모바일 환경 적응 시스템을 위한 보안 서비스 구조 설계 및 구현

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

Design and Implementation of security service framework for mobile adaptation system

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

요 약

본 논문은 모바일 환경 적응 시스템을 대상으로 한 보안 서비스 프레임워크의 요구 사항을 제시하고, 제시된 요구 사항을 만족시킬 수 있도록 개발된 프레임워크의 특징과 구조에 대해서 살펴본다. 개발된 프레임워크는 사용자의 세션과 해당 사용자의 보안 정보를 연계할 수 있는 보안 어댑터 모듈, 사용자 단말의 특성을 이해할 수 있는 단말 프로파일 관리 모듈, 해당 사용자를 인증하고 인증된 사용자의 역할 정보에 기반하여 시스템 자원의 접근을 통제할 수 있는 보안 서비스 모듈로 구성된다.

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 모바일 환경에 적합한 비즈니스 응용들이 등장하고 있으며, 이러한 비즈니스 응용을 개발/배포/운영할 수 있는 모바일 환경 적응(응용서버) 시스템들이 소개되고 있다.

모바일 환경 적응 시스템은 기존의 응용서버 기술뿐만 아니라 무선 네트워크 환경과 무선 단말의 특성을 이해하고 처리할 수 있는 기술들을 추가적으로 요구한다. 본 논문에서 설명하는 보안 서비스 구조는 이러한 모바일 환경 적응 시스템에서의 보안 요구 사항을 분석하여, 시스템 및 응용을 위한 보안 구조를 설계하고, 설계된 구조 속에서 보안 요구 기능이 충분히 제공되도록 기능 보완적인 프레임워크 모듈로서 개발되었다. 개발된 보안 구조를 살펴보기 위해 본 논문은 다음과 같은 순서로 설명 한다.

2장에서는 보안 서비스 구조를 설계하는데 목표가 되는 개발 요구 사항에 대해 설명하며, 3장에서는 요구 사항을 만족시킬 수 있도록 개발된 보안 서비스 구조의 특징과 각각의 주요 모듈에 대해 설명하며, 4장에서는 개발된 구조에서의 보안 서비스 흐름에 대해 설명한다. 마지막으로 5장에서는 본 논문에서 제시한 연구 결과를 요약한다.

2. 개발 요구 사항

무선 인터넷 응용 서비스를 제공하기 위한 플랫폼인 모바일 환경 적응 시스템은 휴대폰, PDA 등 다양한 무선 단말을 대상으로 단말 특성에 적합한 컨텐츠 혹은 비즈니스 서비스를 제공할 것이다. 그러나 이러한 서비스를 제공하기 전의 사용자 인증 절차에 있어서, 무선 단말의 입력 장치의 제약 때문에 사용자ID/비밀정보의 입력에 어려움이 있을 것이라 예상된다. 따라서 모바일 환경 적응 시스템에서의 인증은 유선 장치(PC)에서의 인증 보다는 단순화 된 사용자 확인 방법이 제시되어야 한다. 이러한 요구 사항을 만족시키기 위해, 본 연구에서는 사용자 인증 시, 사용자 단말의 프로파일 정보를 이용하여 자동으로 사용자를 인증하는 메커니즘에 대해 소개한다.

무선 인터넷을 통한 사용자의 이용률이 높아질수록, 무선 단말을 통한 서비스의 형태도 점차 고도화 돼가고 있다. 따라서 무선 환경 적응 시스템에서의 보안 요구 수준은 기존의 유선 환경 시스템과 비교해 최소한 동일한 수준을 만족시킬 수 있어야 한다. 이러한 보안 수준을 모두 만족 시킬 수 있도록, 본 연구에서 개발된 보안 서비스 프레임워크는 유선 시스템에서의 보안 요구 사항을 분석하고 이를 지원하도록 하였다. 즉, 일반적인 비즈니스 응용서버의 보안 요구 사항([6])을 모두 만족 시키도록 하였다. 그리고 앞서 설명한 자동 인증에서 발생할 수 있는 보안 홀을 인식하여, 자원에 대한 보안 요구 수준에 따른 다중 인증 메커니즘을 지원하였다.

3. 개발된 프레임워크의 특징 및 주요 구성 모듈

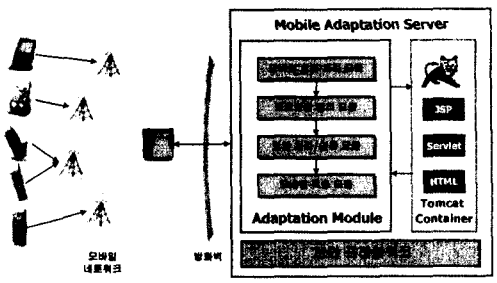

그림 1 개발된 보안 서비스 구조의 전체 개념도

2장에서 제시된 두 가지 요구사항을 만족시키기 위해, 본 연구에서 개발된 보안 서비스 구조는 다음과 같은 모듈들로 구성되어 있다. 첫 번째는 모바일 환경 적응 시스템과 연동될 수 있는 보안 연동 어댑터 모듈, 두 번째는 모바일 단말의 단말 특성을 분석할 수 있는 모바일 디바이스 프로파일 모듈, 그리고 마지막으로 유·무선 대부분의 응용서버 시스템에서 공통으로 사용되는 보안 서비스 모듈이다. 그림 1은 개발된 보안 서비스 구조가 적용된 시스템의 전체 개념도를 도시하였다. 본 연구에서 사용하는 응용서버 시스템으로, 서블릿[2]이나 JSP 같은 응용 로직을 처리하기 위해, 톰캣[1]을 사용하고 있는데, 톰캣 내에 추가된 모바일 요청 처리 모듈이 무선 단말에 특화된 컨텐츠를 생성 변환하는 기능을 제공한다고 가정한다. 특정 무선 단말이 처리할 수 있는 마크업 언어로 자동 변환해주는 도구는 이미 많은 연구가 있어 왔다[7].

3.1 개발된 보안 서비스 구조의 특징

개발된 보안 프레임워크는 다음과 같은 특징을 갖는다.

- 무선 장치의 프로파일 정보를 자동 인식할 수 있는 무선 디바이스 프로파일 관리 모듈 제공
- 시스템 및 응용 자원의 보안 요구 정도에 따라 다중 인증을 요청할 수 있는 구조를 제공
- 여타의 모바일 환경 적응 시스템에 적용할 수 있는 독립적인 구조를 제공
- 시스템에서 사용하는 보안 시스템 환경과 응용의 요구사항에 따라 동적으로 구성될 수 있는 구조를 제공
- Kerberos, LDAP, File, Database, Certificate 과 같은 다양한 인증 방법을 제공
- JAAS 프레임워크 지원 및 Kerberos 통신 모듈 제공
- 모바일 환경 적응 시스템과 보안 연동할 수 있는 어댑터를 제공(현재는 Tomcat 연동 모듈을 제공함)
- 사용자 역할 기반의 시스템/응용 자원의 보호 방법을 제공

3.2 주요 구성 모듈

개발된 보안 프레임워크의 주요 구성 모듈은 아래와 같이 세가지 기능적인 모듈로 구분할 수 있다. 아래에 설명되는 모듈 중에서 보안 서비스 모듈이 본 논문에서 설명하는 주 기능을 수행하는 모듈이다.

3.2.1 서버 보안 연동 모듈

서버 보안 연동 모듈은 서블릿 컨테이너(톰캣)로 들어가는 클라이언트의 요청을 가로채어, 사용자의 세션과 사용자의 보안 정보를 연계 시켜주는 모듈이다. 즉, 사용자의 인증이 완료된 시점에서 사용자의 인증 정보와 해당 사용자의 그룹 및 역할 정보를 사용자 세션에 등록하여 서버 시스템이 사용자에 대한 보안 정보를 재 요청하지 않도록 하는 기능을 제공한다. 일반적인 시스템에서는 각자의 보안 서비스 모듈이 탑재되어 있어 이를 지원하도록 하고 있지만, 본 연구에서 제공하는 보안 서비스 모듈은 독립적인 구조와 기능을 제공하므로 서버와의 보안 연동을 위한 모듈이 제공될 필요가 있다.

3.2.2 프로파일 관리 모듈

디바이스 프로파일 관리 모듈은 다양한 모바일 디바이스들로부터의 요청 헤더를 분석하여, 무선 단말 사용자의 자동 인증을 지원하기 위한 모듈이다(그림 2). 즉, 디바이스 프로파일

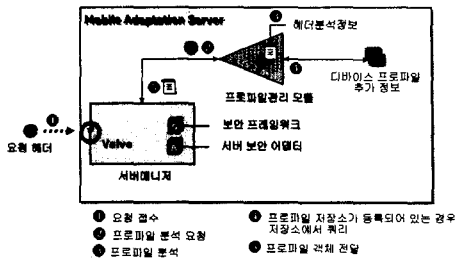

그림 2 프로파일 처리 흐름

관리 모듈은 무선 요청 헤더 속에 포함된 사용자 단말 별로 유일한 특성 정보(통신사, 단말종류, SubscriberID, 등)를 사용하여 사용자가 개입된 인증 절차 없이 사용자를 확인하는 기능을 제공한다.

프로파일 관리 모듈에 의해 분석된 사용자 디바이스 프로파일 정보는 사용자의 자동 인증을 지원하는 용도 이외에도, 무선 디바이스의 브라우저 특징에 맞는 컨텐츠 변환 등에도 사용될 수 있다.

3.2.3 보안 서비스 모듈

보안 서비스 모듈은 본 논문에서 설명하는 모바일 환경 적응 시스템을 위한 보안 서비스 구조의 핵심이 되는 모듈로서, 다음과 같은 세부 모듈로 구성된다.

첫 번째는 보안 관리자(Security Manager) 모듈로 다음과 같은 기능을 수행한다.

- 보안 서비스 프레임워크의 구성
- 서버 시스템의 구동 권한 검사
- 시스템 보안 정책 및 서버 서명용 키 관리
- 인증된 사용자에 대한 서버 신용장 발급
- 하위 보안 서비스 구현 모듈에 대한 접근 통제

두 번째는 보안 도메인(Security Domain) 모듈로 다음과 같은 기능을 수행한다.

- 다중 인증을 위한 다중 보안 영역 구성 지원
- 도메인 보안 정책 관리
- 인증 및 사용자 정보 전달
- 시스템 및 응용 자원 접근 제어 리스트 관리

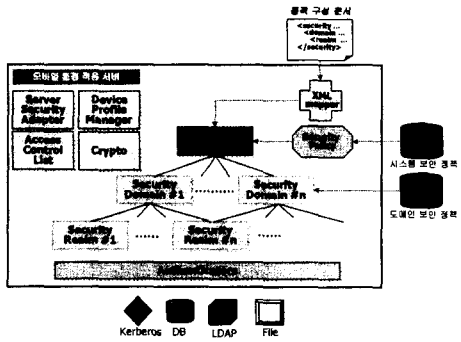

그림 3 보안 서비스 모듈 개념도

세 번째는 보안 영역(Security Realm) 모듈로 다음과 같은 기능을 수행한다.

- 사용자 인증 정보 및 권한 정보(그룹/롤) 관리
- 외부 인증 시스템과의 연동

그림 3에서 보는 바와 같이, 보안 관리자는 하위에 다수의 보안 도메인을 가지고 있는데, 각각의 보안 도메인은 특정 응용의 보안 서비스를 제공하는 주체가 된다. 보안 도메인 하위의 보안 영역은 하나의 공통된 보안 체계에 속하는 사용자, 그룹, 역할을 관리하는 단위로 다중 인증을 위해서는 보안 도메인 내에 다수의 보안 영역을 가지고 있어야 한다.

개발된 보안 서비스 모듈은 다양한 응용 플랫폼에서 독립적으로 보안 업무를 수행할 수 있도록 설계 개발 되었다. 그리고 기업 내 이미 존재하는 보안 시스템의 통합을 고려하여 JAAS[3]를 지원하며, Kerberos[4], DB, LDAP, File 등을 사용한 인증 방법을 지원하고, 역할 기반 사용자 권한 검사 등에 필요한 보안 서비스 API를 제공한다.

4. 보안 서비스 흐름

본 논문에서 설명하는 보안 서비스 구조를 통해, 모바일 환경 적응 시스템은 사용자의 인증 및 접근 제어 서비스를 수행 할 수 있는데, 이러한 서비스를 처리하는 방법에 대해 아래에서 살펴보도록 한다.

4.1 인증

보안 서비스 모듈은 JAAS 인증에 필요한 모듈 및 대부분의 레거시 보안 시스템과 연동할 수 있는 보안 모듈들이 제공되는데, LDAP, Certificate, File, DB, Kerberos 등이 이에 해당한다. 특히 Kerberos는 Kerberos 서버와의 티켓 발급 및 검증을 위한 통신 모듈이 함께 제공되고 있다.

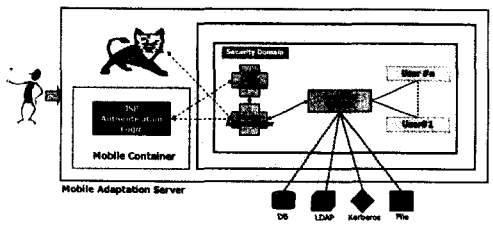

그림 4 인증

인증은 크게 선언적 인증 방법과 비선언적 인증 방법으로 분류할 수 있는데, 선언적 인증을 위해 톰캣의 인증자를 확장한 인증 어댑터를 제공하여 보안 프레임워크와 연동할 수 있도록 하였으며, 비선언적 인증을 위해서는 JSP 혹은 servlet의 로직에서 호출할 수 있는 클래스를 제공하여 인증 서비스를 수행할 수 있도록 하였다(그림 4).

사용자 인증이 정상적으로 수행되면, 보안 관리자는 인증 후에 생성된 사용자의 Subject에 서버 신용장을 발급하여 보안의 강도를 높이는 기술을 추가하였다. 서버 신용장은 불법 사용자가 자신의 인증 정보를 변경하더라도 이를 확인 할 수 있는 방법을 제공한다. 그리고 사용자의 Subject는 인증 정보를 포함하고 있으므로, 다중 인증을 요구하는 응용에서 이를 통해 추가적인 인증이 필요한지를 결정하는데 사용된다.

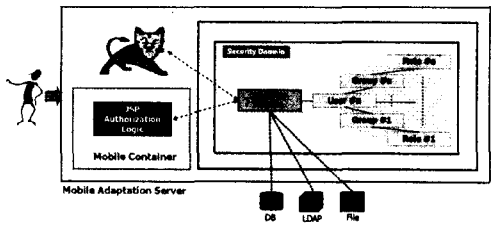

그림 5 접근 제어

4.2 접근 제어

보안 서비스 모듈은 등록된 시스템 및 응용 자원에 대한 접근 제어를 수행할 수 있는 API를 제공하는데, 이러한 API를 통해 응용 개발자들은 배포된 응용에서 사용하는 자원에 대한 사용자의 접근을 통제할 수 있다. 자원 접근 허용 정보는 크게 시스템 접근 제어 정책과 도메인 접근 제어 정책으로 기술되는데, 시스템 접근 제어 정책은 보안 관리자에 의해 관리되며, 시스템 자원에 대한 접근 허용 역할 리스트를 가지고 있으며, 도메인 접근 제어 정책은 해당 도메인에서 관리되어 응용 자원에 대한 접근 허용 역할 리스트를 가지고 있다.

그림 5에서 접근 제어를 수행하는 주체는 톰캣과 응용 로직으로 구분되고 있는데, 응용 로직은 앞서 설명한 API를 통한 접근 제어를 수행하며, 톰캣은 사용자 세션에 등록된 역할 정보에 기반하여, web.xml 파일에 기술되어 있다면, 위치 기반 접근 제어를 수행한다.

5. 결 론

모바일 응용 서비스를 제공하고자 하는 모바일 환경 적응 시스템들은 기존의 응용서버 기술뿐만 아니라 무선 네트워크 환경과 무선 단말의 특성을 이해하고 처리할 수 있는 기술들을 추가적으로 요구한다. 본 논문에서는 이러한 시스템들에 보안 서비스를 제공하기 위해 개발된 보안 서비스 프레임워크를 대상으로, 무선 디바이스 입력 장치의 불편함을 극복하기 위한 자동 인증 기능에 대해 소개하며, 자동 인증 및 무선 환경에서의 보안 취약성을 극복하기 위한 다중 인증 방법을 소개하고 있다. 또한 기존의 유선 시스템에서 제공하는 보안 수준 이상의 보안성을 만족시키기 위한 구조와 다양한 기능적 특징들에 대해 살펴보았다.

6. 참고 문헌

[1] http://jakarta.apache.org/tomcat/index.html
[2] "Java Servlet Specification Version 2.4"
[3] "Java Authentication and Authorization Service(JAAS)," http://java.sun.com/products/jaas/
[4] "Kerberos : The Network Authentication Protocol," http://web.mit.edu/kerberos/www/
[6] "J2EE Specification Version 1.4"
[7] 노명찬, 장철수, 김수형, "Meta-Markup 언어를 이용한 무선 컨텐츠 변환기 구현", 정보과학회 2003 추계학술대회