TRBAC 模型在办公自动化中的应用①

宁运飞 王加阳 (中南大学 信息科学与工程学院 湖南 长沙 410083)

摘 要： 信息系统访问控制已越来越受到重视，特别是在办公自动化领域中控制资源访问要求的访问控制。但是传统的角色访问控制模型和任务访问控制模型并不能满足工作流多变的控制需求，针对此问题，引出了基于任务和角色的访问控制模型，它能够满足办公自动化所涉及的业务领域对权限管理的要求。最后，结合实际的办公自动化系统的开发，给出了基于任务和角色的访问控制模型的一个具体的应用实例。

关键词： TRBAC 模型;办公自动化;访问控制

Application of TRBAC Model to Office Automation

NING Yun-Fei, WANG Jia-Yang

(College of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: Growing attention has been paid to access control in information system, especially the access control of resource access requires in office automation area. However, traditional role-based access control model and task-based access control model cannot satisfy the workflow changeable requirements. To solve these problems, the task-role-based access control mode is introduced, which can satisfy the requirements of authority managements from business fields related to office automation. At the end of the paper, combined with the practical development of office automation system, the detailed implementation instance of task-role-based access control mode is provided.

Keywords: TRBAC model; office automation; access control

1 引言

随着计算机网络和分布式计算机系统的发展，信息安全日益成为人们关注的问题。信息网络的基本安全问题包括认证、授权、访问控制、审计、数据保密性、数据完整性、防否认、安全管理等，其中访问控制是比较重要的信息安全机制之一。

近年来，人们在访问控制的研究方面取得了很大成果，有许多访问控制模型[1]被提出来。访问控制是根据网络中主体和客体之间的访问授权关系，若对访问过程做出限制，可分为自主访问控制(DAC)和强制访问控制(MAC)。自主访问控制主要基于主体及其身份来控制主体的活动，能够实施用户权限管理、访问属性管理等。强制访问控制则强调对每一主、客体进行密级划分，并采用敏感标识来标识主、客体的密级。

访问控制还包括基于任务的访问控制[2] (TBAC)和基于角色的访问控制[3,4](RBAC)。TBAC 是从应用和企业层角度来解决安全问题，采用“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实时的安全管理。在 TBAC 中,对象的访问权限控制并不是静止不变的，而是随着任务的上下文环境发生变化，这是 TBAC 的主要特点。RBAC 的基本思想是职责分离，用户被授予角色,角色被授予权限，权限关联操作，用户通过被授予的角色得到该角色的相应权限，来完成这些操作。

基于任务和角色的访问控制模型[5](TRBAC)不像 RBAC 中没有将任务从角色中分离出来，也不像 TBAC 中没有明确地突出角色的作用，TRBAC 模型把任务和角色置于同等重要的地位，它们是两个独立而又相互

① 基金项目:湖南省科技计划(2008FJ3184);湖南省自然科学基金(06JJ20075)
收稿时间:2009-10-15;收到修改稿时间:2009-11-28

关联的重要概念。TRBAC 模型是先将访问权限分配给任务，再将任务分配给角色，角色通过任务与权限关联，任务是角色和权限交换信息的桥梁。在 TRBAC 模型中，根据具体的执行任务要求和权限约束，任务具有相应的权限，不同的任务拥有不同的权限，权限随着任务的执行而变动，这样才能够满足办公自动化所涉及的业务领域对权限管理的要求。

2　TRBAC模型

2.1 TRBAC 设计模型

基于任务和角色的访问控制模型是一种从任务和角色的双重角度出发来实现访问控制的模型，如图 1 所示：

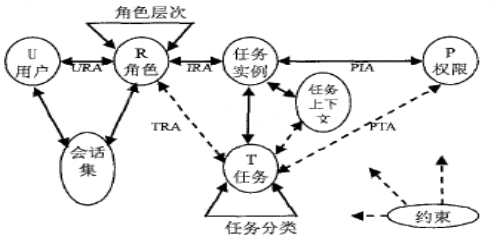

图 1　TRBAC 模型

其基本思想是：用户被赋予角色，并通过承担角色获取要执行的任务，而权限则赋予任务，角色和权限不直接关联而是通过任务把角色和权限联系在一起。给用户指派合适的角色，用户通过其指派的角色获取其可以执行的任务，然后在执行某个任务的某个具体实例时获得该任务所允许访问的客体的权限，方便对权限的管理和控制。角色与权限通过任务关联起来，角色在任务执行期间的权限赋予和任务非执行期间的权限收回使得最小权限约束进一步细化到任务这一级，真正实现了权限的按需分配，从而满足了实际办公自动化系统工作流的需要。

2.2 TRBAC 模型的基本概念

模型主要由如下元素组成：

(1) 用户(U)：是指完成系统活动实例的参与者，既可以是人，也可以是某个应用程序。

(2) 角色(R)：表示执行某一任务的资格，体现了某种权利和资格，是根据部门、职责、权限等抽象出来的某一类型的用户的描述。

(3) 角色层次[6]：角色集到角色集之间的二元关系，具体表现为在一个组织内部的角色等级关系，即关于角色的偏序关系。它包括一般继承和扩展继承两种机制。

(4) 任务(T)：工作流程中的一个逻辑单元，完成一定的功能目标，即工作流的活动，或是若干个活动的组成。任务可按其功能分为管理任务、监督任务和数据操作任务。管理任务用来管理用户组内低级用户的活动任务，并进行任务分派。监督任务用来查看活动任务的活动状态。数据操作任务进行底层的数据存取操作。

任务有静止、存在、失败、运行、等待和完成 6 种基本状态。任务之间存在着相互状态依赖关系，其中包括顺序依赖、失败依赖、分权依赖和代理依赖。TRBAC 模型主要根据状态依赖这个动态约束进行动态授权。

(5) 任务分类：任务根据各组织结构和访问控制要求进行分类，以使模型更有利于划分任务权限，以及任务优先级的配制。

(6) 任务实例：在工作流系统中，任务实例是一个动态的概念，是任务运行中的实例，即任务的一次执行。

每个任务实例包括五个状态：静止态、活动态、挂起态、终止态和夭折态。任务实例被创建，就处于静止态；被激活，就处于活动态；执行是由于某种原因暂停执行，就处于挂起态；如果恢复执行，又重新处于活动态；假设执行任务的条件不能得到满足，任务无法执行中途夭折，那么就处于夭折态。

(7) 任务上下文：对任务是否能被执行的约束条件，任务上下文包括执行任务所需要的用户以及登陆的角色、哪个执行机、什么时间、输入条件（数据）等数据。

(8) 权限(P)：用户所具有的访问系统的能力范围，是对计算机系统中的一个或多个数据对象进行某种方式访问的许可权，是数据操作任务访问数据资源的接口。

2.3 TRBAC 模型内部的各种关系

为了达到访问控制的目的，模型内部各元素之间存在的各种特定约束关系：

(1) 用户角色赋予关系(URA)：为各用户指定其所能充当的角色，表示用户与角色之间的映射关系，它是一种多对多的指派关系，即一个用户可以被授予多个角色，一个角色可以分配给多个用户。

(2) 任务角色赋予关系(TRA)：为各角色定义其可

以执行哪些任务，表示任务到角色之间的映射关系，一个任务可以配置多个角色，而一个角色也可以参与多个任务。任务的性质决定了所配置的角色，反之角色的性质也决定着所参与的任务。

(3) 权限任务赋予关系(PTA)：为各任务模板定义其所需要的最小权限集。它反映了权限到任务的多对一的指派关系。

(4) 实例角色赋予关系(IRA)：根据任务角色赋予关系以及任务与任务实例之间映射关系得到角色可以执行的任务实例集。

(5) 权限实例赋予关系(PIA)：根据任务权限赋予关系以及任务与任务实例之间的映射关系来确定具体的任务实例的权限集。

2.4 TRBAC 模型安全性分析

(1) 权限时间约束。

模型解决了权限控制中的时间约束的问题，时间约束表示用户只能在某个时间段内执行某项任务，它伴随着任务流的推进而进行。当某个任务实例被激活时标志着任务的开始，当任务实例完成时预示着任务的结束，在任务开始和结束时间段内对任务执行者进行授权，由于权限是通过任务与角色联系起来的，所以用户在执行任务过程中对具体数据的操作权限是由权限到任务的指派关系所限定的。任务执行完成后，任务执行者的授权被收回，这样就保证可以授权流与工作流同步，防止一个用户拥有权限的时间长于他所需要权限的时间而导致安全泄露。

(2) 最小特权原则。

最小特权原则要求分配给用户的特权不超过用户完成某个任务所必需的权限。TRBAC 模型中权限不是直接同分配给用户的角色进行联系，而是通过工作流系统中的任务进行关联，在执行任务时只给任务分配所需的权限。分配具有该任务执行权限的角色的授权用户，在未执行任务或者任务终止以后，该用户就不再拥有所分配的权限，未经授权的用户更不能执行该任务，因此很好的保证了最小特权原则。

(3) 职责分离原则。

对于某些特定的任务，某个角色或者用户不可能独立地完成所有的任务操作，这时就需要进行职责分离，目的是通过由多个不同的用户来负责某项任务以分散权利和责任，从而减少可能发生欺诈行为。静态职责分离在工作流执行之前就可以执行，动态职责分离在工作流执行过程中执行。模型中利用对角色的约束以及授权依赖中的分权依赖原则，能够实现工作流系统中任务执行过程中的职责分离原则。

3 TRBAC在办公自动化系统中的应用

在办公自动化系统的公文流转过程中,其主要对象始终是"公文"。无论是在何种类型的工作流中流转,公文一般都会经过已审批、已审核、已签发、存档等状态。在各种"公文"类型中,不同的工作流对数据对象也具有一定的共性,如发文、收文、会议申请、车辆申请、请假等工作流中的公文都包括公文标题、起草日期、起草人、审批人、审核人、批准(签发)人等数据对象。但是在公文流转过程中，并不是某个人自始至终都来承担某个环节的任务，通常是某几个人都拥有完成某个任务的权利，而且几乎每一个人都拥有完成某几个任务的权利，每一个新的流程开始都意味着重新分配任务和权限，这就需要保证模型有动态授权的功能。其次，在系统运行过程中，对于不属于工作流的的任务，如新闻、邮件等，采用被动的访问控制以减少权限控制复杂性；而对于发文、收文、请假等流程，则把他们分成不同的任务，由不同的角色完成，采用主动的访问控制以增加灵活性。TRBAC 模型恰恰可以满足这种需求，模型不但可以实现灵活动态的任务授权，而且增强了系统的安全性。所以系统选用 TRBAC 模型执行权限管理。现在以某院协同办公系统中的发文管理为例来验证 TRBAC 的运作状况。

发文管理是涉及到多部门、多用户、多环节的复杂操作，是系统的一个重要组成部分，也是一个典型的工作流。发文管理工作流的设计是否合理直接影响到公司的工作效率。发文管理大致经过发文拟稿、核稿、会签、审批、签发、分发和归档等处理过程，流程如图 2 所示。

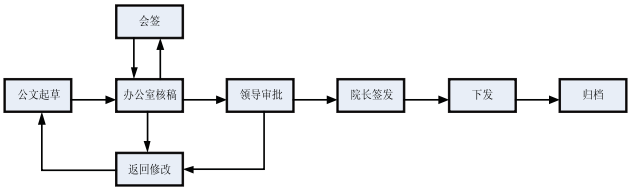

图 2 发文流程

流程的具体过程如下：拟稿人起草新公文后交给办公室核稿；核稿人通过则可以选择会签或领导审批，否

则返回给拟稿人进行修改；如果选择会签，则在会签人员会签完，再由办公室复核公文，然后再到主管院领导审批公文；如果在某些特定的情况不要会签，则可以直接到主管院领导审批；主管院领导审批发现问题则退还拟稿人进行修改，否则递交院长签发；院长签发公文，并交给院办下发；院办根据实际需要下发公文，并将公文整理归档。以上的每个流程的环节都可以看作是一个任务，为其指定相应的角色按照一定的顺序协作完成，并且根据公文的处理情况选择下一个环节。

4 结语

基于任务和角色的访问控制模型是一种面向工作流安全策略的有效的访问控制方法。我们解释了该模型中的重要概念及约束关系，通过访问控制实现了基于任务和角色的授权安全性。TRBAC 相对于传统的访问控制模型来说，是一个重要的发展和改善，具有极其广泛的应用范围。文章以某院协同办公系统的公文处理流程为例，介绍了 TRBAC 模型在企事业单位中的应用。但 TRBAC 中有关任务的分类与分配以及模型更加适合复杂的环境和各种例外情况等，仍有许多值得研究的地方，这将是我们以后研究的问题。

参考文献

1 沈海波,洪帆.访问控制模型研究综述.计算机应用研究, 2005,22(6):9－11.
2 邓集波,洪帆.基于任务的访问控制模型.软件学报, 2003,14(1):76－82.
3 Sandhu R, Conyne EJ, Lfeinstein H. Role-based access control models. IEEE Computer, 1996,29(2):38－47.
4 许春根,江于,严悍.基于角色访问控制的动态建模.计算机工程, 2002,28(1):116－118.
5 文家福,王嘉祯,杨素敏.基于角色和任务的工作流访问控制模型及其应用.计算机应用研究, 2007,24(9):168－169.
6 钟华,冯玉琳,姜洪安.扩充角色层次关系模型及其应用.软件学报, 2000,11(6):779－784.