TRBAC 模型在工作流系统中的研究与实现*

周建美,徐 慧
(南通大学 计算机科学与技术学院,江苏 南通 226019)

摘 要:通过比较现有访问控制模型的各自特点和适用范围,针对现有模型的不足,结合 RBAC 和 TBAC 模型各自的优点,提出了一个新型的访问控制模型 TRBAC。描述了 TRBAC 模型的结构和安全控制原则,结合模型的实际应用指出今后工作的主要目标。

关键词:角色;权限;访问控制
中图分类号:TP311 **文献标识码**:A **文章编号**:1674-7720(2010)15-0004-02

Research and implementation of task-role based access control model on workflow system

ZHOU Jian Mei, XU Hui
(Computer Science and Technology School, Nantong University, Nantong 226019, China)

Abstract: By comparing the characteristics and application scope of existing access control model, this paper proposed a new access control model TRBAC which combines RBAC and TBAC model for their respective advantages to improve the security of information systems. Then it describes the TRBAC model structure and principles of security controls. With an example of application pointed out the main objective of future work.

Key words: role; privilege; access control

随着信息技术在现代企业中的广泛应用,许多工作已越来越多地依赖计算机得以完成,因此许多敏感的信息和技术都需要通过计算机控制和管理。如何确保这些信息和技术不被窃取和破坏,即如何安全使用,是当今计算机技术的研究热点。ISO(国际标准化组织)在网络安全标准(ISO7498-2)中定义了 5 个层次型安全服务,即身份认证服务、访问控制服务、数据保密服务、数据完整性服务和不可否认服务。访问控制是其中的一个重要组成部分[1]。

工作流(Workflow)管理技术起源于 20 世纪 70 年代的生产组织和办公自动化领域,提出的目的是通过将工作分解成定义良好的任务、角色,按照一定的规则和过程来执行这些任务并对其进行监控,达到提高工作效率、降低生产成本、提高企业生产经营管理水平和企业竞争力的目标[2]。工作流管理的最大优点是将应用逻辑与过程逻辑分离,在不修改具体功能的情况下,通过修改过程模型改变系统功能,从而完成对生产经营过程的集成管理,可有效地把人、信息和应用工具合理地组织在一起,发挥系统的最大效能[3]。

由于网络行为的开放性和自由性,工作流管理系统的安全问题越来越重要。确保业务过程中各项任务只能被合法的用户执行,已经成为工作流安全领域中一个重要的课题。因此,如何将访问控制技术应用于工作流中是当前研究的热点问题,研究工作流系统中的访问控制具有非常重要的意义。

1 访问控制研究现状

访问控制的目标是防止对任何资源进行非授权的访问,从而使资源在合法的范围内使用,它决定用户能做什么,以及代表一定用户利益的程序能做什么[4]。当前,访问控制技术的研究热点主要集中在基于角色的访问控制 RBAC(Role-Based Access Control)和基于任务的访问控制 TBAC(Task-Based Access Control)。

1.1 基于角色的访问控制模型

RBAC 以角色为核心,通过用户、角色、权限之间的

*基金项目:南通市科技计划项目(K2009057);南通大学自然科学基金项目(08Z034)

指派关系,实现用户和访问权限的绑定。它的核心思想是:受保护资源的访问权限与角色相联系,而给用户分配各种角色;用户与所要求访问的资源之间没有直接关系,若用户要访问某一资源,则其必须具有可访问此资源的角色[5],进而拥有相应的权限。

由于RBAC拥有诸如安全性高、灵活性强、接近现实世界等优点,一经提出就得到了广泛关注,目前已在很多领域得到了应用,发展较为成熟,但其在分布式应用、工作流应用等领域仍显得力不从心。由于角色是个长期的概念,不经常改动,因而在面对分布式应用的协作性、实时性时需要经常转变角色,这使得效率降低,不符合其设计初衷;而且RBAC不能主动控制任务执行的顺序,无法应对工作流系统的控制要求[6]。

1.2 基于任务的访问控制模型

与以往的访问控制策略相反,TBAC是一种主动访问控制策略。TBAC是在工作流的环境中考虑对信息的保护问题[1]。在工作流环境中,每一步对数据的处理都与以前的处理相关,相应的访问控制也是这样,因而TBAC是一种上下文相关的访问控制。TBAC不仅能对不同工作流实行不同的访问控制策略,而且还能对同一工作流的不同任务实例实行不同的访问控制策略[7]。

TBAC拥有主动控制、动态分配权限的优点,从而适用于工作流、分布式处理、多点访问控制的信息处理,特别是应用于安全工作流管理中。

1.3 基于任务-角色的访问控制

工作流管理系统主要是应用于大中型企业的流程自动化管理,数据在工作流中流动,执行操作的用户在改变,用户的权限也在改变。因此,如果采用RBAC进行权限控制时需要频繁地更换角色,且不适合工作流程的运转,无法实现随工作流运行需要的动态授权;虽然TBAC采用了"面向任务"的观点,从任务的角度来建立安全模型和实现安全机制,在任务处理的过程中提供动态实时的安全管理[1]。但简单地应用TBAC模型时系统必须根据需要不停地更换用户的访问控制策略,这样很可能造成用户权限分配和访问控制的混乱。

考虑到工作流管理系统的实际应用环境以及简化授权操作的复杂性,本文结合RBAC和TBAC的优点,将基于任务和角色的访问控制模型TRBAC(Task-Role-Based Access Control)应用于工作流管理系统中,既解决了动态的访问控制策略,又解决了多应用和多用户情况下权限管理复杂化的问题。

2 TRBAC模型及其特点

2.1 TRBAC模型

TRBAC模型在RBAC96模型的基础上引入"任务"的概念[6,8]。模型的基本结构如图1所示。其思想是:角色被指派给用户,用户通过承担的角色获取要执行的任务,执行任务时拥有相关任务所允许访问的客体权限。

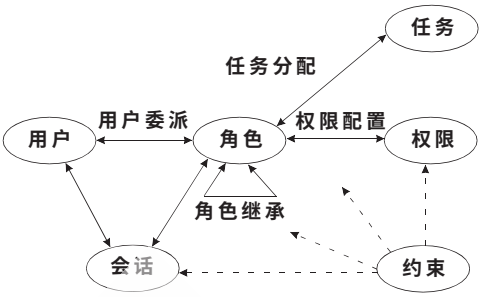

图1 TRBAC模型的基本结构

该模型建立在对任务分类的基础上,从企业和应用级的角度把任务分为工作流类(WF类)任务和非工作流类(NWF类)任务。WF类任务采用主动访问控制(AAC),NWF类任务采用被动访问控制(PAC);根据任务的权限是否可以继承将任务分为可继承权限的任务和不可继承权限的任务,消除增加私有角色带来的角色增长的问题;针对工作流任务,TRBAC实行动态权限分配,在工作流中,权限随着任务的执行而变动,角色只有在执行任务时才具有权限,角色不执行任务时不具有权限,任务根据流程动态到达角色,权限随之赋予角色,当任务完成时,角色的权限也随之收回。

2.2 TRBAC模型的安全控制原则

(1)最小特权原则

所谓最小特权原则是指用户所拥有的权限不能超过其执行任务时所需的权限。这是实现信息完整性的重要保证。执行任务时只给执行任务的角色分配所需的权限,未执行任务或任务终止后该角色不再拥有所分配的权限;而且,在执行任务过程中,当角色的某一权限不再使用时,系统将自动回收该权限。这样,对应执行该任务的角色的用户只能在执行任务时得到执行该任务所需的权限。

(2)责任分离原则

责任分离原则是用来形容多人控制策略的安全原则,本质上要求两个或多个人负责完成某个处理。从理论上来说,对于某些特定的操作集,某一个角色或用户不能单独完成所有这些操作,这样就保证系统中没有任何人拥有足够的权限独立进行欺诈活动。

"责任分离"可以有静态和动态两种实现形式。静态责任分离是指当一个任务与主体所拥有的其他任务彼此不互斥时,这个任务才能授权给该主体执行。动态责任分离是指当一个任务与主体的任何一个当前执行任务都不互斥时,该任务才能成为该主体的另一个执行任务。

(3)数据抽象原则

权限不局限于操作系统提供的典型的读/写执行权限,它可以抽象为实际工作流的操作权限。

3 模型的实例应用

TRBAC模型适合基于工作流的办公自动化、电子政

务和电子商务等系统。企业合同管理系统是一个典型的工作流系统,实现了对企业合同资料的自动管理和存储管理。合同管理的一般流程如图 2 所示。合同资料涉及到系统中多个部门、多个用户以及多个环节的流转,其主要业务流程可分为合同准备、签署、履行和履行后管理四个阶段。具体描述如下:

(1)合同准备阶段:包括合同策划、调查、初步确定准合同对象、谈判、拟订合同文本、审核等程序。

(2)合同签署阶段:包括正式签署合同、将合同分送相关部门等程序。

(3)合同履行阶段:包括合同履行、变更或转让、终止、处理纠纷等程序。

(4)合同履行后管理阶段:包括合同归档保管、执行情况评价等程序。

图 2 合同管理一般流程

合同管理的每个环节均被看作一个任务,为其指定相应的角色按照固定顺序协作完成,并且根据合同的处理情况选择下一个环节。在访问控制中,对于不相互排斥的权限可以由同一个用户承担,否则必须由不同的用户扮演冲突角色执行冲突权限来保证系统的安全性。如同一份合同中,“签署”和“履行监管”属于两个冲突权限,拥有该权限的任务属于冲突任务,执行该任务的角色就是冲突角色,必须由不同的用户来担任。而在不同的合同中,执行“签署”和“履行监管”任务的角色并不是冲突角色,角色 A 可以签署合同 C1,也可以履行监管合同 C2。因此,角色之间的冲突关系并不是固定不变的,而是随着角色权限的变化而发生变化。

把 TRBAC 应用到合同管理系统的访问控制模块中,集成了 RBAC 和 TBAC 的优点,增强了工作流的访问控制能力、增强了动态约束能力,满足了实际业务流程中对访问控制的需求。

访问控制模型的研究实际是为了更好地模拟现实世界的控制模式,是现实控制模式的计算机化。访问控制的发展是希望能让控制更“自然”,从而更高效。加入角色模拟现实中的岗位划分;任务层实际上对应不同岗位的不同工作;权限则相当于最终访问数据的钥匙。

本文在研究了访问控制模型的现状后,对现有模型进行分析比较,总结了访问控制模型研究的一些新思路,对如何在工作流管理系统中实现基于任务和角色的访问控制机制进行了有益的尝试和探讨。这种模型能适合于其他类似的应用环境,具有一定的通用性。但 TRBAC 中还存在一些问题,例如有关角色的分配与继承及管理、任务的分配与分类等,这些问题都有待于今后深入研究。

参考文献

[1] 邓集波,洪帆.基于任务的访问控制模型[J].软件学报,2003,14(1):76-82.

[2] 韵晋峰,唐慧佳.基于角色和任务的访问控制在工作流管理系统中的应用[J].成都信息工程学院学报,2008,23(1):46-49.

[3] 范玉顺.工作流管理技术基础——实现企业业务过程重组、过程管理与过程自动化的核心技术[M].北京:清华大学出版社,2001:28-78.

[4] 黄建,卿汉斯,温红子.带时间特性的角色访问控制[J].软件学报,2008,14(11):1944-1950.

[5] 宋昕,夏辉,王学通.NET 环境下基于 RBAC 的 Web 应用程序访问控制[J].计算机技术与发展,2006,16(4):218-220.

[6] 韩若飞,汪厚祥.基于任务-角色的访问控制模型研究[J].计算机工程与设计,2007,28(4):800-807.

[7] SANDHU R, COYNE E J, LFEINSTEIN H, et al. Role-based access control models [J]. IEEE Computer, 1996,29(2):38-47.

[8] OH S, PARK S. Task-role-based access control model[J]. Information System, 2003,28(6):533-562.

(收稿日期:2010-03-15)

作者简介:

周建美,女,1977 年生,讲师,硕士,主要研究方向:信息系统安全,网络和数据库。