维普资讯 http://www.cqvip.com

第16卷 第2期
2006年2月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.2
Feb. 2006

一种基于任务和角色的访问控制模型及其应用

景栋盛,杨季文
(苏州大学 计算机科学与技术学院,江苏 苏州 215006)

摘 要:近年来RBAC(Role-Based Access Control)及TBAC(Task-Based Access Control)模型得到广泛的研究。文中比较了一些现有访问控制模型的各自特点和适用范围,针对现有模型的不足,为了提高系统的安全性、通用型和实用性,通过结合RBAC及TBAC模型各自的优点,提出了一个新型的访问控制模型T-RBAC(Task-Role Based Access Control)。描述了T-RBAC模型结构和特点,阐述了模型对最小权限原则、职权分离原则、数据抽象原则及角色层次关系的支持,给出了模型在协同编著系统中的一个应用和将来工作的主要目标。

关键词:基于角色的访问控制;基于任务的访问控制;基于任务和角色的访问控制
中图分类号:TP309 **文献标识码**:A **文章编号**:1005-3751(2006)02-0212-03

A Model of Task-Role Based Access Control and Its Application

JING Dong-sheng, YANG Ji-wen
(Computer Dept. of Suzhou University, Suzhou 215006, China)

Abstract: The research work of RBAC (role-based access control) and TBAC (task-based access control) is greatly emphasized in recent years. This paper compares the characteristics and applicability spectrum of some recent models. To the deficiency of the existing model, in order to improve the security, compatibility and practicability of application systems, through combining the advantages of RBAC and TBAC model, a new-type model, T-RBAC(task-role based access control), is discussed. The configuration and characteristics of the model is described. The support of least privilege, separation of duties, data abstraction and roles hierarchies in the model is explained. An application of the model in computer supported cooperative system and the main goal of future research is presented.

Key words: RBAC; TBAC; T-RBAC

0 引 言

访问控制在ISO74982里是网络安全服务5个层次中的重要一层。访问控制的目的是通过某种途径显示的限制用户对系统资源的访问,从而使系统在合法的范围内使用。20世纪70年代Harrison, Ruzzo和Ulman提出了HRU模型,紧接着Jones等人提出了Take-Grant模型。后来又有著名的自主访问控制模型(DAC)和强制访问控制模型(MAC)。从70年代末开始R.S.Sandhu等学者[1]先后提出了存取控制矩阵(TAM),RBAC,TBAC(1993年提出)。由于访问控制模型的适用范围各有不同,提出后各种模型一直不断发展,尤其是RBAC,TBAC至今仍在不断地完善和充实中。

1 各种访问控制方法比较

DAC(discretionary access control)系统中的主体可以自主地将其拥有的对客体的访问权限授予其它主体。其实现方法一般是建立系统访问控制矩阵,矩阵的行对应系统的主体,列对应系统的客体,元素表示主体对客体的访问权限。DAC有其致命弱点:访问权限的授予是可以传递的。一旦访问权限被传递出去将难以控制,访问权限的管理相当困难,会带来严重的安全问题;在大型系统中开销巨大,效率低下;DAC不保护客体产生的副本,增加了管理难度。

MAC(mandatory access control)系统中的主/客体都被分配一个固定的安全属性,利用安全属性决定一个主体是否可以访问客体。安全属性是强制的,由SO向主体和客体分配安全标签。利用下读/上写来保证数据的保密性,并且通过这种梯度安全标签实现信息的单向流通。MAC的缺点很明显:MAC系统的灵活性差;虽机密性得到增强,但不能实施完整性控制,不利于在商业系统中的运用;必须保证系统中不存在逆向潜信道,而在现代计算机中是难以去除的,如各种Cache等。

RBAC引入角色做为中介,本身是中立的访问控制策略,但其扩展模型的扩展策略可能使其与DAC,MAC并存。1996年提出的RBAC96模型[2]是一个权威的基于角色的访问控制参考模型,包括4个层次:RBAC0模型定义了支持基于角色访问控制的最小需求,如用户、角色、权

收稿日期:2005-05-13
基金项目:江苏省高校指导性项目(Q2118042)
作者简介:景栋盛(1981—),男,江苏苏州人,硕士研究生,研究方向为计算机安全、CSCW;杨季文,教授,研究方向为中文信息处理等。

维普资讯 http://www.cqvip.com

限、会话等概念；RBAC1 在 RBAC0 的基础上加入了角色继承关系，并提出了公有角色和私有角色的概念，由于公有角色和私有角色存在数据冗余且动态性差的缺点，2000 年国内提出了公有继承和扩展继承的概念[3]，提出了 EHRBAC（extended hierarchy role－based access control），完善了原有的模型；RBAC2 模型在 RBAC0 的基础上加入了各种用户与角色之间、权限与角色之间以及角色与角色之间的约束关系，包括角色互斥、角色最大成员数、前提权限、前提角色等；RBAC3 是对 RBAC1 和 RBAC2 的集成，包括两者的共同内容。RBAC 的授权是静态的，对于系统中权限动态的更改有着“先天不足”，国内有学者提出了带时间特性的访问控制模型 TRBAC[4,5]（timed role based access control），其实，R. S. Sandhu 早在文献[2]中就认识到了这一点，并在文献[6]正式提出了 4 个 RBWM 模型，给出较为完善的解决方案。

ARBAC97 及 ARBAC02[7]，ARBAC97 由 3 个部分组成，包括 URA97，PRA97，RRA97，完善了用户－角色指派、角色－权限指派和角色－角色指派的管理。URA02 保留了 URA97 的主要特点，重新定义了指派先决条件，将组织结构引入指派候选用户的选择过程中，完善了角色指派过程。ARBAC97 及 ARBAC02 是在原有 RBAC 模型上的扩展，更多地考虑了角色基数、角色互斥、SOD 等方面，但 RBAC 的缺点并没有本质上的改进。

TBAC 是一种上下文相关的访问控制模型，又是一种基于实例的访问控制模型[8]。由于任务的实效性，用户对于授予他的权限的使用也是有实效性的。TBAC 基本概念包括授权步、授权结构体、任务和依赖。TBAC 从工作流中任务角度建模，可依据任务和任务状态的不同，对权限进行动态的管理。但是 TBAC 可能产生最小权限约束的假象，一个主体往往可以执行多项任务，用户一旦激活角色就拥有该主体的全部权限，实际操作时拥有多于单独执行任务的权限，所以 TBAC 没有达到真正的最小权限约束。

2　T－RBAC 模型的提出和特点

2.1　T－RBAC 模型

传统的访问控制模型中，DAC 太弱，MAC 太强，TBAC 应用范围不广，RBAC 较为灵活有效，但模型的核心是静态的，使之做动态的扩充总有一些牵强。文中结合 TBAC 和 RBAC 各自的优点，建立一个灵活有效可以广泛应用的模型 T－RBAC，如图 1 所示。此模型满足安全模型的 3 个原则。

Users(U)＝{u_1，u_2，…，u_m}所用用户(user)的集合。

Roles(R)＝{r_1，r_2，…，r_n}所有角色(role)的集合。

Ops＝{op_1，op_2，…，op_k}所有操作(operation)的集合。

Objects＝{ob_1，ob_2，…，ob_l}所有访问对象的集合。

Sessions(S)＝{s_1，s_2，…，s_p}所有会话(session)的集合。

Perms(P)＝$2^{(Ops\times Objects)}$所有权限(permission)的集合。

Attribute(A)属性表示用户、角色、任务或权限本身的信息以及限制。

UA⊆Users×Roles 为从用户集合到角色集合的多对多映射，表示用户被赋予的角色。

PA⊆Perms×Roles 为从权限集合到角色集合的多对多映射，表示角色被赋予的权限。

assigned_users：(r：Roles)→2^{Users}为返回指定给角色的用户集，assigned_users(r)＝{u∈Users|(u，r)∈UA}。

assigned_perms：(r：Roles)→2^{Perms}为返回指定给角色的权限集，assigned_perms(r)＝{p∈Perms|(p，r)∈PA}。

assigned_roles：(u：Users)→2^{Roles}为返回指定给用户的角色集合，assigned_roles：(u)＝{r∈Roles|(u，r)∈UA}。

Roles Hierarchy(RH)为角色继承关系，与 RBAC96 相同。

Permissions Hierarchy(PH)为权限继承关系。

TT 为任务集。

TI 为任务实例集。

CONTEXT 为上下文。

F 为一个任务到任务实例的映射。

F：TT→2^{TI}such thatF(a)∩F(b)＝øif a≠b and a，b∈TT

taskInstances(taskContext)＝{ti|(∃r'≤r)(∃tt∈tasks(r'))[tiFF(tt)]∧[canExecute(taskContext，tt)＝true]}

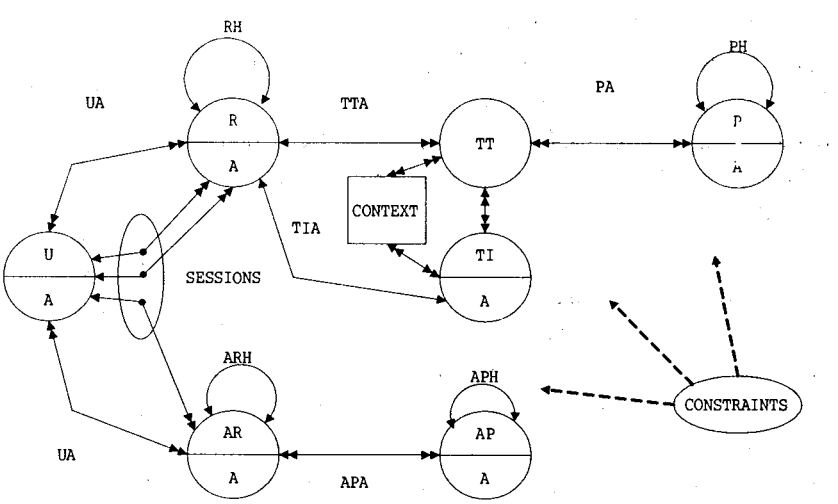

图 1　T－RBAC 模型

2.2　安全控制原则

2.2.1　最小权限原则

在 T－RBAC 模型中的角色拥有的权限不但支持私有权限和公有权限，而且拥有两种状态：睡眠态和激活态。

维普资讯 http://www.cqvip.com

定义 1 睡眠态表示角色拥有的权限处于存在却无效的状态。

定义 2 激活态表示角色拥有的权限处于存在且有效的状态。

管理层分配给角色的权限首先处于睡眠态,只有真正有任务需要角色完成时,任务实例(TI)激活角色中完成任务所需的最小权限,使角色的部分权限的状态由睡眠态转为激活态。不管用户赋予的角色如何,都必须在执行授权任务期间才拥有该操作任务实例的权限。任务执行完毕后自行回收,角色的这部分权限由激活态回到睡眠态。由于权限直接与任务相关,笔者认为最小权限的约束可以得到保证。

2.2.2 职权分离原则

在实际的应用系统中,一旦两个角色可能产生互惠关系,则必须由不同的主体担任,如银行贷款的申请人和审批人是不能由一个人担任的。在 T-RBAC 中,职权分离实现非常方便,系统可以在角色的属性中添加限制条件完成。角色属性内容的定义在 T-RBAC 中是由系统的管理角色完成的,这样较小的修改就可以适应各种不同应用的需要。

2.2.3 数据抽象原则

T-RBAC 支持数据抽象原则在不同的应用系统中的应用,如权限不局限于操作系统提供的读写权限,可以抽象为实际任务中的编辑权限,如主编对文档的阅读/改写操作。

2.3 角色层次关系

T-RBAC 模型支持角色层次的 4 种关系:权限继承关系、角色继承关系、管理层次关系、约束继承关系,具体参见文献[9]。

2.4 角色与组的关系

角色是一组权限的集合,而组典型定义为一组用户的集合。在 RBAC 中没有组的概念,但通常的多用户系统中又常常出现组的概念如不同部门(组)的相同员工,在 RBAC 中只能用不同的角色表示。而在 T-RBAC 中,组可以是用户的属性之一,极为灵活,又符合实际运用的多样性需要。

3 T-RBAC 的一个应用

Z-OFFICE 是一个基于 OpenOffice.org 开发的协同编著系统,它包括工作流模块、协作控制模块、访问控制模块、存取控制模块 4 个主要部分,具体关系如图 2 所示。由于访问此系统的主体包括普通用户、高级用户,甚至可以是一般的 Internet 用户,加上信息种类繁多,信息量巨大以及信息的保密性和完整性,使得安全访问控制非常复杂。笔者把 T-RBAC 运用到 Z-OFFICE 的访问控制模块中,集成了 RBAC 和 TBAC 的优点,增加了工作流的访问控制能力,增强了动态约束能力,满足了实际业务过程对访问控制的需求。

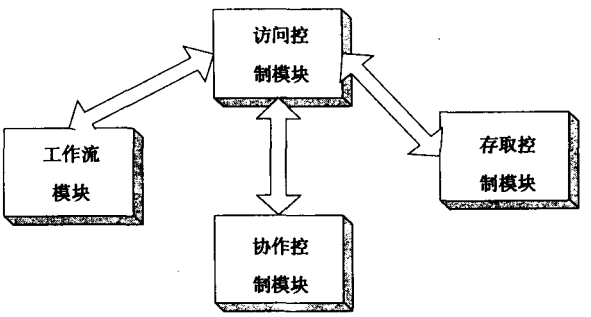

图 2 Z-OFFICE 模块关系

4 结 论

国内外曾有学者也研究过 CSCW 的一般需求,并在文献[10]中总结为 4 点。文中的这个模型完全符合这 4 点的需求。而且模型本身是中性的,在此模型结构上的不同扩展可以使模型运用于各种场合。T-RBAC 模型在各种领域的广泛应用是进一步研究的方向。

参考文献:

[1] Thomas R K, Sandhu R S. Toward a task-based paradigm for flexible and adaptable access control in distributed applications[A]. In: Proc of 1992-1993 ACM SIGSAC New Security Paradigms Workshops[C]. NY:[s.n.], 1993. 138-142.

[2] Sandhu R S, Conyne E J, Lfeinstein H, et al. Role-Based Access control Model[J]. IEEE Computer, 1996, 29(2):38-47.

[3] 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.

[4] 董光余,卿斯汉,刘克龙. 带时间特性的角色授权约束[J]. 软件学报,2002,13(8): 1521-1527.

[5] 黄 建,卿斯汉,温红子. 带时间特性的角色访问控制[J]. 软件学报,2003,14(11):1944-1954.

[6] Kandala S, Sandhu R. Secure Role-Based Workflow Models [A]. In: Proceedings of the 15th IFIP WG 11.3 Working Conference on Database Security [C]. Niagara, Ontario, Canada:[s.n.], 2002.45-58.

[7] Oh S, Sandhu R. A Model for Role Administration Using Organization Structure[A]. In: Seventh ACM Symposium on Access Control Models and Technologies(SACMAT'02)[C]. Monterey, California, USA:[s.n.],2002.155-162.

[8] 邓集波,洪 帆. 基于任务的访问控制模型[J]. 软件学报,2003,14(1):76-82.

[9] 张绍莲,欧阳毅,杜 鹏,等. 角色层次的分析与研究[J]. 计算机科学,2002,29(3): 72-74.

[10] 李成锴,詹永照,茅 兵,等. 基于角色的 CSCW 系统访问控制模型[J]. 软件学报,2000,11(7): 931-937.