

# 基于时间约束的角色访问控制模型研究

李秋敬, 刘广亮, 谢圣献, 张沙沙, 段海霞, 许宏伟

(聊城大学 计算机学院, 山东 聊城 252059)

**摘要:** 基于角色的访问控制模型的研究工作近年来得到了广泛的重视, 但主要工作均立足于与时间特性无关的其他方面, 在现实生活中有很多与时间有关的访问控制不能够得到很好解决, 特别是一些要求时间性很高或者周期性规律很强的访问控制, 都需要进行时间约束的控制。为此形式化描述了一个引入时间后的角色访问控制, 采用周期时间约束的方法描述了时间约束和时间约束模型, 并构建了一个关于时间约束的角色访问控制系统, 解决了一系列与时间有关的角色访问控制问题, 增强了访问控制的力度。

**关键词:** 访问控制; 时间约束; RBAC; 角色

**中图分类号:** TP309.2

**文献标识码:** A

**文章编号:** 1673-629X(2009)08-0162-04

## Temporal Role - Based Access Control Model

LI Qiu-jing, LIU Gang-liang, XIE Sheng-xian, ZHANG Sha-sha, DUAN Hai-xia, XU Hong-wei

(College of Computer Science, Liaocheng University, Liaocheng 252059, China)

**Abstract:** The research work of RBAC is greatly emphasized in recent years. However, the main work focuses on some characters which have nothing to do with the time character. In the real life many access control with the time related cannot obtain very good solution, especially some request very high timeliness or the very strong rule periodic access control. The article describes the RBAC with time character, the temporal authorization and the temporal role - based access control model are presented by cycle restraint. And constructed one role access control system about the time restraint, solved a series problem of time and the role of the access control, enhanced the efforts of access control.

**Key words:** access control; temporal constraints; RBAC; role

## 0 引言

访问控制技术是信息安全的重要保障措施之一, 近几十年来, 访问控制技术有了重大发展, 特别是 Ravis. Sandhu 等人提出的基于角色的访问控制 (RBAC)<sup>[1]</sup>, 将角色的概念引入访问控制, 大大简化了授权管理的方法, 也大大提高了管理的效率。它支持最小特权、责任分离以及数据抽象三个基本的安全原则。虽然 RBAC 有诸多优点, 对其研究也已经相当广泛和深入, 但仍有一些应用是现有 RBAC 模型所不能描述的, 如某些应用中需要时间约束来限制资源的使用, 或用时间约束来控制时间敏感的活动或行为。文中在 RBAC 模型的基础上, 引入了时间约束, 形成了具有时间约束的角色访问控制, 并具体介绍了时间约

束以及时间约束在 RBAC 中的应用, 在周期性的时间变化下, 通过时间的变化和角色的变化的关系来确定角色的访问权限, 从而使角色在不同的时间具有不同的访问权限, 解决了访问控制中对时间的需求问题, 提高了系统的安全性和灵活性。

## 1 TRBAC 模型的基本思想及其形式化描述

目前在文献[2]中介绍的 RBAC 系统中引入时间约束的主要有两种: 其一是对 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。针对这些时间约束, 对会话和全局系统状态空间进行扩展, 以实现解决计算时间约束变化算法。其二是通过引入日历的概念来定义周期时间表达式, 通过周期的时间检测使角色处于许可和非许可状态<sup>[3]</sup>。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, 例如, 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。而第二种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。文中依据时间约束的第二种方

收稿日期: 2008-12-08; 修回日期: 2009-03-19

基金项目: 山东省教育科研发展计划(J08LJ20)

作者简介: 李秋敬(1983-), 女, 硕士研究生, 研究方向为计算机网络与信息安全; 刘广亮, 副教授, 研究方向为信息安全与密码学; 谢圣献, 教授, 研究方向为网络与信息安全。

法来介绍在 RBAC 中引入时间约束的优点。

### 1.1 TRBAC 的基本思想

时间约束模型(TRBAC, Temporal Role-based Access Control Model)<sup>[3]</sup>的基本思想是在 RBAC 模型基础上通过周期的时态检测使角色处于许可和非许可状态。通过角色触发器来实现角色许可与非许可之间的转化,使角色触发器可以执行的约束条件就是角色触发事件,角色触发产生后也可以在有明确的说明时间内进行延迟,许可与非许可活动状态通过优先级的赋予来决定,这样也可以解决许可与非许可活动状态的冲突。

文中对 RBAC 做时间维上的扩展,首先通过定义一个周期时间来表达现实世界中的连续时间列,并在此基础上对时间约束提出了形式化的定义,针对这些时间约束,对用户、角色、权限和会话也做了相应扩展。在用户、权限、角色之间存在着多对多的映射,这就存在着时间约束对其之间的相互影响,例如用户激活时间的集合  $User \cdot \tau$ , 权限有效的时间集合  $Perm \cdot t$ , 角色激活时间集合  $Role \cdot t$  等,在 TRBAC 模型中,要求用户激活时间的集合与角色激活时间集合不能同时存在,权限有效的时间集合与角色激活时间集合也不能同时存在,因为每个用户激活角色时间长度约束与每个角色激活时间长度约束之间存在冲突,如角色  $r$  可被激活的时间约束为  $Da$ , 用户激活角色  $r$  的时间长度约束为  $Dua$ 。若  $Dua > Da$ , 则产生冲突。这就要求对时间约束冲突有了一定程度的定义,没有用户能被赋予两个冲突的角色,即同一个冲突组中的角色不能拥有同一个用户;同样,没有同一个权限能被赋予两个冲突的用户,即同一个冲突组中的用户不能拥有同一个权限。这就解决了一系列的冲突问题。对会话也作了相应的扩展,用相应的函数来表示会话,从而对 RBAC 作了良好的时间扩展。

### 1.2 TRBAC 模型的形式化描述

TRBAC 模型的形式化描述如下:

TRBAC 是在 Core RBAC 的基础上定义的,其中 Core RBAC 是构成一个 TRBAC 控制系统的最小的元素集合,它包含了 Core RBAC 内的所有元素<sup>[4]</sup>。

定义 1:  $Users = \{u_1, u_2, \dots, u_m\}$  所有用户的集合,  $Roles = \{r_1, r_2, \dots, r_n\}$  所有角色的集合,  $Ops = \{op_1, op_2, \dots, op_k\}$  所有操作的集合,  $Objects = \{ob_1, ob_2, \dots, ob_l\}$  所有访问对象的集合,  $Perms = 2^{Ops \times Objects}$  所有权限的集合,  $Sessions = \{s_1, s_2, \dots, s_p\}$  所有会话的集合。

在 TRBAC 中的定义扩展:

时间区间定义:周期的开始时间表示为  $t_i$ , 结束时间表示为  $t_j$ , 则

$TR = \{(t_i, t_j) \mid i < j\}$ , 时间区间由两个时间点构成。

$TRS = 2^{TR}$  表示由时间区间构成的集合。

可以定义:  $\Delta t = t_j - t_i$ , 表示持续的时间表示。

用户  $User = \{UserID, t\}$ ,  $UserID$  为用户唯一标识,  $\tau$  是用户活动的时间集合, 用户集  $Users = \{User_1, User_2, \dots, User_n\}$ , 用  $User \cdot \tau$  表示用户  $User$  的激活时间集合。

访问对象  $ob = \{obID, t\}$ ,  $obID$  为访问对象唯一标识,  $\tau$  是访问对象有效的时间集合, 用  $ob \cdot t$  表示用户  $ob$  的有效时间集合,  $Objects = \{ob_1, ob_2, \dots, ob_l\}$  所有访问对象的集合,  $Ops = \{op_1, op_2, \dots, op_k\}$  所有操作 (Operation) 的集合。

权限  $Perm = \{PermID, t\}$ ,  $PermID$  是权限  $Perm$  的唯一标识,  $\tau$  是权限有效的时间集合,  $Perm \in Ops \times Objects$ ,  $Perm \cdot \tau \subseteq ob \cdot \tau$ , 权限集  $Perms = \{Perm_1, Perm_2, \dots, Perm_n\}$ 。

角色  $Role = \{RoleID, t\}$ ,  $Role = \{Perm_1, Perm_2, \dots, Perm_k\} \subseteq Perms$ ,  $RoleID$  为访问对象唯一标识,  $Role \cdot \tau = Perm_1 \cdot \tau \cup Perm_2 \cdot \tau \cup \dots \cup Perm_k \cdot \tau$ 。

用户角色赋值关系:  $UA \subseteq Users \times Roles$ ,  $(User, Role) \in UA$  表示用户  $User$  被赋予角色  $Role$ , 并且  $User \cdot \tau \cap Role \cdot \tau \neq \emptyset$ 。

角色权限赋值关系:  $PA \subseteq Perms \times Roles$ ,  $(Perm, Role) \in PA$  表示角色  $Role$  被赋予权限  $Perm$ , 并且  $Perm \cdot \tau \cap Role \cdot \tau \neq \emptyset$ 。

不确定函数<sup>[5]</sup>OE 与 AO:

OneElement:  $OE(X) = x_i, x_i \in X$ ,

AllOther:  $AO(X) = X - \{OE(X)\}$

引入的 3 个集合:

$CR^* = \{cr_1, cr_2, \dots, cr_s\}, cr_i \subseteq R$  冲突角色组集合。

$CP = \{cp_1, cp_2, \dots, cp_t\}, cp_i \subseteq P$  冲突权限组集合。

$CU = \{cu_1, cu_2, \dots, cu_u\}, cu_i \subseteq U$  冲突用户组集合。

合。

约束冲突要求:

\* 没有用户能被赋予两个冲突的角色, 即同一个冲突组中的角色不能拥有同一个用户。一阶谓词描述:  $\forall u \in Users, \forall cr \in CR: |assigned\_roles(u) \cap cr| \leq 1$ 。

\* 没有同一个角色能被赋予两个冲突的用户, 即同一个冲突组中的用户不能拥有同一个角色。

一阶谓词描述:  $\forall r \in Roles, \forall cu \in CU: |assigned\_user(r) \cap cu| \leq 1$ 。

\* 没有同一个权限能被赋予两个冲突的用户, 即同一个冲突组中的用户不能拥有同一个权限。

一阶谓词描述:  $\forall p \in \text{Perms}, \forall cp \in \text{CP}: |\text{assigned\_perms}(u) \cap cp| \leq 1$ 。

在 TRBAC 中,用户可根据需要自行定义一阶谓词定义。

会话<sup>[6]</sup>session 由以下七元组来描述  $(u, r, ua, pa, rat, sst, tc)$ 。其中:  $u$  是用户;  $r$  是角色;  $ua$  是用户角色的映射关系;  $pa$  是角色权限的映射关系;  $rat$  是角色激活的时刻,当计算时间约束的激活长度时,将从  $rat$  中查找信息;  $sst$  表示会话建立的时间;  $tc$  表示与该会话相关联的用户和角色的时间约束。

函数扩展:  $\text{Currenttime}: \Phi \rightarrow \text{TE}$ : 是一个全局原子函数,返回当前时间。

$\text{Active\_length}: \text{Session} \rightarrow \text{TE}$ : 记录会话的激活时间。

$\text{start}: \text{TR} \rightarrow \text{TE}: \text{start}((t_i, t_j)) = t_i$ ,

$\text{end}: \text{TR} \rightarrow \text{TE}: \text{end}((t_i, t_j)) = t_j$ 。

## 2 引入时间约束的 RBAC

### 2.1 时间约束的角色访问控制系统

下面描述基于时间约束的角色访问控制系统结构图<sup>[7]</sup>,该系统结构图如图 1 所示。

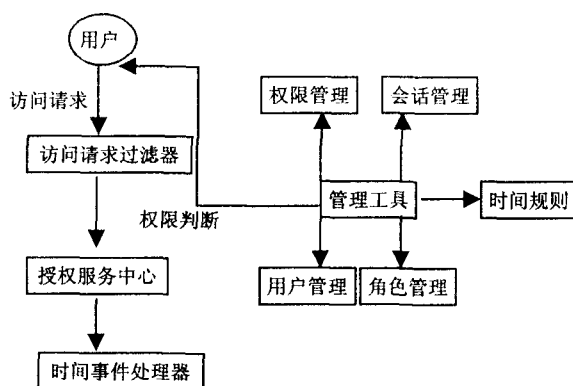


图 1 时间约束的角色访问控制系统图

如图 1 所示,访问控制系统主要包括访问请求过滤器、授权服务中心、管理工具、时间事件处理器四部分,系统中各部分的实现如下:

●访问请求过滤器的主要功能是截获用户发出的访问请求,从中验证出有用的用户信息,并将决策结果返回给用户。

●授权服务中心的主要功能是用来判断用户是否有权限访问所请求资源。它是系统的核心部分,用于决定用户是否可以访问,是否与其它用户存在冲突。

●管理工具是访问控制系统的管理模块,包括了用户管理、角色管理、权限管理、会话管理以及时间规则管理。管理员通过会话管理控制台可以查看用户的会话及用户激活的角色。

●时间事件处理器对时间进行监测,能够使角色的许可和禁止状态随时间变化而相互转化,负责触发各种约束条件,与授权服务中心配合完成时间约束的访问控制。同时时间事件处理器也满足了系统中存在的与时间相关的事件需要自动被触发执行的需要。

### 2.2 时间约束的优点和特点

时间约束可以分为两类,一种是静态的时间约束,一种是动态的时间约束。在 RBAC 中引入时间约束,通过角色触发事件来启动角色触发装置,从而使角色处于许可状态或者处于非许可状态,这就要求时间约束必须采用动态的,通过时间的周期性变化,在时间控制下来确定用户角色执行的先后,因而解决了与时间有关活动的访问控制问题,增强了访问控制的力度,因而引入时间约束后的系统提供了更具体、更全面的安全描述能力。

访问控制系统中时间约束的描述:

因为角色状态因时间变化而变化,因此引入时间约束后首先引起了角色状态的变化。角色有三种状态:禁止态(disabled)、许可态(enabled)和激活态(active)。处于禁止态的角色不允许被任何用户激活;处于许可态的角色可以被用户激活;用户由激活态也可经由冻结状态转变为许可态;角色若处于激活态则自身可以进行转化。

角色状态转换关系如图 2 所示<sup>[8]</sup>。

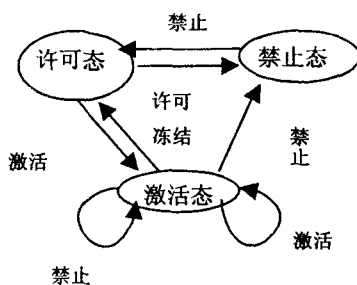


图 2 角色状态转换关系图

引入时间约束后角色冲突的解决:

冲突主要分为三类:

●同类事件之间的冲突,如角色许可(enable  $r$ )与角色禁止(disable  $r$ )之间;

●不同类事件之间的冲突,如角色激活(activate  $r$  for  $u$ )与角色禁止(disable  $r$ )之间;

●约束之间的冲突。

以约束之间的冲突为例,没有用户能被赋予两个冲突的角色,即同一个冲突组中的角色不能拥有同一个用户。在其中设置用户集合与角色集合,让这两个集合不处于同一个激活时间内,来解决它们之间的冲突。

### 3 结束语

描述了引入时间约束的角色访问控制,更好地满足了访问控制最小权限的原则,可以有效地解决时间敏感活动的访问控制问题,增强了访问控制的力度。引入时间后的系统有着更全面、更具体的安全属性描述能力。但是仍然存在许多值得研究的问题,关于时间约束在角色访问控制中的实际应用应进一步进行研究,文中在时间约束的角色访问控制中的整体方面还有待进一步完善。

#### 参考文献:

- [1] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38 - 47.
- [2] 张新华, 陈军冰. 时间约束的 RBAC 模型及应用[J]. 计算

(上接第 158 页)

#### 参考文献:

- [1] Sahami M, Dumais S, Heckerman D, et al. A Bayesian Approach to Filtering Junk E-Mail. In Learning for Text Categorization[C] // 1998 Workshop. Madison, Wisconsin: [s. n.], 1998.
- [2] Duda R O, Hart P E, Stork D G. Pattern Classification 2nd [M]. [s. l.]: Wiley, 2002.
- [3] 杨斌, 路游. 基于统计学习理论的支持向量机的分类方法[J]. 计算机技术与发展, 2006, 16(11): 56 - 58.
- [4] 张丽, 黄东. 基于 Winnow 算法的反垃圾邮件引擎的设计与实现[J]. 计算机技术与发展, 2006, 16(4): 170 - 175.

(上接第 161 页)

需要综合其他多渠道的信息并抽象其特征。另外可以通过对 Snort 规则库的分析,按照协议包头、协议类型、端口等划分、归纳出更多的网络异常特征,然后可以选择适当的串匹配算法,或者特征匹配算法来快速达到定位。

### 3 结束语

特征检测与异常检测是不能分割开来的,如何能更加有效地通过异常检测的手段来发现问题,结合特征检测的方式来提取异常特征,从而更加快速、准确地查找出异常网络的根源,是我们最终要实现的目标。文中主要是将两种检测手段的优势提取出来,并且把各自的特点相结合,在面对更加复杂的网络异常问题时,可以灵活地作出选择与判断,从而为应用各种模型来实现入侵检测作了比较充足的工作。

机技术与发展, 2007, 17(6): 246 - 249.

- [3] Bertino E, Bonatti P, Ferrar E. TRBAC: A temporal Role-based Access Control Model[J]. ACM Transactions on Information and Systems Security, 2001, 4(3): 191 - 233.
- [4] Ferraiolo D F, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 234 - 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 - 1949.
- [6] 胡程瑜, 李大兴. 带时间约束和角色控制的工作流系统授权模型[J]. 山东大学学报, 2006, 36(3): 39 - 43.
- [7] 杨珍, 刘连忠. 时间约束的角色访问控制系统的设计与实现[J]. 计算机应用研究, 2008, 25(1): 195 - 199.
- [8] 张少敏, 王宝义, 周利华. 一种具有时间约束的基于角色的授权管理模型[J]. 武汉大学学报, 2006, 52(5): 578 - 581.

- [5] 成宝国, 冯宏伟. 一个基于 Naive Bayesian 垃圾邮件过滤器的改进[J]. 计算机技术与发展, 2006, 16(2): 98 - 99.
- [6] 戴劲松, 白英彩. 基于贝叶斯理论的垃圾邮件过滤技术[J]. 计算机应用与软件, 2006(1): 110 - 111.
- [7] 汤伟, 程家兴, 纪霞. 一种基于概率推理的邮件过滤系统的设计[J]. 计算机技术与发展, 2008, 18(8): 76 - 79.
- [8] 龚伟, 李柳柏. 基于 IDSS 的中文垃圾邮件过滤模型设计[J]. 计算机技术与发展, 2007, 17(3): 163 - 165.
- [9] Linguistic Data Consortium(LDC)[EB/OL]. 2007. <http://www.ldc.upenn.edu>.
- [10] Oxford Text Archive(OTA)[EB/OL]. 2007. <http://ota.ahds.ac.uk/>.

#### 参考文献:

- [1] 肖海军, 王小非, 洪帆, 等. 基于特征选择和支持向量机的异常检测[J]. 华中科技大学学报, 2008, 36(3): 99 - 102.
- [2] David F, 王建新, 王斌. 基于异常和特征的人侵检测系统模型[J]. 计算技术与自动化, 2004, 23(3): 19 - 22.
- [3] Sielken R S. Application Intrusion Detection[R]. Virginia: University of Virginia, 1999.
- [4] 王平辉, 郑庆华, 牛国林, 等. 基于流量统计特征的端口扫描检测算法[J]. 通信学报, 2007, 28(12): 14 - 18.
- [5] 曹苏来. 典型攻击行为描述及特征向量提取[J]. 科技信息, 2008(2): 37 - 39.
- [6] 李韦韦, 陈海, 徐振朋. 基于多层特征匹配的网络入侵检测系统[J]. 计算机应用与软件, 2008, 25(2): 278 - 280.
- [7] Guimaraes M, Murray M. Overview of intrusion detection and intrusion prevention[C] // Proceedings of the 5th annual conference on Information security curriculum development. [s. l.]: [s. n.], 2008.