

时间约束的 RBAC 模型及应用

张新华¹, 陈军冰²

(1. 河海大学 信息中心, 江苏 南京 210098;

2. 河海大学 科学研究院, 江苏 南京 210098)

摘要:基于角色的访问控制模(RBAC)自提出以来一直被视为用来进行访问控制的普遍方法。时间约束的 RBAC 模型是 RBAC 模型在时间约束上的扩充。描述了时间约束和时间约束模型,重点研究了时间约束模型的系统结构。分析了校园网计费系统的应用需求,设计并实现了基于时间约束机制模型 TRBAC 的访问控制实例。

关键词:时间约束;RBAC 模型;TRBAC 模型

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2007)06-0246-04

Time - Constraint RBAC Model and Its Application

ZHANG Xin-hua¹, CHEN Jun-bing²

(1. Information Center of Hohai University, Nanjing 210098, China;

2. Research Academy of Hohai University, Nanjing 210098, China)

Abstract: Role - based access control (RBAC) model is receiving increasing attention as a generalized approach to access control. Time - constraint RBAC model is an extension on time constraint of the RBAC model. In this paper, the temporal authorization and the temporal role - based access control model are presented. Then the system architecture of temporal role - based access control model emphatically researched. At last, through analysis of the need of campus network charge system, an application instance with TRBAC is designed and implemented.

Key words: time constraint; role - based access control; TRBAC

0 引言

RBAC^[1,2]模型自 1992 年提出以来,经过多次的修订完善,已经成为一个标准。RBAC 模型中,授权约束(Authorization Constraint,也可简称为 Constraint,即约束)规定了访问许可被赋予角色时,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。约束主要有关系约束、前提约束、数值约束、授权约束、势约束和时间约束等。时间约束^[3,4]是时间变化和角色许可的依赖关系的规则表示。TRBAC^[5]模型正是在 RBAC 模型基础上的基于周期时间约束的扩充,该模型的特点在于它适合针对具有周期特性或与时间密切关联的规律性的活动中采用该模型思想进行授权约束设计,从而使角色授权的安全性在一定的时间周期内得以提高。

1 时间约束

目前在 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^[6]。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^[5]。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。

周期时间约束可以用符号表示为 $< [起始时间, 结束时间], P >$, P 是周期表示,表示一个明确的周期, $[起始时间, 结束时间]$ 表示这个周期的起止。该描述来源于日历概念(以下用 C 表示),日历定义为一个相邻时间区间的可数整数集合^[5]。

定义 1 (周期表示) 给定日历 $C_d, C_1, C_2, \dots, C_n$,

收稿日期:2006-09-04

作者简介:张新华(1972-),男,湖南祁东人,工程师,博士研究生,研究方向为计算机网络应用、信息系统集成与开发;陈军冰,博士研究生,副研究员,研究方向为软件工程、网络安全、科研过程管理等。

周期 P 定义为 $P = \sum_{i=1}^n O_i \cdot C_i \triangleright r \cdot C_d$, 这里 $O_1 = \text{all}$, $O_i \in 2^{\text{IN}} \cup \{\text{all}\}$, $C_i \subseteq C_{i-1}$ for $i = 2, \dots, n$, $C_d \subseteq C_n$, 且 $r \in \text{IN}$ 。其中 all 表示 C_i 的所有时间区间, $O_i \in 2^{\text{IN}} \cup \{\text{all}\}$ 是 C_i 的时间区间子集, $C_i \subseteq C_{i-1}$ $i = 2, \dots, n$, $C_d \subseteq C_n$ 是时间区间的长度单位, IN 是自然数集合, r 为时间区间长度。符号 \triangleright 表示将第一部分的周期表示分离出来, 即从它所代表的时间区间的开始点到结束点, 持续的日历长度 C_d 的数量。例如, $\text{all} \cdot \text{year} + \{2, 8\} \cdot \text{months} \triangleright 2 \cdot \text{months}$ 代表所有每年的 2 月、8 月, 即每年的这 2 个月。

2 时间约束模型

2.1 模型简介

时间约束模型 (TRBAC, Temporal Role-based Access Control Model)^[5] 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。这种角色许可、非许可之间的转化是通过角色触发器来控制的。角色触发事件一旦产生则角色触发器可以立即执行, 也可以在一个明确的说明时间内进行延迟。通过赋予许可与非许可活动的优先级, 来解决许可与非许可活动的冲突。

2.2 语法

设 (Prios, \leq) 代表优先级集合的全序, 假设 Prios 包含两个明确的成员 T 和 \perp , 对所有的 $x \in \text{Prios}$, $\perp \leq x \leq T$ 。一般当 $x \leq y$ 且 $x \neq y$ 时, 记作 $x < y$ 。

角色 Roles 和优先级 Prios 引出下列表达类。

定义 2 (事件表示, 角色状态表示)

① 事件表示为角色许可 $\text{enable } R$ 和角色非许可 $\text{disable } R$, $R \in \text{Roles}$;

② 优先事件表示为 $p:E$, 这里 $p \in \text{Prios}$, E 是事件表示;

③ 角色状态表示为 $\text{enabled } R$ 或 $\neg \text{enabled } R$, $R \in \text{Roles}$ 。

以下介绍冲突事件概念, 这是一个定义 TRBAC 语义的关键。

定义 3 (Conflicting Events) 设两个事件 $\text{enable } R$ 和 $\text{disable } R'$, 如果 $R = R'$, 则是冲突的。记为: $\text{conf}(\text{enable } R) \text{ def } \text{disable } R$, $\text{conf}(\text{disable } R) \text{ def } \text{enable } R$ 。

事件表示和角色状态表示是角色许可装置 (Role Enabling Base, REB) 的基础, 它包含关于使角色许可的时态约束。一个角色许可装置定义如下:

定义 4 (角色许可装置 Role Enabling Base, 周期事件 Periodic Event, 角色触发器 Role Triggers) 一个角色许可装置是由周期事件和角色触发器组成的一个元

素集。

① 周期事件表示为 $(I, P, p:E)$

a. I 是时间间隔; b. P 是一个周期表示; c. $p:E$ 是一个优先事件, 表示 $p < T$ 。

② 角色触发器的形式: $E_1, \dots, E_n, C_1, \dots, C_k \rightarrow p:E \text{ after } \Delta t$ (经过 Δt 时间后), 这里的 E_i 是简单事件表达, C_i 是角色状态表示, $p:E$ 是一个优先事件, 表示 $p < T$, Δt 是一个持续时间表达。

优先级和延迟表达 (Δt 之后) 可以忽略。在这种情况下, 缺省值 $p = \perp$, $\Delta t = 0$ 。

定义 5 (运行时间请求表示) 一次运行时间请求表示为:

$p:E \text{ after } \Delta t$

这里 $p:E$ 是优先事件表示, Δt 是持续时间表示。在 $p = T$ 且 $\Delta t = 0$ 的情况下, 可以缺省, 优先级和延迟表示 (Δt 时间后) 可以忽略。

例 1 是一个校园网计费系统的角色许可装置 (REB), 如表 1 所示。

表 1 一个角色许可装置的示例

(PE1). ([1/1/2006, ∞], Night-time, VH: enable staff-on-night
(PE2). ([1/1/2006, ∞], Day-time, VH: disable staff-on-night
(PE3). ([1/1/2006, ∞], Day-time, VH: enable staff-on-day
(PE4). ([1/1/2006, ∞], Night-time, VH: disable staff-on-day
(RT1). enable staff-on-night → H: disable login-on-network
(RT2). disable staff-on-night → H: enable login-on-network
(RT3). enable staff-on-day → H: enable login-on-network
(RT4). disable staff-on-day → H: disable login-on-network
(RT5). enable login-on-network → H: enable browser-network
(RT6). disable login-on-network → H: disable browser-network

表 1 中使用直观的名称表达周期表示。这里 VH (非常高) 和 H (较高) 表示优先级, 且 $H < VH$ 。在 REB 中周期表示和角色触发器规定, staff-on-night 角色必须在晚上被许可 (这个约束被定期事件 PE1 和 PE2 强制执行)。 staff-on-day 角色必须在白天被许可 (这个约束被定期事件 PE3 和 PE4 强制执行)。而且角色触发器 RT1 和 RT2 规定, 只要 staff-on-night 角色处于许可状态下, login-on-network 角色必须被禁止。角色触发器 RT3 和 RT4 强制相同的约束使只要 staff-on-day 角色处于许可状态下, login-on-network 角色必须被许可。最后角色触发器 RT5 和 RT6 指定, login-on-network 角色处于许可时间内, 那么 browser-network 方被许可执行。

3 时间约束模型的系统结构

下面描述 DBMS 中实现 TRBAC 的系统体系结构^[5]。该系统体系结构示意图如图 1 所示。其中矩形表示数据结构, 椭圆表示系统部件, 实体的变化和交互用箭头表示。

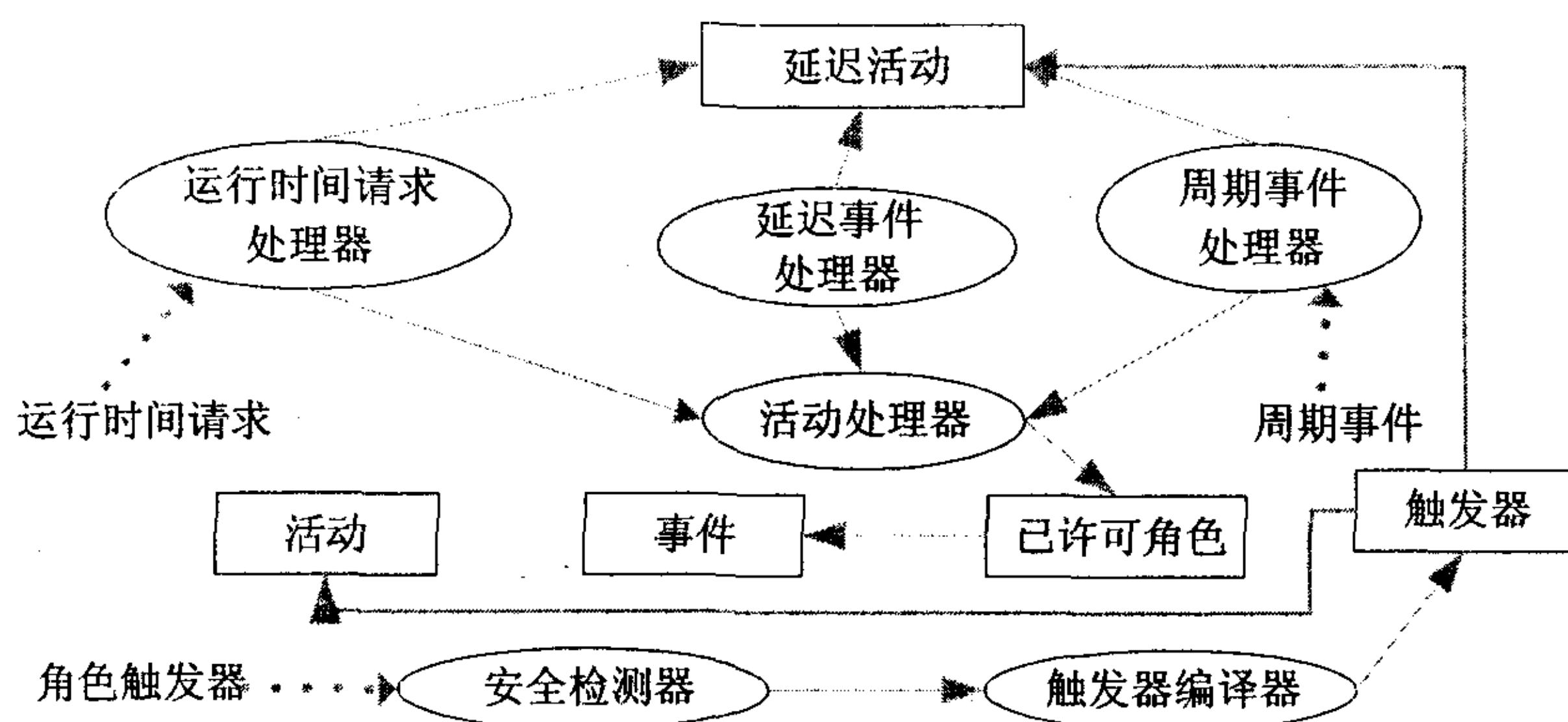


图 1 系统体系结构示意图

3.1 数据结构

该系统结构中包含以下数据结构:已许可角色(Enabled- Roles)、延迟活动(Deferred- Actions)、活动(Actions)、事件(Events)、触发器(triggers)、角色触发器(role trigger)、周期事件(periodic event)、运行时间请求(run-time request)。触发器、角色触发器、周期事件、运行时间请求等的信息在 DBMS 里维护。

(1)已许可角色:该表中每一个已许可角色都对应一个款项。该款项也包含与角色 R 相对应的用户集,它是按照 REB 目录和已签署的那个时刻点的运行时间请求授权激活角色 R 的用户集。

(2)延迟活动:该表中每一个延迟活动都对应一个款项。该款项包含被调度的活动执行的时间持续以及它的优先级。

(3)活动:该表记录已许可角色表中必然执行的活动。这个活动可以是角色触发器的触发、运行时间请求、周期事件等。

(4)事件:该表记录角色处于许可、非许可状态以及个别例外事件。

3.2 功能模块

系统包括 6 个功能模块, 见图 1, 即安全检测器 (Safeness Checker)、触发器编译器 (Trigger Compiler)、周期事件处理器 (Periodic Event Handler)、运行时间请求处理器 (Run - Time Request Handler)、延迟事件处理器 (Deferred Action Handler) 和活动处理器 (Action Handler)。下面依次描述每一个模块。

(1)安全检测器是由一个触发器的插入或修改而激活,并校验这个操作保护 REB 的安全性。

(2) 触发器编译器负责将通过安全检测器检查的角色触发器, 使用由 DBMS 提供的触发机制, 编译成一个相当于 DBMS 触发器附在表 Events 上。

(3) 周期事件处理器负责管理周期的事件。当一个周期的事件插入到 REB, 周期事件处理器在表 Deferred-Action 插入一个相应的款项。当一个周期事件

的删除被请求,相应的款项将从表 Deferred Actions 中删除。

(4)运行时间请求处理器一直处于激活状态,只要每一个运行时间请求被签署。这个处理器首先校验该请求是立即活动还是延迟的活动。前者,它返回活动和优先级到活动处理器;后者,它把活动连同它的产生和活动优先级一起插入到表 Deferred_ Action 中。

(5) 延迟事件处理器负责监视表 Deferred-Action 中执行的活动和它包含的联系时间。这个模块作为后台执行,它维护一个何时被唤醒的活动时间清单。当某活动后台唤醒后,它就从 Deferred-Action 中选择这个活动立即执行。如果活动存在冲突,它就选择优先级最高的(如果优先级相同,那么非许可优先)。然后,它返回该活动连同活动优先级到活动处理器。

(6)活动处理器处于该体系结构的核心,负责按照通过其他模块的请求或与表 Events 相关的触发器的触发而导致的更新表 Enabled_Roles。既然冲突是由请求活动产生的,该活动在表 Enabled_Roles 的执行之前收集到表 Actions。如果冲突产生,活动处理器在更新表 Enabled_Roles 之前解决它们的冲突。

3.3 系统的总体功能描述

(1)在任何给定的时间,按照包含在 REB 中的周期事件和触发器,以及运行时间请求,系统必须能够判定一个用户的角色的激活。

(2)当角色在请求激活的时间里处于许可,并且没有个别的例外事件规定该用户的其他特别角色,而且这个用户拥有权限扮演这个角色,那么可以授权通过该用户的请求来激活一个角色。

(3)在支持 TRBAC 角色许可时,必须考虑的关键因素:角色许可或非许可既能立即执行又能在固定的时间间隔被延迟;处理冲突行为中,必须考虑运行时间请求、周期事件、角色触发器及与之关联的优先级。

4 校园网计费系统应用设计

4.1 校园网计费系统基于时间约束条件分析

目前,高校校园网访问因特网还是收取费用的,其收费策略大致为两种:一种是基于流量计费;另一种是基于时间来计费。两种都提供包月制。在实际运行中,虽然用户的管理和使用分别设置口令提高安全等级,但用户上网策略大都未引入时间特性的约束,在实际应用中,用户无法锁定自己的账号,在非办公时间、夜间某些时间段易被非法盗用,给用户带来损失。针

对校园网计费用户账号盗用问题的时间特征,提出了一个采用基于时间约束的 TRBAC 模型来设计校园网计费用户管理系统的方案。

4.2 系统数据库设计

根据计费系统的功能设计,其业务数据库表不是本文的重点,不作赘述。按照 RBAC 设计本系统的数据库模型中用户身份和权限管理部分,它们分别为用户信息、组信息、权限信息、费率策略、上网控制策略、组与用户关系、组与权限关系、组与费率策略关系、组与上网控制策略关系、用户与上网控制策略。

为了实现 TRBAC,采用数据库的触发器方式实现控制,还需引入下面 6 张表。

●角色许可装置 REB 表:(REB_ID*,周期事件,角色触发器,角色许可的时态约束)

●周期事件 PE 表:(PE_ID*,时态,优先级,活动,角色)

●角色触发器 RT 表:(RT_ID*,活动 1,角色 1,时态,优先级,活动 2,角色 2)

●角色许可(ER)表:(ER_ID*,角色,活动,用户,优先级,时态)

●延迟活动(DA)表:(DA_ID*,角色,活动,用户,优先级,时态)

●活动表:(Action_ID*,角色,活动,用户 ID,优先级)

●事件表:(Events_ID*,事件描述,活动,优先级)

4.3 数据库的触发器的实现

目前对 RBAC 支持的数据库系统有:INFORMIX Online Dynamic Server Version 7.2, Sybase Adaptive Server release 11.5, Oracle Enterprise Server Version 8.0。以下以 Oracle 数据库为例说明角色触发器的类 SQL 语言描述。

角色触发器(RT2)实现强制行政办公人员角色晚 6:00 下班后不能继续连线。即 disable staff-on-day, enable staff-on-night→H: disable staff-on-day,通过触发器编译器把它编译成如下代码:

```
Create trigger RT2
before insert on Events
for each row
when ( new. action = 'disable' AND new. role = 'staff-on-day')
declare
X, Y number;
Begin
select count (*) into X from Enabled_Roles where role =
```

```
'staff-on-night';
if X>0 then
select count (*) into Y from Actions where (role = 'staff-on-night' AND action = 'enable' AND priority>0);
if Y=0 then
insert into Actions values ('staff-on-day', 'disable', all, 0);
endif
endif
end;
```

这个触发器首先校验角色 staff-on-night 是否处于许可。如果检查成功,接着开始校验在触发器(如 disable staff-on-night)体中的事件 event 是否没有被冲突活动所阻塞。如果这个进一步的检查成功,Oracle 触发器就将(staff-on-day, disable, all, 0)插入事件表 Actions。相应地进行一个立即请求,为带有最低优先级的角色 staff-on-day 置为非许可。关键词 all 用来表示这个活动没有为一个特别的用户(在用户集中)所请求,但为所有用户授权成为 staff-on-night 角色。

5 总结与展望

研究了时间约束、时间约束的 TRBAC 模型及其在校园网计费系统上的应用。TRBAC 模型的特点在于对角色的时态变化的描述,但是它没有对时间约束的其他方面进行描述:即受保护的對象、角色和受保护的資源之間联系等。基于时间的角色许可与非许可并非最佳模型,有待于对时间约束模型进一步改进。

参考文献:

- [1] Ferraiolo D F, Kuhn D R. Role-Based Access Controls[C]// Proceedings of the 15th NIST-NSA National Computer Security Conference. Baltimore, Maryland: [s. n.], 1992.
- [2] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.
- [3] Bertino E, Bettini C, Ferrari E, et al. A temporal access control mechanism for database systems[J]. IEEE Transactions Knowledge and Data Engineering, 1996, 8(1): 67-80.
- [4] Bertino E, Bettini C, Ferrari E, et al. An access control model supporting periodicity constraints and temporal reasoning[J]. ACM Trans Database Syst, 1998, 23(3): 231-285.
- [5] 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.
- [6] 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.