제25회 한국정보처리학회 춘계학술발표대회 논문집 제13권 제1호 (2006. 5)

역할기반 접근제어 정책을 통해 강화된Cerberus에 대한 연구*

김종명*, 조준식**, 엄정호**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 컴퓨터공학과
e-mail : {jmkim, jscho, jheom}@imtl.skku.ac.kr , tmchung@ece.skku.ac.kr

A study on Enhanced Cerberus based on RBAC in Ubiquitous Environments

Jong-Myoung Kim*, Joon-Sic Cho, Jung-Ho Eom, Tai-Myoung Chung*
*School of Information Communication Engineering, SungKyunKwan Univ.
**Department of Computer Engineering, SunKyunKwan Univ.

요 약

일리노이 공대의 Gaia 프로젝트는 유비쿼터스 환경에서 컨텍스트 정보를 기반으로 사용자를 인증하고 어플리케이션에 대한 사용자의 접근 제어를 하는 Cerberus 라는 프레임워크를 제안하였다. 그러나 Cerberus 는 사용자의 식별 정보를 통해 접근 제어를 함으로써 생기는 문제점과 어플리케이션이 사용자의 접근 제어에 직접적으로 영향을 주는 문제점이 있다. 본 논문에서는 Cerberus 의 문제점을 개선한 새로운 프레임워크를 제안한다. 이 프레임워크는 RBAC(Role Based Access Control) 기반의 접근 제어 정책을 통한 안전성 향상 뿐만 아니라 어플리케이션에 대한 직접적인 접근 제어 봉쇄를 통해 정책 관리에 대한 일관성을 제공한다.

1. 서론

유비쿼터스 컴퓨팅은 다양한 통신기기와 센서들이 넓게 분산되어 있는 환경을 통해 이루어 진다. 유비쿼터스 컴퓨팅을 통해 컴퓨터 시스템 자원과 물리적 공간의 경계를 넘어 사용자에게 편리함과 풍부한 정보가 존재하는 공간을 제공할 수 있다. 이러한 공간을 스마트 스페이스라고 한다. 이런 환경에서는 컴퓨터가 사용자의 컨텍스트 정보를 수집하고 분석하여 사용자를 인증하고 수집된 정보를 바탕으로 사용자가 이용 가능한 서비스를 제공한다. 여기서 컨텍스트[1]란 엔터티(entity)의 상황을 특징 짓는 데 사용되는 모든 정보를 말하며 엔터티는 사용자와 어플리케이션을 포함하며 사용자와 어플리케이션 상호 작용에 관련되는 사람이나 장소 그리고 객체를 말한다. 이런 컨텍스트는 유비쿼터스 환경에서 사용자에게 서비스를 제공하는데 가장 근본적인 요소이며 유비쿼터스의 특징을 대표하는 것이다.

하지만 유비쿼터스 환경에서 컨텍스트 정보만을 가지고 서비스를 제공하기에는 한계가 있다. 누구나 제한 없이 서비스를 이용할 수 없기 때문이다. 즉 사용자 인증과 서비스에 대한 접근 제어 메커니즘이 필요하다. 전통적인 인증 및 접근 제어 방법에서는 로그인과 로그아웃이라는 상호작용을 통해 인증을 직접 해야만 했지만 유비쿼터스 환경에서는 컨텍스트 정보를 바탕으로 사용자에 대한 인증과 서비스 접근을 제공하기 때문에 새로운 방법이 필요하다.

일리노이 공대의 Gaia 프로젝트에서는 Cerberus[2]라는 유비쿼터스 환경에서의 사용자 인증 및 접근 제어 프레임워크를 제안하고 있다. 본 논문에서는 Cerberus를 분석하고 이를 보완해 더욱 효율적인 사용자 인증 및 접근 제어 프레임워크를 제안한다. 논문의 구성은

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 육성・지원사업의 연구결과로 수행되었음.

다음과 같다. 2 장에서는 일루누이 공대의 Cerberus 에 대해 분석한다. 3 장에서는 Cerberus 를 개선한 사용자 인증 및 접근 제어 프레임워크를 제안한다. 4 장에서는 이 논문의 결론과 향후 연구 방향에 대해 기술한다.

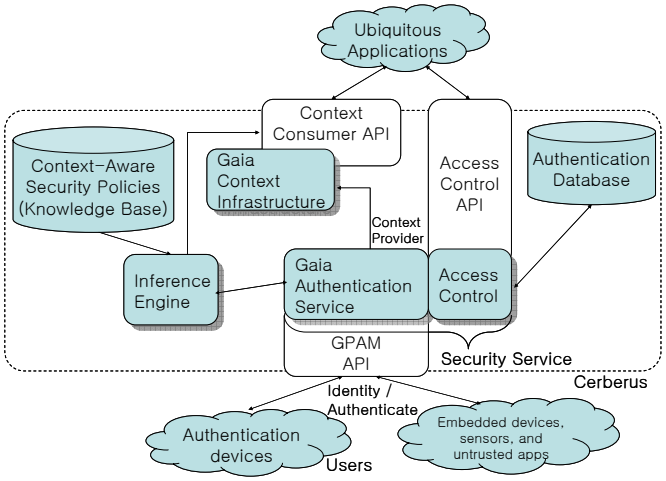
2. Cerberus

2.1 Gaia 프로젝트

일리노이 공대에서는 스마트 스페이스를 구성하기 위한 기반 구조를 제공하기 위해 Gaia 프로젝트를 진행하고 있다. Gaia 프로젝트에서는 스마트 스페이스를 구성하기 위해 두 가지 필수 요소인 보안과 컨텍스트 인식(context awareness)을 위해 Cerberus 라는 핵심 서비스를 제공한다. Cerberus 는 사용자를 식별 및 인증을 하고 컨텍스트 인식과 이에 따른 추론을 통해 스마트 스페이스 환경을 구축하기 위한 기본적인 서비스를 말한다.

2.2 Cerberus 의 구조

Cerberus 는 유비쿼터스 환경에서의 서비스를 제공을 목적으로 사용자를 식별하고 인증하기 위하여 다양한 종류의 기기와 센서들로부터 풍부한 컨텍스트 정보를 얻는 것을 중요시한다. 풍부한 컨텍스트 정보를 바탕으로 사용자 식별 및 인증을 하기 위해서는 다양한 방법의 인증 방법을 제공 해야 한다. 이를 위해 Cerberus 에서는 (그림 1)처럼 GPAM (Gaia Pluggable Module)을 이용한다. 이는 전통적인 PAM[3]을 이용하여 새로운 인증 방법이 쉽게 추가가 가능하도록 하는 메커니즘이다. 이를 통해 Cerberus 는 다양한 인증 방법을 확보할 수 있다.



(그림 1) Cerberus

Gaia 인증 서비스(Gaia Authentication Service)에서는 인증 데이터베이스의 정보를 바탕으로 사용자를 다양한 방법으로 식별 및 인증을 한다. 이런 식별 정보 및 인증 방법 역시 컨텍스트 정보임으로 이를 Gaia 컨텍스트 기반 구조(Gaia Context Infrastructure) 모듈로 보낸다.

Gaia 컨텍스트 기반 구조는 사용자의 식별 정보 및 인증 방법뿐만 아니라 스마트 스페이스 상에 존재하는 다양한 유비쿼터스 컴퓨팅 기기와 센서들로부터 컨텍스트 정보를 얻고 이를 일정한 형태로 가공 표현하여 어플리케이션이나 추론 엔진(Inference Engine) 모듈에서 사용 가능하도록 한다.

추론 모듈에서는 Cerberus 의 보안 정책(Context-Aware Security Policies)에 서술된 내용을 바탕으로 컨텍스트 정보를 Gaia 컨텍스트 기반 구조 모듈로부터 제공 받아 사용자가 사용하려는 어플리케이션이 사용 가능한지를 결정한다. 보안 정책에는 각 어플리케이션 마다 어플리케이션에 접근 가능한 상황을 기술하고 있으며 컨텍스트 정보가 이를 만족할 때 사용자에게 접근 권한을 부여할 수 있도록 되어있다.

2.3 Cerberus 의 인증 방법

유비쿼터스 컴퓨팅 인증 메커니즘은 '인증 강도'와 '사용자 개입' 사이에서의 조절이 중요하다. 예를 들어 좁은 영역에 주파수 신호를 발산하는 스마트 배지(smart badge)를 이용한 인증 방법은 사용자가 의식적인 개입 없이 인증이 되지만 인증의 강도는 낮을 것이다. 하지만 Challenge-response 방법을 이용을 하면 사용자의 개입이 필요하겠지만 인증의 강도는 높아진다.

Cerberus 에서는 착용 가능한 기기나 음성 인식, 안면 인식, 지문인식 그리고 홍채 인식 등 다양한 인증 방법을 포함한다. 이런 다양한 방법들마다 인증 강도가 다를 것이다. 인증 강도에 따라 사용자를 식별하는 신뢰도가 다를 것이며 이를 Cerberus 에서는 [0, 1] 사이의 값으로 표현한다. 이런 신뢰 값은 인증 장비나 사용한 인증 프로토콜의 종류에 따라 결정이 된다. 사용자 한 사람에 대해 여러 가지 인증 방법이 이용될 수 있으며 여러 개의 신뢰 값들을 얻게 된다. 이를 Bayesian probability, 와 fuzzy logic[4]을 통해 통합된 신뢰 값을 얻는다.

Cerberus 에서는 위의 내용을 1 차 논리(first order logic)[5]의 규칙으로 인증 정책을 표현하고 있다. 예를 들어 인증 방법에 따라 신뢰 값을 다음과 같이 서술할 수 있다.

ConfidenceLevel (smart_watch, 70%)
ConfidenceLevel (smart_badge, 10%)
ConfidenceLevel (fingerprint_scan, 90%)

이 때 P 가 smart_watch 로 인증을 했다면 다음과 같이 표현이 된다.

Authentication (P, smart_watch)

P 가 가진 신뢰 값 V 는 다음과 같이 표현된다.

ConfidenceValue (P, V) :- ∃device X (Authenticated(P,X) ∧ ConfidenceLevel (X, V))

2.4 Cerberus 의 접근 제어 방법

Cerberus 에서는 사용자가 어플리케이션에 접근이 가능한지를 알기 위해 어플리케이션 별 접근 제어(Application-specific Access Control) 정책을 이용한다. 어플리케이션 별 접근 제어 정책에서는 어플리케이션에 접근하기 위한 신뢰 값 그리고 사용자가 해당 자원에 접근이 가능한지를 결정할 수 있는 컨텍스트 정

보가 기술되어 있다. 예를 들어 Bob 이 프리젠테이션 디스플레이 기기를 사용하고자 한다면, 1 차 논리의 규칙으로 다음과 같이 기술될 수 있다. 여기서 NetConfidenceValue 는 통합된 신뢰 값을 나타낸다.

∀People X CanAccess (X, Display) :- ∃number V (NetConfidenceValue(P, V) ∧ V>60%)

∀People X Access(X, Display) :- SocialActivity(Room 2401, Seminar) ∧ IsPresenter(Seminar, X)

Bob 이 디스플레이 기기에 접근하기 위해서는 먼저 인증방법으로 얻은 신뢰 값이 프리젠테이션 디스플레이 기기를 사용하기 충분한지를 살펴본다. 그런 후 회의실의 스케줄이 세미나 인지를 확인하고 해당 세미나 발표자가 Bob 인지를 확인을 하도록 되어있다.

2.5 Cerberus 에서 개선되어야 할 사항

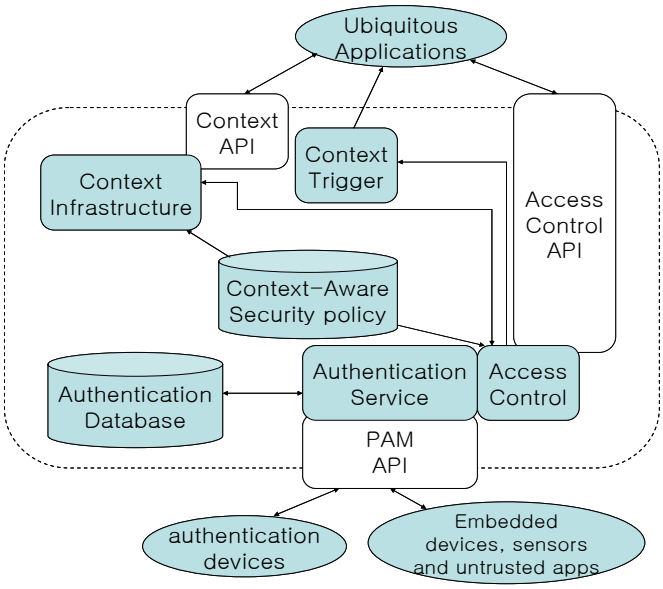
Cerberus 에서 개선되어야 할 점은 크게 두 가지가 있다. 그 중 하나는 사용자의 접근 제어 방법에 있다. Bob 의 프리젠테이션 기기 사용의 예를 다시 살펴보자. 인증 방법을 통해 Bob 이 접근에 필요한 신뢰 값을 가지고 있는지를 확인한 후 "Bob 으로 식별된 상태"에서 프리젠테이션에 대한 접근 가능성을 Bob 의 컨텍스트 정보에 따라 추론하고 있다. 하지만 Bob 이라고 100% 완벽하게 식별 되지 않은 상태임으로 Bob 에 대한 모든 정보를 컨텍스트 정보로 사용해서는 안된다. 예를 들어 "Bob 이 프리젠테이션 기기를 사용하기 위해서는 60% 이상의 신뢰 값을 가져야 한다."라고 하면 이는 "Bob 이 프리젠테이션을 할 수 있는 역할을 가진 사람이다."는 정도를 말하는 것이지 Bob 자체를 의미하는 것이 아니다. 만약 관리자의 실수로 인증 신뢰 값을 낮게 설정한다면, 인증의 강도가 낮아 다른 사람이 Bob 인 척을 할 수 있고 해당 어플리케이션에 대해서는 Bob 의 모든 권한을 행사할 수 있게 된다.

두 번째로 개선될 점은 사용자가 어플리케이션에 접근 권한을 얻어 사용 중일 때, 컨텍스트 정보의 변화에 따라 접근 권한이 상실 될 경우가 있다. 이 때 Cerberus 에서는 "어플리케이션"이 사용자의 접근 권한이 상실될 수 있는 컨텍스트 조건을 접근 제어 모듈에 요구하고 접근 제어 모듈은 컨텍스트 정보의 변화를 체크를 하고 조건이 성립되면 어플리케이션에 통보하는 메커니즘을 이용하고 있다. 이는 접근 제어 정책의 설정에 있어서 심각한 문제가 된다. 어플리케이션이 접근 제어 정책에 직접 개입함으로써 관리자가 설정한 접근제어 정책과 상반되는 결과를 가져올 수 있기 때문이다.

3. 새로운 인증 및 접근 제어 프레임워크 제안

3.1 구조

좀 더 안전하고 효율적인 보안 정책을 위해 기존 Cerberus 의 접근 제어 정책에 RBAC(Role Based Access Control)[6]을 적용하였다. Cerberus 의 추론 엔진은 접근 제어 모듈로 통합하였으며, 컨텍스트 정보의 변화에 따라 어플리케이션을 사용중인 사용자의 접근 권한 상실이 되는 경우를 위해 컨텍스트 트리거(Context trigger) 모듈을 추가하였다. 그 외 컨텍스트 정보 제공을 위한 컨텍스트 기반구조 모듈과 사용자 인증 및 보안 정책을 위한 보안 정책 모듈 등은 그대로 유지하였다.



(그림 2) 컨텍스트 기반 인증 및 접근 제어

3.2 인증 방법

Cerberus 의 인증 방법과 동일하다. 여러 가지 인증 방법을 통해 사용자에 대한 신뢰 값을 산출한다. 이를 위해 PAM 모듈을 수용하고 fuzzy logic 을 이용 여러 신뢰 값들을 통합해 하나의 신뢰 값을 얻어 이를 사용자의 식별 정보와 함께 접근 제어를 위해 접근 제어 모듈로 넘긴다. 넘겨지는 정보를 1 차 논리(first order logic)로 표현하면 다음과 같다.

NetConfidenceValue(Bob, V)

3.3 접근 제어 방법

본 논문에서 제안하는 프레임워크에서는 기존의 RBAC 에 컨텍스트 개념을 적용시킴으로써 유비쿼터스 환경에 맞는 접근 제어를 제공한다. 먼저 RBAC 정책을 바탕으로 시스템에 맞게 역할들을 미리 정의하고, 사용자들에게 역할을 배정한다. 역할을 정의할 때 트랜잭션(transaction)이라는 시스템 자원 접근에 관한 함수를 정의 한다. 역할들은 비 활성화 되어있는 상태이며 각 역할에는 역할이 활성화 되기 위한 신뢰 값과 컨텍스트 조건이 기술되어 있다. 만약 Bob 이 seminar_time(매주월요일 오후 3 시) 에 2401 번 회의실에서 세미나 발표를 한다면 다음과 같이 기술할 수 있다.

CanActivateRole (Bob, Seminar_presenter) :- (NetConfidenceValue(Bob, V) ∧ V>60%) ∧ time(current_time, seminar_time) ∧ location(current_location, Room 2401) ∧ SocialActivity(Room 2401, Seminar)

만약 Bob 의 신뢰 값과 컨텍스트 조건이 일치 하다면 Seminar_presenter 역할을 활성화 시킨다. 이제 Bob

의 Seminar_presenter 역할을 통해 프리젠이션 디스플레이 기기에 접근이 가능한지 확인을 한다. 이때 역할에 기술되어 있는 트랜잭션을 통해 Bob 이 디스플레이 기기에 접근이 가능한지 확인할 수 있다.

?Access(Bob, Display) :- ActivatedRole(Bob, Seminar_presenter) ∧ Roletransacion(Seminar_presenter, Display)

이와 같이 활성화 된 역할을 통해 접근 제어를 함으로써 2.5 절에서 제시되었던 Cerberus 의 첫 번째 문제점을 해결할 수 있다. 신뢰 값에 해당하는 역할을 통해서만 접근 제어를 하기 때문에 해당 어플리케이션에 대해 사용자의 모든 권한을 행사하는 것을 방지할 수 있기 때문이다.

접근 제어 방법을 더욱 효율적으로 하기 위해 접근 제어에서 쓰이는 컨텍스트 정보들을 미리 정의를 해 놓는다. 컨텍스트 정보를 미리 정의함으로써 컨텍스트 기반 구조로부터 컨텍스트 정보를 얻을 때 원하는 형태로 가공된 컨텍스트 정보를 얻을 수 있게 된다. 또한 미리 정의된 컨텍스트 정보들을 바탕으로 새로운 컨텍스트 정보의 정의 및 정책 설정에 활용할 수 있다.

3.4 컨텍스트 트리거

유비쿼터스 환경에서는 컨텍스트 정보가 자주 바뀐다. 이런 컨텍스트의 변화에 따라 어플리케이션을 사용중인 사용자라 하더라도 접근 권한이 상실되는 경우가 있다. 따라서 접근 제어 정책에는 접근 권한이 상실되는 컨텍스트 조건을 기술할 수 있어야 한다. 본 논문에서는 이런 조건을 컨텍스트 트리거(context trigger)라 부르며, 사용자의 역할에 컨텍스트 트리거를 추가 기술할 수 있다. 앞의 프리젠테이션의 예를 기술하면 다음과 같다.

ContextTrigger(X, Display) :- NOT SocialActivity(Room 2401, Seminar) ∨ NOT ActivatedRole(Bob, Seminar _presenter)

일단 사용자가 어플리케이션에 접근 권한을 얻고 사용 중 일 때, 컨텍스트 트리거 모듈은 컨텍스트 트리거를 활성화 하고, 컨텍스트 변화를 관찰하며 조건이 성립되면 어플리케이션에 사용자의 접근 권한이 상실되었음을 통보한다.

이렇게 기술된 컨텍스트 트리거를 통해 2.5 절에 논의된 Cerberus 의 두 번째 문제를 해결 할 수 있다.

3.5 성능 비교

Cerberus 에서는 인증 방법에 따라 사용자에 대한 신뢰 값을 이끌어 내고 어플리케이션에서 요구하는 신뢰 값 이상을 가지면 컨텍스트 정보와 비교를 통해 서비스를 제공한다. 하지만 사용자에 대해 완벽하게 식별되지 않은 상태임으로 식별된 사용자의 정보를 이용해 서비스를 제공하는 것은 보안적 측면에서 문제가 있다. 본 논문에서 제시하는 인증 및 접근 제어 방법에서는 신뢰 값을 통해 사용자의 역할을 이끌어 내고 이 역할을 통해 어플리케이션에 접근함으로써 Cerberus 의 문제점을 보완하고 있다.

또한 Cerberus 에는 어플리케이션이 접근 제어에 직접적으로 참여함으로써 접근 제어 정책의 일관성 문제가 있다. 하지만 본 논문에서 제시한 컨텍스트 트리거를 이용한 방법을 통해 이를 해결하고 있다.

4. 결론 및 향후 연구 방향

본 논문에서는 Cerberus 를 바탕으로 좀더 효율적이고 안전한 사용자 인증 및 접근 제어 프레임워크를 제시하였다. 이런 프레임워크를 통해 유비쿼터스 환경에서 어플리케이션의 서비스 제공을 위한 기반 구조를 구성할 수 있다.

하지만 본 논문에서 제시한 접근 제어 정책에 대해 자세한 연구가 필요하다. 기존의 RBAC 에 컨텍스트 정보를 추가함으로써 더욱 유비쿼터스 환경에 적합한 접근 제어 정책이 연구되어야 한다. 또한 이러한 정책을 표현하기 위한 언어에 대한 연구도 이루어져야 할 것이다. 정책을 좀더 효율적이고 세세하게 표현할 수 있는 언어가 있다면 컨텍스트 정보를 기반으로하는 인증 및 접근 제어가 한층 더 쉬워질 것이다. 앞으로 컨텍스트 정보를 이용하는 RBAC 에 대한 연구를 진행해 더욱 효율적인 접근 제어 정책을 제안하고자 한다.

참고문헌

[1] Dey A.K. and Abowd G.D , “Towards a better understanding of context and context-awareness”, GVU Technical Report GITGVU 99-22, College of Computing, Georgia Institute of Technology, September 1999.

[2] Jalal A., Anand R., Roy C.l and M. Dennis Mikunas, “Cerberus: A Context-Aware Security Scheme for Smart Spaces”, Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on 23-26 March 2003 Page(s):489 – 496.

[3] V. Samar and R. Schemers, “Unified Login with Pluggable Authentication Modules (PAM)”, RFC 86.0, 1995

[4] Klir, G.J., “Fuzzy logic”, IEEE Volume 14, Issue 4, Oct-Nov 1995 Page(s):10 - 15

[5] Shuwei Chen, Yang Xu, “Using first-order logic to reason about policies”, Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE 30 June-2 July 2003 Page(s):187 - 201

[6] David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli, ‘Role-Based Access Control’, Artech House, 2003