第 34 卷 第 6 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.6 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)06—0170—03 文献标识码：A 中图分类号：N945.12

基于带时间特性 RBAC 的使用控制模型及其管理

鲁 柯，周保群，王惠芳
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：介绍和分析了基于角色的访问控制管理模型与使用控制模型，指出使用控制核心模型存在的不足。将权利的授予与撤消分离的授权机制引入使用控制模型，提出一种带时间特性的基于角色的使用控制模型，给出了模型的描述及模型管理的实现。
关键词：使用控制；基于角色的访问控制；时间特性

Usage Control Model Based on Timed RBAC and Its Administration

LU Ke, ZHOU Bao-qun, WANG Hui-fang
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper analyzes the administrative model of RBAC and Usage Control(UCON)model, and points out the deficiency of UCON core model. Based on the results, authorization mechanism of separated rights grant and revoke is introduced into UCON model, and a role-based usage control model with time character is presented. The description of the model and its implementation administration are presented.
【Key words】 Usage Control(UCON); Role-based Access Control (RBAC); time character

使用控制(Usage CONtrol, UCON)是 2002 年出现的一种新的访问控制技术，它包含了传统访问控制、信任管理和数字权益管理(Digital Rights Management, DRM)3 个问题域，并且在定义和范围上超过了它们，被认为是下一代访问控制技术的发展方向。但由于使用控制的提出是为了给现代访问控制技术的研究构造一个统一的框架，使系统全面地描述现代访问控制的需求和特性，因此模型的定义高度抽象，不仅给模型的应用和实现带来了不小的难度，而且给出一个统一的模型管理方案也十分困难。基于角色的访问控制(Role-based Access Control, RBAC)具有策略中立和管理简单等优点，并且有自己完整且系统的管理模型，在现实生活中已经得到了广泛的应用。

1 RBAC 管理模型

RBAC 模型如图 1 所示。

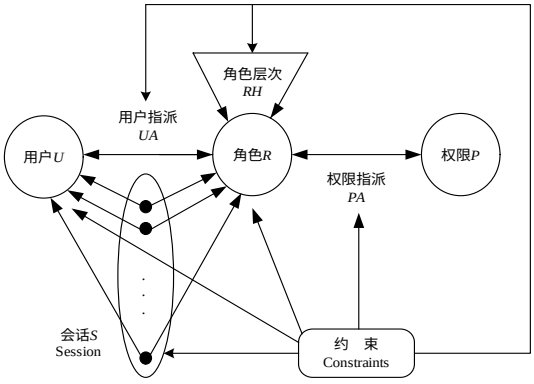

图 1 RBAC 模型

模型中的主要元素定义如下：

(1) U , R , S , P 分别是用户、角色、会话和权限的集合；

(2) $UA \subseteq U \times R$ 是用户到角色的多到多指派关系；

(3) $PA \subseteq P \times R$ 是权限到角色的多到多指派关系；

(4) $RH \subseteq R \times R$ 是角色层次结构；

(5)约束给出了用户、角色和权限定义的限制。

在一个拥有众多角色、用户和权限的大型系统中，只依靠为数不多的管理人员来实现对角色、用户、权限以及它们间相互关系的管理是十分困难的。利用 RBAC 本身更利于实现 RBAC 的管理，ARBAC(Administration of RBAC)模型就是一种基于角色的用于实现 RBAC 管理的模型。

ARBAC模型包含用户角色指派(User Role Assignment, URA)模型、权限角色指派(Permission-role Assignment, PRA)模型和角色继承指派(Role-role Assignment, RRA)模型 3 个子模型，分别从用户角色指派、权限角色指派、角色继承指派 3 个方面实现对RBAC的管理[1]。

2 使用控制模型

UCON的核心模型称为ABC(Authorizations, Obligations, Conditions)模型[2]。如图 2 所示，它由 8 个核心部分组成：

(1)主体(Subjects, S)是控制并能够对客体执行一定权利的具有属性的实体。

(2)主体属性(Subject Attributes, ATT(S))是主体能够用于授权过程中的使用决定的属性，如标记、用户组、角色、成员关系等。主体属性是易变的，在主体访问客体的过程中可能会被系统改变。

(3)客体(Objects, O)是可以提供给主体进行使用的实体。

(4)客体属性(Object Attributes, ATT(O))是客体能够用于授权过程中的使用决定的属性，它可能是客体本身的属性，如安全标记和所有关系，也可能是与权利相关的属性，如客体、访问权利。

(5)权利(Rights, R)是主体能够对客体进行控制和执行的

基金项目：国家部委基金资助项目
作者简介：鲁 柯(1983－)，男，硕士研究生，主研方向：信息安全；周保群，教授；王惠芳，副研究员、博士
收稿日期：2007-05-20 **E-mail：**luke1983212@gmail.com

特权，由主体可以对客体进行的操作许可(Permissions)集组成。

(6)授权(Authorizations, A)：授权是指允许主体使用客体特定权利的规则的集合。传统的访问控制模型都是授权的一种表现形式。授权的形式既可以是使用前授权(preA)，也可以是使用中授权(onA)。

(7)职责(Obligations, B)是指主体获得或行使对客体的访问权利前必须完成的操作。职责可以分为使用前职责(preB)和使用中职责(onB)。

(8)条件(Conditions, C)是指主体获得或行使对客体的访问权利前必须满足的系统或执行环境的强制约束条件。与授权和职责不同，条件不是以主/客体属性或主体请求的权利为依据，而是根据与主体和客体无关的系统状态或执行环境的属性来决定允许或拒绝主体对客体的访问，因此，条件的判定不会改变主体或客体的属性。条件也分为 2 种形式：使用前条件(preC)和使用中条件(onC)。

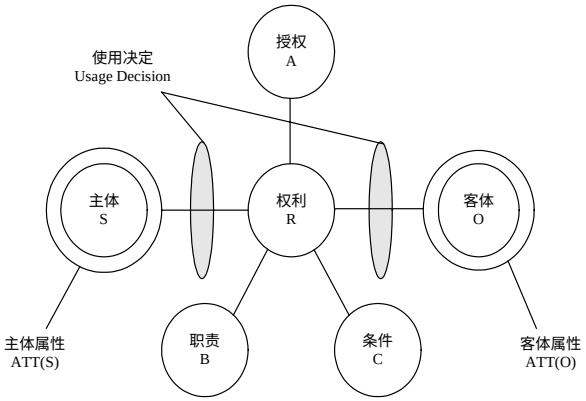

图 2　ABC 模型

其中，主体、客体、权利来自传统的访问控制模型，是比较熟悉的概念。授权、职责和条件是决定主体是否能以特定权力访问一个客体的使用决定因素。与 ABC 模型相比，传统的访问控制模型仅仅使用授权来决定访问请求的处理。职责和条件是访问控制领域的新概念，是对传统访问控制模型基于属性的访问控制策略的补充和丰富。

使用控制ABC模型的 2 个重要特点是使用决定的连续性和属性的易变性[3]。

在 ABC 模型中，权利的赋予和撤消是一体的。这种授权方式的优点是安全性高、动态性好，但缺点是难于实现和应用。因为 ABC 模型想要给出对传统访问控制、信任管理和 DRM 的统一描述，模型的定义高度抽象，所以给出统一的模型管理方案难度比较大。目前也少有文献涉及对模型中主体、客体和权利等的管理。

3　带时间特性的基于角色的使用控制模型

在使用控制模型中，管理员要管理的对象包括主体、客体、权利和授权，这与RBAC模型相同。将RBAC模型中的管理方案用在使用控制模型中，能够解决其对主体、客体和权利的管理问题[4]。在使用控制模型中，没有角色的概念，但角色可以是主、客体的属性，因此，可以沿用角色的概念实现RBAC模型与ABC模型的结合。本文根据权利的授予和撤消分离的思想，将带时间特性的RBAC与ABC模型相结合，提出了一种带时间特性的基于角色的使用控制模型，如图 3 所示。

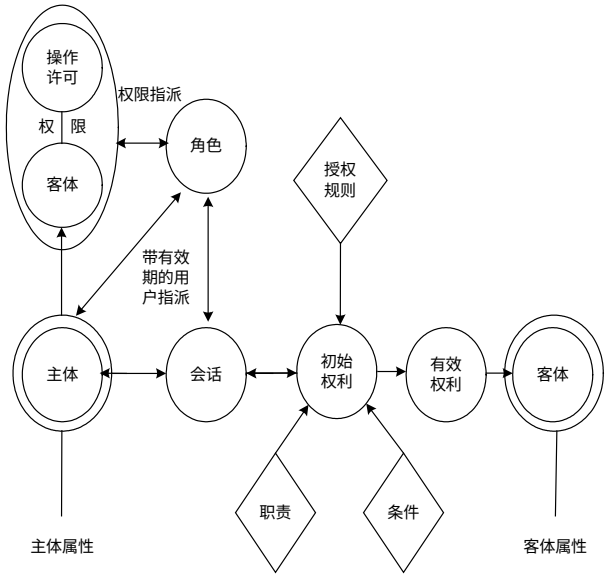

图 3　带时间特性的基于角色的使用控制模型

模型由 10 个核心元素和 5 个授权函数组成。10 个核心元素分别是主体、主体属性、客体、客体属性、角色、权限、会话、操作许可、初始权利和有效权利；5 个授权函数分别是带有效期的用户指派、权限指派、授权规则、职责和条件，其中，前两者是权利的赋予函数，赋予主体带生命周期的初始权利，后三者是权利的撤消函数，终止或撤消主体不合法的权利。主体、主体属性、客体、客体属性和角色、权限、会话、操作许可、权限指派的定义与 ABC 模型和 RBAC 模型相同。授权规则、职责和条件与 ABC 模型中的授权、义务和条件的定义相近，不同的是前三者只能够撤消主体的部分或全部使用权利，而不能够赋予主体任何使用权利，后三者既可以赋予主体特定的使用权利，又可以撤消主体的部分或全部使用权利。带有效期的用户指派、初始权利、有效权利概念的定义如下：

(1)带有效期的用户指派(Timed User Assignment, TUA)

系统为主体指派角色的同时要指定本次指派的有效期，即

$TUA \subseteq U \times R \times TR$

时间区间集合为

$TR \subseteq T \times T$, $(t_i, t_j) \in TR \Leftrightarrow t_i < t_j$

其中， TR 是 2 个时间点所构成的区间的集合。在有效期内，该次用户指派是有效的，主体可以在会话中激活角色从而获得角色关联的权限集，否则主体无法在任何会话中激活该角色。将时间特性引入RBAC中，从时间维上对RBAC进行扩展，使RBAC拥有更全面、具体的访问控制能力[5]。

(2)初始权利(Original Right, OR)

一次会话中主体通过被赋予角色获得的权限的集合。主体在一次会话中激活的角色不同，本次会话中主体的初始权利也不同，初始权利的赋予是一个动态的权利赋予过程。另外，由于主体与被赋予的角色之间的关联(通过 TUA 定义)具有一定有效期，因此主体的初始权利也存在一定的有效期。

(3)有效权利(Effective Right, ER)

初始权利是在使用过程中经过授权规则、职责和条件等使用约束因素的检查和撤消后剩余权限的集合。可以看出，有效权利不但与初始权利有关，还与授权规则、职责和条件 3 大使用约束因素有关，拥有相同初始权利的主体在不同的

应用环境下可能得到不同的有效权利。

4 模型的管理

图 3 的模型具备了 ARBAC 模型中的管理机制，可以从用户角色指派 URA、权限角色指派 PRA、角色继承指派 RRA 3 个方面实现对模型的管理。

(1)基于扩展 URA 的用户指派管理

模型中用户角色指派是与一个特定的有效期关联在一起的，即带有效期的用户角色指派，而用户角色指派模型 URA 中却没有时间的概念，因此，只有将 URA 模型在时间维上扩展，才能完成模型中用户的管理。这里用带有效期的用户角色指派函数和吊销函数代替 URA 模型中的用户角色指派函数和吊销函数。

1)带有效期的用户角色指派函数：

$$timed\_can\_assign \subseteq AR \times CR \times 2^{R} \times TR_{\text{URA}}$$

其中，$timed\_can\_assign(x,y,\{a,b,c\},tr)$ 的含义是管理角色 x (或比管理角色 x 更高级的角色)的用户可以指派成员关系满足先决条件 y 的用户成为角色 (a,b,c) 中的一员，并且 tr' 满足 $tr' \subseteq tr$ ； AR 是管理员角色集； CR 是对指定的角色集 R ，管理员为某成员用户指定角色时该成员用户要满足的先决条件； TR_{URA} 是本次用户角色指派的生命周期。

2)带有效期的用户角色吊销函数：

$$timed\_can\_revoke \subseteq AR \times 2^{R} \times TR_{\text{URA}}$$

其中，$timed\_can\_revoke(x,r,tr)$ 的含义是管理角色(或比管理角色高级的角色)x 的用户可以撤消用户的角色 $r \in R$ ，当且仅当满足条件： $tr' \subseteq tr$ 。

这样，通过扩展后的 URA 就能管理带生命周期的用户指派了。

(2)基于 PRA 的权限指派管理

在权限角色指派模型 PRA 中定义了一个 $can\_assignp$ 函数，用于确定不同层次管理员能够管理的权限角色指派的范围，具体来说，就是确定每个管理员对应于每个角色是否能够进行权限指派：

$$can\_assignp \subseteq AR \times CR \times 2^{R}$$

由于管理员之间也存在一个层次关系，实际的指派模型给每个管理员指定了一个管理范围，可以用一个区间来表示。高级管理员角色的管理区间包含下级角色的管理区间，从而形成了一个有层次的、职责分明的管理层次。区间的定义如下：

1) $[x,y] = \{r \in R \mid x \geq r \wedge r \geq y\}$ ；

2) $[x,y) = \{r \in R \mid x \geq r \wedge r > y\}$ ；

3) $(x,y] = \{r \in R \mid x > r \wedge r \geq y\}$ ；

4) $(x,y) = \{r \in R \mid x > r \wedge r > y\}$ 。

对应于吊销模型，每个管理员也有一个吊销的角色区间，他可以在该区间中吊销任何角色的对应权限。根据管理员层次，同样有一个吊销的继承关系保证管理的不越级操作。由于一个角色对应的权限可以通过角色继承关系得到，因此在吊销模型中又可以分为强吊销(strong revoke)和弱吊销(weak revoke)。如果一个吊销操作是弱吊销，当该权限是通过继承关系成为该角色的关联权限时，吊销操作将不起作用；如果是强吊销，那么将强行剥夺该角色继承的所有权限：

$$can\_revokep \subseteq AR \times 2^{R}$$

(3)基于 RRA 的角色继承管理

角色继承指派模型 RRA 中，定义了 3 种角色：能力(*Abilities*)角色，组(*Groups*)角色，*UP-Roles* 角色。能力角色的职能是把一些相关的权限结合在一起，使管理员可以将这些权限作为一个单一的权限单元(即能力)来处理，那么分配能力给角色相当于分配若干个权限给角色。组角色与能力角色相类似，不同的是组角色针对的是用户而不是权限。一个用户组就是分配给角色的一个用户的集合单元。用户组也可以形成层次关系。UP-Role 角色是对成员资格没有任何限制的角色，代表一般用户和权限的角色。其中一些定义如下：

1)能力角色的指派管理：

$$can\_assigna \subseteq AR \times CR \times 2^{A}$$

2)能力角色的吊销管理：

$$can\_revokea \subseteq AR \times 2^{A}$$

3)组角色的指派管理：

$$can\_assigng \subseteq AR \times CR \times 2^{G}$$

4)组角色的吊销管理：

$$can\_revokeg \subseteq AR \times 2^{R}$$

5)UP-Role 角色与能力角色的关系：

$$Abilities \in UP-Roles \Leftarrow UP-Roles \geq Abilities$$

6)UP-Role 角色与组角色的关系：

$$Groups \in UP-Roles \Leftarrow Groups \geq Up-Roles$$

RRA 模型中还定义了一个 *can_modify* 方法，用于刻画每个管理员是否可以添加、删除角色以及改变角色间的继承关系；并定义了多种角色区间的概念，通过形式化的证明保证这些区间能够安全地实现角色模型的分布式管理，具体证明可以参见文献[1]。

5 结束语

使用控制作为下一代访问控制技术的发展方向，具有涵盖的问题域广、权利的授予与撤销动态性强、安全性更高等优点，但存在着模型的实现、管理困难等不足。RBAC 无论在理论上还是在应用上都已经相当成熟，而且有完善的、系统的管理模型 ARBAC。带时间特性的 RBAC 从时间域上对 RBAC 进行了扩展，使 RBAC 系统有了更全面、又具体的访问控制能力。将带时间特性的 RBAC 应用到 UCON 核心模型 ABC 模型中，既完善了 ABC 模型，又便于实现使用控制模型的管理。

参考文献

[1] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-based Administration of Roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135.

[2] Park J, Sandhu R. The UCON_{ABC} Usage Control Model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128-174.

[3] Zhang Xinwen, Francesco P P, Sandhu R, et al. Formal Model and Policy Specification of Usage Control[J]. ACM Transactions on Information and System Security, 2005, 8(4): 351-387.

[4] 李沛武. 用基于角色访问控制实现使用控制模型的管理[J]. 南昌工程学院学报, 2005, 24(1): 47-50.

[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.