DOI :10. 3969/J. ISSN. 1672-6693. 2009. 03. 016

基于时态信息的 RBAC 建模研究*

刘 智[1], 邹枝玲[2]
(1. 重庆理工大学 计算机科学与工程学院, 重庆 400050 ;2. 西南大学 心理学院, 重庆 400715)

摘要 :经过多年的发展,RBAC 模型理论研究已十分成熟,并广泛成功应用于信息系统访问控制。本文阐述了 RBAC 模型安全控制的思想及原理,它通过抽象用户、角色、目标、操作、许可权 5 个基本数据元素并建立它们之间的联系构建网络状的权限控制模型 ;分析了 RBAC 模型在处理具有时间约束的访问控制时的不足,不能充分考虑时态系统中基于时间约束的授权和访问控制 ;回顾了时态 RBAC 模型的研究现状,讨论了时态 RBAC 模型在时态系统授权中存在的问题,它只在角色层次进行了简单约束,而对授权和角色指派等过程中的细节考虑不够 ;展望了 GTRBAC 模型的思想并进行了讨论,GTRBAC 不仅在时态 RBAC 的基础上考虑了持续约束、周期约束和其他特定形式的激活约束,而且提出了约束冲突的解决办法,是目前在时态环境下定义比较完全和细致的访问控制模型。

关键词 :时态系统 ;基于角色的存取控制 ;时态约束 ;访问控制
中图分类号 :TP311. 13 文献标识码 :A 文章编号 :1672-6693(2009)03-0069-03

数据的网络化存储及共享性要求使得信息系统访问控制研究成为热点[1-3]。RBAC 模型[4] 由于高效的授权管理,面向应用层的自然映象等特点,理论研究和应用开发发展迅速,被公认为是最具发展潜力的新一代存取控制模型,并于 2004 年纳入了 NIST 标准。然而,NIST 标准中的 RBAC 模型[1] 对时间约束的支持功能还相当简单,对时态对象的存取控制建模能力弱。文章简单介绍了 RBAC 模型、时态 RBAC 模型,分析其在实际应用中的优缺点,对 RBAC 模型的最新研究进展—GTRBAC 模型进行了讨论。

1 RBAC 模型简述

NIST(The national institute of standards and technology,美国国家标准与技术研究院)标准 RBAC 模型[1] 由 4 个部件模型组成,这 4 个部件模型分别是基本模型 RBAC0 (Core RBAC)、角色分级模型 RBAC1(Hierarchal RBAC)、角色限制模型 RBAC2 (Constraint RBAC) 和统一模型 RBAC3 (Combines RBAC)。RBAC0 模型如图 1 所示。

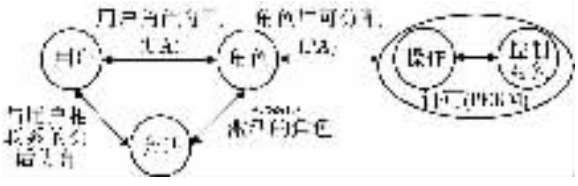

图 1 RBAC0 模型

RBAC0 定义了能构成一个 RBAC 控制系统的最小元素集合。它包含用户(USERS)、角色(ROLES)、目标(OBS)、操作(OPS)、许可权(PRMS)5 个基本元素。权限被赋予角色,而不是用户,当角色被指定给用户时,此用户就拥有了该角色所包含的权限。

RBAC1 引入角色间的继承关系,角色间的继承关系可分为一般继承关系和受限继承关系。一般继承关系仅要求角色继承关系是一个绝对偏序关系,允许角色间的多继承。而受限继承关系则进一步要求角色继承关系是一个树结构。

RBAC2 模型中添加了责任分离关系。RBAC2 的约束规定了权限被赋予角色时,或角色被赋予用户时,以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。责任分离包括静态责任分离和动态责任分离。约束与用户—角色—权限关系共同决定了 RBAC2 模型中用户的访问许可。

RBAC3 包含了 RBAC1 和 RBAC2,既提供了角色间的继承关系,又提供了责任分离关系。

NIST 标准 RBAC 模型具有相当的对授权约束的描述能力,但没有提供对时间约束的建模,不能很好地描述时态系统中用户、角色中权限的时态设置,不能很好满足现代管理信息系统的需求。

2 时态 RBAC 模型

在RBAC系统中引入时间约束主要有两种方

* 收稿日期 :2009-03-27
资助项目 :重庆市自然科学基金计划项目(No. CSTC,2008BB0260)
作者简介 :刘智,讲师,博士研究生,研究方向为信息融合、数据库 ;通讯作者 :邹枝玲,E-mail :zouzl@ swu. edu. cn

法:①对RBAC做时间维上的扩展,通过定义一个离散时间点序列来模拟现实世界中的连续时间序列[5];②通过引入日历的概念来定义周期时间表达式[6,7]。第一种时间系统的定义及时间约束的描述在一些具体的应用过程中并不是最佳的,当时间的粒度很细时,时间状态的监测会占用大量的系统开销,而基于周期时间约束可以方便地描述与时间有关的规律性活动。

为了扩充RBAC的时间建模能力,Bertino等人提出了时态RBAC(Temporal—RBAC,TRABC)模型[6],TRBAC基于周期表达式方法来考虑授权的时态因素,它借用触发器技术在不同的时间段启动或禁用某个角色以及引入角色间的时态约束机制。但对于复杂的时态约束,TRBAC存在明显不足。首先,它不支持用户—角色和角色—权限指派的时态约束,而仅支持角色的启动或禁用,而大多数应用中,角色是静态的,即所有时刻均处于启动状态,而用户对角色的拥有或权限对角色的分配才是动态的;其次,TRBAC不能区分角色的启动和激活概念,不能处理和角色激活相关的一些约束,如设定用户激活角色的最长时间和用户在特定时间内激活某角色的最大次数,因而不能描述角色在激活状态下的约束;再次,TRBAC没有考虑持续时间内的约束和角色激活状态下的约束,不能支持该状态下的约束启用和禁用概念。此外,TRBAC也没有考虑基于时间的角色层次约束和职责分离约束。因此TRBAC只在角色层次进行简单约束,对授权和角色指派等过程中的细节考虑不够,降低了TRBAC使用的灵活性,不能满足现代应用程序的要求。

3 GTRBAC模型

为弥补TRBAC中的不足,Joshi等人提出了GTRBAC(General temporal role-based access control)模型,GTRBAC模型从约束、冲突及解决方法等方面对TRBAC进行了细致的补充[8]。

3.1 GTRBAC中的时态约束

GTRBAC主要考虑了持续约束、周期约束和其他特定形式的激活约束。和TRBAC中不同的是,它严格区分了角色的启用和激活概念,从而引入了角色状态的概念,在GTRBAC模型中,角色有3种状态,它们分别是启用(enabled)、禁用(disabled)和激活(active)状态。禁用状态的角色可以重新启用,而只有在启用状态下的角色才可以被用户请求激活,角色在启用和激活状态可以被管理员禁用。在GTRBAC模型中主要可以指定以下约束:角色启用、用户—角色指派和角色—权限指派的时态约束,激活约束,运行时事件,约束启用表达式和触发器。根据用户的不同需求,角色启用、分配能够精确到指定的任一时间段。

周期约束:角色在何时启用和禁用,或者用户—角色和角色—权限允许分配的时间等都主要由周期约束来指定。周期约束的一般形式为$(I,P,Pr:E)$,(I,P)对指定了事件E发生的时间段,事件E可以是enable/disable r(角色r启用/禁用)、assign_P/deassign_P p to r(角色—权限分配)和assign_U/deassign_U u to r(用户—角色分配)等。

持续约束:持续约束用于指定角色有效或分配的持续有效时间,其一般形式为$([(I,P)\mid D],D_x,P_r:E)$,其中$x$是$R$,$P$或$U$,分别表示enable/disable r、assign_P/deassign_P p to r和assign_U/deassign_U u to r,D和D_x表示持续时间,并且$D\leqslant D_x$,符号"|"表示2选1关系,[]表示里面的元素为可选项。所以持续约束可等价表示为$((I,P),D_x,Pr:E)$,$(D,D_x,Pr:E)$和$(D_x,Pr:E)$3种形式。$((I,P),D_x,Pr:E)$表示在每个(I,P)指定的时间周期内事件E是有效的并且持续时间为D_x;$(D_x,Pr:E)$表示不受周期时间的约束,只受持续时间D_x约束;$(D,D_x,Pr:E)$表示指定持续时间为D,而事件的约束为D_x。

GTEBAC还以相同的方式定义了角色激活、运行时请求、触发器和启用约束等事件的时态约束[3]。

3.2 GTRBAC约束冲突及解决办法

GTRBAC既然支持各种类型的事件,必然存在冲突。例如,如果周期约束发起的角色启用事件和触发器激起的角色禁用事件针对的是同一个角色,那么就产生了冲突。设Γ为所有事件表达式、约束和触发器组成的集合,同时假定用户的运行时请求系列为:$RQ=<RQ(0),RQ(1),\cdots,RQ(t),\cdots>$,$RQ(t)$表示时刻$t$的运行时请求的集合,并且$RQ(t)\in RQ$。给定$\Gamma$和$RQ$,GTRBAC中主要有3种类型的冲突:

1)同类事件间的冲突(类型1)。当同类事件和同一角色或指派的状态关联时会产生冲突。如事件"enabling r"使角色r从禁用切换到启用状态,而事件"disabling r"使角色r从启用切换到禁用状态。同理"assign r for u"和"deassign r for u"也属于同一类型事件。

2)不同事件间的冲突(类型2)。不同类事件间也可能产生冲突,例如,如果激活请求"activate u for r"和角色禁用事件"disable r"同时激发,那么也构成了一个冲突,因为在激发时刻,角色r处于disabled状态。

3)约束间的冲突(类型3)。是指角色启用或角色指派的约束间的冲突。例如,如果持续约束

(D_R,enable r)和(D_R,disable r)在同一周期时间内有效,它们很有可能同时发生,从而造成冲突,这种冲突称之为类型 3a 冲突。同时在"每用户激活约束"和"每角色激活约束"间也可能存在冲突,例如,考虑每角色约束(D_{Active},[D_{Default}],$\text{Active}_{\text{R\_total}}$ r)和每用户—角色约束($D_{U\text{active}}$,u,$\text{Active}_{\text{R\_total}}$ r),前一个约束表示角色 r 在 D_{Active}期间允许被激活,而后一个约束表示在 $D_{U\text{active}}$期间允许用户 u 使用角色 r。如果指定了 D_{Default},则表示所有用户允许的激活时间约束均为 D_{Default},因此就产生了含混不清的约束—用户 u 的激活约束时间究竟是 D_{Default}还是 $D_{U\text{active}}$。注意,在没有指定 D_{Default}时,$D_{\text{Default}} = D_{\text{active}}$,换句话说,任何单个用户在整个 D_{active}内均可以激活角色 r。因此"每用户—角色约束"也会和"每角色约束"产生冲突,这种类型的约束称之为类型 3b 约束。

对于存在的冲突,GTRBAC 提出了解决的办法。对于类型 1 和类型 2 冲突,GTRBAC 采用阻塞事件的思想来处理,通过定义每个事件的优先级来决定阻塞的事件。而类型 3a 的冲突根源在潜在的和时间约束关联的事件冲突,因此可以采用类型 1、类型 2 相似的方法进行处理,类型 3b 的冲突可以采用"角色优先级高于用户—角色指派优先级"和"限制多的约束优先级高"的原则进行处理[8]。

4 结束语

RBAC 模型已经非常成熟并且获得了广泛的应用[9],但时态约束的提出使其满足不了新的需求。TRBAC 从一定程度上解决了时态约束的部分问题,但仅仅考虑到了角色的时态约束问题,也没有考虑时态环境下的职责分离问题。GTRBAC 不仅从更细致的角度定义了角色启用禁用约束,而且也考虑到了角色—权限,用户—角色指派过程中的时间约束,同时分析了在约束指派过程中存在的冲突并给出了解决办法。此外 GTRBAC 也支持时态环境下的角色继承和职责分离问题。GTRBAC 是目前在时态环境下定义比较完全和细致的访问控制模型。

参考文献:

[1] ANSI. ANSI INCITS 359-2004—American National Standard for information technology—role based access control [S]. ANSI,2004.

[2] 王小明,赵宗涛. 基于角色的时态对象存取控制模型[J]. 电子学报,2005,33(9):1634-1638.

[3] 吴明华. 主动网络安全机制研究[J]. 重庆师范大学学报(自然科学版),2003,20(3):19-22.

[4] Ferraiolo D,Sandhu R,Gavrila S,et al. A proposed standard for role based access control[J]. ACM Transactions on Information and System Security,2001:224-274.

[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] Bertino,Bonatti P A,Ferrari E. TRBAC:A temporal role-based access control model[J]. ACM Trans Information and System Security,2001,4(3):191-233.

[7] 欧阳凯,董理君,周敬利. 具有条件时态特性的 RBAC 模型[J]. 华中科技大学学报(自然科学版),2008,36(4):58-61.

[8] Joshi J B D,Bertino E,Latif U,et al. Generalized temporal role-based access control model[J]. IEEE Transactions on Knowledge and Data Engineering,2005,17(1):4-23.

[9] 罗海,安世全. 网格访问控制及对 RBAC 模型扩展的研究[J]. 重庆邮电大学学报(自然科学版),2008,20(6):714-718.

A Survey of Aeneral Temporal RBAC Studying

LIU Zhi[1], *ZOU Zhi-ling*[2]

(1. College of Computer Science, Chongqing University of Technology, Chongqing 400050;
2. School of Psychology, Southwest University, Chongqing 400715, China)

Abstract: After the development of so many years, RBAC has cumulated abundant and mature theory basis and is widely used in access control in information system. In this paper, the access control thinking and principle of RBAC model are illustrated first. It consructs network security control model by abstracting five basic data objects which are user, role, object, operation and permission respectively in building the relationship among them. Then the disadvantages of RBAC in processing time-constraint access control are analysed. Secondly, we retrospect the studying status quo of temporal RBAC model and analyse the existing problem of TRBAC during authorizing in temporal system. It constraints the permission only in role level and does not consider fully the details during authorizing and role assignmeng. Finally a model named GTRBAC and its thinking are prospected. GTRBAC is a well defined access control model in temporal environment by now. It not only considers persistent constraints, circular contraints and other particular activate contraints on the basis of RBAC, but also proposes the methods solving conflicts amongs contraints.

Key words: temporal system; RBAC; temporal contraint; access control

(责任编辑 游中胜)