一种基于 Web 的身份鉴别策略及其实现

高克义* 傅 彦

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】 介绍了 Java 服务端网页在 IBM WebSphere 平台上进行电子商务系统开发的相关原理和模型，提出了一种基于 Web 方式的用户身份鉴别策略，改进了以往在对用户身份鉴别时需要自己输入密码的方式。整个处理流程遵循 J2EE 规范，并贯穿了 Web 应用模式的三层体系结构，在存储过程中完成认证，这种方法对提高电子商务系统的安全性有一定的现实意义。

关 键 词 身份鉴别； 电子商务； 密码处理； 安全性

中图分类号 TP393.08

A Tactics of User Identification Based on Web and Its Realization

Gao Keyi Fu Yan

(College of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract This paper introduces the related theory and model about using JSP to develop Electronic Commerce system upon IBM WebSphere,presented an user identification tactics based on Web,modified the method that needs user to input their password by themselves when been identified, the process follow the criterion of J2EE, run through three layers of Web application model system structure, and realize identifying in SP, it is useful in improving the security of the electronic commerce.

Key words user identification; electronic commerce; dealing with passwords; security

IBM WebSphere Studio和IBM WebSphere应用服务器是一个全面基于Java的Web应用架构，它为Web服务开放式标准和完全Java2平台企业版(J2EE)认证书提供集成支持，涵盖了Javaserverlets, Java Server Pages, Java Beans和Enterprise Java Beans，是目前较为理想的电子商务系统的开发平台。同时，目前开发出来的很多Web应用系统在用户登录时采用的密码认证方法大部分还是要求用户自己提供，直接在网页验证，其验证过程是公开的，无法保证用户的隐私和系统的安全性。若采用PKI/CA认证系统，则可以实现对大型系统的安全保证，但将增加开发过程的难度和系统的复杂性。针对这种情况，本文结合对这种平台的介绍，提出一种易于实现的用户身份鉴别策略，在对网络应用有基本安全要求的环境中有一定的应用价值。

1 相关的原理

WebSphere 的核心组件是 WebSphere 应用服务器，它包含 WebSphere Performance Package、Base

2002年7月25日收稿

* 男 31岁 硕士

Http Server、Java Servlet Engine 和 WebSphere Application Server，其数据库连接模块如图1所示。图中，WebSphere Performance Package 的作用主要在于控制和优化系统性能实现负载平衡，提供缓存机制，完成系统文件备份。

WebSphere Application Server 的工作过程如下：客户发出请求后，由 HttpServer 将 Serlet 调用请求交给 Application Server，由 Applicaion Server 和 Java Servlet Engine 执行用户调用 Servlet 进行数据库连接，将 Sql 请求发送给数据库进行处理，数据库将结果返回给 Application Server，Servlet 生成动态页面后将处理结果交给 HttpServer，HttpServer 实现将页面呈现给用户。

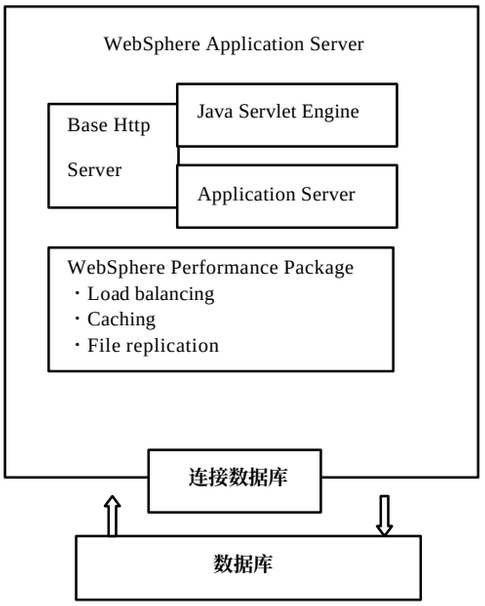

图1　IBM WebSphere 结构示意图

WebSphere 应用服务器对 Java 服务端网页(JSP)的支持是通过 JSP 处理器来实现,在 Web 服务器上安装 WebSphere 应用服务器时，Web 服务器的配置则被设置成对 JSP 文件(即文件扩展名为 jsp 的文件)的 HTTP 请求，并传递至 WebSphere 应用服务器里。WebSphere 应用服务器配置则设置为 JSP 处理器，该处理器不但处理来自客户端的所有请求,还为每个 JSP 文件产生两个文件：

1) java 文件：包含可用于 Servlet 的 Java 语言代码；

2) class 文件：可用于编译过的 Servlet；

由 JSP 文件生成的 Servlet 是 javax servlet http Http Servlet 子的子类或孙类，若 Servlet 类是软件包的一部分，则 Serv-的 let 的 java 代码包含了用于一些必须类和软件包的导入语句。如果 JSP 文件包含 JSP 语法(例如指令和加入网页的 scriptlets)，则 JSP 处理器会将 JSP 语法转换成等价的 Java 代码，如果 JSP 文件包含 HTML 标记，则处理器添加 Java代码，以使 Servlet 能一个一个字符地输出 HTML[1]。

2　应用实例

首先将密码验证放在后台数据库，在存储过程中使数据流的传送穿过 IBM WebSphere 所提供的所有服务接口，读者可以充分了解从客户端的 JSP、JS、HTML 界面程序到中间层的业务逻辑处理程序 Servlet、Java bean、与后台数据库交互的 JSP、Servlet 和 Javabean 程序，最后到直接在数据库中进行数据操作 PL/SQL 存储过程的基于 IBMWebSphere 的应用服务。

2.1 应用背景

应用实例的主要目的是为电子商务交易系统提供一个简单实用的用户身份鉴别手段,为适应客观条件进行的设计。

2.2　系统环境

应用实例建立在 IBM WebSphere 上调用 J2EE 提供的 JavaMail 包，采用的软硬件环境如下[2]：

客户端环境：处理器为 PentiumIII 800 Hz；内存128 M；硬盘10 G；操作系统是 WIN2K Professional; 开发平台 IBM WebSphere Studio4.0；客户端数据库平台 Oracle8.1.7 client；数据库编程平台 PL/SQL；Microsoft IE4.0浏览器；Visual Sourcesafe 源代码版本控制器。

服务器端环境：Pentium III 800 Hz 处理器；256 M 内存；40 G 硬盘；Red hat linux 服务器端操作系统；IBM WebSphere Application Server；MicroSoft IE4.0 浏览器；Visual Sourcesafe 源代码版本控制器。

数据库：Pentium III 800 Hz 处理器；AIX 操作系统；Orcale 服务器端。

2.3 系统配置

在进行应用程序开发之前，需要先配置好系统。因在 WebSphere Studio 里带有 JDK1.1.3，故将 JDK 设置到系统的 CLASS PATH 中，虽然 JavaMail 提供了一个电子邮件系统接口，但为了让其能够运行，还须到 SUN 公司的站点去下载 JavaMail API。SUN 公司是 SMTP 及 IMAP 的服务提供者，还可以到 SUN 公司的网站去下载 POP3邮件服务提供者[3]。

下载的第1个文件为 javamail1_1_3.zip。

将 javamail1_1_3.zip 解压后存入指定的目录，其中一个 mail.jar 即 JavaMail API 的压缩文件，必须将此文件的位置提供给 Windows 操作系统，可在 autoexec.bat 自动执行文件内插入：

set CLASSPATH=％ CLASSPATH%; E:\WebSphere\bin\lib\mail.jar(若指定目录如上)

JavaMail JavaBeans Activation Framework(JAP)软件也必须下载。

下载的第2个文件为 jaf1_0_1.zip。

同样，也要存入指定目录下面，其中一个 activation.jar 即 JAF API 的压缩文件，可在 autoexec.bat 文件中插入：

set CLASSPATH=%CLASSPATH%；E:\WebSphere\bin\lib\activation.jar(若指定目录如上)。

同理，要将包中的 snmp.jar 设进类路径中。

set CLASSPATH=%CLASSPATH%；E:\WebSphere\bin\lib\snmp.jar

安装好 JavaMail 及 JAF API 后，即可发邮件[4]。

2.4 处理流程

首先，用户进入登录界面，如果该用户是合法用户，则输入用户名和密码进入系统；如果是系统用户，则进入注册页面进行新用户注册，在注册页面中填写的信息提交后由系统产生一个随机数密码，并将这个密码用邮件的方式发到用户所填写的邮箱中，同时，这个密码和用户的相关信息均被存入数据库中，其过程如图2所示。

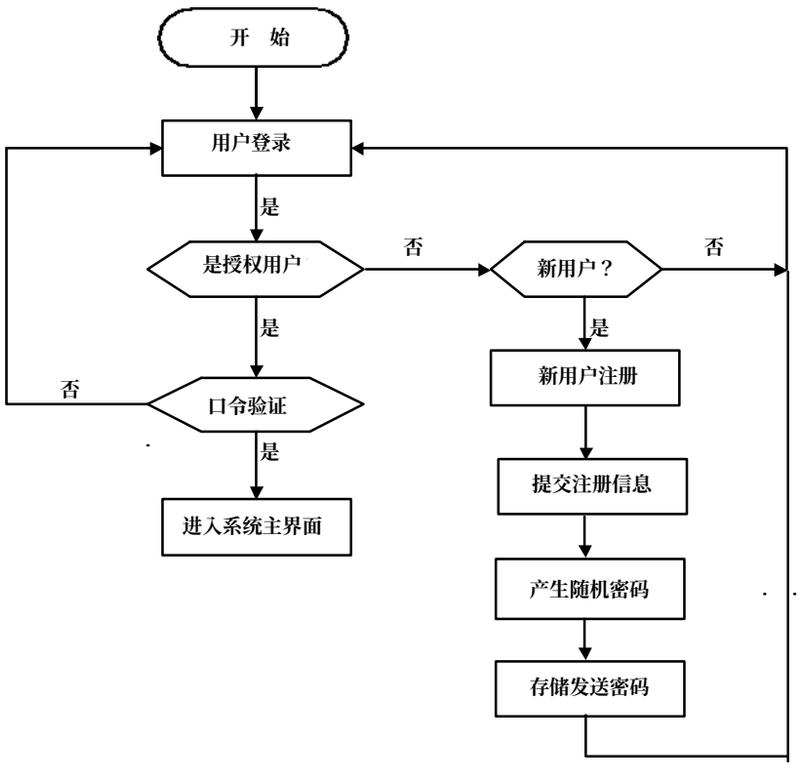

图2 处理流程示意图

用户注册后，将会在自己的邮箱中收到远端系统发送给自己的邮件，在邮件中系统产生随机密码，用户只能使用这个密码去登录远端系统，由远端系统自动执行匹配，和错误检测，将检测结果回送给用户。如果验证通过说明该用户是合法用户，将允许进入系统。

2.5　实现方法

用户登录时所使用的登录界面称为 userlogin.jsp，在这个界面里，用户将输入登录信息，包括：操作员号、会员号、会员密码等字段。用户输入的这些信息将在该页面的 FORM 表单中递交给一个称为 tourlogin.jsp 的 jsp 进行处理，这段 JSP 代码将用户在登录界面中填入的登录字段取出，调用一个专门和数据库交互的 DBProcedure，定义其对象为 dbsp，在对象中调用以 PL/SQL 编写的存储过程实现登录信息与数据库中的字段进行匹配，并在存储过程中进行口令验证，如果没有在存储过程中抛出异常，则用户登录成功，将进入系统的主界面，否则将进行新用户注册。新用户注册页面被命名为 userenroll.jsp。在这个页面中用户将填入注册信息，诸如用户名称、真实姓名、行业、职业、受教育程度和电子邮件地址等，如果填写成功将把这些信息提交给一个称为 enroll.java 的 servlet 来处理。同 login.java 一样，调用公共的数据库连接对象 dbsp，在 dbsp 中调用存储过程将各数据字段连同随机密码填入数据库中，并将密码以邮件方式发送给用户，这里使用了一个发邮件的类对象 Mailbean.java，它实现在程序中将邮件发到用户在注册时提供的邮箱[5]。在 enroll.java 中产生随机数密码是调用 Java 类库中提供的函数，其语句如下：

```
double rnum=Math.random()*100000000.0;
long pnum = Math.round(rnum);
String user_password = String.valueOf(pnum);
```

由此产生一个8位的随机数密码，并将其转换成字符型变量以便于在 Servlet 和存储过程之间进行传递。在 IBM Websphere 的架构下，上述实例的实现方法如图3 所示。

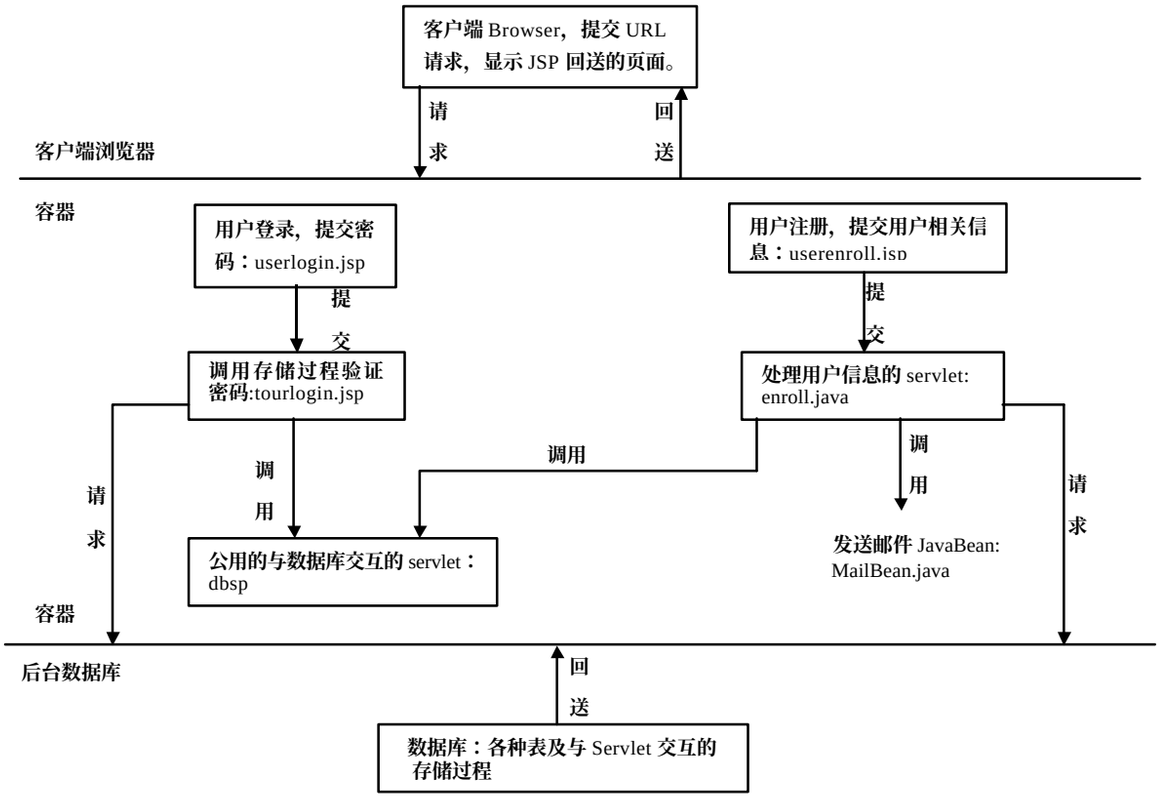

图3　实现方法示意图

3 结 束 语

本文提出的基于Web方式的用户身份鉴别方法，是将用户在帐号申请时填入的注册信息和ervlet产生的随机数密码通过JDBC调用存储过程存入Oracle数据库中，其主要优点如下：1) 密码是随机数，避免了用户用带有自身特征的数据作为密码时容易被熟悉的人猜到，或被恶意破解(目前的破解软件的核心算法大多采用穷举法，其首先检索匹配的将是这些数据)；2) 密码验证过程是在存储过程中进行的由一个专门的Servlet程序来调用存储过程，即所有程序都要通过调用这个封装了存储过程的Servle程序才能实现对用户密码的处理，这样，密码处理过程被屏蔽；3) 密码产生后无须人工发送给用户，可直接在系统中调用Java Mail包用程序发到用户的邮箱中；4) 整个流程只需要在IBM WebSphere的开发平台上实现，所用的语言是目前流行的JSP，所采用的算法非常灵活简便；由于遵循了J2EE的规范，所以具有跨平台、移植能力强的特点。

参 考 文 献

1 林邦杰. JSP交互网站实务经典. 北京：中国青年出版社，2001

2 Vlada M, Beth S 著. J2EE平台上的EJB组件开发. 瞿裕忠，陆海涛，彭晓晖，等译. 北京：机械工业出版社，2001

3 Developing Enterprise Applications with the Java2 Platform, Enterprise Edition, Version1.0, Kassem, Enterprise Team.copyright 2000, Sun Micro systems, Inc.

4 Java2 Platform, Enterprise Edition Specification, Version1.2 copyright 1999 Sun Microsystem, Inc.

5 Java2 Platform, Enterprise Edition, Platform and ComponentSpecification, Shannon, Hapner, Matena, Davidson, PelegriLlopart, Cable, Enterprise Team, copyright 2000, Sun Microsystem,Inc.

· 科研成果介绍 ·

雷达吸波结构机理分析及电磁设计方法研究

主研人员：饶克谨 赵伯琳 高正平 杨华军 饶 力 罗 威 王 卓 苟 益 刘红星

系统地进行了单向和多向碳纤维层板、多向有耗SiC铺层板、加入吸收剂的纺织纤维板雷达反射特性、电磁参数预测方法的研究，完成了预测软件，理论计算结果与实验验证吻合较好；独立开发出了浸渍吸收剂蜂窝板的反射系数和等效电磁参数预测的关键技术，包括研究加入有耗介质的蜂窝结构散射电场的计算和电磁参数预测，完成了预测软件；将遗传算法用于宽频带多层吸波材料的优化设计和电路模拟吸波材料的设计方案探索；进行了吸波结构导流板的机理分析和电磁设计、吸收表面波涂层材料的研究，提出了涂层中表面波的吸波机理分析和设计方法。

·渠 涌·