韓國 컴퓨터情報學會 2006하계학술발표논문집&학회지
第14卷 第1號, 2006. 6.

유비쿼터스 컴퓨팅 환경에서의 컨텍스트 접근 제어 고찰

정 헌 만*, 이 세 훈**

Context Access Control in Ubiquitous Computing Environment

Jung Heon Man*, Lee Se Hoon**

요 약

이 연구에서는 유비쿼터스 컴퓨팅 환경에서 정보 보안 문제를 접근 제어 기법을 중심으로 두가지 방식에 대한 연구 형태를 분석 고찰하며, 기존 연구들의 장단점을 비교하여 유비쿼터스 환경에서의 상황 인식 서비스 플랫폼 개발시 핵심적으로 고려해야할 중요 요소를 설계할 때 필요한 레퍼런스를 제안한다. 첫 번째는, 유비쿼터스 환경에서 역할 기반 접근 제어 방식을 적용하는데 문제점을 상황 정보를 활용하여 해결하는 연구 방향에 대한 고찰이다. 두 번째는, 유비쿼터스 환경에서 상황 정보는 개인의 정보 보호에 관련해 중요한 사항이므로, 여기에 역할 기반 접근 제어 방법을 적용하여 해결하는 연구이다. 이러한 두 가지 연구 방향은 상황 인식 서비스 플랫폼 설계시 중요하게 고려해야 할 사항이다.

Abstract

In this paper, we study to two research direction about information security in ubiquitous computing environment. First, researches on context-aware access control using user's context or environment conditions based on role-based control. Second, researches on model for access control about context information in ubiquitous computing utilizing role base access control model. Two research directions are the one of the most important point technology in that embody ubiquitous environment in the actual world.

▸ Keyword : 역할기반접근제어(role based access control), 컨텍스트 접근제어(Context access control), 유비쿼터스 컴퓨팅(Ubiquitous Computing)

• 제1저자 : 정헌만
* 인하대학교 컴퓨터 공학부 ** 인하공업전문대학 컴퓨터시스템과

Ⅰ. 서 론

유비쿼터스 컴퓨팅 환경은 사람, 컴퓨팅 기기, 환경 등이 상호 작용하여 시스템이 자율적으로 사람을 포함한 사물이 필요로 하는 사항들을 처리해 주는 환경을 의미한다. 이러한 환경에서의 정보 접근은 언제 어디서나 어떤 장치로 접근이 가능하게 구성된다[10]. 여기서 보안 정책은 일반 시스템에서 보다 강건하고 유연해야 하며, 유비쿼터스 환경에 적합한 모델 지원이 중요하며 유비쿼터스 환경 구성의 성패를 결정짓는 중요한 요소라 할 수 있다[13,15].

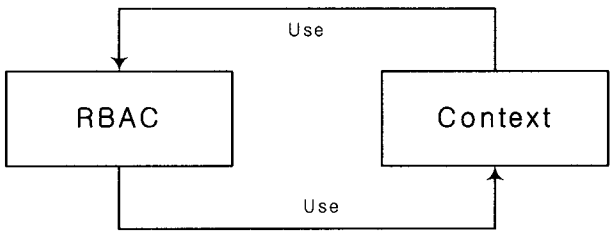
이 연구에서는 유비쿼터스 환경에 알맞게 기존의 접근제어 기법을 보완하는데 상황 정보를 활용하는 모델들을 분석하고, 상황 정보를 보호하기 위해 역할 기반 접근 제어 방법을 활용하는 모델의 두 가지를 분석함으로써, 상황 인식 서비스 플랫폼 설계에 고려되어야 할 핵심적인 요소에 대한 기반 기술을 제공한다.

접근 제어 모델은 정보 보안 분야에서 상당히 많은 연구가 진행되어 왔으며 역할 기반 접근 제어(RBAC : Role Based Access Control) 모델은 접근 권한을 역할 이름에 따라 그룹화하고 사용자 개개인의 책임과 권한에 따라 역할을 부여함으로써 보안 관리의 효율성을 극대화시켰다[1,3,8,9]. 그러나 유비쿼터스 환경에서는 시간에 따른 접근 제어 등과 같이 컨텍스트에 근거한 접근 제어가 필요하며, 역할 기반 접근 제어 모델에서는 이를 수용하기에 한계가 있다.

따라서 유비쿼터스 환경에 맞는 즉, 다양한 컨텍스트 정보를 어플리케이션에서 얻을 수 있는 환경에 역할 기반 접근 제어를 적용할 수 있는 연구들이 진행되고 있다[4,11,12]. 대표적인 연구로 역할 기반 접근 제어 기반에서 컨텍스트 정보를 추가한 일반화된 역할 기반 접근 제어(GRBAC : Generalized RBAC) 모델이 있다[6,13]. GRBAC 모델은 접근 제어 결정에 사용자 역할, 객체 역할, 환경 역할 등을 사용함으로써 기존 RBAC을 확장하였고, 3가지 요소를 역할로 구조화함으로써 접근 제어 정책 기술의 단순함과 융통성을 제공하였다. 다른 연구로는 컨텍스트 정보를 접근 제어 결정에 이용하기 위해 RBAC 제약 사항을 컨텍스트 제약 사항으로 사용하는 xoRBAC 모델이 있다[7,13]. 컨텍스트 제약 사항, 컨텍스트 속성, 컨텍스트 함수, 컨텍스트 조건 등이며 권한은 여러 개의 컨텍스트 제약과 관련되고 모든 컨텍스트 제약이 참 값을 가질 때 접근이 허용된다. 또한 정보의 보안 수준에 따른 접근 제어를 수행하기 위한 컨텍스트 정보 구조화를 통해 컨텍스트 정보를 이용한 접근 제어 기법과 컨텍스트 정보 사이에 충돌 문제 해결을 제안하고 있다[13].

유비쿼터스 환경에서 컨텍스트 정보는 매우 중요한데, 이러한 컨텍스트 정보를 접근 제어하기 위한 방법으로 역할 기반 접근 제어를 사용하는 연구 분야가 있으며, 여기서 컨텍스트에 대한 연관성을 분석하여, 이를 역할 권한에 할당한다[7,15].

그림 1은 유비쿼터스 환경에서 정보보안 연구에서 RBAC 모델에 컨텍스트 정보를 도입하는 연구와 컨텍스트 정보 보호를 위해 RBAC 모델을 도입하는 연구를 그림으로 나타낸 것이다.



[그림 1] 유비쿼스트 환경에서 접근제어

II. 접근 제어와 컨텍스트 인식

2.1 접근 제어

(1) 강제적 접근 제어 및 자율적 접근 제어

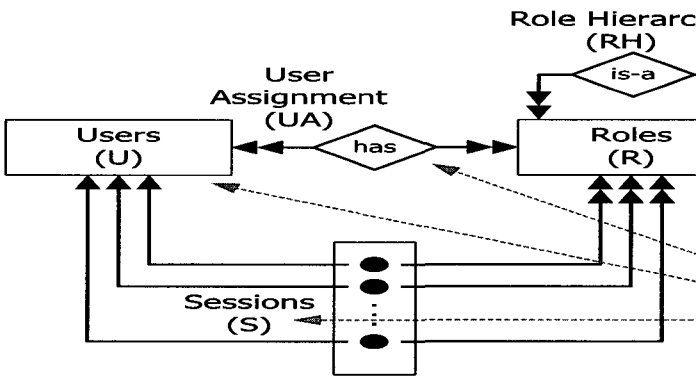
전통적인 접근 제어 정책은 다음과 같이 강제적 접근 제어, 자율적 접근 제어로 분류할 수 있다. 강제적 접근 제어(Discretionary Access Control)는 각 정보에 결합된 비밀 등급과 사용자에 부여된 인가 등급을 미리 규정된 규칙에 따라 비교하여 그 규칙을 만족하는 사용자만에게 접근 권한을 부여하는 접근 제어 방식이다. 자율적 접근 제어(Mandatory Access Control)는 주체나 그들이 소속되어 있는 그룹들의 신분(ID)에 근거하여 객체에 대한 접근을 제한하는 방법이다. 즉, 접근 통제는 개체의 소유자에 의하여 임의적으로 이루어지며, 강제적 접근 제어에 비하여 유연한 권한 부여 기능을 제공한다.

자율적 접근 제어와 강제적 접근 제어의 메커니즘인 접근 제어 목록, 능력 기반 접근 제어, 레이블 기반 접근 제어 기법들은 규칙 수준에서 접근 제어 서비스를 제공하며, 각 사용자에게 권한을 직접 할당함으로써, 대규모화되고 복잡화 되는 접근 제어 요구를 만족시키기 어렵다.

(2) 역할 기반 접근 제어

역할 기반 접근 제어(Role-Based Access Control)는 전통적인 제어 기법과 달리 정보에 대한 사용자의 권한 부여 여부를 각 사용자의 식별자나 이미 정의된 규칙에 의해 판단하지 않고, 사용자가 소속된 조직 내에서의 역할에 의해 결정하는 특징을 가지고 있다. 따라서, 역할과 객체간의 관계로 접근 권한을 관리함으로써, 사용자와 객체의 수가 대단히 많은 분산·기업 환경에 적합한 특성을 제공한다[1,3,8,9].

Sandhu는 역할 기반 접근 제어를 다음과 같은 네 가지 모델로 구분하여 제안하였다. 즉, 역할 기반 접근 제어를 기본 모델인 RBAC0와 기본 모델에 역할의 상속 개념인 역할 계층(role hierarchy)을 추가한 RBAC1, 기본 모델에 제약 조건(constraints)을 추가 시킨 RABC2, 그리고 RBAC1과 RBAC2의 통합 모델인 RBAC3로 구분하였다[8,9]. 그림 2는 이러한 역할 기반 접근 통제 모델의 특징을 보인다.



[그림 2] 역할 기반 접근 제어 모델

역할의 접근 제어 성분은 역할-접근권한(PA) 관계, 사용자-역할(UA) 관계가 있다. PA 관계에서 역할은 다수의 접근 권한이 부여될 수 있고, 동일 접근 권한에 여러 역할이 할당될 수 있는 관계이며, UA 관계는 사용자가 여러 역할을 가질 수 있고 동일 역할에 다수의 사용자가 할당될 수 있는 관계이다.

세션의 접근 제어 성분에는 세션-사용자 관계 함수(user(s_i))와 세션-역할 관계 함수(role(s_i))가 있다. 세션-사용자 관계 함수는 세션의 생명주기 동안 일정하고, 세션-역할 관계 함수에서 세션이 가질 수 있는 접근 권한의 수는

$$\cup r \in roles(si) \{ p \mid (p, r) \ PA\}$$

으로 표시된다. 즉, 세션 안에 있는 역할들이 가지고 있는 접근 권한의 합집합으로 나타낼 수 있다.

역할계층(role hierarchy)은 역할에 배정된 권한들 사이에 포함 관계가 있는 역할들 간의 부분 순서 관계로서 기업의 권한과 책임 체계와 매우 유사하여 기업의 권한체계를 모델링하는데 매우 유용하다. 역할 계층 관계는 수학적으로 반사적(reflexive), 반대칭적(anti-symmetric), 이행적(transitive) 관계이며 도식화된 역할 계층 사이에는 사이클이 존재하지 않는다. 접근 권한(permission)은 정보 객체에 대해 수행 가능한 접근 모드들의 집합으로 구성된다. 허가 정보, 접근 권한, 특권 등이 권한과 같은 의미로 사용된다. 일반적으로 권한은 권한이 적용되는 자원의 특성에 따라 달라진다. 파일 등의 자원에는 읽기, 쓰기, 실행 등의 권한이 적용되지만, 데이터베이스에서는 테이블, 튜플, 속성 등의 자원에 적용되는 권한은 select, update, insert, delete 등으로 두 환경 사이에 사용되는 권한의 종류와 의미에 차이가 있다. 역할 기반 접근 제어 모델에서는 다른 접근 통제 정책에서 사용되는 읽기, 쓰기, 실행 등 운영체제에서 지원하는 저수준의 권한대신 입금, 출금 등 트랜잭션 수준의 보다 의미 있고 추상적인 권한을 허용하여 비즈니스 환경에서의 보안 정책의 설계와 개발 과정을 용이하게 한다.

제약 조건은 정의된 모든 구성요소들에 대하여 적용될 수 있으며, 각 구성 요소가 가지는 특성을 제한 사항이나 조건 등으로 기술한다. 제약 조건의 예로서, 각 구성 요소간의 매핑에 적용되는 일종의 제한(restriction)으로서 3 가지의 원리를 지원한다. 임무 분리(separation of duty)는 정보의 무결성을 침해하는 사기 행위나 부정 수단을 유발 할 수 있는 작업은 상호 감시적인 역할에 할당하여 임무를 분리시켜 수행하는 것이다. 최소 권한의 원칙(least privilege principle)은 조직 구조상의 상위 직위자가 하위 직위자의 모든 권한을 다 행사하도록 하는 것이 아니라, 자신의 직위에 부여된 업무 수행을 위해서 꼭 필요한 최소한의 권한만을 역할에 할당하는 정책이다. 데이터 추상화(data abstraction)는 전형적인 운영체제나 응용 시스템에서 데이터를 처리하기 위해 사용되어졌던 read, write, execute 등의 연산대신 다영한 기능을 수행할 수 있고 명령어를 추상화시키는 비즈니스 처리 명령 credit, debit, transfer 등을 지원한다.

2.2 컨텍스트와 컨텍스트 인식

컨텍스트는 장소, 사람이나 사물들을 구별 짓는 특징인 아이덴티티(identity), 사람이나 사물들을 포함하는 환경의 변화 등으로 설명한다[2,14]. Dey는 컨텍스트를 사용자가 속해 있는 환경 내에서 사용자의 감정적인 상태, 주의력, 위치와 방향, 날짜와 시간, 사람과 사물 등으로 정의한다[2]. 컨텍스트 종류의 분류는 응용 설계자가 컨텍스트들을 쉽게 발견할 수 있게 하며, 다음과 같다[15].

- 컴퓨팅 컨텍스트 : 네트워크 연결, 통신 대역폭, 프린터, 화면, 워크스테이션
- 사용자 컨텍스트 : 사용자 프로파일, 위치, 근처의 사람, 현재 사회적 상태
- 물리적 컨텍스트 : 빛, 소음 정도, 교통상태, 온도 등
- 시간 컨텍스트 : 시간, 일, 주, 월과 같은 시간

컨텍스트 인식이란 어떤 이벤트가 발생하거나 어떤 행위를 하고자 할때 주위의 다양한 환경 요소를 고려하여 다음에 취해야할 행동이 능동적으로 결정되는 것을 말한다. 유비쿼터스 환경에서는 사용자의 입력에 대해 사용자의 상태, 물리적 환경, 컴퓨팅 자원 상태 등의 컨텍스트 정보들이 다양하고, 이 컨텍스트 정보가 자주 변경되는 특징을 갖고 있으므로 사용자의 컨텍스트에 맞는 각각 다른 행동 결과 값을 제공한다. 따라서 컨텍스트 인식 응용은 어떠한 사건이 발생했을 때 시간, 날씨, 온도 등의 컨텍스트를 참조하여 적절할 행위를 수행한다. 컨텍스트 인식 응용이 지원할 수 있는 컨텍스트 인식 특징

은 정보나 서비스들을 한 사용자에게 제공(presentation)하는 것, 서비스의 자동적인 수행, 나중의 검색을 위해 정보에 컨텍스트 태그를 붙이는 것 등의 범주가 있다.

컨텍스트를 이용하는 응용을 개발하는 것은 매우 복잡하고 환경 종속적인 일이어서 응용 개발을 위한 도구에 대한 연구들이 활발히 진행되고 있다. 대표적으로 조지아공대의 컨텍스트 툴킷은 컨텍스트 응용들이 갖고 있는 공통적인 기능들을 재사용 가능하도록 하는데 목표를 두고 있다. 이 외에도 컨텍스트 미들웨어 및 프레임워크에 대한 연구들이 진행되고 있다.

컨텍스트 모델링은 컨텍스트 정보를 이용하는 응용에서는 매우 중요한 요소이며, 컨텍스트 정보에 대한 높은 수준의 추상적 개념을 제공하기 위해 필요하다. 컨텍스트 정보의 다양함과 컨텍스트 정보가 쓰이는 도메인 또한 매우 다양하기 때문에, 컨텍스트 모델링은 여러 방법을 이용한다. 키-값(Key-Value) 모델, 마크업 스키마(Markup Scheme) 모델, 논리 기반 모델, 온톨로지 기반 모델등이 있다[14].

III. 컨텍스트 정보를 이용한 역할 기반 접근 제어

유비쿼터스 컴퓨팅 환경에서 사용자는 시간과 공간의 제약을 받지 않고 원하는 정보를 제공 받을 수 있지만, 이는 사용자가 원하는 모든 정보가 제공되는 것에 따라 정보의 기밀성에 문제를 초래한다. 따라서 유연한 정보 접근과 보안이라는 상반되는 요구 사항을 만족시킬 수 있는 접근 제어가 필요하다.

따라서 정보의 보안 수준에 따른 정보의 접근 제어를 위해서는 접근 권한이 있는 사용자일지라도 사용자의 컨텍스트에 따라 접근 가능한 정보가 제한되어야 한다. 이는 단순히 사용자의 역할에 따라 정보의 접근을 제어하는 기법으로는 사용자의 컨텍스트에 따른 정보의 접근을 제어할 수 없다. 따라서, 사용자의 역할 뿐만 아니라 사용자의 컨텍스트에 따라 필요로 하는 정보에 대한 접근 제어가 필요하며, 이는 사용자의 컨텍스트를 고려한 역할 기반 접근제어 연구의 필요성이 되었다.

3.1 일반화 역할 기반 접근 제어

기존의 역할 기반 접근 제어는 시간에 따른 접근 제어 등과 같이 컨텍스트에 근거한 접근 제어를 수행할 수 없어 컨텍스트에 근거한 접근제어를 수행하기 위하여 일반화 역할 기반 접근제어(GRBAC : Generalized Role-Based Access Control)을 제안하였다. GRBAC 모델은 접근 제어 결정에 사용자 역할, 객체 역할, 환경 역할 등을 사용함으로써 기존 역할 기반 접근 제어를 확장하였다. 사용자, 객체, 환경 요소를 역할로 구조화함으로써 접근 제어 정책 기술의 단순함과 융통성을 제공한다[6,13].

예를 들어, 시간이나 위치와 같은 환경 요소를 환경 역할로 정의하여 접근 제어 정책에 기술한다면, 환경 역할로 일주일을 주중과 주말로 구분되고, 주중은 월요일부터 금요일까지이고, 주말은 토요일과 일요일이 되는 계층적 구조를 갖는다.

보안 관리자는 접근 권한 정보를 주체(subject) 역할, 객체(object) 역할, 환경(environment) 역할, 연산(operation), 부호(sign) 의 5 가지 요소로 기술한다. 예를 들어 의사의 역할을 할당 받은 사용자는 주말에 개인병력 전체를 읽을 수 없음을 다음과 같이 표현할 수 있다.

〈〈lee, medical record, weekdays, write〉, +〉
〈〈doctor, history case, weekends, read〉, -〉

GRBAC 모델은 positive permission 모델, negative permission 모델, mixed permission 모델 등을 사용한다. positive 모델은 허용 권한만이 정책에 기술되며, negative 모델은 거부 권한만이 정책에 기술되는 것이고, mixed 모델은 두 가지를 혼합하여 정책을 기술하는 모델이다.

역할 계층 구조에 의해 발생하는 비명시적인 권한 부여 해결을 위해 역할 계층 구조에서의 권한 상속 개념을 이용한다. 권한 상속은 3 가지 타입이 있으며, 표준(standard), 엄격(strict), 관대(lenient) 가 있다.

사용자가 객체에 대한 특정 연산의 수행을 요청하는 트랜잭션은 〈사용자, 객체, 환경, 연산〉의 구성 요소를 갖고 다음의 과정을 통해 처리된다. 트랜잭션에 기술된 사용자, 객체, 환경 역할과 각 역할의 계층 구조에서 각 역할에 대한 상위 역할들을 원소로 갖는 집합을 각 역할의 엔트리 집합이라고 한다. 이 집합에서 하나의 원소를 선택해 만든 트랜잭션을 매칭 트랜잭션이라고 한다. 접근 정책 중에서 매칭 트랜잭션이 포함된 정책을 찾는다. 요청 트랜잭션은 권한 모델과 찾은 정책을 이용하여 처리된다. 첫째, 허용 권한을 갖는 트랜잭션이 정책에 기술되지 않았다면 사용자 접근은 허용되지 않는다, 둘째, 적어도 하나의 허용 권한을 갖는 트랜잭션이 존재하고 거부 권한을 갖는 트랜잭션이 존재하지 않는다면 사용자 접근은 허용된다. 셋째, 적어도 하나의 허용 권한을 갖는 트랜잭션이 존재하고 적어도 하나의 거부 권한을 갖는 트랜잭션이 존재한다면 정책 충돌이 발생하고 접근은 허용되지 않는다.

이 모델은 컨텍스트 정보를 환경 역할로 표현하여 접근 제어를 위한 권한 정책에 기술하고 전파 규칙을 적용하여 사용자의 접근 요청을 처리한다. 그러나 접근 권한의 전파로 발생하는 권한들 사이의 충돌에 대하여 해결 방안을 제시하지 않았다. 또한 사용자가 사용자의 고려사항을 환경 역할을 정의함에 많은 계층 구조가 발생하여 관리의 어려움이 발생한다.

3.2 컨텍스트 제약사항을 사용한 역할 기반 접근 제어

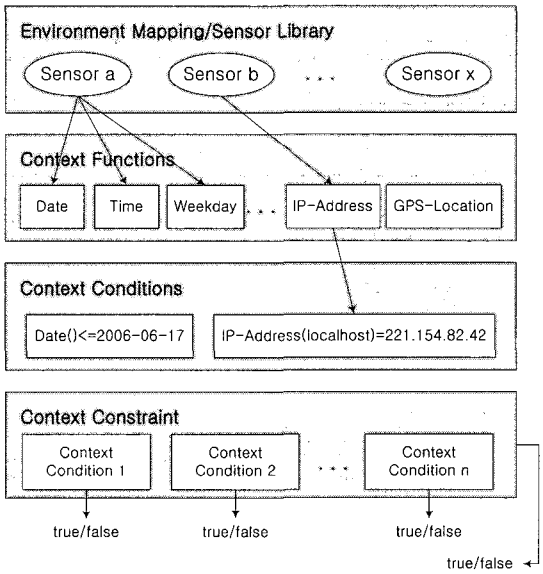
컨텍스트 제약사항을 사용한 역할 기반 접근 제어(xoRBAC)는 컨텍스트 정보를 접근제어 결정에 이용하기 위하여 역할 기반 접근 제어의 제약 사항을 사용하는 모델이다[7,13]. 컨텍스트 제약사항(context constraint)은 컨텍스트 정보 속성의 실제 값을 미리 정의된 조건과 체크하는 역할 기반 접근 제어 제약사항이다. 컨텍스트 제약사항은 특정 연산의 수행을 허용하기 위해 컨텍스트 정보 속성이 충족되어야 할 조건을 기술한다. 컨텍스트 제약사항은 속성, 함수, 조건의 튜플을 갖는다, 속성은 시간 ,요일과 같은 동적으로 변화하는 속성을 나타내거나 위치, 소유관계, 생일, 국적과 같은 객체의 인스턴스에 따라 변화하는 속성을 나타낸다.

권한 결정은 특정 주체 또는 역할이 가지는 권한에 따라 이루어짐에 따라 컨텍스트 제약 사항도 권한과 관련된다. 권한은 여러 개의 컨텍스트 제약과 관련되고 모든 컨텍스트 제약이 참 값을 가질 때 접근이 허용된다. 다음 그림 3에서 환경 매핑은 xoRBAC에 연결된 모든 센서를 관리하는 센서 라이브러리를 구성한다. 각각의 센서로부터 값을 받은 컨텍스트 정보 함수는 컨텍스트 정보 속성의 실제 값을 결정한다. 각 컨텍스트 정보 조건은 센서의 값이 제약 사항을 만족하는지 체크하여 참 또는 거짓 값을 넘겨준다. 이 값들이 모두 참일 때 접근은 허용된다.

이 모델은 컨텍스트 정보를 컨텍스트 정보 제약에 기술하고 각 권한에 대하여 컨텍스트 정보 제약을 둔다. 사용자의 접근 요청은 해당 객체에 대한 연산의 권한이 갖는 컨텍스트 정보 제약이 모두 참 값을 가질때 하용 또는 거부 된다. 따라서, 각 객체의 권한에 대하여 컨텍스트 정보 제약이 기술되므로 사용자의 컨텍스트에 따른 접근 제어를 수행하고자 할 때 최악의 경우

$$\text{사용자수} * 2^{\text{컨텍스트수}}$$

의 제약 사항 기술이 필요하다. 이것은 사용자의 접근 요청이 발생하였을 때 권한을 부여하기 위하여 컨텍스트 정보제약의 탐색과 평가 시간을 길게 하는 문제를 발생시킨다. 또한, 각 객체의 권한을 부여받기 위하여 만족되어야 할 조건을 기술하므로 컨텍스트 정보의 일반화된 정의와 구조를 사용하지 않으므로 관리의 어려움이 따른다.



【그림 3】 xoRBAC의 컨텍스트 제약사항

Ⅳ. 컨텍스트 정보 보호를 위한 역할 기반 접근 제어

유비쿼터스 컴퓨팅 환경에서 컨텍스트 정보 관리는 유비쿼터스 환경 구현에 있어 핵심적인 기술이다. 이를 위해 유비쿼터스 환경을 컨텍스트 사이에 연관 관계로 표현하는 다양한 컨텍스트 모델링 기법이 연구되고 있으며, 이러한 컨텍스트 모델을 이용하여 개발자는 필요한 컨텍스트 정보를 이용하는 응용을 개발한다.

역할 기반 접근 제어 모델은 차세대 환경에 가장 적합한 보안 모델로 평가받고 있지만, 컨텍스트 사이의 연관 관계를 나타내지 못하기 때문에 유비쿼터스 환경에 적용하기에는 한계를 나타내고 있다. 따라서 역할 기반 접근 제어 모델을 이용하여 유비쿼터스 환경에 적합한 컨텍스트 정보에 대한 접근 제어를 위한 모델이 필요하다[5,15].

4.1 컨텍스트 연관성

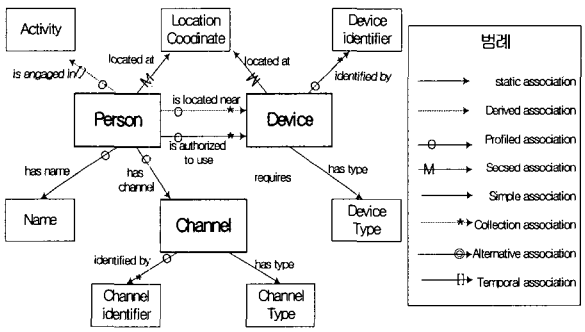
컨텍스트의 연관성은 정적 연관성과 동적 연관성으로 구분할 수 있으며, 동적 연관성은 다시 센서관련 연관성, 유도된 연관성, 프로파일 연관성 등으로 나누어진다.

정적 연관성은 연관성을 갖는 엔티티들의 유효 시간에 고정된 채로 존재하는 관계이다. 이 연관성에 의해 획득된 컨텍스트는 일반적으로 높은 신뢰도를 갖고, 장치와 채널 타입과 같은 연관성이다.

동적 연관성은 정적 연관성과 관계없는 연관성이다. 이 분류는 컨텍스트 정보의 근원에 따른 것이다. 센서와 관련된 연관

성은 하드웨어, 소프트웨어 센서로부터 획득된다. 이 정보는 센서에서 직접적으로 모델에 전달되는 것이 아니고, 응용에서 요구되는 추상적인 수준에 근접하게 변화되어 보내어지게 된다. 유도된 연관성은 단순한 수학적 계산, 복잡한 인공지능 알고리즘과 같은 다영한 영역에 걸친 유도 함수를 사용하여 다른 연관성으로부터 얻어지는 연관성이다. 이 형식의 켄텍스트는 유도 받은 정보 종류의 특성 일부를 그대로 유지한다. 예로 감지된 정보로부터 얻어지는 유도된 컨텍스트 정보는 비슷하거나 확대된 지속성과 에러 특징을 갖는다. 프로파일은 사용자에 의해 제공되는 정보로서, 가장 신뢰성이 있고 정보가 오래 유효하지만, 사용자가 정보 변경에도 불구하고 갱신하지 않는 경우 정보의 불일치성이 존재한다. 예로는 사람 이름, 사람들 간에 존재하는 상하, 협력 등의 관계와 같은 연관성들이 있다.

컨텍스트 정보는 단순하고 단일 사실에서부터 복잡한 과거 이력까지 다양하며, 이러한 구조에 따른 연관성을 분류할 수 있다. 즉, 단순 연관성과 복합 연관성으로 분리하고, 복합 연관성은 콜랙션, 대안, 시간 연관성으로 분리된다. 콜랙션은 소유 엔티티가 여러 개의 속성 값들, 여러 개의 다른 엔티티들과 연관이 있는 것을 의미한다. 많은 다른 사람들과 일을 하고, 여러 개의 통신 채널을 갖는 것이 된다. 대안은 and 연산보다는 or 연산에 의해 논리적으로 관련되는 것으로 간주될 수 있어 대신할 수 있는 가능성을 설명한다. 동일한 정보에 대해 여러 가지의 다른 방법으로 표현이 가능할 때나 두 개 이상의 컨텍스트 정보 소스가 상반되는 정보를 제공해서 각각 다른 가능성을 고려해야 할 때 유용하다. 시간 연관성은 대안 값의 집합들과 관련 있지만, 각각은 주어진 시간 간격을 갖는다. 한 시점에서 유일한 값으로 매칭하는 함수와 같은 기능을 갖는다. 이러한 연관성들을 이용하여 엔티티, 속성간의 연관성 모델의 예는 다음 그림 4와 같다.



【그림 4】 다양한 연관성 모델링의 예

컨텍스트 접근 제어 모델의 기본적인 개념은 컨텍스트 정보에 접근할 수 있는 권한을 역할에 배정하며, 사용자를 그 역할의 구성원에 소속되도록 함으로써 사용자가 그 접근 권한을 획득하도록 하는 것이다. 그러므로 사용자는 자기 권한에 맞는 컨텍스트 정보만을 접근하게 됨으로써 컨텍스트 정보의 안전한 이용을 보장할 수 있다. 또한 유비쿼터스 환경을 위한 컨텍스트 연관 관계 정보를 이용하므로 다양한 수준의 접근 통제 정책을 적용할 수 있는 시스템을 구현하기에 용이하다.

사용자는 로봇, 소프트웨어 에이전트, 컴퓨터, 사람 등이 될 수 있으며, 유비쿼터스 환경 내의 정보를 사용하는 주체이다. 권한은 하나 또는 그 이상의 보호된 컨텍스트 정보 객체에 연산을 수행할 수 있도록 승인하는 것이다. 하나의 권한은 컨텍스트 연관관계와 그 컨텍스트 연관관계 정보에 수행할 수 있는 연산의 관계로 나타낸다. 연산은 보호할 컨텍스트 연관관계 정보에 대해 수행 가능한 접근 모드를 의미하며, 읽기, 쓰기 등이다. 구현 측면에서, 관리자 이용 함수로는 사용자 추가, 삭제, 역할 추가, 삭제, 사용자 할당, 해제, 권한 승인, 제거 등이 있을 수 있다. 접근 제어 시스템에서 이용하는 함수로는 컨텍스트에 대한 사용자 연산, 컨텍스트에 대한 역할 연산, 사용자와 역할 할당 연산, 사용자와 역할 권한 연산 등이 있다.

V. 결론

유비쿼터스 컴퓨팅 환경은 언제, 어디서나, 어떤 디바이스로도 원하는 정보를 접근하여 사용할 수 있어 사람들을 편리하게 해주는 환경을 의미하며, 현재 가장 주목받고 있는 많은 기술들이 포함되어 있다. 그러나 이러한 환경에서의 사생활 침해 등과 같은 역기능에 대한 우려이며, 이러한 우려를 불식시키기 위한 정보 접근 제어 지원이 이루어지지 않는 이상 원하는 환경이 도래하기는 어려울 것이다.

이 연구에서는 가장 중요한 기본 정보 접근 제어 모델로 역할 기반 접근 제어 모델을 고찰하였으며, 이 모델을 유비쿼터스 컴퓨팅 환경에 맞게 컨텍스트 정보 활용을 위한 GRBAC과 xoRBAC 기법을 정리하였으며, 컨텍스트 정보를 보호하기 위한 중요한 방법으로 역할 기반 접근 제어 기법을 이용한 컨텍스트 정보 접근 제어 방법을 정리하였다. 이러한 정리를 컨텍스트 인식 응용을 개발하기 위한 미들웨어, 프레임워크, 툴킷 등의 연구에 기반 연구가 될 것으로 기대된다.

참고문헌

[1] J. F. Barkley, K. Beznosov, J. Uppal, "Supporting Relationships in Access Control Using Role Based Access Control", pp55-65, RBAC '99. Proceedings of the 4th ACM workshop on Rolebased access control, 1999.

[2] A.K. Dey, Providing Architectural Support for Building Context-Aware Applications", Ph.D. Thesis, Geogia Institute of Technology, 2000

[3] D. F. Ferraiolo, J. A. Cugini, D. Richard Kunj, "Role-Based Access Control(RABC) : Features and Motivations", Proceedings of the 11th Annual Computer Security Applications Conferences, pp 241-248, 1995.

[4] C.K. Georgiadis, I.Mavridis, G.Pangalos and R.K.Thomas, "Flexible Team-Based Access Control Using Contexts", ACM Symposium on Access Control Models and Technologies(SACMAT2001), pp21-30, 2001

[5] K. Henricksen,J. Indulska and A. Rakotonirainy, "Modeling Context Information in Pervasive Computing Systems", Proceeding of the First International Conference on Pervasive Computing, 2002

[6] M.J.Moyer and M. Ahamad, "Generalized Role-Based Access Control", IEEE International Conference on Distributed Comuting Systems(ICDCS2001), pp.391-398, 2001

[7] G. Neumann and M. Strembeck, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment" 8th ACM Symposium on Access Control Models and Technologies(SACMAT2003), pp.65-79, 2003

[8] R. S. Sandhu, E. J. Coyne, "Role-Based Access Control Models", IEEE Computer, 20(2), pp 38-47, 1996.

[9] R. S. Sandhu, D. Ferrraiolo and R. Kuhn, "The NIST Model for Role-Based Access Control: Towards A Unified Model Approach", ACM Workshop on Role-Based Access Control", pp.47-63, 2000
[10] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing" Comm. of the ACM, 36(7), 1993
[11] M. Wilikens, S. Feriti, A. Sanna and M.Masera, "A Context-Related Authorization and Access Control Method on RBAC : A case study from the health care domain", 7th ACM Symposium on Access Control Models and Technologies (SACMAT2002) ,pp.117-124, 2002
[12] 김영민, 이상호, "이동 에이전트를 이용한 계층적 조정 모델 기반 협력 작업 응용 개발 환경", 한국컴퓨터정보학회논문지, 제11권 제 2호, 2006.5
[13] 남승좌, 박석, "유비쿼터스 컴퓨팅 환경의 역할 기반 접근제어에서 발생하는 상황 충돌", 정보보호학회논문지, 제15권 제2호, 2005.4
[14] 이승근, 유비쿼터스 컴퓨팅 환경을 위한 온톨로지 기반 상황 인식 서비스 미들웨어, 인하대학교 박사학위논문, 2006.2
[15] 최인한, 유비쿼터스 환경을 위한 컨텍스트 접근제어 시스템의 설계 및 구현, 전남대학교 석사학위논문, 2005.2.

저 자 소 개

정 현 만

1996년 2월 서울산업대학교 전자계산공학과
2001년 2월 인하대학교 전자계산공학과 공학석사
2004년 2월 인하대학교 컴퓨터정보공학과 박사과정 수료

관심분야 상황인식, 시맨틱웹, 웹서비스, 유비쿼터스 센서네트워크

이 세 훈

1985년 2월 인하대학교 전자계산학과
1987년 2월 인하대학교 대학원 전자계산학과(이학석사)
1996년 2월 인하대학교 대학원 전자계산공학과(공학박사)
1987~1990 해병대 장교
1991~1993 (주)비트컴퓨터연구소
2001~2002 미국 NJIT 교환교수
1993년~현재 인하공업전문대학 컴퓨터시스템과 교수

관심분야 유비쿼터스 컴퓨팅, 임베디드 센서 서비스, 상황인식서비스, 웹서비스