책임을 덜 받는 하부관리조직이나 하부 계급으로의 정보흐름을 차단하는 비밀성

기반 접근제어정책과 정보의 불법적인 변경을 예방함과 동시에 정보의 공개와 공유에 초점을 맞추는 수평조직 구조에 알맞은 정책인 무결성 기반 접근제어 정책으로 나뉜다.

● 비밀성 기반 접근제어 정책

비밀성 기반의 대표적인 접근제어 모델로는 BLP(Bell & LaPadula) model이 있는데, 이 모델은 강제적인 정책에 기반을 둔 데이터보호를 위한 참조 모델로서 군사환경이나 매우 제한적인 환경에서 제한된 수의 보안 관리자들에 의해 일정한 규칙에 따라 사용자의 정보에 대한 접근을 통제하고 관리되는 정책으로 규칙기반(Rule-Based) 기법과 관리기반(Administrative-Based)기법이 통제기법으로 이용된다.

각 등급은 두 가지 구성요소에 의해 정의되어지는데, 하나는 보안등급이고 다른 하나는 범주의 집합이다. 보안등급은 TS, S, C, U의 4가지 요소로 구성되고 이들은 TS>S>C>U의 관계를 갖는다. 범주의 집합은 요소들의 비계층 구조를 가지는 부분집합으로 정보가 포함되는 조직의 환경에 의해 명명되어진다[3].

● 무결성 기반 접근제어 정책

권한을 갖지 않는 사용자에게 정보가 흘러가는 것을 예방하는 비밀성에 기반을 둔 정책은 정보의 비밀성은 보장하지만 등급이 낮은 주체가 등급이 높은 객체의 정보를 변경할 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 무결성 기반 접근제어 정책이 제시되었다. 이 정책에서는 주체와 객체의 보안등급에 의해 정책이 수행되는데 특히 보안등급을 무결성 등급이라 한다. 이 무결성 등급은 크게 두가지로 분류한다. 하나는 Crucial(C), Very Important (VI), Important(I)로 구분되는 무결성 등급이고 다른 하나는 범주의 집합이다. 무결성 등급은 C>VI>I의 관계를 형성하며 범주의 집합은 BLP모델과 마찬가지로 비계층 구조 관계를 갖는다. 사용자를 대신하여 수행하는 프로세스나 접근이 수행되는 객체에게 무결성 등급이 부여된다[4].

이 두가지 모델은 등급과 범주가 각각 $C1 \geq C2$ 이고 범주 $S1 \supseteq S2$의 관계를 가지면 등급 $L1=(C1,S1)$은 $L2=(C2,S2)$를 지배한다. 만약 등급이 $L1 \geq L2$ 나 $L2 \geq L1$ 의 관계가 모두 아니면 이 두 등급은 비교불가능하다고 말한다.

시스템의 무결성을 유지하기 위한 모델로는 Biba 모델[5], Goguen-Meseguer model[6], Sutherland model[7], Clark-Wilson model[8], Brewer-Nash model[9], Domain and Type Enforcement model(DTE)[10] 등이 있다. Goguen-Meseguer model, Sutherland model, DTE model은 시스템의 무결성을 예방하는 방법이 제시되지 않았으며 Clark-Wilson model은 비즈니스 환경에서 중요한 역할을 적용했지만 수학적인 증명이나 정형화된 기법을 통한 검증방법이 기술되지 않았다. 1977년 Mitre 회사에서 제안된 Biba 무결성 모델이 수학적인 정형화된 방법으로 기술된 가장 대중적인 무결성 모델이다. Biba의 SIP이 컴퓨터 시스템에서 무결성을 유지하는데 이용되어왔다.

● 격자 기반 접근제어 정책

Denning의 정보 흐름(FM:Flow Model) 모델은 $FM=<N, P, SC, \oplus, \rightarrow>$에 의해 정의되어진다[11,12]. 여기서 N은 객체의 유한집합이며 P는 유한 프로세스 집합(주체 집합), SC는 보안등급 집합, 등급조합 연산자인 $\oplus$는 결합 및 교환법칙 특성을 갖는 이진 연산자, 흐름 관계인 $\rightarrow$는 보안등급의 쌍으로 표현된다. 예로, 등급 A와 B에 대해 $A \rightarrow B$는 만약 A등급의 정보가 B등급의 정보로의 흐름을 허가된다면 우리는 $A \rightarrow B$로 쓰며, 정보는 A등급에서 B등급으로 흘러간다고 말한다.

모델의 보안 요구조건은 흐름 모델 FM이 만약 연산순서의 수행 관계 $\rightarrow$를 침범하는 흐름이 발생하지 않

는다면 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 $B \rightarrow C \Rightarrow A \oplus B \rightarrow C$

격자기반 접근통제는 보안등급에 기반하여 일방향의 정보흐름을 강조하는데 관점을 둔 강제적 접근통제 정책의 한 모델로서, 사용자나 주체에 부여된 인가등급(security clearance)과 객체에 부여된 보안등급(security classification)을 적용하여 접근통제 여부를 결정한다.

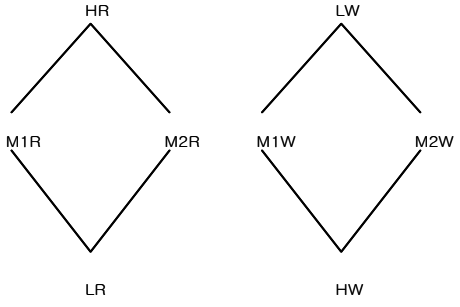

그림 1. 격자구조-단순한 및 관대한 보안특성
Fig. 1 Lattice Structure - Simple and Liberal Security Property

격자기반 접근통제 모델은 그림 1과 그림 2와 같이 비밀성에 기반을 두므로 정보의 흐름이 아래에서 위로 향하는 구조를 갖으며 부분적인 순서지배관계를 갖는 보안등급의 유한격자구조를 갖는다. 이 그림에서 H등급과 L등급은 보안등급의 높고 낮음을 뜻하며 M1과 M2등급은 H등급과 L등급의 중간으로 등급의 비교가 불가능한 경우를 의미한다.

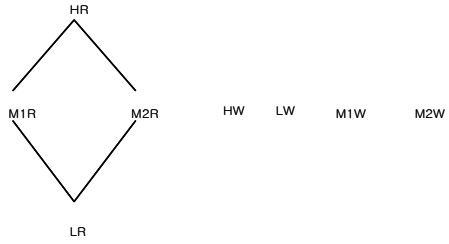

그림 2. 격자구조-단순한 및 엄격한 보안특성
Fig. 2 Lattice Structure - Simple and Strict Security Property

격자기반 접근통제 모델은 다음과 같이 크게 두 가지 특성을 갖는다. 정보의 읽기에 관련된 단순한 보안특성과 쓰기에 관련된 스타 특성으로 나뉜다.

● 단순한 보안 특성(Simple Security Property)

주체 s의 인가등급이 객체 o의 보안등급에 부분순서지배관계이면 객체 o를 읽을 수 있다.

IF $\lambda(s) \geq \lambda(o)$ THEN read(s,o) ELSE reject;

● 관대한 스타 특성(Liberal *-Property)

객체 o의 보안등급이 주체 s의 인가등급에 부분순서지배관계이면 주체 s는 객체 o를 쓸 수 있다. IF $\lambda(s) \leq \lambda(o)$ THEN write(s,o) ELSE reject;

관대한 스타 특성은 낮은 주체가 높은 등급의 객체를 쓸 수 있기 때문에, 무결성 측면에서 보면 높은 등급의 데이터가 의도적이던지 사고에 의하던지 낮은 등급의 주체에 의해 파괴되고 훼손될 수 있음을 의미

한다. 이러한 가능성을 피하기 위해 다음과 같은 엄격한 스타 특성이 적용된다.

• 엄격한 스타 특성(Strict *-Property)

주체s의 인가등급이 객체 o의 보안등급과 같을 경우에 객체 o를 쓸 수 있다.

IF λ(s) = λ(o) THEN write(s,o) ELSE reject;

2.3 역할기반 접근제어 정책

• RBAC

자율적 접근제어 정책은 주체가 객체에 대한 권한을 자율적으로 다른 주체에게 권한을 부여하거나 철회할 수 있어 악의적인 목적에 이용될 수 있는 보안상의 취약점이 있다. 또한, 강제적 접근제어 정책에는 BLP모델과 Biba모델이 있는데, BLP모델은 정보의 비밀성을 중요시하는 군사 분야의 응용에 적합하도록 만들어져서 객체에 대해 엄격하게 제한하기 때문에 일반적인 응용에 적용하기에는 문제점이 있다[13]. 이러한 단점을 보완하고 정보의 비밀성보다는 무결성을 보장하며, 상업적인 환경에 적용하도록 만든 모델이 Biba 모델이다. 하지만 이 두 모델들은 한 주체가 어느 한 객체를 접근하지 못하면 자신의 인가등급을 변경하지 않는 한 그 객체와 동일한 보안등급을 갖는 모든 객체에 접근이 허락되지 않는다. 또한 공통적인 기능을 수행하는 다중 사용자들이 객체를 접근할 수 있는 보안 요구사항을 표현하는데는 부적절하다.

역할기반 접근제어 정책은 상업적인 측면의 보안정책을 강화시킬 수 있는 정책으로, 사용자들이 수행하는 공통적인 기능들에 기반을 둔 그룹들인 역할로 구성되며 조직이나 환경에 따라 역할이 자연스럽게 생성되고 재구성될 수 있는 유연성을 갖는다.

역할기반 접근제어 정책의 개념은 다음과 같이 잘 알려진 세 가지 보안 원리를 뒷받침하는데, 첫째, 역할 계층성을 이용하여 작업에 꼭 필요한 최소한의 권한만을 역할에 배정하는 최소권한원칙(least privilege principle), 둘째, 정보의 무결성을 침해하는 사기행위나 부정수단을 유발할 수 있는 작업은 상호 배타적인 역할로 지정하여 임무를 분리시켜 수행하는 임무 분리(separation of duty), 마지막으로, 전형적인 운영체제나 시스템에서 사용되어졌던 데이터를 처리하는 read, write, execute 등의 권한 대신에, 다양한 기능을 수행할 수 있고 명령어를 추상화시키는 상업적인 처리 명령어 credit, debit, transfer, create account, delete account 등을 사용하는 데이터 추상화(data abstraction)이다[14].

• T-RBAC

테스크-역할기반 접근제어(T-RBAC : Task-Role-Based Access Control)[15]는 RBAC 모델을 기반으로 사업 환경의 특성을 반영하여 태스크-역할에 권한을 할당하여 접근을 통제하는 모델로 구성은 그림1과 같다. 태스크는 사업 환경에서 직위와 사업 역할을 포함하는 조직 구조와 사업 프로세스의 특성에 따라 분류되며, 권한 할당의 기준이 된다. 그래서 T-RBAC은 사업 환경의 특성들을 고려하여 접근제어 요구들을 수용한다. T-RBAC에서 사용되는 태스크의 종류는 표1과 같다.

T-RBAC는 RBAC의 역할계층 대신에 감독 역할계층(S-RH:Supervision Role Hierarchy)을 사용한다. S-RH에서 역할 계층선상에서 상위역할은 하위 역할의 모든 접근권한을 상속받지는 않는다. 클래스 S나 클래스 A에 속한 접근 권한만이 역할 계층선상의 하위역할에서 상위역할로 상속된다. 감독 역할계층을 사용함으로서 최소권한 규칙이 위배되는 문제를 해결한다.

T-RBAC의 작동 절차는 사용자가 특정역할에 할당되고, 직무는 수행하는 업무를 고려하여 가장 적합한 역할에 할당되며 여러 직무들의 집합이 하나의 역할에 할당될 수도 있다. 직무는 위에서 설명한 것과 같이 4가지로 구분되며 이중 Class W에 속하는 직무는 3

가지 속성인 활성화 조건, 시간제약, 최대 활성화 직무 개수를 준수하여야 된다. 객체는 직무에 따라서 접근 가능한 객체로 구분하여 직무에 할당한다. 다음으로 직무에 권한이 할당되는데 여기서느 '쓰기, 읽기, 실행' 등의 기능을 부여할 수 있다. 사용자-역할, 직무-역할, 권한-직무의 할당이 완료되면 세션을 생성하여 접근을 허가하게 된다[16].

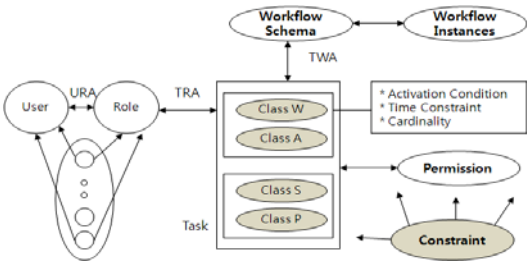

그림 3. T-RBAC 모델
Fig. 3 T-RABC Model

표 1. 태스크 분류
Table 1. Task classification

분 류	특 성	설 명
Class P	사 적 (Private)	상속불가, 수동적 접근 예) 분석, 계획, 결정
Class S	감 독 (Supervision)	상속가능, 수동적 접근 예) 검토, 감사, 감시, 승인
Class W	워크플로우 지향 (Workflow)	상속불가, 능동적 접근 예)워크플로우 내 태스크
Class A	행위 승인 (approval)	상속가능, 능동적 접근 예)워크플로우 내 승인 태스크

III. 본 론

이 논문은 그림 4와 같이 강제적 접근통제 정책에 기반한 BLP와 BIBA의 모순을 해결하기 위하여 비밀성과 무결성의 융합 접근통제 모델을 제시한다. 먼저, BLP와 BIBA의 모든 융합상황을 분석하고 강제적 접근통제 정책의 개념을 진척시키고 이 정책 도메인안에서 비밀성과 무결성이 점검되고 변경된다.

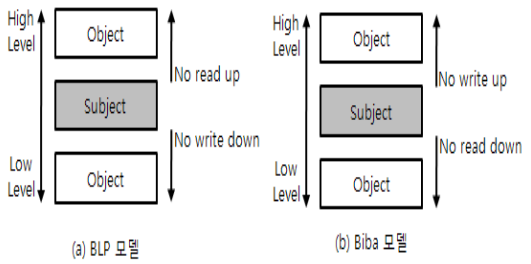

그림 4. BLP/Biba 모델
Fig. 4 BLP/Biba Model

BLP와 BIBA가 동시에 존재할 수 없을 때 주체는 객체와 직접적으로 운용될 수 없다. 다만, 강제적 접근통제 정책 도메인에서 주체는 객체와 간접적으로 운용될 수 있으며, 융합된 모델에서 read와 append 연산과 관련된 객체는 사건을 추적하기 위하여 연산을 생성한 주체에 의해 서명하게 함으로써 BLP와 BIBA 모델의 융합에 의한 상반관계를 해결할 수 있다.

BLP 모델은 보안 운영체제를 실현하는데 있어 전통적인 다단계 비밀성 정책 모델이다. 이 모델은 간단하게 no read up, no write down 정책으로 기술된다. 이 모델은 중요한 정보가 권한을 갖지 않는 불법적인 사용자에게 정보가 누설되는 것을 방지하는데 효과적이다.

이와는 반대로 정보의 누설보다는 정당한 사용자에게 정보의 이용성을 중시하는 무결성 모델에는 BIBA 모델, Lipner Matrix 모델 Clark-Wilson 모델 등이 있는데, 이중에서 Biba 모델은 no read down, no write up 정책을 기반으로 정보의 이용성과 무결성을 제공하는데 대부분의 실질적인 시스템에서 사용되고 있다. 높은 보안 수준을 실현하기 위해서는 BLP와 같은 비밀성 모델과 BIBA와 같은 무결성 모델을 동시에 구현하여야 한다.

주체와 객체의 관련성에 따라 비밀성과 무결성은 4개의 부류로 구분된다. 높은 비밀성과 높은 무결성, 높은 비밀성과 낮은 무결성, 낮은 비밀성과 높은 무결성, 낮은 비밀성과 낮은 무결성이다.

그러나 대부분의 주체와 객체의 비밀성과 무결성은 일관성을 갖는다. 즉, 높은 비밀성 등급을 갖는 주체와 객체는 높은 무결성 등급을 갖거나, 낮은 비밀성 등급의 주체와 객체는 낮은 무결성 등급을 갖는다. 높은 비밀성과 낮은 무결성의 경우 BLP와 BIBA은 단지 read 연산만 허가한다. 그러나 주체는 append 연산의 허가를 원한다. 낮은 비밀성과 높은 무결성의 경우 BLP와 BIBA는 단지 append 연산에 대해서만 허가한다. 그러나 주체는 read 연산 허가를 요구한다. 이렇듯 BLP와 BIBA 모델은 해당 정책의 특성에 의해 비밀성과 무결성을 동시에 제공하기에는 모순을 발생하며, BLP와 BIBA 모델이 엄격하게 수행된다면 적용되는 시스템은 실제 환경에 적용하는데 매우 제한적으로 이용되어 활용성이 낮을 것이다.

그러나 강제적 접근통제 정책내에서 다양한 모델 분석과 공리 제시를 통해 해당 모델들을 융합하므로서 높은 보안수준을 제공하면서 정보의 이용성을 제공할 수 있다면 정보의 비밀성과 무결성과 더불어 가용성까지 제공할 수 있으리라 본다.

본 논문에서는 다양한 모델 분석과 공리 제시를 통해 해당 모델들을 효율적으로 융합함으로서 비밀성과 무결성을 제공함과 동시에 가용성을 높여 높은 보안 수준을 제공할 수 있는 동적융합 모델을 제시한다.

3.1 융합 접근통제 모델

주체/객체의 비밀성과 무결성의 상황을 조합한 결과값은 주체의 비밀성 등급(csi), 객체의 비밀성등급(coj), 주체의 무결성 등급(isi), 객체의 무결성 등급(ioj)으로 구분된다. 이는 csi≥coj and isi≥ioj, csi≥coj and isi≤ioj, csi≤ioj and isi≥ioj, csi≤coj and isi≤ioj, csi=coj and isi=ioj로 나눌 수 있는데, 지금 우리는 다음과 같이 이 모든 상황을 분석기술한다.

1) csi≥coj and isi≥ioj, req(s, o, v/a) = no, (view/append 모두 안됨)

왜냐면, view의 경우 보안특성에 의해 BLP 모델은 적합하지만 BIBA모델은 맞지 않으며, Append 경우 BIBA 모델은 가능하지만 보안특성에 의해 BLP 모델은 맞지 않는다. 또한 Write의 경우 BLP와 BIBA모델 모두에게 적합하지 않는다.

2) csi≤coj and isi≤ioj, req(s, o, v/a) = no, (view/append 모두 안됨)

왜냐면, view의 경우 보안특성에 의해 BIBA 모델은 적합하지만 BLP모델은 맞지 않으며, Append 경우 BLP 모델은 가능하지만 BIBA 모델은 맞지 않는다. Write 의 경우 BLP, BIBA모델 모두 맞지 않는다.

3) csi≥coj and isi≤ioj, req(s, o, v) = yes, req(s, o, a) = no

view의 경우 보안특성에 의해 BLP와 BIBA 모델에 모두 적합하나 Append 와 Write 경우 BLP와 BIBA 모델에 맞지 않는다.

4) csi≤ioj and isi≥ioj, req(s, o, v) = no, req(s, o, a) = yes

view, Append, Write 모든 연산의 경우 BLP와 BIBA 모델에 모두 적합하지 않는다.

5) csi=coj and isi=ioj, req(s, o, w) = yes

Write 연산의 경우만이 BLP와 BIBA 모델에 모두 적합하다.

처음 두 상황, 곧 1)과 2)에서 주체와 객체의 비밀성과 무결성 등급은 일관성을 갖으며, 이는 실질 시스템에서는 매우 일반적이다. 하지만 BLP와 BIBA 모델의 경우에서는 모순을 갖는다. 그래서 많은 시스템을 구현할 때 BLP와 BIBA를 각각 분리하여 구현하거나 ASOS(Army Secure Operating System[4])와 같이 BLP와 BIBA를 간단하게 혼합하여 구현한다. ASOS는 단지 BLP와 BIBA를 각각 따로 구현하였을 뿐 실질적

으로 융합한 모델은 아니다. 세 번째 상황 곧, 3)에서 단지 view 경우만, BLP와 BIBA 모델이 모두 맞는다. 네 번째 상황 곧 4)에서 Append 경우만 BLP와 BIBA 모델이 모두 맞는다. 다번째 상황의 경우는 단지 단지 두 개의 민감도 레이블이 같을 경우에만 Write 경우만이 BLP와 BIBA 모델에 맞는다.

그래서 본 모델에서는 보안특성에 의해 제한적으로 적용되고 실질적으로 적용하기에 적합하지 못했던 두 가지 접근통제 모델의 상반성을 다음과 같이 다양한 권한 규칙에 대한 제반조건을 확장하여 적용하였다.

우리는 세가지 보안 특성을 제공하는 융합 접근통제 모델을 제시하기 위하여 다음과 같은 몇가지 정의와 공리를 기술하였다.

정의 1 : S는 주체의 집합으로 $S \in \{s1,...,sn\}$, O는 객체의 집합으로 $O \in \{o1,...,on\}$, M은 접근모드의 집합으로 $M \in \{ m \mid m=v, a, w, e, c, g, d\}$, req()은 접근요청으로 $req:(s,o,m) \rightarrow R \in \{y, n, er\}$ 값중 하나를 갖는다.

여기에서 v는 변경(append or write)권한이 없는 관찰(view)모드, a는 관찰(view)권한이 없는 변경(append)모드, w는 관찰과 변경이 가능한 쓰기(write)모드, e는 관찰과 변경이 모두 불가능한 에러(error)모드, c는 관찰권한을 포함한 체크(check)모드, g는 객체의 생성(generate)모드 , 마지막으로 d는 객체를 제거하는 삭제(delete) 모드, 그리고 $P = S \times O \times M$는 권한으로서 주체 S는 객체 O에 대해 접근모드 M에 대한 권한을 갖는다고 한다. 또한, $req:(s,o,x) \rightarrow R=\{y, n, er\}$는 주체 s가 객체 o에 대하여 x 접근모드를 요구하고, 주체 s가 x 모드를 갖는 객체 o를 부여받을 때 y(yes) 이고, 주체 s가 x 모드를 갖는 객체 o에 대해 거절될 때 n(no)이고 두 개 이상의 값이 공존할 때 er(error)이다.

정의 2 : $P(s,o,x1,...,xn) = \{o \mid o \in O \wedge [(s,o,x1 \in P \vee ... \vee (s,o,xn) \in P]\}$

$P(s,o,x1,...,xn)$는 특정한 주체 s가 특정 객체 o에 갖는 접근모드를 모아 놓은 집합이다.

정의 3 : $L = \{(c,i) \mid c \in C, i \in I\}$은 민감도 레이블(sensitivity lebel)로서 C는 비밀성 등급(confidentiality level)의 집합이고 I는 무결성 등급의 집합이다. 특히, $C = \{(ts, s, cf, u\}$이고 $I = \{(cr, vi, i)\}$이다. 비밀성 등급의 ts는 top secret, s는 secret, cf는 confidential, u는 unclassified 로서 ts>s>c>u의 관계를 갖는다. 무결성등급의 cr는 crucial, vi는 very important, i는 important로서 cr>vi>i의 관계를 갖는다.

정의 4 : $S/O = \{(cs, cc, co) \mid (cs,cc,co) \in C, (is, ic, io) \in I\}$

S나 O는 비밀성과 무결성에 따라 다음 내용을 갖는다. cs, cc, co는 비밀성과 관련된 등급으로 cs는 주체의 비밀성기반 최대등급, cc는 주체의 비밀성 기반 현재 등급, co는 객체의 비밀성기반 등급이다. 반면, is,ic,io는 무결성과 관련된 등급으로 is는 주체의 무결성 기반 최대등급, ic는 무결성기반 현재 등급, io는 객체의 무결성기반 등급이다.

공리 1 : $b(s,o,v) \neq \varnothing$ and $cc(s) \geq co(o)$ and $ic(s) \leq io(o) \Rightarrow \forall o \in b(s,o,v)$

공리 2 : $b(s,o,a) \neq \varnothing$ and $co(o) \geq cc(s)$ and $io(o) \leq ic(s) \Rightarrow \forall o \in b(s,o,a)$

공리 3 : $b(s,o,w) \neq \varnothing$ and $co(o) = cc(s)$ and $io(o) = ic(s) \Rightarrow \forall o \in b(s,o,w)$

공리 4 : $b(s,o,c) \neq \varnothing$ and $(cc \geq co$ and $ic \leq io) \vee (cs \geq co$ and $is \leq io) \Rightarrow \forall o \in b(s,o,c)$

공리 5 : $b(s,o,g) \neq \varnothing$ and $(cc \geq co$ and $ic \leq io) \vee (cc \leq co$ and $ic \geq io) \vee (cc=co$ and $ic=io) \Rightarrow \forall o \in b(s,o,g)$

공리 6 : $b(s,o,d) \neq \varnothing$ and $\neg(cc \geq co$ and $ic \leq io) \vee \neg(cc \leq co$ and $ic \geq io) \vee \neg(cc=co$ and $ic=io) \Rightarrow \forall o \in b(s,o,d)$

주체의 접근요청을 구현하기 위한 융합 모델에 대한 주체와 객체의 비밀성 / 무결성 함수의 요청 조건은 다음과 같다.

표 2. 융합모델의 접근모드와 규칙
Table 2. Access modes and rules of the Union Model

접근모드	융합모델의 규칙
v	cc≥co and ic≤io
a	cc≤co and ic≥io
w	cc=co and ic=io
c	(cc≥co and ic≤io) ∨ (cs≥co and is≤io)
g	(cc≥co and ic≤io) ∨ (cc≤co and ic≥io) ∨ (cc=co and ic=io)
d	¬(cc≥co and ic≤io) ∨ ¬(cc≤co and ic≥io) ∨ ¬(cc=co and ic=io)

<view 권한 규칙>

규칙 1-1 : x = v ∈ m, cc(si) ≥ co(oj), is(si) ≤ io(oj)

규칙 1-2: x = v ∈ m, cc(si) ≥ co(oj), is(si) 〉 io(oj)

규칙 1-3 : x = v ∈ m, cc(si) 〈 co(oj), is(si) ≤ io(oj)

규칙 1-4 : x = v ∈ m, cc(si) 〈 co(oj), is(si) 〉 io(oj)

<append 권한 규칙>

규칙 2-1 : x = a ∈ m, cc(si) ≤ co(oj), is(si) ≥ io(oj)

규칙 2-2 : x = a ∈ m, cc(si) 〉 co(oj), is(si) ≥ io(oj)

규칙 2-3 : x = a ∈ m, cc(si) ≤ co(oj), is(si) 〈 io(oj)

규칙 2-4 : x = a ∈ m, cc(si) 〉 co(oj), is(si) 〈 io(oj)

<write 권한 규칙>

규칙 3-1 : x = w ∈ m, cc(si) = co(oj), is(si) = io(oj)

규칙 3-2 : x = w ∈ m, cc(si) ≠ co(oj), is(si) = io(oj)

규칙 3-3 : x = w ∈ m, cc(si) = co(oj), is(si) ≠ io(oj)

규칙 3-4 : x = w ∈ m, cc(si) ≠ co(oj), is(si) ≠io(oj)

<check 권한 규칙>

규칙 4-1 : x = c ∈ m, cc(si) ≥ co(oj) ∨ (cs(si)≥ co(oj) and is(si)≤io(oj)) , is(si) ≤ io(oj) ∨ ic(si) ≤ io(oj)

규칙 4-2 : x = c ∈ m, cc(si) ≥ co(oj) ∨ cs(si) ≥ co(oj), is(si) 〉 io(oj) ∨ ic(si) 〉 io(oj)

규칙 4-3 : x = c ∈ m, cc(si) 〈 co(oj) ∨ cs(si) 〈 co(oj), is(si) ≤ io(oj) ∨ ic(si) ≤ io(oj)

규칙 4-4 : x = c ∈ m, cc(si) 〈 co(oj) ∨ cs(si) 〈 co(oj), is(si) 〉 io(oj) ∨ ic(si) 〉 io(oj)

<generate 권한 규칙>

규칙 5-1 : x = g ∈ m, cc(si) ≥ co(oj) ∨ (cs(si)≥ co(oj) and is(si)≤io(oj)) , is(si) ≤ io(oj) ∨ ic(si) ≤ io(oj)

규칙 5-2 : x = g ∈ m, cc(si) ≤ co(oj) ∨ cs(si) ≤ co(oj) , is(si) ≥ io(oj) ∨ ic(si) ≥ io(oj)

규칙 5-3 : x = g ∈ m, cc(si) = co(oj) ∨ cs(si) = co(oj), is(si) = io(oj) ∨ ic(si) = io(oj)

<delete 권한 규칙>

규칙 6-1 : x = d ∈ m, ¬cc(si) ≥ co(oj) ∨ ¬(cs(si) ≥co(oj) and ¬is(si)≤io(oj)) , ¬is(si) ≤ io(oj) ∨¬ ic(si) ≤ io(oj)

Ⅳ. 결 론

유무선 통신 및 컴퓨팅 기술의 급속적인 발전으로 인해 기업과 정부 기관들 뿐만 아니라 개인적으로 소규모 사업을 하는 소호(SOHO)족에도 운영체제의 보안은 정보시스템을 운영하는데 기본이 된다. 더욱이 컴퓨터와 정보통신의 다양한 결합으로 인해 컴퓨터

시스템에 접근하고자 하는 사용자들이 시공을 초월하여 접근함에 따라 인가된 사용자뿐만 아니라 인가된 사용자라고 하더라도 의도적이고 불법적인 자원 접근을 통제하고 관리되어야 한다. 또한, 컴퓨터 시스템이 여러 사용자나 여러 주체가 여러개의 응용프로그램을 동시에 사용하는 다양화된 분산시스템 환경으로 발전하면서 다양한 경로를 통해 부적절하게 접근하는 불법적인 사용자로부터 정당한 자원과 정보를 보호하고 관리되어야 할 필요성이 있다.

컴퓨터 시스템에서 보안정책을 수립하는데 사용되는 보안모델은 보안 시스템을 설계하는데 있어 중요한 역할을 수행하는데 특히, 높은 수준을 갖는 안전한 운영체제를 갖추기 위해서는 정보 자원에 대한 비밀성과 무결성, 그리고 가용성이 보장되여야 한다. 이 세 가지 보안특성은 서로 밀접한 연관성과 더불어 상반관계가 존재하므로 특정 도메인 환경에서 다양한 모델 분석과 공리 제시를 통해 해당 모델들을 융합하므로서 높은 보안수준을 제공함과 동시에 정보의 이용성을 제공할 수 있다면 정보의 비밀성과 무결성 그리고 더불어 가용성까지 보장받을 수 있으리라 본다.

본 논문에서는 안전한 운영체제를 설계하기 위한 기본적인 요소중에 하나인 접근통제 정책을 통해 보안특성의 3요소인 정보의 비밀성과 무결성, 그리고 가용성을 제시할 수 있는 강제적 접근통제 정책 기반 융합 접근통제 모델을 제시하였다. 본 모델은 다양한 접근통제 모델의 특장점의 분석과 연구 그리고 보안특성을 제공할 수 있는 보안정의와 공리를 통한 적절한 보안 모델들의 효율적인 융합을 통해 비밀성과 무결성을 제공함과 동시에 가용성을 높여 높은 보안 수준을 제공할 수 있는 보안모델의 특징을 갖는다.

참고문헌

[1] Bishop, M. Computer Security:Art and Science, Addison Wesley, Boston, MA. 2003.

[2] Warwick Ford, Computer Communications Security, Prentice Hall

[3] 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.

[4] Silvana Castano, DATABASE SECURITY, ADDISON-WESLEY

[5] Zhang Xiangfeng, Sun Yufang. "*Dynamic Enforcement of the Strict Integrity Policy in Biba's Model*", Journal of Computer Reserch and Development. vol.42 No.5, pp. 746-754, 2005

[6] J.A. Goguen, J.Meseguer. "*Security Policies and security models*", The 1982 Symposium on Security and Privacy, Oakland, CA, 1982.

[7] D. Sutherland, "*A model of information*", The 9th National Security Conf, Gaithersburg, 1986.

[8] D. D. Clark, D.R. Wilson, "*A comparision of commercial and military computer security policies*", The 1987 IEEE Symposium on Security and Privacy, Oakland, California, 1987.

[9] D. Brewser, M. Nash, "*The Chinese wall security policy*", In Proc. of IEEE Symposium on Security Press, pp.206-214, 1989.

[10] L. Badger, D.F.Sterne, D.L. Sherman, et al, "*A domain and type enforcement UNIX prototype*", USENIX Computing Systems. 9(1), pp 47-83, 1996.

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

[12] S. Osborn, "*Mandatory access control and role-based access control revisited*," In Proceeding of the 2nd ACM Workshop on RBAC, pp.31-40, 1997.

[13] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, *"Role-Based Access Control Models"*,

COMPUTER SOCIETY, IEEE, FEB. pp.38-47, 1996.

[14] Ravi S. Sandhu and Pierangela Samarati, "*Access Control : Principles and Practice*", IEEE Communications Magazine, pp. 40-48, 9, 1994.

[15] Sejong Oh and Seog Park, "*Task-role-based access control model*", Information System, Vol.28, No.6, pp.533-562, September, 2003.

[16] 엄정호, 박선호, 정태명, "유비쿼터스 컴퓨팅 환경을 위한 보안통제가 강화된 접근제어 시스템 설계에 관한 연구", *정보보호학회 논문지*, 제18권 제5호, pp. 71-81. 10월 2008년.

최은복(Eun-Bok Choi)

1992년 전남대학교 전산학과 졸업

1996년 전남대학교 전산학과 대학원 석사

2000년 전남대학교 전산학과 대학원 박사

2002년~현재 전주대학교 미디어정보학부 교수

※ 관심분야 : 통신망관리보안, 홈 네트워크, 접근통제, IPTV 보안 등

박주기(Joo-Gi Park)

1990년 전남대학교 전산학과 졸업

1993년 전남대학교 전산학과 대학원 석사

2007년 전남대학교 정보보호학과 박사

1993년 ~ 현재 KT 중앙연구소 책임연구원

※ 관심분야 : 인터넷 보안, 인터넷트래픽 분석 및 모델링, IPTV