Computer Science and Application 计算机科学与应用, 2016, 6(7), 399-405
Published Online July 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.67049

Hans汉斯

Role-Based Access Control Application in Campus Network Management System Research

Bingkun Pi[1], Chunxi Wang[2], Hongqiang Zhang[1], Cong Ma[1], Shuwen Wang[1*]

[1]School of Electrical Engineering, Northwest University for Nationalities, Lanzhou Gansu
[2]Zhengzhou Municipal Bureau of Meteorology, Zhengzhou Henan
Email: *shuwenwang@163.com

Received: Jul. 15th, 2016; accepted: Jul. 24th, 2016; published: Jul. 27th, 2016

Abstract

Access control has been an important guarantee information security. Role-Based Access Control (RBAC) is currently widely used as a research application access control model. To ensure the security of the data in the system, based on the distinction among the individual user's access to system as well as to the function of the system, this article proposes the security strategy which is consistent with the campus network organizational structure. It puts stress on the role-based user access control; and in the database, the role's access authority to every item in the data table applied to the Northwest University for Nationalities campus network is also increased. Thus a flexible and stable campus network environment is provided.

Keywords

Campus Network Management System, Access Control, Role, Database

基于角色的访问控制在校园网管理系统中的应用研究

皮炳坤[1]，王春喜[2]，张弘强[1]，马　聪[1]，王书文[1*]

*通讯作者。

文章引用: 皮炳坤, 王春喜, 张弘强, 马聪, 王书文. 基于角色的访问控制在校园网管理系统中的应用研究[J]. 计算机科学与应用, 2016, 6(7): 399-405. http://dx.doi.org/10.12677/csa.2016.67049

[1]西北民族大学电气工程学院，甘肃 兰州
[2]郑州市气象局，河南 郑州
Email: *shuwenwang@163.com

收稿日期：2016年7月15日；录用日期：2016年7月24日；发布日期：2016年7月27日

摘 要

访问控制一直是信息安全的重要保证之一。基于角色的访问控制(Role-Based Access Control, RBAC)也是目前研究应用广泛的一种访问控制模型。为了保证系统的数据安全，严格区分各用户对系统访问的功能和权限的基础上，本文提出在基于角色的访问控制中与校园网组织结构相一致的安全策略，重点阐述所采用的基于角色的用户访问控制，并在数据库中增加角色对数据表中每一项的访问权限表应用于西北民族大学校园网，可提供一个灵活稳定又安全的校园网络环境。

关键词

校园网管理系统，访问控制，角色，数据库

1. 引言

20 世纪 70 年代，为了解决大型主机上共享数据授权访问的管理问题，访问控制技术快速发展起来。为实现信息的可用性，保证合法用户能够访问到资源，可以采用访问控制对系统权限进行设定[1]。因此，将基于角色的访问控制技术应用到高校校园网中并对其进行深入研究对提高用户数据的安全性是具有深刻意义的。

目前，主流的访问控制技术有自主访问控制 DAC (Discretionary Access Control)、强制访问控制 MAC (Mandatory Access Control)和基于角色的访问控制 RBAC (Role-Based Access Control) [2]这三类。随着“互联网+”和大数据的迅速发展，DAC、MAC 已不能满足实际应用的需求，虽然自主访问控制比较灵活，但其安全隐患差，不利于广泛使用；在强制访问控制中，对象用户不能进行权限的更改，灵活性较差；而在校园网应用中，有可能出现大量权限变更，使系统管理变复杂，较难实现。为此，出现了基于角色的访问控制模型(RBAC)，它可以通过分配角色来完成用户权限的授予和通过取消角色来取消用户的权限，而且具有角色分配的规则。本文在 RBAC 的思路之上，对其进行了扩展，提出了一种基于数据项的权限访问控制模型，保护了用户隐私数据，也增强了校园网管理系统的扩展性和适用性。

2. 基于角色的访问控制 RBAC

基于角色的访问控制 RBAC [2]是由美国 NIST (National Institute of Standards and Technology)提出的一种访问控制技术，其核心思想就是建立访问权限与角色的联系，通过给用户分配合适的角色从而建立用户与访问权限的联系。角色可以表示承担特定工作的资格，也可以体现某种权利与责任。安全管理人员根据需要定义各种角色，并设置合适的访问权限，而用户根据其责任和资历再被指派为不同的角色。这样，整个访问控制过程就可以分成两大类，即访问权限与角色相关联，角色再与用户关联，从而实现了用户与访问权限在逻辑上的分离。由于引入角色，实现了用户与权限的分离，授权变得简单而灵活，访问控制框架有了较强的扩展性[3]。例如一个人的职位发生变化，只要将该人当前拥有的角色去掉，加入代表新职务的角色。

基于角色的访问控制的基本模型以及概念结构对应关系主要包括四个实体：用户(User)、角色(Role)、权限(Permission)、会话(Session)。在应用系统方面，用户通过会话激活出角色集，并得到映射在角色集的访问权限，间接地访问应用系统的信息资源。该管理机制主要有 3 种对象：

用户(User)：使用系统的操作人员，可以是人、计算机等。

角色(Role)：是一个组织中的工作或职务，如教师、学生等。它是已命名的权限的集合，也是一个有序对(N，P)。其中 N = 角色名，P = 权限的集合。

权限(Permission)：对系统中的客体进行特定模式访问的操作命令的许可。它是个有序对(X, M)，其中 X 为一个对象，M 表示对 X 的非空的存取方式的集合。在数据库系统中 X 可以是各种数据项、二维表、视图、元组等对象。

用户、角色和权限三者之间的关系模型图如下图 1 所示。

比如西北民族大学新进一名本科生 student1，使这名本科生具有学生的权限。只需系统管理员将学生这个角色分配给 student1，而不用更改访问控制列表。多个角色可以指派给一个用户，比如一个用户有多重身份，可以是学生，也可以是负责授课的老师。学校可以有学生、教师和教务管理人员等不同的角色。在学生成绩管理系统中，假设 Tchl，Tch2，Tch3，…，Tchi 是各位教师；Studl，Stud2，Stud3，…，Studj 是与其对应的学生；Mngl，Mng2，Mng3，…，Mngk 是教务处的相关负责人，那么学生的权限为{查询自己课程的成绩，反馈老师教学的意见}；老师的权限为{录入所教课程的成绩，查询所教学生的成绩，按各种查询结果打印成绩表}；教务管理人员的权限为{日常事务管理，查询所有在校生成绩，按各种查询结果打印成绩表}。

3. 扩展的 RBAC 模型在校园网管理系统中应用

在校园网中，通过管理系统来提供全校统一的用户管理平台和授权认证体系，实现各应用系统的集中认证，规范用户的操作行为，对校园网内一些涉及到钱财方面和个人隐私的信息等进一步安全过滤。校园网管理系统采用单点登陆技术，用户通过一次登陆认证后，即可获得相应权限，能使用数字化校园中所有应用系统提供的服务。这不仅可以通过各种角色来决定哪些数据可访问，实现访问力度控制，而

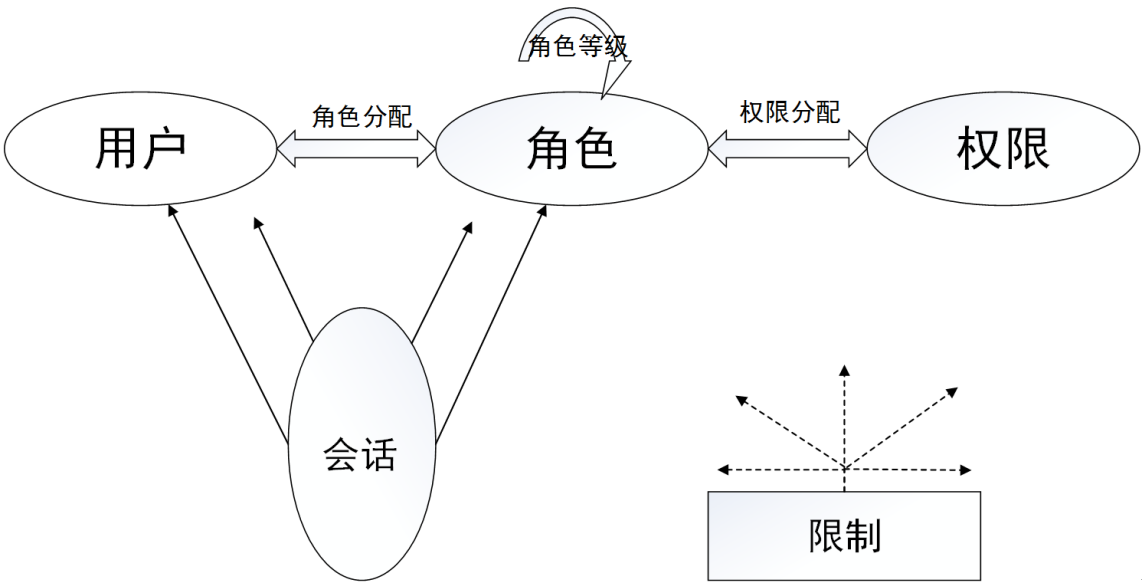

Figure 1. RBAC model structure
图 1. RBAC 模型结构图

且在该用户有权访问数据后再由数据项的访问权限来确定用户可访问的数据项，实现访问粒度控制[4]。

3.1. 用户访问控制原理

用户访问控制设计中采用位映射来组织功能权限信息，即每种功能权限对应一个 bit 位，允许用“1”代表，禁止用“0”代表。这些表示功能权限的位合成二进制，形成了角色权限码。当系统认为当前用户是合法用户时，便可获得该用户所对应的角色权限码，并根据该值和特定的映射关系得出用户对应于每种功能权限的情况[5]。

3.2. 管理系统中数据库设计

对于用户管理和角色管理中涉及到数据库层的用户、角色的增删及角色权限的设定则由 SQL Server 2000 [6]的系统存储过程在后台数据库完成。考虑到提高查询效率并兼顾减少数据冗余，在管理系统的数据库的安全模块中采用 6 个相互关联的数据表，来实现用户，角色，权限之间的映射关系，用以下 6 种表格：用户集合表、角色集合表、权限集合表、用户－角色表、角色－权限表和角色访问数据权限表。

其中，表 1 是作用于系统用户信息；表 2 是作用于保存角色信息；表 3 是作用于保存系统的权限信息，可定义系统哪些模块公开；表 4 是作用于关联用户和角色的关系表；表 5 是作用于关联角色和权限的关系表；表 6 是对于不同的角色，我们需要展示的数据内容也不同；见下表所示。

3.3. 工作流程

管理系统包括两种模块：一部分是针对整个高校校园网信息系统的用户、角色、权限设定的模块。

Table 1. User collection table
表 1. 用户集合表

字段名	数据类型(宽度)	主键	说明
User-ID	Varchar (20)	TRUE	用户编号
Super-user	Varchar (20)		系统管理员，可根据需要增加系统角色，同时设置权限
User-name	Varchar (20)		用户名
Password	Varchar (20)	FALSE	密码

Table 2. Character set table
表 2. 角色集合表

字段名	数据类型(宽度)	主键	说明
Role-ID	Varchar (20)	TRUE	角色编号
Role-name	Varchar (20)		角色名
Description	Varchar (100)	FALSE	该角色的相关描述

Table 3. Privilege set table
表 3. 权限集合表

字段名	数据类型(宽度)	主键	说明
Permission-ID	Varchar (20)	TRUE	权限编号
Permission-name	Varchar (20)		权限名称
Description	Varchar (100)	FALSE	描述权限信息

Table 4. Users-character table
表 4. 用户－角色表

字段名	数据类型(宽度)	主键	说明
User role-ID	Varchar (20)	TRUE	用户角色编号
User-ID	Varchar (20)		合法用户的编号
Role-ID	Varchar (20)		角色编号
Description	Varchar (100)	FALSE	用户角色信息描述

Table 5. Role-permissions table
表 5. 角色－权限表

字段名	数据类型(宽度)	主键	说明
Role permission-ID	Varchar (20)	TRUE	角色权限编号
Role-ID	Varchar (20)		角色编号
Permission-ID	Varchar (20)		权限编号
Description	Varchar (100)	FALSE	角色权限信息描述

Table 6. Role access rights to the data table
表 6. 角色访问数据权限表

字段名	数据类型(宽度)	主键	说明
Role	Varchar (100)	TRUE	角色名
Column1	Varchar (1)		用 0/1 表示访问权限
Column2	Varchar (1)		用 0/1 表示访问权限
.....	.....	.....	.....

在这个模块下可以创建新用户，指定用户能登录的子系统，及为用户分配在可登录的各个子系统中所拥有的不同的角色，不同的角色具有不同的权限。另一部分是嵌入不同的子系统的用户、角色、权限设定模块。在这个模块下创建的新用户被默认为只能登录该模块所在的子系统里。

3.3.1. 用户登录部分

在校园网系统的各个子系统里，未经授权的用户不能对数据库进行任何操作命令。用户输入其账号、密码准确后可取出用户的系统登录权限码来决定用户能否登录该子系统。成功登录后，软件模块根据角色权限码来控制用户分权操作的子系统[7]。用户登录的流程图如图 2 所示。

3.3.2. 用户管理部分

用户管理部分用来创建新用户、维护用户信息、指定用户可以登录的模块，并为用户分配指定模块的多个不同的角色。用户组管理如图 3 所示。

3.3.3. 角色管理部分

角色管理部分用来创建各个子系统下的角色，并给每个角色分配属于该系统下的权限。我们可以根据不同的分类标准来实现角色，进行权限管理。用户通过角色获得该角色对应的权限，我们通过数据库的授权方式来实现基于角色的功能和权限控制。在许多系统中，普通用户的数量都比较多，而且大部分用户具有许多相同的权限，可以把这些具有相同权限的用户(如研究生)组成一个用户组，然后为每一用户

组分好角色。系统管理员设定不同层次的用户组来实现对用户的简单方便的管理。

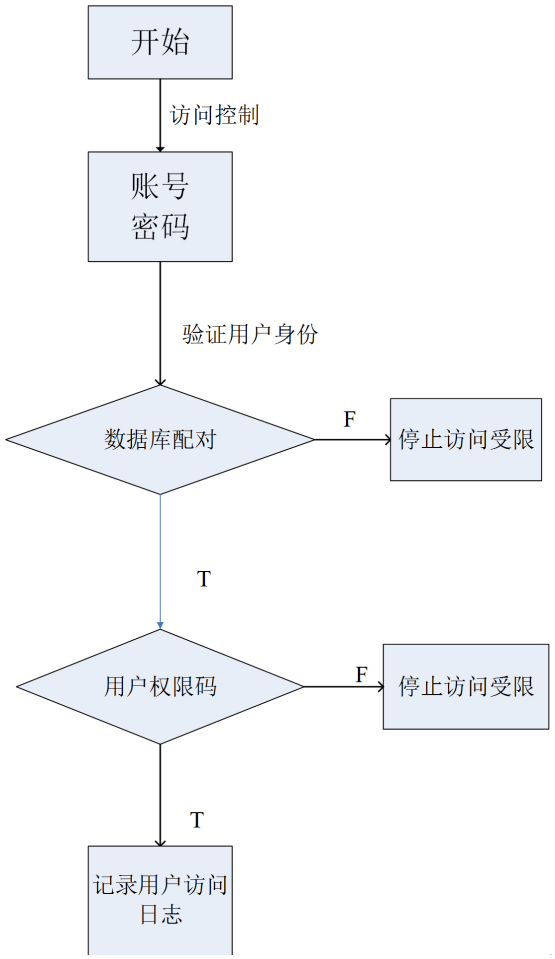

Figure 2. The flow chart of the user login
图 2. 用户登录流程图

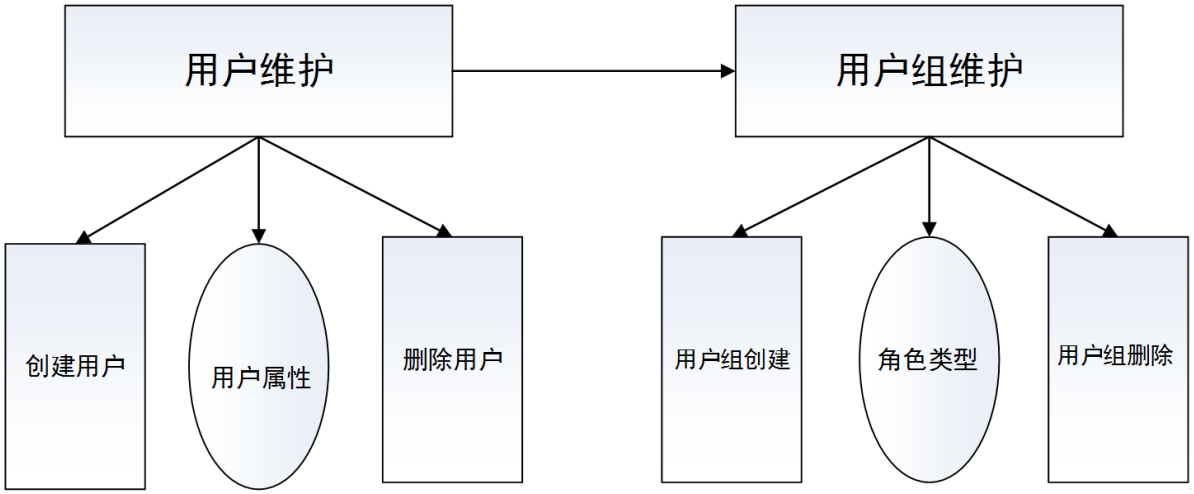

Figure 3. The flow chart of the user login
图 3. 用户登录流程图

4. 结束语

本文主要进行对基于角色的访问控制理论研究，是校园网管理较好的一种访问控制模式。然后在此基础上对 RBAC 模型进行了改进，给出了管理系统的数据库设计表，在数据库中增加角色对数据表中每一项的访问权限表，使用户有权访问数据后再由数据项的访问权限来判断用户可访问的数据项，防止非法访问和泄漏，很好地适应了高校管理系统的安全策略。最后详细介绍了管理系统完整的工作流程，实现了在校园网灵活的管理应用模式。

本文的下一步工作首先是随着校园网管理系统的不断完善，如何更好地提高对权限控制的灵活需求；其次是将此模型应用到企业 OA 管理系统，以保证系统使用的安全性，提高其实用性。

基金项目

本课题得到国家自然科学基金资助，项目号：61261042；本课题得到西北民族大学物联网关键技术研究科研创新团队项目资助。

参考文献 (References)

[1] 郭亚军, 宋建华, 李莉, 等. 信息安全原理与技术[M]. 北京: 清华大学出版社, 2013.

[2] Ferraiolo, D.F., Sandhu, R., Gavrila, S., *et al*. (2001) Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security* (*TISSEC*), **4**, 224-274. http://dx.doi.org/10.1145/501978.501980

[3] 李凤华, 苏锑, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.

[4] 常豆. 海量就业信息数据资源安全访问控制研究与原型实现[D]: [硕士学位论文]. 北京: 北京邮电大学, 2015.

[5] 刘佳. 基于角色的云平台访问控制技术[D]: [硕士学位论文]. 武汉: 武汉理工大学, 2013.

[6] 王玉英. JSP 中 SQL Server2000 数据库访问技术[J]. 电脑与信息技术, 2011(4): 76-79.

[7] 郭军. 基于角色的访问控制分级授权管理的研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2012.