유비쿼터스 환경을 위한 Context RBAC/MAC Model

김규일*, 황현식*, 고혁진*, 신준*, 김응모*, 이혜경**
*성균관대학교 컴퓨터 공학과
**용인송담대학 컴퓨터게임 정보학과
{kisado, hjko, hhs486, crashjun, umkim}@ece.skku.ac.kr
leehk@ysc.ac.kr

Context RBAC/MAC Model for Ubiquitous Environment

Kyu-Il Kim*, Hyun-Sik Hwang*, Hyuk-Jin Ko*, Jun Shin*,
Ung-Mo Kim*, Hae-Kyung Lee**
*Dept of Computer Science, Sungkyukwan University
**Dept of Computer Game&Information, Songdam College

요 약

유비쿼터스 환경은 네트워크로 상호 연결된 디바이스들이 사용자의 상황을 인식하여 언제, 어디서나 사용자가 원하는 정보를 자동적으로 제공할 수 있는 환경을 말한다. 그러나 유비쿼터스 컴퓨팅 환경에서 시,공간의 제약 없이 정보에 접근할 수 있다는 것은 다른 환경에서보다 더 많은 보안 기술이 요구된다. 따라서 본 연구에서는 유비쿼터스 기반 하에서 개인 정보에 대해 기밀성과 무결성을 유지하면서 사용자가 원하는 정보를 자동적으로 인식할 수 있는 접근방법을 제안한다. 제안방법은 기존 RBAC에서 확장한 Context Roles를 정의하여 접근을 통제하였고 복수 정책(Multi-Policy)으로 개인 정보 및 역할 데이터 Object에 대해 제약을 두어 데이터 접근 시 상황정보에 따라 보안 등급을 지정하여 역할 정보에 대한 유출을 막는데 목적을 두었다.

1. 서론

유비쿼터스 환경(Ubiquitous Environment)은 네트워크로 상호 연결된 디바이스들이 사용자의 상황을 인식(Context-Aware)하여 언제, 어디서나 사용자가 원하는 정보를 자동적으로 제공할 수 있는 환경을 말한다[5]. 네트워크를 통해 컴퓨터 시스템과 정보 시스템들이 서로 연결되고 정보공유가 이루어지는 Pervasive Computing 환경에서 개인이 접하는 정보의 양은 계속적으로 증가하고 있으며 이에 따라 개인 프라이버시에 대한 보안 문제도 중요성이 점점 더해지고 있다[2]. 개인의 프라이버시 보호의 주 목적은 개인 정보의 보안, 무결성, 가용성을 보장하는데 있다[8]. 이러한 유비쿼터스 환경에서 기존 데이터 접근 제어 기술은 개인 제어형 데이터에 대한 보호에 적합하지 않다. 기존 접근제어 방법에서는 정책 권한이 시스템 운용 전에 미리 정적으로 정한 보안 정책에 의해 각 데이터에 대한 접근이 제어되는 방법을 취하고 있기 때문에 유비쿼터스 환경 하에서 사용될 수 있는 위치나 공간에 대한 개념은 고려되지 않고 있다.

따라서 본 연구는 유비쿼터스 환경에서의 위치와 상황을 고려한 Context RBAC/MAC Model를 제안한다.

2. 관련연구

2.1 RBAC(Role-based Access Control)

RBAC[4]는 Subject-Centric의 제약을 둠으로서 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할을 할당 받아 작업을 수행할 수 있는 능력과 특정한 역할위치(Role Hierarchies)에 지정됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있다. 하지만, RBAC는 Subject 중심이기 때문에 Object를 액세스 하기위한 다양한 Object 속성을 지원하기 못하고 역할의 위치와, 상황 등 역할 환경 상태를 판

별할 수 있는 기능을 제공하지 않는다. 또한 RBAC는 Time-Dependent한 접근제어를 지원할 수 없다. 예를 들어, 사용자는 아침 9시에서 오후 5시 사이에 오직 Object O를 액세스 할 수 있다고 한다면 기존의 RBAC에서는 시간을 고려한 속성이 없으므로 동적인 기능을 제공할 수 없다.

2.2 GRBAC(Gerneralized Role-Based Access Control)

기존의 역할기반 접근제어는 시간에 따른 접근제어 등과 같이 상황에 근거한 접근제어를 수행하기 위하여 GRBAC[7] 모델을 제안하였다. GRBAC 모델은 접근제어 결정에 사용자 역할, 객체 역할, 환경 역할을 정의함으로써 기존 역할기반 접근제어를 확장하였다. 사용자, 객체, 환경 요소를 역할로 구조화함으로써 접근제어 정책 기술의 단순함(simplicity)과 융통성(flexibility)을 제공한다. 시간이나 위치와 같은 환경 요소를 환경 역할(Environment Role)로 정의하여 접근제어 정책에 기술한다. 사용자가 객체에 대한 특정 연산의 수행을 요청하는 트랜잭션은 <사용자, 객체, 환경, 연산>의 구성요소를 갖고 접근 정책을 찾는다.

GRBAC는 기존 RBAC 모델에서 환경역할을 확장했지만, 환경역할에 대한 구조적인 정의가 미흡하다.

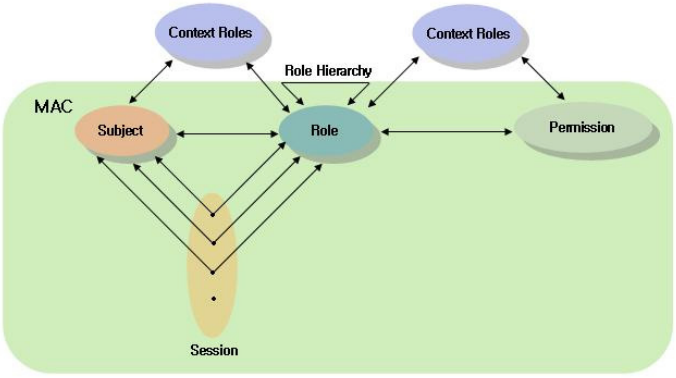
2.3 MAC(Mandatory Access Control)

각 정보에 결합된 비밀등급(Classification Level)과 사용자에게 부여된 인가등급(Clearance Level)을 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 사용자에게만 접근 권한을 부여하는 보안정책으로, 정보의 기밀성이 매우 중요시되는 환경에서 사용되고 있다. 그러나 모든 Object에 제약을 두었기 때문에 유비쿼터스 환경에서는 적합하지 않다.

3. Context RBAC/MAC Model

MAC, DAC, RBAC 등의 접근제어 정책들은 서로 배타적인 정책들이다. 즉, 어떤 조직이나 시스템에서 특정 접근제어 정책을 선택하면 다른 정책들은 수용할 수 없었다. 조직, 시스템의 복잡도와 데이터 보호에 대한 다양한 요구가 증대함에 따라 복수의 접근제어 정책을 동시에 적용할 수 있도록 하는 복수정책(Multi-Policy) 접근제어[3]에 대한 필요성이 대두되었고 연구되고 있다. 하지만 현재의 연구에서는 데이터 접근에 대한 시공간의 제약이 없는 유비쿼터스 환경에 적합한 접근제어 정책의 특정 및 요구사항이 고려되지 않고 있다. 따라서 유비쿼터스 환경에 적합한 접근제어의 연구와 이 접근제어 정책과 기존 접근제어 정책들을 융합할 수 있는 새로운 복수정책 접근제어에 대한 연구가 수행되어야 한다.

기존 RBAC에서 역할은 역할에 해당하는 모든 Object에 권한을 행사할 수 있다. 하지만 대다수의 사용자가 같은 역할을 소유하고 있을 때, 해당 역할은 대다수의 사용자에게 동일한 권한을 부여하게 된다. 이것은 다수의 사용자가 동일한 역할에 해당하면 역할에 대한 모든 정보에 접근이 가능해 진다는 의미로 해석할 수 있다. 이러한 경우, 개인프라이버시와 Object에 제약을 둘 수 없는 문제점이 발생하기 때문에 Multi Policy를 적용하여 다수의 사용자가 동일한 역할을 할당 받더라도 역할에 등급이 지정됨으로써 해당 등급에서만 데이터에 접근할 수 있도록 한다. 이 메커니즘에 Context를 적용하면 기존 RBAC에서 Context를 적용한 방법보다 효율적이고 더 강력하게 제어 할 수 있다. 따라서 (그림1)에서와 같이 인터넷 애플리케이션 및 Pervasive Computing 환경에서는 개인 현재의 상황에 대처할 수 있도록 보안 정책의 변경이 쉽고 유동적인 접근제어 CRBAC(Context Role-Based Access Control)를 제안한다.



(그림 1) Context RBAC/MAC Model

4. Context Roles

사용자의 현재 위치, 행동 및 작업 등 사용자에 대한 상황정보를 컨텍스트(Context)라 한다[6]. 센서, RFID의 디바이스를 통해 사용자 환경을 지속적으로 모니터링하고 이로부터 유익한 Context 정보를 획득한 다음 획득한 컨텍스트 정보를 기반으로 사용자에게 효율적인 서비스를 능동적으로 제공하는 것을 목적으로 하고 있다. Context를 접근제어에 적용하기

위하여 이 절에서는 context, context type, context expression를 정의한다.

Definition1. *(Context) 주체의 상황정보 (ex. Location, Time, Action, etc.) 상황정보(CI)는 CI = {c_1, c_2, c_3, c_4,...c_m}이고 상황정보 cm 원소는 cm∈ CI 에 속한다.*

컨텍스트는 위치, 시간, 날씨, 환율, 건강, 스케줄, 이메일, 사회활동 등 각기 다른 타입으로 나눌 수 있는데 컨텍스트 타입을 다음과 같이 정의 한다.

Definition2. *(Context Type) 컨텍스트 타입(CT)은 한 쌍의 CT=(ct_id, attribute) 표현하고 애트리뷰트는 다시 CTA=[attr_name, attr_domain, a_value) 3개의 요소로 구성할 수 있다.*

Example1. 컨텍스트 타입을 예를 다음과 같이 나타낼 수 있다.
[Location, (위치, String, 천천동 연구실)]
[Time, (시간, Integer, 09:00)]
[Environment (날씨, String, 맑음)]

컨텍스트 연산은 conjunction, disjunction, negation의 연산으로 나타내고 표현은 다음과 같다.

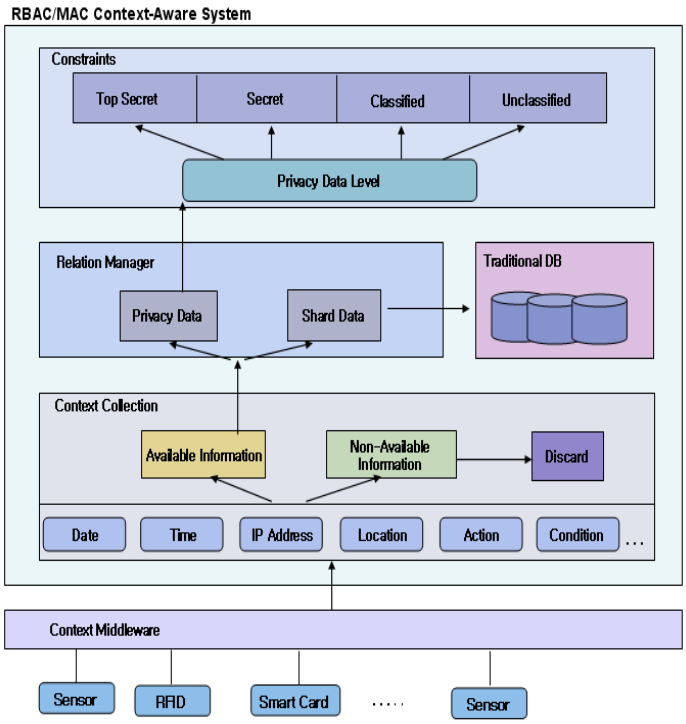
Definition3. *(Context Expression) 컨텍스트 표현은 합집합, 교집합, 부정으로 나타내고 user_id은 전체 사용자 집합 user_id∈U 속한다. user_id($CT_i \wedge CT_j$), user_id($CT_i \vee CT_j$), user_id$\neg$($CT_i \wedge CT_j$) 으로 정의한다.*

Example2. 컨텍스트 표현은 다음과 같이 나타낸다.
철수[Location(위치, String, 집)∧Environment(온도, float, 35)∨Information(동작, String, TV시청)]

5. Context Roles Architecture

현재 사용자의 상황 정보를 가지고 해당 주체가 필요한 데이터를 얻을 수 있도록 Context Roles를 설계한다.

(그림2)에서 Context 미들웨어 기반으로 사용자의 위치와 상황 정보를 수집하기 위해 센서, RFID, Smart Card 등으로 정보를 수집한다. Environment Device에 의해 정보를 수집한 Date, Time, IP Address, Location, Action 등의 자료를 필터링하여 필요한 데이터와 불필요한 데이터를 구분하여 Context Collection에서 분리한다. uT Relation Manager는 분리한 정보에 대해서 역할에 의해 부여되는 Privacy 정보와 Non-Privacy 정보를 분류한다. 분류한 Privacy 정보를 분석하여 만약 사용자가 현재 상황에 Privacy 정보를 요청했을 경우 역할에 대한 기밀성과 프라이버시 보호를 위해 접근제약 조건을 가지고, 사용자가 Non-Privacy 정보를 요구 했을 경우, 제약을 거치지 않고 전통적인 DB 접근방법을 이용하여 정보를 제공한다.



(그림 2) Context RBAC/MAC Architecture

6. RBAC/MAC Context-Aware 정책

Context RBAC/MAC 접근제어 환경은 세 개의 파라미터 <S,O,P,C> : 주체(S), 객체(O), 역할인가(P), 현재 컨텍스트(C)로 구성된다. 인가된 각 주체[1]는 세션의 의해 주체에 맞는 역할에 매핑 된다. 역할인가(P)는 시스템에서 각 역할의 해당하는 특정 연산으로 하나 또는 그 이상의 데이터를 엑세스하는 것을 말한다. 객체(O)는 시스템에서의 데이터 자원으로 역할은 반드시 제약조건의해 필요한 자원을 접근 할 수 있다. 컨텍스트는 (정의1)과 같이 주체의 상황 정보를 뜻한다.

한 예로 주체는 현재 필요한 정보를 획득하기 위

해 시스템으로부터 <S,O,P,C>를 요청한다. 제안시스템은 주체에게 적합한 역할을 부여하고 요청한 데이터를 분석하여 역할 공유권한인지 역할 개인권한인지 판별한다. 만약 요청한 데이터가 공유권한에 속한다면 전통적인 RBAC정책으로 접근제어를 수행하고 반대로 개인권한의 데이터이면 프라이버시 보안 레벨의 제약을 거친다. (그림3)은 제안모델 Context RBAC/MAC의 알고리즘이다.

```
Algorithm: Context RBAC/MAC Algorithm

INPUT: Query <S, O, P, C>
OUTPUT: Decision d {Accept, Deny, N/A}

Let CR/M returned by function evaluate query <S,O,P,C>
For ∀u ∈ CU (Set of Credentials type)
  //A set of roles can be activated for a user
  If ∀cu → 2^R then (u, r∈C)
  // Role Assign
  Create set Role(URA=<UR,O,MACC,CC>
    //Privacy decision
     If ∃query ∈RA then (Set of Role Authorization)
       //Shard decision
        Else Create set Shard Permission(p)
         //MACC S-Level Check
           If UR^CLR > O^CLS then
             //Context and Permission Check
              If PA⊆P×R×2^CR then
                Create set Privacy Permission(p)
   Else Initialize
```

7. 결론

본 연구에서는 유비쿼터스 환경 기반 하에서 개인 정보에 대한 기밀성과 무결성을 유지하는 Context RBAC/MAC 접근제어 기법을 제안하였다. 기존 모델에서는 유비쿼터스 환경에서 개인에 대한 정책측면을 고려하지 않은 반면, 제안 모델은 개인 프라이버시 측면과 공통의 Non-Privacy 측면을 고려하여 개인 정보에 대해선 정보의 노출을 막기 위해 Object에 제약 사항을 두었고 Non-Privacy에 대해 유비쿼터스 환경의 유동적인 측면을 고려하여 사용자가가 요구한 정보를 바로 제공할 수 있는 방법을 제시하였다.

앞으로 유비쿼터스에서 발생할 수 있는 의무분리(SOD), 충돌발생, 사용자의 데이터를 수집하는 Context 자체 보안 문제 등에 연구가 이루어져야 하겠다.

참고문헌

[1] N.R. Adam, V.Atluri, E.Bertino, and E.Ferrari. "A Content-Based Authorization Model for Digital Libraries". IEEE Transactions on Knowledge and Data Engineering (2002) 103-112

[2] Elisa Bertino, Ravi Sandhu. "Database Security-Concept, Approaches, and Challenges". IEEE Transaction vol.2, no.1 (2005) 2-19

[3] Charles E. Phillips, Stenen A.Demurjian. "Security Assurance For an RBAC/MAC security Model", Proceeding of the IEEE, Workshop on Information Assurance N.Y(2003) 260-267

[4] Gustavo H.M.B.Motta, Sergio S.Furuie "A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record". IEEE Transactions on Information Technology in Biomedicine Vol.7 No.3 (2003) 202-207

[5] X.Jinag, J.Hong and J.Landay "Approzimate Information Flow:Socially Based Modeling of Privacy in Ubiquitous Computing". To be published in proceeding. Ubiquitous Computing, Springer-Verlag, Berlin(2002)

[6] Gustaf Neumann, Mark Strembeck "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment", Proceeding of the eighth ACM symposium on Access control models and technologies.(2003)

[7] Matthew J.Moyer, Mustaque Ahamad "Generalized Role-Based Access Control", Distributed Computing System, Proceeding of the IEEE 21st International Conference. (2001)391-398

[8] Apu Kapadia, Geetanjali Sampemance, and Roy H.Campbell, "KNOW Why Your Access Was Denied", Proceedings of the 11th ACM Conference on Computer and Communication. (2004)