

ULSA기반 사용자 인증과 접근제어 모델 제안

최민석⁰ 한동윤 김경석

부산대학교 컴퓨터 공학과 부산대학교 컴퓨터 공학과 부산대학교 정보컴퓨터공학부
 mschoi@asadal.pusan.ac.kr dyhan@asadal.pusan.ac.kr gimgs0@asadal.pusan.ac.kr

The ULSA Model proposal which supports User Authentication and Authorization

Min-suk Choi⁰ Dong-yun Han Kyong-sok Kim

Dept of Computer Engineering, Pusan national university

Dept of Computer Engineering, Pusan national university

Dept of Computer Science and Engineering, Pusan national university

요 약

현재 인터넷의 발전으로 가정집으로 네트워크 환경이 구축됨에 따라 홈 네트워크 분야가 이슈로 등장하였다. 홈 네트워크에는 여러 분야가 존재하지만 그중에서도 중요한 요인 중 하나가 바로 사용자 인증과 접근제어 메커니즘이다. 일반적인 사용자 인증에는 사용하고자 하는 사람이 인증된 사람인지 아닌지 판별하여 인증된 사용자에게는 다양한 서비스가 제공되지만 그렇지 않은 사용자에게는 접근이 제안되는 방식이 대부분이었지만 본 논문에서는 사용자 인증과 함께 레벨링이라는 과정이 추가되어 새로운 구조를 제안하며, 인증된 사용자라 할지라도 차등된 서비스를 제공받게 된다. 그리고 서비스를 객체화하여 세분화 정의함으로써 사용자가 보다 정확하고 명확하게 서비스에 접근할 수 있으며 편의성 또한 보장된다. 이 모델이 바로 본 논문에서 제안하는 ULSA기반 접근제어 모델이다. 본 모델은 비 인증 사용자로부터 안전할 뿐만 아니라 인증된 사용자들도 중요도가 높은 서비스는 제안함으로써 더욱 강화된 안전성을 보장 받을 수 있으며 서비스 객체를 세분화 정의하여 서비스 사용의 퀄리티를 높일 수 있다.

1. 서 론

우리나라에서 급속도로 인터넷의 발전과 더불어 보급이 널리 퍼짐에 따라 다양한 형태의 네트워크 환경이 구축되었다. 그러한 다양한 네트워크들이 더 효율적으로 구축되고 인간을 위한 휴머니즘이 등장하면서 최근에는택내까지 네트워크 환경이 구축되어 홈 네트워크 분야가 크게 대두되고 있다. 기본적으로 홈 네트워크는택내 정보가전기기를 연결하는 residential network 와 wireless access network 를 연결함으로써 사용자가 언제, 어디에서 가정 내에 무엇이든 연결해서 사용할 수 있는 유비쿼터스 홈 네트워크가 도래되었다. 홈 게이트웨이가택내 망과택외 망을 연결시켜줌으로써 이 모든 것들이 가능해지며, 점차 홈 게이트웨이의 역할이 핵심 기술로 발전될 전망이다.

택내 홈 네트워크를 연결하는 방법에는 여러 가지가 존재한다. 유선으로 연결하는 방법도 있고, 무선으로 연

결하는 방법도 있다. 표1에 나와 있듯이 이러한 많은 유무선 네트워크 기술들을 기반으로 다양한 장비들이 서로 다른 하드웨어 플랫폼과 OS, 또는 프로토콜을 바탕으로 동작하게 된다.

표1 홈 네트워크 유무선 표준

종류	표준	전송속도	특징
유선	HomePNA	10Mbps	전화선 이용
유선	HomePlug	10Mbps	전력선 이용
무선	IEEE1394	1,600Mbps	시리얼 버스기술
무선	Bluetooth	1Mbps	10m 이내 무선
무선	HomeRF	11Mbps	50m 이내 무선

이러한 이질적인 환경에서 동작하는 다양한 장비들을 통합하기 위해 동일한 형태의 API 형식을 제공하는 미들웨어 분야가 등장하였다. 이러한 미들웨어 분야는 이기종 정보가전의 통합과 제어를 담당하였다. 표2에서는 다양한 미들웨어 분야를 보여준다.[1]

표2 미들웨어 표준

종류	특징
HAVi	IEEE1394 기반으로 표준
Jini	Java 기반 분산 환경 홈 네트워크 연결
UPnP	IP기반, PC중심의 P2P 방식
LonMark	홈, 빌딩 오토메이션, 홈 네트워크 구축
OSGi	Java 기반 개방형 서비스 플랫폼 제공

홈 네트워크 구축 시 고려해야할 사항 중 하나가 바로 사용자 인증과 인증에 따른 접근제어이다. 우선택내의 정보가전기기를 사용하는 주체가 인증된 사람인지 아닌지 필터링 되어야하며, 인증된 사람이라고 하더라도 사람에 따라 서비스의 차등이 있어야 한다. 예를 들어 같은 사용자라 하더라도 연령에 따라 접근을 제안할 수 있으며, 중요한 서비스일 경우 직접적인 관련이 적은 사용은 제안해야하는 경우가 있다. 하지만 그러한 사항을 고려한 정책이 명확히 정의되지 않고, 사용자에게 맡겨두고 있는 실정이다. 본 논문에서는 사용자의 인증과 인증에 따른 차등된 서비스 접근제어를 모델로 제안함으로써 서비스 번들 사용에 편의성 및 정확성과 명확성을 제공한다.

본 논문의 구성은 2장에서는 연구배경 및 관련연구에 대하여 언급하고, 3장에서는 본 논문에서 제안하는 사용자 인증과 접근제어의 전체적인 모델의 구조에 대해서 설명하며 4장에서는 결론과 향후 연구진행에 대해 언급할 것이다.

2. 관련연구

2-1. OSGi

OSGi(Open service gateway initiative)의 서비스 프레임워크는 자바 언어를 바탕으로 하여 자바 플랫폼과 동적 코드를 이용하여 응용프로그램 개발을 쉽게 할 수 있다. 번들(bundle)이라는 최소 작업 단위로 여러 응용 프로그램을 적당히 묶어서 관리하며, 서비스 번들의 라이프 사이클 관리가 가능하여 시스템과 독립적으로 서비스의 갱신이 용이하다. OSGi 프레임워크 환경에서 서비스는 게이트웨이 관리자와 번들의 라이프 사이클에 따라서 동적으로 서비스 게이트웨이에 배치되며 다른 서비스 번들과의 상호 작용도 일어난다. 이러한 특성으로 인해 네트워크상에서 인증되지 않은 오퍼레이터에 의하여 서비스 게이트가 공격을 받을 수 있다. 그리고 인증된 오퍼레이터라고 하더라도 특정 서비스를 제안한

다는 것이 어려운 현실이다.[2]

현재 OSGi 에서는 PKI(Public Key Infrastructure) 기반 서비스 번들 인증 메커니즘을 이용하고 있다. 하지만 본 논문에서는 단순한 키 인증뿐만 아니라 적당한 숫자 값이 나오게 되어 접근등급이 적용하게 된다.

가. OSGi 프레임워크 구조

OSGi는 홈 네트워크 기술과 독립적으로 가정 내의 홈 네트워크 또는 정보가전 기기에 접근할 수 있도록 구조를 정의함으로써 액세스망을 거쳐서 다중의 서비스를 홈 네트워크와 정보 가전기기에 전달할 수 있는 규격을 만들고 있는 표준화 단체로써, 거의 모든 가정용 네트워킹 표준을 지원하도록 설계되었다. 이 표준은 자바 언어를 기반으로 홈 네트워크 유무선 표준을 통합하기 위해 여러 프로토콜들을 지원한다. 그림1에서는 OSGi 서비스 플랫폼의 전체적인 구조를 나타낸다.

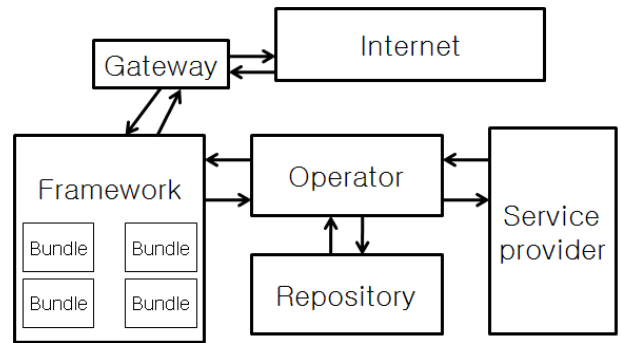


그림1-1 OSGi 플랫폼 구조

- Service provider : 서비스를 개발하고 번들을 제작하고 제공하는 역할.
- Operator : 서비스 게이트웨이와 서비스 번들을 관리하는 역할
- Gateway : 정보 단말과 유무선 인터넷을 연결하는 역할.[3]

나. OSGi 인증 메커니즘

OSGi에서는 공개키 기반 보안구조를 가지고 있다. 인증기관은 인증서를 배포하는 역할을 하며 인증서와 인증된 키로 사용자 인증을 하여 무결성과 기밀성을 보장한다. 서비스 게이트웨이는 오퍼레이터와 상호 인증을 원하고 서비스 번들 인증에 필요한 비밀키를 생성한다. 서비스 게이트웨이와 오퍼레이터에서 난수값을 생성하여 키를 저장한다. 이 키를 이용하여 암호화, 복호화를 실행함으로써 사용자 인증을 거쳐서 서비스를 제공받게

된다.[4]

다. 접근제어

접근제어는 사용자가 인증서버와 인증과정을 거친 후 어플리케이션에 접근 할 때 이루어지며, 다음과 같은 구조가 일반적이다.

- User-pull 구조 : 사용자가 초기에 한 번 인증을 받으면 유효가 만료될 때까지 계속 사용가능.

- Server-pull 구조 : 사용자가 어플리케이션을 사용하고자 할 때 사용자의 권한부여를 서버에게 요청한다.[5]

- 고려사항 : 사용자가 초기에 혹은 어플리케이션 사용할 때, 인증 후에 서비스에 대한 접근을 할 때 모든 사용자가 모든 서비스에 대한 접근의 차등을 준다. 나이에 따른 차등을 줄 수 있고, 서비스의 중요도에 따라서 차등을 줄 수 있다.

3. ULSA(User Leveled Service Access) 기반 모델

ULSA(User Leveled Service Access)기반 모델은 사용자 인증뿐 아니라 인증된 사용자에 따라서 차등된 권한을 부여함으로써 접근제어가 이루어지며, 미리 정의된 객체들의 관계가 등급별로 연결되어 있어 보다 명확하게 서비스를 제공 받을 수 있다. 위 모델은 크게 3가지 단계로 나누어지며 사용자가 서비스 요청 시 인증, 그리고 사용자 등급을 부여하는 레벨링, 마지막으로 레벨링 후에 부여받은 등급으로 서비스를 제공받게 된다.

3-1 인증

ULSA기반 모델은 기본적으로 대칭키와 비밀키를 모두 사용한다. 각 사용자들은 OP와 대칭키를 공유하고 있으며 OP는 개인키를 가지고 있고 공개키를 공개하고 있다. 사용자는 서비스 요청 시 개인 정보를 자신의 대칭키로 암호화한다. 대칭키로 암호화된 정보는 OP의 공개키로 다시 암호화해서 OP로 보내지게 된다. OP는 전달 받은 정보를 자신의 개인키로 복호화하고 다시 사용자의 대칭키로 복호화 한다. 복호화된 사용자 정보를 바탕으로 레벨링 작업이 이루어지게 된다. 사용자는 레벨링 후 정해진 등급에 따라 차등된 서비스를 제공받을 수 있다. 위 과정을 요약해보면 다음과 같다.[6]

- KeyOP, KeyOP' : OP의 공개키와 개인키
- Key_OP_Ur : 사용자와 OP간 대칭키

위 정보로부터 사용자 인증을 위한 암호화, 복호화 작업을 그림으로 간단하게 도식하면 아래 그림과 같다.[7]

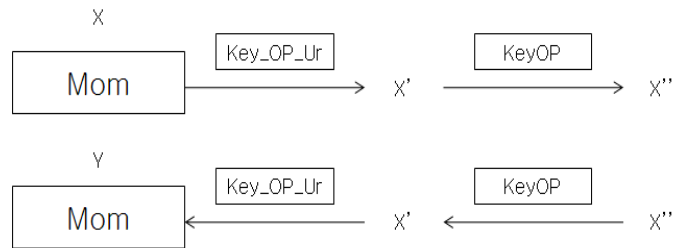


그림 3-1 사용자와 OP간 인증 과정

사용자는 사용자 ID와 기본 정보를 입력하고 그 값을 X라고 두면, X를 사용자와 OP간 대칭키로 암호화한 뒤 다시 OP의 공개키로 암호화해서 OP로 전달된다. OP는 사용자와 반대로 자신의 개인키로 복호화하고 저장하고 있는 대칭키로 복호화 시켜서 사용자 ID를 추려낸 결과값의 Y를 생성하고 사용자 인증을 마치게 된다.[8]

3-2 레벨링

기존의 홈 네트워크 인증 방식에서는 사용자가 인증만 거친다면 모든 서비스를 제공받을 수 있었지만, 본 논문에서 제시하는 ULSA기반 모델은 인증된 사용자라 할지라도 서비스의 종류에 따라 접근제안을 두는데 이것이 바로 레벨링이라는 개념이다. 레벨링은 인증과정에서 얻어진 Y값을 가지고 등급을 나눈다.

사용자 등급은 홈 네트워크 관리자에 의하여 미리 정의한다. OP에서 사용자 ID별로 스키마가 구축되어 있고, 관리자는 인증된 사용자의 ID와 스키마를 비교한다. 예를 들면 관리자 자신의 ID가 Mon이고 사용자 인증을 거쳐 나온 사용자 ID와 스키마를 비교하여 Mon이 1등급에 속하면 그 등급에 맞는 서비스를 이용할 수 있다. 이러한 방식으로 홈 네트워크 관리자는 사용자 ID에 맞는 등급을 지정하여 사용자가 인증을 거치고 난 후 접근 권한을 부여하게 만드는 것이다. 아래 표3은 사용자의 ID로 사용자 정보가 저장되어 있는 스키마를 보여준다.

* 사용자 정보 : ID

- Ur : 사용자
- ID : 사용자 ID

표3 사용자 정보별 등급 스키마

순서	사용자 ID	사용자 등급
1	Mom	1
2	Far	1
3	sun1	2
4	jangki	3
5	bi	2
6	gum	3
...

사용자는 인증 과정을 거쳐서 나온 자신의 ID로 사용자별 등급 스키마에 접근을 하여 자신의 ID에 대응되는 등급을 부여받는다. 부여받은 등급으로 그림 3-2의 접근 등급의 원칙에 따라 자신의 등급에 맞는 서비스에 대한 접근을 함으로써 원하는 서비스를 등급에 맞게 제공받을 수 있다.

- 1등급 : 접근 가능하고 사용가능.
- 2등급 : 접근 가능하지만 부분 사용 가능.
- 3등급 : 접근 불가.

그림 3-2 접근 등급

3-3 User-pull-level 구조

본 논문에서 제안하는 ULSA기반 모델은 서두에도 언급했던 것과 같이 인증, 그리고 레벨링과 레벨링에 따른 서비스 접근 권한을 부여하고 자신의 등급에 맞는 서비스를 이용하기 때문에 새로운 구조를 제안한다. 새로운 구조는 기존의 User-pull 구조를 확장하여 레벨링 과정이 추가되었다.[9][10]

유저는 OP와의 인증과정을 거친 후에 레벨링을 한다. 레벨링을 통해 등급을 부여받은 유저는 부여받은 레벨을 통해 서비스에 접근하는 방식이다. User-pull 구조와 마찬가지로 초기에 한 번의 인증만 거치면 서비스를 원하는 만큼 사용할 수 있으며, 등급이 맞는 서비스만 접근할 수 있다. 아래그림은 User-pull 구조에 레벨링 작업이 추가된 User-pull-level 구조를 보여준다.

3-4 서비스 객체 정의

OP에서 레벨링으로 얻은 등급을 가지고 서비스에 접근을 하기 위해서는 서비스마다 등급에 따라 사용자가 접근할 수 있도록 서비스 객체에 대한 정의가 필요하다.

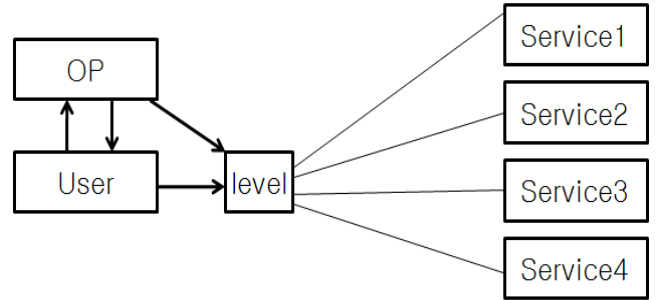


그림 3-3 User-pull-level 구조

서비스 객체에 대한 정의가 명확하지 않으면 사용자들은 자신의 등급으로 어떤 서비스를 사용가능한지 수동적으로 알아야하며 불편함을 느낀다. 그러므로 각 등급에 따라 접근할 수 있는 서비스 객체들을 세분화하여 나타낸다면 정확하고 명확하게 서비스에 대한 접근을 사용자가 편리하게 할 수 있다. 아래 그림은 서비스들을 객체로 정의하고 세분화하고 있는 트리 구조이다.

- root : 홈네트워크
- 1차노드 : 가전제품, 생활용품, 전등
- 2차노드 : TV, PC, 세탁기, 전자레인지, 금고..
- 3차노드 : TV채널, 세탁기 작동...

위 박스에 각 서비스 객체들을 루트에서부터 노드별로 세분화하여 정의하였고 루트로부터 각 노드들은 상위노드로부터 점차적으로 노드가 뺀어져간다.

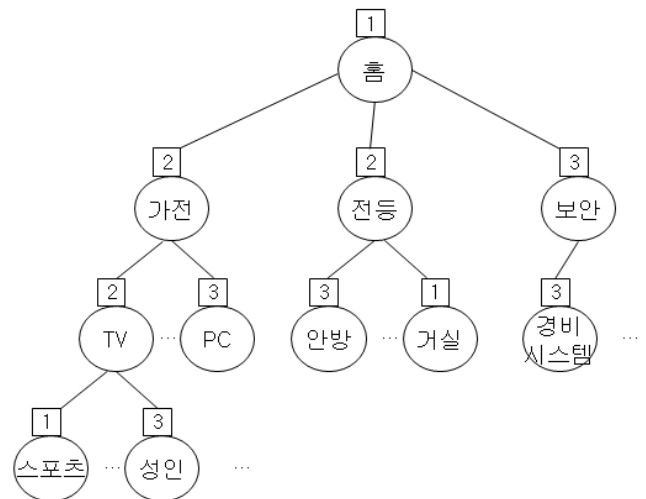


그림 3-4 서비스 객체 세분화

그림 3-4와 같이 트리구조로 나타냄으로써 객체를 정의 할 수 있으며, 사용자가 등급에 따라 서비스를 받을 수 있게 된다.[11]

사용자는 OP로부터 등급을 부여받게 되면 우선 루트로 접근을 한다. 루트가 1등급으로 되어 있어 접근이 가능하며, 원하는 서비스 객체에 접근하게 된다. 만약 사용자가 2등급을 부여받고 TV의 스포츠 채널을 보려고 한다면 사용자는 루트와 가전모두 접근 가능하며, TV에는 스포츠 채널이 1등급이라 시청이 가능하다. 하지만 성인 채널은 3등급이라 불가하며, 루트에서 보안 역시 접근조차 할 수 없다. 이렇게 부여받은 등급과 미리 정의된 서비스 객체를 사용자들이 이용함으로써 안전성과 명확성, 편의성이 제공되는 것이다.[12]

4. 결론 및 향후 연구과제

본 논문에서는 홈 네트워크에서 사용자 인증과 인증 후 접근제어 및 권한제어를 위한 모델을 제안하였다. 키 알고리즘으로 사용자 인증을 하고 추가 작업으로 레벨링을 제안하였으며 레벨링으로 사용자 등급을 정하였다. 그리고 등급에 따라 사용자가 정확하고 명확하게 서비스를 사용할 수 있도록, 서비스들을 객체로 정의하고 서비스 객체들을 사용자 등급에 맞게 세분화하였다.

본 논문에서 제안하는 ULSA기반 모델은 사용자 인증 후 레벨링으로 서비스 접근제어를 하여, 인증된 사용자라 할지라도 나이와 서비스를 사용하는 주체에 따라 다른 등급을 가지고 서비스에 접근함으로써 보다 안전하고 내부 보안문제도 강화할 수 있다. 그리고 사용자 등급에 따른 서비스를 객체화 하여 정의함으로써 정확하고 명확하게 서비스를 사용할 수 있고, 사용자들에게 서비스 객체의 사용에 대한 편의성을 제공해줄 수 있다.

향 후 연구과제로는 본 논문은 모델 제한하는 논문으로 아직 구현단계에는 이르지 못하였으나 앞으로 보완점을 찾아 계속 연구하여 구현단계에 이르러 성능평가까지 이루어져 하는 것이 마지막 과제이다.

참 고 문 헌

[1] 배창석, 이진우, 김채규 “홈서버 기술 현황 및 기술 개발 방향”, 정보처리학회지 제 8권 1호 2001. 01
 [2] OSGi "OSGi Service platform Release 3 Specification" <http://www.OSGi.org/> 2006
 [3] 김영갑, 문창주, 박대하, 백두권 “OSGi 서비스 플랫폼 환경에서 서비스 번들 인증 메커니즘의 검증 및 구현”, 정보과학회 논문지 제 31권 제 1호 2004.2
 [4] 최훈일, 정창훈, 장영건 “원격관리서버 기반의 홈네트워크 사용자 인증 및 접근제어 시스템 설계 및 구현”, 정보처리학회 논문지 제 14-D권 제 5호 2007.8

[5] David F. Ferraiolo, Role-Based Access Control, Artech House, Computer Security, 2003.
 [6] Marc Branchaud, "A survey of public key Infrastructures," Department of computer science, McGill University, Montreal, 1997
 [7] Jone Clark, Jeremy Jacob, "A Survey of Authentication Protocol Literature: Version 1.0," University of York, Department of computer science, November 1997.
 [8] OSGi, "RFC 18-Security Gateway Specification" Draft, <http://www.osgi.org/member>, 2001.
 [9] Joon S. Park and Ravi S. Sandhu, smart certificates: Extending X.509 for secure attribute service in the web, 22nd National Information Systems Security Conference (NISSC), Crystal City(Virginia), pp. 337-348, 1999
 [10] Joon S. Park and Ravi S. RBAC on the Web by smart cerificates, 4th ACM Workhop on Role-Based Access Control (RBAC), pp. 1-9, 1999
 [11] 김학수, 최윤호, 이승미, 손진현 “지능적인 홈네트워크 서비스 제공을 위한 사용자 패턴 분석 기법”, 정보과학회 논문집 Vol.34, No.2 2007.
 [12] 조은애, 문창주, 백두권 “OSGi 서비스 플랫폼에서 RBAC 기반의 사용자 접근제어 프레임워크”, 정보과학회 논문지 제 34권 제 5호 2007.10