文章编号:1000 - 582X(2005)12 - 0059 - 03

基于角色控制的教学权限访问系统的设计与实现*

陈金玉[1],刘东荣[2],李卓伟[3],吴德垠[1]
(1. 重庆大学 教务处,重庆 400030; 2. 深圳市联友科技公司,广东 深圳 518031; 3. 重庆大学 计算机学院,重庆 400030)

摘 要:研究和探讨了实际应用中的用户权限及访问控制设计及实现问题. 以一个教学管理网上系统的权限访问系统实现为例,通过建立一个权限控制矩阵来划分用户的权限访问级别,并结合了动态菜单自动生成、页面跳转限制控制、以及分级打开数据库数据等应用实现方案. 实践表明,基于角色访问控制的权限访问控制系统能严格地控制与防止用户接触与其身份角色不相关的数据信息,有效地避免用户的非法操作,从而切实地提高系统的可用性和健壮性.

关键词:角色控制;RBAC;访问控制;权限管理;教学管理
中图分类号:TP309.2 **文献标识码**:A

教学管理工作是学校管理工作的核心,它对教学过程进行合理的计划、组织、调控、监督、引导及服务,是建立稳定的教学秩序和良好的教学运行机制,保证教学工作正常进行的关键. 近年来,由于高校规模的不断扩大和招生人数的逐年递增,对于传统教学资源的开发、应用、组织与更新都提出了新的要求. 教学管理工作的数字化无疑是优化教学资源、实现教育现代化的重要手段.

同时,由于 Internet 的发展及基于 Internet 服务的迅速崛起,基于 WEB 的教学管理信息系统以其独特的优势,已成为现代管理系统的主流[1-3]. 应该看到,Internet 的开放性不仅仅带来了方便,也引发了许多安全问题. 如何采用可靠的访问控制管理机制来防止信息的外泄,是包括教学管理系统在内的任一系统设计都要面临并须解决的重要问题.

结合重庆大学新"重大教学"教学管理网上系统权限的访问控制子系统设计,讨论了如何运用角色控制技术来实现管理系统的访问权限控制. 实践表明,基于角色访问控制的教学权限访问控制系统能严格地控制与防止用户接触与其身份角色不相关的数据信息,有效地避免用户的非法操作,从而切实地提高了系统的可用性和健壮性.

1 用户权限管理的常用方法

用户权限管理通常有 3 种方法[4-6]:

1) 强制访问控制技术(Mandatory Access Control,简称 MAC). 它采用预先定义用户、及信息的级别,并通过比较这两者的级别来进行合法性验证,是系统强制主体服从事先制定的访问控制策略. 其缺点是这种事先的权限划分与现实可能存在一定的差距. 同级的数据之间缺乏控制机制,且整个体系是事先制定的,修改比较繁琐.

2) 自主访问控制技术(Discretionary Access Control,简称 DAC). 该技术是在确认主体身份及所属组的基础上,对访问进行限定的一种控制策略,访问控制策略保存在一个矩阵中,矩阵的每个元素表示一个主体对一个客体的访问控制. 其优点是比较直观、易于理解,缺点是当系统关系较为复杂时,对用户权限的修改变得十分困难.

3) 基于角色的存取控制技术(Role - Based Access Control,简称 RBAC). 相对于强制访问控制和自主访问控制技术,RBAC 已成为公认的最有发展潜力的存取控制策略. 其核心思想就是将访问权限与角色相联系,通过给用户分配合适的角色,让用户与访问权限相联系.

在 RBAC 技术中,角色作为一个桥梁,沟通于用户和资源之间. 对用户的访问授权转为对角色的授权,然后再将用户与特定角色联系起来. 用户只有通过角色才享有该角色所对应的权限,从而访问相应的客体. 一个用户可以被赋予多个角色,一个角色也可以被赋予多个用户;同样,一个角色可以拥有多项权限,一个权限可以分配给多个角色. 角色的权限即为角色所拥有的功能,表现为对某一子系统或菜单项可执行功能. 所以,一个 RBAC 系统建立起来以后,主要的管理工作即为对角色授权或更改用户的角色.

* 收稿日期:2005 - 07 - 16
基金项目:重庆市科委自然科学基金(102075120050121)
作者简介:陈金玉(1969 -),男,福建仙游人,重庆大学讲师,博士,主要从事控制理论与工程的研究.

2 基于角色控制机制的访问授权

权限是用户对操作所拥有的授权,可以看成是对用户的一种抽象分类. 比如一类部门可以定义为一个权限,一种岗位可以定义为一个权限. 对 WEB 系统而言,权限极限情况是一个个的 WEB 页面集. 用户是权限类的子集,体现业务系统的行政划分. 角色是指操作某一步骤的人员的统称,由一个或多个权限组成,体现了系统对业务的理解. 对教学管理系统的实际使用对象来讲,一般包括:系统管理员、教师、各院教学秘书、教学院长、教务处各科管理员、校级领导、督导组、以及学生等角色分类.

用户、角色、权限之间的关系可表述为:权限是系统最基本关系,权限派生角色,角色决定用户. 对系统内核来讲,没有角色或用户的概念,只有权限的概念,系统管理员通过程序设计者建立的映射机制,构造出一个个角色或用户,其间的授权关系可通过用户表、角色表、权限表、用户 - 角色表、角色 - 权限表进行组织.

其中,用户表用于记录用户的基本信息,权限表用于记录信息系统的每一个独立功能,对应为系统菜单的每一个菜单项,或每一个的基本程序脚本;角色表记录用户登录信息系统时的角色,不同的角色具有不同的权限. 权限是分配给角色的,每种角色所拥有的操作权限由系统管理员通过角色 - 权限表实现. 用户拥有的角色是通过系统管理员授权,通过用户 - 角色表实现的. 其逻辑结构如图 1 所示.

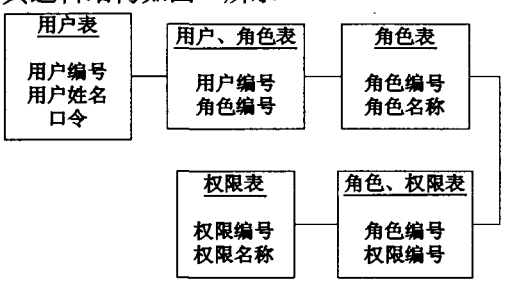

图 1 用户、角色、权限的存储结构

3 访问控制策略的实现

访问控制的实现是教学管理安全子系统的核心和系统安全控制的关键,其执行的好坏直接决定着系统的可靠性与可信性. 以"重大教学"系统为例,分为两个过程:用户的鉴别和用户的访问控制. 包括以下的几个模块,如图 2 所示.

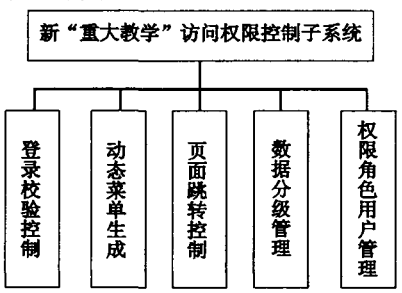

图 2 访问控制策略模型

3.1 用户的鉴别

用户的鉴别是访问控制的基础和关键,是系统安全控制的第一步,在用户登录过程中实施. 用户的鉴别就是向用户索取用户识别信息,如口令、数字签名等,并以此准确地识别用户,判断它是否合法的,还是非法的. 并准许合法用户登录,拒绝非法用户进人数据库系统.

更具体地讲,就是当访问应用系统的主页时,系统要求用户输人用户名和口令进行用户身份认证. 认证合法,则进入访问控制流程,并获得该合法用户的有关信息和他所拥有的访问权限;否则返回注册页面.

3.2 用户的访问控制

当完成系统登录和身份验证后,合法用户成功进入数据库系统并按程序控制中规定的顺序进行数据处理. 此时,访问控制便负责对用户的每一个操作请求进行检查并做出裁决,确保合法的用户执行合法的操作. 具体包括生成动态菜单、页面跳转的控制、以及分级打开数据库数据控制方案等.

3.2.1 菜单动态生成

为简化系统页面,用户对系统的访问是分级进行的. 如对于一般的用户,用户管理功能项是不可见的. 其触发时机是系统认证合法用户进入后,并根据用户的角色分类初始化菜单.

动态生成菜单的实现方式为:首先根据合法登录用户的有关信息,在 RBAC 数据库中查询出用户所对应的角色,其次根据角色拥有的系统资源操作权限动态生成超级链接或菜单. 显然,角色所拥有权限的变化将动态地影响到菜单项的变化.

3.2.2 页面跳转控制的实现

由于 WEB 应用程序的基础是一个个 WEB 页面,所以整个系统功能体现在每个页面上,所有页面的相互调用完成整个系统功能. 但是,由于页面的无记忆性和独立性,使页面的访问实际上是通过 URL 实现的,如果程序不对每个页面进行合法性检验,那么非法用户即使不知道用户名和口令,但只要知道某些页面的 URL,也可以跳过身份验证的页面去直接访问后面的和数据处理的相关页面,从而入侵到系统的核心数据库中. 针对上述问题,可在 WEB 服务器上建立一个 WEB 用户访问页面的权限表,其操作权限匹配表如下:

操作权限匹配表的配置方案是根据矩阵来实现的,行是角色名,列表示为某个具体区域资源划分块名. 各个行列号交叉点存放的数据就是标志具体组对具体记录或区域的操作权限. 权限具体可划分为无权(None)、查询(Search)、修改(Update)、录入(Input)、删除(Delete)、全权(ALL)以及相应权限的组合,如查询和修改等. 各种权限用不同的字符代号在矩阵中进行表示,如查询对应于 B,修改对应于 C,查询和修改对应于 G 等等. 角色组对某区域操作权限分配矩阵,如表 1 所示.

表 1　权限分配矩阵

组	1	2	3	4	5	…
权限 1	A	B	G	E	F	
权限 2	D	E	L	K	O	

可以看到,权限的划分共有 18 种组合. 可以通过一个映照来建立角色权限与给定页面的关系. 定义对应关系如下:

code(0) = "A - 0"
code(1) = "B - 1, G - (1,2), H - (1,3), I - (1,4), J - (1,2,3), K - (1,2,4), L - (1,3,4)"
code(2) = "C - 2, G - (1,2), M - (2,3), N - (2,4), J - (1,2,3), K - (1,2,4), O - (2,3,4)"
code(3) = "D - 3, H - (1,3), M - (2,3), P - (3,4), J - (1,2,3), L - (1,3,4), O - (2,3,4)"
code(4) = "E - 4, I - (1,4), N - (2,4), P - (3,4), K - (1,2,4), L - (1,3,4), O - (2,3,4)"
code(5) = "F - 5"

其中如 I - (1,4) 表示角色具有查询及删除权限动作. 这样用户对给定页面的访问控制即可转化为角色权限匹配表与 Code 数组之间的关系,从而达到页面控制的目的.

3.2.3　数据库设计方案

设计一个安全可靠的系统,当用户通过程序访问数据库时,系统会自动根据用户的级别和权限去访问相应的数据,尽管这些权限可以改变. 同样,WEB 环境下的数据库应用是通过 WEB 页面去访问数据库,所以安全是 WEB 应用程序体系结构中一个重要部分,它意味着应用程序必须确保敏感的用户信息,保护运行应用程序的组件和过程免遭未授权者的篡改或窃取.

也就是说,通过采用不同的数据库角色打开不同应用程序块的办法来达到对数据的分级调用与保护. 首先,赋予数量合适的数据库用户以不同级别的权力和多个特权,这些用户可能等同于应用程序的角色,也可以是自主的;然后建立这些授权用户与系统应用程序块的对应关系,并通过这些用户来访问数据库数据. 更具体一点就是,当利用 ADO 技术联接数据时,不同应用程序块对应不同的数据库用户不同,从而达到保证数据库数据,来增加系统的健壮性.

4　结　语

从系统开发的角度,详细讨论了用户角色权限的构成及系统访问控制策略. 实践表明,基于角色访问技术安全策略能够有效地对通过 WEB 页面访问数据库进行保护,实现基于角色的数据分级目的和流程的自动化.

参考文献:

[1] 祖峰,熊忠阳,冯永. 信息系统权限管理新方法及实现[J]. 重庆大学学报(自然科学版), 2003, 26(11):91 - 94.
[2] 智勇. 基于角色的权限管理在教学资源管理系统中的应用[J]. 计算机与现代化, 2003, 95(7):37 - 39.
[3] 高正宪, 李中学. Web 环境下基于角色的访问控制策略及实现[J]. 计算机工程, 2004, 30(8):133 - 135.
[4] 毛碧波, 孙玉芳. 角色访问控制[J]. 计算机科学, 2003, 30(1):121 - 123.
[5] 徐仁佐,郑红军,陈斌,等. 基于角色和上下文的访问控制模型[J]. 计算机应用研究,2004,(12):140 - 142.
[6] 雷浩,冯登国,周永彬,等. 基于量化权限的门限访问控制方案[J]. 软件学报,2004,15(11):1 680 - 1 688.

Design and Implementation of Role-based Access Control in a Teaching System

CHEN Jin-yu[1], *LIU Dong-rong*[2], *LI Zhuo-wei*[3], *WU De-yin*[1]
(1. Instruction Affairs Office, Chongqing University, Chongqing 400030, China;
2. Shenzhen LIAN-YOU Technology CO., LTD, Guangdong 518031, China;
3. Department of Computer Science and Engineering, Chongqing University, Chongqing 400030, China)

Abstract: This paper discusses how to design and implement a security subsystem, which based on the Role-based Access Control technology. By taking a teaching web system as a practical example, the paper establishes an access control matrix, so dynamic menu, page jump, and data access control are loaded. The experimental shows that, the system can controls the access authorized data, and to avoid the illegality access. The practicability and robust in the system is evident.

Key words: role control; RBAC; access control; management of authorization; teaching management

(编辑　吕赛英)