doi: 10.3969/j.issn.1006-1576.2011.02.015

B/S 系统中跨权访问控制技术

魏玮[1]，张庆[2]，梁文铮[2]
（1. 中国兵器装备集团 信息中心，北京 100089；
2. 中国工程物理研究院 计算机应用研究所，四川 绵阳 621900）

摘要：通过分析 HTTP 请求中的强制访问和信息篡改及伪造问题，设计业务数据访问控制模型和业务活动权限模型，实现了业务数据的访问过滤和业务活动 URL 请求校验。该技术有效地解决了 B/S 系统中的跨权访问问题，实现涉密系统中多维数据的访问控制逻辑。

关键词：访问控制；业务活动；业务数据；面向对象
中图分类号：TP393.08　　**文献标志码**：A

Technique of Access Control Based on B/S System

Wei Wei[1], Zhang Qing[2], Liang Wenzheng[2]
(1. Information Center, China South Industries Group Corp., Beijing 100089, China;
2. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China)

Abstract: Through analyzing the compulsion access in HTTP request and information juggle and forgery, design data access control model and task purview model, and realize access filtering of task data and URL verifying request. The technology can solve the access control problem in B/S system and realize multi-dimension data logic in encrypt system.

Keywords: access control; business activity; business data; object oriented

0 引言

面向对象的 B/S 系统基本由界面类、控制类和实体类构成，界面类和控制类决定了系统的行为，实体类是系统行为操作的数据，整个系统的行为分解就是系统的一个个业务活动。而每个业务活动又体现为一组与业务活动关联的界面对象和控制类对象。目前，B/S 系统中存在 HTTP 请求强制访问和信息篡改等典型的跨权访问问题，由于控制类对象和界面类对象紧密关联，系统只要控制界面类对象的访问，即可控制整个业务活动的访问，故提出一种安全访问控制模型来解决该问题。

1 HTTP 请求中的强制访问及解决措施

B/S 系统通常会把菜单作为控制用户访问系统资源的控制对象，系统将一个功能定义为一个菜单，并把功能的主界面绑定到菜单，将菜单的访问权限分配给某种角色或者用户，用户通过身份认证后，系统根据授权访问的菜单组织界面的导航菜单。由于 B/S 系统中客户端和服务器的交互通过对 URL 资源的请求和响应实现，每次交互都是一次独立的 URL 请求，如果系统没有对每次请求的 URL 资源进行验证合法性，那么恶意用户就能绕过软件界面提供的功能导航，强制访问没有被授权的 URL。

建立一个业务活动权限模型如图 1，业务活动关联一组 URL 资源，角色拥有某些业务活动的访问权限，用户具有某种角色。这样，用户将拥有特定的 URL 资源的访问权限。

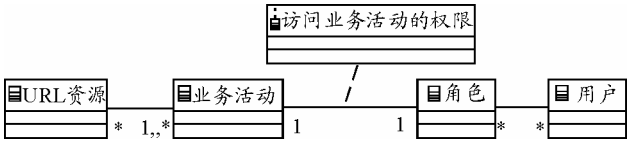

图 1　业务活动权限模型

当用户执行一个业务活动的时候，系统会根据指定的资源链接引导用户请求界面对象。如图 2，JSP-01 的界面处理完后，将跳转到 JSP-02，JSP-02 将弹出一个 JSP-03 的子窗口。为防止恶意用户跨过系统的引导，直接强制请求没有被授权的 URL 资源，系统必须在每个请求响应之前进行检查，一旦发现当前请求的 URL 所属的业务活动没有授权给当前的用户，则系统将停止用户的请求。

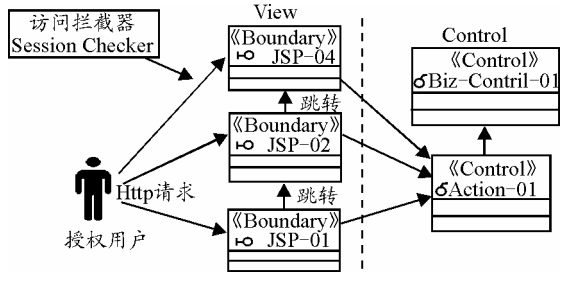

图 2　URL 请求校验示意图

（下转第 65 页）

收稿日期：2010-09-27；修回日期：2010-11-24
作者简介：魏玮（1976—），女，四川人，学士，工程师，从事计算机及网络技术研究。

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

5　结论

经多次实验证明，该测量系统实现了对大型轴类工件的圆度误差在线、动态、高准确度测量。大轴圆度误差测量扩展不确定度为：$U \leq 1.5\ \mu m$（$k=2$）。理论分析和实验结果比较表明，该方法具有较高的测量准确度，可实现数据自动处理，测量过程简单易行，测量装置具有通用性，易于推广。

参考文献：

[1] 玄兆燕, 孙荣平. 滚轮法测量大直径的探讨[J]. 河北理工学院学报, 1998, 20(2): 47-50.

[2] 杨宏宇, 谢丽霞, 殷镇良. 高精度大直径测量的新方法研究与实现[J]. 仪器仪表学报, 2000, 21(6): 597-603.

[3] 王标, 余晓芬, 曾汉平. 高精度大直径在线测量系统数据采集控制方法研究[J]. Key engineering materials, 2008(381): 129-132.

[4] 张宇华, 王晓林. 三点法圆度测量精度分析[J]. 光学精密工程, 1998, 6(4): 127-131.

[5] 费业泰. 误差理论与数据处理[M]. 北京: 机械工业出版社, 2000.

[6] 曾汉平, 余晓芬. 三点法测量大型轴类工件圆度误差分离和评定方法研究[J]. 工业计量, 2008(4): 17-19.

****

（上接第 49 页）

2　HTTP 请求中信息篡改、伪造及解决措施

目前，B/S 系统对数据的操作往往以对象为最小单元，对象的处理过程如图 3。

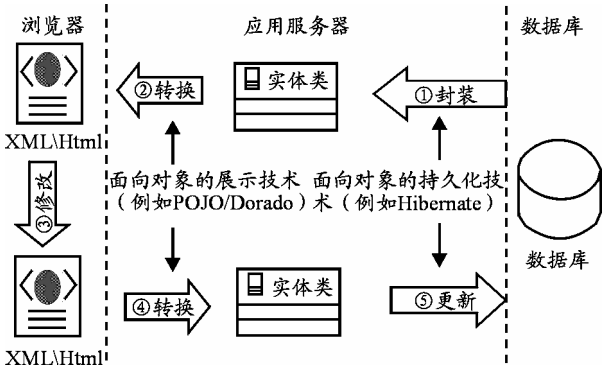

图 3　B/S 系统数据处理示意图

1) 应用服务器从数据库检索一行数据，通过面向对象的持久化技术封装成一个实体类对象；

2) 应用服务器使用面向对象的展示技术，将实体类对象转换成 XML，通过 HTTP 响应传送到浏览器客户端；

3) JavaScript 脚本再次将 XML 封装成 JavaScript 的对象实现界面交互操作，修改对象；

4) 浏览器把修改过的 JavaScript 对象转换成 XML 提交给应用服务器，再次转换成实体类对象；

5) 在应用服务器处理完业务逻辑后，通过面向对象的持久化技术将对象持久化到数据库。

可见，如果在第 4 步之前拦截 Http 提交的请求，分析请求数据，恶意用户可以利用伪造数据和面向对象处理不当的缺陷跨权访问数据。

在保证面向对象的编码技术前提下，建立解决业务数据访问控制的模型，如图 4。

由于业务数据访问控制的核心技术是面向方面的编程技术（AOP），是对部分关心的方法调用进行拦截，通过分析方法所操作的业务数据，是否满足业务数据的多维访问规则，只要有访问规则不通过，则方法的调用失败。这样，即使将实体伪造成另外一个实体对象后，试图在提交给数据库时被拦截，并将作为新的对象进行安全访问过滤，由于新的实体具有不同的安全属性，如果没有被授权给该当前用户，则该请求将被终止。这种访问机制不但能够满足防止篡改和伪造进行跨权访问的控制，而且能够实现多维的安全访问控制的需求。

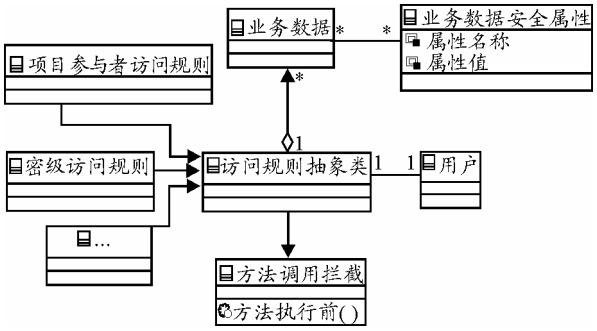

图 4　业务数据访问过滤模型图

3　结语

该技术有效地解决了 B/S 系统中的跨权访问问题。在涉密系统中，对涉密数据的访问存在多种访问规则，也可使用“业务数据的访问控制模型”来实现多维数据的访问控制逻辑。

参考文献：

[1] 熊策. AOP 技术及其在并发访问控制中的应用[J]. 计算机工程与应用, 2005(8): 1-3.

[2] 陆庭辉. B/S 结构下的用户访问控制方法[J]. 计算机工程与设计, 2010(4): 1-3.

[3] 黄凯. 基于角色的 B/S 系统访问控制的研究与应用[J]. 计算机工程与应用, 2009(1): 1-4.

[4] 凯耶尔. Java EE设计模式—Spring企业级开发最佳实践[M]. 北京: 人民邮电出版社, 2010.

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net