情報保護學會論文誌
第18卷 第5號, 2008. 10

유비쿼터스 컴퓨팅 환경을 위한 보안통제가 강화된 접근제어 시스템 설계에 관한 연구*

엄 정 호†, 박 선 호, 정 태 명
성균관대학교 정보통신공학부

A Study on Architecture of Access Control System with Enforced Security Control for Ubiquitous Computing Environment*

Jung-Ho Eom†, Seon-Ho Park, Tai-Myoung Chung
Sungkyunkwan University, School of Information & Communication Engineering

요 약

본 논문에서는 유비쿼터스 컴퓨팅 환경 하에 각종 정보시스템에 대한 접근을 효율적으로 제어하고 불법적인 접근을 차단하기 위하여 상황인식 기술 및 직무-역할 기반의 접근제어 시스템(CAT-RACS)을 설계하였다. CAT-RACS은 상황정보에 따른 정책 구성을 수행할 수 있도록 상황-역할 개념과 정보의 기밀성을 유지시키기 위해 보안등급 속성을 추가한 접근제어 모델(CA-TRBAC)을 적용하였다. CA-TRBAC는 사용자의 직무와 역할이 접근제어 조건에 합당할지라도 상황이 접근제어 조건에 부합하지 않거나, 역할과 직무가 접근하려는 객체의 보안등급과 일치하지 않거나 하위 등급일 경우에는 접근을 허가하지 않는다. CAT-RACS는 상황인식 보안 매니저를 통해 사용자 인증과 접근제어 등의 보안 서비스를 제공하며, 상황정보 융합 매니저를 통해 상황인식 보안 서비스 제공과 보안정책 구성에 필요한 상황정보를 관리한다. 또한, 보안정책 매니저를 통해 CA-TRBAC 정책, 사용자 인증 정책, 보안 도메인 관리 정책을 관리한다.

ABSTRACT

In the paper, we designed a context aware task-role based access control system(CAT-RACS) which can control access and prevent illegal access efficiently for various information systems in ubiquitous computing environment. CAT-RACS applied CA-TRBAC, which adds context-role concept tor achieve policy composition by context information and security level attribute to be kept confidentiality of information. CA-TRBAC doesn't permit access when context isn't coincident with access control conditions, or role and task's security level aren't accord with object's security level or their level is a lower level, even if user's role and task are coincident with access control conditions. It provides security services of user authentication and access control, etc. by a context-aware security manager, and provides context-aware security services and manages context information needed in security policy configuration by a context information fusion manager. Also, it manages CA-TRBAC policy, user authentication policy, and security domain management policy by a security policy manager.

Keywords : ubiquitous computing security, access control, context aware task-role based access control system

Ⅰ. 서 론

무선 통신 및 컴퓨팅 기술의 발전에 따라 IT 환경은 유비쿼터스 컴퓨팅 환경으로 진화하고 있다. 유비쿼터스 컴퓨팅 환경을 구축하는데 필수적인 기술 중 하나는 상황인식 기술이다. 상황인식 기술은 다양한 상황 정보들을 바탕으로 지능적이고 자동화된 서비스를 제공할 수 있다[1].

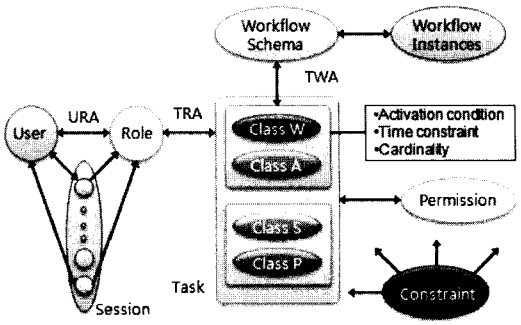
이러한 상황인식 기술을 기반으로 하는 유비쿼터스 컴퓨팅 환경에서는 기존의 보안 기술과는 다른 관점으로 보안 정책과 모델을 구축해야 한다. 특히 접근제어 모델의 경우 기존에는 단순히 접근제어 주체의 관점에서 정책을 부여하고 접근제어를 수행하는 경우가 대다수이어서 상황 정보에 따라 서비스가 제공되는 유비쿼터스 컴퓨팅 환경에는 적합하지 않은 단점을 갖는다. 상황인식 시스템을 위한 접근제어 정책은 상황정보를 기반으로 하여 시스템에 대한 접근을 제어할 수 있어야 하며, 수시로 변하는 상황정보를 보안 서비스에 실시간으로 적용할 수 있어야 한다 [3-6]. 또한, 소통되는 정보의 유출을 방지하기 위해서 정보의 기밀성을 보장해야 한다.

본 논문은 상황정보 기반으로 사용자의 직무와 역할을 적용하여 접근제어를 수행할 수 있는 새로운 접근제어 메커니즘인 상황과 직무-역할 기반의 접근제어 메커니즘(CA-TRBAC : Context Aware-Task Role Based Access Control)을 소개한다. 그리고 CA-TRBAC을 기반으로 한 상황인식 직무-역할 접근제어 시스템을 설명한다. 2장에서는 관련연구를 소개하고, 3장에서는 CA-TRBAC 모델을 서술한다. 4장에서는 CAT-RACS의 설계를 설명하고 5장에서는 정성적 비교평가를 수행한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 T-RBAC

태스크-역할기반 접근제어 (T-RBAC : Task-Role-Based Access Control) [9][10]는 RBAC 모델을 기반으로 사업 환경의 특성을 반영하여 태스크-역할에 권한을 할당하여 접근을 통제하는 모델로 구성은 [그림 1]과 같다. 태스크는 사업 환경에서 직위와 사업 역할을 포함하는 조직 구조와 사업 프로세스의 특성에 따라 분류되며, 권한 할당의 기준이 된다. 그래서 T-RBAC은 사업 환경의 특성들을 고려하여 접근제어 요구들을 수용한다. T-RBAC에서 사용되는 태스크의 종류는 [표 1]과 같다.



〔그림 1〕 T-RBAC 모델

〔표 1〕 태스크 분류

분 류	특 성	설 명
클래스 P	사적 (private)	상속불가, 수동적 접근 예) 분석, 계획, 결정
클래스 S	감독 (supervision)	상속가능, 수동적 접근 예) 검토, 감사, 감시, 승인
클래스 W	워크플로우 지향(workflow)	상속불가, 능동적 접근 예) 워크플로우 내 태스크
클래스 A	행위 승인 (approval)	상속가능, 능동적 접근 예) 워크플로우 내 승인 태스크

T-RBAC는 RBAC의 역할계층 대신에 감독 역할계층(S-RH : Supervision Role Hierarchy)을 사용한다. S-RH에서 역할 계층선상에서 상위 역할은 하위 역할의 모든 접근권한을 상속받지는 않는다. 클래스 S나 클래스 A에 속한 접근 권한만이 역할 계층선상의 하위 역할에서 상위 역할로 상속된다. 감독 역할계층을 사용함으로써 최소 권한 규칙이 위배되는 문제를 해결한다.

T-RBAC의 작동 절차는 사용자가 특정 역할에 할당되고, 직무는 수행하는 업무 기능을 고려하여 가장 적합한 역할에 할당되며 여러 직무들의 집합이 하나에 역할에 할당될 수도 있다. 직무는 위에서 설명한 바와 같이 4가지로 구분되며, 이중 'Class W'에 속하는 직무는 3가지 속성인 활성화 조건, 시간 제약, 최대 활성화 직무

접수일 : 2008년 2월 5일; 수정일 : 2008년 6월 12일;
채택일 : 2008년 8월 24일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0028)
† 주저자, eomhun@gmail.com

개수를 준수해야 된다. 객체는 직무에 따라서 접근 가능한 객체로 구분하여 직무에 할당한다. 다음으로 직무에 권한이 할당되는데 여기서는 '쓰기, 읽기, 실행' 등의 기능을 부여할 수 있다. 사용자-역할, 직무-역할, 권한-직무의 할당 완료되면 세션을 생성하여 접근을 허가하게 된다.

2.2 상황 인식 컴퓨팅

유비쿼터스 컴퓨팅 환경의 기반이 되는 기술은 상황 인식이다. 상황 인식은 사용자의 작업과 관련 있는 적절한 정보 또는 서비스를 사용자에게 제공하는 과정에서 상황을 사용하는 기술을 의미한다. 상황은 실세계에 존재하는 실체의 상태를 특징적으로 정의한 정보로 인간, 장소 또는 인간과 서비스간의 상호작용을 의미한다[11].

GeorgiaTech의 Context Toolkit [12]은 상황인식 어플리케이션 제작을 용이하도록 하기 위해 개발된 상황정보 수집 도구이다. Context Toolkit은 수집한 상황정보를 어플리케이션의 특징에 맞게 가공하여 어플리케이션에 제공한다. Widget, Aggregator, Interpreter의 3가지 오브젝트를 포함하는 객체 지향적 구성 특징을 갖으며, 구성은 다음과 같다.

- Widget : 어플리케이션과 운영 환경간의 중계를 담당하며, 어플리케이션이 상황정보에 접근할 수 있게 한다. 또한 어플리케이션에게 상황정보 수집 메커니즘의 내용을 숨기고 어플리케이션의 요구에 맞춰 상황정보를 추상화한다.
- Aggregator : Widget의 모든 기능을 가지면서 동시에 실제 개체들의 상황정보들을 병합한다. 또한 어플리케이션들과 기본 Widget들 간의 게이트웨이와 같은 역할을 수행한다.
- Interpreter : 저 수준 상황정보를 고 수준으로 추상화하거나 해석한다. 즉, 다른 표현 형식을 갖는 상황정보들을 통일하기 위해 정보의 번역 기능을 수행하거나 다른 상황정보들 간의 결합 등과 같은 기능을 제공한다.

Context Toolkit은 분산 구성 특징으로 상황 인식 어플리케이션에 투명성을 제공해 준다. 따라서 어플리케이션들은 Context Toolkit 구성 요소들이 원격에서 실행되는지 내부에서 실행되는지 알 필요가 없다. 이러한 투명성은 Context Toolkit의 구성 요소가 HTTP 상에서 XML을 이용하여 통신하기 때문에 가능하다.

Ⅲ. CA-TRBAC

상황 인식-직무/역할기반 접근제어(CA-TRBAC : Context Aware - Task Role Based Access Control)는 유비쿼터스 컴퓨팅 환경에서 T-RBAC 모델을 기반으로 상황 인식 메커니즘과 보안등급 속성을 추가하여 보안정책을 구성하고 접근제어를 수행한다[13].

3.1 CA-TRBAC의 요구사항

접근제어 관점에서 유비쿼터스 컴퓨팅 환경은 일반적인 네트워크 환경과는 몇 가지 다른 특성을 지니고 있기 때문에 보다 강화된 보안통제 요구사항을 도출해야 한다.

첫째, 유비쿼터스 컴퓨팅 환경에서는 상황인식 메커니즘을 사용하기 때문에 상황정보 요소를 반드시 반영해야 한다. 일반 네트워크 환경에서 유비쿼터스 컴퓨팅 환경으로 전환하고 있기 때문에 보안정책도 개선되어야 한다. 특히, 유비쿼터스 컴퓨팅 환경에서는 사용자가 언제 어디서든지 정보시스템에 접근할 수 있고 역동적으로 상황이 변화하기 때문에 각종 센서들로부터 수집한 상황정보에 따라 동적인 접근제어 메커니즘을 적용해야 한다.

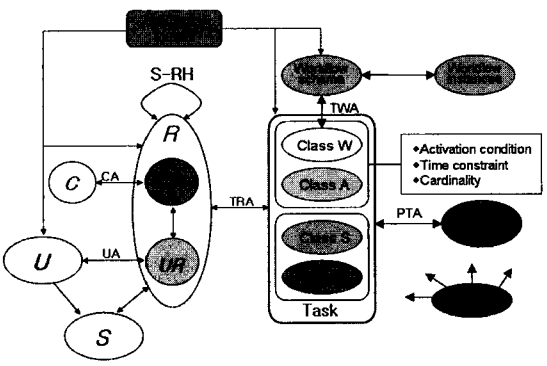
둘째, 정보의 기밀성을 보장해야 한다. 소통되거나 저장되어 있는 내용의 중요도에 따라 각각의 객체에는 보안등급이 설정되어 있다. 이러한 객체들 간에 서로 다른 등급의 객체로 정보가 흘러가지 말아야 하며, 다른 등급을 갖는 사용자도 접근할 수 없도록 해야 한다. 또한, 하나의 직무를 통하여 여러 개의 객체에 접근할 때에도 다른 보안등급의 객체간의 정보의 흐름이 발생해서는 안 된다.

마지막으로 유비쿼터스 컴퓨팅 환경에서 수행되는 업무는 주로 워크플로우 형태의 직무들이다. 예를 들면, 자료수집-자료분석-보고서 작성-보고서 승인-보고서 전파 등이 있다. 이러한 직무들은 정보의 적시성이 중요하기 때문에 작업 과정에 초점을 두어 작업흐름을 관리하는 워크플로우 관리 시스템(WFMS : Workflow Management System)의 기능이 요구된다.

3.2 CA-TRBAC의 구성

CA-TRBAC은 기본적인 T-RBAC의 구성요소와 관계들을 포함한다. 여기서는 T-RBAC의 구성 [9][10]에 포함되어 있는 요소는 생략하고 새로 추가된 요소만 설명할 것이다. CA-TRBAC의 구성은 [그림 2]와 같다.

- C (Contexts) : 관리 도메인 내부의 상황정보들을0 표현한다. 상황정보는 사용자의 위치, 시간, 시스템 CPU 사용량 등 다양한 형태를 갖는다. C는 상황정보들의 집합이다.
- CR (Contexts-Roles) : CA-TRBAC 관리 도메인 내의 모든 상황정보들 중 보안에 관련된 정보들을 추상화시킨 개념으로 상황정보의 형태에 따라 다양한 상황-역할이 존재한다. CR은 상황-역할들의 집합이다.
- CA(Context Assignment) : 상황-역할과 상황정보 간의 매핑 관계를 나타낸다.
- $CA \subseteq C \times CR$: 상황정보와 상황-역할 간의 다대다 할당관계를 나타낸다.
- $R \subseteq UR(User-Role) \times CR$: 사용자-역할과 상황-역할 간의 할당관계인 역할을 나타낸다.
- $PTA(Permission\,Task\,Assignment) \subseteq P(Permission) \times T(Task)$: 권한과 직무 간의 다대다 할당관계를 나타낸다. 권한은 정보 객체와 접근 모드의 한 쌍으로 정의된다.
  $P = \{o \in Object, < read \text{ or } write > \in Mode | (o, read)\}$
  : 객체 o에 읽기 권한이 부여된다는 의미이다.



〔그림 2〕 CA-TRBAC 모델

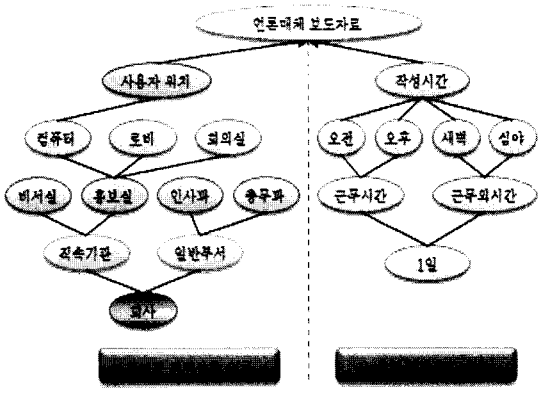
3.2.1 상황-역할

상황정보는 개체(entity)의 상태를 특징짓기 위해 사용될 수 있는 정보들을 의미한다. 상황정보는 사용자의 ID, 활동, 자원의 가용성 및 상태, 일시적 시간 등의 논리적 상황정보와 사용자의 지리적 위치, 주위 환경 등은 물리적 상황정보로 분류된다. 상황정보는 어플리케이션이나 시스템에 종속되어 해당 어플리케이션이나 시스템에 적합한 상황정보 요소들을 정의하여 보안정책에 사용해야 한다.

상황-역할은 다양한 상황정보들을 추상화하여 정책 구성 및 관리에 효율적으로 이용할 수 있도록 해준다. 상황-역할 계층을 구성하는 위치관련 상황정보를 추상화한 물리적 상황-역할과 시간관련 상황정보를 추상화한 논리적 상황-역할의 예는 [그림 3]과 같다.

위치관련 상황-역할에서 컴퓨터는 객체로서 다루어진 것이 아니라 각 객체가 있는 위치관련 상황정보를 상황-역할로 추상화한 것이다. 이러한 방식은 객체들의 위치 변동이 자주 발생하기 때문에 절대적인 좌표 등을 이용한 수치를 이용할 경우 보안정책의 빈번한 수정을 방지하기 위함이다.

상황-역할의 계층화는 일반적인 역할 계층화와 유사하게 상속의 특징을 갖지만 한 가지 큰 차이점을 갖는다. RBAC에서의 역할 계층 트리에서는 상위 쪽일수록 권한의 강도가 강하지만, 상황-역할의 경우 계층 트리의 구성과 권한의 강도 간의 관계가 없다. 이것은 정책 구성 시에 상황-역할에 권한이 할당되는 것이라 아니라 사용자가 어떤 직무를 수행하기 위한 상황 적합 여부만을 판단하기 때문이다.



〔그림 3〕 상황-역할 계층 구성의 예

3.2.2 보안 등급

보안등급(SL : Security Level)은 유비쿼터스 컴퓨팅 환경에서의 사용자, 역할, 직무, 객체가 하나의 속성으로 가지고 있으며, 임의로 변경할 수 없다. 등급은 "Top Secret (TS)", "Secret(S)", "Confidential(C)", "Unclassified(U)"의 집합이며, $SL = \{TS, S, C, U\}$로 표현되며 상속이 가능하며 상속관계는 다음과 같이 표현한다.

$$SL_1, SL_2 \in SL, \quad SL_1 > SL_2, \quad \forall SL_i \in SL_2 \Rightarrow SL_1 inherits \{SL_i\} \qquad (1)$$

CA-TRBAC 모델에서 보안등급 속성의 제약사항을 설정함으로써 정보의 기밀성 파괴를 방지할 수 있다. 정보의 기밀성 파괴는 하위 보안등급의 사용자가 상위등급의 객체에 접근을 시도할 때 발생한다. 즉, 객체가 상위 보안등급에서 하위등급으로 전송될 때 발생된다. 보안등급은 사용자가 객체에 대한 접근을 허용하는 수준을 나타내므로 상위 보안등급의 객체가 하위등급의 사용자에게 노출되면 비밀이 유출되기 때문에 기밀성이 파괴된다. 구체적으로 하위 보안등급의 사용자가 상위등급의 객체에 "read" 접근하거나, 상위 보안등급의 사용자가 하위등급의 객체에 "write" 접근하거나, 하위 보안등급의 사용자가 상위등급의 객체에 "write" 접근할 경우에 발생한다. CA-TRBAC에서는 접근 모드가 "read"일 경우, 사용자가 최종적으로 접근하는 객체의 등급이 사용자의 등급보다 낮거나 같게 설정하고, 접근 모드가 "write"일 경우, 사용자의 등급과 같게 설정함으로써 정보의 기밀성을 유지한다.

3.3 CA-TRBAC의 접근제어 정책

CA-TRBAC은 접근제어의 대상이 되는 개체들 즉, 역할과 이들 역할들의 집합이 접근제어 개체가 된다. 또한, 사용자-역할을 제한하는 제약사항과 사용자, 역할, 직무, 객체들의 보안등급 속성에 따른 접근권한을 상황-역할에 따라서 결정하는 하나의 단위를 구성한다. 그리고 이 단위가 내포하는 접근동작에 대해 허가 또는 불허함으로써 접근을 제어한다. 각 역할들과 접근동작을 포함하여 접근 권한 부과대상이 되는 단위는 트랜잭션(Transaction, Tran)이다. 트랜잭션은 사용자-역할(U-R), 직무(T), 상황-역할(CR), 퍼미션(P)의 집합이다. CA-TRBAC의 접근제어 정책 형식은 [표 2]와 같다.

〔표 2〕 CA-TRBAC의 접근제어 정책 형식

- Transaction : Tran

  $Tran = \langle UR, CR, T, P \rangle$

  *트랜잭션은 사용자-역할이 상황-역할에 해당하는 상황 조건에서 해당 직무를 위한 퍼미션을 수행하는 것.

- Permission Bit : PB

  PB는 Boolean 형 값을 갖는 1bit 크기를 갖는 변수이다. 허가 및 불허는 각각 "+"와 "-"으로 표현.

  $P = \{+, -\}$

CA-TRBAC은 트랜잭션(Tran)과 권한비트(PB)를 인자로 갖는다.

$P = \langle Tran, P \rangle, \quad P = \langle \langle UR, CR, T, P \rangle, PB \rangle$

접근제어 정책은 트랜잭션에 대한 허가 혹은 불허를 나타내는 권한 비트(Permission Bit, PB)가 추가된 형식이다. 다시 말해서, 어떤 사용자-역할이 임의의 직무에 대해 특정 상황-역할 하에서 수행하는 접근동작에 대한 허가 혹은 불허를 결정하는 규칙이다. 사용자-역할은 접근동작을 수행하는 주체 역할 속성을 의미하며, 직무는 사용자-역할이 수행하는 작업으로 접근 권한을 부여받는다. 상황-역할은 주체가 객체에 대해 임의의 접근동작을 수행하는 데 있어서 상황조건을 명시한다. 퍼미션은 객체와 접근동작의 관계를 명시한다. 접근동작은 주체가 객체에 대해서 실행하고자 하는 응용이나 운영체제가 제공하는 서비스에 의존적인 행위의 집합이다.

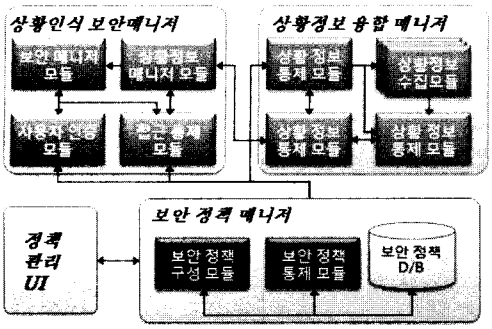
Ⅳ. CAT-RACS

4.1 CAT-RACS의 구성

CAT-RACS(Context Aware Task-Role Access Control System)는 유비쿼터스 컴퓨팅 환경에서 상황인식 기술 기반의 어플리케이션이나 시스템에 적합한 보안 메커니즘을 제공하며, 구성은 [그림 4]와 같다.

CAT-RACS는 상황인식 보안 서비스를 제공하는 상황인식 보안 매니저, 상황정보의 수집, 분석·통합 및 제공하는 상황정보 융합 매니저, 상황인식 기반의 보안정책 구성 및 관리 기능을 제공하는 보안정책 매니저, 웹 기반으로 편리한 정책 구성 및 관리 인터페이스를 제공하는 정책 관리 UI로 구성되어 있다.

CAT-RACS는 사용자가 접근을 요청하면 상황인식 보안 매니저는 사용자 인증과 접근제어를 수행하기 위



〔그림 4〕 CAT-RACS 구성

해 보안정책 매니저에 보안정책을 요구하고 상황정보 융합 매니저에게 상황정보를 요구한다. 보안정책 매니저는 접근제어 및 상황정보와 관련된 보안정책을 제공하며, 상황정보 융합 매니저는 수집된 상황정보를 통합·가공하여 접근제어에 필요한 상황정보만 상황인식 보안 매니저에 제공한다. 상황인식 보안 매니저는 수집한 정보를 바탕으로 요청한 서비스가 보안정책 규칙과 상황조건의 부합 여부를 확인하여 접근을 허가하게 된다.

4.1.1 상황인식 보안 매니저

사용자 인증, 접근제어 및 상황정보 등 보안 서비스를 관리한다. 관리 도메인 내에서 상황인식 어플리케이션들에 대한 사용 요청이 발생하면, CAT-RACS는 상황인식 보안 매니저를 통해 어플리케이션 사용을 요청한 사용자의 식별과 인증, 그리고 접근제어 등의 보안 서비스를 제공한다. 또한, 인증과 접근제어 수행을 위해 보안정책 매니저로부터 제공되는 보안정책과 상황정보 융합 매니저로부터 제공받은 상황정보를 기반으로 보안 서비스를 수행한다. 상황인식 보안 매니저의 구성 모듈의 주요 기능은 다음 [표 3]과 같다.

〔표 3〕 상황인식 보안 매니저 모듈의 기능

모 듈	기 능
보안 매니저 모듈	보안 서비스 요청 처리, 사용자 인증 및 접근제어 관리
사용자 인증 모듈	사용자 인증 및 관련 도구와 프로토콜 관리
접근통제 모듈	CA-TRBAC 모델을 기반으로 접근통제 수행
상황정보 매니저 모듈	접근제어 모듈을 위한 상황정보 관리 및 상황-역할 활성화 기능 제공

4.1.2 상황정보 융합 매니저

상황인식 기반의 보안 서비스를 위해 관리 도메인 내의 상황정보를 수집 및 관리한다. 상황정보의 요청을 받으면, 정보 수집을 위한 질의 메시지를 생성하여 센서 네트워크에 전송한다. 그리고 수집한 상황정보를 보안정책에 사용할 수 있는 정보로 통합·가공한 뒤 상황인식 보안 매니저에게 전송한다. 상황정보 융합 매니저를 구성하는 모듈의 기능은 다음 [표 4]와 같다.

〔표 4〕 정보 융합 매니저 모듈의 기능

모 듈	기 능
상황정보 분석 모듈	상황인식 보안 매니저로부터 받은 상황정보 요청 메시지 분석 상황정보 수집을 위한 질의 메시지 관리 상황정보를 상황인식 보안 매니저에 제공
상황정보 수집 모듈	센서 네트워크와의 통신을 통한 상황정보 수집
상황정보 융합 모듈	수집된 상황정보들을 보안정책에 이용 가능하도록 가공 및 통합
상황정보 통제 모듈	상황정보 수집에 필요한 규칙 통제

4.1.3 보안정책 매니저

보안정책 매니저(SPM)는 상황인식 보안 서비스를 위한 보안정책 구성과 상황인식 보안 매니저의 기능 수행에 필요한 보안정책을 제공한다. 보안정책의 특징은 인증 신뢰 지수를 적용한 사용자 인증 정보 관리와 CA-TRBAC 모델 기반의 접근제어 정책 관리이다. 보안정책 매니저를 구성하는 모듈의 기능은 다음 [표 5]와 같다.

〔표 5〕 보안정책 매니저 모듈의 기능

모 듈	기 능
보안정책 구성 모듈	CA-TRBAC 모델을 기반으로 접근제어 정책 구성 사용자 인증 정보 및 인증 신뢰 지수 관련 보안정책 구성 보안 관리 도메인 정보 관리
보안정책 통제 모듈	상황인식 보안 매니저의 보안 서비스 제공을 위해 요구하는 보안정책 제공 상황정보 융합 매니저의 상황정보 수집 및 관리에 필요한 정책 제공
보안정책 D/B	CAT-RACS의 보안 서비스에 관련된 정책 저장

4.1.4 정책 관리 UI

정책 관리 UI는 상황인식 보안 매니저와 보안 관리자 간의 인터페이스로서 보안정책 설정 및 관리를 용이하게 하기 위해 웹 기반의 그래픽 사용자 인터페이스를 제공한다.

4.2. CAT-RACS의 기능과 동작

4.2.1 사용자 인증 정보 관리

CAT-RACS는 인증 신뢰 지수를 이용하여 사용자 인증 정보를 관리하고, 접근제어 과정에서 사용자-역할 활성화 단계에 적용하여 보다 효율적으로 역할 활성화를 수행하게 된다. 인증 신뢰 지수[14]를 위한 척도는 보안 관리자에 의해 설정된다. 인증 신뢰 지수 적용 메커니즘을 설명하면 다음과 같다.

사용자 인증 신뢰도에 영향을 미치는 원인은 사용자의 인증 실패와 공격자에 의한 인증 공격이 있다. 사용자 인증에 실패하는 것을 사용자 인증의 에러 상황이라고 하면, 인증 에러 요소에는 인증 도구의 분실, 복제, 도난, 변형 등이 있다. 이러한 에러 요소를 인증 신뢰 지수에 적용하는 방법 중에 본 논문에서 적용한 확률적 접근 방식이 있다. 이 방식은 각 인증 에러 요소들마다 인증 수단에 영향을 줄 가능성을 확률로 산출한 결과를 이용하는 것이다. 인증에 영향을 주는 에러 요소들의 집합을 E라고 하고 $P(e)$는 특정 에러 요소의 가능성을 나타내는 확률 값이라고 가정할 때, 인증 신뢰 지수 산출 식은 다음과 같이 표현할 수 있다.

$$P_{authLevel} = 1 - \frac{1}{m}\sum_{i=1}^{m} P(e_i), (m = |E|, e \in E) \quad (2)$$

$P_{authLevel}$은 인증 메커니즘의 인증 신뢰 지수이며 $|E|$는 인증 에러 요소들 집합의 구성 요소 개수를 의미한다. 위에서 설명한 4가지 인증 에러 요소인 분실, 도난, 복제, 변형을 이용하여 확률적 접근 방식으로 인증 신뢰 지수를 산출한다. 이 경우, $E = \{L, C, T, M\}$, $m = 4$가 되고 $P(e_i)$는 하나의 인증 에러 요소가 갖는 인증 실패 발생 확률이다. 각 4가지 에러 요소들의 확률이 모두 0.5라고 가정하면 다음과 같이 인증 신뢰 지수를 구할 수 있다.

$$P_{authLevel} = 1 - \frac{1}{4}\sum_{i=1}^{4} P(e_i)$$
$$= 1 - 0.25 \times (0.5 + 0.5 + 0.5 + 0.5) = 0.5$$

4.2.2 상황정보 관리

CAT-RACS는 상황정보 융합 매니저를 통해 상황정보의 관리 기능을 제공한다. 상황정보 수집 정책에 따라 센서 네트워크에게 정보 수집을 요청하고, 수집되는 상황정보를 접근제어 정책에서 이용 가능하도록 가공한다.

상황정보 수집은 상황정보 융합 매니저에서 상황정보 수집 메시지를 센서 네트워크에 전달하고 수집된 상황정보를 가공하여 필요한 구성 요소에 넘겨주는 폴링 방식과 상황정보 정책으로 지정된 수집 주기 속성에 의해 주기적으로 상황정보를 수집하는 주기적 수집 방식이 있다. 폴링 방식은 보안 서비스 개시와 정책 관리 사용자 인터페이스의 상황정보 현황 시현 등에 사용되고, 주기적 수집 방식은 상황-역할 활성화/비활성화 관리에 사용된다.

상황정보의 가공은 다양한 종류의 상황정보가 갖는 여러 가지 형태의 정보를 정책에 활용할 수 있도록 정보의 형태를 통일하거나 정보를 통합하는 것이다. 예를 들어 시간 정보의 경우 날짜, 요일, 년도, "시, 분, 초" 단위의 시간, 기간 등 다양한 종류로 시간을 표현할 수 있다. 특히, 기간과 같은 경우 "2시간 동안"이라는 "~동안"의 형태와 "2006.10.15~2006.11.14"와 같이 나타내는 형태가 있을 수 있다. 다양한 종류의 시간 형태들은 어플리케이션 특성에 종속적으로 선택되어 이용되기 때문에 보안 관리자가 적절한 형태를 선별해서 정책 구성에 이용한다.

4.2.3 접근제어 정책 관리

CAT-RACS는 CA-TRBAC 기반의 접근제어 정책 관리 기능을 제공한다. 따라서 접근제어 정책 구성을 위해 CAT-RACS의 각 개체들을 CA-TRBAC의 구성 요소와 매핑하고, 사용자와 사용자-역할, 상황정보와 상황-역할, 직무와 직무-역할, 객체, 오퍼레이션과 접근권한 사이의 할당관계를 정의해야 한다. 또한, CA-TRBAC 구성 요소들은 시스템 수준의 구성 요소들을 추상화시킨 것이므로 CA-TRBAC 구성요소들을 시스템 수준의 구성 요소들과 매핑할 수 있는 규칙을 생성해야 한다.

그리고 시스템의 접근제어 리스트(ACL : Access Control List)와 같은 저수준 접근제어 메커니즘을 제어할 수 있는 규칙들을 정의해야 한다.

접근제어를 위해서는 CAT-RACS의 주체들과 사용자, 주체들과 역할, 직무들과 역할간의 연결을 관리한다. 사용자-역할을 계층적으로 구성할 경우, 계층 트리와 권한강도 간의 관계로 인해 트리의 상위 역할에 할당되는 사용자는 보다 높은 권한을 갖게 된다. 사용자와 사용자-역할 간의 다대다 할당 관계로 인해 한 사용자가 가질 수 있는 역할이 여러 개가 될 수 있으며, 이들은 각기 다른 권한 강도를 갖게 된다. 이렇게 직접적인 상속관계에 있는 역할들 간에는 역할 활성화 시에 가장 높은 권한을 갖는 역할을 우선 활성화하는 것이 일반적이며, 특별한 경우에 권한을 제한하고자 할 때에는 역할 활성화시에 동적 제약사항을 적용하여 활성화 관리를 한다.

사용자 인증에서 이용된 인증 신뢰 지수와 보안등급 속성을 사용자-역할 활성화 과정에 이용한다. 보안등급은 사용자 인증 지수를 이용하여 사용자-역할이 활성화되었을 경우, 정보의 기밀성 유출을 방지하기 위하여 한 번 더 검증하는 역할을 수행한다.

상황-역할 활성화 관련 정책은 빠르게 동적으로 변하는 상황정보를 보안 서비스에 적용하기 위해서 별도의 관리가 필요하다. CAT-RACS는 상황-역할의 특성에 따라 상황-역할 활성화 갱신 주기를 설정하여 보안 서비스의 유효성을 계속적으로 확인한다. 만일 어떤 사용자가 특정 상황에서 특정 권한에 대한 허가를 받아 보안 서비스를 제공받는다고 가정하자. 보안 서비스가 시작된 이후 상황조건이 변하게 되면 보안정책에 위배되는 상황이 발생할 수 있으며, 이는 시스템에 치명적인 결과를 가져올 수도 있다. CA-TRBAC의 상황-역할은 RBAC의 제약사항 속성을 유지하기 때문에 이러한 상황-역할 활성화와 관계된 사항들을 상황-역할 제약사항으로서 정의하여 정책에 반영한다.

4.2.4 보안 서비스 관리

CAT-RACS의 보안 서비스는 상황인식 보안 매니저의 보안 매니저 모듈이 주관한다. 보안 관리자가 사용자 인증 모듈에 사용자 인증 요청을 전송하면 사용자 인증 모듈은 서비스 요청이 발생한 정보를 바탕으로 적절한 사용자 인증 메커니즘을 선별하여 사용자 인증을 수행한다. 또한, 사용자에게 할당된 보안등급을 확인한다. 사용자의 보안등급은 보안 서비스를 요청할 때 접근하는 객체에 대한 접근 권한을 결정하는 요소가 된다.

사용자 인증이 종료되면, 사용자 인증 모듈은 사용자 식별자(ID), 보안등급(SL)과 인증 신뢰 지수(AI : Authentication Index) 정보를 보안 관리자에게 제공한다. 보안 관리자는 ID, SL, AI 그리고 사용자가 요청한 서비스 정보(객체와 오퍼레이션 정보)를 접근제어 모듈에 전송하여 접근제어를 요청하게 된다. 접근통제 모듈은 사용자가 서비스를 요청할 때, 상황정보 매니저 모듈에게 상황정보를 요청하고 상황정보 매니저 모듈은 상황정보 융합 매니저에게 상황정보 요청 메시지를 전송한다. 또한, 사용자 ID, SL, AI, 객체 정보, 오퍼레이션 정보 등을 보안정책 매니저에게 전송하여 CA-TRBAC 접근제어 수행에 필요한 사용자-역할, 직무-역할, 보안등급, 권한 정보 등을 요청한다. 상황인식 보안 매니저가 상황정보 융합 매니저와 보안정책 매니저에게 요청한 정보를 전송받으면 접근통제 모듈은 접근제어 수행을 위한 접근제어 트랜잭션을 생성하고 보안정책 매니저에게 정책 규칙 정보를 요청한다. 접근통제 모듈은 정책 규칙 정보를 이용하여 접근제어 결과를 생성하고 보안 관리자에게 반환한다. 보안 관리자는 반환 결과를 통해 사용자가 요청한 서비스에 대한 접근 허용 여부를 반환한다. 또한, 접근이 허용되면 상황-역할 활성화/비활성화 관리를 위해 주기적으로 상황정보를 수집하고, 상황-역할 비활성화 상태가 된다면 보안 관리자에게 서비스 상태 변동 이벤트를 발생시켜 서비스의 지속 여부를 결정한다.

V. CAT-RACS의 평가

CAT-RACS의 정량적 성능 평가는 현실적으로 어렵기 때문에 기존의 접근제어 시스템들과 비교·분석하여 평가한다. 특히, 비교 대상 시스템은 유비쿼터스 컴퓨팅 환경을 대상으로 한 보안 시스템 중 대표적인 연구인 Cerberus [15]와 CASA(Context Aware Security Architecture) [16]를 선택하였다.

Cerberus는 ACL을 기반으로 접근제어를 수행한다. ACL은 전통적인 접근제어 정책 모델로서 간단한 정책 구성이 가능하지만, 데이터 추상화 기능을 제공하지 않기 때문에 보안 서비스를 제공하고자 하는 조직의 권한 및 책임 구조를 보안정책에 적용하기 어렵다. 따라서 Cerberus는 해당 조직의 실제 권한과 책임 구조를 효과

〔표 6〕 CAT-RACS의 정성적 비교 평가

분 류	기 준	CAT-RACS	Cerberus	CASA
사용자 인증	인증 신뢰도 관리	가능	가능	가능
	인증 신뢰 산출 공식	확률적 접근 방식	없음	없음
	보안등급 속성	적용	미적용	미적용
접근제어	접근제어 모델	CA-TRBAC	ACL	GRBAC
	권한 할당	직무	사용자	역할
	데이터 추상화	제공(사용자, 상황정보, 권한)	미제공	제공(사용자, 객체, 환경정보)
	조직 구조 반영	가능	미반영	가능
	정책 구성 오버헤드	CASA보다 적음	적음	도메인 수에 따라 증가
	정보의 기밀성 유지	가능	불가	불가

적으로 반영할 수 있는 보안정책 구성이 어렵다. Cerberus는 상황정보를 보안정책에 이용하기 위해 1차 술어 논리를 이용하나 운영하는 조직의 규모가 커짐에 따라 관리해야 할 상황정보들의 양이 많아져서 상황정보의 추상화가 이루어지지 않으면 보안정책 관리 오버헤드가 발생하게 된다.

CASA는 관리 도메인 내의 사용자, 객체, 환경 정보들을 역할로 추상화하여 보안정책 관리 기능을 제공하는 GRBAC(Generalized Role Based Access Control)을 기반으로 하고 있다. 하지만 GRBAC은 기본적으로 RBAC이 제공하는 권한 추상화를 제공하지 않으며, 관리 도메인 요소들이 많아짐에 따라서 관리해야 할 역할의 양이 많아진다. 또한, 객체 역할과 환경 역할 간의 중복되는 영역이 발생되는 문제로 인해 보안정책 관리 및 구성에 따르는 오버헤드가 많이 발생한다.

사용자 인증 신뢰도를 측정하기 위해 Cerberus와 CASA는 각각 "Confidence Level, Authentication Parameter" 등을 이용하여 인증 신뢰도를 보안정책에 적용한다. 하지만 이들은 인증 신뢰도 산출을 위한 별도의 정형화된 공식을 사용하지 않고 보안 관리자가 임의로 인증 신뢰도를 산출한다. 따라서 각 보안 시스템이 적용되는 상황에 따라 일관성 없이 정책이 구성되고 관리되는 단점을 갖는다. CAT-RACS와 Cerberus, CASA 시스템의 특징을 정성적으로 비교 평가한 결과는 [표 6]과 같다.

CAT-RACS의 접근제어 메커니즘인 CA-TRBAC은 상황정보를 추가하여 유비쿼터스 컴퓨팅 환경에서 T-RBAC이 갖는 단점을 해결하였다. 예를 들어, 홍보실의 언론매체 담당자(C급)가 주요 보도자료(C급)를 작성하기 컴퓨터를 통해 언론 보고서(C급) 객체에 접근한다고 가정하자. T-RBAC은 사용자가 언제 어디서 어떻게 객체에 접근하더라도 역할, 직무, 객체가 올바르게 할당되면 때문에 접근을 허가할 것이다. 또한, 언론매체 담당자가 로비에서 점심시간에 PDA를 통해서 언론 보고서에 접근한다고 하더라도 접근을 허가할 것이다. 그러나 CAT-RACS는 점심시간이라는 시간상황과 PDA라는 위치상황 정보가 상황-역할에 부합되지 않기 때문에 접근을 거부한다. 이것은 사용자의 상황을 판단하여 불법적인 접근과 비인가 접속을 방지하기 위함이다.

CAT-RACS는 정보시스템에서 다루는 정보의 기밀성을 고려하여 보안등급의 속성을 활용하였다. 만약 홍보실의 보도자료 담당자가 보안등급이 "Unclassified"이라면, 주요 보도자료 작성(C급) 직무에 할당을 거부한다. 언론 보고서 접근도 거부한다. 아울러 언론매체 담당자가 보안등급인 Secret인 회사 정책 작성 직무에 할당하지 않는다. 또한, "Secret" 보안등급인 홍보실장이 "Secret"급인 프로젝트 보고서 작성을 하기 위하여 "Secret"인 회사 정책 보고서에 "write" 권한, "Confidential"급의 언론 보고서에 "read" 권한을 줄 수 없다. 만약, 이렇게 권한을 할당한다면 회사 정책 보고서(S) 객체에서 언론 보고서(C) 객체로 정보가 이동되어 정보의 기밀성이 파괴된다.

Ⅵ. 결 론

본 논문은 상황정보와 조직의 직무 특성을 기반으로 한 접근제어 정책 관리와 접근제어를 수행할 수 있는 CA-TRBAC 모델을 기반으로 보안 서비스를 제공하기 위한 접근제어 관리 시스템인 CAT-RACS를 소개하였다. CA-TRBAC 모델은 기존의 직무-역할기반 접근제

어 모델인 T-RBAC을 기반으로 상황정보에 따른 정책 구성을 수행할 수 있도록 상황-역할 개념을 추가하였고, 정보의 중요성을 고려하여 정보의 기밀성을 유지시키고, 불법적인 정보의 유출을 식별하고 차단하기 위해서 보안등급 속성도 활용하였다.

CAT-RACS는 유비쿼터스 컴퓨팅 환경에서 상황 인식 기술 기반의 어플리케이션이나 시스템에 적합한 보안 메커니즘을 제공한다. 유비쿼터스 컴퓨팅 환경에서는 사용자의 상황이 자주 변화하기 때문에 접근을 요청하는 사용자의 위치, 상태 등의 상황정보를 이용하여 접근을 통제하는 기술을 적용하였다. 또한, 기업 내에서 유통되는 정보 즉, 접근 대상인 객체가 때로는 중요한 내용을 포함하고 있기 때문에 서로 다른 보안등급의 객체간의 정보의 흐름과 유출을 방지할 수 있다. CAT-RACS는 접근제어 과정에 앞서 사용자 인증 기능도 제공하는데, CAT-RACS에서는 CA-TRBAC의 사용자-역할 활성화 관리를 용이하게 하기 위해 인증 신뢰 지수를 적용한 사용자 인증 관리 기능을 제공한다.

참고문헌

[1] Frank Stajano, *Security for ubiquitous computing*, Wiley, 2002.

[2] David F. Ferraiolo and D. Richard Kuhn, Ramaswamy Chandramouli, *Role-Based Access Control*, Artech House, 2003.

[3] Weili Han, Junjing Zhang, and Xiaobo Yao, "Context-sensitive Access control Model and Implementation", Proceedings of The CIT'05, pp.757-763, September, 2005.

[4] Antonio Corradi, Rebecca Montanari, and Daniela Tibaldi, "Context-based Access Control for Ubiquitous Service Provisioning", Proceedings of the COMPSAC'04, pp. 444-451, September, 2004.

[5] Antonio Corradi, Rebecca Montanari, and Daniela Tibaldi, "Context-based Access Control Management in Ubiquitous Environments" Proceedings of the NCA'04, pp. 253-260, September, 2004.

[6] Guangsen Zhang and Manish Parashar, "Dynamic Context-aware Access Control for Grid Applications", Proceedings of the GRID'03, pp. 101-108, November, 2003.

[7] 임희섭, *군사환경에 과업-역할기반 접근제어 모델을 적용하기 위한 제약조건*, 석사학위논문, 서강대학교 컴퓨터학과, 2002.

[8] Role Based Access Control, American National Standards Institute, February, 2004.

[9] Sejong Oh and Seog Park, "Task-role-based access control model", Information System, Vol.28, No.6, pp.533-562, September, 2003.

[10] Sejong Oh and Seog Park, "Task-Role Based Access Control(T-RBAC) : An Improved Access Control Method for Enterprise Environment", Proceedings of the DEXA2000, pp. 264-273, September, 2000.

[11] 임신영, 허재두, "상황인식 컴퓨팅 응용 기술 동향" 전자통신동향분석 제19호 제5호, October, 2004.

[12] Anind K. Dey, Gregory D. Abowd, "The context toolkit : Aiding the development of context-aware applications", In Workshop on Software Engineering for Wearable and Pervasive Computing, June 2000.

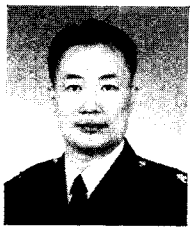
[13] 박선호, *유비쿼터스 컴퓨팅 환경을 위한 상황인식 통합 보안 관리 시스템에 관한 연구*, 석사학위논문, 성균관대학교 컴퓨터공학과, 2006.

[14] 박선호, 김희승, 한영주, 정태명, "*다중사용자인증시스템에서의 인증신뢰지수 적용에 대한 연구*", 한국정보처리학회 추계학술발표대회 논문집 제12권 제2호, November, 2005.

[15] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M. Dennis Mickunas, "Cerberus : A Context-Aware Security Scheme for Smart Spaces", In IEEE International Conference on Pervasive Computing and Communications (PerCom 2003), Dallas-Fort Worth, Texas, March 23-26, 2003.

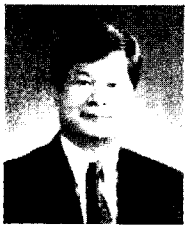
[16] Covington. M.J et al, "A Context-Aware Security Architecture for emerging applications", In IEEE 18th Annual International Conference on Computer Security Applications, pp. 249-258, 2002.

〈著者紹介〉



엄 정 호 (Jung-Ho Eom) 정회원
1994년 2월 : 공군사관학교 항공공학과 공학사
2003년 2월 : 성균관대학교 컴퓨터공학과 공학석사
2008년 2월 : 성균관대학교 컴퓨터공학과 공학박사
1994년 3월~현재 : 대한민국 공군 장교 근무
<관심분야> 취약성평가 및 분석, 위험분석, 접근제어모델, 네트워크보안, 시스템보안

박 선 호 (Seon-Ho Park) 학생회원
2005년 2월 : 성균관대학교 정보통신공학부 공학사
2007년 2월 : 성균관대학교 컴퓨터공학과 공학석사
2007년 2월~현재 : 성균관대학교 전자전기컴퓨터공학과 박사과정
<관심분야> 접근제어모델, 시스템보안, 네트워크보안, 무선센서네트워크 보안



정 태 명 (Tai-Myoung Chung) 종신회원
1981년 2월 : 연세대학교 전기공학과 공학사
1984년 5월 : 일리노이주립대학 전자계산학 공학사
1987년 12월 : 일리노이주립대학 컴퓨터공학 공학석사
1995년 8월 : 퍼듀대학교 컴퓨터공학 공학박사
1985년 8월~1987년 12월 : Waldner and Co., System Engineer
1987년 12월~1990년 8월 : Bolt Bernek and Newman Labs. Staff Scientist
1995년 9월~현재 : 성균관대학교 정보통신공학부 정교수
2008년~현재 : OECD 정보보호 분과 부의장
<관심분야> 실시간시스템, 네트워크 관리, 네트워크보안, 시스템보안, GRID 네트워크, 위험관리, 유비쿼터스 컴퓨팅 보안