基于 B/S 模式下中小型业务系统用户权限探析

张 兴
(湖南铁道职业技术学院，株洲 412001)

摘 要： 针对目前B/S模式下的业务系统中权限设计的重要性，分析了怎样设计用户权限管理的结构更为灵活，并通过高校实训教学管理系统中用户权限设计这一范例，详细阐述了底层的数据库读取数据关系，实现权限管理，并在业务系统功能页面上进行权限验证，使得业务系统权限管理更为灵活，系统更为安全。

关键词： 计算机程序；B/S 模式；用户权限设计

Perception on User Rights of Small and Medium Sized Business Systems in B/S Model

ZHANG Xing
(Hunan Railway Professional Technology College , Zhuzhou 412001)

Abstract: View of the current B/S model business system privileges the importance of design, analysis of how to design the structure of user rights management more flexible and practical teaching through the University of user rights management system designed in this example, elaborated on the bottom relationship database design, database design and how to read and realize rights management, and system functionality in the business page to verify the permissions, rights management system makes the business more flexible, more secure system.

Key words: Computer program ; B/S model ; Design of user rights

1 引 言

用户权限设计一直是业务系统设计的基础，也是大家讨论的热点，因为几乎涉及到每一个开发的业务系统，同时对于 B/S 模式下的系统来说，权限系统的设计显得尤为重要。C/S 系统因为具有特殊的客户端，访问用户的权限检测可以通过客户端实现或通过客户端+服务器检测实现，而 B/S 中，浏览器是每一台计算机都已具备的，如果不建立一个完整的权限检测，一个“非法用户”很可能就能通过浏览器轻易访问到 B/S 系统中的所有功能。因此，B/S 业务系统都需要有一个或多个权限系统来实现访问权限检测，让经过授权的用户可以正常合法的使用已授权功能，而对那些未经授权的“非法用户”将会把他们彻底的“拒之门外”。

权限设计时既要保证业务系统通过这个权限系统得出来的权限是安全的、是可控的，同时还要让管理员对于用户权限的授予的灵活、方便，不至于为对几百用户的权限授予而焦头烂额。以高校实训教学管理系统中权限的管理为例，对权限系统设计进行详细的建模设计。

2 权限管理的任务

高校实训教学管理系统主要完成高校实训教学的管理，实训教学中会涉及教务处对课程的管理，老师对实训室内上课教室的申请，实训室管理员对教师申请实训室的审核、管理层及学生对实训教学内容及教学地点安排的查询等。根据以上需求，可以分析出权限系统面对的主体有学生、教师及管理人员，而管理人员中还包含了实训室管理员，是可以对申报的实训室进行审核安排，而管理人员中其他人只能去安排的实训室进行查询，便可以得出权限管理需如下 3 个方面的功能。

2.1 用户个人权限

对于不同岗位，不同职责的人员来说，权限是不一样的，这也是业务系统最基本的权限功能，如管理员中某些人可以对实训室申请进行审核，而有些人只能进行查看。

2.2 群组（角色）的权限

在系统中教师是可以对实训室进行申报，教务管理人员可以对教学任务进行安排，而教师的数量可能是几百上千个，如果都按个人权限来处理，会给管理员在进行权限分配时造成负担，且这样会使权限数据库的记录变得庞大，影响系统运行速度。基于此原因引入了按群组（角色）给予权限，按群组给权限后，任何新加入或已在该群组中的个人都拥有该群组的权限。如定义一个“教师群组”把所有的老师纳入该群组，只需把实训室申请功能分配给教师群组，所有在该群里的教师都拥有了这一项功能，这样可以大大减少工作量，提高工作效率。

2.3 权限管理可兼容可扩展

如果有多套业务系统都是基于 B/S 的结构的，也可同时纳入至该权限系统中进行权限管理，而不是一个系统一套权限，每开发一个系统还要对其权限系统进行重开发，以此可缩减成本，并将多套业务系统纳入集中管理。

3 权限管理分析与表设计

数据表是实现权限管理的根本，只有将数据表设计得合理，权限管理才能游刃有余，无论是群组（角色）操作的概念，还是整套权限管理系统的灵活和重用性，都在于数据库

收稿日期：2010-05-18

的设计。

3.1 权限管理分析

首先，分析出需哪些类型的表按设计需求，教师信息表、学生信息表、功能表是基础。教师表用来保存教师的用户名和密码信息，学生信息表用来保存学生用户的基本信息和密码信息，功能表用来保存业务系统的相关功能信息，这是3个独立的基础表。其次要实现不同职责的教师拥有不同权限，需要教师权限表；不同群组不同权限，需要群组表和群组权限表；群组里是有组员的，还需群组人员表。由于学生只享有查询功能，考虑到学生群体用户多的特性，学生的功能专门给出一张学生功能表，共8个表基本可以完成业务系统权限的需求。表的关系如图1所示。

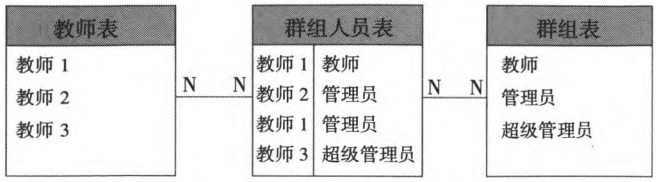

图1 教师表与群组表的关系

教师表和群组表通过群组人员表建立一个多对多的联系，即一个教师可以属于多个群组，一个群组下也可以有多个用户，即一个教师既可为一般教师进行实训室填报，也可以作为管理员对实训室进行管理。

图2所示的教师个人权限通过教师权限表把教师个人的权限建立起关系，一个教师可以有多个权限，同时一个权限也有可能被多个教师使用，所以也是一个多对多的关系表。同理，群组权限库也是一个多对多的关系表，如图3所示。

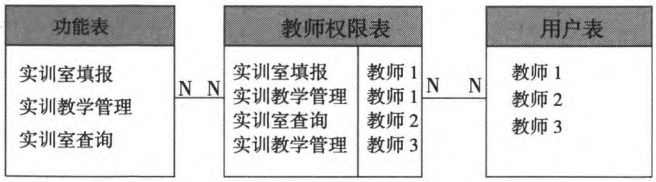

图2 教师个人权限对应关系

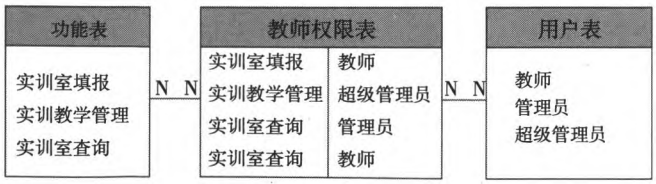

图3 群组权限对应关系

同时，群组表又通过了群组人员表和教师表进行了相互关联，所以分给群组的功能也就相当于分给了相应群组下的所有教师。学生信息表与学生功能表相对来说比较简单，也相互独立，分开检索学生功能表中的数据列给学生使用即可。

3.2 数据表结构

针对以上的分析，进行数据表的设计，首先对系统功能表进行设计，功能表主要是用来存储实训教学管理系统的功能基本信息。对于B/S模式的系统来说，功能表保存的应是功能页的路径或名称信息，功能表如表1所示。

表1 功能表

列名	说明	类型	备注
GNDM*	功能代码	Varchar2 (3)	系统给予功能的代码名，主键
GNMC	功能名称	Varchar2 (20)	功能的名称
GNLXDM	功能类型代码	Varchar2 (2)	分三类，01 系统、02 菜单、03 功能
GNSS	功能所属	Varchar2 (3)	功能所属的业务系统
GNHS	功能函数	Varchar2 (20)	存贮功能页面的路径及页面名称，如 Qxgl/yhgl_add.aspx
SSCD	所属菜单	Varchar2 (3)	如果为功能项，那还需指定该功能应在那一个菜单下
GNBS	功能标识	Varchar2 (1)	标识该功能目前是否启用

功能表用于存储功能的基本信息，当然该功能表还可以将多个业务系统的功能都存入该表中，再按功能类型和功能所属来完成功能的区分。

如表2所示，教师表是相对独对的表，教师表除保存教师的登录密码外不保存任何关于系统权限的信息，以便于能使用权限系统对权限进行分离和方便的管理。

表2 用户表（教师表）

列名	说明	类型	备注
YHDM*	用户代码	Varchar2 (5)	系统给予用户的代码，主键，用于登录
YHMC	用户名称	Varchar2 (16)	用户名称
YHMM	用户密码	Varchar2 (64)	用户密码，通过复杂加密后保存
LXDH	联系电话	Varchar2 (32)	用户联系电话
TXDZ	通信地址	Varchar2 (128)	用户通知地址等信息

表3相当于角色库，也可以认为是一个部门库，该表也只保存群（组）的基本信息，不涉及任何权限相关信息。

表3 群组（组别）表

列名	说明	类型	备注
ZBDM*	组别代码	Varchar2 (5)	系统给予组别的代码，主键
ZBMC	组别名称	Varchar2 (16)	组别名称
JBDM	级别代码	Varchar2 (2)	用于区分该组别的级别，级别自己定义

表4主要用来保存教师与群组的关系，是多对多的关系，两个字段均为主键。

表4 教师群组库

列名	说明	类型	备注
YHDM*	用户代码	Varchar2 (5)	主键
ZBDM*	组别代码	Varchar2 (5)	主键

表 5 主要用来保存教师的功能，是多对多的关系，两个字段均为主键。

表 5 教师权限库

列名	说明	类型	备注
YHDM*	用户代码	Varchar2 (5)	主键
GNDM*	组别代码	Varchar2 (5)	主键

表 6 主要用来保存组别的功能，是多对多的关系，两个字段均为主键。

表 6 组别权限库

列名	说明	类型	备注
ZBDM*	用户代码	Varchar2 (5)	主键
GNDM*	组别代码	Varchar2 (5)	主键

表 7 用于保存学生的基本信息及所属班级信息，学号和班级字段均为主键。

表 7 学生信息库

列名	说明	类型	备注
xh*	学生学号	Varchar2 (5)	主键
Xm	学生姓名	Varchar2 (12)	
Mm	学生密码	Varchar2 (60)	
bj	学生班级	Varchar2 (5)	主键

表 8 用来保存学生的功能信息，由于学生功能有普遍性，所以不需要另外的库进行权限维护。

表 8 学生功能库

列名	说明	类型	备注
GNDM*	功能代码	Varchar2 (3)	系统给予功能的代码名，主键
GNMC	功能名称	Varchar2 (20)	功能的名称
GNLXDM	功能类型代码	Varchar2 (2)	分三类，01 系统、02 菜单、03 功能
GNSS	功能所属	Varchar2 (3)	功能所属的业务系统
GNHS	功能函数	Varchar2 (20)	存贮功能页面的路径及页面名称，如 Qxgl/yhgl_add.aspx
SSCD	所属菜单	Varchar2 (3)	如果为功能项，那还需指定该功能应在那一个菜单下
GNBS	功能标识	Varchar2 (1)	标识该功能目前是否启用

4 权限读取与实现

表设计完成后，接下来就是前台页面来读取相应的权限。权限读取时，首先需要制作一个用户登录页面，如图 4 所示，需要验证用户是不是本系统的用户，即对用户名和密码进行验证，由于面对的群体里有学生，且学生信息与教师数据没有存在于一个功能表中，所以在登录前还需列出用户类型来进行区分。输入用户名和密码验证通过后，由于一个教师有可能存在于多个群组中，可能还存在着拥有操作多个系统的权限，所以还需要进入后的第二个权限选择页，如图 5 所示中需要选择进入哪一个系统和以哪一个组的身份进入。

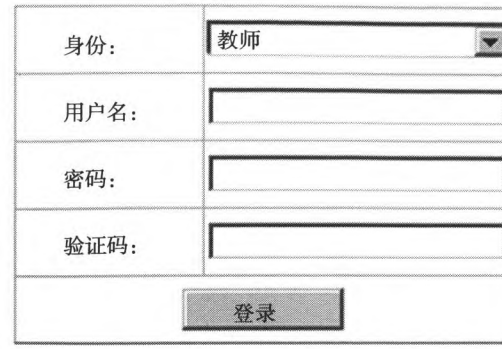

图 4 用户名和密码验证页

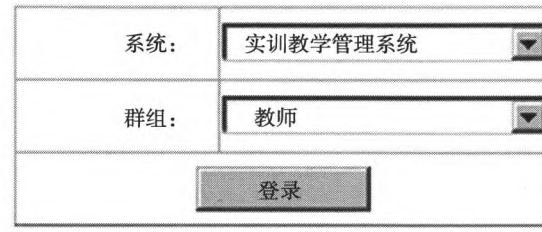

图 5 系统及组别选择页

在第一和第二个页面中，系统可以通过 Session 或 Cookies 记下用户代码和选择系统及选择的组别信息，接下来可以根据这 3 个信息去权限库找出相应的功能。由于实训教学管理系统的主页面为框架结构，如图 6 所示，左则为系统导航菜单，右则为功能显示区，权限通过左则的系统导航菜单进行展示。

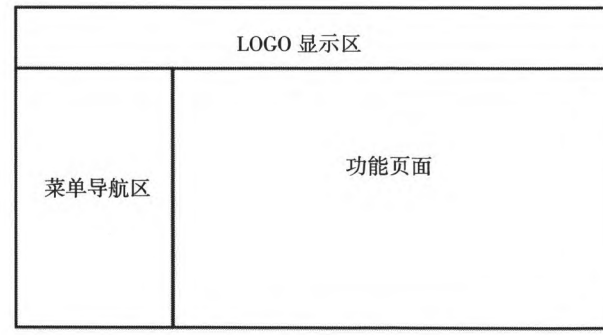

图 6 用户名和密码验证页

由于一个教师可能存在着两种权限，一个是教师特有的权限，即表 5 内的功能，也可能教师所在的群组也有权限，即表 6 内的功能，需要先将这两种权限汇总，去重复后再通过循环的方式把系统的功能列出来，程序相关语句于逻辑如下：

首先将两个权限库中的数据变成一个数据表，并去重复的 SQL 语句。

通过 SQL 语句得到该表后，便可以循环的语句得到系统相关的菜单与功能。

通过以上的循环便可以得到功能导航菜单，通过点击所需功能，链接到相关的功能页面，再在右侧的功能区进行显

示，便完成了根据权限生成相应的系统菜单。

检索权限库的 SQL 语句的代码如下：

```
select distinct * from (
select a.gndm ,a.gnmc ,a.sscd ,b.gnmc as cdmc,a.gnhs
from t_gn a,t_gn b,t_yhgn c
where a.sscd=b.gndm and a.gndm=c.hsdm and a.gnss=系统代码
and c.yhdm=用户代码
union
select a.gndm ,a.gnmc ,a.sscd ,b.gnmc as cdmc,a.gnhs
from t_gn a,t_gn b,t_zbgn c
where a.sscd=b.gndm and a.gndm=c.zbdm and a.gnss=系统代码
and c.zbdm=群组代码) order by sscd,gndm
```

得出菜单功能的逻辑思路的代码如下：

```
    For (int i=0;I < 记录中菜单个数; i++ )
{
  For (int k=0;k < 该菜单下功能个数; k++)
{
  Ouputhtml = "输出菜单的 HTML 代码,并得到指向功能路径的链接";
}
}
```

5 功能页面权限校验

系统导航菜单生成后，便可以通过产生的菜单使用系统。但试想一下，通过上面的操作，系统只是把属于用户的权限显示出来了，如果知道系统功能页面的“非法用户”，只要在地址栏里输入功能页的绝对路径后，仍然可以访问功能页面，如本来某个教师没有实训室的审核功能，只有查询功能，但该教师知道了审核功能的页面地址，便可以在通过页面地址绕过权限系统直接访问该页面，那就给系统的安全性造成了很大的危险。解决这一问题就需要在每一个功能页面加载时也要同时进行功能验证，由于是在每个功能页面加载时都要执行同样的验证操作，便可将要进行验证的语句写成函数，编译成 DLL 以便在不同的系统中进行调用验证。

可以通过系统获取该页面的名称（如：yhgl_add.aspx），再根据页面的名称以及系统登录时获取的用户代码、组别代码等相关信息，去功能表、用户功能表、组别功能表里找是否存在对应的信息，如果存在，返回正确，反之亦然。这样每一个用户在用这个功能页面之前，首先便得到了验证，这样便提高了系统的安全性，让“非法用户”不能进入业务系统之中。

6 结语

通过给高校实训教学管理系统设计权限管理为例，着重对业务系统的权限系统进行了分析与设计。权限管理是每一个业务系统开发的基础，权限管理系统本身并不能服务于业务处理，但是业务系统却离不开权限管理。要使系统权限管理灵活又安全，就需要严谨完善的权限系统设计。权限设计有多种，数据库设计也不尽相同，但是目的都是为了保证业务系统的安全，使得业务系统能更好的处理业务。

参考文献

[1] 苗雪兰．一种信息系统授权管理安全模型及实现方案 [J]．计算机应用与软件，2004，11.

[2] 张晓辉，王培康．大型信息系统用户权限管理 [J]．计算机应用，2000，11.

[3] 苏冠霞，叶念渝．Web 环境下基于 ASP.NET 的用户授权管理[J]．兵工自动化，2005，02.

作者简介

张兴，男（1982-），助理工程师，研究方向：计算机软件。

（上接第 116 页）

x=randsrc (1,50, [4 5 6; 0.1 0.8 0.1])，表示 4,5,6 服从 0.1,0.8,0.1 的概率分布。

4.3 rand 函数

rand 机生成一个在开区间 (0,1) 之间的随机数。

设取值区间为 (a,b)，则要在此区间选取一个 m*n 随机矩阵，程序为：a=rand (m,n) * (b−a) +a 若要求随机数是整数，则添加函数 fix (向零方向去整)、floor (不大于自变量的最大整数)、ceil (不小于自变量的最大整数)、round (四舍五入到最邻近的整数) 即可。

5 结语

在实际应用中很多地方都要用到伪随机数，如何选择生成随机序列的种子参数，以及选用何种随机算法以期生成性能更佳的伪随机序列是计算机软件开发人员追求的目标之一。但是不能一味追求最接近真实的随机数，这是一个很困难的事情，只要把握着够用、实用即可，相信通过不停地尝试总能找到一个合适的方法来生成满足自己条件的伪随机数。

参考文献

[1] 张志勇．精通 MATLAB6.5 版 [M]．北京航空航天大学出版社，2003.

[2] 徐金明．MATLAB 实用教程 [M]．清华大学出版社，北京交通大学出版社，2005.

[3] 求是科技．MATLAB7.0 从入门到精通 [M]．人民邮电出版社，2006.

[4] 姜启源，等．大学数学实验 [M]．清华大学出版社，2005

[5] 王文波．数学建模及其基础知识详解 [M]．武汉大学出版社，2006.

作者简介

张晓军，男（1980-），助教，工学学士，研究方向：计算机应用。

曹惠茹，女（1981-），助教，工学学士，研究方向：数据库应用与开发、嵌入式系统等。