RBAC 在网络管理上的应用

杜诗军，王瑞民，周清雷
（郑州大学 信息工程学院，河南 郑州 450001）

摘 要：基于角色的访问控制(RBAC)是一种方便、安全、高效的访问控制机制。通过分析 RBAC 的模型特点及应用优势，结合著名的 MikroTik RouterOS 路由软件和教学实际情况，对网络管理进行了改进，给出了基于角色的网络访问控制方案。引入角色这个中间桥梁，使权限与角色对应，角色与用户对应。将角色在应用层面上定义，使访问粒度更细、安全性加强。经使用，此方案更具有方便性和安全性。

关键词：基于角色的访问控制；角色；权限
中图分类号：TP393.07　　**文献标识码**：A　　**文章编号**：1673－629X(2007)03－0166－03

Application of RBAC to Administration of Networks

DU Shi-jun, WANG Rui-min, ZHOU Qing-lei
(College of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: RBAC (role based access control) as a convenient, safe and efficient mechanism has proved high flexibility and safety, which by analyzing features of RBAC and its application advantages, combining well－known MikroTik RouterOS and teaching practices, improves network management and offers RBAC solution. By introducing roles as medium, produces an agreement between roles and users, by defining roles at application lever, gets more intensive accessing granularity and reinforced safety.

Key words: RBAC; role; permission

0 引 言

访问控制是防止非法用户使用系统和控制合法用户越权使用系统的重要屏障，经历了自主访问控制(DAC)、强制访问控制(MAC)、基于角色的访问控制(RBAC)等发展阶段。由于 RBAC 中引入了与组织机构中的职务相对应的“角色”，实现了用户与权限的逻辑分离，用通过成为角色的成员而获得相应权限，与自主访问控制和强制访问控制相比，方便了授权管理[1,2]。目前许多组织机构都采用基于角色的访问控制策略。

1 基于角色的访问控制概述

Sandhu 等人给出了 RBAC 模型的一个比较完整的框架[1]，即 RBAC96 模型。经过 10 多年的发展，RBAC 本身的研究已日趋成熟，2004 年初 RBAC 已成为 ANSI 标准[3]。2006 年 1 月开始制定基于角色的访问控制执行标准草案[4]。

收稿日期：2006－06－20
作者简介：杜诗军(1962－)，女，河南郑州人，高工，研究方向为网络安全。

RBAC 的基本思想是，角色是权限的集合，用户通过角色的分配来获得权限。通过用户、角色、权限之间的多对多指派，实现或修改访问控制策略。当用户的职责变化时，只需改变其角色也就改变了用户的权限，简化了权限管理。RBAC 支持的基本安全原则有：最小特权原则，责任分离原则，数据抽象原则。

(1)最小特权原则就是用户所拥有的权限不能超过其工作时所需的权限。在配置角色和权限关系时，仅将执行任务时需要的权限指派给角色。有针对性地按照具体要求定义相应的角色并给用户分配合适的角色，可防止给用户赋予过高的访问权限，提高了系统的安全性。

(2)责任分离原则是对有冲突的角色进行约束。它有两种实现方式：一种是静态分离，在用户到角色的指派中，把互斥的角色指派给不同的用户；另一种是动态分离，在用户建立会话时来决定激活哪些角色。

(3)数据抽象原则是在权限划分时，并不直接定义读、写、执行等权限，而是在应用层面上定义。在具体系统中这些抽象的权限会被赋予实际的含义[5]。

RBAC 的基本结构[3]如图 1 所示。

RBAC 突出的优点在于系统管理员能够按照部门

的安全策略划分不同的角色并将角色分配相应的权限,执行特定的任务。一个 RBAC 系统建立后主要的管理工作是分配或取消用户的角色。用户职责变化时只需要改变角色即可改变其权限,当组织的功能变化时,则只需删除角色的旧功能,增加新功能,或定义新角色,而不必更新每一个用户的权限设置。从而简化了授权管理并能更好地适应特定单位的安全策略。

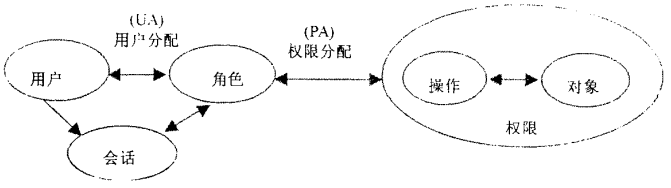

图 1　RBAC 的基本结构

RBAC 另一优势体现在为系统管理员提供了一种比较抽象的、与通常组织管理相类似的访问控制层次。通过定义、建立不同的角色、角色之间的联系以及相应的限制,管理员可动态或静态地规范用户的行为。

2　RBAC 在网络管理系统中的应用

2.1　系统应用背景

计算机实验室有一台教师机和一百多台学生用机,各实验室划分成 VLAN。各实验室交换机汇聚在一台交换机上通过路由软件联通外网,管理机与教师机网络畅通。所有机器上网通过 MikroTik RouterOS 路由软件,该软件能对网络访问进行有效的管理。该路由为用户指派一用户组,组策略是由单个策略项目组合而成,策略项目有:

read – policy that grants read access to the router's configuration. All console commands that do not alter router's configuration are allowed. 对路由器的配置有阅读权,没有改写权。

write – policy that grants write access to the router's configuration, except for user management. This policy does not allow to read the configuration, so make sure to enable read policy as well. 除对用户管理项外,对路由器的配置有写权限。这个策略不允许阅读配置,所以最好要确定能够读的策略。

telnet – policy that grants rights to log in remotely via telnet. 取得 telnet 远程登录操作的权力。

……

并有 full,read,write 三个组不能删除:

0 name = "read" policy = local, telnet, ssh, reboot, read, test, winbox, password, web, ! ftp, ! write, ! policy

1 name = "write" policy = local, telnet, ssh, reboot, read, write, test, winbox, password, web, ! ftp, ! policy

2 name = "full" policy = local, telnet, ssh, ftp, reboot, read, write, policy, test, winbox, password, web

从上述内容易见,该系统要修改路由内容必须具有读、写权限。而这里的写权限太强,不适合实际工作需要。比如在实际工作中仅要对某一项配置进行修改,例:enable 第三实验室网络,而不具有对其它实验室功能项目的添加、改写、删除等权限,而系统对所有具有写权限的用户都一视同仁,并不区分操作的具体对象实例,即粒度太粗。要实现细粒度需对该系统进行改进,将写权限根据需要进一步细化,在考虑粗粒度的对象类别之后再考虑特定实例,因此采用在权限与用户之间添加角色的方法来实现,使权限与角色对应,角色与用户对应。角色在应用层面上定义,将这些抽象的细化的权限赋予实际的含义,用基于角色的访问控制机制加上具体任务来实现较合适。

2.2　策略制定与实现

在实验教学中主要涉及的对象有教务、教师、教辅、学生,这些对应应各负其责:教务员制定班级上实验课时间、地点课表并检查执行情况,实验室教辅人员对各上课用实验室有管理权,教师具有在课内管理所代班级学生及课内学生所在实验室的部分管理权限,课内学生具有使用设备权限。实验室网络访问控制由系统管理员制定,构造如图 2 所示。这样无论是哪个代课教师,只要在其上课期间,通过教师机登录,即可获得教师角色。这里的约束不仅是物理位置还包括时间,引入时间特性主要体现在会话的建立和撤销特性上[6]。

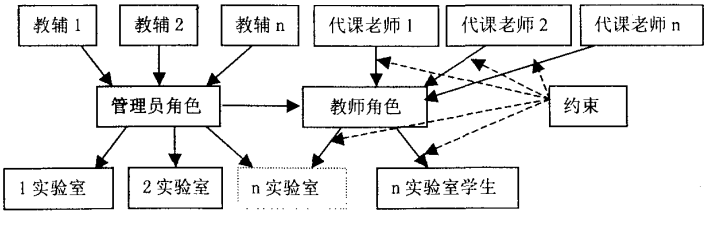

图 2　RBAC 的实现构造图

对实验室网络访问的控制,上课期间各实验室代课老师通过应用界面登录获取教师角色,根据上课内容控制管理本实验室学生机器对网络的访问与禁止。老师输入用户名及口令,系统根据用户名及口令的正确性判断此用户所属的角色,打开相应可操作界面,即具有对此实验室网络的访问控制权,如图 3 所示,而实验室教辅人员不受时间与实验室的约束,具有同时管

理多个实验室对网络访问的权限。

在此系统中,角色作为一个桥梁,沟通于用户和资源之间。对用户的访问授权转为对角色的授权,然后再将用户与特定角色联系起来。用户只有通过角色才享有该角色所对应的权限,从而访问相应的客体。一个角色也可以被赋予多个用户,一个用户也可以被赋予多个角色。同样,一个角色可以拥有多项权限,一个权限可以分配给多个角色。角色的权限即为角色所拥有的功能,表现为对某一菜单项可执行功能。

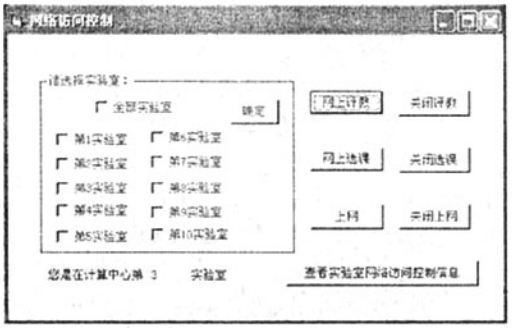

图 3 教师角色网络访问控制管理界面

2.3 系统改进前后的比较

原有系统是通过 winbox 界面操作,如图 4 所示。对每个机房学生机及教师机的网络访问是由系统管理员集中控制管理,而代课教师不能控制他所在的机房学生对网络的访问。若教师具有读写权限,虽然方便但安全方面不能保障,尤其是上课老师多,无意的误操作会影响后续实验课,严重危及网络安全,造成系统不必要的损失。根据实际需求增加了角色概念后,将权限细化、具体化,教师角色不但可通过界面浏览全部实验室网络情况(如图 4 右边)且仅能通过本实验室的教师机控制其所代学生的机器访问网络(如图 3),而不会危及其它,安全有保障。教师不论在哪个实验室,只要在教师机上登录,通过教师角色即可实现对本实验室的学生机的网络控制。此方案减少了用户无意中危害系统安全的可能,增加了安全性,避免了因误操作而造成的网络控制系统错误。

对新来老师,只需将其添加到教师角色中即可拥有教师权限,而某一教师调换岗位,只需将其角色改变即可,操作方便。

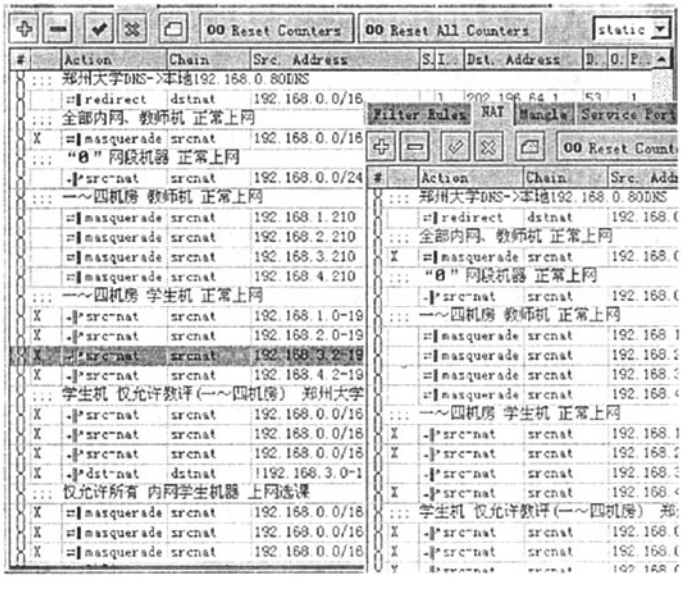

图 4 具有读写权限和浏览权限操作界面

3 结束语

RBAC 为内部网络环境提供了使用基于角色访问控制机制的优势,甚至在改善系统的过程中,可以不改动原有代码而只需加入新的 RBAC 机制来完善现有系统[7]。

在改善本系统的过程中还存在不足,它与原有系统的连接是通过 telnet,虽然现在只允许通过内网的教师机来控制,但安全性及灵活性是将来要进行改进的地方。

参考文献:

[1] Sandhu R, Coyne E J, Feinstein H L, et al. Role - Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38 - 47.

[2] 洪 帆,黎成兵. 多域结盟环境下基于角色的访问控制[J]. 计算机工程与科学, 2005, 27(6): 1 - 3.

[3] American National Standard for Information Technology - Role Based Access Control[EB/OL]. 2003. http://csrc.nist.gov/rbac/rbac - std - ncits, 2003.

[4] Coyne E. New Draft RBAC Implementation Standard [EB/OL]. 2006 - 04. http://csrc.nist.gov/rbac.

[5] 洪 帆,邓 磊. 工作流管理系统中基于角色的访问控制[J]. 华中科技大学学报:自然科学版, 2003, 31(12): 1 - 3.

[6] 董光宇,卿斯汉,刘克龙. 带时间特性的角色授权约束[J]. 软件学报, 2002, 13(8): 1521 - 1527.

[7] 汪厚祥, 李 卉. 基于角色的访问控制研究[J]. 计算机应用研究, 2005(4): 126 - 127.