韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-1-5

유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델

황 유 동*, 박 동 규**

Extended GTRBAC Model for Access Control Enforcement in Ubiquitous Environments

Yu-Dong Hwang*, Dong-Gue Park**

요 약

기존의 접근제어 모델들은 유비쿼터스 환경의 접근제어를 위하여 필요한 시간 제약에 따른 자원의 사용 제한 기능, 역할 계층에서 상위 역할로의 제한적 상속 기능, 정교한 위임 정책, 사용자의 위치에 따른 자원의 사용 제한 기능을 제공하지 않는 단점이 있다. 본 논문에서는 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC 모델에 부역할 개념과 PBDM 개념을 적용하고 사용자의 위치 정보를 임시 제약 조건으로 고려하여 유비쿼터스 환경의 접근제어에 적합한 확장된 GTRBAC모델을 제안한다. 제안 모델은 부역할을 사용하여 역할 계층에서 권한의 상속을 제한할 수 있고, 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임과 같은 정교한 위임 정책을 제공하며, 사용자의 위치 정보를 임시 제약 조건으로 고려하여 유비쿼터스 환경의 특성에 맞는 다양하고 정교한 접근제어 정책을 적용할 수 있도록 한다.

Abstract

The existing access control models have the demerits that do not provide the limit function of using resources by time constraint, the restricted inheritance function as a superior role in role hierarchy, the delicate delegation policy and the limit function of using resources by the location information about a user for the access control in ubiquitous environment. This paper proposes an Extended-GTRBAC model is suited to the access control in ubiquitous environment by applying to sub-role concept of GTRBAC model that the application of resources can be restricted by the period and time and PBDM and considering the location information about a user on temporal constraint. The proposal model can restrict the inheritance of permission in role hierarchy by using sub-role, provide the delicate delegation policy such as user-to-user delegation, role to role delegation, multi-level delegation, multi-step delegation, and apply diverse and delicate access control policy which is suited the characteristic of ubiquitous environment by considering the location information about a user on temporal constraint.

▸ Keyword : Access control, temporal constraint, GTRBAC, ubiquitous

---

• 제1저자 : 황유동
• 접수일 : 2005.04.13, 심사완료일 : 2005.06.26
*순천향대학교 정보기술공학부,
※ 본 논문은 정보통신부와 정보통신연구진흥원에서 지원하는 기초기술연구지원사업을 통해서 연구된 과제임.

Ⅰ. 서 론

인터넷과 웹이 활성화됨으로써 사용자는 문서, 디렉토리, 데이터베이스, 웹 페이지 등과 같은 자원들을 액세스하는 것이 훨씬 더 쉬워졌으나 이로 인하여 네트워크의 인증, 자원들을 액세스하기 위한 권한의 허가, 데이터의 정책과 보안 그리고 보안 시스템의 무결성과 같은 중대한 보안 문제들이 생기게 되었다.[17]

정보 보안의 중요한 서비스 중 하나인 접근제어는 컴퓨터내의 자원, 통신 자원 및 정보 자원 등에 대하여 사용, 변경, 조회 등의 작업을 할 수 있는 능력을 가능하게 하거나 제한할 수 있는 수단으로 식별 및 인증된 사용자만이 허가된 범위 내에서 시스템 내부의 정보에 대한 접근을 허용하는 기술적 방법이다.

접근제어를 위해 개발된 보안 정책으로는 임의적 접근 통제(DAC : Discretionary Access Control)[1], 강제적 접근 통제(MAC : Mandatory Access Control)[1], 역할 기반 접근 통제(RBAC : Role Based Access Control)[2, 3, 16] 및 행위 기반 접근 통제(ABAC : Activity Based Access Control)[4,5] 모델과 기업 환경에 적합한 과업-역할 기반 접근 통제 모델(T-RBAC : Task-Role Based Access Control)[6] 모델 등이 있다.

그러나 이들 모델들은 시간 제약에 따른 자원의 사용제한을 하지 못하는 제약, 역할 계층상에서 상위 역할에 배정된 사용자가 하위 역할의 모든 접근 권한을 상속받게 되어 불필요한 권한의 실행을 허가하게 되므로 최소 권한 원칙을 위배하게 되고, 역할 대 역할 위임, 다단계, 다중 위임과 같은 정교한 위임 정책을 고려하지 않는 제약이 있다. 또한 유비쿼터스 환경에서 빈번히 일어날 수 있는 사용자의 위치에 따른 자원에 대한 접근을 제어 할 수 없는 단점이 있다.

유비쿼터스 환경에서는 동일한 사용자라 할지라도 사용자가 자원에 접근하고자 하는 위치에 따라 다른 접근 권한을 부여할 수 있어야 한다. 예를 들면 사무실 내부에서 업무 중에는 외부에 유출되어서는 안돼는 자원에 접근 가능하지만, 정보보호 시스템으로 보호되지 않는 사무실 외부에서 손쉽게 자원에 접근 할 수 있다면 자원이 외부로 유출 또는 보안 위협의 대상이 될 수 있는 가능성이 커지기 때문이다.

이러한 문제점들을 해결하기 위하여 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC (Generalized Temporal Role Based Access Control)[10,11,12] 모델에 부역할(sub role)[7,8]과 PBDM (Permission Based Delegation Model)[14]을 적용하여 권한의 남용을 방지하고, 정교한 위임 정책을 제공하는 확장된 GTRBAC 위임 모델(Extended GTRBAC Delegation Model)[15]이 제시되었으나 이 모델 또한 사용자의 위치 정보에 따라 역할의 활성화와 권한의 허가 등을 제어할 수 없다는 단점이 있다..

본 논문에서는 보안 관리자가 상위 역할로의 권한 상속을 쉽게 통제할 수 있고, 정교한 위임 정책을 제공하는 확장된 GTRBAC 위임 모델에 사용자의 위치 정보를 임시 제약 조건으로 고려하여 유비쿼터스 환경의 정교하고 복잡한 접근제어에 적합한 확장된 GTRBAC모델을 제안한다.

본 논문에서는 2장에서 기존에 연구되어왔던 접근제어 모델들을 분석하고, 3장에서는 제안 모델의 특징을 서술하고 4장에서는 제안 모델과 기존 모델을 비교 분석하며, 5장에서 결론을 유도한다.

Ⅱ. 기존 접근제어 모델의 분석

이 장에서는 접근제어와 관련이 있는 기존 연구들을 재검토하고 그들이 유비쿼터스 환경에 적용될 때 제한 사항들을 분석한다.

접근제어를 위한 보안 정책으로는 역할기반 접근제어 (Role Based Access Control : RBAC) 및 행위기반 접근제어(Activity Based Access Control : ABAC)모델과 기업 환경에 적합한 과업-역할기반 접근제어 모델(Task-Role Based Access Control : T-RBAC), 시간(기간과 주기)에 따른 제약과 역할의 활성화/비활성화, 이벤트, 트리거를 이용하여 자원의 사용을 제한하여 최소 권한 원칙을 이행할 수 있는 GTRBAC 모델, 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행 할 수 없도록 권한의 상속 정도에 따라 하나의 역할을 여러 개로 나누는 권한 상속 제한 역할계층 모델 등이 있다.

역할기반 접근제어(RBAC)[2,3]는 사용자와 자원 관리를 경감시키기 위해 사용된다. 역할기반 접근제어에서 접근 권한은 역할과 관련이 있으며 사용자는 적절한 역할에 할당된다. 역할기반 접근제어는 접근제어 요구 사항을 지정하는 첫 번째 수단으로서 역할 추상화를 사용한다. 역할을 관리

하는 동안에, 허가들은 역할들에 할당되고, 사용자들은 역할에 할당된다. 허가는 정보에 특정한 오퍼레이션을 수행할 능력을 승인하는 것이다. 현실 세계에서, 하나의 역할은 조직 내에서 하나의 직무 기능으로 정의할 수 있으며, 그 역할에 할당된 사용자에 부여된 권한과 책임을 의미한다. 하나의 역할 계층(role hierarchy)은 일반적으로 조직의 관리 구조에 따라서 역할사이의 권한 상속관계를 나타낸다. 역할 계층은 허가 권한 시스템과 유사하기 때문에 기업 조직 구조의 모델링에 적합하다. 그러나 역할기반 접근제어는 접근 권한의 동적 활성화와 응용 레벨 제약의 명세를 필요로 하는 워크플로우(workflow)를 고려하지 않고 있다.

행위기반 접근제어(ABAC)[5, 7]는 워크플로우에 의해서 표현된 공동 작업 환경을 위하여 연구된 것으로 공통 목표를 달성하기 위하여 결합된 활동의 집합으로 정의된다. DAC, MAC 및 RBAC 모델의 경우는 접근 권한의 부여시점에서 권한이 활성화(activate)되어 임의의 시점에서 사용가능한 반면에 행위기반 접근제어 모델에서는 사용자에 대한 접근 권한 할당(access right assignment)과 접근 권한 활성화(access right activation)로 분리된다. 어떤 사용자가 워크플로우 내의 과업에 대한 실행권한을 부여 받았다하더라도 그 권한의 사용은 워크플로우의 진행 상태에 따라 제약을 받는다. 행위기반 접근제어 모델은 애플리케이션 레벨 제약을 위한 명세를 제공하고 현실 세계의 무결성 규칙의 구현을 지원한다. 그러나 행위기반 접근제어는 기업 환경에서 워크플로우에 속하지 않는 많은 작업들을 다루지 않고 있어 사용이 제한적이다.

과업 역할기반 접근제어 모델(Task-Role Base Access Control Model : T-RBAC)[6]은 역할기반 접근제어 모델을 기초로 하여 행위기반 접근제어 모델을 통합한 모델이다. 과업 역할기반 접근제어 모델과 역할기반 접근제어 모델의 가장 큰 차이점은 접근 권한(access rights)을 부여하는 방법이다. 역할기반 접근제어에서는 접근 권한이 직접 역할에 부여되나, 과업-역할기반 접근 통제 모델에서는 접근 권한이 그 역할이 수행하는 과업(task)을 통해 부여된다는 점이다. 과업 역할기반 접근제어 모델에서 과업은 3개의 클래스로 분류된다. 클래스 S에 속하는 과업은 계승시킬 수 있으며, 그들의 접근 권한은 역할 계층에서 더 높은 역할로 상속된다. 클래스 P에 속하는 과업은 단일 역할에 할당 가능한 과업으로 역할계층에서 상위의 역할로 상속되지 않는다. 클래스 W에 속하는 과업은 활동적인 보안 정책으로 워크플로우 메커니즘에 의해서 관리된다. 그래서 과업 역할기반 접근제어 모델은 기업 환경에 대하여 행위기반 접근제어 모델과 역할기반 접근제어 모델의 제한 사항들을 해결한다. 그러나 과업 역할기반 접근제어 모델은 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한하여 최소 권한 원칙을 이행할 수 있는 방법을 제공하지 않아 최근의 변화하는 기업 환경에 적용하기에는 무리가 따른다.

확장된 GTRBAC 위임 모델(Extended GTRBAC Delegation Model)은 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC 모델에 부역할 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고, 최소권한의 원칙을 지킬 수 있는 확장된 GTRBAC 모델에 PBDM 개념을 적용하여 사용자 대 사용자 위임, 역할 대 역할 위임, 다중 위임과 다단계 위임 기능을 제공한다.

확장된 GTRBAC 위임 모델은 역할과 권한을 위임하고자 할 때 위임 역할(DTR : Delegation Roles)을 생성하고 생성된 위임 역할을 위임받을 사용자의 고유 역할에 역할 대 역할 할당관계에 의해 할당된 임시 위임 역할(TDR : Temporal Delegatable Roles)에 할당되고, 이 역할 대 역할 할당관계에 의해 사용자 대 사용자 위임, 역할 대 역할 위임이 가능해 진다.

확장된 GTRBAC 위임 모델은 다양하고 정교한 위임 정책과 역할 계층에서 상속의 제한 기능을 제공하지만 사용자의 위치 정보에 따른 자원의 사용을 제한하지 않아 모바일 기업 환경에 적용하기에는 무리가 따른다.

위 내용으로 각 접근제어 모델들이 장점을 가지고 있지만 모바일 기업 환경에 적용하기에는 여러 가지 제한 사항들이 있음을 알 수 있다.

본 논문에서는 다음과 같은 특징을 가지는 유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델을 제안한다.

- -. 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있다.
- -. 역할 활성화와 이벤트, 트리거를 이용하여 사용자 수를 제한하고 워크플로우에 해당하는 작업을 다룰 수 있다.
- -. 부역할(sub role) 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고 최소권한 원칙을 이행할 수 있다.

표 1 확장된 GTRBAC 모델의 부역할 특징
Table 1. Sub-Role characteristics of Extended GT-RBAC Model

부 역할	상속의 정도	위임	부 역할에 할당된 권한의 특징
CC	무제한 상속	불가능	-. 조직 내 모든 사용자에게 허가된 권한 -. 부서에 속한 사용자들에게만 허가된 권한 -. 상위 역할은 하위 역할의 모든 권한을 상속
FDCC		가능	-. 조직공통역할(CC)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
RI	제한 상속 - 지정 단계 만큼	불가능	-. 역할 분석과 설계 과정에서 상속이 제한되는 권한에 대한 조사 필요 -. 하위 역할의 권한이 지정된 상위 역할까지만 상위로 상속 -. 역할 간에 제한적 상속이 가능함
FDRI		가능	-. 상속 제한 역할(RI)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
PR	상속 불가	불가능	-. 상위 역할로 상속이 이루어지지 않는 권한을 할당
FDPR		가능	-. 고유역할(PR)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
TDR	상속 불가	가능	-. 위임자로부터 역할 대 역할 할당 관계에 의해 권한을 할당 -. 이 역할에 할당된 권한들은 다단계 위임 될 수 있다.

-. PBDM(Permission Based Delegation Model)을 적용하여 사용자 대 사용자, 역할 대 역할, 다단계, 다중 위임 기능을 제공한다.

-. 사용자의 위치 정보를 제약 조건(Temporal Constraint)으로 고려하여 사용자의 위치에 따른 자원의 사용을 제한할 수 있는 기능을 제공한다.

III. 유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델

유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델은 다음 (그림 1)과 같이 사용자의 위치 정보에 따른 자원의 사용을 제한하기 위하여 확장된 GTRBAC 위임 모델의 제약조건에 위치 정보를 고려한 모델이다.

제안 모델에서는 다음 (그림 1)에서와 같이 사용자 - 역할 할당 관계에 의해서 사용자에게 부역할들 중 고유역할을 할당하고 다른 부역할 들에 할당된 권한은 사용자가 고유역할을 활성화 했을 때 부역할 계층의 상속관계에 의해서 사용자에게 할당된다.

제안 모델에서 부역할은 부역할에 할당된 권한들의 상속정도와 위임 가능성에 따라 〈표 1〉과 같이 분류할 수 있다.

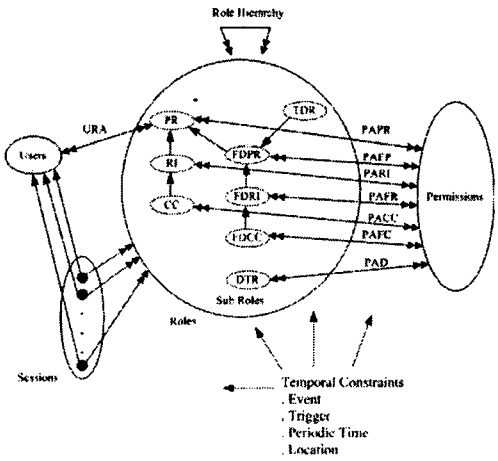

그림 1 유비쿼터스 환경의 접근제어를 위한 확장된 GTRBAC 모델
Fig 1. Extended GTRBAC Model for Access Control Enforcement in Ubiquitous Environments

3.1 정형적 명세

제안 모델을 정형적으로 표현하면 아래와 같고 정의에서 사용되는 기호들은 다음의 〈표 2〉와 같다.

표 2 정형적 명세에 사용된 기호
Table 2. Using Symbol for Formal Definition

명칭	설명
r, u, p, s, l	역할, 사용자, 권한, 세션, 위치 정보
rPR	고유 역할
rFDPR	위임 가능한 고유역할
rRI	상속 제한 역할
rFDRI	위임 가능한 상속 제한 역할
rCC	조직 공통 역할
rFDCC	위임 가능한 조직 공통 역할
pPR	고유역할에 할당된 권한
pFDPR	위임 가능한 고유역할에 할당된 권한
pRI	상속제한 역할에 할당된 권한
pFDRI	위임 가능한 상속 제한 역할에 할당된 권한
pCC	조직 공통 역할에 할당된 권한
pFDCC	위임 가능한 조직 공통 역할에 할당된 권한
rTDR	임시 위임 역할
pDTR	위임 역할에 할당된 권한

제안 모델을 정형적으로 표현하면 다음과 같다.

□□ DBR = FDPR ∪ FDRI ∪ FDCC ∪ TDR : delegatable roles

□□ R = PR ∪ RI ∪ CC ∪ DBR ∪ DTR

□□ (PR ∩ DBR) ∪ (RI ∩ DBR) ∪ (CC ∩ DBR) = Ø

□□ (PR ∩ DTR) ∪ (RI ∩ DTR) ∪ (CC ∩ DTR) = Ø

□□ DBR ∩ DTR = Ø

□□ (FDPR ∩ TDR) ∪ (FDRI ∩ TDR) ∪ (FDCC ∩ TDR) = Ø

□□ URA ⊆ U × PR

□□ PAPR ⊆ P × PR

□□ PAFP ⊆ P × FDPR

□□ PARI ⊆ P × RI

□□ PAFR ⊆ P × FDRI

□□ PACC ⊆ P × CC

□□ PAFC ⊆ P × FDCC

□□ PAD ⊆ P × DTR

□□ PRA = PAPR ∪ PAFP ∪ PARI ∪ PAFR ∪ PACC ∪ PAFC ∪ PAD

□□ RAD = TDR × DTR

□□ user_r(r) : PR → 2U : 고유 역할에 할당된 사용자 에게 고유 역할을 매핑하는 함수

□□ own_ri(r) : RI → PR : 부역할 계층에 의해 상속 제한 역할을 고유역할에 매핑하는 함수

□□ own_cc(r) : CC → RI : 부역할 계층에 의해 조직 공통 역할을 상속 제한 역할에 매핑하는 함수

□□ own_fdpr(r) : FDPR → PR : 부역할 계층에 의해 위임 가능한 고유 역할을 고유역할에 매핑하는 함수

□□ own_fdri(r) : FDRI → FDPR : 부역할 계층에 의해 위임 가능한 상속 제한 역할을 위임 가능한 고유역할에 매핑하는 함수

□□ own_fdcc(r) : FDCC → FDRI : 부역할 계층에 의해 위임 가능한 조직 공통 역할을 위임 가능한 상속 제한 역할에 매핑하는 함수

□□ own_td(r) : TDR → FDPR : 부역할 계층에 의해 임시 위임 역할을 위임 가능한 고유 역할에 매핑하는 함수

□□ ∀rr ∈ PR, ∃u : U, ri : RI, cc : CC, fdpr : FDPR, fdri : FDRI, fdcc : FDCC, tdr : TDR • (u, rr) ∈ URA ∧ rr = own_dpr(r) : FDPR → 2DTR and ∄(fdpr1, fdpr2 ∈ FDPR, dtr ∈ DTR) • (fdpr1 ≠ fdpr2) ∧ (dtr ∈ own_fdpr(fdpr1) ∧dtr ∈ own_fdpr(fdpr2)) : 위임 가능한 고유 역할을 위임 역할에 매핑하는 함수

□□ own_dri(r) : FDRI → 2DTR and ∄(fdri1, fdri2 ∈ FDRI, dtr ∈ DTR) • (fdri1 ≠ fdri2) ∧ (dtr ∈ own_fdri(fdri1) ∧dtr ∈ own_fdri(fdri2)) : 위임 가능한 상속 제한 역할을 위임 역할에 매핑하는 함수

□□ own_dcc(r) : FDCC → 2DTR and ∄(fdcc1, fdcc2 ∈ FDCC, dtr ∈ DTR) • (fdcc1 ≠ fdcc2) ∧ (dtr ∈ own_fdcc(fdcc1) ∧dtr ∈ own_fdcc(fdcc2)) : 위임 가능한 조직 공통 역할을 위임 역할에 매핑하는 함수

□□ rad(r) : TDR → 2DTR : 임시 위임 역할에 위임 역할을 매핑하는 함수

□□ permissions_pr(r) : PR → 2P : 권한 집합을 고유 역할에 매핑하는 함수

□□ permissions_ri(r) : RI → 2P : 권한 집합을 상속 제한 역할에 매핑하는 함수

□□ permissions_cc(r) : CC → 2P : 권한 집합을 조직 공통 역할에 매핑하는 함수

□□ permissions_fdpr(r) : FDPR → 2P : 권한 집합을 위임 가능한 고유 역할에 매핑하는 함수

□□ permissions_fdri(r) : FDRI → 2P : 권한 집합을 위임 가능한 상속 제한 역할에 매핑하는 함수

□□ permissions_fdcc(r) : FDCC → 2P : 권한 집합을 조직 공통 역할에 매핑하는 함수

□□ permissions_d(r) : DTR → 2P : 권한 집합을 위임 역할에 매핑하는 함수

□□ permissions_t(r) : TDR → 2P : RAD 관계로부터 상속된 권한 집합을 임시 위임 역할에 매핑하는 함수

□□ permissions_f(r) : FDPR → 2P : RAD와 PAFP, PAFR, PAFC 관계로부터 위임된 권한 집합을 위임 가능한 고유역할에 매핑하는 함수

□□ permissions_pr(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PAPR}

□□ permissions_ri(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PARI}

□□ permissions_cc(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PACC}

□□ permissions_fdpr(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PAFP}

□□ permissions_fdri(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PAFR}

□□ permissions_fdcc(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PAFC}

□□ permissions_d(r) = {p : P | ∃r′ ≤ r • (r′, p) ∈ PAD}

□□ permissions_t(r) = {p : P | ∃r′ ∈ DTR • (r′, p) ∈ PAD ∧ r′ ∈ rad(r′)}

□□ permissions_f(r) = {p : P | (r, p) ∈ PAFP} ∪ {p : P | ∃r′ ∈ TDR • p ∈ permissions_t(r′) ∧ r = own_td(r′)} ∀dtr ∈ DTR, ∃fdpr ∈ FDPR • ((dtr ∈ own_dpr(fdpr)) ∪ (dtr ∈ own_dri(fdri)) ∪ (dtr ∈ own_dcc(fdcc))) ∧ (permissions_d(dtr) ⊆ permission_f(fdpr)) : 생성된 위임 역할에 RAD와 PAFP, PAFR, PAFC에 의해 위임 가능한 역할들에 할당된 위임 가능한 권한. (다단계 위임에 필요)

□□ can_delegate ⊆ FDPR × Pre_con × P_range × M : Pre_con 은 전제조건(prerequisite condition), P_range 는 위임 범위(delegation range), M 은 최대 위임 단계(maximum delegation depth) : 위임 범위, 전제조건, 최대 위임 단계에 따라 위임 가능한 역할의 매핑 관계 정의

3.2 임시 역할 계층의 정형적 명세

제안 모델의 임시 역할 계층을 정형적으로 표현하면 다음의 정의{1 ~ 9}와 같다.

모든 r(역할), u(사용자), p(권한), s(세션)는 시간 상수 $t \geq 0$, 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소 일 때 다음과 같은 의미를 가진다.

1. assigned(p, rPR, t, l) → can_be_acquired ({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, {rPR, rRI, rCC , rFDPR, rFDRI, rFDCC, rTDR}, t, l)
2. assigned(u, rPR, t, l) → can_activate(u, rPR, t, l)
3. can_activate(u, rPR, t, l) ∧ can_be_acquired ({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, {rPR, rRI, rCC, rFDPR, rFDRI, rFDCC, rTDR}, t, l) → can_acquire(u, {pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, t, l)
4. active(u, rPR, s, t, l) ∧ can_be_acquired ({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, {rPR, rRI, rCC, rFDPR, rFDRI, rFDCC, rTDR}, t, l) → acquires(u, {pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, s, t, l)

각 함수의 의미는 다음과 같다.

-. assigned() : 사용자 또는 권한에 역할의 할당
-. can_be_acquired() : 권한의 획득 가능
-. can_activate() : 역할 활성화 가능
-. can_acquire() : 권한의 획득 가능
-. active() : 세션 상에서 역할의 활성화
-. acquires() : 세션 상에서 권한의 획득

다음의 [정의 1, 2, 3]은 모바일 기업 환경의 접근제어를 위한 확장된 GTRBAC 모델의 일반 역할 계층에 대한 정의이고, [정의 4, 5, 6]은 약한 제한적 역할 계층의 정의이고, [정의 7, 8, 9]는 강한 제한적 역할 계층의 정의 이다.

[정의 1] Unrestricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x \geq_t y$)이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 I-역할 계층은 다음과 같은 의미를 가진다.

- yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 : $\forall p, (x \geq_t y) \wedge$ can_be_acquired({pRI, pCC, pFDRI, pFDCC}, {yPR, yRI, yCC, yFDPR, yFDRI, yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)
- yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 : $\forall p, (x \geq_t y) \wedge$ can_be_acquired({pCC, pFDCC,}, {yCC, yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)

[정의 2] Activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x >_t y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 A-역할 계층은 다음과 같은 의미를 가진다.

- $\forall u, (x >_t y) \wedge$ can_activate(u, xPR, t, l) → can_activate(u, yPR, t, l)

[정의 3] General inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x \geq_t y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 IA-역할 계층은 다음과 같은 의미를 가진다.

- $(x \geq_t y) \leftrightarrow (x \geq_t y) \wedge (x >_t y)$

[정의 4] Weakly restricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x \geq_{w,t} y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 I-역할 계층은 다음과 같은 의미를 가진다.

- yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 : $\forall p, (x \geq_{w,t} y) \wedge$ enabled(xPR, t, l) ∧ can_be_acquired({pRI, pCC, pFDRI, pFDCC}, {yRI, yCC, yFDRI, yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)
- yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 : $\forall p, (x \geq_{w,t} y) \wedge$ enabled(xPR, t, l) ∧ can_be_acquired({pCC, pFDCC}, {yCC, , yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)

[정의 5] Weakly restricted activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x >_t y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 A-역할 계층은 다음과 같은 의미를 가진다.

- $\forall u, (x >_{w,t} y) \wedge$ enabled(yPR, t, l) ∧ can_activate(u, xPR, t, l) → can_activate(u, yPR, t, l)

[정의 6] Weakly restricted general inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x \geq_{w,t} y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 IA-역할 계층은 다음과 같은 의미를 가진다.

- $(x \geq_{w,t} y) \rightarrow (x \geq_{w,t} y) \wedge (x >_{w,t} y)$

[정의 7] Strongly restricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x \geq_{s,t} y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 I-역할 계층은 다음과 같은 의미를 가진다.

- yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 : $\forall p, (x \geq_{s,t} y) \wedge$ enabled(yPR, t, l) ∧ enabled(xPR, t, l) ∧ can_be_acquired({pRI, pCC, pFDRI, pFDCC}, {yRI, yCC, yFDRI, yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)
- yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 : $\forall p, (x \geq_{s,t} y) \wedge$ enabled(yPR, t, l) ∧ enabled(xPR, t, l) ∧ can_be_acquired({pCC, pFDCC}, {yCC, yFDCC}, t, l) → can_be_acquired(p, xPR, t, l)

[정의 8] Strongly restricted activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할($x >_{s,t} y$) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 A-역할 계층은 다음과 같은 의미를 가진다.

• ∀u, (x ⩾s,t y) ∧ enabled(xPR, t, l) ∧ enabled(yPR, t, l) ∧ can_activate(u, xPR, t, l) → can_activate(u, yPR, t, l)

표 3 접근제어 모델의 특징 비교
Table 3. characteristic comparison of Access Control Model

		RBAC	ABAC	TRBAC	GTRBAC	sub-role	PBDM	제안모델
워크플로우 고려		×	○	클래스W 과업 이용	이벤트와 트리거 이용	×	×	이벤트와 트리거 이용
일반 역할 및 권한 고려		○	×	○	○	○	○	○
제약	역할 활성화 시간 / 기간	×	×	×	○	×	×	○
	사용자의 위치 정보	×	×	×	×	×	×	○
역할의 제한적 상속	역할의 활성화 제약과 유효 시간 제약 이용	×	×	×	○	×	×	○
	부역할 이용	×	×	×	×	○	×	○
	사용자의 위치 정보 이용	×	×	×	×	×	×	○
역할 활성화 유효 시간 및 기간 적용		×	×	×	○	×	×	○
위임	사용자 대 사용자	×	×	×	×	○	○	○
	역할 대 역할	×	×	×	×	○	○	○
	다단계	×	×	×	×	×	○	○
	다중	×	×	×	×	×	○	○
	위임된 권한이 할당된 역할의 유효 시간 및 기간에 따른 제약	×	×	×	×	×	×	○
	사용자의 위치 정보에 따라 위임된 권한의 활성화 제약	×	×	×	×	×	×	○

〔정의 9〕 Strongly restricted general inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할(x ⩾s,t y) 이고 사용자가 역할을 활성화 하는 장소 l이 보안 정책에서 요구하는 장소일 때 lA-역할 계층은 다음과 같은 의미를 가진다.

• (x ⩾s,t y) → (x ⩾s,t y) ∧ (x ⩾s,t y)

단, 위 〔정의 1, 2, 3〕은 시간 제약을 이용하여 권한의 상속과 역할의 활성화를 제한하지 않는 경우이다.

Ⅳ. 제안 모델과 기존 모델의 비교

유비쿼터스 환경의 접근제어를 위하여 사용자의 위치 정보를 고려하여 자원의 사용을 제한하는 새로운 접근제어 모델과 기존 접근제어 모델의 특징을 비교하면 〈표 3〉과 같다.

제안 모델의 특징은 다음과 같다.

-. 이벤트와 트리거를 이용하여 워크플로우 고려

-. 기존의 접근제어 모델들과 마찬가지로 일반 역할 및 권한 고려

-. 역할 활성화 시간, 주기, 기간을 이용한 역할 활성화 제약,

-. 사용자의 위치 정보에 따른 역할 활성화 제약

-. 역할 계층에서 역할 활성화 제약을 이용한 권한의 제한적 상속

-. 역할 계층에서 부역할을 이용한 권한의 제한적 상속

-. 임시 위임 역할과 위임 가능한 권한을 할당한 부역할을 이용한 사용자 대 사용자 위임, 역할 대 역할 위임, 다중 위임, 다단계 위임

-. 위임된 권한이 할당된 역할의 시간, 주기, 기간에 따른 역할 활성화 제약

-. 사용자의 위치 정보에 따른 위임된 권한이 할당된 역할의 활성화 제약

위와 같은 제안 모델의 특징은 기존의 접근제어 모델에서는 부분적으로 제공되거나 제공되지 않던 기능이다.

본 논문에서는 위 기능들을 제공함으로써 유비쿼터스 환경에서 복잡하고 정교한 접근제어 정책을 구현 할 수 있도록 한다.

V. 결론

본 논문에서는 기존의 접근제어 모델에서 제공하지 않거나 부분적으로 제공하는 다음과 같은 기능을 제공하는 새로운 접근제어 모델을 제안한다.

-. 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한하는 기능.

-. 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고, 최소권한의 원칙을 지킬 수 있는 제한된 상속 기능.

-. 기업 환경에서 반드시 필요하고 빈번히 발생할 수 있는 사용자 대 사용자(user to user) 권한 위임과 역할 대 역할(role to role) 권한 위임, 다단계 위임 및 다중 위임과 같은 정교한 위임 정책.

-. 사용자의 위치정보를 고려하여 자원의 접근 권한을 제어하는 기능.

따라서 제안 모델은 유비쿼터스 환경의 접근제어 시스템에 적합한 모델이라 할 수 있다.

향후에는 유비쿼터스 환경에서 발생할 수 있는 다양하고 복잡한 문제를 해결하기 위하여 접근제어 시스템에 보안 정책을 적용하였을 때 보안 정책이 자동으로 적용되어 보안 관리자가 정책을 보다 간편하고 효율적으로 관리할 수 있는 형식 언어와 접근제어 관리 모델 및 시스템에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] C.P.Pfleeger, Security in Computing, second edition, Prentice-Hall International Inc, pp.290-315 , 1997

[2] R.S.Sandhu and E.J.Coyne and H.L.Feinstein and C.E.Youman "Role-Based Access control Models", IEEE Computer, vol. 29, pp.38-47, 1996

[3] D.Ferraiom and J.Cugini and R.Kuhm "Role -based Access Control(RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995

[4] Dagstull and G.Coulouris and J.Dollimore "A Security Model for Cooperative work : a model and its system implications" Positions paper for ACM European SIGOPS Workshop, 1994

[5] R.K.Thomas and R.S.Sandhu "Task-based Authorization Controls(TBAC) : A Family of Models for Active and Enterprise-oriented Authorization Management" Proc. of the IFIP WF11.3 Workshop on Database Security, 1997

[6] S. Oh and S. Park "Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment", Proceedings of the 11th International Conference on Database and Expert Systems Applications, pp. 264-273, 2000

[7] HyungHyo Lee and YoungRok Lee and BongNam Noh "A New Role-Based Delegation Model Using Sub-Role Hierarchies" Proceedings of the 18 th Computer and Information Sciences - ISCIS2003, pp.811-818, 2003

[8] YongHoon Yi and MyongJae Kim and YoungLok Leem and HyungHyo Lee and BongNam Noh "Applying RBAC Providing Restricted Permission

Inheritance to a Corporate Web Environment", Proceedings of the 5 th Asia-Pacific Web Conference, pp. 287-292, 2003

[9] E. Bertino and P. A. Bonatti and E. Ferrari "TRBAC: A Temporal Role-based Access Control Model", Proceedings of the fifth ACM workshop on Role-based access control, pp.21-30, 2000

[10] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Hierarchies and Inheritance Semantics for GTRBAC", Seventh ACM Symposium on Access Control Models and Technologies, pp. 74-83, 2002

[11] J. B. D. Joshi and E. Bertino and A. Ghafoor "Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model", Proceedings of the 26 th Annual International Computer Software and Applications Conference, 2002

[12] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Role Hierarchies in GTRBAC", CERIAS, 2002

[13] 황유동, 박동규, "기업환경의 접근제어를 위한 확장된 GTRBAC 모델", 한국멀티미디어학회, 2005.02, 8권 2호, pp211-224

[14] Xinwen Zhang, Sejong Oh, Ravi Sandhu "PBDM : A Flexible Delegation Model in RBAC", SACMAT, pp.149-157, 2003

[15] 황유동, 박동규, "Context를 고려한 확장된 GTRBAC 모델", 순천향산업기술연구소논문집, pp.229-234, 2004.12

[16] 박동규, 황유동, 안현수, "SECOS의 접근제어를 위한 RBAC의 구현", 한국컴퓨터정보학회논문지, 2002.1, 7권 2호, pp.9-18

[17] 김강, 박진섭, "정보시스템 보안을 위한 위험분석 모델", 한국컴퓨터정보학회논문지, 2002.9 7권3호, pp.60-67

저 자 소 개

황 유 동

2000년 : 순천향대학교 전기전자공학과 정보통신전공 석사

2003년 순천향대학교 전기전자공학과 정보보호전공 박사 수료

〈관심분야〉 시스템 보안, 네트워크 보안

박 동 규

한양대학교 대학원 전자공학과 공학박사

1992~현재 : 순천향대학교 정보기술공학부 교수

〈관심분야〉 시스템 보안, 네트워크 보안