第25卷 第8期 计算机工程与设计 2004年8月
Vol. 25 No. 8 COMPUTER ENGINEERING AND DESIGN Aug. 2004

文章编号: 1000-7024(2004)08-1367-03 中图分类号: TP309 文献标识码: A

基于角色的访问控制模型及其面向对象的建模

张志勇

(河南科技大学 电信学院, 河南 洛阳 471003)

摘 要: 访问控制是信息安全的一个研究方向, 基于角色的访问控制(RBAC)是目前理论研究和应用研究比较广泛的一种模型。详细介绍了RBAC96模型家族的特征和它所遵循的安全准则, 并引入面向对象的思想, 采用统一建模语言(UML)对RBAC96进行了静态和动态建模, 这样就缩短了理论模型和实际系统开发之间的差距, 有助于信息系统安全的面向对象的分析与设计。

关键词: 访问控制; RBAC96; 面向对象; UML; 建模

Role-based access control and object-oriented modeling

ZHANG Zhi-yong

(School of Electronic and Information Engineering, HUST, Luoyang 471003, China)

Abstract: Access control is a research direction of information security, Role-based access control is a model that is widely researched in theory and application aspects now. The characters and security rules of RBAC96 model family are introduced in detail firstly, and in the basis of object-oriented thinking, static and dynamic models of RBAC96 are given by using UML. This method reduces gap between theory models and application development, and is beneficial to OOA and OOD in information system security.

Key words: access control; role-based access control96; object-oriented; unified modeling language; modeling

1 引 言

从20世纪90年代开始,在信息安全的研究过程中,访问控制模型的研究占了主导地位。其中基于角色的访问控制(RBAC)模型的研究受到了越来越多的关注,在实际系统中也得到广泛的应用。目前,一些商用大型数据库系统,如Sybase ASE12.5、Oracle 8i、Informix已部分实现了RBAC96模型中的特征[1]。在政府、企事业单位的信息化进程中,管理信息系统和决策支持系统等大型的信息系统,在解决信息安全方面也都才采用了RBAC模型,来保障系统中数据信息的安全性。

2 基于角色的访问控制模型

2.1 RBAC96模型简介

RBAC96模型的一个主要特点是在用户和权限之间引入角色这个概念,并且围绕着角色这个新的概念来实施访问控制策略。不同的角色和它所应具有的权限许可相互联系,而用户作为某些角色的成员,这样便获得了这些角色的权限。角色可以根据实际单位或组织的不同工作职责来划分,依据用户所承担的不同的权力和义务来授予相应的角色。对于一个存在大量用户和权限分配的系统来说,从大量的用户管理转而管理、操纵少量的角色,这样简化了权限分配管理,提高了安全管理的效率和质量,并且能够直接反映企事业单位内部安全管理策略和管理模式。

2.2 RBAC96的主要概念及形式化描述

(1) 用户(user): 主要是和某个计算机系统交互的自然人。

(2) 角色(role): 反映一个组织内部一项具体的工作职责,被授予该角色的用户将具有一定的职权。在一次会话开始时,用户在自身的角色集中所激活的角色构成活跃角色集。

(3) 许可(permission): 作为系统主体的人对客体进行特定模式访问的操作权限。

(4) 会话(session): 一个用户和他所具有的角色集中活跃角色集之间的映射关系,具有动态特征。在一次会话过程中,用户具有活跃角色集所对应的全部权限。

定义用户集合U,R(u∈U)表示用户u所拥有的角色集,AR(u∈U)表示用户u的活跃角色集,P(r)表示角色r所拥有的许可集,S(u∈U)为用户u的会话集[2]。

PA⊆P×R,PA是许可到用户的多对多的关系。

UA⊆U×R,UA是用户到角色的多对多的关系。

RH ⊆R×R, RH是角色上的一个偏序关系,称之为角色层次关系或支配关系,一般记为"≥"。

$roles(S_i)\subseteq\{\ni r|(r'\geq r)[(user(S_i),r)\in UA]\}$

收稿日期: 2003-09-16。

作者简介: 张志勇(1975-),男,河南新乡人,硕士,研究方向为信息安全、智能决策支持系统。

User:S→U,将各个会话映射到一个用户的函数User(S_i)。

roles:S→2^R,将各个会话S_i与一个角色集合联结起来的映射,随时间的变化而变化,而会话S_i的授权Ur ∈roles(Si) {p|(p,r) ∈PA}。

定义谓词exes(u,s):用户u能够执行会话s,谓词exep(u,p):用户u能够执行许可p。

规则1:如果一个用户不具备任何角色,则无权开始一次会话。

$$\forall u,s(u\in U,s\in S)(exes(u,s)\Rightarrow R(u)\neq\varnothing)$$

规则2:用户在一次会话中的活跃角色必须是经过授权的。

$$\forall u(u\in U)(AR(u)\subseteq R(u))$$

规则3:用户所能执行的许可必须是当前活跃角色所拥有的许可。

$$\forall u(u\in U)(\ exep(u,p)\Rightarrow \exists\ r(r\in AR(u)\wedge p\in P(r)))$$

2.3 RBAC96模型家族的主要特征

(1)层次结构:因为角色代表的是一个组织内部的某一项具体职责,因此角色的层次关系是必然存在的。上层角色可以继承下层角色的许可,并且还可能拥有一些特有的私有许可。角色的层次关系属于一个偏序关系,满足自反性、反对称性和传递性。

(2)角色约束:角色静态互斥是要求某些角色不能同时分配给一个用户;动态互斥是一个用户开始会话时,不能同时激活某些角色,否则将会违背本组织的安全策略。

角色基数包括角色可以分配的最大和最小用户数,基数约束并非RBAC模型所要求的,但在具体的应用系统中,却是安全策略所要求的一个方面。大多数的应用系统在RBAC模型的实现过程中,将其作为角色约束的一项来加以实现。

3 面向对象和统一建模语言(UML)

3.1 面向对象的方法和特点

面向对象的方法是一种运用对象、类、继承、封装、聚合、消息传递、多态性等概念来构造系统的软件开发方法[3]。面向对象方法的基本思想是:从现实世界中客观存在的事物(即对象)出发来构造软件系统,并在系统构造中尽可能运用人类自然的思维方式。面向对象方法的主要特性是封装性、继承性和多态性。

3.2 统一建模语言(UML)及图形表示

1997年1月Rational软件公司的3位学者Grady Booch、Jim Rumbaugh和Ivar Jacobson正式提出了面向对象系统的建模语言UML(Unified Modeling Language,简称UML)1.0版,这是OO行业中具有里程碑性质的新进展。UML语言的出现建立了统一的面向对象开发方法。

可视化描述模型元素是面向对象建模方法的一大特点。UML符号表示法定义了可视元素,并为开发者或开发工具使用这些图形符号和文本语法进行系统建模提供了标准。这些图形符号和文字所表达的是应用级的模型,在语义上它是UML元模型的实例。UML表示法的主要内容可由5类(共9种)图来组成,分别为用例图、静态图、行为图、交互图和实现图[4]。其中:

(1)用例图(use case diagram):从用户角度描述系统功能,并指出各功能的作用。

(2)静态图(static diagram):包括类图(class diagram)、对象图(object diagram)和包图(package diagram)。类图描述系统中类的静态结构,不仅定义系统中的类,表示类之间的联系如关联、依赖、聚合、泛化等,也包括类的内部结构(类的属性和操作)。类图描述的是一种静态关系,在系统的整个生命周期都是有效的。对象图是类图的实例,几乎使用与类图完全相同的标识。它们的不同点在于对象图显示类的多个对象实例而不是实际的类,且对象图只能在系统的某一个时间段存在。包图由包或类组成,表示包与包之间的关系。包图用于描述系统的分层结构。

(3)交互图(interactive diagram):动态建模的一种视图,描述对象间的交互关系,包括顺序图(sequence diagram)和合作图(collabration diagram)。顺序图显示对象之间的动态合作关系,它强调对象之间消息发送的时间顺序;合作图也显示对象间的动态合作关系,但更强调上下级关系。这两种图之间通过可视化建模工具(Rational Rose 2002)可以相互转化。

4 基于面向对象思想的RBAC系统建模

4.1 RBAC建模的意义

自从RBAC被广泛地认为是一种已经得到证明的访问控制模型,许多安全方面的研究者和安全系统的开发者花了许多时间来开发基于角色的系统,一些开发基于角色系统的框架引用了此模型。由于这些系统框架比较抽象和形式化,另外一些又主要面向具体应用或是特殊领域,使得早期的工作对于系统开发者来说存在一定的困难。这些框架并不能给系统开发人员一个完好的蓝图。为了缩短理论安全模型和系统开发之间的差距,支持应用系统的面向对象的分析与设计,因此基于面向对象的思想对RBAC进行系统建模是非常必要的[5]。

4.2 RBAC系统的静态建模

关于RBAC的静态建模,主要描述使用RBAC模型的应用系统的用例图、实体类和类图。在RBAC系统用例图

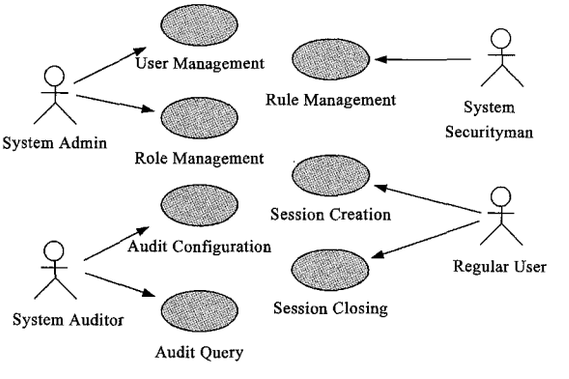

图1 RBAC系统用例图

中，主要描述系统的对外功能。对于这些功能的使用，安全管理的用户主要分为以下3类：系统管理员、系统安全员和系统审计员。这3类用户分别完成不同的工作，属于3类管理角色。系统管理员完成用户和角色的管理；系统安全员负责管理角色规则库，实现角色约束规则；系统审计员负责设置审计对象，查询审计信息等。对于普通用户主要是在系统中建立会话，完成系统相应的功能，关闭会话等。关于审计功能的实现，可以根据实际系统的需要选择使用，但是作为B1以上安全级的数据库系统或其它系统，绝大多数实现了审计功能。它主要完成对普通用户创建会话，使用系统中的数据信息和管理员管理系统的操作进行跟踪监视。用例图如图1所示。

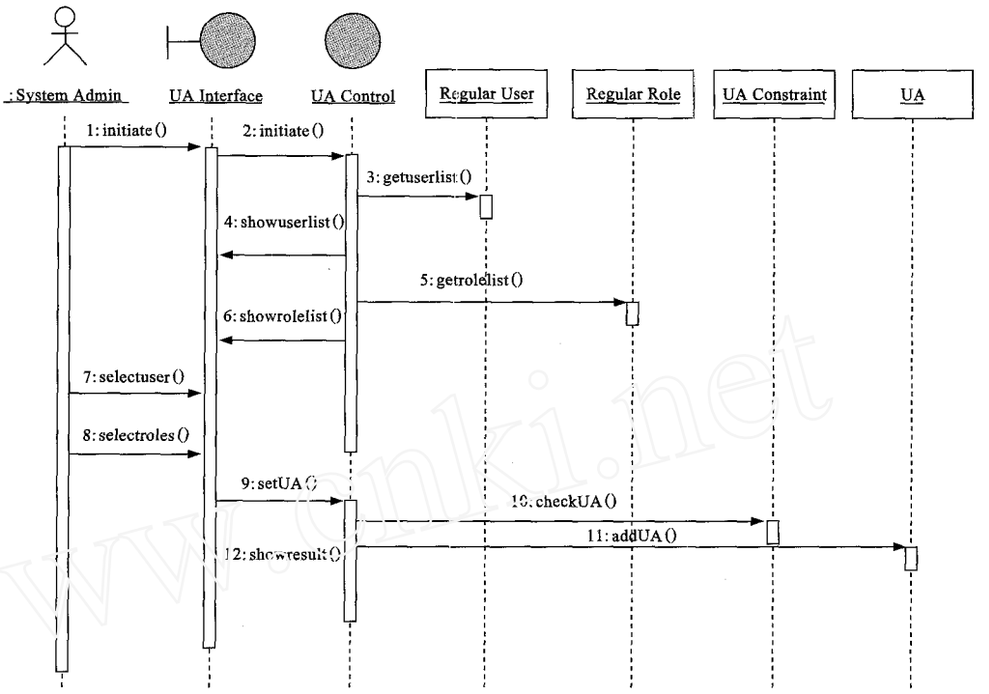

图4 为用户分配角色的顺序图

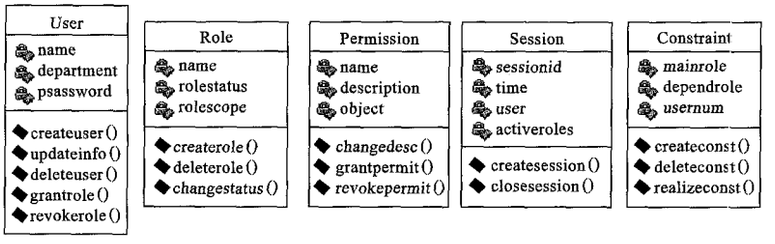

图2 RBAC中的主要实体类

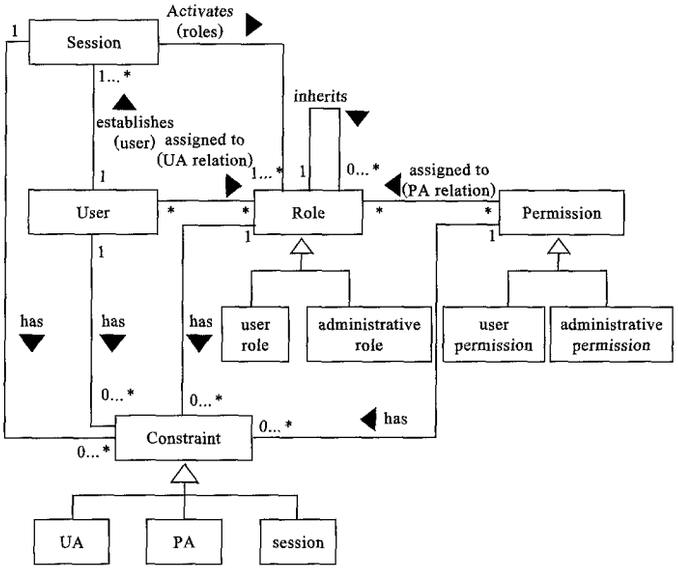

图3 RBAC类关系图

按照RBAC的用例图和面向对象的思想，对整个系统设计以下几个主要的实体类（如图2所示），包括类中主要的属性与方法（操作），并对各个类之间的关系进行了建模（如图3所示）。

各个类之间的关系描述的是RBAC的静态特征。从图3中可以看出各个类之间存在的关联和泛化关系，以及关联关系的基数特征。这里把角色类和许可类分别泛化为管理角色、普通角色和管理许可、普通许可两个子类，它们继承父类的公用的属性和方法，并具有自身特有的属性和操作；这符合RBAC的扩展模型ARBAC（Administrative RBAC）的特征，提高了RBAC模型管理自身的能力[2]。约束类被泛化为3个子类UA、PA和Session，分别完成用户分配和许可分配，以及用户启动与撤销会话3个方面的规则约束。在图2中，也描述了各个类之间的基数特征，如用户、角色和许可3个类之间是多对多的关系等。

4.3 RBAC系统的动态建模

关于RBAC的动态建模，主要描述使用RBAC模型的应用系统的交互图和对象行为图。对于RBAC系统的动态建模，这里由于篇幅问题，不可能完全描述系统所有的动态行为特征。因此，选择具有代表性的为用户分配角色的顺序图（交互图中的一种）加以描述和解释。图4是为用户分配

（下转第1374页）

表 8 AccessMask 取值

值	意义
GENERIC_ALL	完全控制
GENERIC_EXECUTE	执行
GENERIC_READ	读
GENERIC_WRITE	写
DELETE	删除

表 9 Option 取值

值	意义
GRANT_ACCESS	允许存取，保留原有的访问权限（添加）
SET_ACCESS	设置新的允许访问 ACE，并取消原有针对该指定用户的所有 ACE
DENY_ACCESS	设置拒绝访问 ACE，原有的拒绝访问权限保留
REVOKE_ACCESS	取消所有针对指定用户的允许访问 ACE

表 10 InheritFlag 取值

值	意义
CONTAINER_INHERIT_ACE	指定目录中包含的所有子目录继承该 ACE
INHERIT_ONLY_ACE	指定目录下所有文件继承该 ACE，但不对指定目录进行设置
OBJECT_INHERIT_ACE	指定目录下所有文件继承该 ACE

指定文件：

```
dwError = :: SetNamedSecurityInfo (FileName, SE_FILE_
OBJECT,
        DACL_SECURITY_INFORMATION,
        NULL,NULL,NewAcl,NULL);
```

3 结 论

由于 Windows 系统提供了丰富的 API [4]，故一般来说 Windows 平台中的系统管理任务都可以通过程序实现。但底层的 API 函数使用起来毕竟较为复杂，通过 COM 组件实现 Windows 系统或应用系统的管理是 Windows 平台系统管理（如 Active Directory、Exchange Server、IIS 服务、Media Service 等）程序化的主要途径。

参 考 文 献:

[1] Microsoft. Windows platform SDK documentation. [M]. Redmond,USA:Microsoft, 2003.

[2] Microsoft, Exchange SDK documentation [M]. Redmond,USA: Microsoft, 2003.

[3] 郭红芳, 潘战生. 计算机公共课程远程教学系统 [J]. 计算机应用, 2002,(6):97-101.

[4] Microsoft. Win32 程序员参考大全(2)[M]. 北京:清华大学出版社, 1995.

(上接第 1355 页)

[8] Sugano H,Fujimoto S. Common presence and instant messaging presence information data format [EB/OL]. 2002.

[9] Crocker D, Peterson J. Common profile for instant messaging [EB/OL]. 2003.

[10] Crocker D,Diacakis A. Address resolution for instant messaging and presence [EB/OL]. 2003.

(上接第 1369 页)

角色的顺序图，它描述了为用户分配角色这个操作的动态特性，并且从图中可以看出每个步骤之间的时间顺序关系。图 4 的顶部是参与分配角色的用户和相关的对象，虚线代表每个对象的生命周期；箭头所标识的是对象之间消息通信的方向，并在上方注明了消息发送的时间顺序及名称。

5 结束语

在管理信息系统和决策支持系统的安全设计和开发过程中，采用 RBAC 模型可以更好地实现企事业单位的安全控制策略。本文基于面向对象的思想，采用 UML 对 RBAC 的建模在实际的工程项目"黑龙江省防洪指挥决策支持系统"中数据库安全管理系统(DBSMS)的研发过程中，发挥了重要作用，对于其它基于角色的访问控制系统的面向对象分析与设计也将具有一定的实际意义和应用价值。对于 RBAC 的扩展模型中具有委托特性的 RBDM(Role-Based Delegation Model) 模型的面向对象建模需要做进一步研究工作。

参 考 文 献:

[1] Chandramouli Ramaswamy, Ravi Sandhu. Role-based access control feature in commercial database management systems[C]. NISSC,U S,1998.

[2] Ravi Sandhu.Role-based access control models[J].IEEE Computer,1996,29(2):38-47.

[3] 邵维忠,杨芙清.面向对象的系统分析[M].北京:清华大学出版社, 广西科学技术出版社, 1998.

[4] 鲁博, 柴跃廷.关于统一建模语言—UML[J].计算机工程与科学, 2000, 22(4):57-60,70.

[5] Michael E Shin, Ahn Gail-Joon. UML-based representation of role-based access control[C].Proceedings of 5th IEEE International Workshop on Enterprise Security, NIST,MD,2000.