２０２０年２月第３５卷第２期

内江师范学院学报
Journal of Neijiang Normal University

Feb. 2020 Vol. 35 No. 2

基于用户组和二维角色管理访问控制策略

荀 全 登[1,2]*

(1. 内江师范学院 计算机科学学院， 四川 内江 641100； 2. Kharkiv State University of Economics， Kharkiv Ukraine 61166)

摘 要：为解决基于角色的访问控制模型不适用大量用户的信息系统，不能为用户的业务数据进行过滤，安全性不高等问题. 提出基于用户组和二维角色管理的安全访问控制模型，将角色权限直接赋予用户组，提高了授权效率，二维角色分为数据和功能两种角色，其中数据角色用来进行用户的选择和数据的过滤，而功能角色用来限定用户进行系统相关操作的权限. 通过在内江师范学院科研信息化平台中的初步应用表明，该模型具有“最少数据”、“最小权限”特性，安全稳定，可扩展性好，较强的通用性.

关键词：用户组；二维角色；安全模型；功能角色；数据角色

DOI：10.13603/j.cnki.51-1621/z.2020.02.009

中图分类号：TP309.2 文献标志码：A 文章编号：1671-1785(2020)02-0043-04

0 引言

伴随着计算机技术、通信技术和互联网技术的快速发展，高等院校的科研平台信息化建设也如火如荼的进行着. 而信息化建设的重点已从信息化管理转移到以应用为主的数字化校园建设上，各高等院校也加强了教学资源系统及应用系统建设，在这些资源被集成和使用的同时，资源的安全显得尤为重要. 对于资源的安全访问，研究人员设计和实现了许多的访问控制系统，这些系统当中，基于角色的访问控制 RBAC (role-based policies access control) 在应用系统中得到了广泛应用[1-3]，但传统的 RBAC 模型以及许多改进的模型中还存在不能对业务数据进行过滤，使得用户通过某种角色获得，就能够对某类业务数据访问，该用户就可以对这类数据的所有实例进行相应的权限执行[4]；安全性不高，保密性不好等缺点[5-6]；对此熊志辉等[4]提出了基于二维角色用以解决传统的 RBAC 模型中存在的问题. 伴随着大型应用系统的不断涌现，系统中用户的不断增加，要为每个用户分配角色和对其角色进行管理，工作量非常大，因此有不少学者将访问控制模型进行扩展和优化[7-17]. 综合分析这些传统的访问控制模型，主要包括用户、角色、权限和会话等几个实体，它的基本思想就是职责划分，建立用户、角色和权限三者之间的授权关系来实现访问控制. 授予用户角色，角色被授予相应权限，权限关联应用系统的相关操作，用户通过授予给他的相应角色来获得该角色相对应的权限从而完成相关操作，这样使得用户和权限之间不再直接联系，简化了权限的分配和管理. 在一定程度上也限制了数据管理员的权利，增强了系统的安全性，但是不适用于用户数量比较多的系统，随着用户数量的增加，角色的数量相应变多，产生冗余. 鉴于此，综合前面文献研究的基础之上，并结合在开发内江师范学院科研绩效管理系统过程中实践，提出了一种基于用户组和二维角色管理的安全访问控制模型，如图 1 所示.

1 基于用户组和二维角色管理的安全访问控制模型

收稿日期：2019-09-30

基金项目：教育部高等教育司产学合作协同育人项目(201701028034)；校级科研重大项目(2019XZ01)

作者简介:荀全登(1974—),男,四川广元人,副教授,博士研究生,研究方向:计算机应用、智慧教育

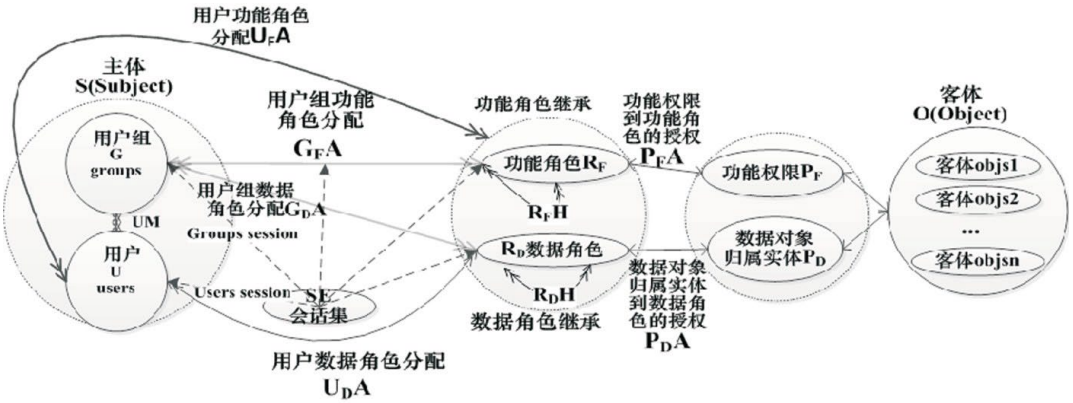

图1 基于用户组和二维角色管理的安全访问模型

1.1 基于用户组和二维角色管理的安全访问模型

定义1 在该模型中,凡是实施操作的用户组称为主体,用集合S表示,$S=\{s_i|1\le i\le n\}$,s_i表示主体集合中的任何一个主体;被操作的数据资源对象称为客体,用集合O表示,$O=\{o_j|1\le j\le m\}$,o_j表示数据资源客体集合中的任何一个客体.

定义2 在该模型中,为了实现"最小权限"和"最少数据"的特性,本文引入二维角色,分别是功能角色和数据角色.R(二维角色集),二维角色为功能角色集$R_F=\{r_{Fi}|0\le i\le m\}$和数据角色集$R_D=\{r_{Dj}|0\le j\le n\}$的笛卡尔积,即$R=R_F\times R_D$,也就是

$R=\{(r_{F0},r_{D0}),(r_{F0},r_{D1}),\cdots(r_{F0},r_{Dn}),(r_{F1},r_{D0}),(r_{F1},r_{D1}),\cdots,(r_{Fm},r_{D0}),\cdots,(r_{Fm},r_{Dn})\}$,在这里引入$r_{F0}$,$r_{D0}$其实是一对并不存在的特殊角色,主要是为了让文章中的二维角色管理能够很好的和以前的一维角色管理兼容.比方说$(r_{F0},r_{Dj})(1\le j\le m)$表示用户只是拥有数据角色,$(r_{Fi},r_{D0})(1\le i\le n)$表示用户只是拥有功能角色.

定义3 在该模型中,基于用户组和二维角色管理的安全访问控制模型中的组成元素.

(1)U(userset)用户集,访问科研系统资源的主体,U表示一个科研用户的集合,即$U=\{u_i|1\le i\le n\}$.

(2)G(user group)用户组,对资源拥有相同权限的用户集合,即$G=\{g_i|1\le i\le n\}$,如具有相同权限的科研秘书用户组.

(3)SE(session set)会话集,会话其实是一个动态的概念,当用户激活用户组时建立会话,一个科研用户可以属于一个或多个科研用户组,所以会话是一个科研用户与多个科研用户组的映射.

(4)UM(user to user group mapping),用户到用户组的映射,即$UM\subseteq U\times G$,这个关系表示一个科研用户可以映射到多个不同的科研用户组中.

(5)RH(role hierarchy),即$RH\subseteq R\times R$,也是一种偏序关系,用$\ge$表示.

(6)U_DA(research user data role assignment)科研用户数据角色分配,表示多对多的科研用户到数据角色的映射关系,即$UDA\subseteq U\times RD$.

(7)U_FA(user function role assignment)用户功能角色分配,表示多对多的用户到功能角色的映射关系,即$U_FA\subseteq U\times R_F$.

(8)G_DA(research user group data role assignment)科研用户组数据角色分配,表示多对多的科研用户组到数据角色的映射关系,即$GDA\subseteq G\times RD$.

9) G_FA (research user group function role assignment)科研用户组功能角色分配,表示多对多的科研用户组到功能角色的映射关系,即 $GFA \subseteq G \times RF$.

10) GH (research user group hierarchy),科研用户组分层,$GH = G \times G$ 表示科研用户组之间的继承关系,也是一种偏序关系,用 $\geq$ 表示 .

11) P_FA (function permission assignment),功能权限多对多的到功能角色的映射关系,表示为 $PFA \subseteq PF \times RF$,其实也就是功能权限到功能角色的授权关系,该功能角色拥有哪些操作权限 .

12) P_DA (data-belonging permission assignment),业务数据归属实体多对多的到数据角色的映射关系,表示为 $PDA \subseteq PD \times RD$,其实也就是该数据角色拥有哪些数据实体 .

定义 4 在该模型中,为了描述方便,二维角色集 R 的元素有时记为 r, 主体 S 拥有的角色集合记为 SR(s);角色 r 对应的主体集合记为 RS(r);客体 O 拥有的角色集合记为 OR(o);角色 r 对应的客体集合记为 RO(r);角色 r 对应的权限集合记为 RP(r);主体 S 基于角色拥有的权限集合记为 SP(s); 客体 O 基于角色允许被使用的权限集合记为 OP(o);所有角色所对应的权限集集合记为 P, $P = P_F \times P_D$.这里的 SR(s)、RS(r)、OR(o)、RO(r)、RP(r)、SP(s)、OP(o)等在本文中都具有二维性质 .

定义 5 在该模型中,用户组缺省角色集 DSet: $G \rightarrow 2^{R\text{是二维角色集}R\text{的一个子集}}$, $\forall u, r, g (u \in g) \in UM \wedge r \in DSet(g)$,换句话说,一个用户映射到某个用户组中他将自动拥有该用户组缺省角色集的所有角色 .如当一个用户登录信息化平台系统时,一个会话被建立并激活用户角色的分配,这个用户分配到的角色包括用户的直接角色分配,用户组缺省角色集 DSet 角色的分配和用户所在用户组所拥有的角色集的继承分配,他将拥有这些角色的所有权限 .

1.2 基于用户组和二维角色管理的访问控制模型中的模块描述

(r) ∪ {p}.

//分别调整功能角色、数据角色和角色的权限集合, $\forall r'_F \in R_F$, $P_F = P_F \cup RP_F(r'_F)$; $\forall r'_D \in R_D$, $P_D = P_D \cup RP_D(r'_D)$; $\forall r' \in R$, $P = P \cup RP(r')$.

//分别修改用户组拥有功能角色、数据角色和角色的权限集, $\forall s' \in RSF(r_F)$, $SPF(s') = SPF(s') \cup RP_F(r_F)$; $\forall s' \in RS_D(r_D)$, $SP_D(s') = SP_D(s') \cup RP_D(r_D)$; $\forall s' \in RS(r)$, $SP(s') = SP(s') \cup RP(r)$

2.4 将角色赋予某用户组主体

Append_rule(s, SR(s), s': r, RS(r), RP(r), RO(r)) //将角色 r 赋予某用户组主体,这里的 r

在 GB-R²BAC 管理模块中,设置了用户组管

= {r_Fi

, r_Dj

), p = {p_Fs

, p_Dt}.

理、角色管理和其它维护三个模块，其中用户组管理，包括用户组的增加、用户组的删除、用户组修改、用户组查询、用户的增加、用户的删除、用户的修改、用户查询等；角色管理包括创建新的角色、删除已有角色、角色赋予主体和主体角色回收等．

2 基于用户组和二维角色管理的访问控制模型的规则

2.1 用户组和用户管理操作

对用户和用户组的管理主要是用户或用户组的添加、删除等操作．

操作 1：add_user(u)，U = U ∪ {u}//添加用户 u；add_group(g)，G = G ∪ {g}//添加用户组．

操作 2：del_user(u)，U = U − {u}//删除用户 u，RS(r') = RS(r') − {u}//修改角色集合所拥有的用户；del_group(g)，G = G − {g}//删除用户组 g，RS(r') = RS(r') − {g}//修改角色集合所拥有的用户组．

2.2 用户组角色的创建

Creat_role(s，SR(s)，r，RS(r)，RP(r)，RO(r))//为用户组主体 S 增加新的角色 r，这里假设 $r = \{r_{Fi}, r_{Dj}\}$．

//分别创建用户组的功能角色集 RF、数据角色集 RD 和角色集 R，$R_F = RF \cup \{r_{Fi}\}$；$R_D = RD \cup \{r_{Dj}\}$；$R = R \cup \{r\}$．

2.3 为角色赋予权限

Append_purview(s，SR(s)：r，RS(r)，RP(r)，p)//为角色 r 授予相应权限 p，r 对应的权限集合 RP(r)，这里的 $r = \{r_{Fi}, r_{Dj}\}$，$p = \{p_{Fm}, p_{Dn}\}$．

//分别刷新 r 对应的功能角色、数据角色分量和 r 对应权限的权限集，$RP_F(r_{Fi}) = RP_F(r_{Fi}) \cup \{p_{Fm}\}$；$RP_D(r_{Dj}) = RP_D(r_{Dj}) \cup \{p_{Dn}\}$；$RP(r) = RP$

//分别在角色 r 对应的功能角色、数据角色和角色 r 的对应的主体集合中添加用户组主体 S'，$RS_F(r_F) = RS_F(r_F) \cup \{s'\}$；$RS_D(r_D) = RS_D(r_D) \cup \{s'\}$；$RS(r) = RS(r) \cup \{s'\}$．

//分别修改用户组主体 S' 拥有的功能角色集、数据角色集和角色集，$SR_F(s') = SR_F(s') \cup \{r_{Fi}\}$；$SR_D(s') = SR_D(s') \cup \{r_{Dj}\}$；$SR(s') = SR(s') \cup \{r\}$．

3 GB-R^2BAC 模型安全访问控制流程

该模型中主要由访问科研资源的主体 S、角色 R（功能角色 RF 和数据角色 R_D）、权限 P（功能权限 PF 和数据归属实体 P_D）、被访问资源的客体 O 和会话 SE 五部分组成．主体对客体访问的主要流程如下．

（1）科研用户输入用户名和口令信息提交后，信息系统读取数据库的用户信息表对用户信息进行验证．验证成功，顺利登陆系统，并将个人信息存入个人会话 SE 中，此时该用户分配到的角色包括用户的直接角色分配，所在用户组缺省角色集 DSet 角色的分配和用户所在用户组所拥有的角色集的继承分配，他将拥有这些角色的所有权限；反之，重新提交信息进行验证．

（2）通过功能角色 RF 对该科研用户进行功能授权，决定他拥有资源的哪些操作权限，实现“最小权限”特性．在这个过程中，首先要对用户－功能角色表进行读取，获取相应的功能角色；然后读取功能角色－功能权限表，获取相应的功能权限，统计出他所拥有的权限集合 SP(s)；最后执行相应操作时，系统进行权限验证，判断其是否具有执行该项操作的权限．

（3）通过数据角色 RD 对该用户进行数据过滤，决定其用户哪些可以访问的数据资源，实现“最少数

据”特性.在这个过程中,首先要对用户-数据角色表进行读取,获取相应的数据角色;然后读取数据角色-数据权限表,获取能够进行访问的数据资源,实现数据资源的过滤,把属于该用户管辖的业务数据
提供其进行相应操作.

4 结束语

基于用户组和二维角色管理的访问控制模型通过在我校科研管理系统中的实际应用,可以充分体现出它很好的为用户业务数据进行过滤,简化用户角色的授权和管理,保证了不同用户组的用户只能操作本组内的数据,增强了系统的安全性,提高了工
作效率.在后续的研究中,将深入研究角色的分组管理、角色等级和继承问题,解决大数据的访问安全.

参考文献:

[1]王益民,茅玉龙,姚坤.改进的RBAC模型在大型OA系统中的应用[J].信息技术,2011(3):142-146.

[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,2004,40(22):156-160.

[3]ZHANG Y, JAMES B D. A role-based administration model for RBAC with hybrid hierarchy [C]. IEEE International Conference on Information Reuse and Integration. As Vegas, NV Press, 2007:196-202.

[4]熊志辉,张茂军,王炜,等.面向安全信息系统的二维角色访问控制模型[J].计算机工程与科学,2008(9):1-3.

[5]KANDALA S, SANDHU R S. Secure role based workflow models [C]// Proc of the 15th Annual Working Conference on Database and Application Security, 2002: 45-58.

[6]FABIO M, JOHN M. Minimal disclosure in hierarchical hippocratic databases with delegation [J]. Lecture Notes in Computer Science, 2005, 3679(1):438-454.

[7]江南,王士同,贺杨成.关于改进的RBAC模型研究及应用实现[J].微计算机信息,2011(3):169-171.

[8]QIL, MING WX, XINW Z. Towards a group-based RBAC model and decentralized user-role administration [C]. The 28th International Conference on Distributed Computing SystemWorkshops, 2008:441-446.

[9]LIS, QIN AM, ZHENGXL. Improvement and implementation of RBAC access control model [C]. 2012 International Conference on Management of e-Commerce and e-Government, 2012:110-115.

[10]LEI S, SUN SQ, JUN Y. Research on improved RBAC model and its access control strategy [C]. The 9th International Conference on Computer-Aided Industrial Design and Conceptual Design, 2008:1067-1071.

[11]龙勤,刘鹏,潘爱民.基于角色的扩展可管理访问控制模型研究与实现[J].计算机研究与发展,2005,42(5):868-875.

[12]邢汉发,许礼林,雷莹.基于角色和用户组的扩展访问控制模型[J].计算机应用研究,2009,26(3):1098-1100.

[13]齐庆芳,李丹.RBAC模型的改进与应用[J].信息技术与信息化,2016(5):38-40.

[14]慕晓冬,李飞行.用户组在RBAC模型中的应用[J].火力与指挥控制,2012,37(8):170-173.

[15]安沛,王春玲.OA系统中RBAC扩展模型的研究与实现[J].西安工程大学学报,2015,29(1):78-83.

[16]李尧.浅谈数据系统的安全策略及其实现方案[J].内江师范学院学报,2002,17(6):84-87.

[17]龙文光.基于RFID标签隐私查询策略[J].内江师范学院学报,2013,28(6):17-20.

The Access Control Strategy Based on User Groups and Two-dimensional Role Management

GOU Quandeng[1,2]

(1. College of Computer Science, Neijiang Normal University, Neijiang, Sichuan 641100, China;
2. Kharkiv State University of Economics, Kharkiv 61166, Ukraine)

Abstract: In order to solve the problems of the role-based access control model being not applicable to the information system with a large user population, the business data of users being unable to be filtered, and the security being not high, a security access control model, based on user groups and two-dimensional role management, has been set up, which gives the role authorization directly to user group and thus it helps to improve the efficiency of authorization. Two-dimensional role is divided into two: data and function, of which, the former is used for user selection and data filtering, and the latter is used to restrict users' permissions from performing system operation. The preliminary application of the model in the scientific research information platform of our university shows that it has the characteristics of "minimum data" and "minimum authority", with security and stability, good expansibility and strong universality.

Keywords: user group; two-dimensional role; security model; functional role; data role

(责任编辑:王 佩)