프라이버시 보장을 위한 RBAC 기반의 접근 제어 프레임워크

홍성호[O†] 조은애[†] 문창주[*] 백두권[†]
† 고려대학교 컴퓨터학과, * 건국대학교 컴퓨터응용과학부
{shhong[O], eacho99}[†]@software.korea.ac.kr, cjmoon@kku.ac.kr[*], baikdk@korea.ac.kr[†]

RBAC-Based Access Control Framework for ensuring Privacy

Sung-Ho Hong[O†], Eun-Ae Cho[†], Chang-Joo Moon[*], Doo-Kwon Baik[†]
† Department of Computer Science and Engineering, Korea University
* Department of Computer Science, Konkuk University

요 약

이동 단말기, 무선인터넷 기술, 센서 기술의 발달로 인한 유비쿼터스 환경의 등장은 사용자의 위치에 상관없이 자유롭게 네트워크에 접속하여 다양한 서비스 이용과 정보 공유를 가능하게 하였다. 따라서 원할한 정보 공유와 서비스 이용을 위해서는 사용자에 대한 정보 보호 기술이 요구되어 진다.
또한 이런 유비쿼터스 환경에서의 프라이버시 정보는 개인의 동의 없이도 노출될 수 있으며, 제 3자에에 의해 공유되거나 또는 악용적으로도 이용될 수 있다.
이에 본 논문에서는 유비쿼터스 환경 내에서 사용자의 프라이버시를 보장하기 위해 사용자에게 프라이버시 정보에 대한 배타적인 통제권을 부여함으로써 사용자 편의성이 제공되는 개인에 의한 RBAC 기반의 접근 제어 프레임워크를 제안한다.

1. 서 론

Mark Weiser에 의해 제시된 유비쿼터스 컴퓨팅 환경은 컴퓨터나 이질성을 가지는 디바이스들이 일상생활 속에 스며들어 사용자가 인지하지 못하는 사이에도 다양한 디바이스간의 정보 교환이 가능하며, 사용자는 디바이스에 대한 거부감을 느끼지 않고도 언제, 어디서나, 사용자의 위치에 상관없이 자유롭게 네트워크에 접속하여 환경 내의 모든 데이터를 공유하거나 원하는 다양한 서비스를 제공 받을 수 있는 인간, 사물, 정보 간의 최적의 컴퓨팅 환경을 말한다[1][5].
따라서, 이런 유비쿼터스 환경에서의 개인 정보는 개인의 동의 없이도 노출되어 질 수 있으며, 누군가에 의해 공유되거나 또는 악용 되어 이용될 수도 있다.
즉, 유비쿼터스가 갖는 태생적 한계로 인해 사용자가 인지 못하는 사이에 야기 되어지는 프라이버시 침해 문제는 유비쿼터스 환경의 연구에 있어서 해결되어야 하는 직면된 문제 중 하나이다[6].
한 편, 유비쿼터스 컴퓨팅 환경에서는 다양한 상황 정보들에 따라 여러 가지 형태의 서비스들이 요청되어, 처리되어야 하기 때문에, 유비쿼터스 환경에 맞는 접근 제어 모델이 요구되어진다.
본 논문에서는 사용자에게 프라이버시 정보에 대한 배타적인 통제권을 부여함으로써, 사용자 편의성을 제공하며, 서비스 요청 시 사용자의 프라이버시 정보를 보호하고자 한다.
이를 위해 유비쿼터스 환경에서 사용자 편의성이 제공되는 RBAC 기반의 접근 제어 프레임워크를 제안하고자 한다.

2. 관련 연구

2.1 RBAC 모델

RBAC 모델은 1970년대에 개발된 온라인 시스템의 개념으로 다중 사용자, 다중 애플리케이션과 함께 시작되었다[2]. RBAC 모델에서는 역할(role)의 개념을 사용함으로써 사용자와 그들의 권한(permission)들을 효과적으로 관리할 수 있다. RBAC 모델 내에서의 권한은 역할과 관련이 있으며, 사용자들은 역할의 한 멤버가 됨으로써 권한을 배정 받게 된다. 이 기본 개념은 권한의 이해와 관리를 간편하게 해주는 장점이 있다. 그림 1은 RBAC96의 개념 모델이다[2].

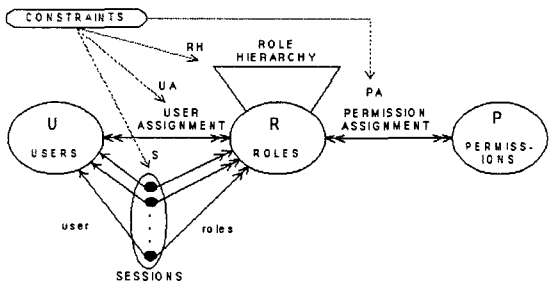

그림 1. RBAC 모델

위 개념 모델은 사용자(users: U), 역할(roles: R), 권한(permissions: P), 세션(sessions: S)의 4개의 요소를 포함한다. 역할(R)이 역할의 하나로 부여된 승인과 책임감을 고려하여 어떤 관련이 있는 의미를 가진 일의 기능이

나 일의 이름인 반면에 사용자(U)는 인간의 행동이나 자율적인 에이전트를 나타낸다. 권한(P)는 시스템에서 하나 이상의 대상(object)에 대한 접근의 특정 형태에 대한 허가이다. 또한 사용자 할당(user assignment: UA)과 권한 할당(permission assignment: PA)이 다-대-다 관계를 가지고 있는 것을 보여준다. 제약조건(constraints)은 UA와 PA에서 관찰되어야만 하는 규칙을 서술한다. 역할 계층(Role hierarchy: RH)은 역할의 계층적인 구조와 제약조건의 특정한 형식을 나타내며, 상위의 역할은 계층을 통해서 하위 역할의 권한들을 모두 가진다[3][4].

2.2 응용 RBAC 모델

기존의 역할기반 접근제어에서는 위치와 시간 등에 따른 접근 제어 등과 같이 다양한 상황 정보에 근거한 접근 제어를 수행할 수 없는 문제점을 가지고 있다.
이에 따라, 아래 SRBAC 모델과 TRBAC 모델과 같은 다양한 상황 정보를 표현하기 위한 접근제어 모델들이 제안되고 있다. 하지만 이런 모델들도 제한적인 상황 정보를 표현하는 제약으로 유비쿼터스 환경으로의 적용에 있어서 한계를 가지고 있다.

2.2.1 SRBAC : A Spatial Role-Based Access Control Model

SRBAC 모델[9]은 기존의 역할기반 접근 제어 모델에서 역할에 배정된 권한에 위치 정보를 기술하는 RBAC의 응용 모델이다. 그림 2는 SRBAC 모델에서의 위치정보를 반영하는 SOD(임무의 분리)관계를 보여준다.

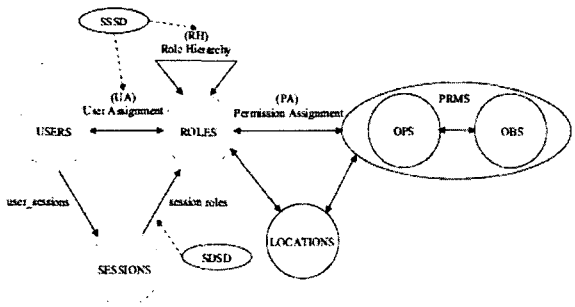

그림 2. 위치에 대한 SOD 관계

2.2.2 TRBAC : A Temporal Role-Based Access Control Model

Bertino 는 시간상의 고려를 해결하기 위하여 역할기반 접근제어 모델에 역할과 시간과의 종속성을 표현하기 위한 TRBAC 모델[8]을 제안하였다.
하지만, TRBAC 모델에서는 접근제어를 시간상의 제약사항 간의 문제로 한정하고 접근하여, 유비쿼터스 환경으로의 적용에 있어 또한 여러 제약과 표현상의 문제를 가지고 있다.

2.3 Privacy Policy

프라이버시 정책은 유비쿼터스 컴퓨팅 환경에서 프라이버시를 해결하기 위한 방법의 하나로서 제안되고 있다[7]. 유비쿼터스 컴퓨팅 환경을 반영하는 여러 항목을 설정하고 설정된 항목에 대한 세부 정책을 생성하여 사용자의 직접적인 개입으로서, 프라이버시 정보가 기술되어질 수 있다면, 프라이버시는 보장되어진다는 측면에서의 논의이다[7].

3. 접근제어 프레임워크

유비쿼터스 환경에서의 접근제어는 사용자의 상황 정보가 반영되어야 하며, 다양한 사용자의 요구에 따른 적절한 접근 제어가 수행되어야 한다.
이에 기존의 RBAC 모델을 기반으로 하는 유비쿼터스 환경에서의 프라이버시를 보장하기 위한 접근제어 프레임워크를 제안하고자 한다.

3.1 제안된 RBAC 모델

기존의 역할 기반 접근제어 모델에서는 보안 관리자에 의해서만 역할과 해당 권한을 생성, 관리할 수 있다.
이에 따라 사용자의 개입이 배제되어 사용자의 다양한 요구를 처리하는데 한계가 있으며, 사용자의 의도되지 않은 개인 정보까지 노출될 위험이 있다.
이에 보안 관리자의 권한부여 정책 작성 권한의 일부분을 사용자에게 이양하여 사용자에게 자신의 데이터 접근에 대한 통제권한을 보유하게 하여 사용자의 의도가 반영되는 그림 3과 같은 접근제어 모델을 제안한다.

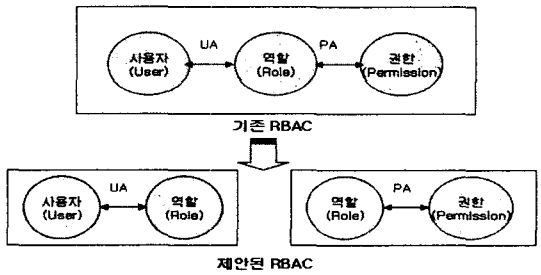

그림 3. RBAC 기반의 제안 모델

사용자 할당(user assignment: UA) 권한을 사용자에게 이양하고, 보안 관리자는 권한 할당(permission assignment: PA)을 관리하게 된다.
사용자에게 자신의 데이터에 접근을 통제하는 권한 부여 정책을 직접 작성하게 하여, 사용자 편의성이 제공되는 개인에 의한 프라이버시 데이터의 접근 제어가 가능해진다. 즉, 사용자는 서비스를 요청 시, 자신의 프라이버시 데이터가 반영된 정책을 생성하고, 사용자에 의해 생성된 정책과 보안 관리자에 의해 생성된 정책에 의해 서비스의 접근제어가 이루어진다.

3.2 프라이버시 정책 기술

유비쿼터스 환경에서의 사용자가 작성해야 하는 정책의 항목은 표 1과 같다.
이들 항목은 역할기반 접근제어 모델의 제약사항의 일부로서 보안 관리자의 권한 배정 정책과 비교되어 사용자에게 적절한 권한을 배정하게 된다.

표 1. 프라이버시 정책

정책	설명
User	사용자
Time	서비스 요청 시간 정보 (현재 시간정보)
Location	서비스 요청 위치 정보 (현재 위치정보)
Request-to	서비스 요청 대상 정보
Purpose	사용자의 서비스 요청에 대한 목적 정보
What	사용자가 요청하는 서비스
Retention Time	생성된 정책의 유효 시간

3.3 접근제어 프레임워크

논문에서 제안하는 접근제어 프레임워크는 그림 4와 같다.

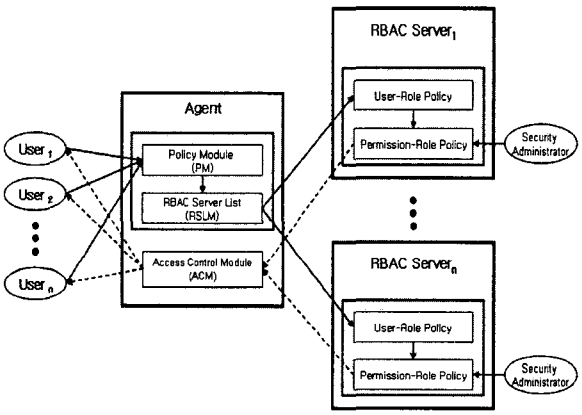

그림 4. 접근제어 프레임워크

유비쿼터스 환경 내에서의 사용자는 다양한 상황 정보를 가지면서 하나 이상의 여러 서비스를 요청하기 때문에 신뢰 할 수 있는 Agent를 통해 서비스 요청이 처리되어야 한다. 이에 Agent는 사용자의 서비스 요청을 처리할 수 있는 Policy 모듈, 실제 서비스를 처리하게 될 서버 리스트를 관리하는 RBAC Server List 모듈, 마지막으로 해당 서비스 제공자에 의해 배정된 권한을 사용자에게 전송해 주는 Access Control 모듈의 세 개의 모듈로 구성된다.

그림 4의 접근 제어 프레임워크를 이용하여 사용자 Alice가 A 회사 전산실에서 구동 중인 메인컴퓨터의 현재 온도를 점검한다고 가정하고, 시나리오를 제시해 보았다.

(1) Alice는 다음과 같은 정책 (Alice, 10:00-12:00, 성북구, 회사 A, 관리, 구동중인 메인컴퓨터의 현재 온도, Unlimited)을 작성하게 된다.
(2) 사용자에 의해 작성된 정책은 Agent 내의 정책 모듈로 보내지게 되며, RSLM 모듈에서는 Request-to 항목을 참조하여 A 회사의 RBAC 서버로 정책을 전송한다.
(3) 해당 RBAC 서버에서는 Agent에 의해 전송된 Alice의 정책을 User-Role Policy에 저장하게 된다.
(4) 보안 관리자에 의해 미리 작성된 Permission-Role Policy과 전송되어진 Alice의 정책간의 권한 부여에 의해 Alice에게 적절한 권한을 배정하게 된다.
(5) 권한 성공이 확인되면, Alice는 메인컴퓨터의 현재 온도를 Agent를 통해 모바일단말기로 전송 받게 되며, 오전 근무시간에는 해당 정보를 접근할 수 없다는 등의 제약사항으로 권한 부여가 실패한다면, 해당 요청은 거부된다.

4. 결론 및 향후 연구

본 논문에서는 사용자에게 배타적인 통제권을 부여하기 위하여 사용자에게 권한의 일부분을 이양하고 사용자 스스로가 개인의 의도가 반영된 정책을 생성하도록 UA(User Assignment)와 PA(Permission Assignment)를 기존의 RBAC 모델에서 분리하였으며, 분리된 모델을 기반으로 접근 제어를 위한 프레임워크를 제안하였다.
또한 유비쿼터스 컴퓨팅 환경에서의 개인 프라이버시를 고려하기 위해 사용자의 상황정보가 반영된 정책을 제시하였다.
향후 연구과제로서는 프라이버시 정책을 기술하는 방안에 대한 연구와 Agent내에서의 세부 모듈에 대한 보완 연구, 그리고 제안된 RBAC 모델 정의에 대한 연구를 수행하는 것이다.

5. 참고 문헌

[1] Mark Weiser, Some Computer Science Problems in Ubiquitous Computing. Communications for the ACM, July 1993.
[2] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink , Charles E. Youmank, Role-Based Access Control Models , IEEE Computer, Volume 29, Number 2, pages 38-47, February 1996.
[3] DAVID F. FERRAIOLO, Role-Based Access Control, Artech House, Computer Security, 2003, Ch1
[4] Ravi Sandhu, David Ferraiolo, Richard Kuhn, The NIST Model for Role-Base Access Control: Toward A Unified Standard, Proceedings, 5th ACM Workshop on Role Based Access Control, 2000.
[5] Mark Weiser, Ubiquitous Computing. Nikkei Electronics, pp.137-143. December 1993.
[6] Belloti, V. and Sellen, A. Design for privacy in Ubiquitous Computing Environments. Proceeding of ECSCW'93, Milan, Italy, P.77-92
[7] George Yee, Using Privacy Policies to Protect Privacy in UBICOMP, Proceeding of AINA'95, Tamkang University, Taiwan. March 28-30, 2005.
[8] E. Bertino, P.A. Bonatti, and E. Ferrari, TRBAC: A temporal role based access control model, ACM Trans. Information and System Security, vol.4, no.3, pp.191 - 223, 2001.
[9] F. Hansen and V. Oleshchuk, SRBAC: A spatial role-based access control model for mobile systems, Nordec 2003, Gjovik, Norway, 2003.