OSGi 서비스 플렛폼에서 사용자 접근제어를 위한 프레임워크와 사용자 관리 서비스

김수정*, 조은애**, 문창주***
*고려대학교 컴퓨터과학기술대학원 디지털정보공학과
** 고려대학교 정보통신대학 컴퓨터학과
**건국대학교 컴퓨터 응용과학부
e-mail : kimsuj1@npa.go.kr, eacho@software.korea.ac.kr, cjmoon@kku.ac.kr

A Framework and User Admin Service for User Access Control in OSGi Service Platform

Su-Jong Kim*, Eun-Ae Cho**, Chang-Joo Moon***
*Graduate School of Computer Science Technique, Korea University
**Dept. of Computer Science & Engineering, Korea University
***Dept. of Computer Science, Konkuk University

요 약

OSGi 는 이질적인 다양한 기술들이 존재하는 홈 네트워크 환경에서 상호 운영성을 보장하는 서비스 플렛폼을 제공한다. 사용자 접근제어는 홈 네트워크에서 반드시 해결해야 하는 보안의 핵심분야 중에 하나지만 아직은 구체적인 연구가 진행되고 있지 않다. 본 논문에서는 OSGi 서비스 플렛폼이 운영되는 홈 네트워크 환경에서 사용자 접근제어를 위한 RBAC 기반의 권한부여 정책 관리 플렛폼과 보완된 사용자 관리 서비스를 제안한다. 제시된 접근제어 프레임워크는 사용자의 프라이버시 문제를 해결함과 동시에 사용자 편의성도 제공을 한다. 또한 보완된 사용자 관리 서비스의 인터페이스는 요구되는 주요 기능들을 추가 함으로써 접근제어를 위한 OSGi 서비스 프레임워크 구현에 가이드 라인을 제공 한다.

1. 서론

인터넷은 빠른 속도로 발전하고 있으며 이를 효율적으로 사용하기 위하여 다양한 네트워크가 구축 되었다. 최근에는 네트워크 환경이 가정에까지 파고 들어 홈 네트워크 분야를 탄생시켰다. 홈 네트워크에서 홈 게이트웨이는 유무선의 액세스 망과 댁내 망을 연결하여 다양한 서비스를 제공할 뿐 아니라 휴대 정보단말기를 통한 원격 자동제어, 홈 보안기능 및 관리기능을 제공한다. 따라서 홈 게이트웨이는 향후 홈 네트워크가 구축된 디지털 홈의 핵심적인 역할을 수행한다.

현재 홈 네트워크 환경에는 다양한 유무선 네트워크 기술을 기반으로 다양한 홈 게이트웨이, 지능형 정보가전 및 미들웨어들이 존재하며 서로 다른 H/W 플랫폼, 운영체제 및 네트워크 프로토콜에 따라 수많은 서비스 개발 환경이 존재한다. 이와 같은 홈 네트워크의 이질성과 복잡성을 해결하기 위하여 OSGi(open service gateway initiative)는 동일한 형태의 API(Application Programming Interface)를 통하여 서비스 제공업체, 망 관리업체, 시스템 개발업체 및 정보가전 기기 업체 간의 상호 운용성을 보장하는 서비스 플렛폼을 정의하고 있다[1]. 따라서 홈 네트워크에서의 보안 문제는 홈 게이트웨이 상에서의 OSGi 서비스 플렛폼과 밀접한 관계를 가지고 있으며 이 부분에서 신규 보안 취약성이 발생한다.

홈 게이트웨이 상에서의 주요 핵심 보안 이슈는 홈 네트워크에 접근하는 사용자에 대한 인증(Authentication)과 접근제어(Authorization) 이다[2]. 인증은 신뢰할 수 있는 제 3 의 기관에 의해서 실행되고 기존의 인증기술들이 성숙해 있어 상당 부분 홈 게이

트웨이와 독립적으로 적용된다. 그러나 접근제어는 접근가능 여부를 판단하는 작업이 홈 게이트웨이에서 사용자가 댁내 정보가전과 자동화 기기를 접근할 때마다 이루어져야 하므로 홈 게이트웨이와 밀접한 관계를 가지고 있다. 또한 사용자의 댁내 정보가전과 자동화 기기들의 접근권한을 명세한 권한부여(Authorization) 정책은 개인 프라이버시에 해당함으로 생성과 관리에 있어 세밀한 운영이 필요하다.

가장 최근에 배포된 OSGi 서비스 플랫폼 3.0 에서는 사용자 접근제어 부분을 사용자 관리 서비스 부분에서 언급하고 있다[1]. 그러나 이분은 버전 1.0 부터 변동이 없는 부분으로 많은 주요 기능들이 누락 되어 있다. 또한 권한부여 정책 관리와 운영을 위한 구체적인 프레임워크가 아직 제시 되지 못하고 있다. 본 논문에서는 이러한 문제들을 해결하기 위해서 OSGi 서비스 플랫폼이 운영되는 홈 네트워크 환경에서 사용자 접근제어를 위한 RBAC(Role-Based Access Control) 기반의 권한부여 정책 관리 플랫폼[3][4][5]과 UML(Unified Modeling Langiage)을 이용하여 설계된 진보된 사용자 관리 서비스를 제시한다.

본 논문의 구성은 다음과 같다. 2 장에서는 OSGi 서비스 플랫폼에 대해서 언급한다. 3 장에서는 본 논문에서 제안하는 접근제어 프레임워크에 대해서 설명 하고 4 장에서는 기능이 강화된 사용자 관리 서비스에 대해서 설명 한다. 마지막으로 5 장에서 본 연구의 결론 및 향후 연구 과제에 대해 서술한다.

2. OSGi 서비스 플랫폼

OSGi 는 홈 게이트웨이 표준화 단체 중의 하나로 업계표준을 정하는 단체이다. 현재 OSGi 에는 Sun microsystems, IBM, Sony, Samsung 등 세계 유수의 기업이 참여하고 있다. 서비스에 대한 기본적인 프레임워크는 거의 완성되었지만, 보안에 대한 상당 부분은 지금도 진행 중에 있다. OSGi 서비스 플랫폼의 전체적인 구조는 그림 1 과 같다.

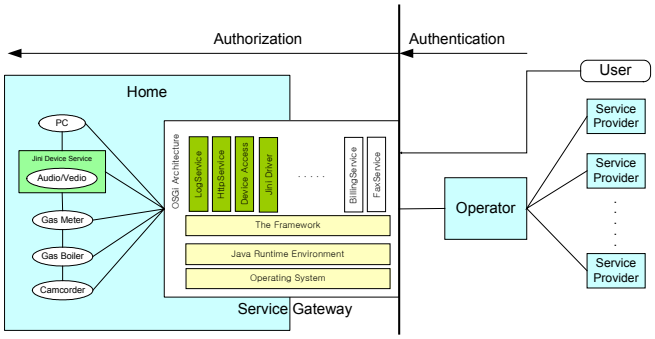

그림 1. OSGi 서비스 플랫폼 구조

OSGi 서비스 플랫폼은 서비스 제공자, 오퍼레이터, 홈 게이트웨이로 구성된다[2][6]. 서비스 제공자는 번들을 제작하여 오퍼레이터에게 제공한다. 오퍼레이터는 각 가정의 홈 게이트웨이를 관리하는 사업자로 홈 게이트웨이에 대한 정보, 사용자 정보, 번들 관련 정보들을 관리한다. 홈 게이트웨이는 댁내망과 외부망의 경계선에 위치한다. OSGi 프레임워크는 자바 프로그래밍 언어의 플랫폼 독립성과 동적 코드 로딩 능력을 이용하여 소형 메모리 디바이스에 적합한 응용프로그램인 번들을 쉽게 개발하고 동적으로 배치할 수 있도록 한다[6]. 홈 게이트웨이에 배치된 여러 번들은 사용자가 원하는 서비스를 제공하며 사용자의 필요에 따라 오퍼레이터로부터 동적으로 설치 제거된다. 사용자는 Home User 와 Travel User 로 구분된다. Home User 는 하나의 홈 게이트웨이 에서 여러 서비스를 사용하는 사람이고, Travel User 는 각 홈 게이트웨이를 돌아다니면서 특정 서비스를 사용한다[2].

3. 접근제어 프레임워크

접근제어는 인증된 사용자에 의해 요청된 서비스의 수행가능 여부를 결정하는 과정이다. 접근제어를 위한 프레임워크는 그림 2 와 같다.

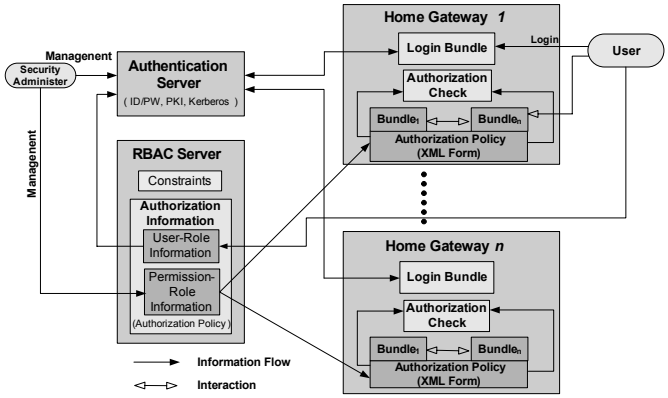

그림 2 접근제어 프레임워크 구조

각각의 홈게이트웨는 가정마다 분산되어 있다. 인증된 사용자가 서비스를 요청하면 OSGi 프레임워크의 권한부여 검사 기능은 XML 형태의 권한부여 정책을 참조하여 접근가능 여부를 판단한다. 권한부여 서버인 RBAC 서버는 모든 사용자들에 대한 권한부여 정보를 관리하며 각 홈 게이트웨이는 RBAC 서버의 권한부여 정보 중 해당 가정에 대한 권한할당 정보(Permission-Role Information)만을 복사하여 저장한다. 권한할당 정보는 권한부여 정책의 내용이 된다. 보안 관리자는 인증서버와 RBAC 서버를 관리하며 홈 게이트웨이 내부의 인증 번들은 별도의 인증 서버와 연동하여 인증 서비스를 제공한다.

권한부여 정책에서 사용자에게 특정 번들에 접근할 수 있는 권한을 명세하였다면 사용자는 번들이 제공하는 서비스를 사용할 수 있다. 이러한 권한부여 아키텍쳐는 server-pull 방식이 변형된 형태이다[7]. 즉 권한부여 정보가 권한부여 서버에 위치하지 않고 홈 게이트웨이에 번들과 같이 위치하게 된다. 이러한 구조로 가는 이유는 다음과 같다. 첫째. 각 가정에서 사용자의 서비스 요청이 있을 때 마다 권한부여 정보를 권한부여 서버에게 질의하는 것은 네트워크 트래픽을 고려 할 때 적당하지 않다. 둘째, 가정의 프라이버시에 관련된 정보를 전적으로 외부에 의존하는 것은 역시 바람직 하지 않다. 따라서 사용자는 자신의 집에

해당하는 권한부여 정책을 작성하고 관리하는 것이 필요하다. 그러나 사용자들은 권한부여 정책을 작성하고 관리할 능력이 없으며 사용자 편의성 측면에서도 좋지 않아 사용자들로부터 외면 당할 수 있다.

접근제어를 하는 과정에서 사용자의 프라이버시를 보호 하면서 사용자 편의성을 제공하는 방법은 사용자 할당(User-Role Information)은 사용자에 의해서 결정되게 하고 권한 할당(Permission-Role Information)은 오퍼레이터에 의해서 결정되는 것이다. 즉 오퍼레이터는 각 서비스들을 분석하고 적절한 역할을 정의하여 역할에 적합한 권한들을 할당해 놓으면 이는 프라이버시 문제하고는 상관이 없다. 그 다음 사용자는 자신이 어느 역할에 속할 것인가를 결정 함으로써 자신의 권한부여 정책을 직접 작성하지 않고 간접적인 방법으로 자신의 프라이버시를 보호하면서 권한부여 정책을 작성할 수 있다. 즉 사용자는 자신이 할당될 역할을 선택함으로 자신에게 적용되는 권한부여 정책을 선택할 수 있다. 접근제어의 융통성을 제공 하기 위하여 사용자가 원하는 경우 홈 게이트웨이에 복사된 권한부여 정책을 수정 할 수 있도록 한다. 이때 공공의 목적에 의해서 주로 Travel User 에 의해서 주로 사용되는 전기, 수도, 가스 검침 서비스 등은 수정하지 못하도록 해야 한다.

만일 사용자가 직접 접근제어 정책을 작성한다면 댁내에는 적은 수의 사용자와 제한된 자원이 존재 하므로 사용자와 서비스를 직접 맵핑 하는 ACL(Access Control List)과 같은 접근제어 방법을 사용할 수 있다 [7]. 즉, 대규모 환경에 적합한 RBAC 모델을 사용할 필요가 없다. 그러나 본 논문에서처럼 오퍼레이터에 의해서 관리 된다면 많은 사용자와 다양한 정보가전과 자동화 기기들에 대한 다양한 서비스들이 존재 함으로 RBAC 모델을 사용하는 것이 적합하다.

4. 사용자 관리 서비스

사용자 관리 서비스는 인증과 권한부여를 위한 서비스이다. 패키지 형태로 존재하며 주로 오퍼레이터에 의해서 사용되며 서비스 번들도 이 패키지를 임포트 하여 사용 할 수 있다. 홈 네트워크 환경에서 사용자와 서비스 사이의 권한부여를 관리하는 작업은 많은 시간이 소요되고 오류가 일어날 가능성이 많음으로 이들을 효과적으로 관리하기 위한 관리 서비스가 필요하다.

기존의 OSGi 스펙에 명세된 사용자 관리 서비스의 스펙은 다음과 같은 문제점을 가지고 있다.

1)접근제어를 위한 권한(Permission)과 접근대상(Object)에 대한 언급이 없어 접근대상과 권한을 명확히 정의하지 않아 실제 적용하는데 많은 어려움이 있다.

2) 접근 주체(Subject)가 접근 대상에 대한 접근권한을 가지고 있는지를 확인하는 Authorization Check 기능이 없다.

3) 접근의 주체와 대상이 구분되어 관리되지 않는다.

4) Role 의 개념은 사용하지만 RBAC 의 Role 과는 상이한 개념으로 사용되고, Role, Group 이 혼재 되어 명확하게 정의 되지 않아 효과적인 권한부여 정보관리 어려움

5) 권한부여 정보 관리를 위한 사용자, 번들, 서비스, 역할 등에 대한 검색기능 부족하여 보안관리자가 권한부여 정책작성을 위한 정보를 효과적으로 획득할 수 없다.

6) 구체적으로 권한부여 정책의 형태에 대한 언급 이없다.

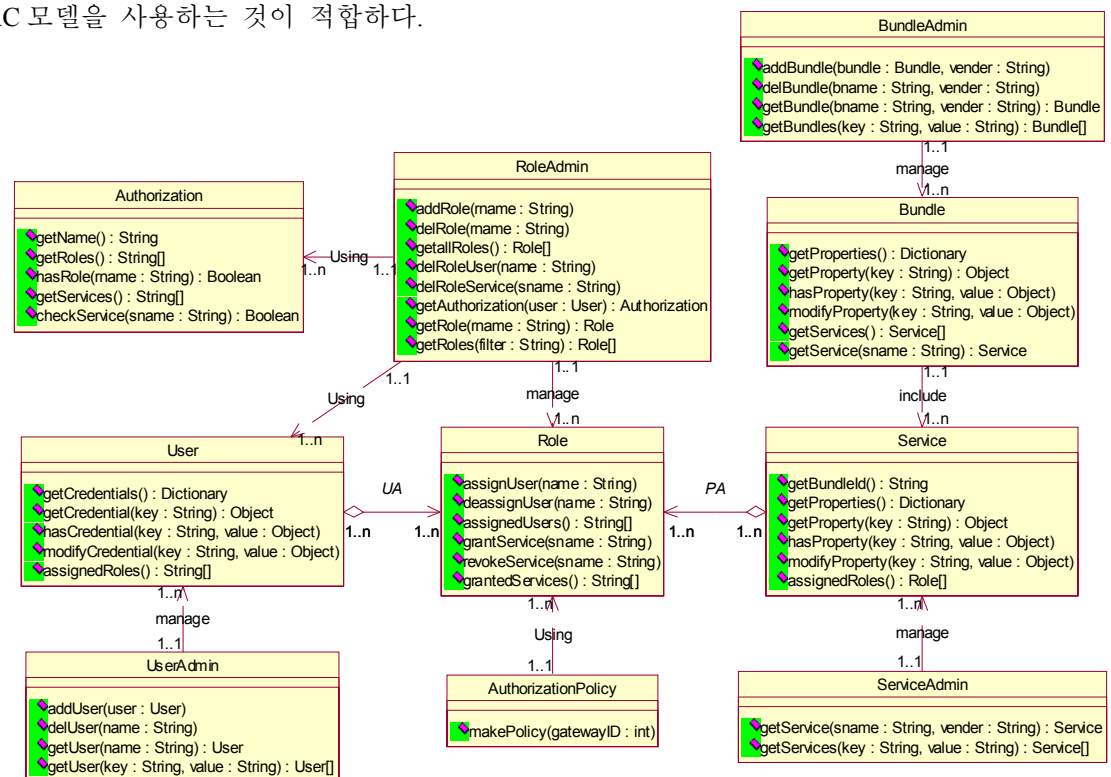

그림 3 사용자 관리 서비스 클래스 다이어그램

위에서 언급한 문제점들을 해결하기 위한 보완된 사용자 관리 서비스의 클래스 다이어그램은 그림 3 과 같다. 기존의 UserAdmin 인터페이스의 기능을 User, Bundle, Service, Role 등으로 세분화하였고 각각에 대해서 관리 인터페이스를 추가하였다. 또한 기존의 스펙에 명시된 인터페이스를 기반으로 하여 Role 과 RoleAdmin 인터페이스를 RBAC 모델을 지원하는 형태로 보완하였다. 표 1 은 각 인터페이스에 대한 세부적인 설명이다.

표 1 사용자 관리 서비스를 위한 인터페이스

인터페이스	내용
User	사용자의 인증에 관련된 기밀정보들을 관리한다. 원하는 기밀 정보를 획득하고 수정한다. .
UserAdmin	사용자를 생성, 삭제, 검색한다. User 객체는 사용자 생성과정에서 사용자 기밀 정보를 제공한다.
Bundle	번들과 관련정보를 관리한다. 번들은 권한부여 과정에서 접근의 대상이 되는 서비스를 담고 있는 컨테이너이다.
BundleAdmin	번들에 대한 정보를 추가, 삭제, 검색한다. 다른 서비스 제공자에 의해서 작성된 동일 이름의 번들이 존재할 수 있음으로 검색시 밴더의 이름이 필요하다
Service	접근대상이 되는 서비스와 관련 정보를 관리한다. 사용자가 서비스에 접근할 수 있는 권한을 가지면 서비스를 이용할 수 있다.
ServiceAdmin	서비스는 보안 관리자에 의해서 생성될 수 없음으로 검색의 기능만을 가진다
Role	역할과 관련정보를 관리한다. 역할 객체에 할당된 사용자에 대한 정보(User Assignment)와 서비스에 대한 정보(Permission Assignment)를 같이 가지고 있음으로 사용자가 멤버로 있는 역할을 파악하면 그 사용자가 사용할 수 있는 서비스들을 파악할 수 있다.
RoleAdmin	역할을 추가, 삭제, 검색한다. 보안 관리자는 보안요구사항 변동에 따라 새로운 역할을 생성하거나 삭제해야 한다
Authorization	인증된 사용자의 신원과 그 사용자가 가지고 있는 역할을 파악하여 최종적으로 그 사용자가 특정한 서비스를 사용할 수 있는지를 결정한다.
AuthorizationPolicy	데이터베이스안의 권한부여 정보를 사용하여 홈 게이트웨이에 적합한 권한부여 정책을 작성한다.

홈 게이트웨이의 권한부여 정책은 RBAC 서버에서 퍼미션 할당 정보의 부분집합을 XML 형태로 표현한 것이다. Authorization 인터페이스의 getRole()을 통하여 인증된 사용자가 소속된 역할들을 파악하고, checkService() 메소드를 통하여 XML 기반의 권한부여 정책에 접근하여 파악된 역할들이 사용자가 접근하려는 서비스에 대한 권한을 가지고 있는지를 파악한다. 권한부여 정책에 접근하기 위해서는 SAX(Simple API for XML), DOM(Document Object Model) 등이 사용될 수 있다. 그림 4 는 권한부여 정책의 DTD(Document Type Definition)를 나타낸 것이다.

```
<?xml version=’1.0’ encoding=’euc-kr’?>
<!ELENENT authorization-policy (role+) >
<!ATTLIST authorization-policy name CDATA #REQUIRE >
    <!ELENENT role ( bundle*) >
    <!ATTLIST role name CDATA #REQUIRE >
        <!ELENENT bundle (service+) >
        <!ATTLIST bundle name CDATA #REQUIRE >
            <!ELENENT service (#PCDATA) >
```

그림 4 권한부여 정책의 DTD

5. 결 론

OSGi 서비스 플렛폼의 사용자 관리 서비스 부분은 권한부여 정책 관리와 운영을 위한 프레임워크가 제시 되지 못했고 사용자 접근제어 부분은 주요 핵심 기능들이 누락 되었다. 따라서 본 논문에서 OSGi 서비스 플렛폼이 운영되는 홈 네트워크 환경에서 사용자 접근제어를 위한 RBAC 기반의 권한부여 정책 관리 프레임워크와 UML 을 이용하여 설계된 진보된 사용자 관리 서비스를 제시하였다. 이들은 홈 네트워크 환경에서 안전한 사용자 접근제어를 가능하게 하여 사용자들이 안전하게 제공 서비스를 사용할 수 있게 한다.

참고문헌

[1] OSGi "OSGi Service Platform Release 3 Specification" http://www.osgi.org/

[2] 전경석, 문창주, 박대하, 백두권 “OSGi 서비스 플랫폼 환경에서의 사용자 인증 메커니즘”, 정보과학회논문지, 제 9 권 제 3 호

[3] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink , Charles E. Youmank, Role-Based Access Control Models , IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[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, July 26-27, 2000.

[5] Chang-Joo Moon, Dae-Ha Park, Soung-Jin Park, Doo-Kwon Baik, Symmetric RBAC Model that Takes the Separation of Duty and Role Hierarchies into Consideration, Computers & Security, 23/2, pp. 126-136

[6] 김영갑, 문창주, 박대하, 백두권, “OSGi 서비스 플랫폼 환경에서의 서비스 번들 인증 메커니즘의 검증 및 구현”, 정보과학회논문지, 제 31 권 제 1 호

[7] DAVID F. FERRAIOLO, Role-Based Access Control, Artech House, Cpmputer Security, 2003, Ch1