基于 RBAC模型的角色权限及层次关系研究

鞠成东, 廖明宏
(哈尔滨工业大学 计算机科学与技术学院, 黑龙江 哈尔滨 150006)

摘 要: 针对经典的 RBAC96模型及相关模型中角色私有权限处理方法的不足之处, 提出了一个改进的角色层次关系模型 HRBAC. 该模型通过在角色权限委派关系中引入角色权限继承极限值和最大继承极限值, 划分角色权限为私有权限和公有权限, 定义私有化继承和公有化继承二种继承方式, 形成了一个支持安全管理员宏观控制下的角色权限委派分级管理的改进模型, 克服了多数模型集中式管理模式的局限性, 并能够灵活地反映复杂的角色层次关系.

关键词: 基于角色的访问控制; 私有权限; 权限继承; 角色层次关系
中图分类号: TP311 文献标识码: A 文章编号: 1007- 2683(2005) 04- 0095- 05

Research on Role Permission and Role Hierarchy Based on Role- based Access Control Model

JU Cheng-dong, LIAO Ming-hong
(Institute of Computer Science and Technology, Harbin Institute of Technology, Harbin 150006, China)

Abstract: According to the shortcoming of the classic RBAC96 model and its relative ones, an improved hierarchy role- based access control model HRBAC is presented. By using the concepts of role- permission inheritance limit and extreme limit in the relation of role- permission assignment, the role permissions are divided into private permissions and public ones, and the concepts of privatizing inheritance and publicizing inheritance are defined. In HRBAC model, the multi- level management of role- permission assignment can be used under the control of security manager, which can overcome the limitations of central administration mode in most RBAC models, and flexibly describe the more complicated role relationships.

Key words: RBAC; private permission; permission inheritance; role hierarchy

1 引 言

访问控制是计算机网络信息安全管理的主要策略, 是通过某种途径显式地准许或限制用户、组或角色对信息资源的访问能力及范围的一种方法[1]. 访问控制技术有多种, 如强制访问控制技术、自主访问控制技术、基于角色的访问控制 (RBAC)等, 其中 RBAC是一种已经被公认为较适合在大型企业的计算机网络中实施访问控制的访问控制技术[2]. 基于角色的思想早在 20世纪 60年代就已经提出, 但直到 20世纪 90年代, RBAC模型才逐步得到足够的重视和研究, Ferraiolo与 Kuhn最早使用了“基于角色的访问控制”这个词汇[3,4], 此后, Sandhu等人对 RBAC做了进一步研究, 他们提出的 RBAC96模型 (如图 1所示)得到了学术界的广泛认可[4,5]. RBAC模型的基本特征就是在用户和访问权限之间引入角色这一概念, 根据安全策略划分角色, 对每个角色分

收稿日期: 2005- 03- 10
作者简介: 鞠成东 (1969-), 男, 哈尔滨工业大学硕士研究生.

配操作许可; 为用户指派角色, 用户通过角色间接地对信息资源进行访问. 基于角色的访问控制优势在于能够降低安全管理成本和管理复杂性, 解决传统的自主访问控制和强制访问控制的管理困难问题, 从而能够解决大型网络系统的访问控制问题[5,6]. 为方便权限管理, 在 RBAC模型中引入了角色继承关系, 但在该模型的角色继承关系中存在一些缺点, 即子角色的全部权限都被父角色继承, 而不能拥有自己的私有权限, 这一点没有全面的反映实际应用中复杂的角色层次关系. 对此, Sandhu等人通过引入私有角色[5]这一概念来解决这个问题, 如图 2所示, 为使 T_1、T_2、P_1、S_1等角色能够保留部分权限不被继承, 而相应增加了 T_1'、T_2'、P_1'、S_1'等私有角色, 很显然这一处理方法使得系统内的角色数量成倍激增, 角色继承关系也变得异常复杂, 这必然会增加系统安全管理的复杂度, 降低 RBAC模型本身的管理优势. 本文在相关研究的基础之上[5,7~9], 提出了一个基于 RBAC模型的角色层次关系改进模型 HRBAC(Improved Hierarchy Role- based Access Control). 其特点是能够支持系统用户在安全管理员控制之下的角色权限委派的分级管理, 满足现实应用中角色权限委派关系中的个性化需求, 降低管理成本, 提高系统安全管理的效率以及角色私有权限问题的表达力和可用性.

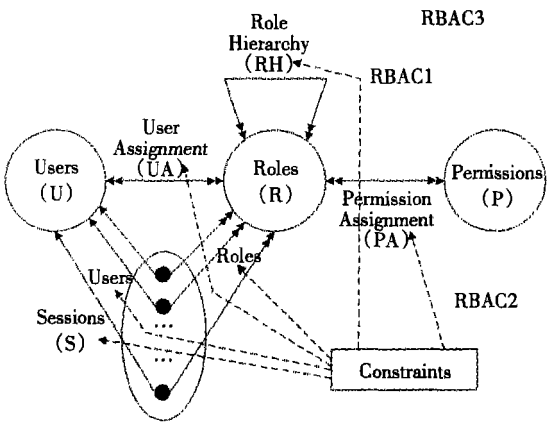

图 1 RBAC 模型

2 支持角色权限委派分级管理的角色层次关系改进模型 HRBAC

2.1 HRBAC模型的形式化描述

定义 **1** 用户集 (USERS): 用户就是一个可以独立访问被保护数据或资源的主体, 它可以是人或自治代理, 此处简化为人, 用 USERS表示一个用户集合, 用 u表示用户集合 USERS中的一个用户, 即 $\exists\ u \in$ USERS.

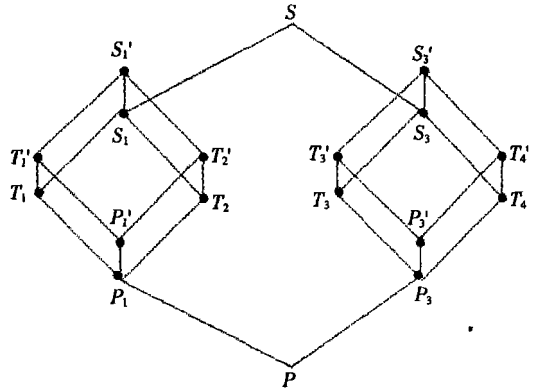

图 2 RBAC96 模型的角色层次关系图例

定义 **2** 权限集 (PERMISSION): 权限是对计算机系统中被保护数据或资源的访问许可. 用 PERMISSION表示一个权限集合, 用 p表示 PERMISSION中的某个权限, 即 $\exists\ p \in$ PERMISSION.

RBAC模型是"策略中立"的模型, 它没有对权限作具体的定义, 因此权限的本质是开放的, 可以依据不同的应用和安全策略进行定义, 一般地, 可以将权限看作是一个二元组 (O, M), 其中 O是客体或客体标识符, 也就是被保护的系统数据或资源, 而 M是 O的非空访问模式集.

定义 **3** 角色集 (ROLES): 角色是在特定组织中的一个工作职责或工作头衔, 它代表一种资格、权利和责任. 用 ROLES表示一个角色集合, 用 r表示角色集 ROLES中的一个角色, 即 $\exists\ r \in$ ROLES.

定义 **4** 用户角色委派 (UA): 用户角色委派是 USERS和 ROLES之间的一个二元关系, 即用 $UA \subseteq$ USERS × ROLES表示一个用户角色委派集合, 用 $(u, r) \in UA$ 表示用户 u被委派了一个角色 r, 用户和角色之间是多对多的关系.

定义 **5** 角色权限委派 (PA): 角色权限委派关系定义为 ROLES与 PERMISSION及 STEP之间的三元组, 即用 $PA \subseteq$ ROLES × PERMISSION × STEP表示一个角色权限委派集合, 其中 STEP为整数集合 $[0, \infty)$, 用 $(r, p, step) \in PA$ 表示一个角色 r拥有一个权限 p, 且可以被向上继承的角色层次极限值为 step. 角色和权限之间也是多对多的关系.

为使角色能够保留部分权限不被继承, 本文将一个角色所拥有的权限集划分为公有权限集和私有权限集.

定义 **6** 令 $PubP: ROLES \rightarrow 2^{PERMISSION \times STEP}$, $PubP(r)$为角色 r所拥有的公有权限集合.

定义 **7**　令 rPriP: ROLES→ $2^{PERMISSION \times STEP}$, rPriP(r)为角色 r所拥有的私有权限集合.

定义 **8**　令 rP: ROLES→ $2^{PERMISSION \times STEP}$, rP(r)为角色 r所拥有的全部权限集合, 根据定义 6和 7, 有 rP(r) = rPubP(r) ∪ rPriP(r).

规则 1　一个角色的私有权限不能被继承; 而其公有权限则可以被继承.

定义 **9**　角色继承(RR): 表示角色与角色之间的二元关系, 用 RR⊆ ROLES × ROLES表示一个角色继承关系集合. 对于∀ r1, r2∈ ROLES, 则(r1, r2) ∈ RR表示角色 r2可以继承 r1的所有公有权限.

而对于一个角色的公有权限引入两种继承机制: 私有化继承 PriI(Privatizing inheritance)和公有化继承 PubI(Publicizing inheritance).

定义 **10**　私有化继承 PriI: 私有化继承定义了角色与角色之间的一个二元关系: $I_{PriI} \subseteq R \times R$, 即对于∀ r1, r2∈ ROLES, 若∃(r1, r2) ∈ I_{PriI}, 则表示角色 r2私有化继承角色 r1的公有权限, 用符号 r1→ ⊗r2表示. 反之, 若 r1→ ⊗r2, 且对于∀ p∈ rPubP(r1), 则有 p∈ rPriP(r2).

定义 **11**　公有化继承 PubI: 公有化继承定义了角色与角色之间的一个二元关系: $I_{PubI} \subseteq R \times R$, 即对于∀ r1, r2∈ ROLES, 若∃(r1, r2) ∈ I_{PubI}, 则表示角色 r2公有化继承角色 r1的公有权限, 用符号 r1→ ⊕r2表示. 反之, 若 r1→ ⊕r2, 且对于∀ p∈ rPubP(r1), 则有 p∈ rPubP(r2).

定义 **12**　角色权限最大向上继承极限值 MAXSTEP: 对于一个角色所拥有的某个公有权限, 可以由安全管理员定义能够被向上继承的最大角色层次极限值 MAXSTEP, 这样定义 5中的日常的角色权限委派工作可以交给次级别的安全管理员(部门安全管理员)来完成, 这样既可以减少系统安全管理员的工作复杂度和可能的工作疏忽, 又可以实现在系统安全管理员的宏观控制下实现角色权限委派的分级管理.

定义 **13**　显式的角色私有(公有)权限: 称直接由安全管理员配置而形成的角色权限委派关系中包含的私有(公有)权限为显式的角色私有(公有)权限.

定义 **14**　隐式的角色私有(公有)权限: 称由继承关系而得到的角色私有(公有)权限为隐式的角色私有(公有)权限.

规则 2　在角色权限委派关系中配置的权限向上继承极限值 step= 0, 表示该权限不能被继承; step= ∞则表示权限可被继承到最高级的角色; step= n, n∈ (0, ∞), 表示权限可以自下而上被继承到第 n层角色.

规则 3　任何角色的显式私有权限的 step值均为 0, 而显式公有权限的 step值∈ [1, ∞).

规则 4　低级角色的显式公有权限被其上一级角色继承后, 其 step值自减 1, 自减 1后, 若 step值= 0, 则该权限加入到上一级角色的私有权限集中, 表现为私有化继承方式; 否则加入到上一级角色的公有权限集中, 表现为公有化继承方式, 之后继续沿着角色层次关系被向上继承.

规则 5　低级角色公有权限被上一级角色继承的同时, 低级角色权限的 MAXSTEP值也相应自减 1.

规则 6　对于任何一个角色的公有权限的 step值和 MAXSTEP值中, 只要有一个为 1, 即 min(step, MAXSTEP) = 1, 则无论相应的 step或 MAXSTEP值为多少, 均按私有化继承方式被上一级角色继承.

2.2　基于 HRBAC模型的角色权限继承关系分析

根据上述的定义和规则, 现以表 1为例, 分析基于 HRBAC模型中的角色权限继承关系. 为简化分析, 表一中包含 6个角色 r1, r2……r6, 分别代表各个不同层次上的角色, 上一层次的角色继承相邻的下一层次的角色权限, 比如 r6继承 r5, r5继承 r4…r2继承 r1, 其中 r1为最低级角色, r6为最高级角色.

对表 1, 仅以 4种具有代表性的角色继承关系进行说明:

1)角色 r1的显式公有权限 pubp13, 尽管次级安全管理员(部门安全员)将该权限的向上传播度配置为 5, 即可以被继承到 r6, 但在系统安全管理员的宏观控制下, 该权限只能被 r2继承, 又因 MAXSTEP为 1, 因此, 角色 r2只能通过私有化继承方式继承该权限, 继承后该权限将成为角色 r2的隐式私有权限, r2的其他上级角色均不能再继承权限 pubp13.

2)角色 r3通过角色 r2间接地继承了角色 r1的显式公有权限 pubp11, 继承后成为角色 r3的隐式公有权限, 尽管系统安全管理员允许权限 pubp11被角色 r5继承(此时 pubp11的 MAXSTEP值为 2), 但部门安全员处于对本部门的安全需求考虑, 只允许该权限被私有化继承到角色 r4.

3)由于系统安全管理员和部门安全员的观点一致, 因此角色 r1的显式公有权限 pubp12一直被继承到最高级角色 r6.

表 1 基于 IHRBAC 模型的角色权限继承关系

	私有权限集		公有权限集			
	显式私有权限	隐式私有权限	显式公有权限	MAXSTEP	隐式公有权限	MAXSTEP
	(prip,step)	(prip,step)	(pubp,step)		(pubp,step)	
r6	(prip61,0)	(pubp51,0)				
		(pubp41,0)				
		(pubp31,0)				
		(pubp12,0)				
r5			(pubp51,1)	1	(pubp41,1)	1
					(pubp31,3)	1
					(pubp12,1)	1
r4	(prip43,0)	(pubp22,0)	(pubp41,2)	2	(pubp31,4)	2
	(prip42,0)	(pubp11,0)			(pubp12,2)	2
	(prip41,0)					
r3		(pubp21,0)	(pubp31,5)	3	(pubp22,2)	1
					(pubp12,3)	3
					(pubp11,1)	2
r2	(prip21,0)	(pubp13,0)	(pubp22,3)	2	(pubp12,4)	4
			(pubp21,1)	1	(pubp11,2)	3
r1	(prip12,0)		(pubp13,5)	1		
	(prip11,0)		(pubp12,5)	5		
			(pubp11,3)	4		

4)角色 r3和角色 r5均没有显式的私有权限, 它们的公有权限可以被上级角色继承.

3 IHRBAC模型与其他模型的比较

Sandhu等人的 RBAC96模型以及其他的一些相关文献分别从不同角度, 对基于 RBAC模型的角色私有权限问题进行了深入研究, 提出了不同的解决方法, 做出了贡献, 但都有一些不足之处.

1) 在 RBAC96模型[5]中, 通过在系统内增加私有角色, 即将一个逻辑上是完整的、统一的角色一分为二的方法来解决角色的私有权限问题, 这势必要成倍地增加系统内角色的数量, 并且使得角色之间的继承关系变得更加复杂, 这种解决方法实质上是以增加系统管理的复杂度为代价的, 而 IHRBAC模型中的角色权限完整、统一.

2) 文[7]提出了一个简单、有效的角色私有权限解决方法, 为本文提供了很好的思想指导, 但是这种方法本质上是集中式的管理模式, 仅依靠系统管理员独立完成角色的管理工作是很艰巨的. 因此, 该方法不适合应用在大型复杂的计算机系统之中. 另外, 文[7]将权限 p的形式表达为 N(X, M), 来代表该权限的传播深度. 这种方法没有反应角色权限委派的个性化需求, 因为在系统中可能会有多个角色继承关系集合, 而在不同的角色继承关系集合中, 对于某权限被继承的层数可能会有不同的需求. IHRBAC模型克服了文献[7]中集中式管理模式的应用局限性, 能够减轻系统管理的复杂度, 同时更能够灵活表达复杂的角色层次关系.

3) 在 EHRBAC模型[8]中引入了一般继承和扩展继承, 其中扩展继承方式不但可以继承公共权限, 也能继承私有权限, 继承过来的权限属性仍保持不变. 本文认为角色的私有权限不应被继承, 对于 EHRBAC模型中角色私有权限的继承关系完全可以转化为继承层数受限制的公有权限继承关系, 即 IHRBAC模型中的公有化继承方式, 这样, 角色私有权限概念的表达和实现更清晰.

4) 文[9]也较好地提出了一个解决角色私有权限问题的改进模型, 其不足是, 对于角色的权限类型划分和继承机制的定义有重叠, 缺乏统一性. 比如, 在文[9]中, 对于某角色 r的特征权限, 若角色 r的所有上级角色均采用一般继承方式, 则等同于对角色 r的公有权限的公有化继承方式. 另外, 在文[9]中, 角色的权限组成最多有 7个部分, 而在 IHRBAC模型中, 角色的权限组成被简化为至多 4个部分: 显式的私有权限、显式的公有权限、隐式的私有权限和隐式的公有权限.

具体比较结果见表 2

表 2 IHRBAC模型与其他模型的简单比较

	角色权限的表达及角色继承关系特点	管理模式	模型适用性
RBAC96模型[5]	角色不完整, 需增加私有角色、继承关系异常复杂	集中式	小型系统
文[7]	角色完整、角色权限关系缺少个性化	集中式	中、小型系统
EHRBAC模型[8]	角色完整、继承方式不合理	集中式	中、小型系统
文[9]	角色完整、权限类型有重叠、继承方式不统一	集中式	中、小型系统
IHRBAC模型	角色完整、角色权限类型清晰合理、继承方式统一	支持分级管理	大型系统

4 结 语

基于角色的 RBAC模型, 通过引入角色, 作为用户和被访问的客体(数据或资源)的中间媒介, 使得安全的授权管理复杂度和管理成本得到明显改善, 但是基于 RBAC96模型的私有角色处理方法却不能够充分发挥 RBAC模型的自身优势. 本文在相关研

究工作的基础之上, 提出了一个基于 RBAC模型的角色层次关系改进模型 IHRBAC, 在 IHRBAC模型中重新定义了角色权限的委派关系, 通过引入参数 step和 MAXSTEP, 私有化继承和公有化继承二种继承方式以及定义若干规则, 使 HRBAC模型支持在系统安全管理员宏观控制下的角色权限委派的分级管理, 能够降低系统安全授权管理的复杂度和管理成本. 新模型能够保持角色私有权限和公有权限的完整和统一, 能够较好地表达角色权限委派的个性化需求和复杂的角色继承关系.

下一步的研究工作应在 IHRBAC模型基础上, 深入研究用户角色的委派关系和新型的约束机制, 以使 IHRBAC模型成为一个统一的、完整的模型, 另外, HRBAC模型融入新型的约束机制后, 应具有良好的动态授权管理功能.

参 考 文 献:

[1] 杨亚平, 李伟琴, 刘怀宇. 基于角色的细粒度的访问控制系统的研究与实现 [J]. 北京航空航天大学学报, 2001, 27(2): 178-181.
[2] 黄益民, 杨子江, 平玲娣, 潘雪增. 安全管理系统中基于角色访问控制的实施方法 [J]. 浙江大学学报(工学版), 2004, 38(4).
[3] DAVID Ferraiolo, RICHARD Kuhn. Role-based access controls[EB/OL]. In: Proceedings of the 15th National Computer Security Conference, Baltimore, MD, 1992: 554-563. http://csrc.nist.gov/staff/kuhn/rkhome.html.
[4] 刘　斌, 李瑞芳, 刘东苏. 信息系统中的访问控制模型研究 [J]. 情报杂志, 2003, 11.
[5] RAVI Sandhu and EDWARD Coyne. Role-based Access ControlModels[J]. IEEE Computer, 1996, 29(2): 38-47.
[6] David Ferraiolo, Ravi Sandhu, et al. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security(TISSEC), 2001, 4(3): 224-274.
[7] 余文森, 张正秋, 章志明, 余　敏. 基于角色的访问控制模型中私有权限问题的研究 [J]. 计算机应用研究, 2004, (4).
[8] 钟　华, 冯玉琳, 姜洪安. 扩充角色层次关系模型及其应用 [J]. 软件学报, 2000, 11(6): 779-784.
[9] 吕宜洪, 宋瀚涛, 龚元明. 基于 RBAC改进模型的角色权限及层次关系分析 [J]. 北京理工大学学报, 2002, 22(5).

(审稿: 郝忠孝教授, 陈德运教授; 编辑: 王　萍)

(上接第 **94**页)

在国内刚刚起步, 专家知识库的建立还需要不断完善, 参数还待进一步优化.

参 考 文 献:

[1] 陈善本. 焊接过程现代化控制技术 [M]. 哈尔滨工业大学出版社, 2001.
[2] GE Hydro. ScompiR System[Z]. Last Revision, 2002.
[3] 所丽娜, 周欣荣. 水轮机修复专用机器人位姿控制方法 [J]. 哈尔滨理工大学学报, 2003, 8: 1-4.
[4] 李士勇, 模糊控制和智能控制理论与应用 [M]. 哈尔滨工业大学出版社, 1999.
[5] 郑宜庭, 黄石生. 弧焊电源[M]. 北京: 机械工业出版社, 2003.

(审稿: 徐松源 教授, 杜德生教授; 编辑: 高长福)