

企业信息系统中的权限管理研究

肖江文¹, 沈国钧^{1,2}

(1. 华中科技大学 控制科学与工程系, 湖北 武汉 430074;

2. 恩施职业技术学院 计算机与信息工程系, 湖北 恩施 445000)

摘 要:在企业信息系统的建设过程中,权限的管理是一个很重要的问题,如果权限管理不当,造成的后果将极其严重。文中针对该问题,从用户管理、功能菜单管理、客户机登录管理等角度综合考虑,提出了一种简洁的通用权限管理思路,规划了相关的数据表,并探讨了其中的部分关键技术。若干大型企业信息系统中的应用情况表明,该方法简洁易行。

关键词:企业信息系统;权限管理;数据表

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2006)08-0146-03

Study on Authority Management in Information Systems of Enterprises

XIAO Jiang-wen¹, SHEN Guo-jun^{1,2}

(1. Dept. of Control Sci. and Eng., Huazhong Univ. of Sci. and Tech., Wuhan 430074, China;

2. Dept. of Computer and Info. Eng., Enshi Vocational and Technical Coll., Enshi 445000, China)

Abstract: Authority management is an important part in development of information systems of enterprises. Improper authority management will result in fearful aftereffect. Aiming at this, presents a terse method of general authority management. Some correlative tables for management of users, menus, objects and clients in enterprises information systems are designed. The key technologies are discussed. In practice, this method has been proved to be successful.

Key words: enterprise information system; authority management; table

1 问题的提出

众所周知,在企业信息系统的建设过程中,权限的管理是一个很重要的问题,以笔者参与过的云南华能澜沧江水电有限公司 YLC-MIS 的建设为例。该公司是由华能电力集团公司、云南省投资公司和红塔集团共同出资组建的股份公司,主要负责云南省境内澜沧江和金沙江的水电开发,从“流域规划”、“工程建设”、“电厂运营”三个方面对这两个流域进行全面开发和管理,其中仅澜沧江上小湾电站的建设资金就达几百亿。如此浩大的工程,相应的 MIS 系统的大型功能模块十来个,涉及的往来单位几百家,日常操作的用户上百人,可登录的客户机也有上百台。如果权限管理不当,造成的后果将极其严重。

所以,如何合理地对企业信息系统中的用户及其权限进行管理,是一个值得多下功夫考虑的问题。文献[1]提出了一种基于岗位角色的用户权限控制管理的方法,通过分配和取消岗位角色来完成用户权限的控制;文献[2]从建立基于角色的权限管理体系出发展开研究,包括体系的

基本元素、角色的特性分析、权限管理模型等关键问题,并提出应用中角色部署的有关策略;文献[3]应用 RBAC 机制把用户角色区分为系统角色和业务角色,并与业务逻辑相结合,提出了一套高效的企业信息系统权限管理解决方案和具体实现方法;文献[4]对多权限信息系统中的授权机制问题进行了研究,提出了动态授权机制和增强的授权机制,并遵循软件复用的思想,利用软件构件技术开发了权限管理构件;文献[5]通过分析传统 RBAC 技术存在的局限,结合现代企业管理的新特点,提出了一种新的基于用户功能项的权限管理机制;文献[6]则尝试设计了一种通用的权限管理工具。

文中基于以上文献所作的研究,从用户管理、功能菜单管理、客户机登录管理等角度综合考虑,提出了一种简洁的通用权限管理思路。以下将以 YLC-MIS 为例,对其中主要的权限管理工作加以介绍。

2 数据表规划

企业信息系统中的权限管理,至少应该包括对用户组和管理、对功能模块和菜单对象的管理以及对客户机登录的管理。

为此,建立如下 3 张数据表:

收稿日期:2005-12-01

作者简介:肖江文(1972-),男,湖南宁乡人,副教授,研究方向为企业信息工程。

表 1 SYS-User 表

列名	列中文名	列类型	可否为空	备注
sys-user-accounts	用户(组)帐号	varchar(10)	NOT Null	主键
sys-user-name	用户(组)名称	varchar(20)	NOT Null	
sys-user-password	用户(组)口令	varchar(20)	Null	加密存储
sys-user-role	所属的用户组	varchar(10)	NOT Null	
sys-user-forbidden	禁止登录	char(1)	NOT Null	0/不禁止、1/禁止
sys-user-memo	备注	varchar(20)	Null	

注:“用户(组)帐号”与“所属的用户组”相同时为用户组,否则为用户。

表 2 SYS-Authority 表

列名	列中文名	列类型	可否为空	备注
sys-authority-code	功能对象代码	varchar(100)	NOT Null	联合主键
sys-authority-name	功能对象名称	varchar(100)	NOT Null	
sys-authority-event	功能对象事件	varchar(30)	NOT Null	联合主键
sys-authority-role	用户组或个人	varchar(250)	Null	各帐号间以“;”分隔
sys-authority-memo	备注	varchar(20)	Null	

表 3 SYS-Client 表

列名	列中文名	列类型	可否为空	备注
sys-client-mac	客户机 ID	varchar(20)	NOT Null	主键
sys-client-name	客户机名称	varchar(40)	NOT Null	
sys-client-login	可登录用户清单	varchar(250)	Null	各帐号间以“;”分隔
sys-client-forbidden	禁止登录	char(1)	NOT Null	0/不禁止、1/禁止
sys-client-memo	备注	varchar(20)	Null	

3 代码实现

在此以 PowerBuilder 编程语言为例,对权限管理的主要代码加以讨论。

3.1 菜单的遍历

在主窗口中建立如下菜单函数 wf-menucontrol,并在 Open 事件中调用:

```

int li-loop, li-cnt, li-loop2, li-cnt2 //用于存放循环变量
string ls-menu, ls-uppername, ls-uppername2, ls-tmp //用于存放菜单名、上级菜单名、临时信息 menu lm-menu //用于存放子菜单项
ls-menu = Lower(ClassName(THIS.menuid)) //处理一级菜单
ls-uppername = Lower(THIS.menuname) //一级菜单名
li-cnt = UpperBound(THIS.menuid.item) //一级菜单的菜单项数目
FOR li-loop = 1 TO li-cnt //遍历一级菜单各菜单项
    lm-menu = THIS.menuid.item[li-loop] //取菜单项
    IF wf-MenuControl2(ls-uppername, lm-menu, ls-menu + String(li-loop * 100, '0000')) = FALSE
        THEN //调用窗口函数 wf-MenuControl2 对数据表 SYS-Authority 中相应记录进行操作
            RETURN //如失败则退出
    END IF
    ls-uppername2 = ls-uppername + ' / ' + Lower(lm-menu.ClassName()) //处理二级菜单
    li-cnt2 = UpperBound(lm-menu.item) //二级菜单的菜单项数目
    FOR li-loop2 = 1 TO li-cnt2 //遍历一级菜单各菜单项

```

```

IF wf-MenuControl2(ls-uppername2, THIS.menuid.item[li-loop].item[li-loop2], ls-menu + String(li-loop * 100 + li-loop2, '0000')) = FALSE THEN //再次调用窗口函数 wf-MenuControl2

```

```

RETURN //如失败则退出

```

```

END IF

```

```

NEXT

```

```

NEXT

```

其中窗口函数 wf-MenuControl2 根据指定的菜单在功能对象授权表中查找其授权角色清单以确定该菜单是否可用,如尚无清单则相应添加一条记录。

3.2 权限综合管理窗口

建立权限综合管理窗口。

窗口的 Open 事件主要内容如下:

……//各 DW 与事务对象连接,功能对象 DW 和客户机 DW 执行 Retrieve 操作

```

wf-ScanTree() //调用窗口函数得到左侧用户树型视图

```

其中窗口函数 wf-ScanTree 主要内容如下:

```

string ls-code, ls-name, ls-tmp //用于存放:用户代码、用户名称、临时信息

```

```

long ll-parent, ll-cur, ll-cur2 //用于存放:父节点句柄、当前节点句柄、当前节点句柄

```

```

int li-loop, li-cnt, li-loop2, li-cnt2 //用于存放循环变量

```

```

treeviewitem ltv-tree //用于存放子节点

```

```

DataStore lds-tmp //临时数据存储

```

……//dw-sys-userlist 检索得到所有用户组和用户信息,并备份到 lds-tmp 中

```

ll-parent = wf-AddItem(tv-user, 3, 4, 0, 'ALL(所有人)')

```

//利用窗口函数 wf-AddItem 添加根节点

```

tv-user.SelectItem(1) //选定根节点

```

```

ltv-tree.Children = TRUE

```

```

dw-sys-userlist.SetFilter('Lower(sys-user-accounts) = Lower(sys-user-role)')

```

```

dw-sys-userlist.Filter() //过滤得到用户组

```

```

li-cnt = dw-sys-userlist.RowCount() //得到用户组数目

```

```

FOR li-loop = 1 TO li-cnt

```

```

    ls-code = dw-sys-userlist.GetItemString(li-loop, 'sys-user-accounts') //取用户组代码

```

```

    ls-name = dw-sys-userlist.GetItemString(li-loop, 'sys-user-name') //取用户组名称

```

```

    ll-cur = wf-AddItem(tv-user, 1, 4, ll-parent, ls-code + '(' + ls-name + ')') //添加一级节点

```

```

    IF ll-cur > 0 THEN

```

```

        lds-tmp.SetFilter('(' + Lower(sys-user-role) = Lower('(' + ls-code + ')') AND (Lower(sys-user-accounts) <> Lower(sys-user-role))')

```

lds-tmp.Filter() //利用备份数据存储过滤得到该组所有用户

```

li-cnt2 = lds-tmp.RowCount() //得到该组用户数目

```

```

FOR li-loop2 = 1 TO li-cnt2

```

```

ls_code = lds_tmp.GetItemString(li_loop2, 'sys_user_accounts') //取用户代码
ls_name = lds_tmp.GetItemString(li_loop2, 'sys_user_name') //取用户名称
ll_cur2 = wf.AddItem(tv_user, 2, 4, ll_cur, ls_code + '(' + ls_name + ')') //二级
IF ll_cur2 > 0 THEN
    //添加成功
ELSE
    DESTROY lds_tmp //添加二级节点失败,取消数据存储
    MessageBox('信息窗口', '生成树型视图出错! 请重试! rr 出错用户:' + ls_code + '(' + ls_name + ')', 'Exclamation!')
    RETURN //退出
END IF
NEXT
ELSE
    DESTROY lds_tmp //添加一级节点失败,取消数据存储
    MessageBox(gs_messbox, '生成树型视图出错! 请重试! rr 出错用户组:' + ls_code + '(' + ls_name + ')', 'Exclamation!')
    RETURN //退出
END IF
NEXT
DESTROY lds_tmp //处理完毕,取消数据存储
tv_user.ExpandAll(ll_parent) //展开树型视图

```

(上接第 145 页)

行金融服务和支付功能,也具有在校园内各类消费和校园管理的功能,其功能主要包括身份验证、存款消费和信息查询。

4.5 系统拓朴结构

本系统校园部分的拓朴结构如图 3 所示。

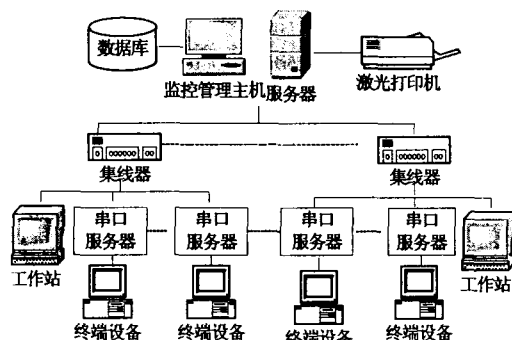


图 3 校园部分的拓朴结构

5 小结

文中的研究成果适合于现代化数字校园信息化的需

tv_user.SelectItem(1) //焦点落在根节点

4 结束语

文中所述方法已成功应用于多个大型企业综合管理信息系统,其中包括上海市苏州河综合整治建设有限公司 SSRCC-MIS 和云南华能澜沧江水电有限公司 YLC-MIS。苏建公司负责上海市苏州河环境综合整治一期工程的建设、管理、融资、还贷,二期工程部分项目的建设管理,注册资金人民币 11 亿元。澜沧江公司主要负责云南省境内澜沧江和金沙江的水电开发,从“流域规划”、“工程建设”、“电厂运营”三个方面对这两个流域进行全面开发和管理,其中仅澜沧江上小湾电站的建设资金就达几百亿。

参考文献:

- [1] 刘清欣,徐 启. 信息系统安全性分析与设计[J]. 企业技术开发, 2004, 23(10): 17-18.
- [2] 曾隽芳,温大勇,杨一平. 电子政务系统基于角色的权限管理研究[J]. 计算机工程与应用, 2004(22): 156-160.
- [3] 王 超,边小凡. 基于角色访问控制机制在 MIS 权限管理中的应用[J]. 微机发展, 2004, 14(5): 50-52.
- [4] 龚洪泉,姚 丹,钱乐秋. 多权限信息系统授权机制的研究与实践[J]. 计算机应用与软件, 2004, 21(4): 16-17.
- [5] 唐成华,陈新度,陈 新. 管理信息系统中多用户权限管理的研究及实现[J]. 计算机应用研究, 2004(3): 217-219.
- [6] 杜宏伟,田盛丰,于 剑. 一个通用权限管理工具的设计与实现[J]. 铁路计算机应用, 2003, 12(1): 6-8.

求,而且能实现银行学校双赢战略,具有普及应用的前景。但是笔者对该领域的研究也刚刚起步,在以后的科研工作中,还有很多尚待研究的问题,如:新兴密钥算法研究;对于小面积指纹、残纹、较干较湿手指的指纹识别算法的研究等等,均有待于去深入研究。

参考文献:

- [1] 彭曙蓉. 射频卡和指纹识别技术在数字校园系统中的应用研究[D]. 长沙:湖南大学, 2003.
- [2] 须文波,朱丽娟,刘 渊. 一种基于指纹识别技术的银行储蓄网络身份认证系统[J]. 计算机应用研究, 2003(6): 67-69.
- [3] 吕知辛,黄遵令. 指纹识别方法及其应用[J]. 计算机系统应用, 2004(5): 32-35.
- [4] 王业琳,宁新宝,尹义龙. 一种新的指纹匹配方法[J]. 中国图像图形学报, 2003(2): 203-208.
- [5] 冯国进,顾国华,张保民. 指纹图像预处理与特征提取[J]. 计算机应用研究, 2004(5): 183-185.
- [6] 王波涛,蔡安妮,孙景鳌. 指纹图像识别技术及其应用[J]. 计算机工程与应用, 2001(7): 79-82.