JAAS 在网上阅卷系统中的应用研究

Research on Application of JAAS in Online Marking System

陈晓苏　章丽玲　吴永英　(华中科技大学计算机科学与技术学院 武汉 430074)

摘要:在阐述 JAAS 安全框架的基础上,详细描述了网上阅卷系统认证和授权机制的设计思想,给出了网上阅卷系统安全管理类的实现方法,并简单的描述了用户认证和授权的工作流程。

关键词:J2EE JAAS 基于角色的访问控制 EJB

1 引言

网上阅卷是把传统的人工阅卷积累起来的丰富经验与现代高新技术相结合,以信息技术和电子扫描技术为依托,通过计算机网络完成评卷工作过程。在这种阅卷方式中,评卷教师不再对考生的原始纸质答卷直接评分,而是在网络上对电子化的考生答卷进行评分。与传统的阅卷模式相比,这种阅卷方式具有客观、高效、公正等特点。必须指出,网上阅卷可能会存在不安全因素,如在网络上传输的评分结果易被人窃听或篡改、阅卷教师的身份可能被假冒等等。从提升网上阅卷系统的安全强度出发,本文探讨了如何利用 JAAS (Java Authentication and Authorization Service)技术实现网上阅卷系统的用户身份认证和授权。

2 JAAS 概述

Java 认证和授权服务 JAAS 是组成 J2EE 安全框架的三个 API 之一,它提出了以用户为中心的安全框架,强调通过验证谁在运行代码以及运行者的权限来保护系统免受攻击。

JAAS 实现可插拔的安全认证(PAM: Pluggable Authentication Module),使得上层的 Java 应用程序和底层的安全认证相互分离,这样有利于使用新的登录模块或者更改已有的登录模块而不用修改上层应用。JAAS 的验证机制使用 LoginContext 类实现独立于底层验证技术的登录。在 LoginContext 类的下面是一个或多个动态可配置的登录模块,这些登录模块对应相应的安全机制,处理实际的验证服务,比如一个登录模块对应着执行基于 Kerberos 协议的验证,而另一个登录模块可能对应着执行基于智能卡的硬件方式的验证。SUN 公司提供了几个已经封装好了的 LoginModule 实现,如 JndiLoginModule、Krb5LoginModule、NTLoginModule 等。

JAAS 使用配置文件来指定每个登录模块的认证项。配置文件是一个以 config 为扩展名的纯文本文件,其中包含了 LoginContext 构造函数中引用的应用程序名称以及登录模块列表。由于 JAAS 框架是可扩展的,只要在配置文件中插入所需的 LoginModule,就可以实现相应的认证方法,也可以自己编写 LoginModule。JAAS 中更换 LoginModule 只要修改配置文件即可,无需要修改应用程序。配置文件实例如下所示:

```
Simple{
Com. sun. security. auth. module. JndiLoginModule required;
Com. sun. security. auth. module. Krb5LoginModule optional;
};
```

其中,required、optional 等参数用于指定一个给定的验证过程的成功或失败对总体验证过程的影响。

在 JAAS 推出之前,访问控制以代码为中心,通过了解代码的来源和数字签名者的身份判定其访问的权限。在 JAAS 中,通过将 Subject(主体)添加到 LoginContext 中,实现基于用户角色的访问控制,即根据谁在执行代码来授予访问权限或拒绝访问。JAAS 的授权可以通过编程和声明两种方式实现。编程方式下,程序通过检查经过认证的 Subject 中的权限特征决定是否授予访问权限;声明方式下,访问控制器通过将包

含在 LoginContext 的权限特征与策略文件中的权限配置进行对比，以决定是否允许敏感操作。

3 JAAS 在网上阅卷系统中的身份认证和授权机制

3.1 设计思想

对于用户的认证，一般的设计思路为：在服务器和客户端两边同时编写登录模块。这样做的好处是客户端和服务器端同时进行认证，从而加大了系统的安全系数，但这样却加重了客户端的负担，也违背了表现逻辑与业务逻辑分离的思想。怎样才能既保证系统的安全，又不加重客户端的负担呢？解决的思路是把客户端的认证信息一次性传递给服务器，并在服务器端通过认证。具体实现方法为：将服务器端的登录模块注册到 JNDI，客户端通过 JNDI 获取登录模块的引用，并直接进行服务器端的登录。网上阅卷系统中，客户端通过 JSP 自定义表单登录的方式提交用户登录请求，该请求被发送给 Servlet 进行处理，Servlet 通过 JNDI 来定位 EJB，服务器端将登录信息序列化为 Invocation 实例，Invocation 中包含了用户详细的认证信息。这样就实现了客户端的认证信息向服务器传递过程，从而只需编写服务器端的登录模块即可。

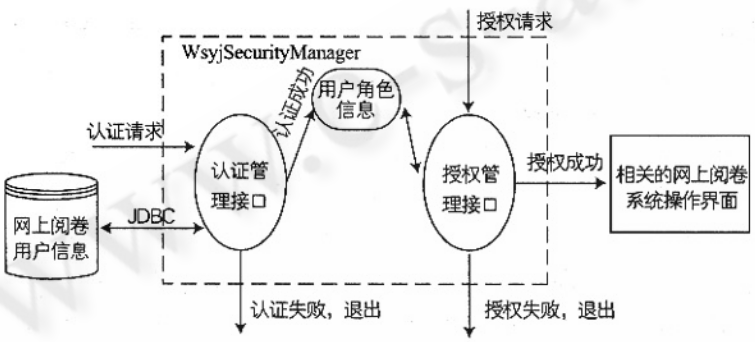

图 1　网上阅卷系统服务器端认证和授权机制架构

网上阅卷系统采用基于角色的访问控制，用户角色采用层次结构，从高级向低级分为系统管理员、科目主管、题组长、小组长、普通评卷员。高级角色只对他下属的低级角色有控制权，对其他的低级角色无控制权，如题组长只能管理小组长，而不能管理普通评卷员。所有角色，由系统管理员管理，系统管理员通过管理控制台负责建立和维护角色以及角色之间的层次关系，分配各角色之间的权限，并根据用户角色的不同授予用户不同的访问权限，如普通评卷员只有评阅试题的权限，而小组长除了评阅试题外，还有管理小组成员和分析统计结果等权限。在服务器端，不使用配置文件来表示用户角色集合信息，因为使用配置文件不能体现用户之间的层次关系以及他们的权限继承关系，因此采用数据库技术。将用户角色放到数据库的用户信息表中，这样既增加了程序的灵活性和安全性，又弥补了修改配置文件繁琐的缺点。图 1 为网上阅卷系统服务器端认证和授权机制架构图。

在图 1 中，安全管理类 WsyjSecurityManager 是实现网上阅卷系统服务器端认证和授权的关键。该类包括两个接口——认证管理接口和授权管理接口，分别实现认证和授权功能。认证管理接口根据客户端传递来的用户信息首先访问数据库，将用户的登录名和口令与数据库用户信息表中的信息核对，如果不存在此用户，认证失败，程序退出；如果存在此用户，取出用户角色信息，并把该信息传递给授权管理接口，由其基于事先定义的角色特权来判断是否允许用户访问所请求的资源。

认证管理接口定义为 AuthencationManager，主要负责验证相关联的 Principal 和 Credential 是否有效，申明认证的方法为：Boolean IsValid (Principal, Credential)。

授权管理接口定义为 AuthorizationManager，主要负责根据事先定义的角色特权来判断经过认证的 Subject 是否有权访问所请求的资源。申明授权的方法为：Boolean DoesUserHaveRole(Principal, RoleSet)。

3.2 WsyjSecurityManager 类的实现

为了保存用户角色信息，定义两个私有域：UserInfo 和 UsersTableCache。其中 UserInfo 域用来存放认证后用户角色信息变量，UsersTableCache 域则是用户信息表缓存，他使用 Principal 作为索引来缓存 UserInfo 信息。WsyjSecurityManager. IsValid ( ) 方法根据传入 Invocation 中的 Principal 和 Credential 进行服务器端的 JAAS 登录。

具体过程：创建登录文本，并传入网上阅卷系统安

全域(WsyjContext)和相关的 Principal 和 Credential;调用其 Login( )方法进行用户认证。

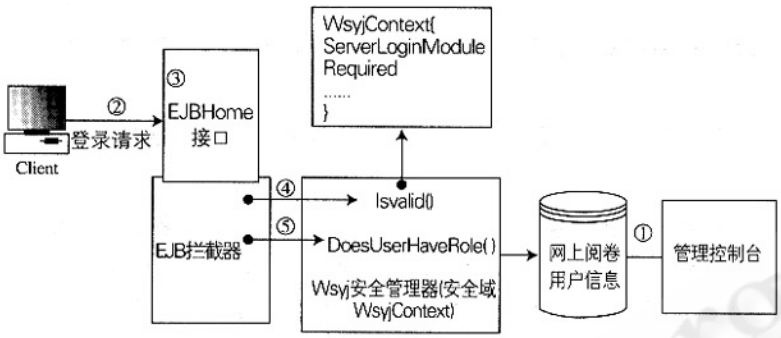

图 2　网上阅卷认证和授权流程

在所给代码中,当 LoginContext 的实例调用 Login( )方法时,首先会调用由网上阅卷系统安全域所决定的登录模块(ServerLoginModule)的 Login( )方法,如果成功,返回 true,如果不成功,返回 false。若返回 true,则调用 ServerLoginModule 的 commit( )方法,这样 ServerLoginModule 中的主体与角色、Principal 和 Credential 等内容相关联,从而完成认证过程。在一次成功登录之后,调用 LoginContext 的 Logout( )方法去除所有的认证状态,同时从用户信息库中取出用户角色信息,赋给 UserInfo 并在 UsersTableCache 中缓存。

WsyjSecurityManager. DoesUserHaveRole( )方法实现用户授权过程,其实现算法如下:

授权前先根据 Principal 遍历 UsersTableCache,如果存在该 Principal,则取出该 Principal 对应的 UserInfo,然后根据事先定义的角色特权来判断是否允许用户访问所请求的资源。如果 UsersTableCache 中没有该 Principal,则说明该用户没有经过认证过程,就调用 IsValid( )方法进行强制认证,认证成功后再调用 DoesUserHaveRole( )方法进行授权。授权成功后,根据用户的角色提供给与用户角色相关的操作界面。

3.3 网上阅卷系统认证和授权流程

图 2 简单地描述了网上阅卷系统用户认证和授权的工作流程,包括:

(1) 系统管理员通过管理控制台设定用户与角色、角色与权限的映射关系和约束关系。

(2) 客户端通过 JSP 自定义表单登录的方式提交用户登录请求,该请求被发送给 Servlet 进行处理,Servlet 通过 JNDI 来定位 EJB 的 Home 接口。

(3) 应用程序取得 EJB 的 Home 接口,请求创建 EJB 实例。此时的请求信息,包括认证所需的 Principal 和 Credential 以 Invocation 类实例的形式传递到 J2EE 应用服务器。

(4) EJB 容器的安全拦截器截获 Invocation,取得 Principal 和 Credential,调用 Wsyj 安全管理器的 IsValid( )方法进行用户认证;若认证成功,继续步骤(5);反之,退出应用程序。

(5) 安全拦截器取得认证成功后的 Subject,调用 Wsyj 安全管理器的 DoesUserHaveRole( )方法进行授权。若授权成功,则根据用户角色提供与之相关的操作界面;反之,退出应用程序。

4 结束语

采用 JAAS 技术实现客户的认证和授权技术,优点在于当出现新的鉴别服务程序或者当前的服务程序过期时,系统管理员可以轻易地将它们插入或者卸载,而不用修改或编辑现有的应用程序。本文采用在 EJB 容器中实现基于 JAAS 技术的网上阅卷系统的认证和授权机制,其特点在于客户端无需编写登录模块,只是简单的将客户认证信息通过 JNDI 传递给服务器端,在服务器端实现认证过程。此外采用基于角色的访问控制,对不同的角色赋予不同的访问权限,较好的保证了网上阅卷系统的使用安全。

参考文献

1 JavaTh Authentication and Authorization Service (JAAS) 1.0 Developer's Guide, http://java.sun.com/security/jaas/doc/api.html.

2 [美] Ed Roman 著,刘晓华等译,精通 EJB(第二版)。北京,电子工业出版社,2003。

3 刘晓华等编著,精通 Java 核心技术。北京,电子工业出版社,2003。

4 王敏、吉逸,Java2 环境下身份认证和授权机制的研究,[J]微机发展,2003,13(5):40-42。