Z언어로 정형화된 역할기반 다중 보안등급 접근통제 모델

최은복*

요약

인터넷, 이동통신, 전자상거래 등과 같은 획기적인 서비스들을 제공하고 있는 정보통신 시스템은 엄청난 속도로 발전하며 진화해 나가고 있다. 이러한 흐름속에서 시스템과 더불어 한 조직의 중요한 가치를 지닌 정보를 안전하게 유지하는 것이 무엇보다도 중요한 항목중의 하나이다. 본 논문에서는 정보의 비밀성과 무결성 특성에 따라 주체와 객체에 세분화되고 실질적인 보안 클래스를 갖는 역할 기반 다중 보안등급 모델을 제안한다. 이 모델은 상업적인 환경의 기업에서 적용될 수 있도록 보안등급이 부여된 역할로 세분화됨으로서 조직이나 환경에 따라 역할이 재구성될 수 있는 유연성을 갖으며, 역할들의 제약조건들을 Z언어를 이용하여 정형화된 구조로 명확하게 표현함으로서 모델을 설계하고 구현할 경우 시간과 비용을 줄일 수 있는 장점을 제공한다.

A Role Based Multi Security Label Access Control Model formalized by Z Language

Eun-Bok Choi*

ABSTRACT

This paper proposes the differential multi security label model which has the detailed security classes with the confidentiality and integrity of the subject and object. We were specially described a role with the security classes to be applied to commercial enterprises. And the model has a role flexibility that can be reconfigured according to the organization and the environment. Finally, accurately expressed by the constraints of the roles to the formalized structures using Z language, it provide the advantage that you can reduce the cost and time to design and implement a model.

Keywords : Access Control, DAC, MAC, RBAC, Z Language

* 전주대학교 스마트미디어학부(✉ebchoi@jj.ac.kr)
· 제1저자(First Author) : 최은복 · 교신저자(Correspondent Author) : 최은복
· 접수일(2012년 8월 28일), 수정일(1차 : 2012년 10월 16일), 게재확정일(2012년 10월 19일)

Ⅰ. 소 개

유무선 통신 환경의 급속한 발전으로 대규모로 운영되는 기업뿐만 아니라 소규모의 소호에서도 정보보호 기능은 없어서는 안되는 필수적인 요소이다. 정보를 안전하게 유지하기 위한 기술중에 하나인 접근통제는 원천적으로 불법적인 사용자로부터의 접근을 차단하므로써 네트워크 자원을 안전하게 보호하기 위한 주요 수단으로 이들의 주요 업무는 시스템 자원을 서로 공유하며 사용자 접근 권한을 관리하는 것이다. 접근통제는 해당 주체가 객체에 접근하기 위한 제약이나 제한사항을 규정하며 주체의 인증을 통해 해당 자원의 접근 요청을 제어하는 정책으로 시스템의 정보자원을 안전하기 유지해야 하는 컴퓨터 시스템에서 매우 중요하고 기본적인 보호 메카니즘이다[1].

안전하게 유지되어야 데이터베이스의 특성에따라 크게 데이터는 두가지로 나뉜다. 인가되지 않은 사용자나 불법적인 사용자로부터의 원천적인 접근과 불법 유출을 방지하는데 목적을 갖는 비밀성과 일반적인 접근이 가능한 정보의 공개 원칙을 갖으면서 다만 권한을 갖는 사용자에 한하여 정보의 수정이 가능하도록 하는 무결성으로 나뉜다.

현재, 정보보호에 이용되는 주요 접근통제 모델은 세가지 종류를 포함하는데, 소규모이거나 폐쇄적인 응용 환경에 적합한 임의적인 접근 통제 모델(DAC), 체계적이고 일괄적인 정보 흐름이 요구되는 군사적인 분야에 적합한 강제적인 접근통제 모델(MAC) 그리고 실질적인 기업 환경에 적합한 사용자의 역할과 역할의 접근권한에 기반하여 정책을 수행하는 역할기반 접근통제 모델(RBAC)로 구분된다[2].

Ⅱ. 관련연구

2.1 임의적 접근통제 모델

임의적 접근통제 모델은 정당한 사용자나 사용자 그룹에 대하여 배정된 객체에 대한 접근만을 허가하는 정책으로 자신의 접근 권한을 다른 사용자에게 자율적으로 양도하는 것을 허용한다. 리눅스, 유닉스 그리고 윈도우 NT/서버와 같은 대부분의 시스템은 임의적인 접근 통제 모델을 갖는데, 이를 구현하기 위하여 시스템은 사용자의 신원을 정의하고 사용자에게 접근 통제 리스트에 있는 권한에 따라 객체 자원의 이용을 허가하거나 제한하며 주체의 통제 권한도 권한을 갖고 있는 사용자나 그룹에 의해 수정되어진다[3].

접근통제 행렬은 임의적 접근통제 모델을 구현하기 위한 정책으로 주체와 객체의 접근 권한을 규정하기 위해 2차원 행렬을 사용한다. 행렬에 있는 행은 사용자, 프로그램 그리고 에이전트로 구성되는 주체들의 접근 권한 속성을 갖으며 열은 문서, 장비, 자원 그리고 서비스와 같은 객체들의 접근 권한 속성으로 구성된다. 표 1은 접근행렬의 한 예로서 Own은 관리 연산, R은 읽기, W는 쓰기, E는 수행, A는 추가, D는 삭제, Ui는 사용자, Pi는 프로세서, Fi는 파일, Si는 자원이나 서비스를 의미한다[4].

표 1. 접근통제 행렬
Table 1. Access Control Matrix

객체 / 주체	F1	F2	S1	S2
U1	Own, R		R, E	
U2	W	A, D		R, W
P1		R	R, W	
P2		R, W		R

2.2 강제적 접근통제 모델

강제적 접근통제 모델은 시스템의 정보흐름을 제어하는데 효율적이지 않은 임의적 접근통제 모델의 단점을 개선하기 위해 제안된 모델이다. 각 사용자와 파

일은 단지 보안관리자 이외에는 변경될 수 없는 보안 클래스가 부여되며 사용자의 보안 클래스와 접근된 파일의 클래스를 비교함으로서 사용자에 대한 파일의 접근여부를 결정하는 엄격한 접근통제 모델이다. 접근통제 모델의 보안 클래스에는 TS(Top Secrete), S(Secrete), C(Confidential), R(Restricted) 그리고 UR(Unrestricted)로 구성되며 TS>S>C>R>UR의 관계를 갖는다[2,5].

강제적 접근통제 모델은 비순환의 단방향 정보흐름을 위배하는 어떠한 행위도 명백히 금지하는 엄격한 정책으로 이 모델의 핵심은 주체와 객체 그리고 보안통제 단위에 대해 보안 기호를 명명하는 점이다. 이 모델은 부당한 사용자나 악의적인 프로그램으로부터 시스템이 피해를 받는것으로부터 예방을 할 수 있다.

2.3 역할기반 접근통제 모델

역할기반 접근통제 모델은 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. 사용자는 역할을 수행하기 위해서는 트랜잭션에 해당하는 세션을 설정한다.

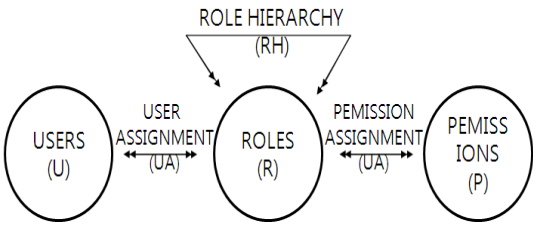

그림 1. 역할기반 접근통제 모델
Fig. 1. Role-Based Access Control Model

하나의 사용자가 여러 개의 역할을 동시에 수행할 수 있는 일 대 다 구조를 가질 수 있으며 사용자에 의해 자율적으로 생성, 변경, 소멸될 수 있다.계층성은 권한과 책임을 수반하는 구조적 역할이라 할 수 있다. 권한은 단계별로 해당역할을 계층성에 부여하며, 역할에 대한 감사 추적시 계층구조를 이용한다. 하위역할은 상위역할에 모든 허가사항을 상속하므로 상위역할은 자신의 허가사항 뿐만 아니라 하위 역할의 허가사항도 포함하게 된다[6].

2.4 Z 명세 언어

시스템을 개발하는데 있어서 개발을 의뢰한 고객 또는 실제 사용할 사용자의 요구사항과 다르게 구성되는 오류중 하나는, 시스템의 개발단계에서 비정형적인 요구사항 기술로 인한 부정확성, 모호성, 불완전성, 이해오류 등에 기인한다. 이러한 문제에 대한 방안으로 제시된 Z언어와 같은 명세 언어는 의미가 명확한 수학적 기호를 이용하고, 집합, 관계, 함수 등을 가지는 집합론에 기초를 두고 있다[7].

정형적 명세 언어인 Z는 시스템의 오퍼레이션 뿐만 아니라 시스템의 다양한 상태를 나타내는 스키마 구조를 포함하며 일반적으로 상태스키마(State Schema)와 오퍼레이션 스키마(Operation Schema)를 포함하고 있으며 이들 스키마는 다른 스키마에 의해 참조될 수 있도록 이름이 주어진다[8].

지금까지 기술된 접근통제 모델은 몇가지 문제점을 갖고 있다. 먼저, 임의적 접근통제 모델은 객체의 권한 연산이 어떤 한 주체에게 양도되면 아무런 제약사항이 없이 반복적인 재수행이 가능하기 때문에 정보의 안전성을 보장하지 못한다. 많은 보안상의 취약점이 반복적인 정보의 전송으로 인해 발생됨을 고려할 때 양도받은 주체는 또 다른 주체에게 재 양도될 수 있는 있기 때문에 정보의 비밀성과 무결성 측면에서는 적합하지 않다고 볼 수 있다. 더불어, 대규모 시스템에 접근통제 행렬을 구현할 경우 데이터베이스 측면에서 너무 많은 빈 공간이 발생하므로 저장 공간 낭비가 초래하여 시스템의 효율성을 떨어뜨리는 결과를 초래한다.

강제적 접근통제 모델은 보안 클래스를 주체와 객체에 부여하는 배정문제가 매우 복잡하고 배정 규칙을 기술하는 사항이 난해함으로 인해 실질적인 시스템에 적용하기에는 융통성과 편의성이 결여되여 있다는 문제점을 갖고 있다[4].

정보보호를 위한 기술적인 방법들은 다양하게 개발되어 있지만 어느 한 가지 방법으로 모든 정보보호 문제가 해결될 수 없다. 보다 효율적인 정보보호가 이루어지기 위해서는 다양한 정보보호 기능들을 적절히 도입하고 이에 대한 지속적인 관리 체계가 이루어져야 한다.

본 연구와 관련하여 기존에 연구되었던 BLP/BIBA 융합 접근통제 모델[17]에서는 모델에 대한 접근모드와 규칙을 기술하는데 반하여 본 논문에서는 이들 접근모드에 대한 정형적인 명세화와 알고리즘을 통해 구현시 시간과 비용을 줄일 수 있는 장점을 제공한다. 또한 본 논문이 제시한 모델은 강제적 접근통제 모델의 보안 클래스에대한 배정문제를 보다 명확히 해결하기 위해 단순한 읽기 쓰기와 같은 접근모드가 아니라 보다 실질적이고 광범위한 접근모드를 제시하므로서 융통성 있는 시스템을 제공한다. 그리고 정보의 활용성과 정보 보호 정도에 따라 데이터의 정보보호 보장을 위한 비밀성과 더불어 정보 공시가 목적인 무결성을 동시에 고려하는 차등적인 다중 보안등급을 갖는 모델을 제안하므로서 보다 효율성을 강화하였다. 또한, 기업에서 적용되는 상업적인 측면의 보안정책을 위하여 보안등급이 부여된 역할로 세분하므로서 조직이나 환경에 따라 역할이 재구성될 수 있는 유연성을 갖는다. 마지막으로 역할들의 제약조건들을 Z언어를 이용하여 정형화된 구조로 명확하게 표현함으로서 모델을 설계하고 구현할 경우 시간과 비용을 줄일 수 있는 장점을 갖는다.

III. 역할기반 다중 보안등급 접근통제 모델

3.1 기본 타입 정의

업무기반 역할그래프 모델은 사용자, 역할, 업무 그리고 권한의 개념을 사용한다. 권한은 객체에 대한 연산의 집합인 (x, m)으로 구성되는데, x는 객체, m은 x에 대한 접근 모드를 나타낸다. 논문에 필요한 기본타입과 이들을 Z 언어를 이용하여 정형적으로 기술하기 위하여 우리는 몇가지 정의를 기술하였다.

정의 1 : S는 주체의 집합으로 $s \in S$, O는 객체의 집합으로 $o \in O$를 갖는다. 각 주체와 객체에게는 허용된 비밀등급과 무결성 등급이 할당된다.

정의 2 : $L = \{(c,i) \times K \mid c \in C, i \in I\}$은 보안 레이블로서 C는 비밀성 등급의 집합이고 I는 무결성 등급의 집합 그리고 K는 카테고리 집합이다. 특히, C = {(ts, s, cf, r, ur}이고 I = {(cr, vi, i, uc)}이다. 비밀성 등급의 ts는 top secret, s는 secret, cf는 confidential, r은 restricted ur는 unrestricted 로서 ts>s>cf>r>ur의 관계를 갖는다. 무결성등급의 cr는 crucial, vi는 very important, i는 important, uc는 unclassified로서 cr>vi>i>uc의 관계를 갖는다.

정의 3 : M은 M은 접근모드의 집합으로 M = {v, a, m, c, g, d}을 갖는다. 여기에서 v는 관찰모드, a는 추가모드, m은 관찰과 변경이 가능한 수정모드, c는 객체의 상태 체크모드, g는 객체의 생성모드 , 마지막으로 d는 객체를 제거하는 삭제 모드를 의미한다.

정의 4 : req()은 접근요청 함수이며 R은 접근요청의 결과 집합으로 req:(s,o,m)→R∈{yes, no, error} 이다.. 모든 접근 요청은 다음 세가지 값중 하나를 갖는데, 주체 s가 m 모드를 갖는 객체 o를 부여받을 때 yes이고, 주체 s가 m 모드를 갖는 객체 o에 대해 거절될 때 no이고 두 개 이상의 값이 공존할 때 error이다.

정의 5 : 시스템 상태 V를 (b, A, f, H)로 정의한다. 여

기에서 b는 현재 접근 집합으로 b ∈ P(S×O×M)이며 이는 어떤 주체가 객체에 대해서 어떤 권한을 갖는지를 의미한다. 또한 여기에서 P(X)는 X의 모든 부분집합을 의미한다. A는 접근행렬의 집합이며 f는 4개의 튜플의 집합으로 fs(s), fc(s), fr(s), fo(o)으로 fs(s)는 주체의 보안등급함수, fc(s)는 주체의 현재 보안 등급 함수으로 fs(s)∝ fc(s)이며, fr(s)는 주체의 최대 보안등급 함수, fo(o)는 객체의 보안등급 함수를 의미한다. H는 계층 함수를 의미한다.

정의 6 : S/O = {(cs, cc, co), (is, ic, io) | (cs,cc,co)∈C, (is, ic, io)∈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.

□ 스키마 명세 정의

아래의 명세들은 본 모델에 사용되는 기본적인 스키마들을 Z언어를 기반으로 정형화한 내용이다.

READ_PRIV_SET

object : P_OBJECT
Access_mode : ACCESS_MODE

Access_mode : view, check

<읽기 권한 집합>

WRITE_PRIV_SET

object : P_OBJECT
Access_mode : ACCESS_MODE

Access_mode : modify, append

<쓰기 권한 집합>

GENERATE_PRIV_SET

object : P_OBJECT
Access_mode : ACCESS_MODE

Access_mode : generate

<생성 권한 집합>

DELETE_PRIV_SET

object : P_OBJECT
Access_mode : ACCESS_MODE

Access_mode : delete

<삭제 권한 집합>

ROLE

v_level, c_level : P_OBJECT
r_scope : READ_PREV_SET
m_level, a_level : P_OBJECT
w_scope : WRITE_PREV_SET
g_level : P_OBJECT
g_scope : GENERATE_PREV_SET
d_level : P_OBJECT
d_scope : DELETE_PREV_SET

<역할>

LEVEL_TO_INT

level_to_int : CON_LEVEL, INT_LEVEL → N

∀s : CON_LEVEL, 1 : N ·
(s = ts => l = 1) ∨
(s = s => l = 2) ∨
(s = cf => l = 3) ∨
(s = r => l = 4) ∨
(s = ur => l = 5)
∀s : INT_LEVEL, 1 : N ·
(s = cr => l = 1) ∨
(s = vi => l = 2) ∨
(s = i => l = 3) ∨
(s = uc => l = 4)

<등급 변환>

□ 역할/제약조건 정의

주체의 접근요청을 구현하기 위한 본 모델에 대한 주체와 객체의 비밀성 / 무결성 함수의 역할 및 제약 조건은 다음과 같다.

[view 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, view 역할 그리고 그 역할에 할당된 보안등급을 v-level이라 할 때 비밀성과 무결성에 관련된 주체가 view 역할에 배정되기 위한 제약조건은 비밀성 주체의 보안등급이 비밀성 객체의 역할 보안등급보다 크거나 같아야하며 무결성 주체의 보안등급이 무결성 객체의 역할 보안등급보다 적거나 같아야 한다. 이를 정형적으로 기술하며 다음과 같다.

VIEW_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
v_level : CON_LEVEL & INT_LEVEL

Level_to_int(Scc) ≥ level_to_int(v_level(Rco)) ∧
level_to_int(Sic) ≤ level_to_int(v_level(Rio))

[append 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, append 역할 그리고 그 역할에 할당된 보안등급을 a-level이라 할 때 비밀성과 무결성에 관련된 주체가 append 역할에 배정되기 위한 제약조건은 비밀성 주체의 보안등급이 비밀성 객체의 역할 보안등급보다 작거나 같아야하며 무결성 주체의 보안등급이 무결성 객체의 역할 보안등급보다 크거나 같아야 한다. 이를 정형적으로 기술하며 다음과 같다.

APPEND_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
a_level : CON_LEVEL & INT_LEVEL

Level_to_int(Scc) ≤ level_to_int(a_level(Rco)) ∧
level_to_int(Sic) ≥ level_to_int(a_level(Rio))

[modify 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, modify 역할 그리고 그 역할에 할당된 보안등급을 m-level이라 할 때 비밀성과 무결성에 관련된 주체가 modify 역할에 배정되기 위한 제약조건은 비밀성 주체의 보안등급이 비밀성 객체의 역할 보안등급과 같아야하며 무결성 주체의 보안등급이 무결성 객체의 역할 보안등급과 같아야 한다. 이를 정형적으로 기술하며 다음과 같다.

MODIFY_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
m_level : CON_LEVEL & INT_LEVEL

Level_to_int(Scc) = level_to_int(m_level(Rco)) ∧
level_to_int(Sic) = level_to_int(m_level(Rio))

[check 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, check 역할 그리고 그 역할에 할당된 보안등급을 c-level이라 할 때 비밀성과 무결성에 관련된 주체가 check 역할에 배정되기 위한 제약조건은 비밀성 주체의 현재 보안등급이 비밀성 객체의 역할 보안등급보다 크거나 같아야하며 무결성 주체의 현재 보안등급이 무결성 객체의 역할 보안등급보다 적거나 같아야 한다. 또한, 비밀성 주체의 최대 보안등급이 비밀성 객체의 역할 보안등급보다 크거나 같아야하며 무결성 주체의 최대 보안등급이 무결성 객체의 역할 보안등급보다 적거나 같아야 한다. 이를 정형적으로 기술하며 다음과 같다.

CHECK_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
c_level : CON_LEVEL & INT_LEVEL

[Level_to_int(Scc) ≥ level_to_int(c_level(Rco)) and
level_to_int(Sic) ≤ level_to_int(c_level(Rio))] ∨

[Level_to_int(Scs) ≥ level_to_int(c_level(Rco)) and
level_to_int(Sis) ≤ level_to_int(c_level(Rio))]

[generate 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, generate 역할 그리고 그 역할에 할당된 보안등급을 g-level이라 할 때 비밀성과 무결성에 관련된 주체가 generate 역할에 배정되기 위한 제약조건은 비밀성 주체의 현재 보안등급이 비밀성 객체의 역할 보안등급보다 크거나 같아야하며 무결성 주체의 현재 보안등급이 무결성 객체의 역할 보안등급보다 적거나 같아야 한다. 또한, 비밀성 주체의 현재 보안등급이 비밀성 객체의 역할 보안등급보다 작거나 같아야하며 무결성 주체의 현재 보안등급이 무결성 객체의 역할 보안등급보다 크거나 같아야 한다. 또한, 비밀성 주체의 보안등급이 비밀성 객체의 역할 보안등급과 같아야하며 무결성 주체의 보안등급이 무결성 객체의 역할 보안등급과 같아야 한다. 이를 정형적으로 기술하며 다음과 같다.

GENERATE_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
g_level : CON_LEVEL & INT_LEVEL

[Level_to_int(Scc) ≥ level_to_int(g_level(Rco)) and level_to_int(Sic) ≤ level_to_int(g_level(Rio))] ∨

[Level_to_int(Scc) ≤ level_to_int(g_level(Rco)) and level_to_int(Sic) ≥ level_to_int(g_level(Rio))] ∨

[Level_to_int(Scc) = level_to_int(g_level(Rco)) and level_to_int(Sic) = level_to_int(g_level(Rio))]

[delete 역할]

비밀성에 관련된 주체 Sc와 무결성에 관련된 주체 Si, delete 역할 그리고 그 역할에 할당된 보안등급을 d-level이라 할 때 비밀성과 무결성에 관련된 주체가 delete 역할에 배정되기 위한 제약조건은 generate 역할의 상반 개념으로 비밀성 주체의 현재의 보안등급이 비밀성 객체의 역할 보안등급보다 작아야 하며 무결성 주체의 현재 보안등급이 무결성 객체의 역할 보안등급보다 커야 한다. 또한, 비밀성 주체의 현재 보안등급이 비밀성 객체의 역할 보안등급보다 커야 하며 무결성 주체의 현재 보안등급이 무결성 객체의 역할 보안등급보다 작아야 한다. 또한, 비밀성 주체의 보안등급이 비밀성 객체의 역할 보안등급과 같지 않아야 하며 무결성 주체의 보안등급이 무결성 객체의 역할 보안등급과 같지 않아야 한다. 이를 정형적으로 기술하며 다음과 같다.

DELETE_ROLE_ASSIGN

Sc : CON_LEVEL, Si : INT_LEVEL
Level_to_int : CON_LEVEL → N, INT_LEVEL → N
d_level : CON_LEVEL & INT_LEVEL

¬[Level_to_int(Scc) ≥ level_to_int(d_level(Rco)) and level_to_int(Sic) ≤ level_to_int(d_level(Rio))] ∨

¬[Level_to_int(Scc) ≤ level_to_int(d_level(Rco)) and level_to_int(Sic) ≥ level_to_int(d_level(Rio))] ∨

¬[Level_to_int(Scc) = level_to_int(d_level(Rco)) and level_to_int(Sic) = level_to_int(d_level(Rio))]

3.2 알고리즘

View 역할에 대한 배정함수는 주체의 비밀성 보안등급이 객체의 보안등급을 지배하고 주체의 무결성 보안등급이 객체의 보안등급에 지배된다면 View 역할에 비밀성과 무결성에 대한 주체를 객체에 배정한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Rv)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
 IF  λ(Scc) ≥ v-level(Rco) AND λ(Sic) ≤
v-level(Rio)
 THEN
yes = RoleAssign(Sc&Si, Rv) ;
  ELSE
no = RoleAssign(Sc&Si, Rv) ;
END IF
```

Append 역할에 대한 배정함수는 주체의 비밀성 보안등급이 객체의 보안등급에 지배되고 주체의 무결성 보안등급이 객체의 보안등급을 지배한다면 Append 역할에 비밀성과 무결성에 대한 주체를 객체에 배정한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Ra)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
 IF  λ(Scc) ≤ a-level(Rco) AND λ(Sic) ≥
a-level(Rio)
  THEN
 yes = RoleAssign(Sc&Si, Ra) ;
   ELSE
 no = RoleAssign(Sc&Si, Ra) ;
 END IF
}
```

Modify 역할에 대한 배정함수는 주체의 비밀성 보안등급과 객체의 무결성 보안등급이 서로 동일하면 Modify 역할에 비밀성과 무결성에 대한 주체를 객체에 배정한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Rm)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
 IF  λ(Scc) = m-level(Rco) AND λ(Sic) =
m-level(Rio)
  THEN
 yes = RoleAssign(Sc&Si, Rm) ;
   ELSE
 no = RoleAssign(Sc&Si, Rm) ;
 END IF
}
```

Check 역할에 대한 배정함수는 주체의 비밀성 보안등급이 객체의 보안등급을 지배하고 주체의 무결성 보안등급이 객체의 보안등급에 지배되며, 주체의 현재의 비밀성 보안등급이 객체의 보안등급을 지배하고 주체의 현재의 무결성 보안등급이 객체의 보안등급에 지배되면 Check 역할에 비밀성과 무결성에 대한 주체를 객체에 배정한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Rc)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
 IF  [λ(Scc) ≥ c-level(Rco) and λ(Sic) ≤
c-level(Rio)] ∨ [λ(Scs) ≥ c-level(Rco) and λ(Sis) ≤
c-level(Rio)]
  THEN
 yes = RoleAssign(Sc&Si, Rc) ;
   ELSE
 no = RoleAssign(Sc&Si, Rc) ;
 END IF
}
```

Generate 역할에 대한 배정함수는 주체의 비밀성 보안등급이 객체의 보안등급을 지배하고 주체의 무결성 보안등급이 객체의 보안등급에 지배되는 경우, 주체의 비밀성 보안등급이 객체의 보안등급에 지배되거나 주체의 무결성 보안등급이 객체의 보안등급을 지배하는 경우 그리고 주체의 비밀성 등급과 무결성 등급이 객체의 보안등급과 동일한 경우에 Gernerate 역할에 비밀성과 무결성에 대한 주체를 객체에 배정한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Rg)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
```

```
IF  [λ(Scc) ≥ g-level(Rco) and λ(Sic) ≤
g-level(Rio)] ∨  [λ(Scc) ≤ g-level(Rco) and λ(Sic)
≥ g-level(Rio)] ∨ [ λ(Scc) = g-level(Rco) and λ(Sic)
= g-level(Rio) ]
 THEN
yes = RoleAssign(Sc&Si, Rg) ;
  ELSE
no = RoleAssign(Sc&Si, Rg) ;
END IF
}
```

마지막으로 Delete 역할의 경우는 Generate 역할의 반대개념으로 만약 더 이상 주체에 대한 역할이 배정되지 않아야 하는 상황의 경우 주체에 대한 역할을 삭제하는 Delete 역할이 수행되어야 한다. 이에 대한 역할배정함수는 다음과 같다.

```
char RoleAssign(int Sc, int Si, char Rd)
{
FOR ALL Sc, Si, Scc, Sic ∈S, Rco, Rio ∈R
IF ¬[λ(Scc) ≥ d-level(Rco) and λ(Sic) ≤
d-level(Rio)] ∨ ¬[λ(Scc) ≤ d-level(Rco) and λ(Sic)
≥ d-level(Rio)] ∨ ¬[ λ(Scc) = d-level(Rco) and λ
(Sic) = d-level(Rio) ]
 THEN
yes = RoleAssign(Sc&Si, Rd) ;
  ELSE
no = RoleAssign(Sc&Si, Rd) ;
END IF
}
```

본 모델을 위한 최종적인 알고리즘은 다음과 같다. 먼저 각각의 접근모드에 대한 값을 열거형 함수로 선언한 후 접근모드에 대한 각각의 값에 따라 해당하는 역할에 대한 배정함수를 수행하도록 한다.

```
BEGIN
FOR ALL m = {v, a, m, c, g, d } ∈ M  / *
{
 ENUM RoleAssignType {View, Append, Modify,
Check, Generate, Delete} RoleAssignValue;

 SWITCH ( RoleAssignValue)
 {
 CASE 0 : RoleAssign(Sc&Si, Rv); /* View 역할
배정함수
 BREAK;
 CASE 1 : RoleAssign(Sc&Si, Ra); /* Append 역
할 배정함수
 BREAK;
 CASE 2 : RoleAssign(Sc&Si, Rm); /* Modify 역
할 배정함수
 BREAK;
 CASE 3 : RoleAssign(Sc&Si, Rc); /* Chcck 역할
배정함수
 BREAK;
 CASE 4 : RoleAssign(Sc&Si, Rg); /* Generate 역
할 배정함수
 BREAK;
 CASE 5 : RoleAssign(Sc&Si, Rd); /* Delete 역할
배정함수
 }
 END SWITCH
END FOR
END BEGIN
```

Ⅳ. 결 론

정보통신 기술은 빠른 속도로 변하고 있으며 정보통신 기술의 변화가 정보통신산업의 구조를 바꾸어

나가고 있다. 새로운 기술이 나타나면 기존의 기업들은 변화를 요구받는데, 이 변화에 적응하지 못하는 기업은 순간적으로 사라지거나 합병되며 새로운 기업들이 빠른 속도로 성장한다. 이러한 시스템과 더불어 한 조직의 정보도 그 조직에 중요한 가치를 가지며 따라서 적절히 보호되어야 한다. 정보보호는 조직의 손실을 최소화하고 이익을 최대화하기 위하여 다양한 위협에서부터 정보를 보호하는 것이다. 이를 위해 정보보호는 비밀성, 무결성, 가용성의 3가지를 유지하고 보장하여야 한다.

본 논문에서는 강제적 접근통제 모델의 문제점인 주체와 객체에 보안 클래스를 부여하는 배정문제를 보다 명확히 해결하기 위해 단순한 읽기 쓰기와 같은 접근모드가 아니라 보다 실질적이고 광범위한 접근모드를 제시하므로서 융통성 있는 시스템을 제공한다. 그리고 정보의 활용성과 정보 보호 정도에 따라 데이터의 정보보호 보장을 위한 비밀성과 더불어 정보 공시가 목적인 무결성을 동시에 고려하는 차등적인 다중 보안등급을 갖는 모델을 제안하므로서 보다 효율성을 강화하였다. 또한, 기업에서 적용되는 상업적인 측면의 보안정책을 위하여 보안등급이 부여된 역할로 세분하므로서 조직이나 환경에 따라 역할이 재구성될 수 있는 유연성을 갖는다. 마지막으로 역할들의 제약조건들을 Z언어를 이용하여 정형화된 구조로 명확하게 표현함으로서 모델을 설계하고 구현할 경우 시간과 비용을 줄일 수 있는 장점을 갖는다.

참고문헌

[[1] Charles P. Pfleeger, Security In Computing, Prentice Hall, 1996.

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

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

[4] BAI Qing-hai, ZHENG Ying, "Study on the Access Control Model in Information Security", IEEE Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, pp.830-834, 2011.

[5]Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Prentice Hall, 1995.

[6] Ravi sandhu, David Ferraiolo, Richard Kuhn, "The NIST Model fo Role-Based Access Control:Towards A Unified Standard", Procedings of RBAC of ACM, pp47-63, 2000.

[7] David Rann, John Turner and Jenny Whitworth, Z : A Beginner's Guide, School of Computing Staffordshire University, 1994.

[8] Bryan Ratcliff, Introducing Specification Using Z : A Practical Case Study Approach, McGraw-Hill, 1994.

[9] Graeme Smith, The Object-Z Specification Language, Kluwer Academic Publishers, 1999.

[10]JiaJu WU, Chuan Yu XI, "The Study on Service Oriented Access Control Model", IEEE Int'l Conference on Information and Computing Science, pp.50-53, 2009.

[11]Kapil Singh, "xAccess:A Unified User-Centric Access Control Framework for Web Applications", IEEE Network Operations and Management Symposium, pp.530-533, 2012.

[12]Keith Irwin, Ting Yu, William H. Winsborough, "Enforcing Security Properties in Task-based Systems", IEEE Symposium on Access Control Models and Technologies, pp.41-50, 2008.

[13]M. Fahim Ferdous Khan, Ken Sakamura, "Context-Aware Access Control for Clinical Information Systems", IEEE Int'l Conference on Innovations in Information Technology, pp.123-128, 2012.

[14]Shaomin Zhang, Haiyan Zhang, Baoyi Wang, "Study on Centralized Authorization Model Supporting Multiple Aceess Control Models", IEEE Int'l Conference on Information Assurance and Security, pp.769-772, 2009.

[15]Yanfang Fan, Zhen Han, Jiqiang Liu, Yong Zhao, "A Mandatory Aceess Control Model with Enhanced Flexibility", IEEE Int'l Conference on Multimedia Information Networking and Security, pp.120-124, 2009.

[16]Zahid Rashid, Abdul Basit, Zahid Anwar, "TRDBAC :

Temporal Reflective Database Access Control", IEEE Int'l Conference on Emerging Technologies, pp.337-342, 2010.

[17] E.B. Choi, J.G. Park, “A BLP/BIBA union access model based on mandatory security property”, Jounal of The Korea Knowledge Information Technology Society, vol 5, no 6, pp. 111-121, 2010.

저자소개

최은복(Eun-Bok Choi)

1992년 전남대학교 전산학과 졸업
1996년 전남대학교 전산학과 대학원 석사
2000년 전남대학교 전산학과 대학원 박사

2002년~ 현재 전주대학교 스마트미디어학부 교수
※ 관심분야 : 통신망관리보안, 홈 네트워크, 접근통제, IPTV 보안 등