

基于任务的访问控制在成绩发送系统中的应用

何 青, 张 毅

(广东医学院 网络中心, 广东湛江 524023)

摘要: 实际的信息系统往往需要由多个相关的任务构成业务流程(工作流) 来完成, 静态的访问控制不能满足工作流对访问控制的要求. 文章介绍了一种新兴的访问控制机制——基于任务的访问控制(TBAC), TBAC 可依据任务和任务状态的不同, 对权限进行动态实时的管理. 在开发远程成绩发送系统的实例应用中, 把 TBAC 和 RBAC(基于角色的访问控制) 结合, 实现一种灵活有效的访问控制策略.

关键词: 访问控制; 工作流; 信息系统

中图分类号: TP391

文献标识码: A

文章编号: 1007-7162(2004) 04-0026-05

引言

当前, 出于高校发展的需要, 高校异地建分校的情况非常普及, 而各分校的学生成绩都要经过学校总部的学籍管理科进行审查, 然后存档. 为了提高工作效率, 需要建立远程成绩发送系统. 由于高校的学生成绩至关重要, 远程成绩发送系统对安全性和完整性有着很高的要求, 而有效的安全访问控制机制是实现信息系统安全性和完整性的重要手段, 强有力的访问控制能有效地防止进入系统的用户越权访问自己不该访问的信息. 目前流行的安全访问控制策略主要有 3 种: 1) 自主访问控制(Mandatory Access Control, MAC), MAC 是在确认主体身份及所属组的基础上, 在系统已命名的用户和已命名的客体(如文件和程序)之间进行定义和控制访问, 是根据访问者的身份和授权来决定访问模式, 对访问进行限定的一种控制策略. 2) 强制访问控制(Discretionary Access Control, DAC), DAC 是指系统强制主体服从事先制定的访问控制策略. 它对外部主体能够直接或间接访问的所有资源实施强制访问控制, 为这些主体及客体指定敏感标记, 这些标记是等级分类和非等级类别的组合, 它们是实施强制访问控制的依据. 3) 基于角色的访问控制(Role-based Access Control, RBAC)^[1], RBAC 的基本思想就是将用户划分成与其所在组织结构相一致的角色, 然后把访问权限与角色相联系, 通过给用户分配合适的角色, 让用户与访问权限相联系, 从而实现用户与访问权限的逻辑分离. RBAC 以减少授权管理的复杂性, 降低管理开销和为管理员提供一个比较好的实现复杂安全策略的环境而著称.

以上的 3 种访问控制都是建立在主体、客体访问控制思想上的, 主体只要拥有对客体的访问权限就可以对客体进行访问, 它们基本上是一种静态的授权控制方式. 但在实际的信息系统中, 为了完成某一目标, 往往需要由多个相关的任务构成业务流程(工作流) 来完成^[2,3], 如图 1 远程成绩发送系统的工作流程所示, 对这些任务需要一种短暂的授权和控制, 静态的授权方式

收稿日期: 2004-04-28

基金项目: 2003 年湛江市科技攻关项目(编号: ZK0406)

作者简介: 何青(1968), 女, 广东湛江人, 讲师, 硕士, 主要研究方向为信息安全技术、数据库技术.

不能满足工作流应用访问控制. 为此, 需要采用动态的授权控制方式.

1 基于任务的访问控制

1.1 基于任务的访问控制概述

基于任务的访问控制(Task- base Access Control, TBAC) 首先由美国 George Mason 大学的 R. S Sandhu 教授提出, 它关注的是信息系统内任务(活动)的管理和模型化, 首要的目标是确保系统信息完整性, 防止未授权的行为对信息进行未授权的修改^[4]. 在 TBAC 中, 对象的访问权限控制并不是静止不变的, 而是根据信息在系统内的流动和任务情况灵活甚至主动地更新授权信息来实现访问控制^[5 6]. TBAC 的基本思想有以下几点.

- 1) 将访问许可与任务相结合, 每个任务的执行都被看作是主体使用相关访问许可访问客体的过程, 在任务执行过程中, 因为任务都是有时效性的, 所以在基于任务的访问控制中, 用户对于授予他的权限的使用也是有时效性的.
- 2) 访问许可的有效性与任务的执行状态有关, 只有当任务处于运行状态时, 主体才能使用许可.
- 3) 任务与任务之间存在着一定的依赖关系. TBAC 是在工作流的环境考虑对信息的保护问题, 在工作流环境中, 每个任务的执行都与以前的任务相关, 相应的访问控制也是一样.

1.2 TBAC 的基本概念

- 1) 任务(Task): 工作流程中的一个逻辑单元. 它是一个可区分的动作, 可能与多个用户相关, 也可能包括几个子任务.
- 2) 授权步(Authorization Step): 一个工作流程中对处理对象的一次处理过程, 是访问控制所能控制的最小单元. 授权步由受托人集和多个许可集组成, 其中受托人集是可被授予执行授权步的用户的集合, 许可集则是受托人集的成员被授予授权步时拥有的访问许可.
- 3) 授权单元(Authorization Unit): 由一个或多个授权步组成的单元, 它们在逻辑上是联系在一起的. 授权单元可以分为一般的授权单元和原子授权单元. 一般授权单元内的授权步依次执行, 原子授权单元内各个授权步紧密联系, 任何一个失败或取消都可导致整个单元的失败.
- 4) 依赖(Dependency): 指授权步之间或授权单元之间的相互关系, 它包括顺序依赖、失败依赖、分权依赖、代理依赖和级别分权依赖. 依赖反映了 TBAC 的原则, AS 表示授权步, TBAC 的依赖关系如表 1 所示.

2 TBAC 和 RBAC 结合在远程成绩发送系统中的应用

当前, TBAC 还处于一种高度抽象的概念阶段, 只定义了基本概念, 是一个研究热点, 具体的实现技术还处于研究中. 笔者在开发远程成绩发送系统中, 将 TBAC 和 RBAC 灵活地结合, 把

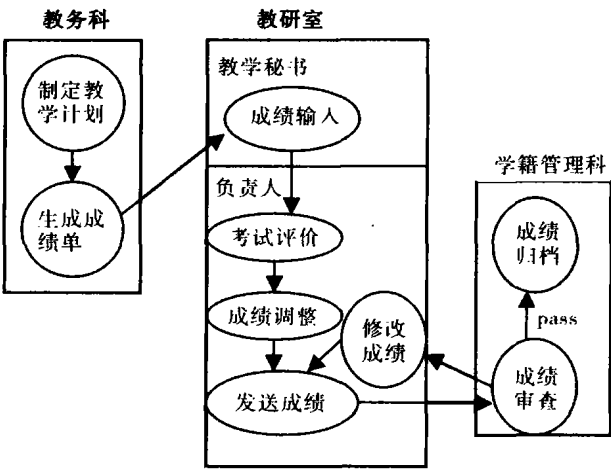


图 1 远程成绩发送系统工作流程

TBAC 的授权步中受托人说明为角色集, 为系统建立了一种结合性的访问控制策略.

表 1 TBAC 的依赖关系

依赖关系	符 号	说 明
顺序依赖	AS1 $\longrightarrow$ AS2	AS1 完成后, AS2 才被激活
失败依赖	AS1 $\xrightarrow{\times}$ AS2	AS1 失败后, AS2 才被激活
代理依赖	$\begin{matrix} \{r, d\} \\ AS1 \xrightarrow{\times} AS2 \end{matrix}$	r 表示 AS1 失败后, AS2 的授权被收回. d 表示 AS1 失败后, AS2 代理 AS1 的授权
分权依赖	AS1 $\longleftrightarrow$ AS2	AS1 和 AS2 必须由不同的用户完成
级别分权依赖	AS1 $\xrightarrow{H/L} AS2$	AS1 和 AS2 必须由不同的用户完成, AS1 的用户级别要高于 AS2

系统建立了授权管理数据库, 授权管理关系表包括用户表 Users、角色表 Roles、许可表 Permission、用户角色关系表 UserRole、和角色许可表 roleper 等. 图 2 列出各个表的关系.

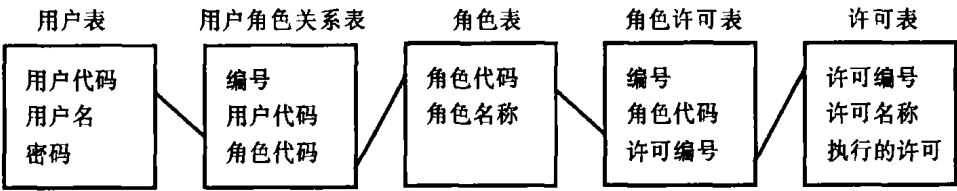


图 2 授权管理数据库表之间的关系

其中角色代码 roleid 由长度为 8 的数字编码组成, 代码前两位代表部门类别, 如 01 为教务处, 04 为教研室等, 代码第 3、4 位表示其责任, 代码的后 4 位是具体部门的编码. 现以角色为计算机教研室主任为例, 其角色代码为“04010123”, 第 1、2 位代码为 04, 代表其为教研室类用户, 第 3、4 位代码 01, 代表其为部门主管(02 为教学秘书, 03 为普通教师), 后 4 位为所在教研室编码 0123(教研室编码前两位为教研室所在的二级学院代码), 代表用户所在的教研室为计算机教研室.

在程序实现上, 把授权管理工作写成函数文件放入文件 logincheck. inc 之中, 在需要的地方调用函数文件. 授权函数必须遵循授权规则, 从形式上来说, 一条 TBAC 的授权规则可以写成五元组的形式(S, O, AS, P, L), 其中 S 表示主体, O 表示客体, AS 表示授步权, P 表示 AS 所激活的权限, L 表示 AS 的存活期限. AS 被触发之前, 五元组(S, O, AS, P, L) 无效; 当 AS 被触发时, S 可在 O 上执行 P, 同时 L 开始被消耗, 五元组(S, O, AS, P, L) 有效, 当生命期终止, AS 被定为无效, 五元组(S, O, AS, P, L) 无效, S 所拥有的 P 被收回. 运行授权函数首先检查授权步的状态, 包括所要求的先行操作是否完成, 已授的权限是否过期, 访问许可是否用完, 执行的任务如果有问题, 则给用户提示信息, 并暂时终止该任务的执行; 在某一授权步完成后, 自动激活相关联的授权步.

具体的实现方法是在授权管理数据库建有教学计划表 teachplan, 教学计划表存储着本学期的学校开课情况, 每笔记录记载着工作流的目标及授权步的状态, 含有 kcmc(课程名称)、deptid(授课单位代码)、input(是否输完成绩)、submission(提交情况)、save(成绩是否归档) 等字段. 系统的工作流如图 1 所示, 当教务科为某年级某专业的学生在某学期安排某门课程时(如图 3), 系统

自动把该批学生的成绩单导入负责该门课程的教研室成绩表中,并在 teachplan 记录该教学计划,教研室教学秘书获得对该门课程的成绩输入授权(如图 4),教务科排课和教学秘书输入成绩之间存在着顺序依赖和分权依赖,成绩输入必须在课程分配到教研室才能进行,两部分工作必须由不同权限的用户完成.成绩输完后,该课程记录中的 input 字段值为“Y”,收回教学秘书成绩输入的权限,激活教研室负责人处理成绩授权步,教研室负责人负责审查成绩的真实性,并在权限内调整分数,成绩经教研室负责人电子签字后可以提交(如图 5),成绩输入和成绩提交存在着顺序依赖和级别分权依赖,教研室负责人可以指派本教研室教学秘书.成绩提交后,该课程记录中的 submission 字段值为“Y”,收回教研室负责人的权限,激活学籍管理科成绩审查授权步,教研室负责人处理成绩和教务科成绩审查存在着顺序依赖、分权依赖和失败依赖的关系,学籍管理科只对已提交的成绩进行审查,已提交的成绩只有在学籍管理科成绩审查不通过时,该课程记录中的 submission 字段值由“Y”改为“N”,教研室负责人处理成绩这一授权步才会又被重新自动激活.学籍管理科成绩审查和成绩归档是原子授权单元,学籍管理科成绩审查和成绩归档两个授权步任一个失败都会导致整个授权单元的失败,而且第一步授权成功后,紧接着进行第二步授权,不能出现界于两者之间的状态.成绩归档后信息可供其它系统共享.



图3 课程安排



图4 成绩输入



图5 成绩提交

3 结论

TBAC 是一种高层次的访问控制模型, 它从任务(活动)的角度来建立安全模型和实现安全机制, 在任务过程中提供动态实时的安全管理. 笔者在实际信息系统开发中, 通过把 TBAC 和 RBAC 结合, 为信息系统构建灵活有效的访问控制策略, 其优点如下.

1) 支持两个著名的安全控制原则.

(1) 最小特权原则: 即在给用户分配权限时, 根据每个用户的任务特点使其获得完成自身任务的最低权限, 不给用户赋予其工作范围之外的任何权力. 在执行任务时只给用户分配所需的权限, 未执行任务或任务终止后用户不再拥有所分配的权限; 而且在执行任务的过程中, 当某一权限不再使用时, 授权步自动将该权限收回. 如图 5, 一个用户以计算机教研室主任这个角色登录系统, 提

交本教研室所授课程的成绩时,他能且仅能提交本教研室本学期所授课程的成绩,并且提交前,该课程成绩的输入必须完成了;当成绩提交了,教研室主任不能再去处理该课程的成绩。

(2) 职责分离原则:重要的任务需要由不同的用户执行,用户并为其所执行的任务负责,这可通过授权步的分权依赖实现。如:课程成绩的提交由教研室主任执行,教研室主任要为提交的课程成绩真实性负责;课程成绩归档由学籍管理科负责,学籍管理科要为课程成绩的完整性负责。

2) 实现授权的动态管理.TBAC 能清晰地表达复杂工作流的控制机制,保证工作流按预期的方向流动。

3) 简化了权限管理.由于与 RBAC 结合,授权步中受托人说明为角色集,而 RBAC 的特点是通过分配和取消角色来完成用户权限的授予和取消,并提供了角色分配规则和操作检查规则。通过改变用户的当前角色集就可以改变用户的权限,而改变某种角色所含的权限也可以改变一组用户的权限。如:当某个用户不再担任教研室主任,只需要把其角色改为普通教师,该用户的教研室主任的权限就被取消了,无需修改任何代码。

4) 减少开发复杂度,提高效率.授权管理可作为系统的整体核心控制部分,单独地被分离出来进行设计和开发;有效地利用系统已有的资源,增加代码的可复用性,使系统更有条理。该系统建立的授权管理数据库目前也应用于其后开发的网络应用系统中。

参考文献:

- [1] Ferriolo D F, Sandhu R, Guirila S, Kuhn D R, Chandramouli R. Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.
- [2] Botha R A, Eloff JHP. Access control in document centric workflow system: an agent-based approach[J]. Computers & Security, 2001, 20(6): 525-532.
- [3] 史美林, 杨光信, 向勇, 伍尚广. WMS: 工作流管理系统[J]. 计算机学报, 1999, 22(3): 325-334.
- [4] Thomas R K, Sandhu R S. Conceptual Foundations for a Model of a task-based Authorization[A]. In: Proc of the 7th IEEE Computer Security [C]. Franconia: NH, Foundations Workshop, 1994. 66-79
- [5] 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.
- [6] 王锐, 胡金柱. 基于任务的访问控制在法院系统中的应用[J]. 计算机工程与应用, 2003, 39(2): 224-226.

Application of Task-based Access Control in Submit Subject Achievement System

HE Qing, ZHANG Yi

(Network Center, Guangdong Medical College, Zhangjiang 524023, China)

Abstract: Information system sometimes needs many correlative tasks form workflow. Static access control cannot meet the needs of workflow for access, control. This paper introduces a new access control mechanism called task-based access control, which can dynamically manage the permissions through tasks and tasks' status, and combines task-based access control with role-based access control to realize a flexible and effective access control strategy in an actual application.

Key words: access control; workflow; information system