ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.17, No.3 January 2021

E-mail: wltx@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

基于资源控制的权限管理系统设计方法

李卫丽,金小俊*,赵化

(上海赛可出行科技服务有限公司南京分公司, 江苏 南京 210018)

摘要:[目的]为了解决传统的基于角色的权限控制系统在实施过程中的重复性工作量大及配置过程较为抽象的缺点。[方法]采用“一切皆资源”的理念,以资源树为基本配置模型,构建新的基于资源的权限控制系统。[结果]这种理念及实施过程易于理解,并能有效减少大量重复性配置工作。[结论]基于资源的权限控制的系统设计方法,可极大提高权限控制的工作效率,并减轻系统的维护成本。

关键词:权限管理系统;基于角色的权限控制;一切皆资源;资源树

中图分类号:TP311 文献标识码:A

文章编号:1009-3044(2021)03-0044-02

开放科学(资源服务)标识码(OSID):

DOI:10.14004/j.cnki.ckt.2021.0116

A Design Method of Permission Management System Based on Resource

LI Wei-li, JIN Xiao-jun*, ZHAO Hua

(Shanghai SAIC Mobility Technology and Service Co., LTD., Nanjing 210018, China)

Abstract: For solving the disadvantage in traditional permission management based on roles, which makes the operation complex and abstract, this article tries to construct a new permission manage system which based on the idea of ‘everything is resource’ and the model of resource tree. This operation of this new system is easier and more understandable which can efficiently reduce the repetition. This design method based on resource can effectively raise the working efficiency and cut down the cost of maintenance.

Key words: permission management system; permission controlling based on roles; everything is resource; resource tree

基于角色的访问控制(Role-Based Access Control, RBAC)[1]模型是20世纪90年代研究提出的一种模型,其中以美国George Mson大学信息安全技术实验室提出的RBAC96模型最具代表性,并得到了普通的公认。RBAC是当前非常流行的权限管理系统设计[2],它认为权限授权的过程可抽象地概括为:Who是否可以对What进行How的访问操作,并对这个逻辑表达式进行判断是否为true的求解过程。Who, What, How构成了访问权限的三元组。RBAC是一种基于角色的权限管理系统设计方案,通过角色,可以批量赋予用户相同的权限。RBAC主要用于控制用户对资源等的访问。通过对进程和用户应用安全属性,RBAC可以向多个管理员分派超级用户功能[3]。RBAC在实际应用中,更像是一种模型,一种思想,不需要完全参照其实现。RBAC简化了给用户赋权的操作,其基础架构如图1所示[4-5]:

图1 基础架构图

1 基于角色的权限控制系统现状

RBAC存在的一个最大的缺点是,配置操作比较抽象。权限的描述,一般会采用前后端都可识别的编码格式。尤其对于页面元素相关的权限,若存在描述相似的功能,很难进行直观区别,这就容易导致在权限配置过程中配置错误。

2 基于资源控制的权限管理系统设计方案描述

2.1 概述

在RBAC基础之上,本文提出了一种“一切皆资源”的设计理念,在权限之下再下沉一层,提出资源的概念。“一切皆资源”,即所有想要进行控制的具体的(页面、按钮都能)以及抽象的(接口等)等对象都视为资源。资源是实现权限控制的最小原子单位,资源在本质上就是权限,只不过在资源的概念之上,可认为权限是资源的集合。在“一切皆资源”的实践中,可以进行数据控制,举例说明:对某个公司的数据的可访问权限,可建立一种抽象的数据权限资源。通过该类资源所关联的权限配置,可控制不同角色或具有不同权限的人员看到不同的数据,从控制层面实现“千人千面”。

收稿日期:2020-10-10

作者简介:李卫丽(1985—),女,工程师,硕士,研究方向为软件工程;通信作者:金小俊(1987—),男,工程师,硕士,研究方向为计算机应用;赵化(1988—),男,助理工程师,学士,研究方向为软件架构与设计。

2.2 详述

在“一切皆资源”的基础之上，我们进而提出资源树的概念。资源树是一种将抽象的权限资源用树形结构上的节点来具体化，即：对应于页面上的对象，如页面、菜单、按钮等，可按各元素之间的层级依次建立对应的资源节点，根据层级关系进而形成权限资源树。资源树建立完成后，可对应创建需要的权限，然后与角色绑定实现权限的控制。资源树的建立，将权限对应地进行形象化，树形结构的层级化使得在权限分配过程中，可按照树形结构进行权限分配，分配过程对于操作者直观且易于操作。

2.3 实施

基于资源的权限控制整体架构图如图2所示。

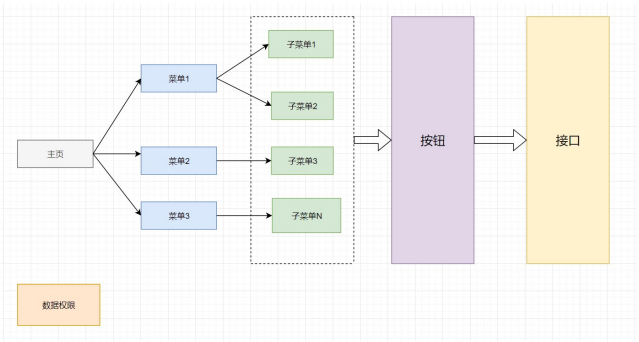

图2　权限控制整体架构图

下面主要描述基于资源的权限管理系统的实现过程：

首先是资源的创建。依据“一切皆资源”的概念，资源的概念包括具体的，例如：页面、菜单、按钮等，还包括抽象的，比如：接口、可筛选的数据范围，甚至可扩展至系统、业务线等等一切想进行操作权限区分的事物。资源的实现可以通过将资源详情用易解析、易扩展的json格式来保存，对于具体类型的资源类型，资源详情可保存对应的资源所属页面的url地址、icon以及唯一性标识id等信息，可参考如下配置：{"key": "sub00-08-05-01", "icon": "", "name": "报表权限申请", "path": "/pmo-config-form", "description": "报表权限申请"}；对于抽象资源，可按照业务需求保存为业务端可识别的编码，比如典型的数据权限可参考如下配置：{"permissionCode": "tmOrgRole_001"}, {"comp_code": ["own"], "dept_code": ["own"], "costcenter": ["own"]}。

接着就是资源树的构建。按照“一切皆资源”的方法，根据页面的层级关系，依次建立具有层级关系的资源树。为保存层级关系，每级的资源需保存其父节点的唯一标识，同时，为支持各种类型的资源，可在资源创建时为资源划分类型，如常用的数据权限等。

剩余的工作则是RBAC的通用操作部分。建立角色，角色与权限的绑定，人员通过角色得到对应的权限。

系统整体可分为组织架构模块和权限控制模块，架构图如图3所示。

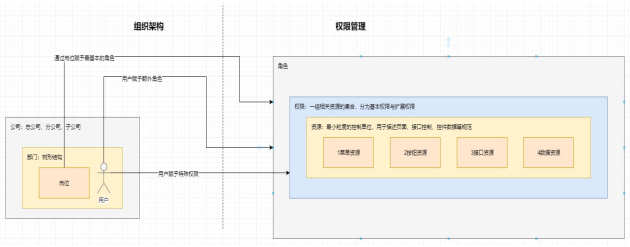

图3　系统整体架构图

组织架构部分，可采用领域驱动设计，从不同视角根据公司业务创建公司、部门、岗位、人员等信息，必要时可以扩展大区等信息。组织架构虽然不是权限管理的范畴，但却是权限管理的必要条件，权限管理必须依托于各公司独特的组织架构，否则脱离了公司的组织架构，同样会带来管理维护困难等问题。

权限管理模块，可根据要控制的对象分为控制权限和数据权限。对控制权限，根据所要控制的元素做最小划分，自顶而下依次创建页面、菜单、按钮、接口等控制类资源，在数据存放时需要保存资源的父子节点关系，并且接口权限资源根据页面的调用可挂载至对应的页面资源下，实现接口权限的精准控制。对数据权限，比如针对不同的用户、角色，即使都拥有A接口的访问权限，但可以通过指定查询范围实现数据的精准控制。数据权限不区分页面，根据业务需要建立前后端约定好的、可识别的资源。资源详情可采用易于解析的json格式存储，以便后期资源定义的扩展，同时也是对“一切皆资源”的有效支撑。资源建立完成后，可以在资源管理页面清晰看到所创建的资源树及要进行控制的数据权限资源。接下来根据权限管理的业务需求，对资源进行组合从而创建适当粒度的权限，更进一步创建角色。

3 结束语

本文详情阐述了基于资源树的权限控制系统的实现方式，较之于基于角色的控制体系，基于资源树的权限控制系统提出“一切皆资源”的理论，并以此为基础，构建权限控制系统的权限树，资源是进行权限配置的基础，通过对所有要控制的对象简历对应的资源模型，并依据其对应的页面关系逐一建立资源，可实现精准的权限控制。对于抽象的赋权操作形象化，增加的分层操作也使得权限控制系统可以有更多的灵活性及可扩展性，极大提升了权限控制系统的可用范围。

参考文献：

[1] 刘强.基于角色的访问控制技术[M].广州:华南理工大学出版社,2010.
[2] 黄建,卿斯汉,魏丕会.基于角色的访问控制[J].计算机工程与应用,2003,39(28):64-66,71.
[3] ORACLE.系统管理指南:安全性服务.基于角色的访问控制[EB/OL].https://docs.oracle.com/cd/E24847_01/html/819-7061/rbac-1.html#scrolltoc.
[4] 尹刚,王怀民,滕猛.基于角色的访问控制[J].计算机科学,2002,29(3):69-71.
[5] 汪厚祥,李卉.基于角色的访问控制研究[J].计算机应用研究,2005,22(4):125-127.

【通联编辑：代影】