모바일 응용 서버의 사용자 관리 시스템 설계 및 구현

김수형[0] 장철수 노명찬 김중배
한국전자통신연구원
(lifewsky[0], jangcs, mcroh, jjkim)@etri.re.kr

Design and Implementation of user management system for mobile application server

Soo-Hyung Kim[0] ChoulSoo Jang MyungChan Roh Joong-Bae Kim
Electronics and Telecommunications Research Institute

요 약

본 논문은 모바일 응용 서버 시스템에서 인증, 역할 기반 접근 제어, 사용자 개인 정보 관리 등과 같은 보안 서비스를 제공하기 위해 개발된 사용자 관리 시스템에 대한 구조와 기능에 대해 설명하고자 한다. 또한, 모바일 환경에 따른 특이 사항들을 처리하는 기능과 방법들에 대해 살펴 볼 것이다. 개발된 사용자 관리 시스템은 크게 응용 서버 시스템의 하위 보안 프레임워크 부분과 모바일 응용 개발자에게 직접 응용의 보안 로직을 개발할 수 있도록 지원 API를 가지며 모바일 응용 서버 시스템 특화된 보안 서비스를 제공하는 모바일 보안 처리 부분으로 나뉘어져 있다.

1. 서 론

현재 무선 인터넷 분야에서는 이동통신 기술의 발전에 힘입어 데이터 전용의 넓은 대역폭을 갖는 무선 인터넷 단말기들이 광범위하게 보급되어 활용되고 있다. 이에 따라 새로운 형태의 무선 인터넷 서비스들이 등장하고 있고, 디지털 컨텐츠, 어플리케이션 서비스 등이 통합되어 개인화된 형태로 다양한 종류의 장비와 네트워크를 통해 무선 인터넷 사용자들에게 제공되어야 한다. 따라서 무선 인터넷 단말 사용자의 서비스 요청 처리를 원활하게 수행하기 위한 모바일 응용 서버가 요구된다.

모바일 응용 서버는 기존의 응용 서버 기술뿐만 아니라 무선 네트워크 환경과 무선 단말의 특성을 이해하고 처리할 수 있는 기술들을 필요로 한다. 본 논문은 다양한 무선 단말들에 대한 비즈니스 및 컨텐츠 서비스를 제공하기 위해 개발된 모바일 응용 서버 내 사용자 관리 시스템에 대해 설명하고자 하며, 무선 환경에서의 고려사항, 고 가용성을 위한 클러스터링 환경에서의 고려사항, 멀티모달을 지원하기 위한 기능 등, 유선 환경에서의 사용자 관리 시스템과 대비되는 특성들에 대해 설명한다.

2장에서는 모바일 응용 서버에 대한 개괄적인 구조와 모바일 요청 처리 과정에 대해 설명하며, 3장에서는 사용자 관리 모듈의 하위 프레임워크인 보안 서비스 프레임워크에 대해 설명하며, 4장에서는 모바일 환경에 특화된 사용자 관리 모듈에서 제공하는 기능 별 특성들에 대해 자세히 설명한다. 마지막으로 5장에서는 본 논문의 결론과 향후 보완해야 할 사항에 대해 다루고자 한다.

2. 모바일 비즈니스 응용 서버

무선 인터넷 서비스를 제공하기 위한 플랫폼인 모바일 응용 서버는 휴대폰, PDA 등 다양한 무선 단말을 대상으로 한번 저작된 동일한 컨텐츠를 단말기 종류에 상관없이 지원할 수 있도록 설계□개발되었다. 무선 마크업 언어는 이통사 별로 다양하게 존재하는데, 한번의 저작으로 다양한 무선 마크업 언어를 지원하기 위해, 모바일 응용 서버 시스템은 PWML이란 가상의 단일 무선 마크업 언어에 대한 문서 변환 기능을 통해 다양한 이통사의 단말기를 지원할 수 있게 하였다. 또한 모바일 응용 서버 위에 구축된 비즈니스 업무들은 무선 인터넷의 간헐적 단절성, 업무의 긴급성, 입출력 장치의 제약, 이동성 등을 고려해 단일 사용자가 단말기의 종류를 변경하여 접속하더라도 이전에 처리하였던 내용을 계속 이어 받아 업무를 진행시킬 수 있도록 멀티모달을 지원한다. 그리고 모바일 응용 서버 설계 시 고려됐던 다음의 네 가지 주요 문제들을 해결하고 있다.

- 메모리 크기, 단말의 계산 능력, 스크린 크기 및 키보드 등과 같은 입출력의 어려움에 의한 모바일 단말의 제약사항
- 유선 네트워크와 비교해 상대적으로 낮은 대역폭과 간헐적으로 연결이 단절되는 무선 네트워크 환경
- 무선 클라이언트 대규모 요청 처리와 고가용성을 위한 클러스터링 문제
- 기존 유□무선 시스템과의 연동 문제

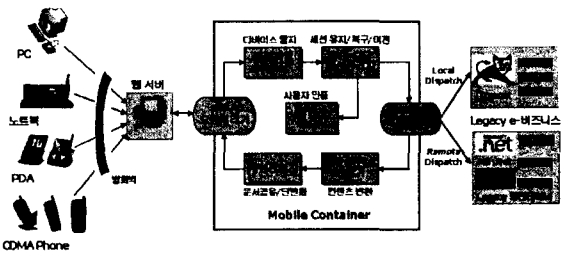

그림 1 모바일 응용 서버의 요청 처리 흐름도

그림 1은 무선 단말을 통해 사용자의 서비스 요청이 접수되었을 때 모바일 응용 서버에서 그 요청을 처리하여 응답하는 과정 동안의 개괄적인 흐름도이다. 사용자의 요청은 무선 요청 처리기를 통해 접수되며, 프로파일 관리자는 접수된 요청의 HTTP 헤더정보로부터 단말기의 특징 정보를 추출한다. 멀티모달 세션 관리자는 단말 특징 정보와 인증된 사용자를 기반으로 응용의 세션을 관리하거나 복구하여 사용중인 세션을 유지시키는 기능을 수행한다. 동적 컨텐츠 변환기는 응용 로직이 수행되고 난 후의 컨텐츠를 단말의 프로파일 정보를 가지고 사용자 단말 환경에 적합하도록 변환한다. 캐쉬 관리자는 변환된 페이지에 대한 정보를 캐쉬하여, 이후 같은 페이지에 대한 요청이 있을 때 캐쉬된 페이지를 사용하여 응답 속도를 개선한다.

그림 1의 요청 처리 흐름 설명에서 간단히 언급한 프로파일 매니저와 멀티모달 세션 매니저는 사용자 매니저와 밀접하게 관련이 있으므로 아래에 좀 더 자세히 해당 기능을 살펴보고자 한다.

2.1 프로파일 관리자

프로파일 관리자는 모바일 단말기의 메모리, 화면 크기, 키보드 타입 등과 같은 컨텐츠 변환을 위한 사용자 단말기의 특성 정보, 컨텐츠 변환기로부터 생성된 변환 프로파일 정보, 사용자 관리에 필요한 단말 정보 등을 제공한다. 사용자 단말의 특성 정보는 단말에서 요청이 서버로 접수되는 시점에서 요청 헤더 정보인 UAProf(User Agent Profile)를 분석하여 프로파일 레파지토리에 저장되며, 프로파일 관리자가 프로파일 편집 도구를 이용하여 추가적인 단말 정보를 추가할 수 있도록 하였다. 프로파일 레파지토리에 저장된 단말 정보를 통해 컨텐츠 변환기는 사용자 단말에 가장 적합한 형태의 컨텐츠를 생성한다.

2.2 멀티모달 세션 관리자

모바일 응용 서버를 이용하여 비즈니스를 처리하는 사용자는 특정 단말에 구애 받지 않으면서 원하는 단말기 종류를 이용하여 비즈니스 서비스를 지원 받을 수 있다. 즉, 긴급하고 이동성이 강조되는 업무에서는 화면표시 능력이 떨어지고 불편한 입력 수단을 갖고 있는 휴대폰으로도 간단한 메시지 확인이나 적은 양의 입력이 요구되는 단순 업무를 처리할 수 있도록 하고, 좀 더 세밀한 화면 조회가 요구되거나 많은 정보의 입력 작업이 요구되는 복잡한 비즈니스 업무를 위해서는 PDA, 핸드헬드 PC와 같은 무선 단말을 통해 이전 업무를 이어 받아 수행하도록 할 수 있다.

세션 객체는 유선상에서의 단일 단말기를 고려하여 만들어진 것이기 때문에 단말기를 변경한다거나 하는 경우에는 세션을 이용할 수 없는 단점을 갖고 있다. 따라서 멀티모달 세션은 이러한 세션 객체의 단점을 극복하여 다중 단말간 세션 전이가 가능하도록 하였으며, 사용자 ID와 연계하여 실제 세션 및 멀티모달 세션을 관리하도록 구현하였다.

3. 보안 프레임워크

개발된 보안 프레임워크는 다양한 응용 플랫폼에서 독립적으로 보안 업무를 수행할 수 있도록 설계/개발 되었다. 그리고 기업 내 이미 존재하는 보안 시스템의 통합을 고려하여 JAAS[4]를 지원하며, Kerberos, DB, LDAP, File 등의 인증 지원, 역할 기반 사용자 권한 체크, 사용자 정보 제공과 같은 API를 제공하여, 다양한 응용의 보안 요구를 만족시킬 수 있는 기술이 포함되어 있다.

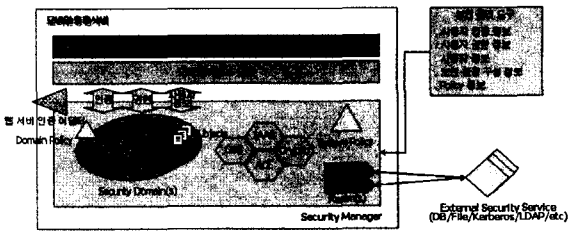

그림 2 보안 프레임워크 구조도

개발된 보안 프레임워크는 모바일 응용 서버 시스템 및 EJB 컨테이너 시스템에 적용되어 테스트 되었으며, 그림 2와 같은 구조를 지닌다.

보안 프레임워크에서 제공되는 기능은 4장의 사용자 관리자 시스템의 기초가 되는 것으로 4장에서 함께 설명하도록 한다.

4. 사용자 관리 시스템

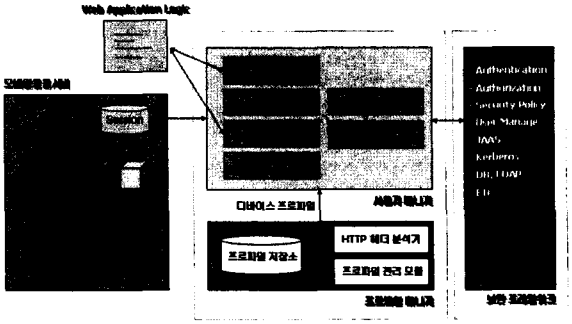

그림 3 사용자 관리 시스템

모바일 응용 서버의 사용자 관리 시스템은 유선 응용 서버의 사용자 관리 시스템에서 제공하는 기능들과 더불어 무선 환경의 요구 사항을 만족시킬 수 있는 기능들이 제공되어야 한다.

본 논문에서 설명하는 사용자 관리 시스템은 무선 환경의 요구사항을 만족시킬 수 있도록 개발되었으며, 그림 3과 같은 구조를 가진다. 아래에서 사용자 관리 시스템의 기능별로 자세히 설명하고자 한다.

4.1 사용자 인증

모바일 응용 서버 시스템은 다양한 무선 비즈니스 환경을 고려하여 설계되고 개발되었다. 따라서 사용자 관리 시스템에서의 인증 기능은 다양한 보안 플랫폼을 지원할 수 있어야 한다.

사용자 관리 시스템은 3장에서 설명하는 보안 프레임워크 위에서 동작하므로 보안 프레임워크에서 제공하는 인증 서비스를 모두 활용할 수 있도록 설계되었다. 보안 프레임워크는 JAAS 인증 및 대부분의 레거시 보안 서버와 연동할 수 있는 보안 모듈들이 제공되며, 사용자 관리 시스템은 응용의 보안 정책에 따라 필요한 보안 서비스 도메인을 구성하여 인증 서비스를 제공할 수 있다. 따라서 모바일 응용 개발자는 Servlet

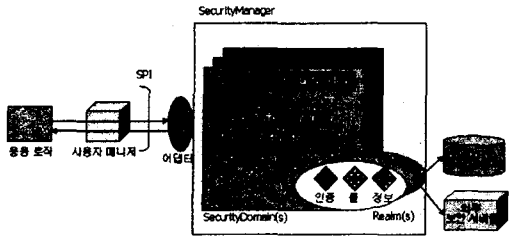

그림 4 사용자의 인증

스펙[2]에서 설명하는 인증 방법과 함께 기존 인증 시스템의 통합 및 사용자 관리에서 좀 더 자유로울 수 있다.

부가적으로 프로파일 관리자를 통해, 사용자의 무선 단말기가 입력 기능이 취약한 단말인지를 체크하여 Subscriber ID만으로 자동 로그인을 수행할 수 있는 서비스를 제공한다. 이는 응용 서비스가 보안에 크게 영향 받지 않는 서비스여야 하므로, 보안 정책 파일에 이 기능을 지원할지 명시해야 한다.

4.2 사용자 권한 관리

사용자 관리 시스템은 모바일 응용 개발자가 프로그램 로직 상에서 응용 자원에 대한 접근 제어를 처리할 수 있는 API를 제공하기 위해, 보안 프레임워크의 권한 관리 기능을 사용한다. 사용자의 권한은 JAAS 기반하의 인증된 사용자의 Principal을 통한 역할 기반 보안뿐만 아니라 자원에 대한 접근 권한을 제어하는 ACL, 그룹 개념을 통해서 수행될 수 있다.

개발자는 Request 객체에 대한 isUserInRole 함수을 통해 기본적인 접근 제어를 수행할 수 있으며, 사용자 관리 시스템을 통해 좀더 정밀한 접근 제어 로직을 개발할 수 있다.

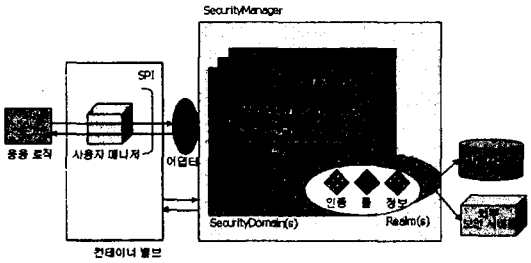

그림 5 사용자의 접근 통제

4.3 사용자 정보 제공

모바일 응용에서 사용자의 기본적인 정보나 무선 특화된 서비스를 위한 정보는 필수적이며, 모바일 응용 서버는 사용자 관리 시스템을 통해 이를 제공한다. 특히 프로파일 관리자, 멀티모달 세션 관리자와 연계하여, 사용자의 무선 단말에 대한 특징과 사용자가 선호하는 페이지 등의 정보를 통해, 입출력이 취약한 무선 단말의 제약을 극복할 수 있는, 응용을 개발할 수 있도록 하였다.

사용자 정보는 응용에 따라 보안 프레임워크에서 기본적으로 제공하는 파일 및 DB Realm을 통해 구축할 수 있으며, 보안 프레임워크 확장 인터페이스를 구현함으로써, 응용이 요구하는 다양한 수준의 사용자 정보 제공 서비스를 구축할 수 있다.

4.4 세션

모바일 응용 서버는 2.2절에서 설명하는 다중 단말간 세션 전이를 지원하기 위해, 멀티모달 세션을 관리하며, 사용자 관리 시스템은 멀티모달 세션과 사용자를 연결하는 키를 제공한다. 인증된 사용자는 전체 시스템에 유일한 사용자 ID를 가지고 있으므로, 사용자 ID를 키로 하여 사용자의 이전 작업 정보를 멀티모달 세션 관리자를 통해 관리하도록 하고 있다. 또한 사용자가 로그아웃 하거나 세션이 만기되었을 때 멀티모달 세션 매니저와 연계하여 이를 처리하도록 하였다.

4.5 클러스터링 환경

클러스터링 환경에서 각각의 노드는 인증된 사용자에 대한 인증 정보와 멀티모달 세션을 멀티캐스트 프레임워크[3]를 통해 공유하고 있어야 한다. 멀티모달 세션은 멀티캐스트 통신을 지원하는 클러스터링 프레임워크 하에서 각 노드에 전달되며, 사용자의 정보는 보안 프레임워크 Realm 환경에서 클러스터 전체 노드에 공유된다.

인증된 사용자가 클러스터링 환경에서 또다시 인증 작업을 수행하지 않게 하기 위해, 사용자의 인증 정보는 쿠키를 이용하여 각 노드로 전달되도록 하였다. 또한 쿠키를 지원하지 않는 무선 단말을 처리하기 위해 URL Rewriting 방법이 제공된다. 쿠키의 보안 데이터 설정은 사용자 관리 시스템에서 이루어지며, 서버 시스템의 보안 키로 암호화되어 처리된다. 그리고 응용 서버에서 EJB를 호출하거나 다른 도메인의 서비스를 호출하는 경우를 위해, Kerberos[5] 및 GSS[6]를 통해 단일 인증(Single Sign-On)을 제공한다.

5. 결론 및 향후 연구

모바일 인터넷 서비스를 제공하고자 하는 서버들은 기존의 유선 환경에서의 사용자 관리 요구 사항들뿐만 아니라 사용자의 무선 네트워크 환경과 입출력이 제한된 사용자 단말의 특성들을 고려하여 설계되어야 한다. 본 논문에서는 클러스터링 기능, 가상 마크업 언어 지원 기능, 멀티모달 세션 지원 등의 다양한 기능이 제공되도록 설계/개발된 모바일 응용 서버 시스템에서 사용자의 인증, 사용자 정보 제공, 권한 관리 등의 기능을 수행하는 사용자 관리 시스템에 대해 살펴 보았다.

사용자 관리 시스템은 유무선 서버의 공통 보안 프레임워크인 보안 서비스 부분과 모바일 환경 적응 부분으로 나뉘어 개발 완료되었으나 향후 실제 업무에 적용될 수 있도록 사용자 정보 구축 도구 및 보안 관리 도구가 함께 제공되어야 할 것이다.

6. 참고 문헌

[1] Peter Lowber, Wireless Application Gateways : A Technology Perspective, Gartner Technology Overview, 2000.

[2] Java Servlet Specification Version 2.4

[3] 김수형, 이경호, 김중배, "Clustered EJB 서버의 멀티캐스트 보안 연구," 정보과학회 2003 춘계 학술대회

[4] "Java Authentication and Authorization Service(JAAS)," http://java.sun.com/products/jaas/

[5] "Kerberos : The Network Authentication Protocol," http://web.mit.edu/kerberos/www/

[6] "Generic Security Service Application Program Interface Version 2," http://www.ietf.org/rfc/rfc2743.txt