文章编号：1000-8608(2011)01-0132-05

基于组织的访问控制系统授权验证单层关系模型

丁 锋*[1,2]， 陈雪龙[3]， 王延章[3]， 郭剑锋[2]

（1.大连理工大学 软件学院，辽宁 大连 116024；
2.辽宁省信息安全与软件测评认证中心，辽宁 沈阳 110001；
3.大连理工大学 管理与经济学部，辽宁 大连 116024）

摘要： 由于在目前的各种组织授权模型中缺乏对授权系统访问许可的检验，提出了对OB4LAC模型授权情况进行验证的基于组织的访问控制系统授权验证单层关系模型，通过向量和矩阵对用户-岗位-角色-操作之间的关联方式进行了描述，实现在多用户情况下，将每个用户通过组织授权系统所得到的系统操作权限进行直观的统计.通过算法实例对单层关系模型进行了实际验证，验证结果清晰直观地反映了组织内部人员的系统权限分配情况，对系统安全访问控制提供了有力支持.

关键词： 组织；授权；访问控制；OB4LAC
中图分类号： TP393 **文献标志码：** A

0 引 言

基于角色的访问控制(RBAC)模型[1,2]是一种适用于大型组织的、有效的访问控制模型[3~6].近年来许多学者、研究机构和系统开发商进行了大量的研究与设计工作，对RBAC模型进行了多方面的增强.RBAC模型在大规模多级多部门多应用系统环境下，仍不能有效地减少授权工作量，同时与组织人事的管理理念仍有脱节.OB4LAC模型[3]从管理、信息系统和安全基础技术的整体出发，以组织人事管理为基础，按照物理世界的组织机构体制，把人员与机构岗位进行逻辑分离，增加机构岗位层.同时，将角色相对细化，并形成角色关联网络层.操作功能集是业务系统所提供的所有服务和资源总和.

在OB4LAC模型中，组织人事机构管理是基础，它包含人员、组织机构和岗位管理，同时包含部分的通用或静态公共服务性角色的管理.为了便于大规模的授权管理，OB4LAC引进通用岗位概念，纳入相应的管理中.通用岗位指局长、处长、中共党员、共青团员、干部、教师、市民等抽象岗位，不具体隶属于某一个组织机构，可以理解为一个岗位类.

在组织机构岗位的基础管理模块中，除基本的人员、组织机构和岗位等信息管理外，就是关于1、2层间以及部分2、3层间的映射管理及相应的安全权限封装，关于2、3层间的映射管理实现相对简单.人员与岗位的映射实质上是一个组织内的职责分配问题，是一种广义概念下的授权.一般情况下，人员与机构岗位的映射是多对多的，同时，组织机构之间、组织机构和岗位之间、岗位之间均存在一定的业务、权限等关联关系，因此，除了基本的映射管理外，必须梳理这些关联机制，建立相应模型描述和控制权限的传递、继承和审计，比如上下级关系、具体岗位与通用岗位关系、同级岗位的代理关系、岗位联席关系等.

机构岗位与角色在概念和内涵上是不同的，机构岗位是组织中的职位，角色是一个业务系统的一个职能对应的操作功能集，一个职位可能对应一个业务系统中的多个职能(角色)，并且一个机构可能对应多个业务系统.因此，在一般意义下，4层之间都是多对多的映射关系.所以，组织授权管理从广义上讲就是要科学地管理这4层之间的多对多映射关系.1、2层之间的映射管理属

收稿日期： 2008-12-18； **修回日期：** 2010-11-16.
基金项目： 中央高校基本科研业务费专项资金资助项目.
作者简介： 丁 锋*(1979-)，男，博士，讲师，E-mail:dingfeng@dlut.edu.cn；王延章(1952-)，男，博士，教授，博士生导师.

于组织人事管理范畴，3、4 层之间是关于业务功能与职能角色的对应管理，应在业务系统平台中进行. 2、3 层即岗位与角色的映射管理，是行政组织管理与业务管理部门的铰链地带，也是统一与分布式授权的模糊域.

本文针对 OB4LAC 模型，提出一种基于组织的访问控制系统授权验证单层关系模型.

1　组织授权系统单层关系模型算法

通过岗位网络轻而易举地将不同系统中的用户、岗位、角色、操作关联到一起，如图 1 所示.

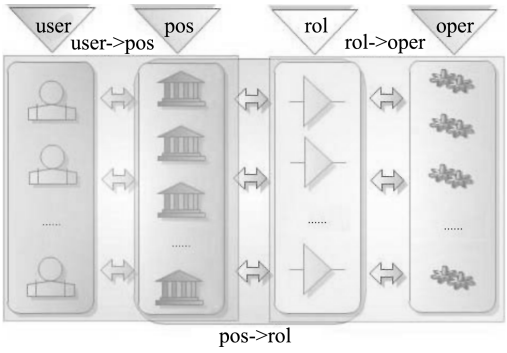

图 1　用户-岗位-角色-操作模型

Fig. 1　User-position-role-operation model

现实的政府部门中大量存在一个工作人员同时拥有几个工作岗位的现象，所以组织授权系统中的用户本体和岗位本体之间并不是一对一的简单映射，而是多对多的复杂映射，如图 2 所示.

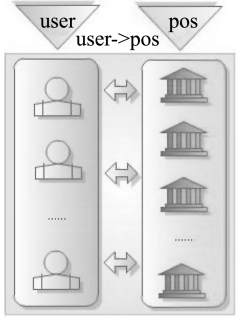

图 2　用户-岗位映射

Fig. 2　User-position mapping

定义一组用户本体：$\{user_1, user_2, \cdots, user_m\}$，记为向量 $\boldsymbol{U} = (user_1 \quad user_2 \quad \cdots \quad user_m)^{\mathrm{T}}$；

定义一组岗位本体：$\{pos_1, pos_2, \cdots, pos_n\}$，记为向量 $\boldsymbol{P} = (pos_1 \quad pos_2 \quad \cdots \quad pos_n)^{\mathrm{T}}$；

将每一个用户 $user_i$ 和岗位 pos_j 之间的关联 $user_i \rightarrow pos_j$ 记为 u_{ij}，用 $\boldsymbol{U} \cdot \boldsymbol{P}^{\mathrm{T}}$ 的形式来描述这一关联关系：

$$\boldsymbol{U} \cdot \boldsymbol{P}^{\mathrm{T}} = \begin{pmatrix} user_1 \\ user_2 \\ \vdots \\ user_m \end{pmatrix} \cdot (pos_1 \quad pos_2 \quad \cdots \quad pos_n) = \begin{pmatrix} user_1 pos_1 & user_1 pos_2 & \cdots & user_1 pos_n \\ user_2 pos_1 & user_2 pos_2 & \cdots & user_2 pos_n \\ \vdots & \vdots & & \vdots \\ user_m pos_1 & user_m pos_2 & \cdots & user_m pos_n \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & & \vdots \\ u_{m1} & u_{m2} & \cdots & u_{mm} \end{pmatrix}$$

将 $\boldsymbol{U} \cdot \boldsymbol{P}^{\mathrm{T}}$ 简记为 $\boldsymbol{U}_{\boldsymbol{P}}$，则有 $\boldsymbol{U}_{\boldsymbol{P}} = (u_{ij})_{m \times n}$.

在此结构下，如果仅仅为了表示 $user_i$ 和 pos_j 之间是否存在关联关系，可以用 0 和 1 来方便地表示：

如果 $user_i$ 没有权限访问 pos_j，$user_i \rightarrow pos_j = 0$，记为 $u_{ij} = 0$；

如果 $user_i$ 有权限访问 pos_j，$user_i \rightarrow pos_j = 1$，记为 $u_{ij} = 1$.

如此一来也就形成了形如 $\begin{pmatrix} 1 & 0 & \cdots & 1 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ 的矩阵，其中的子元素只有 0 和 1.

由于传统的 RBAC 模型中的角色具有层次性，为了适应这一点，在组织授权系统中对角色依然保持 RBAC 的相关定义和属性，为系统的兼容性提供保障. 为了实现这一目标，在系统中允许岗位和角色是多对多的关系，如图 3 所示.

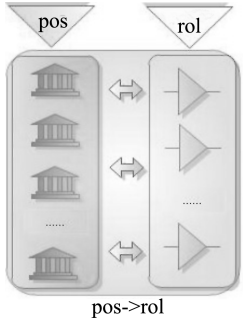

图 3　岗位-角色映射

Fig. 3　Position-role mapping

定义一组角色本体：$\{rol_1, rol_2, \cdots, rol_l\}$，记为向量 $\boldsymbol{R} = (rol_1 \quad rol_2 \quad \cdots \quad rol_l)^{\mathrm{T}}$；

将每一个岗位 pos_i 和角色 rol_j 之间的关联 $pos_i \rightarrow rol_j$ 记为 p_{ij}，用 $\boldsymbol{P} \cdot \boldsymbol{R}^{\mathrm{T}}$ 的形式来描述这一关联关系：

$$\boldsymbol{P} \cdot \boldsymbol{R}^{\mathrm{T}} = \begin{pmatrix} pos_1 \\ pos_2 \\ \vdots \\ pos_n \end{pmatrix} \cdot (rol_1 \quad rol_2 \quad \cdots \quad rol_l) = \begin{pmatrix} pos_1 rol_1 & pos_1 rol_2 & \cdots & pos_1 rol_l \\ pos_2 rol_1 & pos_2 rol_2 & \cdots & pos_2 rol_l \\ \vdots & \vdots & & \vdots \\ pos_n rol_1 & pos_n rol_2 & \cdots & pos_n rol_l \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1l} \\ p_{21} & p_{22} & \cdots & p_{2l} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nl} \end{pmatrix}$$

将 $\boldsymbol{P} \cdot \boldsymbol{R}^{\mathrm{T}}$ 简记为 $\boldsymbol{P_R}$，则有 $\boldsymbol{P_R} = (p_{ij})_{n \times l}$.

对于系统中角色与操作的关系采用 RBAC 模型的描述，对角色和可执行操作建立多对多的关联，以满足简化系统功能分配的需求，如图 4 所示.

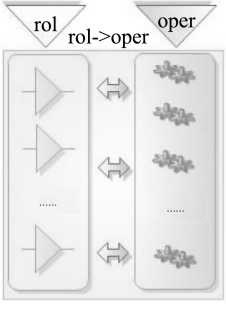

图 4 角色-操作映射

Fig. 4 Role-operation mapping

定义一组操作：$\{oper_1, oper_2, \cdots, oper_k\}$，记为向量 $\boldsymbol{O} = (oper_1 \quad oper_2 \quad \cdots \quad oper_k)^{\mathrm{T}}$；

将每一个角色 rol_i 和操作 $oper_j$ 之间的关联 $rol_i \rightarrow oper_j$ 记为 r_{ij}，用 $\boldsymbol{R} \cdot \boldsymbol{O}^{\mathrm{T}}$ 的形式来描述这一关联关系：

$$\boldsymbol{R} \cdot \boldsymbol{O}^{\mathrm{T}} = \begin{pmatrix} rol_1 \\ rol_2 \\ \vdots \\ rol_l \end{pmatrix} \cdot (oper_1 \quad oper_2 \quad \cdots \quad oper_k) = \begin{pmatrix} rol_1 oper_1 & rol_1 oper_2 & \cdots & rol_1 oper_k \\ rol_2 oper_1 & rol_2 oper_2 & \cdots & rol_2 oper_k \\ \vdots & \vdots & & \vdots \\ rol_l oper_1 & rol_l oper_2 & \cdots & rol_l oper_k \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1k} \\ r_{21} & r_{22} & \cdots & r_{2k} \\ \vdots & \vdots & & \vdots \\ r_{l1} & r_{l2} & \cdots & r_{lk} \end{pmatrix}$$

将 $\boldsymbol{R} \cdot \boldsymbol{O}^{\mathrm{T}}$ 简记为 $\boldsymbol{R_O}$，则有 $\boldsymbol{R_O} = (r_{ij})_{l \times k}$.

通过对上面建立的“用户 - 岗位”“岗位 - 角色”“角色 - 操作”3 个矩阵进行计算可以得出用来判别权限分配关系的 $m \times k$ 阶组织授权单层关系矩阵：

$$\boldsymbol{T} = \boldsymbol{U_P} \cdot \boldsymbol{P_R} \cdot \boldsymbol{R_O} = (u_{ij})_{m \times n} \cdot (p_{ij})_{n \times l} \cdot (r_{ij})_{l \times k}$$

用 t_{ij} 表示矩阵 $\boldsymbol{T}$ 中的元素，t_{ij} 为用户与操作之间的关联关系，由此得出组织授权系统单层关系模型算法，即

$$\boldsymbol{T} = (u_{ij})_{m \times n} \cdot (p_{ij})_{n \times l} \cdot (r_{ij})_{l \times k} = (t_{ij})_{m \times k}$$

当 t_{ij} 不为 0 时，意味着系统中第 i 个用户具有进行第 j 项操作的权利；当 $t_{ij} = 0$ 时，意味着系统中第 i 个用户不具有进行第 j 项操作的权利. 这一矩阵清楚地表明了每一个用户所能执行的所有操作，为系统管理员检查用户权限分配的合理性提供了依据，增强了系统的可靠性.

在上述过程中 $(u_{ij})_{m \times n} \cdot (p_{ij})_{n \times l}$ 反映了用户与角色之间的对应关系，记为 $\boldsymbol{U_R} = (u_{ij})_{m \times n} \cdot (p_{ij})_{n \times l}$，而 $(p_{ij})_{n \times l} \cdot (r_{ij})_{l \times k}$ 则反映了岗位与操作之间的对应关系，记为 $\boldsymbol{P_O} = (p_{ij})_{n \times l} \cdot (r_{ij})_{l \times k}$.

$\boldsymbol{U_R}$ 和 $\boldsymbol{P_O}$ 这两组矩阵可以对组织授权系统进行中间环节的授权检查，在实际工作中对系统管理人员非常有帮助.

2 单层关系模型算法应用举例

例 1 对于一个已经存在的组织授权系统，对其用户、岗位、角色和操作之间的权限分配情况进行分析. 用户与岗位间存在的关联关系如图 5 所示.

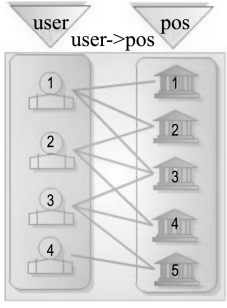

图 5 用户-岗位映射

Fig. 5 User-position mapping

则有

$$\boldsymbol{U_P}=(u_{ij})_{m\times n}=\begin{pmatrix}u_{11}&u_{12}&u_{13}&u_{14}&u_{15}\\u_{21}&u_{22}&u_{23}&u_{24}&u_{25}\\u_{31}&u_{32}&u_{33}&u_{34}&u_{35}\\u_{41}&u_{42}&u_{43}&u_{44}&u_{45}\end{pmatrix}=\begin{pmatrix}1&1&1&0&0\\0&1&1&1&0\\0&0&1&1&1\\0&0&0&0&1\end{pmatrix}$$

岗位与角色间存在的关联关系如图 6 所示，则有

$$\boldsymbol{P_R}=(p_{ij})_{n\times l}=\begin{pmatrix}p_{11}&p_{12}&p_{13}\\p_{21}&p_{22}&p_{23}\\p_{31}&p_{32}&p_{33}\\p_{41}&p_{42}&p_{43}\\p_{51}&p_{52}&p_{53}\end{pmatrix}=\begin{pmatrix}1&0&0\\1&1&0\\1&1&1\\0&1&1\\0&0&1\end{pmatrix}$$

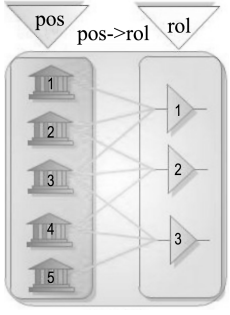

图 6　岗位-角色映射

Fig. 6　Position-role mapping

角色与操作间存在的关联关系如图 7 所示，则有

$$\boldsymbol{R_O}=(r_{ij})_{l\times k}=\begin{pmatrix}r_{11}&r_{12}&r_{13}&r_{14}&r_{15}\\r_{21}&r_{22}&r_{23}&r_{24}&r_{25}\\r_{31}&r_{32}&r_{33}&r_{34}&r_{35}\end{pmatrix}=\begin{pmatrix}1&1&0&0&0\\0&1&1&0&0\\0&0&1&1&1\end{pmatrix}$$

由此构成的整个组织授权结构如图 8 所示.

由 $\boldsymbol{U_R}=(u_{ij})_{m\times n}\cdot(p_{ml})_{n\times l}$ 可得

$$\boldsymbol{U_R}=\begin{pmatrix}3&2&1\\2&3&2\\1&2&3\\0&0&1\end{pmatrix}$$

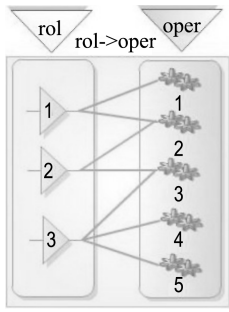

图 7　角色-操作映射

Fig. 7　Role-operation mapping

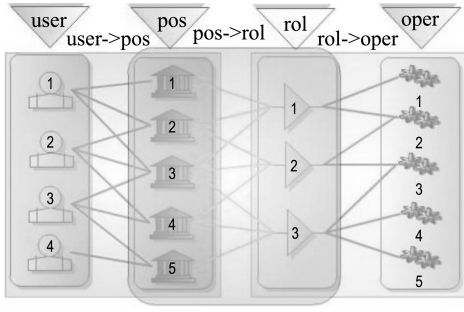

图 8　授权结构映射

Fig. 8　Authorization structure mapping

由 $\boldsymbol{P_O}=(p_{ij})_{n\times l}\cdot(r_{ij})_{l\times k}$ 可得

$$\boldsymbol{P_O}=\begin{pmatrix}1&1&0&0&0\\1&2&1&0&0\\1&2&2&1&1\\0&1&2&1&1\\0&0&1&1&1\end{pmatrix}$$

由 $\boldsymbol{T}=(u_{ij})_{m\times n}\cdot(p_{ij})_{n\times l}\cdot(r_{ij})_{l\times k}$ 可得

$$\boldsymbol{T}=\begin{pmatrix}3&5&3&1&1\\2&5&5&2&2\\1&3&5&3&3\\0&0&1&1&1\end{pmatrix}$$

由以上的计算结果可以看出：

用户与角色的对应关系 $\boldsymbol{U_R}$ 中，1 号用户有 3 条途径获得 1 号角色，有 2 条途径获得 2 号角色，有 1 条途径获得 3 号角色，1、2 和 3 号用户均获得了系统的所有角色使用权，而 4 号用户只获得了 3 号角色使用权，这也是 4 号用户的唯一可以使用的角色；从岗位与操作的对应关系 $\boldsymbol{P_O}$ 中，可以很容易地发现 1 号岗位的操作权限较少，只有两项，而 3 号岗位的操作权限较大，获得了系统所有的操作权限；用户与操作的对应关系 $\boldsymbol{T}$ 中，1、2、3 号用户获得 2 号或 3 号操作的途径多达 5 条，充分说明此系统授权的重复性，威胁到系统安全. 因为

如果有用户可以通过多条途径获得某一操作的权限,在将来进行操作权限调整时虽然禁止了该用户获得此操作的一条途径,该用户仍可通过其他途径获得此操作权限,这将会带来安全隐患.

3 结 论

基于OB4LAC体系的组织授权单层关系算法为简单的授权系统提供了分析方法,同样适用于RBAC模型,且十分便利,直观有效,对组织授权过程中的权限分配情况提供了审计依据. OB4LAC是对RBAC模型的扩展,它通过定义组织结构及其权限,大大减少了角色的数量,从而降低了应用系统访问控制的复杂程度,减少了系统管理员的设置和维护权限的工作量. OB4LAC模型结构比RBAC模型复杂,在实际应用过程中,适宜用于解决组织机构庞杂的授权管理问题.

参考文献:

[1] FERRIAOLO D, CUGINI J, KUHN R. Role-based access control (RBAC): Features and motivations [C] // **Proceedings of 11th Annual Computer Security Application Conference**. New Orleans: IEEE Computer Society Press, 1995:241-248

[2] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models [J]. **Computer**, 1996, **29**(2):38-47

[3] LI Huai-ming, WANG Yan-zhang, DING Feng, *et al*. Research and realization of information exchange and share platform for municipal government [C] // **2006 IEEE International Conference on Service Operations and Logistics, and Informatics**. Piscataway:IEEE, 2006:21-23

[4] BERTINO E, BONATTI P A, FERRARI E. TRBAC: A temporal role-based access control model [J]. **ACM Transactions on Information and System Security**, 2001, **4**(3):191-233

[5] 洪 帆,段素娟,黎成兵. 基于图的委托授权模型[J]. 北京邮电大学学报, 2005, **28**(6):5-8

[6] 徐 震,李 斓,冯登国. 基于角色的受限委托模型[J]. 软件学报, 2005, **16**(5):970-978

Single-layer authorized access control system verification model based on organization

DING Feng[*1,2], CHEN Xue-long[3], WANG Yan-zhang[3], GUO Jian-feng[2]

(1. School of Software, Dalian University of Technology, Dalian 116024, China;
2. Liaoning Province Information Security & Software Testing Evaluation and Certification Center, Shenyang 110001, China;
3. Faculty of Management and Economics, Dalian University of Technology, Dalian 116024, China)

Abstract: The situation of the authorized system accessing permissions by the organization authorization model was seldom verified. A single-layer access control authorized verification model based on organization for OB4LAC model was put forward, and the relationships between user, position, role and operation were also described by the vectors and matrices. The system operation permission of each user got from organization system were counted directly when multi-user existing in one system. An example to verify the single-layer access control verification model is given and the results clearly show the situation of all the users to allocate authorization. This model is helpful to system security and access control.

Key words: organization; authorization; access control; OB4LAC