확장된 역할기반 접근제어 모델에서 GRBAC을 이용한 프라이버시 제어

정회원 박 종 화*, 김 지 홍**, 김 동 규***

Privacy Control Using GRBAC In An Extended Role-Based Access Control Model

Chong hwa Park*, Ji hong Kim**, Dong kyoo Kim*** ***Regular Members***

요 약

최근 프라이버시 적용이 IT분야의 가장 중요한 문제의 하나로 대두되고 있다. 프라이버시 보호는 조직의 데이터 처리 시스템에 프라이버시 정책을 적용함으로써 달성될 수 있다. 전통적인 보안 모델은 목적 결합(purpose binding)과 같은 프라이버시의 기본적인 요구사항을 적용하기에 부적절하다. 본 논문은 기존의 보안모델에 통합하여 쉽게 적용할 수 있는 프라이버시 제어 모델을 제안한다. 이를 위하여 기존의 보안모델로 RBAC과 도메인-타입을 적용하여 문맥기반 접근제어를 제공하는 하나의 확장된 역할기반 접근제어 모델이 사용되었고, 프라이버시 제어 모델에서는 프라이버시 선호로 표현되는 목적 결합을 적용하기위해 GRBAC이 사용되었다. 또 이 모델의 응용을 위하여 작은 병원 모델이 고려되었다

Key Words : Security, Access Control, Privacy, Generalized Role-Based Access Control

ABSTRACT

Privacy enforcement has been one of the most important problems in IT area. Privacy protection can be achieved by enforcing privacy policies within an organization's online and offline data processing systems. Traditional security models are more or less inappropriate for enforcing basic privacy requirements, such as purpose binding. This paper proposes a new approach in which a privacy control model is derived from integration of an existing security model. To this, we use an extended role-based access control model for existing security mechanism, in which this model provides context-based access control by combining RBAC and domain-type enforcement. For implementation of privacy control model we use GRBAC(Generalized Role-Based Access Control), which is expressive enough to deal with privacy preference. And small hospital model is considered for application of this model.

Ⅰ. 서 론

오늘날 인터넷의 발달과 함께 건강관리 환경에서 내부적으로 컴퓨터 시스템들 사이에, 그리고 지역적으로 분산된 기관들 사이에 정보 교환에 대한 욕구가 크게 증가하고 있다. 또한 인구의 유동성 증가와 함께 환자의 데이터는 지역적으로 분산된 여러 의료기관에 위치하게 되며, 이들 데이터를 지역적인 범위에서 또는 범국가적인 범위로 관리하여 접근이 가능하도록 할 필요가 있다. 이와 같은 분산된 의료 정

* 세명대학교 소프트웨어학과(chpark@semyung.ac.kr), ** 세명대학교 정보보호학과, *** 아주대학교 컴퓨터공학부
논문번호 : KICS2004-08-169, 접수일자 : 2003년 8월 26일

보 시스템에의 접근은 무결성, 비밀성, 부인방지 등을 제공할 뿐 만 아니라, 환자 개인의 프라이버시 보호도 제공되어야 한다. 그러나 인터넷 기술은 정보 보호 보다는 정보 공유를 목적으로 최적화하기 위해 설계되어 있어, 적정 수준의 보안을 제공하지 못하고 있다. 이러한 인터넷 보안을 만족스러운 수준으로 유지하기 위한 최근의 노력들이 활발히 진행되고 있으며, 이들 대부분은 공개키 암호학(public-key cryptography)에 기반을 두고 있다. 여기서, 공개키 기반구조(PKI : Public-Key Infrastructure)는 사용자의 신원확인 등의 인증기능을 제공하기 위해 사용되고, 권한관리 기반구조(PMI : Privilege Management Infrastructure)는 사용자의 임무, 지위, 역할 등의 속성정보를 제공하기 위해 사용된다. 이와 같은 PKI, PMI 환경에서 건강관리 인트라넷 응용에 적정 수준의 보안과 환자의 프라이버시 보호를 제공하기 위해서는 PKI와 PMI 환경에서 공존할 수 있는 프라이버시 보호를 갖는 적절한 보안정책이 수반되어야 한다.

프라이버시 보호는 조직의 보안정책에 프라이버시 정책을 적용함으로써 이루어질 수 있다. 시스템에 적용된 프라이버시 정책은 데이터의 비밀성과 무결성을 제공한다는 측면에서 보안정책과 중복되는 면이 없지 않다. 그러나 프라이버시 보호는 보안정책의 접근제어를 확장하는 것에 의하여 조직에 보안정책과 함께 제공되어야 함이 참고문헌[1]에서 제안되고 있다.

전통적인 접근제어 모델에는 강제적 접근제어(MAC: Mandatory Access Control)[2]나 임의적 접근제어(DAC: Discretionary Access Control)[3] 등과 같은 모델들이 있으나, 이 들은 프라이버시 정책을 적용하기 위해 설계되지 않았다. 참고문헌[4]에 발표된 잘 알려진 보안 모델에 대한 프라이버시 평가 요약에서 전통적인 보안 모델들은 목적 결합(purpose binding)(하나의 목적으로 수집된 데이터는 고객의 동의 없이 다른 목적으로 사용되어서는 안 된다.)이나 필요의 원칙(principle of necessity)(데이터의 분배와 처리는 적절한 일을 위해 필요할 때 만 허용되어야 한다)과 같은 기본적인 프라이버시 보호의 요구사항을 적용하는데 다소 부적절함을 언급하고 있다.

역할기반 접근제어(RBAC: Role-Based Access Control)[5]는 최근 임의적 접근제어와 강제적 접근제어의 유망한 대안으로 주목을 받고 있다. RBAC에서 역할(role)의 특성은 프라이버시 정책의 중요한 요소인 목적(purpose)과 관계를 갖고 있다. RBAC에서 역할은 그 역할에 할당된 사용자에게 책임과 권한이 부여된 조직에서의 일의 기능으로 정의된다. 이 때 역할에 부여된 책임은 역할의 목적을 함축적으로 포함한다. 또한, RBAC은 프라이버시 보호에 중요한 문맥기반 접근제어(context-based access control)를 적용하는데 적당한 환경을 제공한다.

환자의 프라이버시를 보호해야 하는 건강관리 응용시스템의 보안정책은 HIPAA 보안 표준[6]에 따를 것을 권고 받게 되는데, 이 표준에서 건강관리 응용시스템은 사용자기반(user-based) 접근제어, 역할기반(role-based) 접근제어, 그리고 문맥기반(context-based) 접근제어의 특징을 가져야 함을 규정하고 있다. 문맥기반 접근제어는 데이터에 접근하는 사용자와 접근하는 데이터의 유형을 고려할 뿐만 아니라, 시도된 처리의 문맥까지도 고려한다. 프라이버시를 인식할 수 있는 환경에서 문맥은 역할의 책임, 특정 고객에 의해 동의 된 데이터 사용 정책, 그리고 역할의 데이터 접근을 위한 주체 등이 될 수 있다.
문맥기반 접근제어를 제공하는 모델로 DAFMAT (Dynamic Authorization Framework for Multiple Authorization Types)[7] 는 RBAC과 DTE가 조화된 건강관리 응용 시스템을 제안하였다. DAFMAT의 가장 중요한 특성은 문맥기반 권한부여, 긴급 권한부여와 같은 다중 유형의 권한부여를 지원하는 것이며, 또 권한부여 요청을 체계화하여 요청의 정당성을 결정하기 위한 논리 유도 권한부여 엔진을 사용하는 것이다. 그러나 문맥기반 접근제어의 기반을 제공함에도 불구하고 DAFMAT의 한계는 프라이버시 보호 정책을 적용함에 있어 목적결합(purpose binding)과 필요의 원칙(principle of necessity) 등을 모델링 하지 못하고 있다는 것이다.

본 논문의 목적은 프라이버시 보호를 제공하기 위해서, 참고문헌[1]에서 제안한 것과 같이, 기존의 보안모델에 프라이버시 제어를 추가하여 새로운 모델로 확장하는 것이다. 이를 위하여 기존의 보안모델로 확장된 역할기반 접근제어 모델인 DAFMAT가 사용되었고, 프라이버시 제어를 위하여 GRBAC(Generalized Role-Based Access Control)[8]모델을 사용하였다.

본 논문의 구성은 2장에서 관련 기술이 언급되고, 3장에서 본 논문에서 제안된 모델이 기술되며, 4장에서 제안된 모델의 응용이 다루어진다. 그리고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 기술

2.1 역할기반 접근제어(Role-Based Access Control : RBAC)

RBAC는 보안 분야에서 전통적인 임의적 접근제어와 강제적 접근제어의 유망한 대체로서 주목을 받아왔다. 1996년 이래로 ACM RBAC/SACMAT 일련의 워크숍은 이 연구 경향이 주목받고 있음을 보이는 예이다. 최근 RBAC는 NIST 표준으로 제안되었다[9].

RBAC에서 사용자는 객체에 접근이 허용된 허가를 가진 역할에 할당되었을 경우, 해당 객체에 접근할 수 있다. RBAC의 중요한 이정표는 RBAC96 모델이다[10]. RBAC96은 여러 사용자와 여러 자원 사이의 복잡한 시스템에서 권한부여를 관리하는 RBAC 모델 family를 정의하였다. RBAC의 역할의 개념은 조직의 기능적 역할과 유사하다. 따라서 RBAC은 조직의 보안정책을 모델링하는데 직관적인 방법을 제공한다. 후에 RBAC은 정책 중립적인 모델임이 입증됐는데 이는 RBAC이 어느 특정한 보안 정책을 포함하는 대신 그 정책을 표현하는 방법이기도 하다는 것이다. 또한 RBAC은 전통적인 강제적이고 임의적인 접근제어 정책을 포함하는 구성을 가질 수 있다[11]. 그리고 RBAC은 여러 잘 알려진 보안 원칙인 정보은폐(information hiding), 특권 최소화(least privilege), 의무 분리(separation of duties), 데이터 추상화(data abstraction) 등을 지원한다. RBAC의 또 다른 장점은 역할이 사용자의 교체나 일의 재 할당에 비해 지속적이므로 권한부여의 관리가 전통적인 보안 모델에 비해 쉽다는 것이다. RBAC에서 조직 내의 역할에 허가를 할당함은 복잡성, 비용, 오류의 가능성을 줄이는데 기여하기도 한다. 또한 RBAC은 웹 상에서 보안 정책을 적용하기 위해 사용되기도 했고[12], 다중 도메인 환경에서의 사용 가능성이 확인되기도 했다[13].

2.2 도메인-유형의 적용(Domain-Type Enforcement : DTE)

DTE[14]는 하위 수준의 강제적 접근제어(low-level mandatory access control) 메커니즘으로 주체에 도메인 라벨 그리고 객체에 유형 라벨을 사용하는 것에 의해 객체에 대한 주체의 접근을 제한한다. DTE와 RBAC 사이에 다른 점은 RBAC은 사용자와 역할이 관련되어 있어, 역할이 어떻게 사용자에게 가능한 연산을 제한하는지를 설명한다. 반면에 DTE은 주체를 도메인에 연관지어, 어떻게 도메인이 주체에 가용한 연산을 제한하는지를 설명한다. 이 때 RBAC은 DTE와 결합하여 HIPAA 보안 표준이 제안한 프라이버시 적용 메커니즘을 제공할 수 있는 문맥기반 접근제어의 특징을 갖는 모델로 확장할 수 있다. 그 예를 DAFMAT에서 볼 수 있다.

2.3 DAFMAT(Dynamic Authorization Framework for Multiple Authorization Types)

DAFMAT[7]는 RBAC과 DTE를 결합함으로써 건강관리 응용 시스템에서 문맥기반 권한부여, 긴급 권한부여와 같은 다중 유형의 권한부여를 지원한다. 또 DAFMAT는 권한부여 요청을 공식화하기 위해 그리고 요청의 타당성을 결정하기 위해 논리유도 권한부여 엔진(logical-driven authorization engine)을 사용한다. DAFMAT의 가장 중요한 특성은 문맥기반 권한부여, 긴급 권한부여와 같은 다중 유형의 권한부여를 지원하는 것이다. 그리고 이는 문맥기반 권한부여를 사용하는 프라이버시 정책을 적용하기위한 기본 구조를 제공한다. 그림1는 DAFMAT에서 권한부여 개체들 사이의 관계를 도식적으로 표현하고 있다.

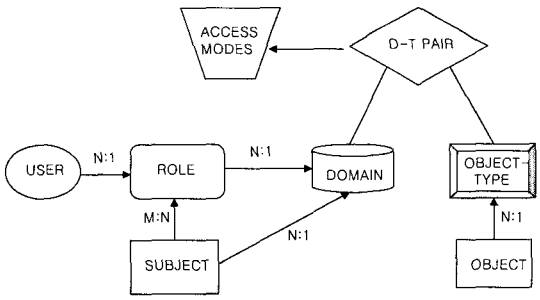


그림 1. DAFMAT에서 권한부여 개체간의 관계

그림 1에서와 같이 프라이버시 보호를 적용하는데 있어 DAFMAT의 한계는 목적결합과 필요의 원칙 등을 모델링하지 못한다는 것이다. 목적결합과 필요의 원칙 등은 프라이버시 선호(privacy preference)로 표현될 수 있어, 결과적으로 정보제공자의 선택에 의한 정보제공자의 정보를 공개하는 것 등을 DAFMAT은 수용하지 못하는 것이다. 자신의 정보를 공개하기 위한 정보제공자의 선택 즉 프라이버시 선호는 다음의 4가지 관점을 포함한다.

- 누구에게 정보를 공개할 것인가.
- 무엇을 공개할 것인가.

- 언제 공개할 것인가.
- 어떻게 공개할 것인가.

정보제공자의 프라이버시 선호를 표현하기 위해 본 논문에서는 프라이버시 제어 모델에서 GRBAC모델을 사용하였고, 이를 위하여 기존의 보안모델인 DAFMAT를 확장하였다.

2.4 GRBAC(Generalized Role-Based Access Control)

GRBAC[8]은 풍부한 접근제어 정책을 생성하고 유지할 수 있는 새로운 패러다임이다. 이는 접근제어 결정에 주체역할(subject roles), 객체역할(object roles), 그리고 환경역할(environment roles)을 포함함으로써 전통적인 RBAC의 능력을 확장한다. 이 모델의 4개 기본 구성요소는 다음과 같다.

- 주체역할(subject role): 주체들을 분류하는 집합체 배치 메커니즘;
- 객체역할(object role): 객체들을 분류하는 집합체 배치 메커니즘;
- 환경역할(environment role): 환경에 대한 보안 관련 정보를 획득하기 위해 사용된다.
- 처리(transaction): 처리는 <S, O, E, op>의 튜플 형태이며, 여기서 S는 하나의 주체역할을, O는 하나의 객체역할을, E는 하나의 환경역할을, 그리고 op는 연산(operation)을 규정한다. 의미론적으로, 처리는 하나의 연산으로 주체역할 S를 행하는 하나의 주체가 E에 의해 규정된 환경조건 하에서 객체역할 O안의 하나의 객체에 대해 연산 op를 수행함을 의미한다.

하나의 역할 계층(role hierarchy)은 방향성 비 순환 그래프로, 여기서 모든 노드는 하나의 역할을 그리고 모든 간선(edge)은 두 노드들 사이의 부모-자식 관계를 나타낸다. 만약 노드 Ri에서 시작하여 노드 Rj로 끝나는 어떤 진로(path)가 존재한다면, 역할Ri는 역할 Rj의 하나의 상위-역할(super-role)이다. 어떤 역할 R에 대한 엔트리 집합(entry set) ESr = {R} ∪ {R': R'는 R의 하나의 상위역할}이다.
하나의 GRBAC 정책 데이터베이스는 정책 규칙들(policy rules)의 목록으로 구성되며, 정책 규칙은 처리(transaction)로서 정의된다. 즉, R = <S, O, E, op>, 여기서 S ∈ SRset, O ∈ ORset, E ∈ ERset, op ∈ OPset이다. 하나의 규칙 R' = <S', O', E', op>은 만약 S' ∈ ES_S, O' ∈ES_O, E'∈ES_E 이면 처리 T=<S, O, E, op>의 조화 규칙(matching rule)이 된다.

여기서, 개인 정보 데이터베이스에 대해 모든 역할들과 연산들은 미리 정의된다고 가정한다.

- SRset = {S_1, S_2,..., S_m}은 모든 주체역할을 포함한다.
- SRHset = {..., <S_i, S_j>,...}은 부모-자식 관계의 모든 쌍을 포함하며, 모든 주체역할의 계층관계를 정의한다. 비슷하게 ORset, ORHset, ERset, ERHset 그리고 OPset이 존재한다. 이 모든 집합들은 정책 규칙이 정의될 수 있는 영역을 구성하며, 모든 GRBAC 시스템들은 이 영역에서 정의되어진다.

Ⅲ. 제안된 모델

본 논문에서 제안한 모델은 프라이버시 제어를 제공하는 확장된 역할기반 접근제어 모델로서, RBAC과 DTE를 결합하여 문맥기반 권한부여와 긴급 권한부여와 같은 다중 권한부여를 지원하는 DAFMAT의 하부구조에 프라이버시 선호를 제공하기위해 GRBAC을 이용한 프라이버시 제어 모델을 결합하였다.

3.1 제안된 모델의 구성 요소 및 접근 제어 의사결정 절차와 알고리즘

제안된 모델은 크게 두 부분으로 구성된다. 하나는 프라이버시 제어를 적용하기위한 보안 모델이고, 또 하나는 그 보안 모델에 적용되는 프라이버시 제어 모델이다. 사용자, 역할, 주체, 도메인, 객체, 객체유형, 프라이버시 제어, 프라이버시 정책 규칙 DB등으로 구성된다. 그림 2는 제안된 모델의 구조를 보이고 있다.

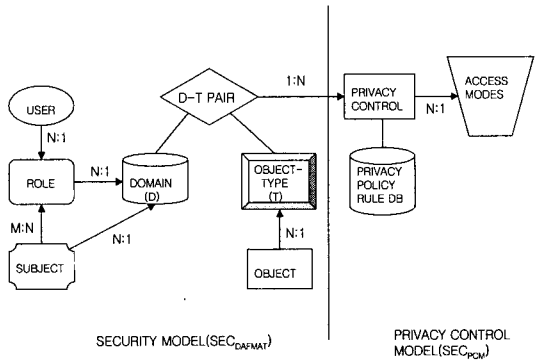


그림 2. 제안된 모델

제안된 모델의 접근 요청은 보안 모델과 프라이버시 제어 모델 양쪽에서 모두 허가 될 때에만 허용된다. 제안된 모델의 접근요청에 대한 권한부여 의사결정 절차 또는 알고리즘은 다음과 같다.

(Algorithm)

```
BEGIN
  Receive an access request
  /* Validate this access in SEC_DAFMAT */
  FIRST VALIDATION:
    Formulate the authorization request
predicate using some session-related
functions.
    (This request is designated as one of
the three types of authorization (Normal,
          Emergency and Context-based).)
    Using the validation conditions for each
authorization type, determine whether the
        current authorization request is
valid.
    IF not valid
      Deny Access
      GOTO END
    ELSE
      GOTO SECOND VALIDATION
  /* Validate this access in SEC_PCM */
  SECOND VALIDATION:
    Transform the access request to a
transaction T = <S, O, E, op>
    Search all matching rules R' = <S',
O', E', op> for T, where R'∈SEC_PCM
    IF no matching rule is found
      Deny Access
    ELSE FOR each O'∈ES_O, there is at
least one R'
      Allow Access
END
```

3.2 보안 모델(SECURITY MODEL)

3.2.1 개체들 간의 관계

제안된 모델의 보안 모델(그림 2)에서 개체들 간의 관계는 출발개체와 목적개체 사이에 다대다(M:N), 다대일(N:1), 일대다(1:N), 또는 일대일(1:1) 관계의 사상을 화살표로 나타낸다.

－User_Role(user, role) : 다대다

한 사용자에 여러 역할들이 부여될 수 있고, 또 하나의 역할에 여러 사용자가 할당될 수 있다.

－Role_Domain(role, domain) : 다대일

하나의 도메인은 조직에서의 한 기능적 분야를 나타낸다. 따라서 여러 역할이 한 도메인에 연관되어지며, 하나의 역할은 항상 특정 도메인에 속한다.

－Subject_Role(subject, role) : 다대다

주체는 사용자를 대신하여 특정한 일(task)을 수행한다. 따라서 하나의 주체가 여러 역할들에 의해 호출될 수 있다. 또 하나의 역할은 지정된 일을 수행하기 위해 여러 주체를 호출할 수 있다.

－Subject_Domain(subject, domain) : 다대일

각 주체는 하나의 특정 도메인과 연관되어지며, 하나의 도메인에 여러 주체들이 관련된다.

－Object_ObjectType(object, object-type) : 다대일

하나의 객체유형(object type)은 관련된 정보를 가지는 객체들의 모임이다. 따라서 각 객체는 특정한 객체유형에 사상되며, 하나의 객체유형은 여러 객체를 포함한다.

－DTE_Entry(domain, object-type, access-modes) : 다대다

도메인-유형이 도메인-유형 접근 행렬 표(Domain-Type Access Matrix : DTE table)에 나타낸다. DTE table의 각 항목에 허용 할 수 있는 접근모드가 표시된다.

3.2.2 개체 간 관계에 대한 제한

개체들 간의 관계는 제한에 의해 한정되어질 수 있다. 제한은 RBAC에서 가장 중요한 특징 중의 하나이며, 의무분리(separation of duties)와 같은 보안 요구를 표현하는데 사용된다. 다음의 제한에서 ∀은 "for any"를, ∃는 "there exists"를, &는 "logical and"를, 그리고 ⇒는 "implies"를 나타낸다.

제한 : 주체를 불러일으키는 모든 역할들은 주체와 연관된 같은 유일한 도메인에 할당되어져야 한다.

∀(subject, domain, role), Subject_Domain(subject, domain) & Role_Domain(role, domain) ⇒ Subject_Role(subject, role)

3.2.3 여러 권한부여 유형에 대한 인증 조건

보안모델은 3가지 유형의 권한부여를 지원한다. 그들에 대한 인증조건은 다음과 같다.

－정규 권한부여 요청에 대한 인증 조건
Subject_Role(subject, role) →
Normal_Auth_Req(user, role, subject)
－긴급 권한부여 요청에 대한 인증 조건
ER_Role_Map(role, mapped_role) &

Subject_Role(subject, mapped_role) →
Emer_Auth_Req(user, role, subject)

여기서, ER_Role_Map 함수는 긴급 상황에서 지정된 역할을 의미하며, 모델의 긴급 역할에서 정규 역할로의 사상은 긴급시를 위하여 안전한 장소에 보관된다.

- 문맥기반 권한부여 요청에 대한 인증 조건
  IF cv = 'CTXT_VAR1'
  THEN
  Subject_Role(subject, role) & <Context Predicate relevant for CTXT_VAR1> →
  Context_Auth_Req(user, role, subject, cv, cv_value)

문맥기반 권한부여에 대한 인증조건은 문맥변수(context variable: cv)에 의존하며, 각각의 문맥변수에 따라 다른 인증규칙이 적용된다.

3.3 프라이버시 제어 모델(PRIVACY CONTROL MODEL)

프라이버시 제어 모델은 프라이버시 제어 시스템을 위한 체제이며 기존의 보안 메커니즘과 함께 구현될 수 있다. 이를 위하여 우리는 간단하면서도 표현력이 풍부한 GRBAC을 사용한다.

프라이버시 관점에서 정보 제공자는 자신의 프라이버시 선호를 결정할 필요가 있고, 프라이버시 선호는 다음을 포함한다.

- 누가 접근할 수 있는가(GRBAC의 주체역할(Subject Role), S)
- 언제 접근할 수 있는가(GRBAC의 환경역할(Environment Role), E)
- 어떤 정보에 접근을 허용할 것인가(GRBAC의 객체역할(Object Role), O)
- 어떻게 접근할 것인가(GRBAC의 연산(Operation), op)

여기서 프라이버시 선호의 형태가 하나의 GRBAC 정책규칙(policy rule) 즉 처리 <S, O, E, op>와 동일함을 알 수 있다. 따라서 정보 제공자의 프라이버시 선호는 GRBAC의 정책 규칙(policy rule)으로 표현될 수 있다. 결국 GRBAC의 표현력은 조직의 프라이버시 정책을 일련의 GRBAC 정책 규칙들로 바꾸어 놓게 한다. 그림 2의 프라이버시 정책 규칙(privacy policy rule) DB에는 GRBAC 정책규칙으로 표현된 정보 제공자의 프라이버시 선호가 저장된다.

3.4 프라이버시 정책 규칙 적용

프라이버시 정책 규칙들을 적용하는데 세 가지 상태가 가능하다.

- 만약 정보 제공자가 규칙을 그림 2의 SEC_{PCM}에 규정하지 않았다면 즉 $SEC_{PCM} = \varnothing$ 이면 병원의 정보 제공자의 개인적인 정보에 접근이 가능하지 않다.
- 만약 SEC_{PCM} = {<모든 사용자 역할, 모든 객체, 모든 환경, read>}이면, 정보 제공자의 개인적인 정보에 접근은 오직 그림 2의 보안 모델 SEC_{DAFMAT}에 의존한다.
- 위의 두 극단적인 경우 외에서, 정보 제공자는 자신의 프라이버시를 보호하기 위해서 융통성 있게 규칙을 규정할 수 있다.

Ⅳ. 제안된 모델의 응용

제안된 모델을 설명하기 위해 간단한 응용을 제시한다. 이 응용은 4명의 사용자(John, Smith, Susan, Patricia), 병원의 각각 다른 부서에서 4개의 역할, 4개의 주체(subject) 그리고 4개의 도메인으로 구성된다. 사용자 John에게는 Administration 역할이 할당되고, 사용자 Smith에게는 Logistics 역할이, 사용자 Susan에게는 Head Nurse 역할이, 그리고 사용자 Patricia에게는 Personal Doctor 역할이 할당된다. 이 때 사용자, 역할, 주체, 그리고 도메인 간의 관계는 다음의 매핑 함수와 그림 3에서 표현된다.

4.1 응용에서 보안모델의 개체와 개체간의 관계

Users = {John, Smith, Susan, Patricia}
Roles = {A, L, HN, DP}
A: Administration, L: Logistics
HN: Head Nurse, PD: Personal Doctor
Domains = {AD, LD, PHD, MDD}
AD: Administration Domain,
LD: Logistics Domain
PHD: Patient Hospitalization Domain,
MDD: Medical Decision Domain
Subjects = {IDP, PSP, XRP, DGP}
IDP: Insurance Data Proc,
PSP: Patient Supply Proc

XRP: X-Ray Proc, DGP: Diagnoses Proc

User-Role Assignment={User_Role(John, A), User_Role(Smith, L), User_Role(Susan, HN), User_Role (Patricia, PD)}
Role-Domain Mapping={Role_Domain(A, AD), Role_Domain(A, LD), Role_Domain(L, LD), Role_Domain(HN, PHD), Role_Domain(HN, MDD), Role_Domain(PD, MDD), Role_Domain(PD, PHD)}
Subject-Domain Mapping = {Subject_Domain (IDP, AD), Subject_Domain (PSP, LD), Subject_Domain (XRP,PHD), Subject_Domain(DGP, MDD)}
Subject-Role Mapping = {Subject_Role(IDP, A), Subject_Role(PSP, L), Subject_Role (PSP, A), Subject_Role(XRP, HN), Subject_Role(XRP, PD), Subject_Role(DGP, PD), Subject_Role(DGP, HN)}

Domain-Type Access Matrix
(C: create, U: update, D: delete, V: view) :

표 1. 도메인-타입 접근 행렬

Domain	Object-Type / Access Modes			
	Patient Registration Type	Patient Supply Type	Patient Hospitalization Type	Patient Diagnoses Type
AD	C, U, D, V	V		
LD		C, U, V		
PHD			C, U, V	V
MDD			V	C, U, V

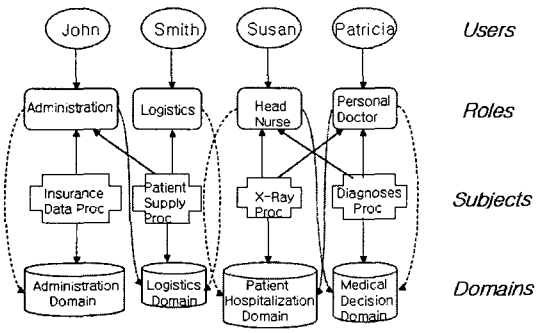


그림 3. 제안된 모델의 접근제어

4.2 응용에서 GRBAC을 이용한 프라이버시 제어

위의 병원 예에 대한 프라이버시 시스템 요소들은 다음과 같이 식별될 수 있다.

- 조직(Organization): Small Hospital
- 정보 제공자: Kim, Park
- 사용자 역할: Administration, Logistics, Head Nurse, Personal Doctor
- 데이터: Insurance Data, Patient Supply, X-ray, Diagnoses

위의 문제 설명으로부터 프라이버시 정책 규칙의 도메인은 다음과 같이 규정될 수 있다.

- SRset = {모든 사용자 역할, Administration(A), Logistics(L), Head Nurse(HN), Personal Doctor (PD)}
- SRHset = {<모든 사용자 역할, 어떤 사용자 역할>}
- ORset = {모든 객체, Insurance Data, Patient Supply, X-ray, Diagnoses}
- ORHset = {<모든 객체, 어떤 객체>}
- ERset = {모든 환경, 정규 권한부여 요청, 긴급 권한부여 요청, 문맥기반 권한부여 요청}
- ERHset = {<모든 환경, 어떤 환경>}
- OPset = {read}

정보 제공자는 위의 프라이버시 정책 규칙 도메인 상에서 그들의 프라이버시 정책 규칙을 정의할 수 있다. 즉, 정보 제공자는 자신의 프라이버시 선호로서 프라이버시 정책 규칙을 규정할 수 있다. 이 프라이버시 정책 규칙들은 그림 2의 SEC_{PCM}의 프라이버시 정책 규칙(privacy policy rule) DB에 저장되어진다.

Ⅲ.4의 프라이버시 정책 규칙 적용을 기반으로 정보 제공자인 Kim, Park이 다음과 같은 프라이버시 정책 규칙을 규정하였다고 가정한다.

$SEC_{PCM,Kim}$ = {R: R=<any-role, any-object, 긴급 권한부여 요청, read>}

$SEC_{PCM,Park}$ = {R: R=<HN, X-ray, 정규 권한부여 요청, read>}

4.3 응용에서 제안된 모델의 적용 예

앞에서 제안한 권한부여 절차를 통해 여러 데이터 사용자의 요청들을 시험하고, 그 요청들을 허가 할 것인지 또는 거부할 것인지를 분석한다.

요청 1 : 사용자 John이 정규 권한부여 요청으로 Insurance Data Procedure(IDP)를 호출하여, Kim의

Insurance Data를 View할 것을 요청한다.

Ⅲ.2.2에서의 개체 간 관계에 대한 제한에 의해 John의 역할인 Administration(A)이 Administration Domain과 연관되는지 Role-Domain Mapping을 통하여 확인하고, IDP가 Administration Domain에 속하는지를 Subject-Domain Mapping을 통하여 확인한 후, Subject-Role(IDP, A) 즉 A와 IDP의 연관성을 확인한다. 또 DTE 테이블을 통해 View할 수 있음을 확인한다. 그러나 프라이버시 제어 모델의 정보 제공자 Kim의 프라이버시 정책 규칙($SEC_{PCM,Kim}$)에서 정규 권한부여 요청 시에는 어떠한 역할도 자신의 객체에 접근(read)을 허용하지 않으므로 요청이 거절된다.

요청 2: Head Nurse(HN)의 역할을 갖는 Susan이 정규 권한부여 요청으로 X-Ray Procedure(XRP)를 호출하여 Park의 X-Ray 결과에 접근(view)을 요청한다.

Ⅲ.2.2의 개체 간 관계에 대한 제한에 의해 HN가 Patient Hospitalization Domain(PHD)과 연관되는지 Role-Domain Mapping을 통하여 확인하고, XRP가 PHD에 속하는지 Subject-Domain Mapping을 통하여 확인한다. 또 HN와 XRP의 연관성을 Subject-Role(XRP, HN)을 통하여 확인한 후, DTE 테이블을 통해 접근(view)할 수 있음을 확인한다. 또 프라이버시 제어 모델에서 정보 제공자 Park의 프라이버시 정책 규칙($SEC_{PCM,Park}$)에서 정규 권한부여 요청 시 Head Nurse 역할에 X-ray 결과의 접근(read)이 허용되므로 요청이 허가된다.

Ⅴ. 결 론

프라이버시 보호는 조직의 데이터 처리 시스템 안에서 프라이버시 정책을 적용함으로써 이루어 질 수 있다. 따라서 프라이버시 보호는 시스템 보안과 함께 고려되어야 하고, 데이터 관리 기술들과도 결합되어야한다. 본 논문에서 제안된 모델은 정보 제공자의 프라이버시 선호(privacy preference)를 적용하기 위하여 기존의 확장된 역할기반 접근제어 모델에 GRBAC을 이용한 프라이버시 제어 모델을 결합하였다. 이 모델은 조직의 관점에서 보안을 제공할 뿐 아니라, 고객(정보 제공자)의 관점에서 고객의 프라이버시를 보호한다. 특히 환자의 프라이버시를 보호해야하는 의료기관에서 더 잘 적용됨을 보였다. GRBAC을 이용한 프라이버시 제어 모델의 장점은 기존의 접근제어를 변형하지 않고 통합하여 사용할 수 있고, 쉽고 경제적으로 프라이버시 제어 시스템을 구현할수 있음에 있다.

본 논문에서 제안된 모델이 모든 프라이버시 문제를 해결하지는 못한다. 오직 수집된 고객의 데이터에 대한 프라이버시를 보호하는데 초점이 맞추어져 있다. 여러 다른 프라이버시 문제들, 예를 들면, 데이터 마인닝(data mining)에 의한 프라이버시 침입, 익명(anonymity)과 같은 문제들은 앞으로 연구할 과제들이다.

참 고 문 헌

[1] Calvin S. Powers, Paul Ashley, Matthias Schunter, "Privacy Promises, Access Control, and Privacy Management," Proc. of the 3rd International Symposium on Electronic Commerce, pp. 13-21, IEEE, 2002.

[2] Ravi S. Sandhu, "Lattice-Based Access Control Models," IEEE Computer, Vol. 26 Issue 11, pp. 9-19, Nov. 1993.

[3] R. Sandhu, P. Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine, Vol. 32 Issue 9, pp. 40-48, Sep. 1994.

[4] Simone Fischer-Hubner, "IT-Security and Privacy," Lecture Notes in Computer Science 1958 (LNCS 1958), Springer-Verlag, 2001.

[5] Ravi S. Sandhu, Edward J. Coyne, Hall L. Feinstein, Charles E. Youman,"Role-Based Access Control Models," *IEEE Computer*, Vol 29 Issue 2, pp. 38-47, Feb.1996.

[6] Security and Electronic Signature Standards; *Proposed Rule. Federal Register*, Vol 63, No. 155, August 12,1998.

[7] Ramaswamy Chandramouli, "A Framework for Multiple Authorization Types in a Healthcare Application System," *Proc. of the 17th Annual Computer Security Applications Conference (ACSAC 2001)*, pp. 137-148, IEEE, 2001.

[8] M. J. Moyer, M. Ahamad, "Generalized role-based access control," In Proceedings of

21st International Conference on Distributed Computing Systems, pp. 391-398, 2001.

[9] David F. Ferraiolo, Ravi Sandhu, Serban Gavrial, et al., "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and System Security*, Vol 4 No.3, pp. 224-274, August 2001.

[10] Ravi S. Sandhu, Edward J. Coyne, Hall L. Feinstein, Charles E. Youman,"Role-Based Access Control Models," *IEEE Computer*, Vol 29 Issue 2, pp. 38-47, Feb.1996.

[11] Mavridis I., Pangalos G., Khair M., "eMEDAC: Role-Based Access Control Supporting Discretionary and Mandatory Features," Proceedings of 13th IFIP WG 11.3 Working Conference on Database Security, Seattle, Washington, USA, 1999.

[12] Joon S. Park, Ravi Sandhu, Gail-Joon Ahn,"Role-Based Access Control on the Web," *ACM Transactions on Information and System Security*, Vol 4 No.1. pp. 37-71, Feb.2001.

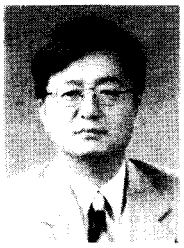
[13] James B. D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford, "Security Models for Web-Based Applications," *Communications of the ACM*, Vol 44 No.2, pp.38-44, Feb. 2001.

[14] John Hoffman, "Implementing RBAC on a Type Enforced System," Proc. of the 13th Annual Computer Security Applications Conference, pp. 158-163, IEEE, 1997.

박 종 화(Chong hwa Park) 정회원

1974년 2월 숭실대학교 전자공학과 졸업
1990년 1월 미국 Syracuse University 컴퓨터공학과 석사
2005년 2월 아주대학교 컴퓨터공학과 박사
1976년~1978년 (주)CDC
1979년~1981년 전자통신연구원
1994년 3월~현재 세명대학교 소프트웨어학과 교수
<관심분야> 정보보호, 시스템 소프트웨어 보안, 네트워크 보안

김 지 홍(Ji hong Kim) 정회원



1982년 2월 한양대학교 전자공학과 졸업
1984년 2월 한양대학교 전자통신공학 석사
1996년 2월 한양대학교 전자통신공학 박사
1982년~1991년 엘지전선 연구소 근무
1995년 정보통신기술사
1991년~2002년 세명대학교 전자공학과 교수
2002년~현재 세명대학교 정보보호학과 교수
<관심분야> 네트워크, 인증 및 접근제어, PKI

김 동 규(Dong kyoo Kim) 정회원

1973년 2월 서울대학교 공과대학 응용수학과 졸업
1979년 2월 서울대학교 자연과학대학원 전자계산학과 석사
1984년 미국 Kansas State University 전자계산학과 박사
1986년~IEEE 802.4, 802.6, 802.10 Working Group Member
1979년~현재 아주대학교 정보 및 컴퓨터공학부교수, Asiacrypt '96 조직위원장, 건설교통부 항공교통관제소 신공항 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국정보보호학회 부회장 역임
<관심분야> 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링