논문 99-24-6T-4 한국통신학회논문지 '99-6 Vol.24 No.6T

통신망 관리정보베이스의 역할기반 접근제어에 관한 연구

정회원 김 종 덕*

A Study on Role-based Access Control of Communication Network Management Information Base

Jong-Duk Kim* *Regular Member*

요 약

통신망관리 시스템의 여러 가지 구성 요소들 중 가장 핵심적인 요소 중의 하나는 통신망관리에 필요한 정보들인 관리 객체들의 개념적인 저장소인 관리 정보베이스이다. 관리 정보베이스에 저장된 관리 객체들은 통신망관리에 필수적이며 중요한 모든 정보들을 유지하고 있기 때문에 안전하게 유지 되어야 한다. 본 논문에서는 관리정보베이스에 대한 접근 제어 보안 모델을 정의한 ISO/IEC 10164-9 권고안을 바탕으로 기존의 표준 관리 객체 클래스 구조를 크게 확장 및 보완하였다. 즉 확장된 관리 객체 클래스 구조에서는 역할기반 접근 제어를 위한 역할 관리 객체 클래스를표현하였으며 규칙의 구조를 보다 명확히 하기 위해 명시적 규칙과 묵시적 규칙으로 세분화함으로써 접근 제어 규칙의 명확성과 함께 융통성을 크게 보장하였다. 또한 권고안과 확장된 모델에서 정의된 GDMO(Guideline Definition of Managed Object)의 비정형적인 표현을 명세언어 Z를 이용해 정형화된 구조로 표현하였다.

ABSTRACT

MIB(Management Information Base), one of the key components of communication network management system, is a conceptual repository for the information of the various managed objects. MIB stores and manages all the structural and operational data of each managed resources. Therefore, MIB should be protected properly from inadvertant user access or malicious attacks. International standard ISO/IEC 10164-9 describes several managed object classes for the enforcement of MIB security. Those managed object classes described access control rules for security policy. But the exact authorization procedures using those newly added managed object classes are not presented. In this paper, we divide managed object classes into two groups, explicit and implicit ones, and describe the access authorization procedure in Z specification language. Using Z as a description method for both authorization procedure and GDMO's action part, the behaviour of each managed object class and access authorization procedure is more precisely and formally defined than those of natural language form.

I. 서 론

통신망 관리정보베이스에 대한 접근 제어의 목적은 망의 합법적인 사용자들이 수행할 수 있는 동작이나 연산을 제어함으로써 통신망관리 정보를 안전하게 유지하는데 있다.

ISO/IEC 10164-9(Objects and Attributes for Access Control) 권고안(국제표준)에 망관리 정보의 접근 제어를 위한 포괄적인 클래스 정의 및 접근 제어 보안 모델을 정의하였다. 권고안에 정의된 접근 제어를 위한 관리 객체 클래스 구조는 접근 제어 정책중 자율적 접근 제어(DAC : Discretionary

* 전남도립 담양대학 전산·정보통신공학부
논문번호 : 99001-0303, 접수일자 : 1999년 3월 3일

Access Control) 정책인 접근 제어 리스트(Access Control List) 스킴과 능력(Capability) 스킴, 그리고 강제적 접근 제어(MAC: Mandatory Access Control) 정책인 레이블 기반(Label based) 스킴에 대해서만 정의를 하였을 뿐, DAC과 MAC의 단점을 보완한 새로운 접근 제어 정책으로서 최근 들어 활발히 연구가 진행되고 있는 역할 기반 접근 제어(RAC: Role-based Access Control) 정책에 대한 정의가 포함되어있지 않다. 그리고 접근 제어를 위한 각종 관련 정보 및 규칙을 보안관리자가 사전에 정의해 놓은 명시적인 접근 규칙(Explicit Access Rule)만을 정의함으로써 망의 규모가 점점 확대되고 이로 인한 관리 객체의 수가 급격히 증가되는 경우에 모든 관리 객체에 대해서 명시적 규칙을 낱낱이 정의하기가 사실상 불가능하다. 또한 접근 제어 규칙 수행 중에 각 관리 객체 클래스간의 계층구조에 의한 상호관련성에 의해 수시로 발생할 수 있는 규칙 또한 정의하기가 무척 어렵다. 따라서 이에 대한 보완책으로서 기존의 권고안 구조에 묵시적인 규칙(Implicit Access Rule)을 포함시킴으로써 명시되지 않은 규칙에 대해서도 관리 객체간의 상호 관계를 이용해 접근 제어 규칙을 융통성 있게 적용하여 보안관리자의 권한부여를 크게 단순화 시킬 수 있고 각 규칙을 따로따로 정의하는데 따른 부가적인 간접경비를 대폭 줄일 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관리정보베이스에 대한 접근 제어 정책을 설명하고 3장에서는 ISO/IEC 10164-9 권고안의 접근 제어 관리 객체 클래스 표준 구조를 설명한다. 그리고 4장에서는 역할기반 접근 제어를 위한 확장된 접근 제어 관리 객체 클래스 구조를 설명하고, 명세언어 Z를 이용해 GDMO의 비정형적인 표현을 정형화된 구조로 명세화한 후 역할기반 접근 제어 정책에 대한 접근제어 규칙의 타당성을 검증한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관리 정보베이스 접근제어 정책

1. 자율적 접근 제어 정책

자율적 접근 제어는 접근을 요청한 관리자의 신원(identification)에 근거를 두고 있다. '자율적'이라고 하는 말은 관리자가 관리 객체에 대한 접근 권한을 자율적으로 부여하거나 철회할 수 있다는 것을 의미한다. 이것은 접근 권한의 통제가 관리 객체의 각 소유자에 의하여 분산화되어 수행됨을 의미하지만, 이러한 통제는 보안 관리자에 의하여 중앙집중적으로 수행될 수도 있다.

자율적 접근 제어를 구현하기 위한 메카니즘에는 접근 제어 리스트 방법과 능력 리스트 방법이 있다.

2. 강제적 접근 제어 정책

강제적 접근 제어는 자율적 접근 제어와는 달리 관리자와 관리 객체에 부여된 보안 등급을 기반으로 접근을 제어하는 방법이다. 각각의 관리자와 관리 객체에게는 보안 등급이 부여되며, 특히 사용자의 보안 등급을 인가 등급(clearance level)이라고도 한다. 강제적 접근 제어 정책을 이용한 대표적인 예로 BLP(Bell and LaPadula) 모델이 있다[1].

3. 역할기반 접근 제어 정책

강제적 접근 제어 정책이 군대와 같은 엄격한 보안 통제를 필요로 하는 환경에서 개발되었고, 자율적 접근 제어는 학술 연구 단체와 같은 자율적이고 협동적인 환경에서 개발되었기 때문에, 두 보안 정책이 모두 상업적인 분야에 적용하기에는 다소 부적합한 면이 있다. 따라서 전통적인 자율적 접근 제어에서처럼 사용자나 사용자의 그룹에게 객체에 대한 접근 권한을 부여하고, 강제적 접근 제어에서처럼 접근 권한을 부여하는데 제한을 가할 수 있는 접근 제어 방법에 대한 연구가 진행되었다. 그 결과로서 역할기반 접근 제어 정책이 만들어지게 되었다.

역할기반 접근 제어 정책에서는 데이타 또는 객체를 몇 개의 범주로 나누었으며, 여러 명의 사용자는 역할이라고 하는 클래스들로 그룹화 되어진다. 역할은 어떤 조직체의 사용자들의 임무를 여러 개의 영역으로 분할해 놓은 것으로서 역할 이름과 범주에 접근할 수 있는 권한으로 구성되어 있다.

역할기반 접근 제어 정책은 자율적 접근 제어와 강제적 접근 제어의 장점을 모두 가지고 있으며, 개개의 관리자가 아닌 역할 단위로 접근을 통제하므로써 관리자의 역할 변화에 따른 접근 권한의 감독 및 관리를 용이하게 할 수 있는 장점을 가지고 있다[2]. 따라서 본 논문에서는 최근 들어 활발히 연구가 진행되고 있는 역할기반 접근 제어 정책을 이용하고자 한다.

Ⅲ. 접근 제어 관리 객체 클래스 표준 구조

다음 그림 1은 ISO/IEC 10164-9 권고안(국제표준)에 정의된 관리 객체 클래스들의 상속 계층구조

로서 여기에는 접근 제어를 위해 필요한 관리 객체들을 모형화하여 계층구조로 표현하였다. 권고안에는 자율적 접근 제어 정책과 강제적 접근 제어 정책에 관련한 관리 객체들을 포함하고 있다.

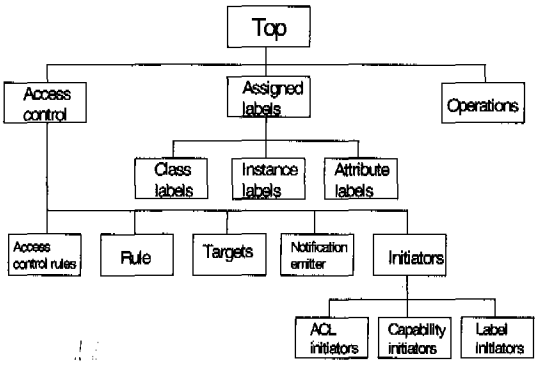


그림 1. 관리 객체 클래스 상속 계층구조

다음 그림 2는 그림 1에서 정의된 관리 객체 클래스 상속 계층구조를 이용해 관리 객체들 간의 상호관계를 나타낸 것이다.

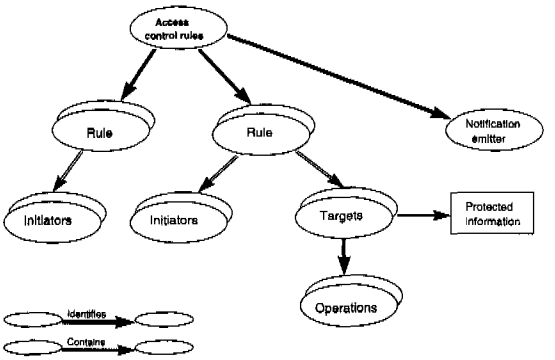


그림 2. 관리 객체 상호관계

Ⅳ. 확장된 접근 제어 관리 객체 클래 스 구조

1. 관리 객체 클래스 계층 구조

권고안(국제표준)에 정의된 접근 제어를 위한 관리 객체 클래스 구조는 접근 제어 정책중 자율적 접근 제어 정책인 접근 제어 리스트(Access Control List) 스킴과 능력(Capability) 스킴, 그리고 강제적 접근 제어 정책인 레이블 기반(Label based) 스킴에 대해서만 정의를 하였을 뿐, 자율적 접근 제어 정책과 강제적 접근 제어 정책의 단점을 보완한 새로운 접근 제어 정책으로써 최근 들어 활발히 연구가 진행되고 있는 역할기반 접근 제어 정책에 대한 정의가 포함되어있지 않다. 따라서 이에 대한 보완책으로써 기존의 표준구조에 역할기반 관련 객체 클래스와 속성을 정의해서 포함시킬 필요가 있다[3][4].

그리고 접근 제어를 위한 각종 관련 정보 및 규칙을 보안관리자가 사전에 정의해 놓은 명시적인 접근 규칙(Explicit Access Rule)만을 정의함으로써 망의 규모가 점점 확대되고 이로 인한 관리 객체의 수가 급격히 증가되는 경우에 모든 관리 객체에 대해서 명시적 규칙을 낱낱이 정의하기가 사실상 불가능하다. 또한 접근 제어 규칙 수행 중에 각 관리 객체 클래스간의 상호관계에 의해 수시로 발생할 수 있는 접근 제어 규칙 또한 정의하기가 무척 어렵다. 따라서 이에 대한 보완책으로서 기존의 권고안 구조에 묵시적인 규칙(Implicit Access Rule)을 포함시킴으로써 명시되지 않은 규칙에 대해서도 관리 객체간의 상호 관계를 이용해 접근 제어 규칙을 융통성 있게 적용함으로써 보안관리자의 권한부여관리를 크게 단순화 시킬 수 있고 각 규칙을 따로따로 정의하는데 따른 부가적인 간접경비를 대폭 줄일 수 있다.

다음 그림 3은 그림 2의 표준 관리 객체 클래스 계층구조를 확장한 것으로써 여기에는 규칙의 구조를 보다 명확하게 구체화 하기 위해 명시적인 규칙(Explicit Rule)과 묵시적인 규칙(Implicit Rule)을 구분하였다.

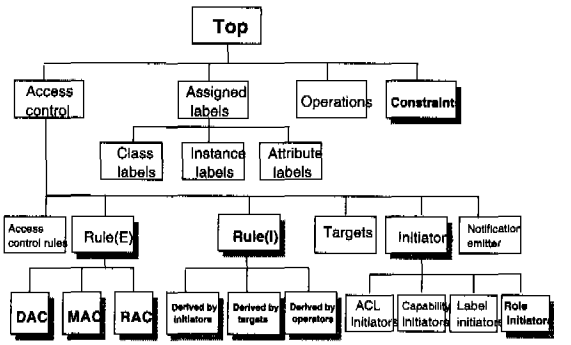


그림 3. 확장된 관리객체 클래스 상속계층 구조

명시적인 규칙은 Rule(E)에서 DAC, MAC, RAC 관리 객체 클래스로 세분화시키고, 묵시적인 규칙은 Rule(I)에서 Initiators와 Targets 그리고 Operators 관리 객체 클래스로 세분화시킴으로써 계층구조에 의한 상호관계에 의해 파생되는 묵시적인 규칙에 대해서도 효율적인 접근 제어가 가능하다. 또한 RAC 정책을 지원하기 위해 Initiators 관리 객체에

Role initiators 관리 객체를 추가시킴으로써 DAC과 MAC의 단점을 보완하므로서 기존의 표준 구조를 크게 확장하였다.

2. 관리 객체 상호 관계

위에서 정의한 확장된 관리 객체 클래스 상속 계층 구조에 의해 관리 객체간의 상호관계 중에서 역할기반 접근 제어에 대해 나타내면 그림 4와 같다.

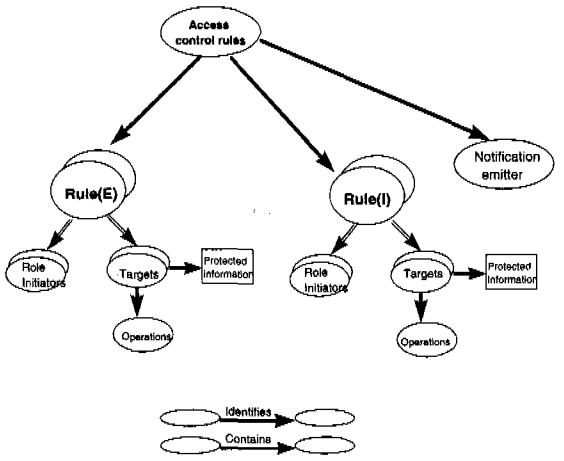


그림 4. 관리객체 상호관계(역할기반 접근 제어)

3. 접근 제어 모델링

여기서는 ISO/IEC 10164-9 권고안을 바탕으로 확장된 역할기반 접근 제어 정책을 Z 명세언어를 이용하여 모형화 하고자한다[5].

역할기반 접근 제어 정책에 필요한 관리 객체 및 속성을 중심으로, 권고안의 기본구조와 함께 확장된 구조에서는 'Role Initiators'를 추가하여 역할기반에 의한 접근 제어가 가능하도록 하였다. 그리고 명시적 규칙과 묵시적 규칙에 대해서도 접근이 허용되는 경우와 허용되지 않는 경우를 접근 제어 규칙으로서 정의하였으며, 이와 관련한 관리 객체 클래스에 대해 스키마 정의 및 제약사항을 명세언어 Z를 이용해 나타냄으로써, GDMO의 비정형화된 행위 부분이 정형화된 구조로 명확하게 표현되어 역할기반 접근 제어 규칙에 대한 타당성 및 보안검증이 용이해졌다[6].

다음은 역할기반 접근 제어 관련 관리 객체 클래스들과 속성을 이용하여 역할기반 접근 제어가 이루어지는 모형화에 대한 Z 표현이다.

위의 스키마 구조는 역할기반 접근 제어에 대한 Z표현으로서 roleinitiator가 해당 target 및 operator

MIBAccess_Validation

ΞMIB
roleInitiator? : InitiatorName
operator? : OperationType
object? : ManagedObject
evaluation! : BOOLEAN

((∃ rule : Rule • roleInitiator? ∈ rule.roleInitiatorsList ∧
object? ∈ rule.targetsList.managedObjectClasses ∨
object? ∈ rule.targetsList.managedObjectInstances) ∧
operator? ∈ rule.targetsList.operationsList) **//Explicit//**
∨
(∃ rule : Rule; ∃i ∈ AccessPropagatedByRoleInitiator(roleIinitiator?);
∃op ∈ AccessPropagatedByOperator(operator?);
∃obj ∈ AccessPropagatedByObject(object?) •
i ∈ rule.roleInitiatorsList ∪ {roleInitiator?} ∧
(obj ∈ rule.targetsList.managedObjectClasses ∪ {object?} ∨
obj ∈ rule.targetsList.managedObjectInstances ∪ {object?}) ∧
op ∈ rule.targetsList.operationsList ∪ {operator?}) **//Implicit//**
⇔ evaluation! = True

에 의해 접근 제어가 수행되는 절차를 명시하고 있으며 또한 관리 정보베이스에 저장된 관리 객체 데이터에 대한 접근 요청을 보안 관리자에 의해 기술된 명시적 규칙과 접근 요청 'initiator', 'operator', 관리 객체별 상속특성에 의해 추론된 묵시적 규칙을 이용한 접근 규칙을 규정하고 있다.

위의 스키마 구조에서 묵시적인 규칙을 적용하기 위해 필요한 관리 객체, 접근 'roleinitiator'간의 계층 구조 및 'operator' 특성에 따른 접근 권한 전파(propagation) 특성은 다음과 같다[7][8].

■ 접근 요청 'roleinitiator'

망관리 정보베이스에 접근할 수 있는 사용자 역할(roleinitiator)간 계층 구조에 의해 접근 권한은 상위 계층으로부터 하위 계층으로 전파된다.

■ 접근 요청 'operator'

ISO/IEC 10164-9 권고안에 제시된 9개의 관리 operation은 그 동작 특성에 따라 크게 3개의 그룹으로 분류되며 접근 권한은 상위 그룹에서 하위 그룹으로 전파되는 특성을 갖는다.

■ 접근 요청 'object'

망관리 정보베이스에 저장되는 관리 객체 클래스간의 계층 구조와 관계에 의해 관리 객체 클래스간의 접근 권한 전파 특성이 달라진다. 일반화(generalization) 관계와 집단화(aggregation) 관계에서의 접근 권한 전파 특성은 일반적으로 상위 객체 클래스에서 하위 객체 클래스로 전달되지만, 집단화의 경우는 상위 객체 클래스에서 접근이 허용된 부분만이 하위 객체 클래스에서 접근이 허용된다.

망관리 정보베이스 접근 요청에 대한 타당성 검증중 묵시적 규칙은 주어진 접근 제어 요청에 대해 위의 접근 권한 전파 특성을 이용하여 구성한 추론된 접근 제어 규칙 집합에 하나 이상의 명시적 규칙이 포함되어 있는지를 확인하는 과정이다[9].

□ 추론된 접근 제어 규칙

: {(inf-initiator, inf-operator, inf-object)}, where
inf-initiator ∈ AccessPropagatedByIniiator(initiator?)
inf-operator ∈ AccessPropagatedByOperator(operator?)
inf-object ∈ AccessPropagatedByTarget(object?)

- AccessPropagatedByInitiator(initiator?), APBI(initiator?) : initiator들의 계층 구조 에서 initiator?의 하위 계층에 속하는 initiator 집합 계산 함수
- AccessPropagatedByOperator(operator?), APBO(operator?) : operator들의 계층 구조에서 operator?의 상위 계층에 속하는 operator 집합 계산 함수
- AccessPropagatedByTarget(object?), APBT(object?) : 관리 대상 객체 클래스 계층 구조에서 object?의 상위 클래스 집합 계산 함수

위의 APBI(roleinitiator?),APBO(operator?), APBT(object?) 계산 함수는 확장된 접근 제어 관리 객체 클래스 DerivedByInitiator, DerivedByOperator, DerivedByTarget 속성에 저장된 값을 이용, 추론된 접근 제어 규칙을 생성한다.

4. 접근 제어 시스템 검증 예

여기에서는 망관리 정보베이스에 대한 확장된 접근 제어 규칙이 실제 적용될 수 있는 프린터 관리 정보베이스를 모델링하고자 한다. 모델의 구성요소는 네트워크에 의해 연결된 주변장치인 프린터로서 계층구조로 구성된 프린터 자원에 대해서 다음 세 가지 유형의 사용자, 즉 일반 사용자, 중간 관리자, 그리고 시스템 관리자가 각각 프린터 자원에 대해 접근 요청을 했을 때 각 권한에 따른 적절한 접근 제어가 네트워크 상에서 이루어지는가를 살펴보는 것이다. 위에서 정의한 프린터 관리 정보베이스에 대한 관리 객체를 OMT(Object Modeling Technique) 표기법에 의해 나타내면 다음 그림 5와 같다[10][11].

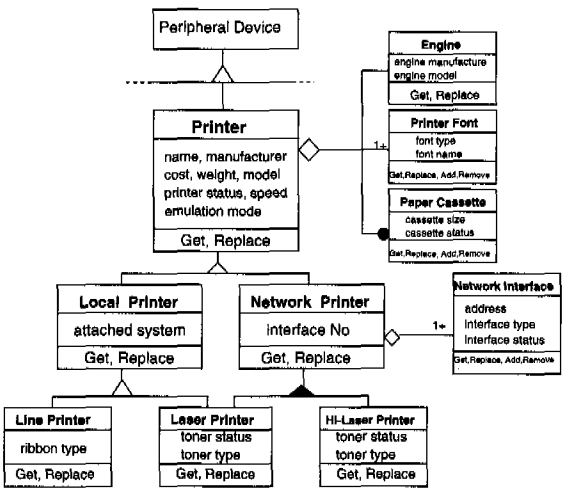


그림 5. 프린터 망관리 정보베이스 모델

프린터 망관리 정보베이스의 관리 객체에 접근하는 사용자의 계층구조는 크게 일반 사용자 층과 중간 관리자층, 그리고 시스템 관리자층으로 구분되며 접근 권한은 시스템 사용자가 가장 높다.

앞에서 정의한 접근 제어 규칙이 프린터 관리 정보베이스의 각 관리 객체에 대해 접근하려고 할 때, 각 사용자의 접근요청에 대해 명시적인 규칙은 물론 묵시적인 규칙에 대해서도 적절한 접근 제어가 이루어지는가를 확인해 봄으로써 접근 제어 규칙에 대한 수행 및 접근 제어 검증을 하고자한다.

명시적 규칙과 묵시적 규칙에 따른 접근 규칙의 구조는 다음과 같다.

(Initiator, Target, {Access_Type})

먼저, 자율적 접근 제어 규칙을 적용해보기위해 시스템 보안 관리자에 의해 사전에 각 관리 객체에 부여된 명시적 규칙은 다음과 같다.

□ **명시적 규칙(Explicit Rule)**

(U1, Printer, {all})
(U2, Local Printer, {get, replace})
(U3, Network Printer, {replace})
(U4, Local Printer, {print})
(U5, Laser Printer, {get})

여기서 get 오퍼레이션은 CMIP 오퍼레이션의 READ 그룹 오퍼레이션에 해당하고, replace 오퍼레이션은 CMIP 오퍼레이션의 WRITE 그룹 오퍼레이션에 해당한다. 그리고 print 오퍼레이션은 CMIP 오퍼레이션의 create, delete, action을 포함한 MANAGE 그룹 오퍼레이션에 해당한다. 위에서 정의된 명시적 규칙에 의한 접근 제어는 해당 규칙과 일치하는 접근 요청에 대해서만 망관리 정보베이스에 대한 접근을 허용한다.

다음에는 명시적 규칙에 정의되어 있지 않은 관리 객체에 대해 접근을 요청하는 경우, 즉 묵시적 규칙(Implicit Rule)에 대한 접근을 제어하는 과정을 살펴보자.

□ **접근 요청1**

(U3, Network Printer, getInterfaceNo)
중간 관리자 U3가 Network Printer에 대해 InterfaceNo 속성값을 가져오기 위해 접근을 요청한다.

이때 접근 요청1에 대한 명시적 규칙은 정의가 되어 있지 않으므로 묵시적인 규칙을 적용하기 위해서는 관리 객체 클래스간의 계층구조를 분석하여 해당 관리 객체를 필터링 해주는 함수를 이용하여 해당 관리 객체를 추출한 후 규칙을 만족하면 접근을 허용하고 그렇지 않으면 접근을 허용하지 않는다.

각 관리 객체에 대해 추론된 접근 제어 규칙을 생성하여 적용해보면 다음과 같다.

APBI(U3) = {U4,U5} ∪ {U3} = {**U3**,U4,U5}
APBT(Network Printer) = {Printer} ∪ {Network Printer} = {Printer, **Network Printer**}
APBO(getInterfaceNo) =
{create, delete, action, replace, addMember, removeMember, replaceWithDefault} ∪ {get} = {create, delete, action, **replace**, addMember, removeMember, replaceWithDefault, get}
Evaluation Result ⇒ **Grant**

위의 결과를 분석해 보면 접근 요청1에 대한 명시적 규칙은 정의되어 있지 않으나 묵시적 규칙에 의해 각 관리 객체를 추출해 보면 결국 U3에 대한 명시적 규칙(U3, Network Printer, {replace}) 이 적용됨으로써 접근 요청1에 대해 접근을 허용(Grant)한다는 것을 알 수 있다.

□ **접근 요청2**

(U2, Hi-Laser Printer, print)
중간 관리자 U2가 Hi-Laser Printer 대한 접근 요청이다.

접근 요청1에서와 같은 방법으로 추론된 접근 제어 규칙을 생성하여 적용해보면 다음과 같다.

APBI(U2) = {U2, U4}
APBT(Hi-Laser Printer} = {Hi-Laser Printer} ∪ {Network Printer} ∪ {Printer} = {Hi-Laser Printer, Network Printer, Printer}
APBO(print) = ∅ ∪ {print} = {print}
Evaluation Result ⇒ **Deny**

위의 결과를 분석해 보면 접근 요청2에 대한 명시적 규칙이 정의되어 있지 않아 묵시적 규칙에 의해 각 관리 객체를 추출해 보았으나 U2 및 U4에 대한 명시적 규칙이 적용되지 않아 결국 접근 요청2에 대해 접근을 거절한다는 것을 알 수 있다.

V. 결 론

통신망관리 시스템의 여러 가지 구성 요소들 중

가장 핵심적인 요소 중의 하나는 망관리에 필요한 정보들인 관리 객체들의 개념적인 저장소인 망관리 정보베이스이다. 망관리 정보베이스에 저장된 관리 객체들은 망관리에 필수적이며 중요한 모든 정보들을 유지하고 있기 때문에 안전하게 유지되어야 한다.

본 논문에서는 접근 제어를 위한 포괄적인 클래스 정의 및 접근 제어 보안 모델을 정의한 ISO/IEC 10164-9 권고안을 바탕으로 기존의 표준 관리 객체 클래스 구조를 크게 확장 및 보완하였다. 즉 확장된 관리 객체 클래스 구조에서는 역할기반 접근 제어를 위한 역할 관리 객체 클래스를 표현하였으며 규칙의 구조를 보다 명확히 하기 위해 명시적 규칙과 묵시적 규칙으로 세분화함므로써 접근 제어 규칙의 명확성과 함께 융통성을 크게 보장하였다. 또한 권고안과 확장된 모델에서 정의된 GDMO의 비정형적인 표현을 명세언어 Z를 이용해 정형화된 구조로 표현함으로써 관리 객체간의 연관성은 물론 접근 제어 규칙에 대한 세부적인 명세가 가능하여 역할 기반 접근 제어 정책에 따른 접근 제어 규칙의 보안 검증이 가능하다.

추후 연구 방향은 관리 정보베이스에 대한 접근 제어뿐만 아니라, 사용자 및 데이타에 대한 인증 서비스 기능을 추가하고자 한다.

참 고 문 헌

[1] David d. Clark, David R. Wilson, "A Comparison of commercial and Military computer security policies," IEEE, 1987.

[2] Matunda Nyanchama, Sylvia Osborn, "Role-Based Security, Object Oriented Databases & Separation of Duty," SIGMOD RECORD, Vol. 22, No. 4, December 1993, pp. 45-51.

[3] ISO/IEC 10165-1/ITU-T X.720 "Management Information Model," 1992.

[4] ISO/IEC 10165-2/ITU-T X.721, "Definition of Management Information," 1992.

[5] ISO/IEC 10165-4/ITU-T X.722, "Guidelines for the Definition of Managed Objects," 1992.

[6] ISO/IEC 10164-3/ITU-T X.732, "Attributes for Representing Relationships," 1992.

[7] ISO/IEC 10164-9/ITU-T X.741, "Objects and Attributes for Access Control"

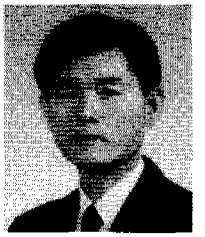
[8] David Rann John Turner and Jenny Whitworth, "Z: A Beginner's Guide," School of Computing Staffordshire University UK, 1994.

[9] E. B. Fernandez, R. B. France, and D. Wei, "A formal specification of an authorization model for object-oriented database," Workshops in Computing security for object-oriented systems, Washington DC, 1996

[10] ISO/IEC 0165-4/ITU-TX.722, "Guidelines for the Definition of Managed Objects," 1992.

[11] ISO/IEC10164-3/ITU-TX.732, "Attributes for Representing Relationships," 1992.

김 종 덕(Jong Duk Kim) 정회원



1983년 : 전남대학교 전산학과 졸업(이학사)

1988년 : 국방대학원 전자계산학과 졸업(이학석사)

1997년 : 전남대학교 대학원 전산통계학과 졸업(이학박사)

1995년~1997년 : 전남대학교 전산학과 시간강사

1998년~현재 : 전남도립 담양대학 전산·정보통신공학부 전임강사

<주관심 분야> 통신망관리, 정보통신 보안, 객체지향 시스템