# 응용서버를 위한 보안 프레임워크 설계 및 구현

김수형, 장철수, 노명찬, 김성훈, 김중배
한국전자통신연구원 인터넷컴퓨팅연구부
e-mail : {lifewsky, jangcs, mcroh, saint, jjkim}@etri.re.kr

# Design and Implementation of Security Framework for Application Server

Soo-Hyung Kim, Choul-Soo Jang, Myung-Chan Roh, Sung-Hoon Kim, Joong-Bae Kim
Dept of Internet Computing,
Electronics and Telecommunications Research Institute

요 약

본 논문은 웹 응용 서버 및 모바일 응용 서버 시스템을 위해 개발된 보안 프레임워크의 설계 및 구현과 관련된 내용을 다루고 있다. 본 논문에서 설명하는 보안 프레임워크는 레거시 보안 시스템과의 연동, J2EE 보안 지원, JAAS 지원, Kerberos 지원 등 응용 서버 시스템들이 요구하는 다양한 보안 기능을 제공하도록 모듈화하여 설계.개발된 것을 특징으로 한다.

## 1. 서론

인터넷 환경에서 다양한 응용의 구축과 실행을 지원하도록 개발된 미들웨어 시스템인 응용 서버 시스템은 응용 구축을 위한 다양한 지원 도구 및 기능들을 포함하고 있으며, 그 중 응용의 보안을 담당하기 위한 보안 서비스 프레임워크는 응용 개발자의 노력을 최소로 하여, 인터넷 환경에서 필수적으로 요구되는 보안 기능을 응용서버 및 응용 서비스 로직에 제공하는 것을 목표로 하고 있다.

본 논문에서 설명하는 보안 프레임워크는 웹 응용 서버 및 모바일 응용 서버 내에 포함되어, 응용 서버 위에 구축된 다양한 웹 응용 및 모바일 응용에게 보안 서비스를 제공하도록 설계•개발되었으며, 레거시 보안 시스템과의 연동, J2EE 보안 지원, JAAS 지원 등, 응용 서버 시스템들이 요구하는 다양한 보안 기능을 제공하도록 모듈화하여 설계.개발된 것을 특징으로 하고 있다.

2 장에서는 예시로 보안 프레임워크가 적용된 응용 서버 시스템 중 하나인, 모바일 응용 서버에 대한 개괄적인 구조와 모바일 사용자 관리 모듈에 대해 설명하며, 3 장에서는 보안 프레임워크의 구조와 환경, 제공되는 서비스들에 대해 설명하며, 4 장에서는 보안 프레임워크의 주요 기능인 인증과 권한 관리에 대해 설명한다. 마지막으로 5 장에서는 본 논문의 결론과 향후 보완해야 할 사항에 대해 다루고자 한다.

## 2. 모바일 응용서버

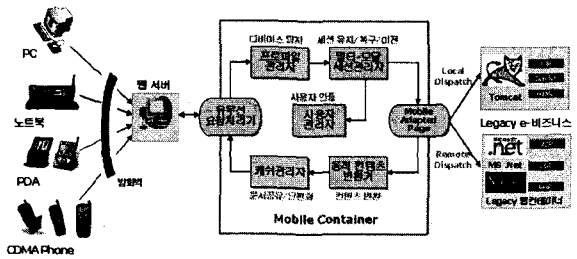


그림 1 모바일 응용서버 흐림도

무선 인터넷 서비스를 제공하기 위한 플랫폼인 모

바일 응용 서버는 휴대폰, PDA 등 다양한 무선 단말을 대상으로 한번 저작된 동일한 컨텐츠를 단말기 종류에 상관없이 제공할 수 있도록 설계•개발되었다. 무선 마크업 언어는 이통사 별로 다양하게 존재하는데, 한번의 저작으로 다양한 무선 마크업 언어를 지원하기 위해, 모바일 응용 서버 시스템은 PWML 이란 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.

그림 1 은 무선 단말을 통해 사용자의 서비스 요청이 집수되었을 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 사용자 관리자를 통해 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.

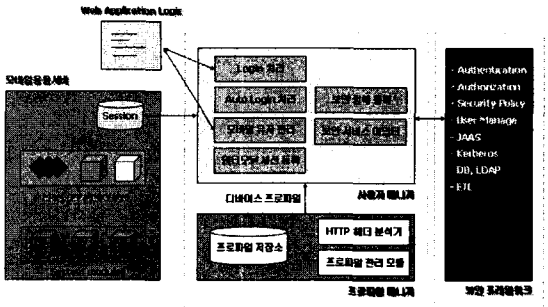


그림 2 사용자 관리 시스템

모바일 응용서버의 기능 모듈들 중, 그림 2 의 사용자 관리자는 모바일 사용자의 인증 및 모바일 응용서버 내 자원들에 대한 접근 권한 관리, 모바일 특화된 보안 서비스를 제공하도록 설계 되었으며, 본 논문에서 설명하는 보안 프레임워크는 사용자 관리자에게 보안과 관련된 API 를 제공하여, 모바일 응용서버 시스템의 사용자 보안을 강화하도록 하였다. 또한 모바일 응용 서버 시스템의 소스 기반 보안 및 자원 보호를 위한 플랫폼을 제공한다.

## 3. 보안 프레임워크의 구조 및 서비스

보안 프레임워크는 다양한 응용 플랫폼에서 독립적으로 보안 서비스를 제공할 수 있도록 설계•개발 되었다. 그리고 기업 내 이미 존재하는 보안 시스템의 통합을 고려하여 JAAS[4]를 지원하며, J2EE 보안 스펙[1] 지원, Kerberos, DB, LDAP, File 기반의 인증 서비스 지원, 역할 기반의 사용자 권한 관리, 인증된 사용자에 대한 정보 제공 기능을 제공하여, 다양한 응용의 보안 요구를 만족시킬 수 있는 기술들이 내포되어 있다.

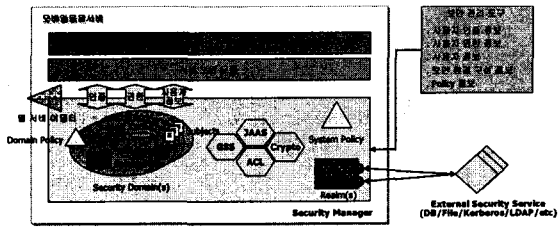


그림 3 보안 프레임워크 구조도

보안 프레임워크는 모바일 응용서버 시스템 및 웹 응용서버 시스템에 적용되어 테스트 되었으며, 그림 3 과 같은 구조를 지닌다. 보안 프레임워크의 모든 서비스는 보안 프레임워크의 보안 관리자에 등록되며, 응용 별로 보안 도메인을 구성하여, 해당 보안 정책과 Realm 을 관리하도록 하였다. 이를 위해, 인증 방법 및 역할에 따른 접근 제어 방법을 환경 파일에 기술하여, 응용 구축자가 원하는 형태로 보안 서비스가 이루어지도록 하였다.

### 3.1 Add-on Module

보안 프레임워크의 사용 예를 들기 위해, 2 장에서 설명한 모바일 응용 서버는 JSP 와 Servlet 을 지원하기 위해 Tomcat 서버와 함께 구성되는데, Java Servlet 스펙[2]에서 요구하는 보안 요구 사항을 만족시키기 위해, Tomcat 의 보안 서비스와 연동하여야 하여야 한다. 보안 프레임워크는 이를 위해, Tomcat 에 Add-on 되는 모듈들을 제공하여, 선언적 보안을 제공하기 위한 Security Realm 어댑터와 명령적 보안을 제공하기 위한 Security Valve 를 둘 수 있도록 하였다.

Security Realm 어댑터는 보안 프레임워크 내에 등록된 Realm 를 선언적인 방법으로 Tomcat 과 연동하도록 구현 하였으며, Security Valve 는 응용 로직 상에서 구현된 보안 로직이 Tomcat 의 보안 서비스와 연동할 수 있도록 세션과 사용자 Subject 를 사용하여 구현하였다.

### 3.2 Security Realms

Security Realm 은 하나의 공통된 보안 체계 안에 속하게 되는 사용자들과 그룹, 역할 등의 목록을 구성하고 있는 단위로, 시스템에 접근하려는 사용자가 인증된 사용자인지를 확인하고 해당 사용자가 어떠한 그룹에 속하며 어떤 역할을 가지고 있는지, 또 사용자

나 그룹이 어떤 자원에 접근이 가능한지를 판단할 수 있도록 하였다. 또한 인증된 사용자의 기본 정보를 제공하여 응용 개발자가 사용자 정보에 접근할 수 있도록 하였다.

아래 텍스트 상자는 'WebDomain'이라는 이름으로 보안 도메인을 구성한 예제이며, 보안 도메인 내에 JDBCRealm 을 두어, Oracle 데이터베이스에 사용자 그룹 및 역할들에 대해 정의하고 사용자 기본 정보를 관리하도록 하였다.

```
<Security defaultDomain="WebDomain">
<SecurityDomain DomainName=" WebDomain " useServerLogger="true">
    <Realm RealmName="JDBCRealm"
      className="org.etri.security.realm.sample.JDBCRealm"
      driverName="oracle.jdbc.driver.OracleDriver"
      connectionURL="jdbc:oracle:thin:@129.254.189.26:1521:ecdir">
    <AuthenticationHandler
className="org.etri.security.auth.sample.JDBCAuthenticationHandler"/>
    </Realm>
</SecurityDomain>
</Security>
```

### 3.3 Configurations

보안 환경 파일은 응용 서버의 전체 보안 정책, 도메인 별 보안 정책, 응용 별 보안 도메인 구성 방법 등을 기술하며, 각각 server.xml, security.policy, web-security.xml 파일로 저장되는데, 보안 관리 도구를 사용하여, 응용 구축자가 직접 관리할 수 있도록 하였다. 보안 관리 도구는 현재, 시스템 및 응용을 위한 환경 설정 파일을 생성.기술하는 도구로서 구현되었으며, 사용자.그룹 관리에 필요한 기능은 제공되지 않는다. 단, 보안 프레임워크는 사용자.그룹 정보를 응용에서 활용할 수 있도록 User 인터페이스를 제공한다.

### 3.4 Session

사용자 세션의 관리는 응용서버 별로 다양한 형태로 제공될 수 있지만, 기본적으로 인증된 사용자 정보가 그 사용자 세션에 등록되어 응용서버의 보안 서비스에 접근할 수 있는 방법을 제공할 것이다. 본 논문에서 설명하는 보안 프레임워크는 3.1 절에서 설명한 Add-on 모듈을 통해, 사용자 세션에, 인증된 사용자의 보안 정보를 등록하도록 하였다. 세션에 등록된 인증 정보는 응용 개발자나 시스템에 의해 활용할 수 있으나 정보의 변경 및 읽기에 제약을 둘 수 있도록 하였다. 그리고 시간 제한에 의한 세션의 파기 시에, 세션 리스너(Listener)와 연동하여, 인증된 사용자는 자동적으로 로그아웃처리 되도록 하였다.

### 3.5 Cluster

응용서버가 클러스터링을 지원하는 시스템에서는 각각의 클러스터 노드가 인증된 사용자에 대한 인증 정보와 세션을 멀티캐스트 프레임워크[3]를 통해 공유하고 있어야 한다. 보안 프레임워크는 인증된 사용자가 클러스터링 환경에서 또다시 인증 작업을 수행하지 않게 하기 위해, 쿠키 또는 커버로스 티켓을 사용하여 단일 인증을 지원하고 있다. 또한 각각의 클러스터 노드들에 대한 상호 인증 및 전송 데이터 보안을 위한 API 를 제공하여, 클러스터링 환경에서의 보안을 지원한다.

### 3.6 SSO(Single Sign-On)

보안 프레임워크는 SSO 를 제공하기 위해, 쿠키 또는 커버로스를 사용하고 있는데, 쿠키의 보안 데이터 설정은 사용자 관리 시스템에서 이루어지며, 서버 시스템의 보안 키로 암호화되어 처리된다. 그리고 응용 서버에서 EJB 를 호출하거나 다른 도메인의 서비스를 호출하는 경우를 위해, Kerberos[5] 및 GSS[6]를 통해 SSO 을 제공할 수 있는 기능을 포함하고 있다.

## 4. Authentication & Authorization

사용자 인증과 권한 관리는 보안 프레임워크에서 제공하는 기본적인 보안 서비스로, Java2 Security Manager 를 통해 소스 기반 접근 제어를 담당하도록 하였으며, JAAS 를 통한 인증 및 역할 기반 보안, ACL 을 통한 접근 제어, 등으로 구성되어 인증 및 권한 관리를 수행하도록 하였다.

### 4.1 사용자 인증

웹 응용 서버 시스템에서 제공하는 가장 기본적인 인증 방법은 브라우저가 사용자 신원 정보를 수집하여 웹 응용 서버에 이를 전달하는 선언적 인증 방법이다. 선언적 인증은 *Basic, Form-based, Client-certificate,* Digest 인증 방법이 있으며[2], 브라우저가 사용자 신원 정보를 수집하는 방법과 웹 컨테이너에 신원 정보를 전달하는 방법에 따라 분류된다. 선언적 인증은 응용 개발자가 선택할 수 있는 가장 쉬운 인증 방법이지만, 응용에서 필요한 완벽한 보안 체계를 제공하지는 않는다. 본 보안 프레임워크에서는 선언적 인증을 위해, 웹 응용 서버에 전달된 사용자 인증 정보를 3.1 절에서 설명하는 Add-on 모듈에서 가로채, 보안 프레임워크를 통해 인증 받도록 하였으며, 이러한 방법으로 보안 프레임워크에서 제공하는 다양한 인증 방법을 사용할 수 있도록 하였다. 그리고 개발자가 직접 응용 로직 상에서 인증을 제어할 수 있도록 하기 위해, 프로그램 인증에 필요한 API 를 제공하였으며, 인증된 사용자의 정보가 보안 프레임워크 및 웹 응용

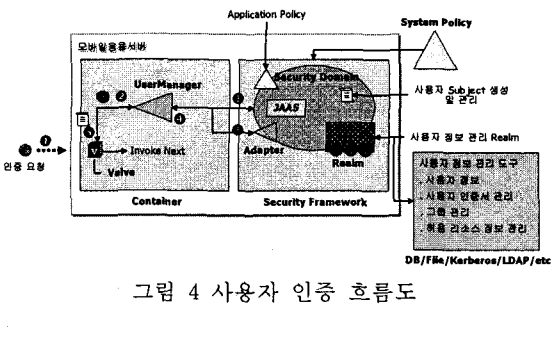


그림 4 사용자 인증 흐름도

서버와 연동되도록 설계되었다.

JAAS(Java Authentication and Authorization Service)는 사용자 인증 및 권한 할당을 위한 프레임워크와 표준 프로그래밍 인터페이스를 제공하며, 사용자 기반 인증 및 권한 부여를 지원하도록 Java2 플랫폼의 액세스 제어 구조를 확장한 PAM(Pluggable Authentication Module) 표준을 기반으로 한다. 보안 프레임워크는 JAAS 를 완벽히 지원하며, 기본적으로 Kerberos, DB, 인증서 기반의 인증을 위한 LoginModule 을 제공한다. 또한 LoginModule SPI(Service Provider Interface)를 통해 특정 LoginModule 를 제공하는 보안 서비스 제공자가 보안 프레임워크와 연동할 수 있는 방법을 제공한다.

그림 4 는 모바일 응용 서버 시스템에서 사용자 인증을 처리하는 과정을 설명한 개괄적인 흐름도이다. 선언적으로 보호된 모바일 응용 서버의 자원에 접근하려는 사용자가 있을 때, 응용 로직 또는 모바일 응용 서버는 사용자에게 인증을 요구하게 된다. 사용자 인증 정보가 모바일 응용 서버에 접수되면, Tomcat Valve 및 모바일 사용자 관리자를 거쳐, 보안 프레임워크로 전달된다. 전달된 인증 정보는 초기 응용의 배포 시에 기술한 인증 방법을 통해 사용자 인증을 수행하고 그 결과를 되돌려 준다.

인증된 사용자의 인증 정보는 3.4 절에서 설명한 바와 같이, 사용자의 세션에 등록되어 관리되는데, 인증 정보는 사용자의 Subject 객체로 표현된다. Subject 객체에 대한 변경은 인증이 일어나는 시점에만 가능하며, 특별한 상황에서는 보안 프레임워크를 개시한 시스템 Subject 에 의해서만 변경이 가능하도록 하였다.

### 4.2 사용자 권한 관리

사용자가 응용서버의 자원 및 서비스에 접근하기 위해서는 해당 자원 및 서비스에 대한 권한을 가지고 있어야 한다. 또한 응용서버의 보안을 위해서, 응용 개발자의 코드가 불법적으로 시스템 자원에 접근하는 것을 방지하도록 설계되어야 한다. 보안 프레임워크는 이러한 권한 관리 및 접근제어를 위해, JAAS 기반 하의 인증된 사용자의 Principal 을 통한 역할 기반 보안, 자원에 대한 ACL(Access Control List) 관리 서비스를 제공하며, 코드 기반의 접근 보안을 위해 Java 의 Security Manager 를 이용한다.

응용 개발자는 웹 서버의 Request 객체에 대한 isUserInRole 함수를 통해 기본적인 접근 제어를 수행할 수 있으며, 보안 프레임워크에서 제공하는 권한 관리 서비스 API 를 통해 보다 정밀한 접근 제어 로직을 개발할 수 있다.

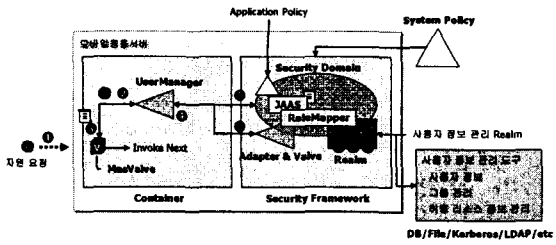


그림 5 접근 제어 흐름도

그림 5 는 모바일 응용서버 시스템에서 사용자가 어떤 모바일 응용서버 자원 또는 서비스를 요청하였을 경우에 이를 처리하는 과정을 설명한 개괄적인 흐름도이다. 선언적으로 보호된 모바일 응용 서버의 자원에 접근하려는 사용자가 있을 때, 먼저 인증 과정을 요구하며, 인증이 완료된 이후에 사용자의 Subject 객체를 통해 사용자 Principal 혹은 Group Principal 을 가져오며, 이를 보안 프레임워크에 전달하여 JAAS 혹은 ACL 를 통해 사용자 접근 권한을 체크하고, 접근 권한을 가진 사용자에게 자원 및 서비스에 대한 접근을 허용한다.

응용 로직 상에서 접근 제어를 수행하기 위해서, 보안 프레임워크는 응용이 사용하는 Realm 에 사용자 Principal 과 요구되는 역할을 기반으로 접근 권한을 검사하는 함수를 제공하고 있다.

## 5. 결론 및 향후 연구

응용서버 시스템은 응용이 필요로 하는 다양한 기능들을 제공하여야 하며, 그 중 보안 기능은 인터넷 환경과 같은 공개형 네트워크에서 서비스를 제공하고자 하는 응용에서는 필수적으로 요구된다. 응용이 제공하는 서비스는 다양하기 때문에 그에 따른 보안의 강도와 시스템 또한 다양하며, 응용 서버 내 보안 프레임워크는 이를 만족할 수 있는 기능을 제공하여야 한다. 또한 기존 레거시 보안 시스템과 연동할 수 있는 방법을 제공하여야 한다.

본 논문에서는 레거시 보안 시스템과의 연동, J2EE 보안 지원, JAAS 지원, Kerberos 지원 등 응용 서버 시스템들이 요구하는 다양한 보안 기능을 제공하도록 모듈화하여 설계.개발된 것을 특징으로 하는 보안 프레임워크에 대해서 살펴보았다. 보안 프레임워크는 현재 모바일응용서버 및 웹 응용 서버 시스템에서 테스트되었으며, 커버로스 서버와 통신하는 통신 모듈을 개발하여 보다 강화된 인증 서비스가 가능하도록 하였다.

이후 시스템의 활용도를 높이기 위하여, 보안 프레임워크에서 요구하는 보안 환경 설정을 응용 구축자가 편리하게 작성할 수 있도록 응용서버 구축 도구와 연계한 보안 환경 설정 및 사용자 정보 등록 도구를 개발할 필요가 있다.

## 참고 문헌

[1] "Java2 Platform Enterprise Edition Specification, Version 1.4"

[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