망관리 객체에 대한 접근제어 모델의 상호연동 및 정형적 기술

최은복°, 이형효, 노봉남

전남대학교 전산학과

Interworking and Formal Description of Access Control Models for Managed Object

EunBok Choi, HyungHyo Lee, BongNam Noh
Dept. of Computer Science, Chonnam National University

요 약

본 논문에서는 ITU-T 권고안에 정의된 강제적 접근제어 모델과 역할기반 접근제어 모델을 상호연동한 모델의 관리객체 상호관계구조를 정의하였다. 또한 관리속성값을 제어하는 관리연산을 연관된 유형별로 묶어 역할로 정의하였으며 관리자와 관리객체에 보안등급을 부여함으로써 무결성을 보장하고 관리자 관리객체 사이에 역할을 배정하므로써 실생활에 적용될 수 있는 접근제어 모델을 제시하였다. 그리고 역할배정규칙과 제약조건을 기반으로 하여 'rule' 관리객체 클래스의 접근제어 결정함수와 접근제어 집행함수의 동작과정을 동적특성 기술언어를 사용하여 체계적이고 정형적으로 기술하였다.

1. 서 론

통신망 관리시스템은 이질적 통신기술과 컴퓨터 네트워크로 구성된 통신망의 통합적인 관리기능의 수행을 위하여 관리대상 통신망 구성요소들의 특성 중 통신망 관리에 필요한 정적, 동적 정보만을 추출, 추상화한 관리객체(managed object)로 모델링한다. ITU-T X.741 표준안[X741]에서는 접근제어 관리정보에 표현된 접근제어 정책에 따라 원하는 관리 객체에 대한 접근을 허가하거나 금지시키는데 사용되는 관리객체와 속성들을 기술하고 있다. 또한 ITU-T의 X.722[X722]에 기술된 GDMO(Guidelines for the Definition of Managed Objects) 표현법은 9가지 템플릿을 이용하여 관리객체의 정적 속성과 동적 특성 외에, 통신망 관리시스템에게 관리객체 내부에서 관리상에 주요한 사항이 발생했음을 알리는 통지(notification)에 대해서 자세히 기술하고 있다.

정보 통신망의 관리 정보를 이용하는 사용자의 환경이 동적으로 변화하는 현대의 네트워크 환경에서는 접근제어 정책을 어느 하나의 정책에 근거한 일괄적 정의로는 부적절하다. 따라서 실질적인 접근제어 시스템에 적용이 가능하도록 관련된 몇 가지 정책들간의 연관성을 연구할 필요가 있다.

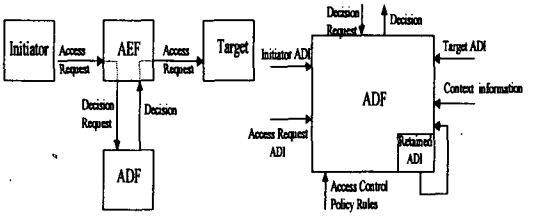
본 논문에서는 망관리 객체에 대한 접근제어 모델을 상호연동한 관리객체 상호관계구조와 관리정보의 무결성을 보장하고 실생활에 적용되어질 수 있도록 주체와 객체에 보안등급과 역할을 부여하였다. 그리고 상호연동한 접근제어 모델의 보안규칙과 제약조건을 기반으로 한 접근제어결정함수와 접근제어 집행함수를 동적특성 기술언어[최99]를 이용하여 체계적이고 정형적으로 기술하였다.

2. 관리정보베이스의 접근제어

망 자원에 접근을 원하는 사용자가 자신의 신원을 제시하고 인증 시스템으로부터 신원 인증을 받은 후, 확인된 사용자에 대한 망 자원을 접근하는 권한을 확인하는 과정을 접근 제어라고 한다. 접근제어는 컴퓨터 시스템의 합법적인 사용자가 수행하는 연산이나 행위를 제한하는 것이다. 이러한 접근제어를 효과적으로 수행하기 위해서는 접근권한의 불법 취득을 방지하고, 접근 권한에 관한 불법 변조가 일어나지 않도록 하여야 한다.

☑ 접근제어 기능 모델

기본적인 접근제어의 수행을 위한 기능모델이 그림 1에서 나타내고 있다. 접근제어에 관련된 기본적인 개체와 기능은 접근을 요청하는 관리자나 프로세스에 해당하는 initiator, 접근요청을 접근제어결정함수(ADF)에 전송하고 접근에 대한 응답을 처리하는 접근제어집행함수(AEF), 접근제어집행함수로부터 전송받은 접근요청의 가부를 결정하는 접근제어결정함수, 그리고 실제 관리객체에 해당하는 target 으로 나뉠 수 있다[X741].



(그림 1) 접근제어 기능 모델

대표적인 접근제어 모델인 Biba 모델과 역할기반 접근제어 모델의 특성은 다음과 같다.

☑ Biba 모델

BLP모델은 권한을 갖지 않는 사용자에게 정보가 흘러가는 것을 예방하는 비밀성에 기반을 둔 모델이다. 이 모델은 정보의 비밀성은 보장하지만 등급이 낮은 주체가 등급이 높은 객체 정보를 쓸 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 Biba 모델이 제안되었다. Biba 모델은 다음의 보안 성질을 갖는다[Cas94].

- Simple integrity : 주체의 무결성 등급이 객체의 무결성 등급에 지배된다면 주체는 객체에 읽기 연산을 수행할 수 있다. ⇨ $L(s) \le L(o)$ ⇒ Read
- Integrity *-property : 주체의 무결성 등급이 객체의

무결성 등급을 지배한다면 주체는 객체에 쓰기 연산을 수행할 수 있다. ⇨ L(s)≥L(o) ⇒ Write

▨ 역할기반 접근제어 모델

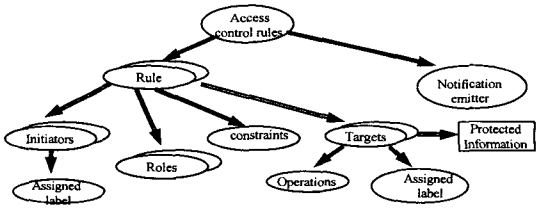
역할기반 접근제어정책의 주요 동기는 상업적인 측면의 보안정책을 강화시키기 위한 것과 임의적 접근제어정책과 강제적 접근제어정책으로부터 융통성과 세부적인 접근제어를 강화시키는데 있다. 많은 기업이 사용자에게 정보의 소유권을 부여하지 않고 회사나 대리점에 정보의 변경이나 삭제, 첨가 등 연산의 소유권을 부여하고 있다 이러한 강제적 접근제어 정책은 다단계 보안정책을 구현하는데 미흡하다. 이에 반해 역할기반 접근제어 정책은 상업적인 환경을 지원하는 다양한 보안 정책을 강화시킬 수 있다. 단, 역할기반 접근제어 정책의 구성요소들은 관리자에 의해 조정된다.

접근제어 정책은 역할과 허가사항, 사용자와 역할, 그리고 역할과 역할의 관계와 같은 역할기반 접근제어 정책 구성요소를 포함하는데 이들 구성요소는 시스템관리자에 의해 직접적으로 구성되거나 위임을 통해 간접적으로 구성된다[San96a].

3. 접근제어 모델의 상호연동

컴퓨터를 사용하는 사용자의 수가 급증하고 상호 독립적으로 운영되는 통신망들이 상호연동됨에 따라 전체적인 통신망의 규모가 점점 커지고 복잡해지고 있다. 또한 통신망을 이용하는 사용자들의 요구사항이 다양해져 이를 효율적으로 관리해 줄 수 있는 망관리 시스템이 통신망 운용에 필수적인 요소가 되었다. 그러므로 정보 통신망의 관리 정보를 이용하는 사용자의 환경이 동적으로 변화하는 현대의 네트워크 환경에서는 접근제어 정책을 어느 하나의 정책에 근거한 일괄적 정의로는 부적절하다. 따라서 실질적인 접근제어 시스템에 적용이 가능하도록 관련된 몇가지 정책들간의 연관성을 연구할 필요가 있다.

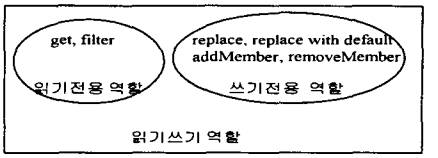
ITU-T X.741 권고안에는 정의된 접근제어를 위한 관리 객체 클래스 구조를 자율적 접근제어 정책과 강제적 접근제어 정책으로 나누어 정의하고 있다. 그림 2는 강제적 접근제어와 역할기반 접근제어를 상호연동한 관리객체 상호 관계를 나타내고 있다.



(그림 2) 관리 객체 상호관계(상호연동한 접근제어)

3.1 역할 영역

관리정보 모델에는 관리연산을 크게 전반적인 관리객체에 적용되는 연산과 속성값에 적용되는 연산으로 구분하고 있다[Slo94]. 전반적인 관리객체에 적용되는 연산에는 관리객체의 인스턴스를 생성하고 삭제하는 create, delete 연산과 개별적인 관리객체의 요구조건을 정의하는 action 연산이 있다. 그리고 속성값에 적용되는 연산에는 속성값을 읽는 get 연산, 속성값을 쓰는 replace 연산, 그리고 관리객체 정의시 명기되어있는 값으로 재정의하여 쓰는 replace with default 연산 등이 있다. 또한 특별한 속성 타입을 정의하기 위한 것으로 동일한 데이터 타입의 멤버들의 비순서 집합을 추가, 삭제하는 addMember와 removeMember 등이 있다. 본 논문에서는 실질적으로 관리정보베이스의 속성값을 수정하고 읽는 관리연산들에 대해서 그림 3과 같이 읽기전용역할, 쓰기전용역할 그리고 이들 두 연산을 포함하는 읽기쓰기 역할로 세분하였다.



(그림 3) 역할 영역

3.2 제약조건 및 정형적 기술

본 절에서는 인가등급을 갖는 관리자가 무결성등급을 갖는 관리객체를 수행하기 위한 역할 배정규칙과 제약조건[최98]을 기반으로 하여 'rule' 관리객체 클래스를 기술하였다. 현재 권고안에는 동작과정을 자연어로 기술하고 있어 동작절차가 명확치 않아 관리객체 설계자나 프로그래머가 이해하는데 어려움이 있다. 그러므로 본 절에서는 'rule'관리객체 클래스의 구조를 사건, 제약조건, 선결조건, 그리고 동작절차로 구분지어 동적특성을 부여하였으며 세부적인 과정은 관리객체 동적특성 기술언어[최99]를 사용하여 체계적이고 정형적으로 기술하였다.

세부적인 동작절차를 기술하기 위한 표기법은 다음과 같다.

$\mathbf{S}$: 주체의 집합 $S \in \mathbf{S}$
$\mathbf{R}$: 역할의 집합, $R \in \mathbf{R}$
R_r : 읽기전용 역할
R_w : 쓰기전용 역할
R_{rw} : 읽기쓰기 역할
$\lambda(S)$: 주체의 무결성 보안등급
RoleAssign(S , R) : 주체 S의 역할 R에 대한 배정함수
w-level(R) : 쓰기전용 역할 중에서 최대의 보안등급
r-level(R) : 읽기전용 역할 중에서 최소의 보안등급

[제약조건 1] $\forall S \in \mathbf{S}, \forall R_r \in \mathbf{R}$
RoleAssign(S, R_r) ⇒ $\lambda(S) \le$ r-level(R_r)
읽기전용 역할(R_r)이 배정되기 위해서는 주체의 인가등급이 해당 역할의 최소 보안등급에 해당하는 r-level(R_r)에 지배되어야 한다.

[제약조건 2] $\forall S \in \mathbf{S}, \forall R_w \in \mathbf{R}$
RoleAssign(S, R_w) ⇒ $\lambda(S) \ge$ w-level(R_w)
쓰기전용 역할(R_w)이 배정되기 위해서는 주체의 인가등급이 해당 역할의 최대 보안등급에 해당하는 w-level(R_w)을 지배하여야 한다.

[제약조건 3] $\forall S \in \mathbf{S}, \forall R_{rw} \in \mathbf{R}$
RoleAssign(S, R_{rw}) ⇒ r-level(R_r) ≥ w-level(R_w) AND
$\lambda(S) \le$ r-level(R_r) AND $\lambda(S) \ge$ w-level(R_w)

다음으로 읽기쓰기 역할(R_{rw})을 고려하자. 이 경우에는 읽기전용 역할의 r-level(R_r)이 쓰기전용역할의 w-level(R_w)을 지배하고 주체의 등급이 r-level(R_r)보다 적거나 같고 w-level(R_w)보다는 크거나 같은 경우에만 읽기쓰기 역할에 배정이 가능하다.

rule 관리객체는 관리자가 특정 관리객체에 접근하고자 할 때 규칙에 근거하여 접근여부를 결정하는 기능을 수행한다. 본 절에서는 관리객체의 동적 특성을 기술하기 위한 프로그래밍언어형태의 동적특성 기술언어를 이용하여 'rule' 접근제어 관리객체 클래스의 접근제어 결정함수와 집행함수에 대한 수행절차를 체계적이고 정형적으로 기술하였다.

rule MANAGED OBJECT CLASS
DERIVED FROM accessControl;
CHARACTERIZED BY rulePackage **PACKAGE**
BEHAVIOUR ruleBehaviour **BEHAVIOUR**

```
DEFINED AS
EVENT : AccessControlEnforcementEvent
        accessControlObject : accessControlObjectName;
PRECOND:
   administrativeState == unlocked AND
   operationalState == enabled AND
   availabilityStatus != Offduty;
PROCEDURE:
  emit AccessControlDecisionEvent notification;
  if (enforcementAction == allow) then
    "access is permitted";
    validAccessAttempts = validAccessAttempts + 1;
    "send to a security audit trail log";
    emit usageReport notification;
   if (enforcementAction == deny with response) then
    "access is denied";
     invalidAccessAttempts = invalidAccessAttempts + 1;
     "send to a security audit trail log";
         emit usageReport notification;
     endif;
  endif;

EVENT : AccessControlDecisionEvent
        accessControlObject : accessControlObjectName;
PRECOND:
   administrativeState == unlocked AND
   operationalState == enabled AND
   availabilityStatus != Offduty;
PROCEDURE:
switch(Role)
{
case   readonlyRole : if r-level(Rr) DOMINATES
       initiator-level then
         enforcementAction = allow
       else enforcementAction = deny with response ;
       endif;
case   writeonlyRole : if initiator-level DOMINATES
       w-level(Rw) then
         enforcementAction = allow
       else enforcementAction = deny with response ;
       endif;
case   readwriteRole : if initiator-level(Rr) DOMINATES
       target-level(Rw) then
         if (r-level(Rr) >= w-level(Rw) ) AND
            (initiator-level <= r-level(Rr) ) AND
             (initiator-level >= w-level(Rw) )
           then
             enforcementAction = allow
           else enforcementAction = deny with response ;
      endif;
   endif;
   }
```

(그림 4) 동적특성 기술언어를 이용한 rule 관리 객체 클래스의 동작 특성 기술

그림4 에서 'rule' 관리객체 클래스는 'accessControlEnforcementEvent' 사건이 발생하면 먼저 'PRECOND' 상태조건을 점검한 후 해당되는 동작절차를 수행한다. 이 절차를 거친 후에 'accessControlDecisionEvent' 통지를 발생시켜 해당 관리자가 접근하고자 하는 역할을 수행할 수 있는지 여부를 점검한다. 만약 'enforcementAction' 속성값이 'allow'값을 갖으면 접근을 허용하고 보안 감사를 위해 'log' 관리객체에 'usageReport'통지를 전송한다. 그렇지 않고 'enforcementAction' 속성값이 'deny with response'값을 갖으면 접근은 불허되고 이 또한 보안 감사를 위해 'log' 관리객체에 'usageReport'통지를 전송한다.

4. 결 론

컴퓨터와 통신기술의 급속한 발전은 과거의 독립적으로 존재하던 컴퓨터 시스템들을 망을 통하여 연결함으로써 규모가 커지게 되어 이를 관리하는 일이 더욱 복잡하게 되었다. 그러므로 통신망 관리시스템은 이질적 통신기술과 컴퓨터 네트워크로 구성된 통신망의 통합적인 관리기능의 수행을 위하여 관리대상 통신망 구성요소들의 특성 중 통신망 관리에 필요한 정적, 동적 정보만을 추출, 추상화한 관리객체로 모델링한다. 망관리시스템의 여러 가지 구성요소들 중 가장 핵심적인 요소중의 하나가 관리정보베이스이다. 관리정보베이스에 저장된 관리객체들은 망관리에 필수적이며 중요한 모든 정보를 유지하고 있기 때문에 안전하게 유지되어야 한다.

본 논문에서는 권고안에 정의된 강제적 접근제어 모델과 역할기반 접근제어 모델을 상호연동한 모델의 관리객체 상호관계 구조를 정의하였다. 또한 관리속성값을 제어하는 관리연산을 연관된 유형별로 묶어 역할로 정의하였으며 인가등급을 갖는 관리자와 무결성등급을 갖는 관리객체 사이에 역할을 배정하므로서 관리정보의 무결성과 실생활에 적용될 수 있는 접근제어 모델을 제시하였다. 그리고 역할배정규칙과 제약조건을 기반으로 하여 'rule' 관리객체 클래스의 접근제어 결정함수와 접근제어 집행함수의 동작과정을 동적특성 기술언어를 사용하여 체계적이고 정형적으로 기술하였다.

[참고문헌]

[Cas94] Silvana Castano, DATABASE SECURITY, ADDISON-WESLEY, 1994

[For94] Warwick Ford, Computer Communications Security, Prentice Hall, 1994

[Osb97] Sylvia Osborn, "Mandatory Access Control and Role-Based Access Control Revisited", Second ACM Workshop on RBAC, 11. 1997, pp. 31-40.

[San96a] Ravi S. Sandhu, "Role Hierarchies and Constraints for Lattice-Based Access Controls", Proc. Forth European Symposium on Research in COMPUTER SECURITY, 9. 1996. pp. 1-19.

[San96b] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models", COMPUTER SOCIETY, IEEE, FEB. 1996, pp.38-47.

[Slo94] Morris Sloman, Network and Distributed System Management, Addison-Wesley Publishing Company, 1994

[X722] ITU-T X.722|ISO DIS 10165-4: "Information Processing Systems - Open Systems Interconnection - Management Information Services - Structure of Management Information Part 4: Guidelines for the Description of Managed Objects", Geneva

[X741] ITU-T X.741|ISO DIS 10164-9: "Information Technology - Open Systems Interconnection - System Management - Objects and Attributes for Access Control "

[최98]최은복, 이형효, 노봉남, "Biba 모델과 역할기반 접근제어 모델의 상호연동", 한국통신정보보호학회 종합학술발표회 논문집, 제8권제1호, 1998

[최99]최은복, 이형효, 노봉남, "망관리객체의 시간지원 능동특성에 대한 정형적 모델링", 정보처리학회 논문지, 제6권 제8호, 1999(게재예정)