基于角色的访问控制在网络教育中的应用研究*

杨宗凯，刘宏波，刘琴涛
(华中科技大学 电子与信息工程系，湖北 武汉 430074)

摘 要：基于角色的访问控制(RBAC)作为一种安全机制，是当前研究的热点之一。如何根据网络教育的特点应用 RBAC 是当前网络教育的重点和难点。在分析了 RBAC96 模型的基础上，结合网络教育的特点进行系统设计，建立符合网络教育特色的新的权限管理模型，兼顾对个性权限的修改能力，最后给出该模型在网络教育中的系统实现，通过项目验证了 RBAC 在网络教育中的可行性。

关键词：网络教育；基于角色的访问控制；访问控制
中图法分类号：TP309.2 文献标识码：A 文章编号：1001-3695(2005)10-0134-03

Application Research for Role Based Access Control Technique in E-Learning

YANG Zong-kai, LIU Hong-bo, LIU Qin-tao
(Dept. of Electronic & Information Engineering, Huazhong University of Science & Technology, Wuhan Hubei 430074, China)

Abstract: As a sort of security mechanism, Role Based Access Control(RBAC) technique has been one of the hotspots in current research. How to apply RBAC according to the characteristics of E-Learning application is a challenge work. Based upon the RBAC96 model, the paper builds a new permission manage model and relates to the ability of modifying individual permissions, achieving the system design by combining with the characteristic of E-Learning. Finally this paper gives the system realization in E-Learning for this model and certifies the feasibility for RBAC in E-Learning.

Key words: E-Learning; RBAC(Role Based Access Control); Access Control

1 引言

远程教育在中国发展到第三代称为现代远程教育，即网络教育。网络教育是以学习者为主体，建立在与教育传播理论、现代学习理论紧密结合的计算机、网络、多媒体和通信等技术基础上，以交互性、网络化、实时性、综合性和适应性等为基本特征的新型教育方式，是远程教育的新发展。网络教育以计算机网络技术为支撑，具有时空自由、资源共享、系统开放、便于协作等优点[1]。而这些特点决定了在网络教育中的访问控制问题是研究的重点和难点。

传统的强制访问控制(Mandatory Access Control, MAC)和自动访问控制(Discretionary Access Control, DAC)，是对系统中的所有用户进行一维的权限管理，它既不能有效地适应网络教育中的安全性要求，也不能快速地实现。而 20 世纪 90 年代以来出现的基于角色的访问控制(Role Based Access Control, RBAC)技术，被认为是有效地克服了传统的访问控制技术中的不足。本文以基于角色的基本思想和网络教育中的实际情况相结合为立足点，根据 RBAC 的研究成果，建立了符合网络教育特色的新的权限管理模型，通过网络教育的项目实践，验证 RBAC 在网络教育中的可行性。

收稿日期：2004-11-12；修返日期：2004-12-15
基金项目：武汉市中小企业创新基金项目(200316)；湖北华大网络教育技术有限责任公司华大远程教育平台联合资助项目(VAD2.0)

2 RBAC 基本模型和原理

(1) RBAC 的基本模型

在目前出现的模型中 RBAC96 模型由于系统和全面地描述了 RBAC 多层次、多方面的意义而得到广泛的认可[2]。RBAC 的基本模型结构图如图 1 所示。

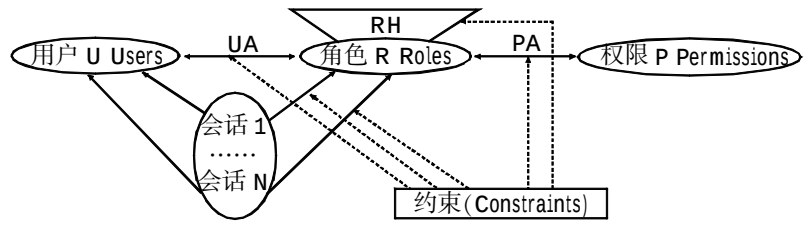

图 1 RBAC96 模型

形式化描述[3]如下：

U 表示用户集。
R 表示相应的一般角色集和管理角色集。
P 表示相应的一般权限集和管理权限集。
$UA \subseteq U \times R$ 是一个多对多的从用户到角色的授权关系集。
$PA \subseteq P \times R$ 是一个多对多的从角色到权限的授权关系集。
$RH \subseteq R \times R$ 是一个偏序的角色继承关系集。
S 表示会话集。

从图 1 中可以看出，RBAC 模型由四个实体组成，分别是：用户(U)、角色(R)、权限(P)，还有一组会话(S)。用户和角色之间，以及角色和权限之间用双箭头相连表示用户角色分配 UA 和角色权限分配 PA 关系都是多对多的关系。为了对系统资源进行访问，用户需要建立会话，每个会话 S 将一个用户与他所对应的角色的一部分建立映射关系，这一角色子集称为被会话激活的角色集，那么在这次会话中，用户可以执行的操作

就是该会话激活的角色集对应的权限所允许的操作。权限的粒度大小取决于实际系统的定义。

(2) RBAC 的核心思想

RBAC 的核心思想[3]是将访问权限和角色相联系,通过给用户分配合适的角色,让用户与访问权限相联系。在网络教育中,用户就是教师、学生和管理人员,角色是根据在教育中完成不同的教、学和管理任务需要而设置的,根据用户在网络教育中的职责和职权来设定他们的角色。用户可以在角色间进行转换,系统可以添加、删除和修改角色,还可以对角色的权限进行添加、删除和修改。这样通过应用 RBAC 将安全性放在一个接近组织结构的自然层面上进行管理,使网络教育的管理机制更符合现实教育系统的管理流程。

3　RBAC 在网络教育中的应用分析

(1) 网络教育的特点

在任何教学环境中,通常包含以下四个要素: 教师、学习者、通信系统或模式、讲授或学习的内容。在传统教学中教师和学习者处于同一时间、空间中,所以他们所采用的通信系统或模式通常是常规的口头讲授方式; 而在网络教育中,由于教师和学生在地点和时间上处于准永久的分离状态(即教与学的分离) 以及由此产生的心理上的分离,因此在网络教育中必须采用以技术手段为依托的双向通信系统或模式来弥合这种分离,使得教与学的行为得到再度综合。

随着现代信息技术的迅速发展,网络教育要满足人们对终身教育的发展要求,必须实现“五个任何”,即: 不受空间和时间的限制,任何人、在任何时间、任何地点、从任何章节开始、学习任何课程。而要实现这个目标,首先在通信系统或模式上,即在学习支持的服务系统上,要做好访问控制的工作,基于角色的访问控制(RBAC) 是一个比较好的解决方案。

(2) 网络教育系统设计及 RBAC 应用分析

笔者曾设计并实现一个网络教育平台,该平台的结构示意图如图 2 所示。

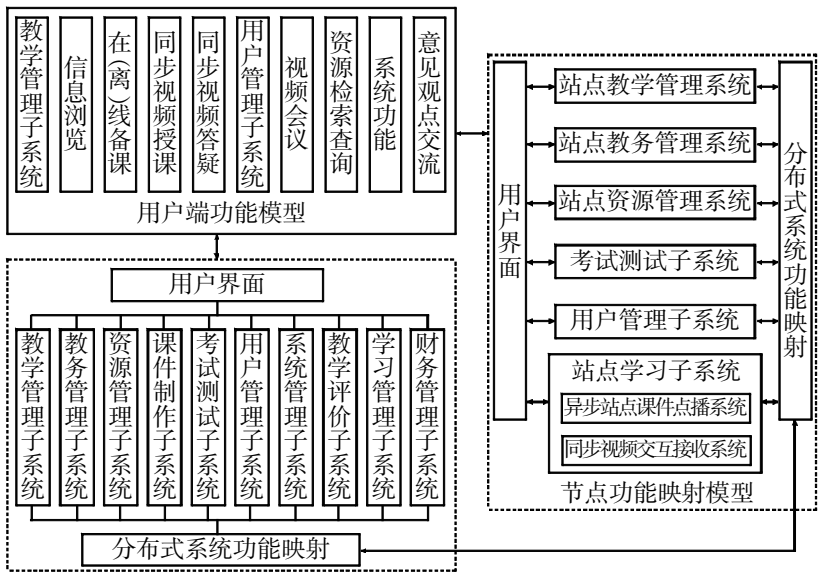

图 2　网络教育平台结构示意图

该平台是一个基于 J2EE 架构的符合国家 CELTS 标准的教育平台。该平台集网络课程开发、教育资源管理、网上教学支持与管理、网上教学评价与分析等功能于一体的开放式的网络教育集成应用环境和软件工具集合,总体上由学习和辅导系统、学习管理系统、教学评价系统、教务管理系统、教学管理系统、财务管理系统、考试测试系统、网络课程制作系统、教学资源管理系统、中央管理系统十大部分组成。由于功能不一样,数据对象相应的权限也不一样。根据网络教育的实际情况,满足自动化远程管理的需求,将平台分为三级(图 3) : 第一级为网校级,在这一级,设计一个具有最高权限的系统管理员,同时具有该角色的管理员创建下一级的管理员角色,并设定角色所能操作的数据库的范围和数据对象的权限(包括添加、修改、删除等) ,并将这些角色指派给用户; 第二级为班级级,在这一级,将班级设为管理角色,并制定该班级所具有的权力范围为相应的学生和老师,同时要求有班长和班主任角色,这个功能在后面将详细分析; 第三级为用户级,在这一级,包括学生和教师,定义学生和教师对其权利范围内的信息资源具有的相应操作权限。为了方便管理,引入用户组的概念。用户组就是用户的集合,例如学生组、教师组等。

下面以教师升为班主任为例,利用 RBAC 理论研究成果,详细分析一名教师所生成的个性化权限。通过权限矩阵,分析用户与其权限控制点之间的关系。

参考图 1,作如下定义:

M_{ur}表示用户和角色之间的关系。

M_{rp}表示角色和权限控制点之间的关系。

M'_{up}表示中间的用户和权限控制点之间的关系(简称中间用户 - 控制点矩阵) 。

$M_{sup\ a}$表示强制有权限矩阵。

$M_{sup\ m}$表示强制无权限矩阵。

M''_{up}表示用户和有权限控制点之间的关系(简称中间有权限用户 - 控制点矩阵) 。

M_{up}表示最终的用户和权限控制点之间的关系(简称最终用户 - 控制点矩阵) 。

教师通过对角色的继承关系,可以得到中间用户 - 控制点矩阵 M'_{up},则有

$$M'_{up} = M_{ur} \cdot M_{rp} \tag{1}$$

由网络教育系统的特点决定,一名教师所具有的权限是最基本的权限,当教师升为班主任的时候,该班主任角色所具有的权限控制矩阵,称为强制有权限矩阵 $M_{sup\ a}$,那么该教师所获得的权限是中间用户 - 控制点矩阵 M'_{up}和强制有权限矩阵 $M_{sup\ a}$进行按位或的关系,从而得到其中间有权限的用户 - 控制点权限 M''_{up}:

$$M''_{up} = M'_{up} \cdot M_{sup\ a} \tag{2}$$

由于管理员对该权限有最高的权限,称为强制无权限矩阵 $M_{sup\ m}$,所以中间有权限的用户 - 控制点权限 M''_{up}和强制无权限矩阵 $M_{sup\ m}$进行按位与的关系,从而得到其最终用户 - 控制点权限 M_{up}:

$$M_{up} = M''_{up} \cdot M_{sup\ m} \tag{3}$$

如果将该教师的最终控制权限矩阵 M_{up}表达成布尔矩阵[4],则为

$$M_{up} = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{pmatrix} \tag{4}$$

在这个布尔矩阵表达式中,P_{ij}等于 1 或者 0,代表第 i 个教师对第 j 个权限控制点的权限值,其中,1 代表该教师对该权限

控制点具有权限,0 则表示没有。这样,以布尔矩阵形式表示了一名教师升为班主任所获得的权限。

4 RBAC 在网络教育中的管理模型及系统实现

根据网络教育的实际需要,基于上述 RBAC 在网络教育平台中的应用分析,建立符合网络教育特色的基于角色的管理模型,如图 3 所示。

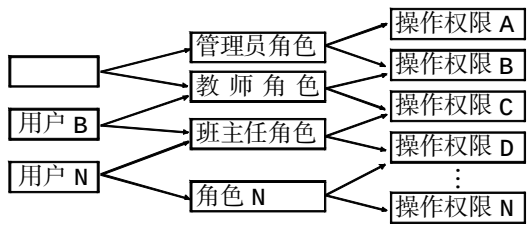

图 3 网络教育平台中基于角色角色的权限管理模

在模型中用户和角色的关联表示该用户拥有该角色所拥有的操作权限集,角色和操作权限的关联表示角色拥有该操作权限,角色之间的关联表示角色之间具有的继承关系。访问操作权限的分配由用户角色分配和角色操作权限分配组成。

在实际网络教育平台中,设置级别最高的系统管理员。由其控制整个系统的权力范围和创建管理角色,界定这些管理角色的管理范围和将相应的管理权限授予相应角色,这些管理角色具有下一级管理员的权利。创建用户并指派管理角色给相应的用户。

由于 RBAC 的实现在不同的系统中是不一样的,与实现的平台有关。例如在笔者的慧眼网络教育平台中,使用的操作系统是 Linux,服务器是 BEA 公司的 WebLogic 7.0,开发架构是基于 J2EE 分布式应用程序架构。下面以教师升为班主任的例子,介绍该模型在网络教育中的系统实现。

具体流程如下:当一名用户选择了“教师组”角色,则即可获得该角色的权限;如果将其升为班主任,将其选择“升级为班主任”,可以获得为这个班主任角色的权限,则这名用户获得的权限就是“教师组”权限和班主任权限的按位或的关系,称其为中间权限;当系统管理员对其某一具体权限做修改的时候,则这名用户获得的最终权限就是中间权限与这一具体权限的按位与的关系。实现的界面图如图 4 所示。

图 4 网络教育平台的实现界面图

在网络教育平台中,设定教师角色,获得教师角色权限和设定班主任角色,获得班主任角色权限,实现了基于角色的访问控制;同时根据网络教育中的实际情况,班主任是在教师中选定,具有教师的所有权限,同时具有班主任特殊的权限,所以设定班主任角色是教师角色权限和班主任角色权限的按位或的关系。而系统管理员具有权限的最终决定权,因此最终班主任角色的权限是上述权限与系统管理员指定权限的按位与的关系。这样基于角色的基本思想和网络教育中的实际情况相结合,实现了网络教育的实际情况。

5 结束语

面对网络教育中要管理的大量的、负责的权限,基于对象的访问控制(RBAC)提供了灵活的、动态的方法,RBAC 非常适合于网络教育系统中的权限管理。本文在 RBAC96 模型的基础上,结合网络教育的特点,建立了符合网络教育特色的新的权限管理模型,很好地管理了大量的权限,并且在自然层面上进行人性化管理,在实际的网络教育系统中,以教师升为班主任为例,从理论和实践上验证了该管理模型在网络教育中的可行性。目前,利用该权限管理模型研发生产的《华大网络教育平台 V2.0》,在华中师范大学网络教育学院等大专院校平稳运行,有近二万名使用者长期在这个平台上进行学习和从事教学、教学管理工作。在实际运行效果方面,整个平台易于管理和维护,取得了良好的经济效益和社会效应,充分显示了 RBAC 与网络教育结合的优势。

参考文献:

[1] 杨宗凯,吴砥,刘清堂. 网络教育标准与技术[M]. 北京:清华大学出版社,2003. 1-3.

[2] 夏志雄,张曙光. RBAC 在基于 Web 管理信息系统中的应用[J]. 计算机应用研究,2004,21(7):198-199.

[3] 李孟珂,余祥宣. 基于角色的访问控制技术及应用[J]. 计算机应用研究,2000,17(10):44-47.

[4] 李健,唐文忠. 角色访问控制技术在管理信息系统中的应用[J]. 北京航空航天大学学报,2003,(6):534-538.

作者简介:

杨宗凯(1963-),男,国家信息技术委员会教育技术分技术委员会(CELTS)委员,ISO/IEC JC1/SC36 /SP 联合主席,国家“十五”攻关网络教育关键技术及其示范工程专家组成员,教授,博士生导师,博士,主要研究方向为网络教育、电子商务、智能信号处理与应用、宽带网络通信技术;刘宏波(1979-),男,黑龙江省齐齐哈尔人,教师,硕士研究生,主要研究方向为网络教育;刘琴涛(1982-),女,四川省乐山人,硕士研究生,主要研究方向为信息处理。