基于时间分区的改进RBAC授权模型

王晓琳 史有群 唐 成 徐 康
(东华大学计算机科学与技术学院 上海 201620)

摘 要 针对传统RBAC授权模型灵活性低的问题,提出了一种基于时间分区的改进RBAC授权模型。首先将系统的整体进程分成若干时间分区,分别在每个分区里分配角色和权限,使得各个分区独立且紧密相连。其次,将时间分区具体化为阶段集,并在基本RBAC模型中引入阶段集使其构成改进RBAC模型。管理员只需要控制阶段的进度就可以控制各角色、各用户的访问权限。该改进模型在公选系统的实际应用中取得了很好的效果。

关键词 RBAC,访问控制,时间分区,阶段
中图法分类号 TP311 **文献标识码** A

Improved RBAC Authorization Model Based on Time Partition

WANG Xiao-lin SHI You-qun TANG Cheng XU Kang
(School of Computer Science and Technology, Donghua University, Shanghai 201620, China)

Abstract The traditional RBAC model has less flexibility to assign permissions of users. This paper proposed an improved RBAC authorization model based on time partition. The whole system process is divided into several time partitions. The permissions associated with each role are distributed in each independent partition. The set of stages which have the permissions of each time partition constructs the improved RBAC model by combining the basic RBAC model. When the stages are determined, the permissions of roles and users can be configured by the administrator. The proposed RBAC model is applied in public selecting system stably and obtains good performance.

Keywords RBAC, Access control, Time partition, Stage

1 引言

随着计算机网络的飞速发展,网络系统数据资源的安全管理问题已成为一个有价值的研究课题。为了保证信息资源的安全性和有效性,信息管理系统除了需要分辨用户的身份是否合法外,还需要判断该用户是否有权使用或更改某一项数据信息[1]。常用的自主访问控制(Discretionary Access Controls)和强制访问控制(Mandatory Access Controls)方法都是由主体和访问权限直接发生关系,根据主体/客体的所属关系或主体/客体的安全级来决定主体是否有对客体的访问权[2]。这种访问控制方法比较僵化,不能满足大型网络系统对灵活性的要求。

基于角色的访问控制RBAC(Role-Based Access Control)是一种重要的访问控制方式,是当前访问控制研究和应用的热点[3]。它引入了角色的概念,将原本直接相关联的用户和访问权限相脱离,通过角色来关联用户和访问权限。它由于实现了用户与访问权限的逻辑分离,更符合企业的用户、组织、数据和应用特征,已逐渐成为前面两种模型的最佳替代者。

公选系统旨在建立基于互联网的干部公开选拔工作的信息平台,实现网上发布公告、接受报名、公布成绩、任职公示等各环节工作,借助信息技术分析报名、考试测评、任职人选等相关情况,同时又服务于相关部门发布相关竞争性选拔信息,并完成相关工作。

公选系统的权限控制主要是对后台管理用户的控制。系统中一个任务就是指一次公开选拔。在实际情况中,一个管理用户可能同时处在不同任务的不同阶段,此时其所担任的角色也可能不相同。为避免描述复杂,本文仅讨论在一个任务期间的权限分配。对于一次任务,任务管理员会根据各阶段的需求对权限进行合理的分配。

2 传统的RBAC模型

传统的RBAC模型主要是指由Sandhu等人于1996年提出的RBAC96模型[4],它是一个模型族,包括4个子模型,分别为RBAC0,RBAC1,RBAC2和RBAC3。RBAC0又称为基本RBAC模型,是其他3个模型的基础。

(1)RBAC0的定义如下:

用户集 *users*(U)、角色集 *roles*(R)、权限集 *permissions*(P)、会话集 *sessions*(S)。

$UA \subseteq U \times R$,表示用户和角色之间是多对多关系,即一个用户可以具有多个角色,一个角色也可以被多个用户成员所拥有。

到稿日期:2012-12-10 返修日期:2013-03-23

王晓琳(1989—),女,硕士生,主要研究方向为软件工程,E-mail:wxl-kalice@163.com;史有群(1964—),男,博士后,教授,主要研究方向为人工智能、网络计算;唐 成(1987—),男,硕士生,主要研究方向为软构件和多Agent系统;徐 康(1989—),硕士生,主要研究方向为软件工程。

$PA \subseteq P \times R$，表示权限和角色之间是多对多关系，即一个权限可以分配给多个角色，一个角色也可以拥有多个权限[5]。

$user: S \to U$，一个用户可以有多个会话，一个会话只对应一个用户，此函数用于将会话映射到用户。

$roles: S \to 2^R$，此函数用于将一个会话映射到一个角色集。

$roles(Si) \subseteq \{r | (user(Si), r) \in UA\}$，会话中包含的是用户集中被激活角色(它们是用户授权角色集的一个子集)。

(2)RBAC1 又称分级 RBAC 模型，它在 RBAC0 的基础上引入了角色分级(RH)的概念。角色分级是指一个 RBAC 系统中角色与角色之间存在上下级关系。在分级模型中一个角色可以有上级角色和下级角色。角色在分级模型中是向下继承的，而权限在分级模型中是向上继承的。这些继承是符合偏序关系的，即具有传递性、自反性和反对称性。RBAC1 模型增加了以下两个实体：

$RH \subseteq R \times R$，角色间具有偏序关系，用"≥"表示，例如 $r_1 \geqslant r_2$ 表示 r_1 是 r_2 的上级角色。

$roles: S \to 2^R$，$roles(S_i) \subseteq \{r | (\exists r' \geqslant r)[(user(S_i), r') \in UA]\}$，在分级模型中，一个会话包含一个用户授权角色集的一个子集(激活角色)，这些激活角色的下级角色也包含在对话中。

(3)RBAC2 又称约束 RBAC 模型，它在 RBAC0 的基础上引入了约束(constraint)。约束是 RBAC 中非常重要的概念。约束也可认为是 RBAC 背后的主要推动力之一[6]，同时约束常常也是一个组织在制定安全策略时一个强有力的保障机制。约束主要分为 3 类：职责分离约束(SOD)、预请求约束、基数约束。

(4)RBAC3 称为综合 RBAC 模型，它包含了 RBAC1 和 RBAC2，并间接包含了 RBAC0，是一个综合的角色访问控制模型[7]。

RBAC96 模型如图 1 所示。其中，用户与角色以及角色与权限之间都是多对多关系。角色权限的分配实现了权限的封装，用户角色的分配实现了权限到用户的传递[8]。

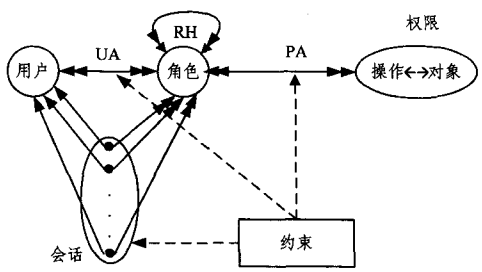

图 1　RBAC96 模型

虽然传统的 RBAC 模型容易配置，但是这种授权方式缺乏一定的灵活性。例如，某地区下半年需要招聘各种岗位的人员，授权给甲用户后台添加岗位的角色，乙用户后台审核岗位的角色，丙用户前台报名的角色。按照传统的 RBAC 模型，各种角色都拥有其相应的权限，而且权限一旦分配就不能自动更改。例如，当丙用户处在网上报名的阶段，甲和乙的工作都不应该再进行，这时就需要手动更改或取消角色被赋予的这些权限，只留给甲、乙查看的权限。所以，在整个干部公选过程中的每个阶段，后台管理员都需要手动地配置各种角色的权限，工作量繁琐且易出错。因此，这样的授权模式缺乏灵活性，不适合用于这种在各个阶段具备不同权限的系统。

针对这种情况，需要重新考虑系统的权限分配问题。为了更好地根据需求来调整权限管理模型，提高权限分配的灵活性和动态性，本文提出了一种改进型的 RBAC 方法。

3　基于时间分区的改进 RBAC 模型

3.1　时间分区的概念

时间分区的概念是指对任何一个系统，将控制进程按时间进行分区，每一个时间区域内按照传统 RBAC 中的($P \times R$)二元关系进行权限分配，且各时间分区之间相互独立，这样可以灵活地改变每个时间分区的权限分配，增加了权限分配的灵活性。基于时间分区的 RBAC 授权框架如图 2 所示。图中顶部的水平箭头表示系统进程，按时间轴从左到右递增。若干条垂直虚线将系统进程分割成不同的时间区，分别为时间区 1，时间区 2，…，时间区 n。每个时间区内根据传统的 RBAC 授权方式进行权限分配。椭圆表示角色集和权限集，矩形表示二者的关系表。

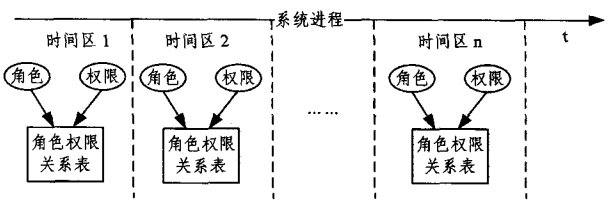

图 2　划分时间分区的 RBAC 授权框架

与传统授权模式相比，划分时间分区的方法加强了权限分配的可控性。每个时间区的跳转可人工操作也可配置成指定时间跳转。这样，在某一时间区正在进行的情况下，管理员可随时修改其他时间分区的权限配置而不影响整个系统进程。

时间分区是一个抽象的理论概念，将其具体化应用到实际系统中，即为将一个系统分为若干个阶段，各个阶段都有其不同的角色权限分配。将阶段集加入到传统的 RBAC 模型中，使其构成改进 RBAC 模型。这样，只需控制系统阶段的跳转，就可对各阶段进行独立的权限分配，效率明显提高。

3.2　改进的 RBAC 模型

为了详细阐述上述模型，定义 4 个集合：用户集(Users)、角色集(Roles)、阶段集(Stages)和权限集(Permissions)。

用户集：表示所有登录系统的用户的集合，用 U 表示。

角色集：表示该系统中拥有特定职能的岗位，带有特定的权利范畴，用 R 表示。

阶段集：表示该系统进程从创建起到结束要经过的所有阶段，用 S 表示。

权限集：该系统的用户进行特定模式的访问操作，用 P 表示。

UA：$UA \subseteq U \times R$，用户与角色的分配关系，是一个多对多关系。

PA：$PA \subseteq P \times R \times S$，权限、阶段、角色之间的分配关系。

在改进 RBAC 模型中，一个用户所拥有的权限，除了与

它本身的角色有关，还与它所处的阶段有关。图 3 显示了改进型 RBAC 与传统型 RBAC 的分配模式。

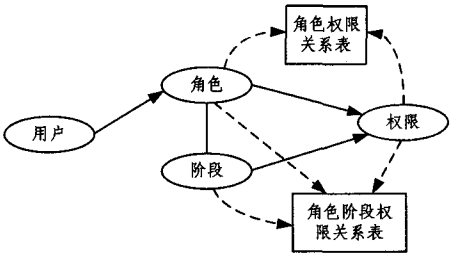

图 3　用户、角色、阶段及权限关系图

如图 3 所示，椭圆代表 4 个集合，即用户集、角色集、阶段集和权限集。矩形框代表集合之间的关系表。实线箭头代表用户权限的分配路径。虚线箭头代表关系表由哪些集合关联得到。从图 3 中可以看出，一个用户的权限分配有 2 条路径，一条是“用户→角色→权限”，表明用户的权限与角色有关，这是传统 RBAC 模型的分配模式；另一条是“用户→角色→阶段→权限”，表明用户的权限与角色和阶段有关，这是改进 RBAC 模型的分配模式。由角色集、权限集和阶段集构成了角色阶段权限关系表，由角色集和权限集构成了角色权限关系表。

3.3　在公选系统中的应用

公选系统的访问控制主要是指对单位用户进行管理，并设定他们的权限，权限主要包括任务管理、职位管理、职位审核、考场安排、面试安排、公告发布等。一个任务从创建到结束，分为若干个阶段；每个阶段各角色所拥有的权限不同，且权限的更改由阶段控制。

3.3.1　权限控制模块分析

应用 3.2 节所述的改进模型，使权限分配由 $(P\times R)$ 二元关系变成 $(P\times R\times S)$ 三元关系，简化了权限管理。图 4 为权限分配表，展现了在公选系统中传统 RBAC 模型和改进 RBAC 模型是如何进行权限分配的。

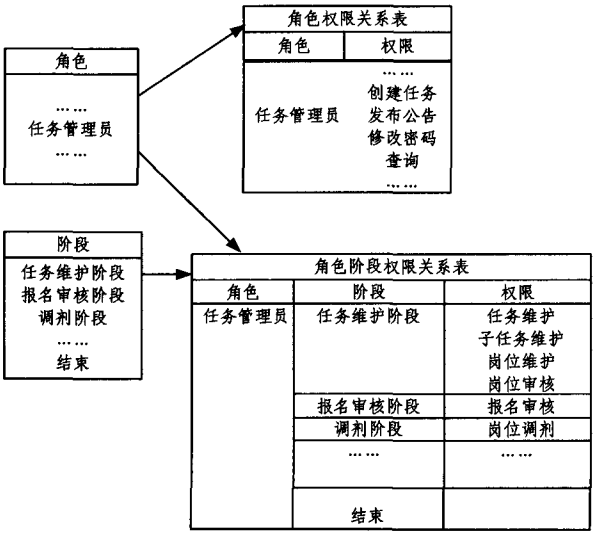

图 4　权限分配表

在公选系统中，传统的 RBAC 授权方法会使管理操作复杂，不能满足要求。但如果仅用改进的 RBAC 授权方法，则要求在每个阶段都必须分配通用的权限，从而造成很大的冗余，降低系统的效率。所以，本系统将二者结合使用，相互补充，使每种方法都充分发挥其优越性，从而提高权限管理的使用效率。

(1)如图 4 所示，假设我们有一个任务管理员的角色，运用改进型的 RBAC 方法，将系统进程根据阶段进行划分，任务管理员的权限将随着系统进程的不同阶段有所改变。例如：在任务维护阶段，任务管理员拥有任务维护、子任务维护、岗位维护、岗位审核的权限；在报名审核阶段，任务管理员拥有报名审核的权限。当任务未处于任务维护阶段时，任务管理员即使拥有岗位审核的权限，也不可以审核岗位。在改进型 RBAC 方法中，一个用户的权限由角色、阶段和权限三者的关系来决定，这就是 $(P\times R\times S)$ 三元关系分配。

(2)与此同时，运用传统的授权方法，任务管理员角色具有创建任务、发布公告、修改密码、查询等权限。这些权限跟阶段无关。只要创建了一个任务，任务管理员在该任务生存期的任何阶段都可以进行这些操作，这就是 $(P\times R)$ 二元关系分配。

按照上述方法，在整个任务进行期间，任务管理员只需要控制阶段的进度就可以控制各角色各用户的访问权限，操作起来十分简便。

3.3.2　数据库表设计

传统的 RBAC 模型实现中通常包含 5 张表，即：用户表、角色表、权限表、用户角色关系表和角色权限关系表。而改进的 RBAC 模型根据需求又添加了阶段信息表和角色阶段权限关系表。

阶段信息表的核心字段如表 1 所列。

表 1　阶段信息表 T_RW_JDXX

字段名	字段描述	数据类型
ID	唯一标识号，主键	VARCHAR(32)
JDDM	阶段代码	VARCHAR(2)
JDMC	阶段名称	VARCHAR(60)

表 T_RW_JDXX 里存放的是所有阶段的信息。管理员可在创建任务时添加本任务所用到的阶段。角色阶段权限关系表的核心字段如表 2 所列。

表 2　角色阶段权限关系表 T_RW_ROLE_JD_QX

字段名	字段描述	数据类型
ID	唯一标识号，主键	VARCHAR(32)
ROLE_ID	角色 ID，外键，关联角色表	VARCHAR(32)
JD_ID	阶段 ID，外键，关联阶段信息表	VARCHAR(32)
QX_ID	权限 ID，外键，关联权限表	VARCHAR(32)

表 T_RW_ROLE_JD_QX 里存放的是阶段与角色权限相结合的记录。ROLE_ID 是外键，关联角色表；JD_ID 是外键，关联阶段信息表；QX_ID 是外键，关联权限表。每一条记录都表示某种角色在某一阶段下所拥有的某种权限。

这样，所有的角色权限都可以分阶段进行配置，不同的阶段可分配不同的权限。权限更改也更加灵活。

结束语　基于角色的访问控制是一个重要的研究课题。本文在传统 RBAC 模型基础上提出一种基于时间分区的改进 RBAC 授权模型。首先将系统的整体进程按时间进度分成若干时间分区，并在每一个分区里进行传统的权限分配。

然后，将时间分区的概念具体化，加入阶段集，形成具体的改进 RBAC 模型。该模型将传统的“角色-权限”二元关系改进为“角色-阶段-权限”三元关系，增强了 RBAC 在实际运用中的灵活性。由于改进模型与传统模型是相容的，因此可同时使用两种权限控制方法进行系统的权限分配，从而大大提高权限管理的使用效率。

该改进模型的有效性[9]在实际项目中得到了验证，但是其通用性还有待进一步的研究。

参 考 文 献

[1] Xing Tian-yang, Cao Min. Research and application of algorithm for generating authority-tree based on TP-RBAC model [J]. Computer Engineering and Design, 2010, 31(5): 950-953

[2] 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

[3] 信科，杨峰，杨光旭，等. 基于 RBAC 权限管理系统的优化设计与实现[J]. 计算机技术与发展，2011，21(7)：172-174

[4] Sandhu R, Coyne E J, Feinstein H, et al. Role-based access control models [J]. IEEE Computer, 1996, 29(2): 38-47

[5] Zhou Wei, Meinel C. Team and task based RBAC access control model[C]// Network Operations and Management Symposium, 2007, LANOMS 2007. Latin American, IEEE, 2007: 84-94

[6] Ferraiolo D, Kuhn R. Role-Based Access Controls [C]// Proceedings of the 15th NIST-NCSC National Computer Security Conference. 1992: 554-563

[7] Yu Su, Wang Yin, Hua Kun. The research of information security based on RBAC with SOD [J]. International Journal of Advancements in Computing Technology, 2012, 4(14): 482-490

[8] 杨彩侠，王小慧，曹旻. OF_RBAC 权限控制模型的研究及应用[C]// Proceedings of 2010 International Conference on Management Science and Engineering. 2010: 65-69

[9] 董理君，胜生，杜敏，等. 一种基于环境安全的角色访问控制模型研究[J]. 计算机科学，2009，6(1)：1-54

(上接第 134 页)

[4] 曲向丽. 网格环境下互信机制关键技术研究[D]. 长沙：国防科学技术大学计算机学院，2008

[5] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]// Dale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996: 164-173

[6] 朱艳春，刘鲁，张巍. 在线声誉系统中的信任模型构建研究[J]. 控制与决策，2007，22(4)：413-417

[7] Blaze M, Feigenbaum J, Keromytis A D. Keynote: Trust management for public-key infrastructures [C] // Christianson B, Crispo B, William S, et al. , eds. Cambridge 1998 Security Protocols International Workshop. Berlin: Springer-Verglag, 1999: 59-63

[8] Chu Y H, Feigenbaum J, Lamacchia B. REFEREE: trust management for Web applications[J]. WordWideWeb Journal, 1997, 2(2): 127-139

[9] Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems[C]// Proceedings of the IEEE Canadian Conference on Electrical&Computer Engineering. 2002: 1424-1429

[10] Azzedin F, Maheswaran M. Towards Trust-Aware Resource Management in Grid Computing Systems [C] // Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid. 2002: 452-452

[11] Azzedin F, Maheswaran M. A Trust Brokering System and Its Application to Resource Management in Pubic-Resource Grids [C]// Proceedings of the 18th International Parallel and Distributed Processing Symposium. 2004: 289-298

[12] Beth T, Borcherding M, Klein B. Valuation of trust in open system[C] // Collmann D, ed. Computer Security, ESORICS'94. volume 875 of Lecture Notes in Computer Science, Berlin: Springer Verlag, 1994: 3-18

[13] Abdul-Rahman A, Hailers S. A distributed trust model[C]// Proceeding of the 1997 New Security Paradigms Workshop. Cumbia, UK: ACM Press, 1997: 48-60

[14] Kamvar S D, Schlosser M T. EigenRep: Reputation management in P2P networks[C] // Lawrence S, ed. Proc. of the 12th Int'l World Wide Web Conf. Budapest: ACM Press, 2003: 123-134

[15] Zhang Q, Zhang X, Wen X Z, et al. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96-107

[16] Yuan L L, Zeng G S, Jiang L L, et al. Dynamic Level Scheduling Based on Trust Model in Grid Computing[J]. Chinese Journal of Computers, 2006(7): 1217-1224

[17] Richardson M, Agrawal R, Domingos P. Trust management for the semantic web[C]// Proceedings of the Second International Semantic Web Conference. 2003: 351-368

[18] Christian B, Radoslaw O. Using context-and content based trust policies on the semantic web[C]// Proceedings of the 13th international World Wide Web Conference on Alternate track papers & Posters. 2004: 228-239

[19] 李海华，杜小勇，田萱. 一种能力属性增强的 Web 服务信任评估模型[J]. 计算机学报，2008，31(8)：1471-1477

[20] 董晓华，吴中福. 网格服务信任的赔偿评估模型[J]. 重庆大学学报，2010，33(6)：121-127

[21] 董晓华. 网格服务的信任机制研究[D]. 重庆：重庆大学，2010

[22] Ziegler C N, Golbeck J. Investigating interactions of trust and interest similarity[J]. Decision Support Systems, 2007, 43(2): 460-475

[23] 李景涛，荆一楠，肖晓春，等. 基于相似度加权推荐的 P2P 环境下的信任模型[J]. 软件学报，2007，18(1)：157-167

[24] 袁传思. 基于用户信任的攻击检测防御模型[J]. 重庆理工大学学报：自然科学版，2010，24(6)：72-77