一种基于角色的权限分配及访问控制模型*

王姝妲, 李　涛, 杨　杰, 胡晓勤, 王丹丹, 黄　锐
(四川大学 计算机学院, 四川 成都 610065)

摘　要: 提出了一种基于角色的权限分配及访问控制模型,并在政府采购系统中实现了该模型。该系统在用户角色分配的基础上加入了权限裁减机制,有效地解决了政府采购系统中错综复杂的访问控制问题,大大降低了系统授权管理的复杂性,提高了权限管理的效率。该系统可配置性强,维护容易。

关键词: 基于角色的访问控制; 权限裁减; 访问控制; 角色
中图法分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1001-3695(2006)10-0183-03

Role-based Permission Assignment and Access Control System

WANG Shu-da, LI Tao, YANG Jie, HU Xiao-qin, WANG Dan-dan, HUANG Rui
(College of Computer, Sichuan University, Chengdu Sichuan 610065, China)

Abstract: A role-based permission assignment and access control system with for government procurement system is presented. This system adds a permission reduction mechanism into user assignment process. It can figure out the complex access control in government procurement system, and decrease the complexity of the authorization and management of users. This system is configurable and can be maintained easily.

Key words: RBAC(Role-Based Access Control); Permission Reduction; Access Control; Roles

政府采购系统是一个拥有大量用户和海量数据资源的电子政务信息平台。利用一个健壮高效的权限分配和访问控制机制来保障整个平台的信息安全显得非常重要。

基于角色的访问控制(Role-Based Access Control, RBAC)[1,2]技术将用户和它的具体权限分离开来,管理员可将用户的授权和权限的划分分别进行处理,给用户授予角色来实现对用户的授权操作。文献[1,3]的调查研究表明,RBAC 降低了安全管理成本和管理复杂性,解决了传统的强制访问控制 MAC[8]和自主访问控制 DAC[8]的管理难度大的问题。

在政府采购系统中,工作人员的职责划分非常灵活。即使同部门的人员,职责范围也会有细微差别,分配的权限也会有所不同。如果采用传统的 RBAC 模型[4~6]需要对各种权限分配情况定义不同的角色。最坏的情况下,可能需要为每一个用户定义一个角色,从而使权限角色分配(Permission Assignment)[3]成为复杂且繁重的工作,增加了授权管理的负担。

针对以上的问题,提出了一种基于角色的权限分配及访问控制模型,并在政府采购系统中实现了该模型。该模型将权限裁减机制引入到用户角色分配(User Assignment)[3]过程中,根据实际情况在授权时对分配给用户的权限进行裁减。这样,既体现了基于角色访问控制的优势,又满足了政府采购系统中授权活动的各种复杂要求,提高了授权管理的效率。

1　系统方案模型

在政府采购系统的授权活动模型中,定义了标准角色集 *SR*,该集合中的元素为实际政务中标准工作职务或工作资格对应的标准角色,系统为这些角色预先分配了其相应职责范围内的所有权限。同时还定义了裁减权限集,在用户角色分配过程中,利用该集合可对标准角色所对应的权限进行必要的裁减,以适应实际授权活动的需要。基于角色的权限分配及访问控制模型如图 1 所示。

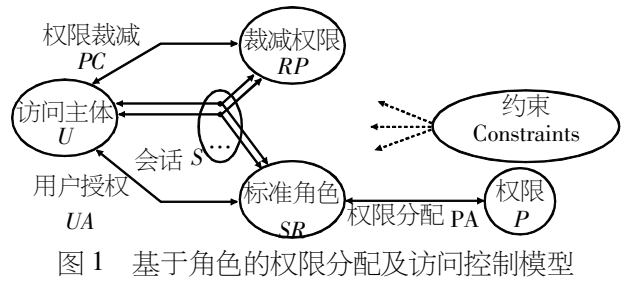

图 1　基于角色的权限分配及访问控制模型

用户集 U:{$u_1, u_2, \cdots, u_n$}, u_i 为第 $i(1 \le i \le n, n$ 为系统中用户的个数$)$ 个用户。其中 $u_i(sn_i)$, sn_i 是用户拥有数字证书的序列号,通过 sn_i 可以唯一地确定一个 CA(认证中心)[7]颁发的数字证书,也就可以唯一地确定拥有该数字证书的用户。

标准角色集 SR:{$sr_1, sr_2, \cdots, sr_m$}, sr_i 为第 $i(1 \le i \le m, m$ 为系统中标准角色的个数$)$ 个标准角色。其中 $sr_i(name_i, PER_i)$, $name_i$ 为标准角色的名称, PER_i 为标准角色拥有的权限集合。在这里, $PER_i \in P$。在政府采购系统中的标准角色有授权管理人员、栏目管理人员、安全管理员、采购执行人员等。

权限集 P:{$p_1, p_2, \cdots, p_l$}, p_i 为第 $i(1 \le i \le l, l$ 为系统中权限的个数$)$ 个权限。其中 $p_i(object_i, ops_i)$, $object_i$ 是对权限 p_i 的操作对象的描述。ops_i 表示 p_i 在操作对象 $object_i$ 上具有某种操作的权限,若 $object_i$ 是采购公告,则 ops_i 可以是增加公告等。

裁减权限集 RP:{$rp_1, rp_2, \cdots, rp_k$}, rp_i 为第 $i(1 \le i \le k, k$ 为系统中裁减权限的个数$)$ 个裁减权限。其中 $rp_i(sn_i, sr_i, flag_i, PRE_i)$, sn_i 是用户的数字证书的序列号。sr_i 表示证书序列号为 sn_i 的用户所分配的某标准角色。$flag_i$ 表示 PRE_i 是否为空

收稿日期: 2005-07-26; 修返日期: 2005-09-05
基金项目: 国家自然科学基金资助项目(60373110); 国家教育部博士点基金项目(20030610003); 四川大学创新基金资助项目

的标志位，也就是表示该用户，在赋予了标准角色 sr_i 后，权限是否经过了裁减。PRE_i 为该用户被分配标准角色时裁减的权限集合。在这里，PRE_i = { PER | (name, PER) = sr_i} 。

会话集 S:{ s_1, s_2, …, s_j} ，会话是用户登录时系统为用户建立的，它完成将用户拥有的相关角色和裁减集合激活。

$UA \subseteq U \times SR$: 用户和标准角色的分配关系，是多对多的关系[3]。

$PA \subseteq P \times SR$: 权限和标准角色的分配关系，是多对多的关系[3]。

$PR \subseteq U \times P$: 用户与标准角色分配关系 UA 和权限裁减对应关系，是一对多的关系。

Constraints(约束):

互斥标准角色对集 EA: $EA \subseteq SR \times SR$, EA 中包含的各标准角色对是互斥的，EA 的约束表达为: $(\forall u \in U)(\forall sr_i, sr_j \in SR)[u \in rm(sr_i) \wedge u \in rm(sr_j)] \Rightarrow (sr_i, sr_j) \notin EA$。

在这里，函数 rm: $SR \rightarrow 2^u$，将一个标准角色映射到所有被分配该标准角色的用户集。

互斥权限对集 $EP \subseteq P \times P$, EP 中包含的各权限对是互斥的，EP 的约束表达为: $\exists (p_i, p_j) \in EP$, $\exists (sr_i(name_i, PER_i), sr_j(name_j, PER_j) \in SR)$, $p_i \in PER_i, p_j \in PER_i \Rightarrow (sr_i, sr_j) \in EA$。

2 设计与实现

2.1 数据模型

图 2 为政府采购系统中的访问控制子系统数据模型的 E-R 图[9]。

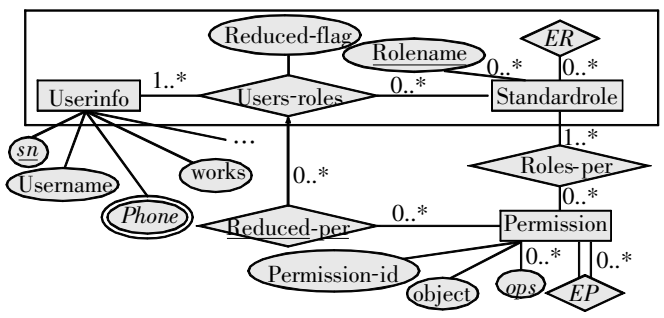

图 2 政府采购系统访问控制子系统 E-R 图

本文将政府采购访问控制系统的数据表达为 Userinfo, Standardrole, Permission 三个实体集以及 Users-roles, Roles-per, Reduced-per, EP, ER 五个联系集。

实体集 Userinfo 表示整个政府采购系统中所有用户的基本信息。它有 sn(数字证书序列号), Username(姓名), Works(工作单位), Phone(电话号码), Identitycard(身份证号)等属性。属性 sn 能够唯一地标志系统中的某一个用户，因此 sn 为 Userinfo 实体集的主码。另外，属性 Phone 为多值属性，即一个用户可能对应一组电话号码。

实体集 Standardrole 表示政府采购系统定义的所有标准角色。其中标准角色名称 Rolename 为最重要的属性，可唯一标志系统设定的标准角色，为该实体集的主码。

实体集 Permission 表示系统中的所有权限。它的属性有 Permission-id(权限号码), Object(权限的操作对象), Ops(对操作对象拥有的权限)。其中 Permission-id 是系统定义的权限唯一标志，为本实体集的主码。

联系集 EP 表示系统中的互斥标准权限对。它是{ ($Permission1_i$, $permission2_j$) | $Permission1_i$, $Permission2_j \in$ Permission } 的一个子集，其中($Permission1_i$, $Permission2_j$) 是一个联系。

联系集 ER 表示系统中的互斥标准角色对。它是{ ($Standardrole_i$, $Standardrole_j$) | $Standardrole_i$, $Standardrole_j \in$ Standardrole} 的一个子集，其中($Standardrole1_i$, $Standardrole2_j$) 是一个联系。

联系集 Users-roles 体现实体集 Userinfo 和 Standardrole 之间的联系，即用户和标准角色的分配关系。该联系集是{ ($Userinfo_i$, $Standardrole_j$) |$Userinfo_i \in$ Userinfo, $Standardrole_j \in$ Userinfo} 的一个子集，其中($Userinfo_i$, $Standardrole_j$) 是一个联系。实体集 Userinfo 与 Standardrole 的映射基数为多对多。也就是 Userinfo 中的一个用户可以分配 Standardrole 中任意数目的标准角色。Standardrole 中的一个标准角色也可以被分配给 Userinfo 中任意数目的用户。因此{ sn, Rolename} 构成了联系集 Users-roles 的主码。同时，我们设置了一个描述性属性 Reduced-flag 与 Users-roles 联系，用来标志该联系集中的每个联系是否参与了联系集 Roles-per。系统中，当 Reduced-flag 值为 TRUE 时，表示参与了 Roles-per; 当 Reduced-flag 值为 FALSE 时，表示没有参与 Roles-per。

联系集 Roles-per 体现实体集 Standardrole 和 Permission 之间的联系，即权限和标准角色的分配关系。该联系集是{ ($Standardrole_i$, $Permisson_j$) | $Standardrole_i \in$ Standardrole, $Permisson_j \in$ Permisson} 的一个子集，其中($Standardrole_i$, $Permisson_j$) 是一个联系。实体集 Standardrole 与实体集 Permisson 的映射基数同样为多对多。也就是 Standardrole 中的一个标准角色可以分配 Permisson 中任意数目的权限。Permisson 中的一个权限也可以被分配给 Standardrole 中任意数目的标准角色。同时，Standardrole 中的所有标准角色必须全部参与 Roles-per 联系集，即每个标准角色必须分配权限。因此，{ Rolename, Permisson-id} 构成了联系集 Roles-per 的主码。

联系集 Reduced-per 表示体现联系集 Users-roles 与实体集 Permisson 之间的联系，即用户角色分配的权限裁减关系。该联系集是{ ($Users\text{-}roles_i$, $Permisson_j$) | $Users\text{-}roles_i \in$ Users-roles, $Users\text{-}roles_i$. Reduced-flag = TRUE, $Permisson_j \in$ Permisson, $\exists$ ($Users\text{-}roles_i$. Rolename = $Roles\text{-}per_k$. Rolename) $\Rightarrow$ $Permisson_j$. Permisson-id $\in$ $Roles\text{-}per_k$. permisson-id} 的一个子集，其中($Users\text{-}roles_i$, $Permission_k$) 是一个联系。Users-roles 与 Permission 的映射基数为多对多。因此{ sn, Rolename , Permission-id} 构成了联系集 Users-roles 的主码。

2.2 主要算法描述

2.2.1 角色—权限分配算法描述

```
be in
  for each ((∏rolename(standardrole) ∏rolename(roles-per)) 中的 standardrole do
  begin
  rolename = standardrole. rolename;
  if 要给 standardrole 分配权限
  for each permission 中权限 permissioni do
  begin
  if 要将 permissioni 分配给 standardrole &&
  ep(permissioni. permission-id, rolename) = = F) then
  将(rolename, permission-id) 添加进 roles-per;
  else
  continue;
  end
  else
  将(rolename, null) 添加进 roles-per;
```

```
    end
    end
```

其中函数 ep 的参数为 permission-id 和 rolename, 用来检查分配给某标准角色的权限与该角色已分配的权限组成的权限对是否属于联系集 *EP*。返回值 *T* 表示属于, *F* 表示不属于。

2.2.2　用户—角色分配算法描述

```
be in
  for each ( ( ∏sn( userinfo) -∏sn( users-roles) ) 中的 sn do
    begin
    if 要给 sn 分配标准角色
      then begin
      for each standardrole 中标准角色 standardrolei do
    begin
    rolename = standardrolej. rolename;
    if ( 要将 standardrolei 分配给 sn&&er( rolename, sn) = = F)
    then begin
    if 要对此次分配裁减权限
      then begin
      将( sn, rolename, TRUE) 添加进 users-roles;
      for each( ∏permission-id( σrolename = " rolename" ( roles-per) ) )
  中的 permission-idi do
      if 裁减权限编号为 permission-idi 的权限
      将( sn, rolename, permission-idi) 添加进 reduced-per;
      else
      continue
      end
      else
    将( sn, rolename, FALSE) 添加进 user-roles;
    end
    else
    continue;
    end
      end
    else
      将( sn, null, FALSE) 添加进 uses-roles;
    end
  end
```

其中函数 er 的参数为 rolename 和 sn, 用来检查分配给某用户的标准权限与该用户已分配的标准角色组成的角色对是否属于联系集 *ER*。返回值 *T* 表示属于, *F* 表示不属于。

2.2.3　用户登录控制算法描述

```
be in
  获得登录用户的证书序列号 sn;
  if σsn = " sn" ( userinfo) ! = Φ
    then begin
    R = ∏rolename( σsn = " sn" ( user-soles) ) ;
    输出: sn 分配的标准角色列表 R;
    输入: 获得用户从 R 列表中选择的标准角色名称 rolename;
     if ∏reduced-flag ( σsn = " sn" ∧ rolename = " rolename" ( users-roles) ) = =
  TRUE;
      then begin
      Ps = ∏permission-id( σrolename = " rolename" ( roles-per) ) ;
      Pc = ∏permission-id( σsn = " sn" ∧rolename = " rolename" ( reduced-per) ) ;
      P = Ps - Pc;
      end
    else
    P = ∏permission-id( σrolename = " rolename" ( roles-per) ) ;
    根据用户的权限列表 P 装载功能菜单;
    end
  else
    输出: 非法用户;
  end
```

3　结束语

在政府采购系统中设计并实现了基于角色的权限分配及访问控制子系统。该系统在用户角色分配的基础上加入了权限裁减机制, 让访问控制实现起来更加灵活, 既体现了基于角色访问控制的优势, 又满足了政府采购系统中错综复杂的访问控制问题。同时, 该系统可配置性强, 升级和维护容易, 使用简单。该系统已投入使用。

参考文献:

[1] andhu R, Coyne E, *et al*. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

[2] Ravi Sandhu, Venkata Bhamidipati, Qamar Munawer. The ARBAC97 Model for Role-based Administration of Roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135.

[3] Ferraiolo D F, Sandhu R, *et al*. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[4] Barka E, Sandhu R. Framework for Role-based Delegation Model [C]. New Orleans, LA: Proceedings of the 16th Annual Computer Security Application Conference, 2000. 168-176.

[5] Gavrila S, Barkley J. Formal Specification for Role-based Access Control User/Role and Role/Role Relationship Management[C]. Virginia: Proceeding of the 3rd ACM Workshop on Role-based Access Control, 1998. 81-90.

[6] Ferraiolo D, Barkley J. A Role-based Access Control Model and Reference Implementation Within a Corporate Intranet[J]. ACM Transactions on Information and System Security, 1999, 2(1): 34-64.

[7] 李涛. 网络安全概论[M]. 北京: 电子工业出版社, 2004. 93-95.

[8] 卿斯汉, 刘文清, 刘海峰. 操作系统安全导论[M]. 北京: 北京科学出版社, 2003. 241-290.

[9] Abraham, Sillberschat, *et al*. Database System Concepts[M]. 北京: 机械工业出版社, 2003. 18-84.

作者简介:

王姝妲(1981-), 女, 四川人, 硕士, 主要研究方向为网络安全与人工智能; 李涛(1965-), 男, 四川人, 博导, 主要研究方向为网络安全与人工智能; 杨杰(1979-), 男; 胡晓勤(1977-), 男, 博士研究生; 王丹丹(1980-), 女; 黄锐(1981-), 男, 硕士研究生。

(上接第 155 页)

[5] Bosworth, T Koshimizu, S T Acton. Multi-resolution Segmentation of Soil Moisture Imagery by Watershed Pyramids with Region Merging [J]. Int. J. Remote Sensing, 2003, 24(4): 741-760.

[6] F Jing, M J Li, H J Zhang *et al*. Unsupervised Image Segmentation Using Local Homogeneity Analysis[C]. Proc. of IEEE International Symposium on Circuits and Systems, 2003.

[7] P D Smet, R L Pires. Implementation and Analysis of an Optimized Rainfalling Watershed Algorithm[C]. Proc. of SPIE, Image and Video Communications and Processing, 2000. 759-766.

[8] 罗玲, 解梅, 陈杉. 基于多尺度形态滤波的分水岭图像分割方法[J]. 计算机辅助设计与图形学报, 2004, 16(2): 168-173.

[9] Haris K, Efstratiadis S, *et al*. Hybrid Image Segmentation Using Watersheds and Fast Region Merging[J]. IEEE Transactions on Image Procosing, 1998, 7(12): 1684-1698.

作者简介:

陈忠(1974-), 博士研究生, 主要研究方向为遥感图像的分类与识别、图像分割等。