基于 RBAC 的 SaaS 系统的权限模型

马立林[1] 李 红[2]
[1](九江学院信息技术中心 江西 九江 332005)
[2](九江学院理学院 江西 九江 332005)

摘 要 在研究 RBAC 模型的基础上,通过引入访问控制分层管理的思想来改良和扩展 RBAC 模型,建立了 SaaS(软件即服务)系统的一种权限管理模型。从系统访问许可证、系统功能操作控制、系统数据访问控制三个层次建立了结构模型,并对其做了形式化定义。最后指出了新模型的优点。

关键词 软件即服务 基于角色访问控制 访问控制 模型

A PERMISSION MODEL OF SaaS SYSTEM BASED ON RBAC

Ma Lilin[1] Li Hong[2]
[1](*Information Technology Center, Jiujiang University, Jiujiang 332005, Jiangxi, China*)
[2](*College of Science, Jiujiang University, Jiujiang 332005, Jiangxi, China*)

Abstract Based on the research of RBAC model, the thought of access control with layered management is imported to improve and extend the RBAC model, and a permission management model of SaaS system is built up. Then, the structural model is established from three aspects of access permission card, functional operation control and data access control, together with a formal definition given. At last, the advantages of the new model are pointed out.

Keywords Software as a service(SaaS) Role based access control(RBAC) Access control Model

0 引 言

SaaS 系统可以定义为“将软件部署为服务并通过 Internet 进行访问”的系统,是单实例、多用户体系结构、基于 Internet 访问的系统。系统中每个环节都可能受到安全威胁。为了确保系统中数据的安全性、一致性、完整性,使客户能够放心地将具有重要性、机密性的商业数据交给 SaaS 服务提供商进行管理和控制,在开发一个 SaaS 系统的过程中,作为 SaaS 系统的重要组成部分——权限管理模块变得尤为重要。本文在研究基于角色的访问控制(RBAC)模型的基础上,提出了 SaaS 系统的一种权限管理模型。

1 RBAC 模型研究

访问控制是针对越权使用资源的防御措施。基本目标是为了限制访问主体(用户、进程、服务等)对访问客体(文件、系统等)的访问权限,从而使计算机系统在合法范围内使用;决定用户能做什么,也决定代表一定用户利益的程序能做什么。企业环境中的访问控制策略一般有三种:自主型访问控制方法、强制型访问控制方法和基于角色的访问控制方法。其中,自主式太弱,强制式太强,二者工作量大,不便于管理。基于角色的访问控制方法是目前公认的解决大型企业的统一资源访问控制的有效方法。其基本原理是在用户和访问权限之间加入角色这一层,实现用户和权限的分离,用户只有通过激活角色才能获得访问权限,提高了防护的力度。同时通过角色对权限分组,大大简化了用户权限分配表,间接地实现了对用户的分组,提高了权限分配的效率。而且加入角色层后,访问控制机制更接近真实世界中的职业分配,便于权限管理,提高了灵活度。其显著的两大特征是:(1)减小授权管理的复杂性,降低管理开销;(2)灵活地支持企业的安全策略,并对企业的变化有很大的伸缩性。美国国家标准与技术研究院 NIST(The National Institute of Standards and Technology)标准 RBAC 模型由四个部件模型组成,这四个部件模型分别是基本模型 RBAC0(Core RBAC)、角色分级模型 RBAC1(Hierarchal RBAC)、角色限制模型 RBAC2(Constraint RBAC)和统一模型 RBAC3(Combines RBAC)[1]。RBAC0 模型如图 1 所示。

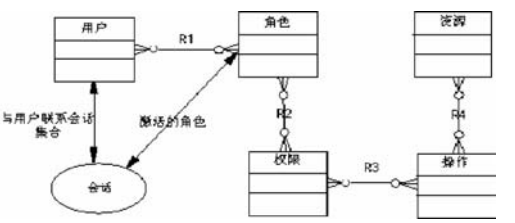

图 1 RBAC0 模型

RBAC0 定义了能构成一个 RBAC 控制系统的最小的元素集合。在 RBAC 之中,包含用户(USERS)、角色(ROLES)、目标(OBS)、操作(OPS)、许可权(PRMS)五个基本数据元素,权限被

收稿日期:2008 - 07 - 15。国家自然科学基金资助(70471066)。**马立林**,硕士生,主研领域:网络信息安全,企业信息化。

赋予角色,而不是用户,当一个角色被指定给一个用户时,此用户就拥有了该角色所包含的权限。会话 sessions 是用户与激活的角色集合之间的映射。RBAC0 与传统访问控制的差别在于增加一层间接性带来了灵活性,RBAC1、RBAC2、RBAC3 都是先后在 RBAC0 上的扩展。

RBAC1 引入角色间的继承关系,角色间的继承关系可分为一般继承关系和受限继承关系。一般继承关系仅要求角色继承关系是一个绝对偏序关系,允许角色间的多继承。而受限继承关系则进一步要求角色继承关系是一个树结构。

RBAC2 模型中添加了责任分离关系。RBAC2 的约束规定了权限被赋予角色时,或角色被赋予用户时,以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。责任分离包括静态责任分离和动态责任分离。约束与用户 - 角色 - 权限关系一起决定了 RBAC2 模型中用户的访问许可。

RBAC3 包含了 RBAC1 和 RBAC2,既提供了角色间的继承关系,又提供了责任分离关系。

通过上面对 RBAC 模型的研究,在 RBAC 模型中,访问控制都与角色相关,系统权限控制都通过角色来实现,权限粒度不够细化,权限层次不够清晰,不能很好地区分系统功能操作控制与系统数据访问控制。基于这些问题的考虑,提出了一种新型的权限管理模型——基于 RBAC 的分层控制模型。

2　SaaS 系统的权限模型

随着社会的不断发展、竞争的不断加剧、社会分工的不断细化、企业之间的合作不断加强、业务的灵活性不断增强,企业对系统数据的安全性要求越来越高,原有基于单一角色的粗放式系统权限管理模式已不能满足现在用户的需要,需要对系统权限管理进行细化,实行更精细化的管理。根据对 SaaS 系统的分析了解,运用分层控制的思想对 SaaS 系统的权限管理实施多层访问控制,能够确保系统的安全性和数据访问的灵活性。分层控制的思想是基于 RBAC 模型的权限设计思想,对 RBAC 模型进行了部分改良和扩展。把 SaaS 系统的权限管理模型划分为系统许可证权限管理、系统功能操作控制管理、系统数据访问控制管理三个层次;引入许可证、岗位、组织机构(部门、小组、虚拟团队)等数据实体,并定义岗位与用户、用户与不同组织机构等实体之间的关系。其总体模型如图 2 所示。

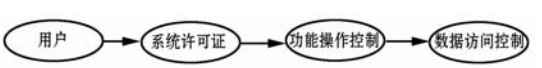

图 2　SaaS 系统权限总体模型

SaaS 系统权限管理模型包含的基本元素主要有:用户、小组、角色、资源、操作、岗位、许可证、虚拟团队、部门、组织、权限。主要的关系有:分配角色权限、分配用户角色、分配用户岗位、分配组织许可证、分配权限操作、分配操作资源、分配小组到不同组织机构。其形式化描述可以从系统许可控制、系统功能操作控制、系统数据访问控制三个层次对其进行描述。

2.1　系统许可证控制

定义 1　许可证　许可证一般分为用户许可证和功能许可证。用户许可证控制访问系统的用户数,功能许可证控制访问功能模块的用户数。

定义 2　分配组织许可证　实现组织和许可证之间多对多的关系。即一个组织可以拥有多个许可证,一个许可证可以分配给多个组织。

2.2　功能操作控制

功能操作控制层主要表示用户对系统功能和系统资源两个层面的访问控制。用户可以访问哪些系统功能,怎样访问这些功能;用户可以操作哪些系统资源,怎样操作这些资源。系统功能的访问控制和系统资源的访问控制最终反映到对系统页面的控制。一个用户拥有怎样的页面访问权限也就具有相应的系统功能及系统资源访问权限。操作控制层主要涉及到数据实体:用户、角色、权限、操作、资源;数据实体关系:用户角色分配、角色权限分配、权限操作、操作资源等。其模型如图 3 所示。

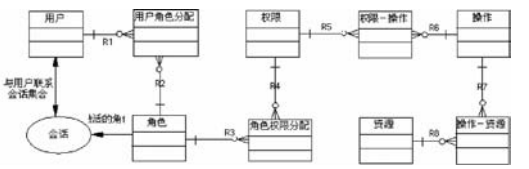

图 3　SaaS 功能操作控制模型

定义 3　资源　是系统所要保护的,可以被访问的对象。

定义 4　角色　角色对应于某一特定的工作岗位,是一组可执行任务的集合。在视图层面的控制,表现为角色的赋予,不同角色具有不同的功能视图。用户根据被赋予的角色个性化地使用系统。系统用户看到的页面视图范围为该用户所具有的所有角色所定义的视图的总和。其关系图如图 4 所示。

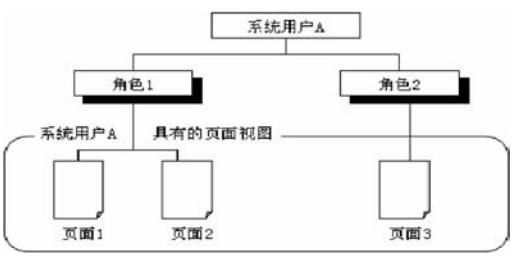

图 4　角色页面视图模型

定义 5　权限　权限是对计算机系统中的一个或多个数据对象进行某种方式访问的许可权,是数据操作任务访问数据资源的接口。权限分配的单位与载体,用来定义用户执行各种功能的权限。同时,还用于控制用户看到的各种页面布局和选项卡。

定义 6　用户　是权限的拥有者或主体。用户和权限实现分离,通过授权管理进行绑定。

定义 7　操作　完成资源的类别和访问策略之间的绑定。

定义 8　会话　一个会话是一个用户对多个角色的映射,当用户激活了部分或全部他被授予的角色时,他就建立了一个会话,用户实际上可以执行的任务是在这次会话期间被激活的角色的任务集。

定义 9　分配角色权限(PA)　权限配置表示权限和角色之间多对多的分配关系,即一个角色可以被授予多个权限,一个权限可以分配给多个角色。

定义 10　分配用户角色(UA)　分配用户表示用户和角色之间多对多的分配关系,即一个用户可以被授予多个角色,一个角色可以分配给多个用户。

定义 11　分配权限操作　分配权限操作表示权限与操作之间多对多的分配关系,即一个权限可以包含多个操作,一个操

作可以分配给多个权限。

定义 12 *分配操作资源* 分配操作资源表示操作与资源之间多对多的分配关系,即一个操作可以对应多个资源,一个资源可以分配给多个操作。

2.3 数据访问控制

现代企业内部之间的协作不断加强,企业之间的合作越来越紧密,根据不同的业务活动需要,在企业部门内部、企业部门之间、企业之间设立了不同的小组、虚拟组织等工作组织形式,有些组织中的员工虽然具有相同的功能操作权限,但具有不同的数据访问权限,这需要系统对数据访问进行严格、灵活的控制,数据访问控制层能很好地解决这些问题。数据访问控制层主要是对系统数据访问进行控制,控制系统数据的访问权限及数据的共享权限。不同级别用户群体具有不同的数据访问权限;不同机构用户群体具有不同的数据共享权限。其模型如图 5 所示。

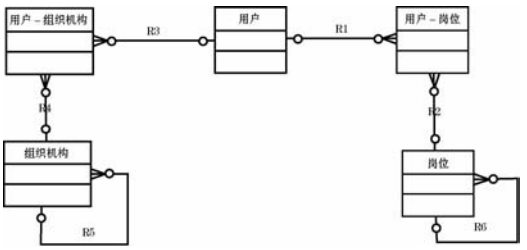

图 5 SaaS 数据访问控制模型

定义 13 *岗位* 是一个企业的某个部门的职位(相当于在部门下有相同职能的员工的集合),它隶属于某个具体的部门,并且可以有一个或多个员工在岗位上任职。一般情况是一人一岗,同时提供一人多岗的功能,以完成权限在数据层面的灵活控制。一个系统用户如果有两个岗位,那么他只能看到当前岗位下的数据,通过岗位切换,可以达到查看所属其它岗位下的数据信息。另外岗位有上下级关系,上级可以查看下级的数据,下级不能访问上级的数据,平级之间不能互相访问。其关系图如图 6 所示。

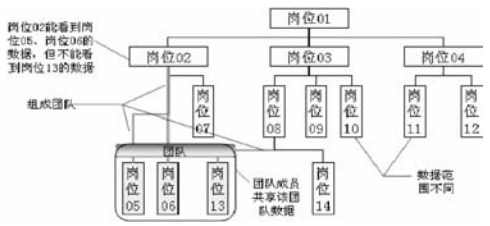

图 6 SaaS 岗位关系

定义 14 *用户* 是权限的拥有者或主体。用户和权限实现分离,通过授权管理进行绑定。

定义 15 *组织机构* 根据不同用户属性划分的用户群体。在一个企业内部可以划分为部门、小组等不同组织形式;在企业之间可以划分为小组、虚拟团队等不同组织形式。一个部门可以划分多个小组,一个小组可以包含多个用户;部门跟用户存在一对多的关系,用户小组跟用户存在多对多的关系。组织机构与用户之间的关系具有多样性、灵活性,根据不同的业务活动需要可以进行细化。

定义 16 *分配用户岗位* 表示用户与岗位之间多对多的分配关系,即一个用户可以拥有多个岗位,一个岗位可以分配给多个用户。

3 结束语

本文论述了一种基于 RBAC 模型的 SaaS 系统权限管理模型的研究。该权限管理模型已成功应用于系统的设计和开发实践,与应用系统具有很好的集成。实践表明,采用基于 RBAC 模型的新系统权限管理模型表现出以下优点:(1)采用分层思想实现权限管理,有利于权限控制与管理。(2)权限分配直观、容易理解,便于使用。(3)扩展性好,支持岗位、权限多变的需求。(4)通过资源的细分,为系统提供了不同粒度的权限控制。特别是将权限粒度控制到页面一级,并通过不同用户到不同页面的映射,可以实现用户界面的定制,实现了更大的灵活性。

参 考 文 献

[1] 周文峰,尤军考,何基香. 基于 RBAC 模型的权限管理系统设计与实现[J]. 微计算机信息,2006,22(5):35-36,155.

[2] 吴耀华,李宁. 适用于 B/S 结构的 RBAC 模型研究及实现[J]. 计算机应用,2004,24(12):84-87.

[3] 韩若飞,汪厚祥. 基于任务·角色的访问控制模型研究[J]. 计算机工程与设计,2007,28(4):800-803.

[4] 田敬东,何再朗,王向东,等. 基于角色的强制访问控制模型研究[J]. 电子科技大学学报, 2006,35(6):950-952.

[5] 李志英,黄强,楼新远,等. RBAC 模型研究、改进与实现[J]. 计算机应用,2006,26(12):2945-2947.

[6] 许春根,江于,严悍. 基于角色访问控制的动态建模[J]. 计算机工程,2002,28(1):116,118.

[7] 乔颖,须德,戴国忠. 一种基于角色访问控制(RBAC)的新模型及其实现机制[J]. 计算机研究与发展,2000,37(1):37-44.

[8] 陈风珍,洪帆. 基于任务的访问控制(TBAC)模型[J]. 小型微型计算机系统,2003,24(3):621-624.

[9] 付松龄,谭庆平. 基于任务和角色的分布式工作流安全模型[J]. 国防科技大学学报,2004,26(3):57-62.

[10] 邓集波,洪帆. 基于任务的访问控制模型[J]. 软件学报,2003,14(1):76-82.

[11] 李卿,乔元松,郑慧. 角色分离的层次化 RBAC 模型[J]. 计算机工程与设计,2005,26(6):1563-1565.

[12] 李帆,郑纬民. 基于角色与组织的访问控制模型[J]. 计算机工程与设计,2005,26(8):2136-2140.

[13] 程玉松,孟丽荣,盛琦,等. 利用规则 RBAC 模型实现门户的安全访问控制[J]. 计算机工程与设计,2005,26(5):1299-1301.

(上接第 41 页)

参 考 文 献

[1] Feldman M, Chuang C. Overcoming free riding behavior in peer-to-peer systems [J]. ACM SIGecom Exchanges, 2005, 5 (4): 41-50.

[2] 时金桥,程晓明. 匿名通信系统中自私行为的惩罚机制研究[J]. 通信学报,2006,27(2):80-86.

[3] 金瑜,古志民. 对等网中基于声誉的信任关键问题综述[J]. 小型微型计算机系统,2007,28(9):1604-1609.

[4] Reiter M K, Rubin A D. Crowds: anonymity for web transactions [J]. ACM Transactions on Information and System Security, November 1998, 1(1): 66-92.