基于角色访问控制的协同办公系统设计与实现

路 川,胡欣杰,纪 锋
(装备指挥技术学院 信息装备系,北京 101416)

摘 要:介绍了基于角色访问控制模型(RBAC),给出了RBAC96中用户、权限、角色、会话集及角色的层次、授权等之间的关系。基于RBAC96设计并实现了协同办公系统,给出了该系统的功能模块、技术路线和实现方法。重点论述了本系统实现过程中的权限列表和角色列表的创建方法、协同办公中的访问控制特点及实现方法、权限控制子系统应用层开发流程等关键问题,提出了权限控制子系统服务器端三层B/S结构设计方法,解决了协同办公中的访问控制问题。实现协同办公系统所采用的方法和技术路线具有通用性。

关键词:基于角色的访问控制;协同办公;角色;权限
中图分类号:TP317.1 **文献标识码**:A **文章编号**:1673-629X(2010)03-0230-04

Design and Implementation for Cooperation Office System Based on Role-Based Access Control

LU Chuan, HU Xin-jie, JI Feng
(Department of Information and Equipment, Academy of Equipment Command & Technology, Beijing 101416, China)

Abstract: Introduces a role-based access control model(RBAC). It introduces relation about user, permission, role, conversation , levels and accredit of role in RBAC96. Proposes design and implementation of OA based on it. Then give the system's functional modules, technology path and method. And discuss some key issuses of the access control: the permissions list and the role of list creation, access control in the coordination office, the application-layer development process of access control subsystem. At last, provide an access control subsystem server-side B/S structural design . It is commonality about the methods and techniques used in this paper.

Key words: role-based access control; cooperation office; role; permission

0 引 言

在计算机技术、网络技术迅速发展的今天,使用计算机进行网上协同办公变得更加普及,协同办公系统正越来越多地应用到日常事务处理和办公中。由于协同办公信息的安全、保密的需求,协同办公系统中的权限管理也就成为开发人员必须解决的难题,基于角色权限的访问控制提供了一种新颖的权限管理实现方式。

在基于角色访问控制中,权限和角色相关,用户通过饰演不同的角色获得角色所拥有的系统访问许可权。这不仅简化了系统权限的管理,而且为系统提供了必要的安全性能。

收稿日期:2009-03-24;**修回日期**:2009-09-03
基金项目:军队重点项目(2007ky003).获全军三等奖
作者简介:路 川(1963-),男,硕士,教授,从事计算机网络、信息管理系统等教学和科研工作;胡欣杰,教授,从事信息管理系统、装备信息系统等科研和教学工作。

1 基于角色的访问控制

访问控制是实施允许被授权的主体对某些客体的访问,同时拒绝向非授权的主体提供服务的策略。其中有自主访问控制(DAC);强制访问控制(MAC);基于角色的访问控制(RBAC)三种类型[1,2]。

在RBAC中,角色是实现访问控制策略的基本语义实体。系统管理员根据职能或机构的需求策略来创建角色、为角色分配权限和为用户分配角色等。RBAC的核心思想是将权限同角色关联起来,而用户的授权则通过赋予相应的角色来完成,用户所能访问的权限就由该用户所拥有的所有角色的权限集合的并集决定。角色之间有继承、限制等逻辑关系,并通过这些关系影响用户和权限的实际对应。在实际应用中,根据单位不同工作的职能可以创建不同的角色,每个角色代表一个独立的访问权限实体。在建立了这些角色的基础上根据用户的职能分配相应的权限,这样用户的访问权限就通过被授予角色的权限来体现。当单位的

组织机构权限发生变动时,可以很灵活地将该用户从一个角色移到另一个角色来实现权限的协调转换,降低了管理的复杂度,而且这些操作对用户完全透明。因此 RBAC 的访问方式具有灵活性和易操作性。

RBAC 独立于其他安全手段,系统灵活而且低冗余,并且可以实现多管理员协同管理。RBAC 模型的用户、权限、角色、会话集、角色层次、角色权限设置、用户角色授权之间的关系如图 1 所示。

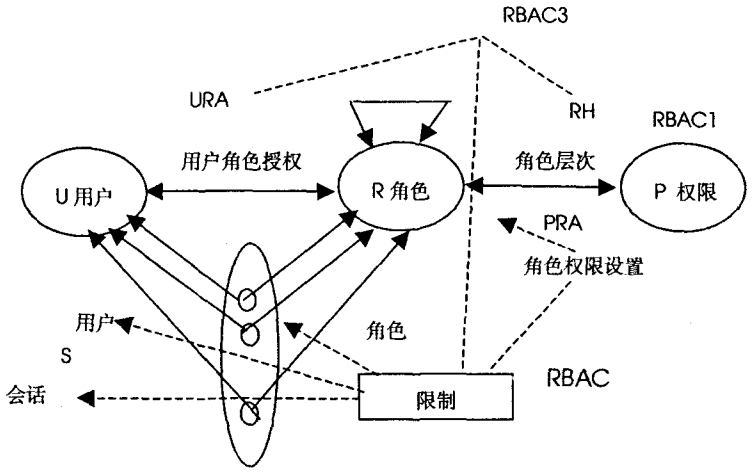

图 1　基于角色的访问控制模型(RBAC96)

图 1 中一个会期代表某段期间使用者和角色间的一个对映关系。使用者先透过建立的会期(可以不只一个)对映至角色上,而角色再对映到事先被授权的权限上,这些对映要满足使用者、角色、角色阶层间的限制[3,4]。

RBAC 支持三种安全规范:最少的授权;权责区分;数据抽象化。

2　协同办公系统的设计与实现

2.1　协同办公系统软件框架

目前常用三种方式建设办公自动化系统:

(1)采用 IBM LOTUS NOTES 作为软件平台,利用 NOTES 强大的邮件功能实现办公自动化的功能,缺点是在客户端必须采用自己的平台;

(2)采用 Microsoft Exchange Server 作为软件平台,客户端可以直接采用 Outlook 和 IE;

(3)采用数据库的方式,直接传递信息。

NOTES 和 Exchange 的编程方便,流程定义易于实现,用户界面友好。但是两者的数据存储均采用一个大的文档数据库,如果要求把办公自动化中某些数据提取出来并保存到协同办公管理系统中时,在软件开发上增加了较大难度。采用数据库方式建立办公自动化系统,不仅数据随时可以和其他业务系统相关联,并且易于管理。采用数据库方式还可以方便地和其他模块结合起来,建设企事业内部信息平台。

协同办公系统在体系结构上可分为:集中式、分布式和混合式,在实现方式上分为 C/S 结构和 B/S 结构。B/S 模式随着 Internet 的发展,已经成为了企事业信息系统建设的首选。文中所设计的协同办公系统采用 SQLServer 数据库管理方式,基于 B/S 结构。系统的总体逻辑架构如图 2 所示。

该协同办公系统采用多层架构,分为接入层、展现层、业务层和基础设施层四层。

(1)接入层:系统用户使用专用的 PC 终端设备与外网连接,通过授权用户登入协同办公平台的门户网站,实现对系统的个性化访问。

(2)展现层:提供一个内部信息交互及所有业务系统的统一展现入口。实现展现、认证授权、用户管理三大类服务。

(3)业务层:又可分为基础信息服务和应用业务服务两个层次。其中基础信息服务层一般不独立存在,而作为一些应用业务的底层支撑,如流程管理、信息整合等;而应用业务服务层则直接提供给用户具体的应用,如公文流转、信息管理、个人办公等。

(4)基础设施层:包括基础网络及硬件设施等,保证协同办公系统的正常运行和访问。此外,本协同办公系统还包括贯穿各个层次的系统及安全管理和接口管理。

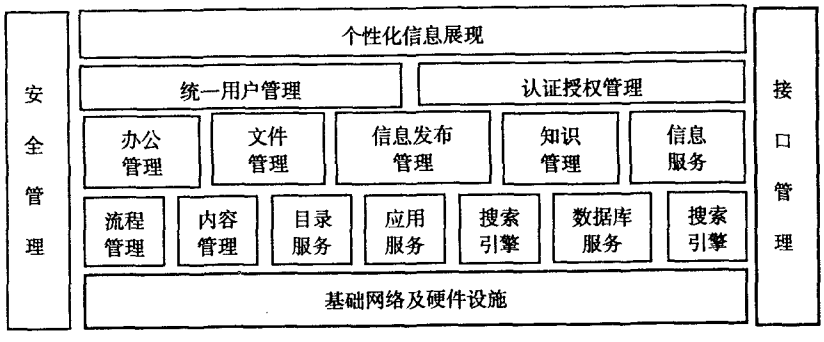

图 2　协同办公系统软件架构

2.2　主要功能模块

协同办公系统由系统管理、个人办公、协同办公、实用链接四个模块组成,每个模块下又有若干子模块,如图 3 所示。

系统中用户的定义采用 RBAC 原理,首先定义网站功能权限,然后根据权限定义出相应的角色和组,最

后将为创建的用户分配角色，使得用户在分配权限时效率高，操作简便。图 4 是该系统创建的角色列表和权限列表，并给出了“系统管理”角色所拥有的权限(权限列表中带有√部分)。

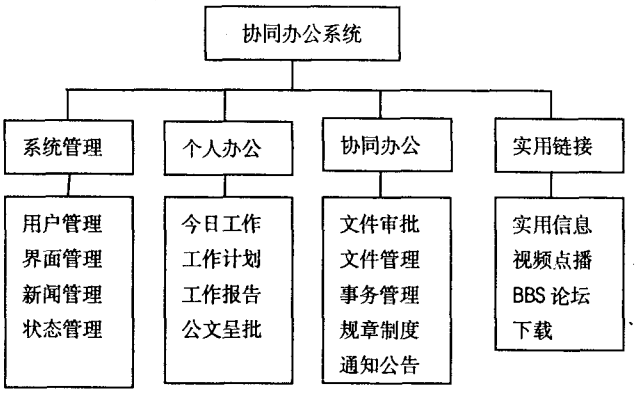

图 3 系统主要功能结构图

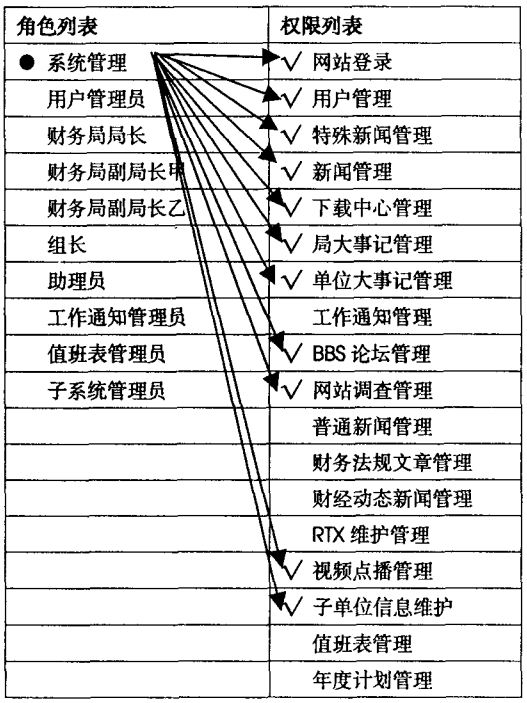

图 4 权限列表和角色列表

在图 4 中利用角色，将用户和权限进行了绑定，使得用户对应的权限一目了然，维护管理起来也很方便。

使用用户权限工具的方法一般为创建权限列表，创建角色列表，为角色绑定权限功能，创建功能用户组(组可以绑定一个或多个角色)，创建用户，将用户指派到相应的功能用户组中，以完成用户与权限的绑定操作。

2.3 协同办公中的访问控制

访问控制模块用于控制用户进入其他各个子系统和控制用户进入子系统后对数据的操作，如查询、修改数据等。具体功能包括：用户注册、建立新用户、修改权限、查看权限等。对协同办公系统的访问先通过访问控制模块，然后才能进入其他相应模块。协同办公的活动表现为办公数据的创建、发放和更改。它的实施涉及不同管理权限的人员。每个人员分别参与日常办公具体实施的某个或者某几个或全部过程，不同的人拥有不同的访问权限[5]。

协同设计中的数据以电子文件形式在网上传输，访问控制要求能够实现根据系统人员所承担的不同职责，分别赋予不同的数据访问权利，处理不同范围的资料。同时还要保证数据在权限许可的范围内，随时可以把正确的资料送到需要该资料的人员，实现数据共享。

一般的访问控制需要解决 3 个问题：

身份鉴别，即识别与确认访问系统的用户；

权限分配，即决定该用户对系统资源的访问级别；

操作过程监控，即用某种方法监控用户的动作，控制对资源的访问[6]。

协同办公中的访问控制具有如下特点：

(1)角色划分和权限分配决定于任务小组和任务关联。参与协同办公的人员分为不同的用户组，负责工作的不同节点。他们之间的协同既有小组内部的，也有小组间的。因此对办公数据的访问权限将由用户组的划分和任务关联情况来决定。

(2)角色划分和权限分配具有多级性。由于协同任务可以划分为多个小组，而这些小组又可以往下划分若干级，形成任务树，任务划分的多级性决定了角色权限的多级性。

(3)系统存在特权用户。

(4)权限存在动态性。协同办公中的 1 个用户可以有多个角色，而 1 个角色也可以分配给多个用户。

随着协同办公事务的变化，系统中将出现用户的增减和调度，用户角色的变化，被保护数据安全级的改变等动态事件，访问控制要求能适应这些变化。

2.4 权限控制子系统服务器端结构设计

采用三层 B/S 结构(如图 5 所示)，将应用功能分成表示层、功能层和数据层三部分。这三层进行明确分割，并在逻辑上使其独立[6]。

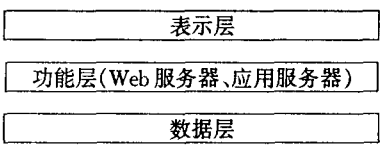

图 5 三层 B/S 结构

(1)表示层。表示层是应用的用户接口部分，负责用户与应用间的对话，检查用户从键盘等输入的数据，显示输出数据。表示层采用客户端的 Web 浏览器，浏览器负责接收、解释并显示服务器端发送的 HTML 代

码,实现用户与服务器的信息显示、信息交互。

(2)功能层。功能层实现具体的业务处理。可以将整个应用逻辑驻留其上。Web服务器既作为一个浏览服务器,又作为一个应用服务器。浏览服务器向客户浏览器提供WWW网页下载服务,而具体提供给用户的网页内容由应用层动态生成。本系统的开发平台选用Microsoft公司的.Net平台,为了保证系统的稳定性,采用IIS作为Web服务器。

功能层实现具体的业务处理,实现的主要功能有:

* 处理用户浏览器发送的请求,动态生成HTML语句提供给WWW服务器;

* 用户身份验证与传输加密,角色赋予,权限检验,约束控制,会话管理;

* 向数据库服务器发送SQL数据库查询语句并且接收、处理查询结果。

(3)数据层。数据层就是数据库管理系统DBMS,负责维护和管理数据库,解释并执行从功能层发送来的对数据的查询、更新和删除操作命令。数据库管理系统必须能够迅速地执行大量数据的更新和检索。从功能层传送到数据层使用SQL语言。本系统出于条件限制,功能层和数据层用同一PC实现。

在数据层维护的主要数据有:

用户基本注册信息;

各等级规则角色、管理角色、权限的基本信息;

角色-权限分配;

用户-角色分配;

角色继承关系信息。

2.5 权限控制子系统应用层开发流程

在本系统中实现基于角色访问控制的Web应用,采用.Net技术在Web服务器上构建应用层,来实现WWW访问的基于角色访问控制的关键业务逻辑,包括用户身份验证,角色分配,动态约束访问控制,权限分配与校验等动态RBAC访问控制功能。

其应用层工作流程为[7,8]:

(1)用户根据自己的权限使用帐号登录。向身份认证服务器用加密方式提送用户/密码对,身份认证服务器查询用户密码数据库信息,印证密码是否符合。

(2)若密码符合,动态约束器DCS向数据库查询该用户的动态约束信息(包括时间约束和来源位置约束),计算出对应这次会话的用户UDCMa。

(3)访问控制器ACS向数据库查询该用户的用户/角色信息和角色/权限信息、角色动态约束信息,生成该用户权限的最大值的权限标志码。询问动态约束器DCS得到UDCM,把该用户权限的最大值的权限标志码与UDCM进行与运算得到访问控制掩码ACM。再根据ACM得到访问权限描述对象。

(4)该访问权限描述对象作为会话属性被赋予当前会话。

(5)用户提出一个访问/操作请求,访问过滤器AFS根据访问权限描述对象判断是否允许,若允许,把该请示传送给应用服务器处理,并接收应用器根据处理结果生成的动态HTML网页传给用户,在用户的浏览器上显示。

(6)如果用户当前角色是管理角色,可以远程在浏览器上通过访问应用服务器查询、更改用户/角色信息库、角色/权限信息库、动态约束信息库实现远程管理。Web应用程序根据该管理角色当前的可执行权限动态定制管理界面。

3 结束语

系统实现了基于角色的安全访问控制协同办公系统,对系统权限进行了细致的划分,并创建了相应的角色,为每位用户绑定了相应的若干个角色。可使用第三方工作流图形描述软件,生成了适合本单位实际工作状况的工作流模型,并与系统进行了较好的结合,完成了协同工作的目的。

建立了授权灵活、发布便捷的信息发布平台,便于用户之间信息的交流和领导掌握单位工作状况,通过一定的统计处理,使得用户积极主动发布信息,起到了很好的效果。

参考文献:

[1] Ferraiolo D, Cugini J, Kuhn R. Role Based Access Control: Features and Motivations[C]//In Computer Security Applications Conference. [s.l.]:[s.n.],1995:81-85.

[2] Park J S, Sandhu R S. Role-Based Access Control on the Web[J]. ACM Transactions on Information and System Security,2001,4(1):37-71.

[3] 李　仲,杨宗凯,刘　威.一种基于RBAC的实现动态权限管理的方法[J].计算机技术与发展,2006,16(10):1-4.

[4] 邹　晓.基于角色的访问控制模型分析与实现[J].微计算机信息,2006,22(6-3):108-110.

[5] 汪厚祥,李　卉,邱志明.一种RBAC组图模型研究[J].计算机工程与设计,2005,26(11):2972-2974.

[6] 张晓群,董丽丽.角色访问控制模型的研究及应用[J].计算机技术与发展,2007,17(2):42-45.

[7] 郑　刚.一种基于工作流的协同办公系统的设计[J].计算机技术与发展,2007,17(1):24-26.

[8] 李　向,郭晓兰,严　烨.基于角色的Web系统安全策略研究[J].计算机技术与发展,2006,16(10):155-156.