

基于 T_RBAC 的 CSCW 系统访问控制模型研究

梁泽梅, 李蜀瑜

(陕西师范大学 计算机科学学院, 陕西 西安 710062)

摘 要: 在 TBAC 和 RBAC 的基础上, 综合两者的优点提出了一种新的模型, 即基于 T_RBAC 的 CSCW 系统访问控制模型。该模型延用 RBAC 作为系统的总体构架, 在原来的 RBAC 中加入任务的概念, 再将角色与任务, 权限与任务联系起来, 通过任务来实现对权限的动态管理。将工作流程的外部状态引入到访问控制模型中, 与任务的内部状态共同作用, 控制任务权限的分配, 满足了 CSCW 系统协同工作的特点。

关键词: T_RBAC; RBAC; TBAC; CSCW

中图分类号: TP311

文献标识码: A

文章编号: 1000-7180(2011)06-0084-04

Research of T_RBAC-based Access Control in CSCW System

LIANG Ze-mei, LI Shu-yu

(College of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Based on TBAC and RBAC, this article synthesized advantages of both and proposed one kind of new model, namely T_RBAC-Based CSCW System Access Control Model. The model continues to use RBAC as the system overall structure and adds the concept of task in original RBAC. After connecting role and task, permission and task, it realizes the dynamic management authority by the method of the task. Introduced the exterior state of the work flow to the access control model to work with the internal state of the task, the model controls the assignment of task permission's it meet the joint work characteristic of the CSCW system.

Key words: T_RBAC; RBAC; TBAC; CSCW

1 引言

随着网络的发展, 网络安全越来越受到人们的重视。访问控制是对需要访问的主体(用户或者进程)进行身份验证, 限制主体对于访问客体(文件或系统)的访问权限, 即防止合法的用户进行不合法操作, 阻止不合法用户的非法访问。调查显示, 网络中 80% 的攻击和入侵都来自组织内部, 来源于合法用户的非法使用和越权访问。访问控制可以最大程度阻止这种来自内部的破坏。

本文在基于任务的访问控制模型, TBAC^[1] 和基于角色的访问控制模型 RBAC^[2-3] 的基础上, 结合现实社会企业系统中的访问控制等级体制, 提出基于 T_RBAC 的 CSCW 系统访问控制模型。

2 基于 T_RBAC 的访问控制模型

2.1 T_RBAC 模型的基本思想

基于 T_RBAC 的访问控制, 就是将“任务”和“角色”都应用到访问控制模型中, 由于 TBAC 作为一种策略很难单独模型化, 实际应用中往往需要和其他的访问控制模型相结合, 而 RBAC 模型作为总体构架, 静态管理用户、权限方面有很多优点, 且理论研究与实际应用都已经很丰富^[4]。因此, 如何将 TBAC 策略引用到 RBAC 模型中来, 构建基于任务与角色的 T_RBAC 模型成为近几年来研究的热点^[5]。

T_RBAC 的基本思想是首先延用 RBAC 作为系统的总体构架, 以实现对现实世界的模拟, 方便对用户权限的静态管理; 同时, 在原来的 RBAC 中加

入任务的概念,将系统要实现的一系列功能细化为一个任务,再将角色与任务,权限与任务联系起来,通过任务来实现对权限的动态管理.

2.2 T_RBAC 模型结构

T_RBAC 模型基本结构如图 1 所示,由用户(U)、角色(R)、会话(S)、任务(T)、权限(P)、任务实例(TI)和约束规则这几部分组成.模型中增加了任务实例的概念,作用是为了说明模型支持动态授权,模型中的任务是 workflow 任务中的模板.

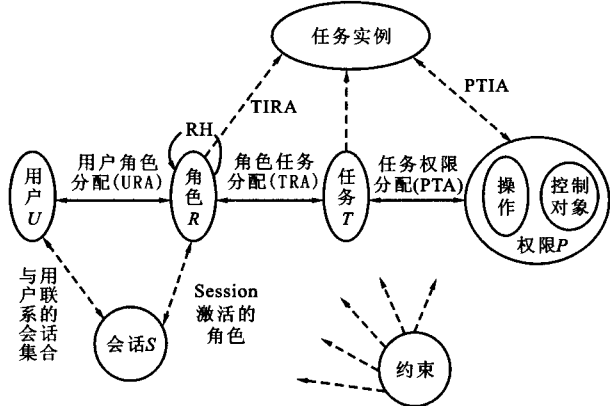


图 1 T_RBAC 模型的基本结构图

图 1 中的实线所表示的指派关系在 workflow 配置阶段进行,其在实际 workflow 运行过程中由虚线部分来执行.即用户建立一个会话,根据用户与角色在配置阶段的指派关系来激活用户拥有的角色,用户请求执行任务时,再根据角色与任务在配置阶段的指派关系来执行相应的任务实例,同时拥有执行任务时被激活的权限,该权限是根据任务与权限在配置阶段的指派关系,再加上一些动态约束和执行任务的上下文共同来决定的.

模型中的元素的定义如下:

定义 1 用户(U):是一个可以独立访问计算机系统中的数据或资源的主体.用户一般情况下指自然人,但有时也包括计算机或一些具有自治性的软件系统. $U = \{ U_1, U_2 \dots \}$,表示用户的集合.

定义 2 角色(R):组织内部的工作职能,它代表了一种资格、权利和责任. $R = \{ R_1, R_2 \dots \}$,表示角色的集合.

定义 3 权限(P):是对计算机系统中的数据或者其他资源对象进行访问的许可.权限的划分是一项复杂的工作,它直接决定着访问控制服务的粒度与深度. $P = \{ P_1, P_2 \dots \}$,表示权限的集合.P 是由 OP 和 OB 组成的,OP 是一系列操作的集合,OB 是客体对象的集合.

定义 4 会话(S):一个用户和该用户所担任的

角色集合的子集的映射.当用户激活部分或者全部他被授予的角色时,就建立了一个会话,用户拥有的权限是在这次会话中被激活的角色的权限.一个会话是用户的一个活跃进程,它代表了用户与系统的交互.

用户与会话的关系是一对多的关系:一个用户可以同时打开多个会话运行,而一个会话只能为一个用户服务,并且在会话周期内,用户固定不变.会话与角色的关系是一个多对多的关系:一个会话可以激活多个角色,一个角色也可能在多个会话中被激活.

定义 5 任务(T):任务是系统执行过程中完成一定功能目标的最小工作单元,通过其自身的权限属性进行功能操作,具有原子性.在实际工作中,一个任务包含如下特征:长期存在;可能包含多个子任务;完成一个任务可能需要不同的用户. $T = \{ T_1, T_2 \dots \}$,表示任务的集合.

定义 6 任务实例(TI):是以任务为模板生成的任务运行实例,实际运行过程中执行的是任务实例,而不是任务本身.一个任务可以对应多个任务实例,但一个任务实例只能是一个任务的运行,因此认为与任务实例之间是一对多的映射关系.

规则 1 U 与 R 的关系(URA)是 $n:n$ 的关系,如果 $F(U_i) = R_i$,则用户 U_i 被指派了角色 R_i .

规则 2 T 与 R 的关系(TRA)是 $n:n$ 的关系,如果 $G(T_i) = R_i$,则任务 T_i 被指派了角色 R_i ,即表示角色 R_i 可以执行任务 T_i .

规则 3 P 与 T 的关系(PTA)是 $n:n$ 的关系,如果 $H(T_i) = P_i$,则任务 T_i 拥有权限 P_i ,PTA 指定要完成某些任务所需要的最小权限集,即完成任务时至少要对资源对象进行那些操作.

规则 4 TI 与 R 的关系(TIRA):表示任务实例与角色之间的关系,任务实例可以由哪些角色来执行,要通过 TRA、任务与任务实例的映射关系以及任务上下文来共同决定.

规则 5 P 与 TI 的关系(PTIRA):表示任务实例与权限之间的关系,任务实例的权限集,要根据 PTA、任务与任务实例之间映射关系以及执行任务上下文来共同决定.

2.3 T_RBAC 模型访问控制

系统中的用户通过角色分配成不同的用户组,角色之间可以根据角色的约束关系相互继承,角色反映了企业的机构组织关系,每种角色都有自己特定的权限集合.用户通过建立会话获得自身所拥有

的角色,一个用户可以建立多个会话,但是一个会话只能服务于一个用户,用户只有在会话中才是有效的。

workflows的状态决定了当前的任务,以及该状态下任务所应具有 的权限和可访问的资源. 当任务的执行条件满足时,会处于执行态,这时任务被实例化成一个任务实例,并将相应的权限赋给任务,通过消息驱动机制将任务分配给会话中相应的用户,同时也将权限赋给满足条件的用户. 如果该用户对对应的角色集合中有相应的权限,该用户就可以执行相应的任务. 随着任务的完成,该权限也从该用户中移除. 在整个过程中,执行权限不再与角色相关,而必须通过任务才能与角色关联起来. 这时权限也不再表示操作与任务,只是单纯地表示对数据对象的访问操作。

3 T_RBAC 模型在 CSCW 系统中的应用

为了分析模型的可行性,将模型应用于计算机协同管理系统(CSCW 系统)中. 该系统采用了工作流技术,将企业的日常工作转化成了电子化的工作流程,提供了工作效率,并且通过 T_RBAC 模型在该系统中的应用,保证了系统的信息安全性。

CSCW 系统采用三层体系结构设计思想. 可以分成应用层、业务逻辑层和数据层. 在应用层包括了权限管理、应用程序客户端、流程管理等工具;在业务逻辑层主要包括邮件及短消息管理服务器、访问控制服务器、流程定义服务器、工作流引擎等模块功能;在数据层主要是包括了支持上述操作的数据库服务器。

图 2 描述了本文系统的访问控制框架,其中的访问控制服务器是本系统安全框架的核心模块,它控制着权限的动态分配与移除,授权约束的检查等,它和工作流引擎共同控制任务的激活以及状态的变化。

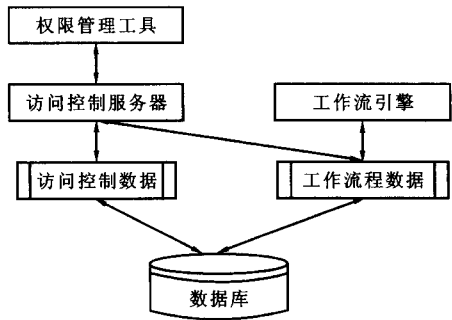


图 2 CSCW 系统的访问控制框架

系统主要由以下几个数据表组成:用户信息表、角色信息表、权限信息表、用户角色信息表、任务权限表、用户任务表、授权约束表、角色互斥表、任务信息表等,这些数据表通过访问控制服务器管理与维护,控制着整个协同管理系统的访问安全性。

系统访问控制的逻辑执行顺序如图 3 所示,首先用户启动应用程序,输入用户 ID、密码登录系统,访问控制服务器会根据输入的内容判断用户身份的合法性,如果不合法直接退出,否则查询用户角色集合,获得用户所具有的静态角色集合,并根据所具有的角色控制用户所具有的功能菜单项,最后登录系统,在信息表中为该用户创建一个会话。

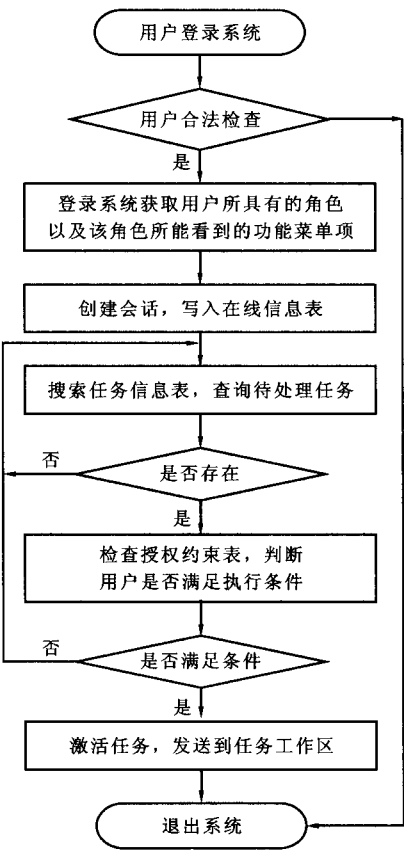


图 3 系统访问控制的逻辑执行顺序图

当用户登录系统创建会话后,访问控制服务器根据在线用户的 ID 查询任务信息表,获取与该用户 ID 相关的待处理任务,如果有与之相关的待处理任务,查询任务权限表,以及授权约束表获取执行该任务的角色以及该任务的约束关系等信息,并判断用户是否有执行该任务的权限,如果通过,激活用户执行该任务的最小权限,将该任务转换成有效状态,提交到邮件及短消息服务器,发送到相关用户的工作区中,同时启动任务的生命周期。

对于 workflow 中的任务由 workflow 引擎根据 workflow 的流程模型按照一定的逻辑顺序自动执行,当轮到某个任务执行时,就会自动的将任务放到任务信息表中,该任务的状态信息以及所需的最小权限信息和其他相关的信息也会被记录到任务信息表中,当条件满足时就会将激活任务发送到相关人员的工作区中。

根据任务状态,按 workflow 流转. 当用户接到任务后,就有了执行该任务的权限. 这时任务的生命周期也开始启动,当任务完成或是生命周期结束都会改变任务的状态,使其挂起或是处于终止状态,这时访问控制服务器会移除用户所具有的权限,在任务信息表中改变任务的状态,根据任务的流程信息表查找下一个待处理的任务。

下面是一种动态授权的算法描述:

```
//返回值为 true 表示授权成功,否则授权失败
Bool Authorization(userID,taskID,roleID)
{
    //根据任务的 ID 查询该任务的约束关系以及
    //生命周期
    time=getLifeCycle(taskID);
    checkCondition=getRestrictCondition(taskID);
    //判断该用户满足的角色集合是否满足约束关系
    Bool isFill
    isFill=checkCondition(userID,roleID, heckCondition);
    if(isFill==true)
    {
        //获取该任务的最小权限
        minPermission=getTaskPermission(taskID);
        //激活该用户的角色集合的相应权限
        ActivePermission (roleID, userID, minPermission);
        //启动任务的生命周期
        StartLifeCycle(lifetime, roleID,taskID);
        return true;
    }
    else
        return false;
}
```

4 结束语

本文分析评价了基于角色的访问控制模型(RBAC)和基于任务的访问控制模型(TBAC),结合这两种模型的优点,提出了基于 T_RBAC 的 CSCW 系统访问控制模型. 该模型将权限的粒度细粒化到任务以及,有效保证了最小特权原则;将 workflow 的外部状态引入到访问控制模型中,与任务的内部状态共同作用,控制任务权限的分配,满足了 CSCW 系统协同工作的特点. 通过对系统实际运行情况分析,证明了改进模型的可行性。

参考文献:

- [1] Roshan K, Sandhu R S. Conceptual foundations for a model of task-based authorizations[C]// Proceedings of IEEE Computer Security Foundations Workshop (CSFW) 1994. Franconia, NH, USA; IEEE, 1994: 66-79.
- [2] Ferraiolo D, Kuhn R. Role-based access controls[C]// Proceedings of the 15th NIST-NCSC National Computer Security Conference. Baltimore, Maryland: NIST-NCSS, 1992: 554-563.
- [3] Barkley J F, Cincotta A V, Ferraiolo D F, et al. Role-based access control for the World Wide Web[C]// 20th National Information System Security Conference. Baltimore, MD: NIST/NSA. 1997.
- [4] 罗养霞, 冯健, 陈晓江, 等. 基于任务角色访问控制的数据版权管理模型[J]. 计算机应用与软件, 2008, 25(7): 51-52.
- [5] 姚婷, 胡业发. 制造企业内容管理系统中基于角色和任务访问控制的研究 [J]. 计算机应用研究, 2008, 25(12): 3575-3577.

作者简介:

梁泽梅 女, (1986-), 硕士研究生. 研究方向为计算机软件与理论.

李蜀瑜 男, (1979-), 副教授. 研究方向为嵌入式系统、中间件技术.