doi:10.3969/j.issn.1673-9833.2012.04.020

基于RBAC和Web服务的统一授权研究

居庆玮，李长云，赵正伟，霍 阔

（湖南工业大学 计算机与通信学院，湖南 株洲 412007）

摘 要：运用统一认证和RBAC模型等原理，结合Web服务技术，提出了一种统一的身份认证和授权服务接口规范，并在企业应用系统中进行了试用。试用表明，该授权方法与接口规范能实现各应用系统间的一次登录、统一认证、统一权限管理，但单点登录和审计方面的功能还需进一步完善。

关键词：RBAC；Web服务；统一认证；服务接口；授权

中图分类号：TP315；F270.7 **文献标志码**：A **文章编号**：1673-9833(2012)04-0088-04

Study on Unified Authorization System Based on the RBAC and Web Service

Ju Qingwei，Li Changyun，Zhao Zhengwei，Huo Kuo

（School of Computer and Communication, Hunan University of Technology, Zhuzhou Hunan 412007，China）

Abstract: Using the theory of unified authentication and RBAC model and combining with the Web service technology, presents a unified identity authentication and authorization service interface specification, and gives it on trial in the enterprise application system. It shows that the authorization method and interface specification achieve a login, unified authentication and unified rights management between each application system, but the single sign-on and audit functions need to be further improved.

Keywords: RBAC; Web services; unified authentication; service interface; authorization

0 引言

随着信息技术和网络技术的广泛应用，各种应用系统得以快速发展与广泛普及。但由于信息化建设时期资源投入、软硬件技术平台的不同，使得企业在建设这些应用系统时具有明显的差异性，各个应用系统采用的技术、架构不同，且相互独立，具有不同的用户管理、认证及授权方式。本文运用统一认证[1-2]和基于角色的访问控制（role-based access control，RBAC）模型[3-4]等原理，结合Web服务技术[5]，提出具体的接口规范，研究了认证与授权的统一。企业试用表明，该授权方法与接口规范能实现应用系统认证与授权的统一管理和统一调度。

1 统一认证

统一认证方式主要有传统方式、改进方式、以应用为主的认证方式和用户独立的统一认证方式等。1）传统的统一认证方式以统一认证为中心，比较直接、直观，容易实现。但是，在认证过程中，系统直接操作底层数据库，这违背了面向服务体系结构（service-oriented architecture，SOA）的理念。2）改进的统一认证方式以统一认证为中心，实现模式固定，且容易实现，运用标准Web服务访问底层数据，符

收稿日期：2012-06-09

基金项目：国家住建部基金资助项目（2010FJ3041），湖南省自然科学基金资助重点项目（12JJ2036）

作者简介：居庆玮（1987-），男，山东青岛人，湖南工业大学硕士生，主要研究方向为物联网安全机制，

E-mail: jvwei236632@126.com

合基于 SOA 的理念。但是，这种方式要求各个应用系统采用相同的用户密码，或者设置空密码（直接分配给登录名的访问令牌）。3）以应用为主的认证方式以各个应用系统为主，采用标准的 Web 服务提供用户的统一验证，系统主要做后台服务性的工作。这种方式要求各个应用服务器中都必须安装一个代理程序完成用户的身份认证工作，各个应用系统需要自己开发登陆页面，实现比较麻烦。4）用户独立的认证方式以统一认证为主，分工明确，思路清晰，实现了用户映射，为以后给各个应用系统的简单授权提供了便利。

目前，大部分应用系统都要求用户在应用系统中建立自己的账户，可称为子账户，子账户存储在各个应用系统中。用户在统一认证和授权系统中也需要建立自己的账户，可称为主账户，主账户集中存储在统一认证服务器的用户管理系统中。主账户与子账户通过一定的机制建立对应关联。关联关系建立后，用户采用主账户对不同的应用系统进行统一认证时，系统会根据主账户与子账户的对应关联，自动使用子账户登陆应用系统。对应关联建立后，如果应用系统与统一认证服务网络通讯中断，用户仍然可以使用主账户登陆应用系统。

为了使系统对各个应用系统都能实现用户授权的调度和管理方面的统一，减少应用系统开发者在统一授权开发方面的工作量，应制定出必要的接口标准和规范，且尽可能地多次复用，同时保证各个应用系统可以独立运行。因此，本文选择用户独立的认证方式为试用系统的认证方式。

2　统一授权与接口规范设计

统一认证和授权系统主要包括认证和授权两方面的工作。统一认证和授权系统是各应用系统公共模块的集成。作为统一认证和授权系统的一部分，统一授权也是对应用系统授权模块的一个集成提取，是多个应用系统授权的一个公共模块。虽然不同的应用系统提供的资源不同，操作功能也可能不同，但是访问控制方式却可以相同，授权方式也可以规范化、统一化。不需要考虑底层数据库的具体实现，只需一个统一的标准接口规范，应用系统按照规范进行设计，就能够实现授权方式的统一。统一授权方式与应用系统的授权模型联系密切，因此，应根据应用系统的授权模型来设计统一认证系统的授权方式。

2.1　RBAC 模型分析

作为传统访问控制（自主访问、强制访问）的有前景的代替，RBAC 受到广泛的关注。目前，大部分企业应用系统的授权都是采用这种方式。

用户、角色、权限是 RBAC 模型中的 3 个主要实体对象。用户是应用系统的访问者，角色是应用系统中一个组织或任务中的位置，权限是应用系统中的数据或其他资源的访问许可。一个用户可以在一个应用系统中拥有一个或多个角色，一个角色可以拥有多个权限。

在 RBAC 中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限，这就极大地简化了权限的管理。在一个组织中，角色是为了完成各种工作而创造的，用户则依据其责任和资格被指派相应的角色，用户可以很容易地从一个角色被指派到另一个角色。角色可依据新的需求和系统的合并而赋予新的权限，而权限也可根据需要从某角色中收回。

RBAC 模型没有说明用户的组织形式，加入用户组能够使应用系统更适合于分散式权限管理。用户组是指一群用户的集合。在企业应用系统中，部门众多，机构庞大，如不引入用户组，对部门内部用户的授权比较混乱、繁琐，而引入用户组，将部门按照行政或其他隶属关系进行组织，形成树形结构，授权就会变得清晰。当某个组的所有用户职能相同时，可以将相应角色授予整个组，这个组的用户也就获得了权限；改变该组对应角色的权限时，整个组用户的权限也相应地被改变，从而简化了授权管理。企业应用系统的数据是按部门或用户组来组织的，可以用户组为单位来分配数据资源权限，将角色作为操作功能的组合单位。

本文设计的授权模型的基本思想是：用户与功能、用户与资源不直接发生关系，而是分别通过角色和用户组间接关联。其中，用户组通过用户组与资源关系分配资源，用户组通过用户组与用户关系添加用户，用户通过用户与角色关系获得角色，角色通过角色与功能关系分配功能。具体模型见图 1。

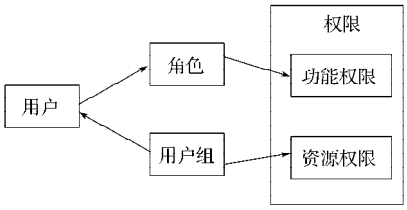

图 1　授权方式示意图

Fig. 1　Authorization mode diagram

该模型在企业应用系统中具有如下优势：

1）用户、用户组、角色及权限的设置将企业结构和岗位人员职责简单地映射到企业应用系统中，使系统权限部分的设计和应用更加直观、灵活，易

于管理和维护。2）若企业内部某个职位的职责发生变化，不需逐一改变处于这个职位的所有职员的权限，只需改变系统中对应这一职位的角色权限。3）当企业对某些职员进行了平行的部门间调整但职员的职责没有任何变化时，只需更改用户所对应的用户组，这样，用户所对应的资源权限就发生了相应的改变，而无需直接更改用户的授权资源。4）若企业中某些职员的职责发生变化，而所在部门或用户组无变化时，只需稍微更改一下用户对应的角色即可。5）如果企业某些职员的职责与所属部门同时发生变化，需要同时修改用户对应的角色和用户所属的用户组，这样，用户的功能权限和资源权限就得到了相应的修改。

2.2 统一授权方式

通过以上对RBAC授权模型的分析，本文提出的统一授权的设计方法如下：

1）统一认证系统在用户通过认证后，授予用户在应用系统内对应的用户组和角色，角色和用户组所对应的功能权限和资源权限，将通过与应用系统交互获得。2）针对已有的应用系统，需先将接口规范所需数据信息列出，数据信息主要指授权信息，然后实现符合接口规范的可编辑的授权功能，简单地讲，授权操作也要按照标准接口实现，以实现统一管理和统一调度；针对新开发的应用系统，只要其结构的设计是按照标准规范进行的，一般不需重新开发，即可做成统一的接口规范实现。3）信息的存放。应用系统的信息、用户表、用户与用户组映射表、用户与角色映射表、用户在具体应用中的映射名和加密信息等，存放至统一认证系统中，其他的信息，如角色、用户组、资源权限、功能权限等，存放至各个应用系统中。

2.3 Web服务分析

设计了上述统一授权方式后，需要在一种统一的协议下具体实现这种统一授权，本研究采用Web服务。Web服务是一套定义了应用程序如何在Web上实现互操作的标准，是基于可扩展标记语言（extensible markup language，XML）和以安全为目标的超文本传送协议通道（hypertext transfer protocol over secure socket layer，HTTPS）的一种服务。其通信协议主要基于简单对象访问协议（simple object access protocol，SOAP），服务的描述通过Web服务描述语言（Web services description language，WSDL）来进行，通过通用描述、发现与集成服务（universal description, discovery and integration，UDDI）来发现和获得服务的元数据。Web服务相当于部署在Internet上的应用程序编程接口，能够方便地应用在网络上的应用程序中，构成新的应用服务，具有良好的可集成性、封装性和松散耦合性。

SOAP, WSDL和UDDI是Web服务体系结构的3个部分：

1）SOAP是一种轻量、简单、基于XML的协议，其设计功能为交换结构化和固化的信息。

2）WSDL是一种接口定义语言，是用于描述Web服务的接口信息和说明如何与Web服务通信的XML语言。

3）UDDI是一种目录服务，其功能主要是对Web服务进行注册和搜索，主要提供基于Web服务的注册和发现机制，为Web服务提供3个重要的技术支持，即标准、透明、专门描述Web服务的机制，调用Web服务的机制，可以访问的Web服务注册中心。通过UDDI，可以发布和查看Web服务的信息，然后运用统一的调用方法来享用这些Web服务。

2.4 接口服务规范

Web服务可以写在任何平台上，适用任何语言。XML文本是Web服务信息交换的标准方式。结合RBAC模型，运用Web服务可较好地为上文的解决方案提供一套标准服务接口。本文设计的具体接口规范及其说明见表1。

表1 接口规范说明

Table 1 Interface specification

接口名称	输 入	输 出	说 明
USERTREE	ApplicationID	XML数据	获取应用系统的用户树
ROLE_GROUP	UserID，ApplicationID，Instruction	XML数据	获取用户对应的角色和用户组
R_G_DISTR	UserID, ApplicationID, RoleID/UsergroupID, Instruction	是否成功	调整用户对应的角色、用户组
USERLOG	ApplicationID, UserID	XML数据	获取用户应用系统下的操作日志
ROLETREE	ApplicationID, Instruction	XML数据	获取应用系统的角色树
USERGROUP	ApplicationID, Instruction	XML数据	获取应用系统的用户组
DATARANGE	UsergroupID, ApplicationID, Instruction	XML数据	获取用户组对应的数据范围信息
OPERATION	RoleID, ApplicationID, Instruction	XML数据	获取角色对应的操作功能信息

3　试用系统的系统框架和访问流程

3.1　系统框架

统一认证系统的设计涉及身份认证、授权等多方面的技术。根据上文的统一认证和授权方式，基于RBAC访问控制模型，运用Web服务技术作为底层，制定了服务接口规范。该接口规范在试用系统中应用的系统框架图见图2。

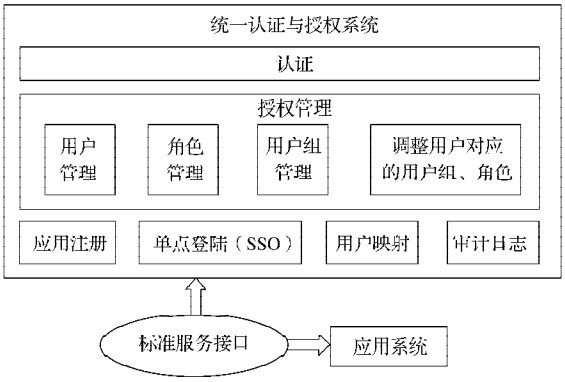

图2　系统框架图

Fig. 2　The system frame diagram

统一认证与授权系统主要由认证模块和授权管理模块组成，授权管理包括用户管理、角色管理、用户组管理等。统一认证与授权系统通过底层的以上设计的具体服务接口，与各个应用系统协作完成用户、角色和用户组的管理。

3.2　访问流程

当用户向应用系统提出访问请求时，应用客户端发送请求给认证服务器。服务器在对用户进行认证后，若用户认证成功，服务器会授予用户相应的角色和用户组；若认证失败，服务器继续搜索用户信息，直到认证成功。用户在统一认证服务器获取角色和用户组后，在应用系统内获得相应的权限，若获取成功，应用系统接受访问；若获取失败，应用系统提示用户进行注册。企业试用中系统的访问流程见图3。

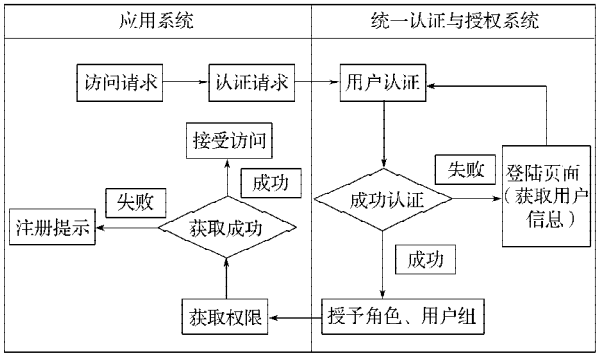

图3　用户访问系统流程图

Fig. 3　The flow chart for users accessing the system

应用了本研究中提出的接口后，试用系统较好地完成了多企业应用系统的统一认证、统一授权管理和调度，具有较好的重用性和扩展性。

4　结语

借助于Web技术，可以对多种应用系统的认证授权进行松散、动态地集成，为企业自身用户和客户提供一个统一的分布式服务。本文结合Web服务，以基于角色的访问控制为策略，提出了一种统一的身份认证和授权服务接口，并在企业应用系统中进行了试用，实现了各应用系统间的一次登录、统一认证、统一权限管理，具有高安全性、松耦合度的特点。但同时，单点登录和审计方面的功能还需进一步研究，制定出更实用有效的操作实现方法，进一步完善系统功能。

参考文献：

[1] 刘　敏，吕先竞，宋玉忠. 基于OpenID的分布式认证系统的设计与实现[J]. 现代情报，2008(6)：90-92.
Liu Min，Lü Xianjing，Song Yuzhong. Design and Implementation of the Decentralized Authentication System Based on OpenID[J]. Modern information，2008(6)：90-92.

[2] 季　旻，林　中. 单点登录方案的研究与设计[J]. 计算机工程与设计，2009，30(12)：2862-2864.
Ji Min，Lin Zhong. Research and Design of Single Sign-On Scheme[J]. Computer Engineering and Design，2009，30(12)：2862-2864.

[3] 王成良，姜　黎. B/S应用系统中的细粒度权限管理模型[J]. 计算机系统应用，2010，19(7)：79-82.
Wang Chengliang，Jiang Li. Fine-Grained Privilege Management Model and Its Application in B/S Application System[J]. Computer Systems & Applications，2010，19(7)：79-82.

[4] 信　科，杨　峰，杨光旭，等. 基于RBAC权限管理系统的优化设计与实现[J]. 计算机技术与发展，2011，21(7)：172-174.
Xin Ke，Yang Feng，Yang Guangxu，et al. Optimum Design and Realization of Privilege Management Based on RBAC[J]. Computer Technology and Development，2011，21(7)：172-174.

[5] 柴晓路，梁宇奇. Web Services技术、架构和应用[M]. 北京：电子工业出版社，2003：10-11.
Chai Xiaolu，Liang Yuqi. The Technology, Architecture and Application of Web Services[M]. Beijing：Publishing House of Electronics Industry，2003：10-11.

（责任编辑：徐海燕）