

원격관리서버 기반의 홈네트워크 사용자 인증 및 접근제어 시스템 설계 및 구현

최 훈 일[†] · 정 창 훈^{**} · 장 영 건^{***}

요 약

현재까지의 개발된 홈네트워크 사용자 인증 및 접근제어 기술은 각 가정의 홈네트워크 내에 보안 시스템이 위치하여, 홈구성원이 직접 보안 관리를 하는 형태가 대부분이다. 이런 형태는 비전문가인 홈구성원이 보안 관리를 함으로써, 보안상의 취약점이 발생할 가능성이 매우 높으며, 보안 시스템이 각 가정의 홈네트워크 내에 위치함으로써 시스템 구축 비용이 발생하며, 보안 시스템의 유지 보수와 관리에 많은 취약점이 발생할 수 있다. 이에, 본 연구에서는 가격, 서비스의 유연성에서 경쟁력이 있고, 네트워크를 보유한 개인의 전문적 지식과 작업을 요구하지 않고, 아파트 단지, 대형 건물과 같은 집단 주거 형태에 적합한 원격관리서버 기반의 홈네트워크 사용자 인증 및 접근제어 시스템을 설계하고 구현하였으며, 정보가전용 데모 시스템을 제작하여 시험하였다. 시험결과 인증과 접근제어 기능이 안정적으로 동작하였다.

키워드 : 홈네트워크, 원격관리서버, 사용자 인증, 접근제어, OSGi

Design and Implementation of User Authentication and Authorization System based on Remote Management Server for Home Network

Hoon-Il Choi[†] · Chang-Hoon Jung^{**} · Young-Gun Jang^{***}

ABSTRACT

The user authentication and authorization in the current home network system almost works at home and home users, sometimes novice, should manage the system directly. This situation can make much of troubles, sometimes cause some security problems. Moreover, the system costs high to build up, demands special user knowledge to maintain.

In this paper, we propose the user authentication and authorization system based on remote management server to solve the problems, designed and implemented the system. To verify the system performance and function, we built a demo system for information appliances. The results of the test, the authentication and authorization function works well and reliably.

Key Words : Home Network, Remote Management Server, User Authentication, Authorization, OSGi

1. 서 론

IT 기술의 급속한 발달과 초고속망을 통한 인터넷 보급에 힘입어, 기업이나 공공기관의 사무실 중심으로 구축되던 네트워크 환경이 가정 내의 전자기기로까지 확산되어 가면서 홈네트워크 시장에 대한 관심이 높아지고 있으며, 정부는 2007년까지 1000만 가구에 디지털 홈을 구축하겠다는 계획을 발표한 바 있다. 최근에는 홈네트워크 시장이 2007년까지 22조 2천 억원에 달하는 생산유발 효과와 16만 명 규모의 고용창출 효과가 발생할 것이라는 전망을 내어 놓고 있을 만큼 홈네트워크의 성장성과 파급 효과는 크다고 할 수 있다[1].

이러한 홈네트워크 시스템의 핵심은 네트워크를 가정 내 각종 기기까지 연결시켜 원격지에서도 가정 내의 각종 기기를 제어 및 모니터링을 할 수 있도록 하여 생활의 편리를 도모하도록 하는 것이다. 홈네트워크 시스템에서는 기존 네트워크 환경에서 문제가 되고 있는 해킹, 바이러스, 개인정보 침해, 불건전 정보 등의 보안 문제가 그대로 나타나게 되며, 네트워크에 연결된 기기들이 단순한 기기가 많아, 새로운 보안문제가 나타날 수도 있다. 이러한 문제는 시장 활성화를 저해하는 주요 기술적 요인이 되고 있으며[2], 정보보호 및 보안에 대한 필요성이 강하게 대두되고 있다[3-5]. 특히, 홈네트워크 시스템은 네트워크를 통해 가정 내의 정보가전이나 헬스케어기기를 조작할 수 있기 때문에 인증되지 않은 사용자의 접근을 차단하고, 인증된 사용자라 할지라도 사용자의 특성에 따라 기기의 사용을 제한하여 부적절한 기기의 사용으로 인한 안전 피해와 생체정보의 유출 등을

[†] 준 회 원 : 청주대학교 컴퓨터정보공학과 박사과정

^{**} 정 회 원 : 주식회사 에스티 대표이사

^{***} 정 회 원 : 청주대학교 컴퓨터정보공학과 부교수

논문접수 : 2007년 1월 19일, 심사완료 : 2007년 4월 20일

막을 수 있도록 하여야 한다. 예를 들어, DTV를 통해 VOD 서비스의 사용할 경우, 인증된 사용자가 어린이일 경우, 성인 채널은 볼 수 없도록 하거나, 가스 제어 등의 위험 요소에 대한 사용 권한을 제한하도록 하는 기능이 필요하다.

현재까지 홈네트워크의 보안을 위하여 불법 침입에 대한 일차적인 대응을 위한 Firewall, VPN 등의 기능이 탑재된 홈게이트웨이의 개발이 가장 많이 이루어져 있다[6-7]. 안전한 홈 서비스를 제공하기 위해서는 홈 네트워크 자원 및 서비스에 대한 접근제어 및 인증 기능이 제공되어야 하며, 국내에는 ETRI, 안랩유비웨이, 이니텍, 소프트포럼 등이, 국외에는 MicroSoft, CablesLabs, NTT 등에서 기술 및 제품들이 개발되고 있다. 그러나, 현재까지의 기술은 각 가정의 홈네트워크 내에 보안 제품이 위치하며, 홈구성원이 직접 관리하는 형태가 대부분이다[7].

본 연구에서는 비전문가인 홈구성원이 보안 관리를 함으로써, 발생할 수 있는 보안상의 취약점과, 보안 기술이 각 가정의 홈네트워크 내에 위치함으로써 발생하는 비용 문제 등을 해결하고, 아파트 단지, 대형 건물과 같은 집단 주거, 업무 공간에 적용하기 적합한 원격관리서버[8]를 기반으로 하는 사용자 인증 및 접근제어 시스템을 설계하고 구현하였다.

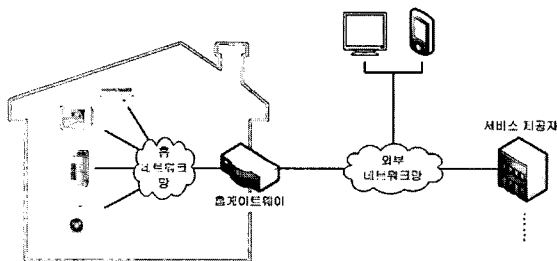
2. 홈네트워크 시스템과 인증 및 접근제어

2.1 홈네트워크 시스템

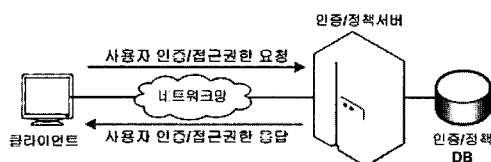
일반적인 홈네트워크 시스템은 (그림 1)과 같이 맥내의 정보기기들은 홈게이트웨이를 통해 외부 네트워크망과 연결되어 송수신이 이루어지며, 맥내에서는 홈네트워크망을 통해 송수신이 이루어지며, 홈네트워크망과 외부 네트워크망의 연결은 홈게이트웨이를 통해 이루어진다. 맥외에서는 휴대폰, PDA, 컴퓨터 등의 네트워크가 가능한 장치를 통해 맥내의 정보기기들을 제어할 수 있다[9].

2.2 일반적인 사용자 인증/접근제어

일반적인 네트워크 시스템에서의 사용자 인증과 접근제어



(그림 1) 일반적인 홈네트워크 시스템 구조



(그림 2) 일반적인 네트워크 시스템의 사용자 인증/접근제어

처리 방법은 (그림 2)와 같이 사용자를 검증할 사용자 인증 정보와 접근제어 권한을 부여하기 위해 접근제어 정책 등의 데이터가 필요하며, 이 데이터는 DB와 같은 저장소에 저장된다. 또한, 사용자의 인증 요구를 처리하기 위한 인증 서버, 접근제어 처리를 위한 정책 서버 등이 필요하며, 이 서버들은 사용자 인증 및 접근제어 요청에 대해 데이터가 저장된 DB와 연동하여 처리하게 된다.

2.3 홈네트워크 사용자 인증/접근제어

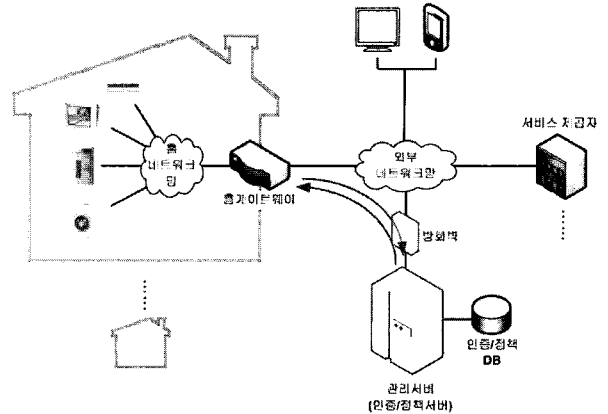
홈네트워크를 구성하는 맥내의 다양한 장치들은 전력선, 센서네트워크, 무선인터넷 망 등의 다양한 네트워크로 연결될 수 있다. 센서네트워크의 경우에는 데이터를 수집하여 전달하는 센서노드는 초소형, 빈번한 데이터 이동, 제한적인 계산능력 및 저장능력 그리고 배터리 전력사용이라는 특성을 갖고 있어, 전통적인 공개키 기반의 보안도구를 사용할 수 없어서 안전한 통신을 위한 키 갱신 방식에 대한 연구가 이슈가 되고 있다[10, 11]. Tine 등은 특정 응용에 적합한 정책을 지원하기 위하여 기존의 시스템이 접근제어를 지원하는 API를 제공하는 데 반하여 모듈화된 접근제어 서비스를 제안하였다[12]. 접근제어에 사용되는 다양한 정책들을 수용하기 위하여 Duan 등은 조직적 접근제어 정책, 광역적 접근제어 정책, 지역적 접근제어 정책의 세가지 수준으로 정책을 구분하여 접근하고 있으며[13], Elisa 등은 다중정책 접근제어 시스템의 구조와 확장이 가능한 규격 언어를 제안하였다[14]. 정재학은 기기 정비 서비스는 서비스 사용 중의 문제발생, 기능 개선, 문제 보완 등의 이유로 모듈을 갱신 또는 추가할 필요성이 발생하며, 이를 위하여 이를 위해서는 전자서명 방식을 사용해야 하는데, 국내에서 가장 많이 사용되는 액티브 X 컨트롤의 경우 프로그램 제조사를 확인시켜 주는 역할만을 제공하여 설치여부는 사용자의 판단에 맡기는 문제점을 지적하였다[5]. 이는 사용자의 전문성과 법적 책임을 동시에 강조하는 측면이 있다. 또한 인증에 있어서도, 기본적인 ID/비밀번호 방식과 함께, 공인 인증서, 생체 인증 등이 사용될 수 있다. 따라서 홈네트워크에 연결된 기기의 계산능력과 어플리케이션의 다양성, 접속 가능한 네트워크의 이질성 등으로 인증과 접근제어는 가능한 유연하게 설계되어야 하며, 다양한 정책, 인증방식 및 응용을 수용할 수 있어야 한다.

홈네트워크 시스템에서의 사용자 인증과 접근제어 방법은 DB와 인증정책 서버 기능을 위치시키는 방식에 따라 맥내에 위치시키는 홈서버 기반과 맥외에 위치시키는 원격관리서버 기반으로 나눌 수 있다[8]. 현재까지 제작되거나 구현된 대부분의 시스템은 홈게이트웨이에 탑재된 침입차단기능 및 VPN 기능, 홈서비스 사업자와 홈게이트웨이간의 디바이스 인증 기능정도가 상용화된 보안기능을 갖는 정도였으며, 2004년부터 정통부의 선도기술개발과제로 ETRI에서 홈서버 기반으로 홈네트워크 인증 및 접근권한 제어기술개발과제를 진행하였다[9]. ETRI에서 진행한 홈서버 기반의 사용자 인증 및 접근제어 방법은 개인 정보보호 입장에서는 개인 정보를 외부에 노출시키지 않고 직접 관리함으로써, 개인 정보의 노출 문

제에는 좀 더 유리하나 사용자 인증과 접근제어를 위한 인증/정책 등의 데이터와 DB관리, 인증/정책 서버 관리 및 유지보수, 시스템 업그레이드 등의 작업을 가정 내의 구성원이 직접 수행해야 한다. 이는 비전문가인 사용자가 직접 보안 관리를 하는데서 오는 실수 및 오류 등의 보안 관리의 안정성과 신뢰성 측면과 보안 시스템 관리와 유지보수 측면에서는 매우 취약하게 된다. 또한, 인증/접근제어 시스템이 가정내에 존재하여 사용자에게 시스템 구축을 위한 비용과 시간이 증가하여 홈네트워크 활성화에 나쁜 영향을 미칠 수 있다.

홈네트워크에 홈서버를 가정 밖에 설치한 개념을 도입한 사례는 2002년 처음 제안되었으나, 당시에는 가정의 인터넷이 변동 IP를 갖는 문제와 방화벽 및 프록시를 홈네트워크에 설치해야 하는 문제를 풀기 위한 방법론으로 제안되었으며, 가상적 홈서버를 가정 밖에 설치하여 해결하는 방안을 제시하였다. 이 방식은 LG세탁기를 인터넷으로 제어하는데 사용된 것으로 알려져 있으며, 범용적인 원격관리서버를 구현한 것은 아니다[15]. 원격관리서버 기반의 사용자 인증 및 접근제어 방법은 사용자 인증/정책 등의 데이터와 DB, 인증/정책 서버 기능이 외부에 위치하여 전문가를 통해 데이터 관리와 DB, 인증/정책 서버 관리 및 유지 보수, 시스템 업그레이드 등의 작업이 이루어지므로 보안 관리에 안정성과 신뢰성을 확보할 수 있고, 지속적으로 발전하는 보안체계와 다양한 인증, 접근제어 방식을 유연하게 적용시키는데 홈서버방식보다 유리하다. 특히, 우리나라와 같은 아파트 단지 형태의 주거환경에서는 아파트 단지의 관리 사무소에 원격관리서버를 배치하고 각 세대의 사용자 인증과 접근제어를 원격관리서버에서 처리하도록 함으로써, 각 가정 내에 인증 및 접근제어 등의 처리를 위한 보안 시스템을 설치하는 비용을 절감할 수 있고, 사용자는 홈네트워크 시스템의 서비스 이용에만 집중할 수 있도록 하여, 홈네트워크 활성화에 긍정적인 요소로 작용할 수 있다.

본 연구에서는 기존의 연구들이 홈서버 기반의 단위 기술에 치중한 반면에 본 연구에서는 홈네트워크 보안 시스템의 구축 비용 절감과 사용자의 편의성을 고려하여 원격관리서버를 기반으로 보안 시스템을 구현하였다. 또한, 접근제어에 다중의 정책들을 수용할 수 있도록 정책서버를 설계하였다. 제안한 원격서버기반의 인증 및 접근제어 방식은 홈 애플리케이션 서버의 위치를 대외로 위치한 것을 제외하고는 2006년 12월 ITU-T에서 홈네트워크를 위한 보안기술 프레임워크에 대한 표준으로 승인된 ITU-T X.1111을 준수하였다.



(그림 3) 원격관리서버 기반 사용자 인증/접근제어

3. 설계 및 구현

3.1 시스템 구성

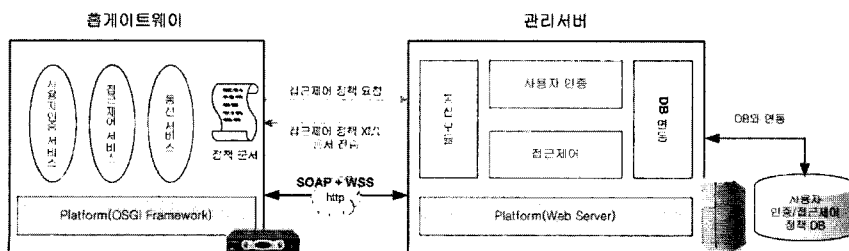
본 연구에서는 원격관리서버 기반의 홈네트워크 사용자 인증 및 접근제어 시스템을 구축하기 위하여 홈게이트웨이의 사용자 인증과 접근제어 서비스는 OSGi 프레임워크[16]를 기반으로 구성하였고, 홈게이트웨이와 관리서버와 인증, 권한 등의 요청/응답 전송을 위한 XML 기반의 통신 프로토콜과 통신 서비스와 관리서버에 사용자 인증과 접근제어 정책을 저장하기 위한 DB를 구성하고, 웹 기반의 원격관리서버는 원격지에서도 접근이 가능하도록 웹서버를 기반으로 설계 및 구성하였으며, 그 내용은 다음과 같다.

- 사용자 인증 및 접근제어 서비스 설계 및 구현
- 데이터베이스 설계 및 구축
- 홈게이트웨이-관리서버 통신 프로토콜 설계 및 구현
- 홈게이트웨이-관리서버 통신 서비스 설계 및 구현
- 사용자 인증 및 접근제어 관리 시스템 설계 및 구현

3.2 개발환경

본 연구에서 구현한 시스템의 개발환경은 다음과 같다.

- J2SDK 1.4.2
- Eclipse 3.1 with WTP 0.7
- Oracle 9.2.0.1.0
- Tomcat 5.0
- JSP, Servlet, JavaScript, ...



(그림 4) 원격관리서버 기반의 사용자 인증 및 접근제어 시스템 구성도

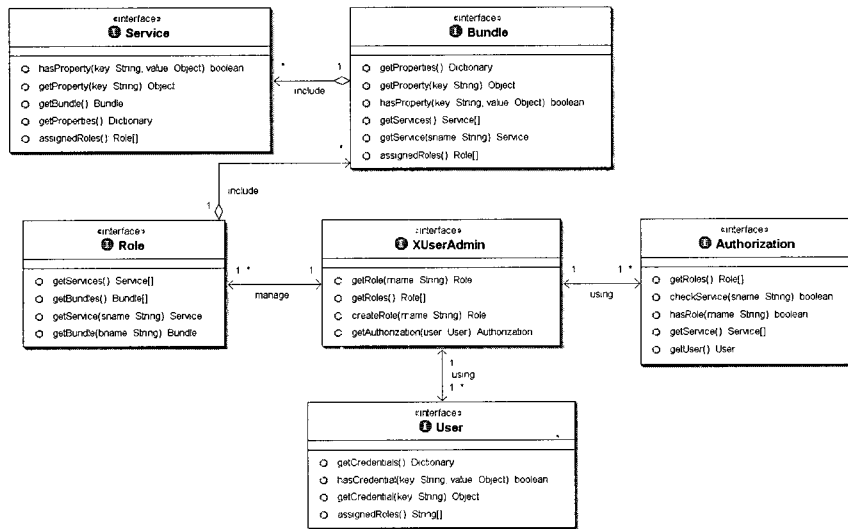
3.3 사용자 인증 및 접근제어 서비스 설계 및 구현

OSGi에는 사용자 인증 및 접근제어를 위한 UserAdmin Services가 정의되어 있는데, 이 서비스에는 번들(Bundle)과 서비스에 대한 정보가 명확하게 표현되어 있지 않으며, 역할을 기준으로 한 접근제어를 명확하게 나타내지 못하고 있어, 본 연구에서 제안한 원격관리서버 모델에는 적합하지가 않다. 이에 원격관리서버 모델에 적합한 OSGi용 번들형태로 사용자 인증 및 접근제어 서비스를 설계 및 구현하였다. (그림 5)는 본 연구에서 구현한 사용자 인증 및 접근제어 서비스에 대한 인터페이스의 구성을 나타낸다.

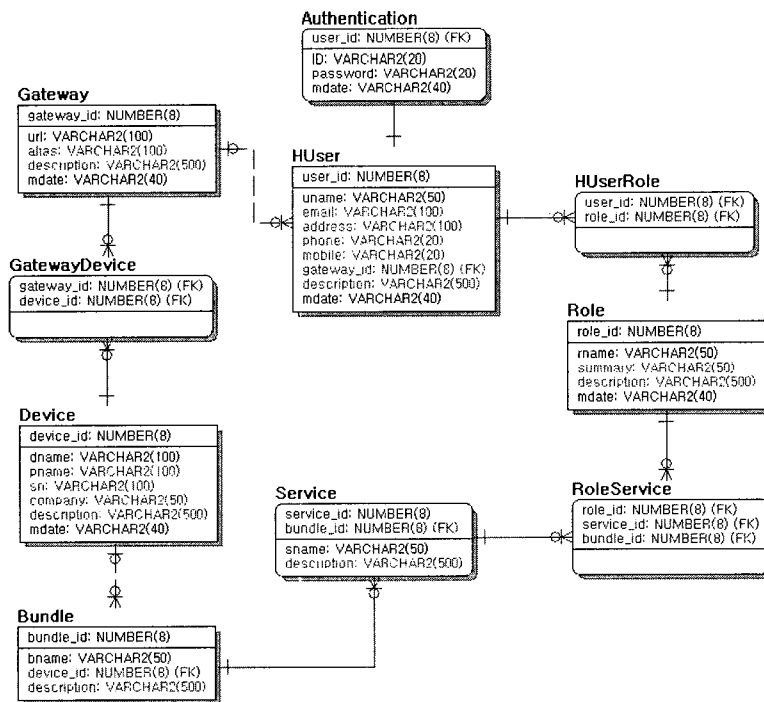
3.4 데이터베이스 설계 및 구축

본 연구에서 개발한 사용자 인증과 서비스에 대한 접근 권한 부여를 위해 관련된 정보들은 DB화 되어 있으며, 이 DB는 관리서버와 연동된다. 홈게이트웨이의 사용자 인증 요청과 접근제어 정책 요청이 있으면 관리서버는 이 DB에 질의를 통하여 필요한 데이터를 가져오게 된다.

인증 테이블은 사용자와 관련된 기밀 정보와 인증 정보가 저장된다. 현재 인증에 관련된 정보는 ID/PW 정보만 저장되어 있으며, 새로운 인증 방법이 추가되는 경우 인증 방법마다 사용자 테이블과 일대일 관계에 있는 테이블을 작성하면 된다.



(그림 5) 사용자 인증 및 접근제어 서비스 인터페이스



(그림 6) DB 모델

3.5 홈게이트웨이-관리서버 통신 프로토콜 설계 및 구현

본 연구에서 개발한 사용자 인증 및 접근제어 모델은 홈게이트웨이와 원격관리서버와의 질의/응답에 의해 수행되는 모델로써, 사용자 인증과 접근제어를 위해 홈게이트웨이와 관리서버 사이에 상호 통신 과정이 필요하게 된다. 이를 위해 홈게이트웨이와 관리서버간의 통신 프로토콜이 필요하며, 이 통신 프로토콜은 향후 확장성을 고려하여 <표 1>과 같이 세 종류의 XML 기반의 메시지 스키마[17]를 설계하고, Java 프로그램에서 사용할 수 있도록 Jar 형태의 라이브러리를 구현하였다.

<표 1> 통신 프로토콜 스키마

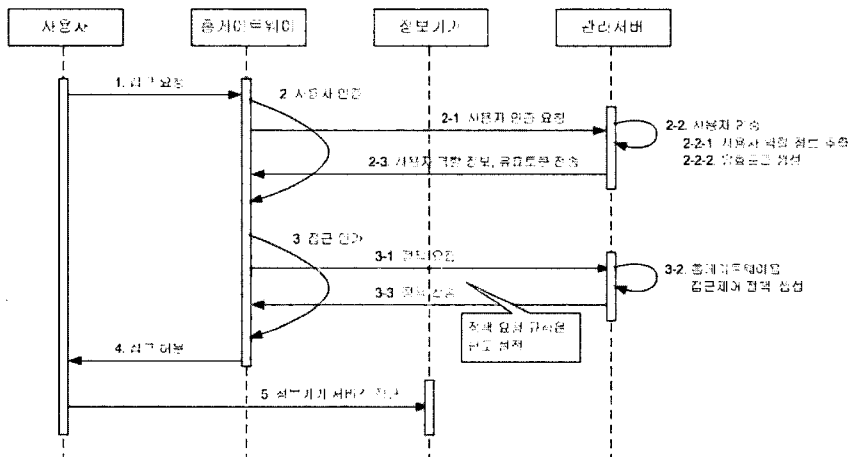
스키마 종류	설명
사용자 인증 토큰	관리서버에 요청시 사용자 인증 토큰을 표현한 XML 메시지 구조
요청/응답 메시지	홈게이트웨이와 관리서버간의 요청/응답을 표현한 XML 메시지 구조
접근제어 정책	홈게이트웨이용 접근제어 정책을 표현한 XML 메시지 구조

3.6 홈게이트웨이-관리서버 통신 서비스 설계 및 구현

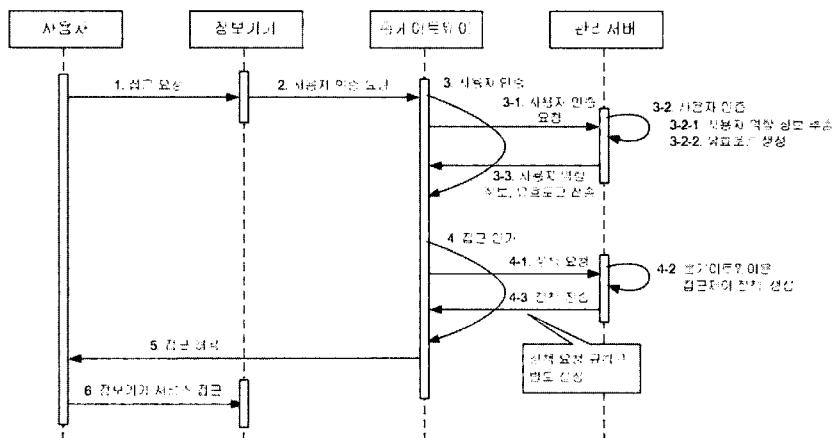
본 연구에서 개발한 사용자 인증 및 접근제어 모델은 홈게이트웨이와 외부 관리서버와의 질의/응답에 의해 수행되는 모델로써, 사용자가 정보기기 서비스에 접근하는 형태는 크게 홈 외부에서의 접근과 홈 내부에서의 접근으로 나눌 수 있으며, 이에 대한 서비스 접근 시퀀스는 각각 (그림 7), (그림 8)과 같다.

먼저, 홈 외부에서의 접근과정은 사용자가 홈게이트웨이에 접속하여 정보기기에 대한 접근을 요청하면 홈게이트웨이는 사용자 인증을 위한 사용자 정보를 요청하고, 사용자가 사용자 정보를 입력하면 홈게이트웨이는 이 정보를 원격관리서버에 전송하고, 원격관리서버는 사용자 인증 작업을 수행하고, 유효한 사용자이면, 사용자 역할 정보와 세션관리를 위한 유효토큰을 홈게이트웨이에 전송하고, 홈게이트웨이는 유효한 접근 인가 정책이 없으면 접근 인가 정책을 원격관리서버에 요청하여 수신하고, 사용자 역할에 따라 접근 허용여부를 결정한다.

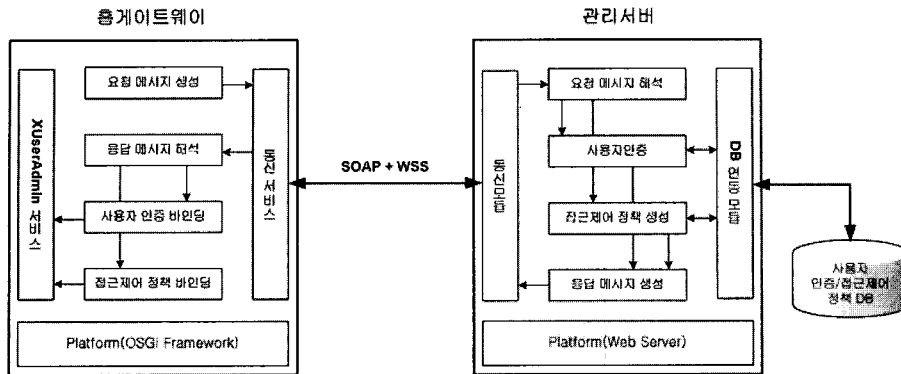
홈 내부에서의 접근과정은 사용자가 정보기기에 접근하면 정보기기는 홈게이트웨이에 사용자 인증을 요청하고, 홈게



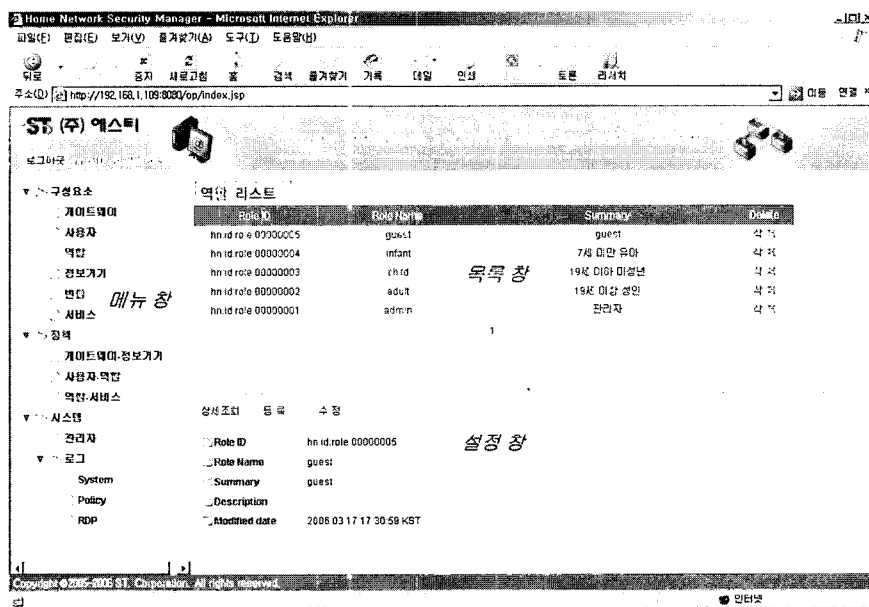
(그림 7) 홈 외부에서의 정보기기 서비스 접근 시퀀스



(그림 8) 홈 내부에서의 정보기기 서비스 접근 시퀀스



(그림 9) 홈게이트웨이-관리서버 통신 서비스 구조



(그림 10) 관리 시스템 화면 구성

이트웨이는 홈 외부의 접근과정과 마찬가지로 원격관리서버에 사용자 인증과 접근 인가 정책을 요청하여 접근 허용여부를 결정한다.

위의 접근 시퀀스처럼 홈게이트웨이와 관리서버간의 상호작용은 SOAP 프로토콜[18]을 통해 이루어지며, 이 SOAP 프로토콜의 보안을 위해 WS-Security[19]를 적용할 수 있다.

SOAP 프로토콜은 홈게이트웨이의 요청과 관리서버의 응답을 위의 통신 프로토콜에서 설계한 XML 메시지를 실어 전송하게 된다. 홈게이트웨이와 관리서버의 상호작용을 위해 (그림 9)와 같은 구성요소들을 설계하고, 구현하였다.

3.7 사용자 인증 및 접근제어 관리 시스템 설계 및 구현

사용자 인증 및 접근제어 관리 시스템은 사용자 인증 및 접근제어 서비스를 위한 사용자 관리(등록, 삭제, 수정)와 역할, 정보기기, 번들, 서비스 등의 접근제어를 위한 요소들을 등록, 삭제, 수정 등의 작업을 수행하고, 사용자가 역할 할당, 역할에 접근가능 서비스 할당 등의 접근제어 정책 설정 등을 쉽게 할 수 있도록 GUI를 제공하는 관리 시스템을

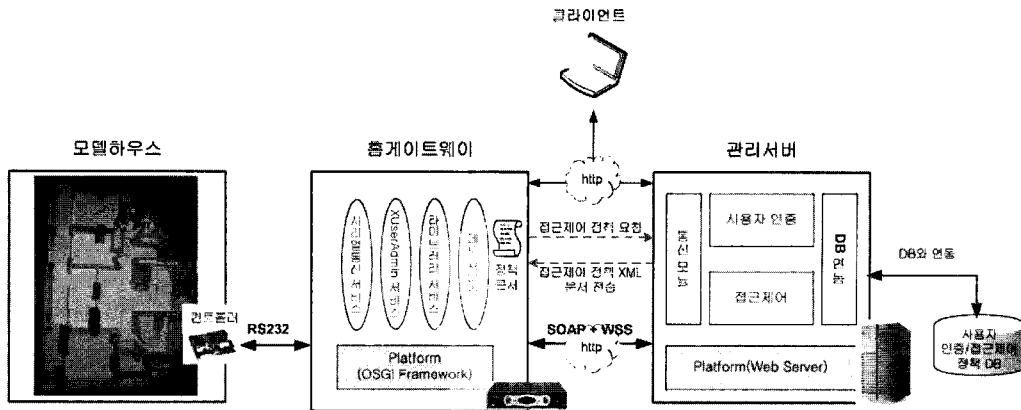
말하며, 본 연구에서는 위와 같은 작업들을 브라우저를 통해 원격지에서도 제어할 수 있도록 웹 어플리케이션 형태로 구현하였으며, 관리자만이 등록, 수정 등의 작업을 할 수 있도록 하였다.

관리 시스템 GUI의 기본 프레임은 (그림 10)과 같이 메뉴창(왼쪽), 목록창(오른쪽 위), 설정창(오른쪽 아래)으로 이루어진다.

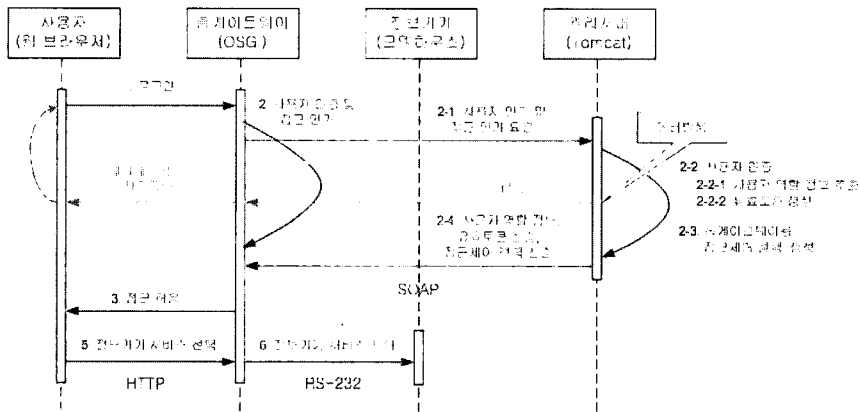
4. 실험 및 결과

본 연구에서 설계 및 구현한 원격관리서버 기반의 사용자 인증 및 접근제어 시스템을 실험하기 위하여 (그림 11)과 같은 데모 시스템을 구현하였다.

데모 시스템의 동작 실험은 사용자가 웹 브라우저를 통해 홈게이트웨이에 접근하면, 홈게이트웨이는 ID/PW기반의 사용자 로그인을 요청하고, 사용자가 ID/PW를 입력하면, 홈게이트웨이는 관리서버에 사용자 인증을 요청한다. 관리서버는 유효한 사용자가 아니면 에러 메시지를 전송하여 홈게이



(그림 11) 데모 시스템 구성도



(그림 12) 데모 시스템 시나리오 흐름도

트웨이를 통해 웹 브라우저에 표시된다. 유효한 사용자이면 관리서버는 사용자 역할 정보와 세션관리를 위한 유효토큰과 3.5에서 설계한 XML 기반의 홈게이트웨이용 접근제어 정책 스키마에 맞게 접근제어 정책을 생성하여, SOAP 프로토콜을 통해 홈게이트웨이에 전송하고, 홈게이트웨이는 접근제어 정책을 3.3과 같이 구현된 사용자 인증 및 접근제어 서비스에 바인딩시키고, 현재 로그인한 사용자의 정보기전들에 대한 접근가능여부를 웹 브라우저 화면에 표시하고 접근 가능한 정보기전의 서비스를 동작시킨다.

정보기전 서비스의 동작여부는 홈게이트웨이와 RS232를 통해 연동하는 컨트롤러를 통해 모델하우스에 정보기전을 대신하는 LED를 부착하여 On/Off를 통해 실험하였다. 본 실험의 흐름도는 (그림 12)와 같으며, (그림 13)은 유효한 사용자일 경우 관리서버에서 생성한 사용자 역할 정보, 유효토큰과 홈게이트웨이용 접근제어 정책에 대한 XML 기반의 응답 메시지의 예이다.

본 데모 시스템에서 구현한 정보기전들과 서비스들은 <표 2>에 표시였으며, 사용자가 할당된 역할과 서비스에 따른 역할별 접근권한은 <표 3>과 <표 4>와 같다. 사용자, 역할, 접근권한 등은 3.7에서 구현한 관리 시스템을 통해 변경이 가능하다.

<표 2> 데모 시스템의 정보기전 서비스 목록

정보기기	서비스명	서비스요약
조명등	PowerService	전원 On/Off
	PowerService	전원 On/Off
	AdultChannelService	성인채널 선택
DTV	CommonChanelService	일반채널 선택
	PowerService	전원 On/Off
냉장고	TempService	온도제어
	PowerService	전원 On/Off
에어컨	WindService	풍속제어
	PowerService	전원 On/Off
경보기	PowerService	전원 On/Off
	OperationService	경보기 전체/해제
보일러	PowerService	전원 On/Off
	OperationService	보일러 난방제어
도어락	OperationService	도어락 개폐제어
가스밸브	OperationService	가스밸브 개폐제어

<표 3> 사용자-역할 관계

사용자 목록	역할 목록
아버지	부모
어머니	
아들	자녀
딸	

```

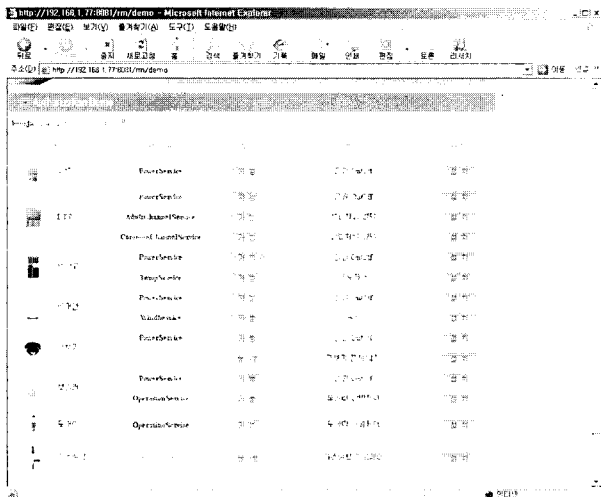
<?xml version="1.0" encoding="euc-kr"?>
<comm:Response xmlns:comm="http://hn.stkorea.net/comm">
  <comm:Gateway URL="192.160.120.101" />
  <comm:Demand>Authentication_Authorization</comm:Demand>
  <comm:ValidToken>
    22299991241228571066340157859657790
  </comm:ValidToken>
  <comm:UserRole>adult</comm:UserRole>
  <pol:AuthorizationPolicy URL="192.160.120.101"
    PolicyId="policy:auth:00000001"
    xmlns:pol="http://hn.stkorea.net/policy">
    <pol:Description xsi:nil="true"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" />
    <pol:Timestamp>
      <pol:Created>2007-01-05T12:38:35.281Z</pol:Created>
      <pol:Expires>2007-01-05T13:38:35.281Z</pol:Expires>
    </pol:Timestamp>
    <pol:Role Name="adult">
      <pol:Bundle Name="RefrigeratorBundle">
        <pol:Services>
          <pol:Service>
            refrigerator.OnOffService
          </pol:Service>
          <pol:Service>
            refrigerator.ControlService
          </pol:Service>
        </pol:Services>
      </pol:Bundle>
      <pol:Bundle Name="DTVBundle">
        <pol:Services>
          <pol:Service>
            dtv.AdultOrderService
          </pol:Service>
        </pol:Services>
      </pol:Bundle>
      :
    </pol:Role>
    <pol:Role Name="child">
      <pol:Bundle Name="RefrigeratorBundle">
        <pol:Services>
          <pol:Service>
            refrigerator.OnOffService
          </pol:Service>
        </pol:Services>
      </pol:Bundle>
      <pol:Bundle Name="WatchCameraBundle">
        <pol:Services>
          <pol:Service>
            watchcamera.OnOffService
          </pol:Service>
        </pol:Services>
      </pol:Bundle>
      :
    </pol:Role>
  </pol:AuthorizationPolicy>
</comm:Response>

```

(그림 13) XML 기반의 응답 메시지의 예

〈표 4〉 역할-서비스의 접근권한 관계

정보기기	서비스명	역할	
		부모	자녀
조명등	PowerService	가능	가능
DTV	PowerService	가능	가능
	AdultChannelService	가능	가능
	CommonChanelService	가능	가능
냉장고	PowerService	가능	가능
	TempService	가능	가능
에어컨	PowerService	가능	가능
	WindService	가능	가능
경보기	PowerService	가능	가능
	OperationService	가능	불가능
보일러	PowerService	가능	가능
	OperationService	가능	가능
도어락	OperationService	가능	가능
가스밸브	OperationService	가능	불가능



(그림 14) 서비스 목록 화면(아들 사용자)

데모 시스템의 홈게이트웨이에 웹 브라우저를 통해 로그인하였을 때 사용자에게 할당된 역할이 갖는 서비스들의 접근권한에 따라 사용 가능한 서비스 목록이 제대로 표시되었으며, 각 서비스의 동작 여부는 모델하우스에 연결된 LED의 점멸을 통해 확인할 수 있었다. (그림 14)는 아들 사용자가 로그인 하였을 때 사용가능한 서비스 목록을 표시한 화면이다.

〈표 2〉에 나타난 모든 서비스에 대하여 표 3에 나타난 부모, 자녀의 역할로 (그림 14)와 같은 목록 화면을 조작하여 접근 시험을 각각 20회씩 반복하여 수행하였고, 모델하우스의 정보기기에 나타난 결과를 보고 접근제어의 적합성을 판별하였다. 시험 결과, 모든 시험에서 데모 시스템이 적합하게 동작하였다.

5. 결 론

홈네트워크 시스템에서의 사용자 인증과 접근제어 방법은 크게 DB와 인증/정책 서버 기능을 태내에 위치시키는 홈서버 기반과 태외에 위치시키는 원격관리서버 기반으로 나눌 수 있는데, 홈서버 기반에 비해 원격관리서버가 안정성과 신뢰성 및 비용 측면에서 많은 장점을 가지고 있다. 본 연구에서는 홈네트워크 시스템의 사용자 인증과 접근제어를 위해 원격관리서버를 기반으로 하는 시스템을 설계 및 구현하였고, 이를 실험하기 위해 데모 시스템을 구축하여 실험하였으며, 사용자 인증과 접근제어 기능이 안정적으로 동작하였다.

본 연구에서 구현한 원격관리서버 기반의 사용자 인증 및 접근제어 시스템을 아파트 단지와 같은 주거환경에 적용하면, 사용자의 비용 부담을 줄일 수 있으며, 홈네트워크 시스템을 사용하기위해 습득해야 하는 지식을 서비스의 이용 방법에만 집중할 수 있어 사용자의 지식 습득 부담을 줄일 수 있어 홈네트워크 활성화에 도움이 되리라고 판단된다. 문헌상에서 조사한 바로는 구현된 사용자 인증 및 접근제어 시스템은 원격관리서버를 이용한 측면에서 국내에서는 최초의 시스템으로 여겨진다.

현재 구현된 시스템은 사용자의 인증을 위해 패스워드 기반의 방식만을 제공하고 있으나, 향후에는 다양한 사용자 인증 방식(인증서, 생체인식 등)을 적용할 수 있는 방안에 대한 연구가 필요하다.

참 고 문 헌

- [1] 이윤철, "최근의 홈 네트워크 기술동향 및 시장 전망," 정보통신연구진흥원 주간기술동향 통권 1098호, 2003.6.4.
- [2] 이영진, "홈네트워크 시장 활성화 저해 요인과 주요 갈등," 정보통신정책, 제18권 5호, pp.19-31, 2006.
- [3] 유동영, "홈네트워크 서비스에서 정보보호 필요성 및 고려사항," 한국통신학회지(정보통신), 제22권 8호, pp.51-62, 2005.
- [4] 한종욱 등, "안전한 홈네트워크 구축을 위한 보안요구사항," 정보처리학회지, 제11권 3호, pp.38-45, 2004.
- [5] 정재학, "홈네트워크에서의 보안 요구사항 분석," 정보보호학회지, 제14권 5호, pp19-22, 2004.
- [6] Shintaro Mizuno et al, "A new remote configurable firewall system for home-use gateways," 2nd IEEE Consumer communications and network conference, pp.599-601, 2005
- [7] 한종욱, 이덕규, 정교일, "홈네트워크 보안기술 동향," 한국통신학회지(정보통신), 제23권 9호, pp113-124, 2006.
- [8] 최훈일, 장영건, "홈네트워크 시스템의 사용자 인증 및 접근제어 방법, 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호, pp.897-900, 2006.11.
- [9] 한종욱, "홈네트워크 사용자 인증 및 접근제어 솔루션," 한국홈네트워크산업협회, 2006.5.30.
- [10] 김중은, 조경산, "센서네트워크의 노드간 세션키 생성을 위한 개선된 프로토콜," 정보처리학회논문지, 제13-Crnjs 2호, pp. 137-146, 2006.4.

[11] 이주영 등, "계층적 센서 네트워크에서 안전한 통신을 위한 키 갱신 프로토콜," 정보처리학회논문지, 제 13-C권 5호, pp. 541-548, 2006.10.

[12] Tine Verhanneman et al, "A Modular Access Control Service for Supporting Application-Specific Policies," IEEE Distributed Systems Online, Vol.7, No.6, pp., June, 2006.

[13] Duan Haixin et al, "Policy-based access control framework for large network," ICON 2000, pp.267-272, Sep., 2000.

[14] Elisa Bertino et al, "A System to specify and manage multipolicy access control models," POLICY'02, 2002.

[15] Jonghwan Lee et al, "Development of internet home server to control information appliances remotely," LNCS 2343, pp561-588, 2002.

[16] OSGi, <http://www.osgi.org>.

[17] XML Schema, <http://www.w3.org/XML/Schema>.

[18] Simple Object Access Protocol(SOAP)1.1, <http://www.w3.org/TR/SOAP>

[19] OASIS Web Service Security TC, <http://www.oasis-open.org/committees/wss>



최 훈 일

e-mail : choihi@stkorea.net
 2000년 청주대학교 컴퓨터정보공학과 (공학사)
 2002년 청주대학교 전산정보공학과 (공학석사)
 2006년~현 재 청주대학교 컴퓨터정보공학과 박사과정

2002년~현 재 주식회사 에스티 과장

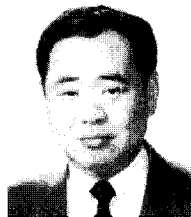
관심분야: 홈네트워크 보안, 웹서비스 보안, 웹 2.0, 시맨틱 웹, ID 관리



정 창 훈

e-mail : iqjump@stkorea.net
 1988년 경북대학교 전자공학과 (공학사)
 1990년 경북대학교 전자공학과 (공학석사)
 1990년~2000년 한국전자통신연구원 선임연구원

2000년~2003년 고려대학교 정보보호 대학원 박사과정 수료
 2000년~현 재 주식회사 에스티 대표이사
 2000년~현 재 한국정보보호학회 충청지부 이사
 관심분야: 정보보호 프로토콜, 웹서비스, ID 관리



장 영 건

e-mail : ygjang@cju.ac.kr
 1980년 인하대학교 전자공학과 (공학사)
 1979년~1983년 국방과학연구소 연구원
 1983년~1994년 대우중공업 중앙연구소 책임연구원
 1991년 인하대학교 전자공학과 (공학석사)

1995년 인하대학교 전자공학과 (공학박사)
 1995년~1996년 고등기술연구원 책임연구원
 2003년~2004년 University of California, Davis visiting Professor
 1996~현 재 청주대학교 정보기술공학부 부교수
 관심분야: HCI, 지능 로봇, 보조기술, 재활공학, 생체정보시스템