SharePoint 中基于角色的访问控制体系的研究

王 韦,王 颖
(华北电力大学 计算机科学与技术学院,北京 102206)

摘 要:介绍了在企业信息化发展的过程中,企业门户的应用背景、特点以及普遍采取的三种访问控制方法。讨论了SharePoint门户的体系结构和基于角色的访问控制体系,并在此基础上讨论了基于SharePoint门户的体系结构对RBAC方法的扩展应用,以及该体系结构所采用的层级继承和安全策略。将SharePoint中的RBAC体系与Windows Server 2003操作系统的NTFS权限进行了比较,指出了其中的优点和不足。通过将Windows Server 2003操作系统的活动目录与SharePoint中的RBAC体系进行结合,提供一个更为安全的企业门户平台。

关键词:SharePoint;RBAC;门户;NTFS权限
中图分类号:TP311.5 **文献标识码**:A **文章编号**:1673-629X(2009)07-0163-03

Research on RBAC Systems in SharePoint

WANG Wei, WANG Ying
(College of Computer Sci. and Techn., North China Electric Power University, Beijing 102206, China)

Abstract: Introduce the application background of enterprise portal and the access control methods adopted during the process of the enterprise information development. Then architecture of SharePoint portal and the RBAC systems adopted by SharePoint is discussed in detail, and then talk about the hierarchy-inherit and the security strategy. At last, compare the RBAC systems in SharePoint portal with NTFS rights system in Windows Server 2003 OS, and then point out the advantage and shortage of the RBAC systems in SharePoint portal. Through combining the active directory with RBAC systems in SharePoint, can provide a safe enterprise portal platform.

Key words: SharePoint; RBAC; portal; NTFS rights

0 引 言

随着网络的日益普及,信息化技术的日益成熟,企业信息化已经成为各个企事业单位整合现有系统资源,共享数据和信息,提高工作效率的必然选择。而企业门户(Enterprise Portal)的出现为企业的信息化建设提供了很好的解决方案。

企业门户[1]是一种基于B/S结构的应用程序解决方案,通过它可以将企业内部的各应用系统、数据库、电子邮件等资源集成起来,从而形成一个统一的应用平台。借助企业门户这个平台,可以使得用户能够轻松地共享数据和信息,简化彼此之间的沟通和协作;提供单一的访问路径;基于用户的角色来提供个性化的界面和信息。最终达到通过企业门户来提高用户的工作效率,为企业的经营、管理和决策提供支持的目的。但是,企业门户中的用户群体比较庞大,所具备的权限又不尽相同,而存储的信息也很复杂,如何有效地控制用户对信息采取操作的权限,从而保证信息数据的安全,成为企业信息化过程中比较关切的问题。目前存在三种用于控制用户针对特定信息采取特定操作的方法,分别是:自主型访问控制(DAC),强制性访问控制(MAC)[2],以及基于角色的访问控制(RBAC)。其中基于角色的访问控制将用户和他的具体权限分离开来,从而能更灵活地控制用户所具有的权限。

文中接下来,将结合SharePoint门户的体系结构,来讨论其中采用的基于角色的访问控制体系。

1 基本理论

Microsoft Office SharePoint Server 2007(MOSS)是一种基于Windows SharePoint Services 3.0(WSS)技术的新型服务器应用程序。

WSS提供的基本功能,如SharePoint站点、列表、文档库、文档协作等在MOSS中都是可用的,并在此基础上进行了扩充,提供了诸如企业搜索、Business

收稿日期:2008-10-12;**修回日期**:2009-01-16
基金项目:国家自然科学基金资助项目(60305009)
作者简介:王 韦(1983-),男,硕士研究生,研究方向为企业信息化与系统安全;王 颖,教授,硕士生导师,研究方向为企业信息化、地理信息系统(GIS)等。

Data Catalog、Web 内容管理等功能，使企业能够简化协作、实现内容管理功能、实施业务流程，并能够进行很好的扩展和集成。

1.1 SharePoint 门户的体系结构

SharePoint 门户构建在 Web 应用程序的基础上，对应于一个独立的网站集。Web 应用程序构建在以 Windows Server 2003 为操作系统，以 SQL Server 2005 为内容数据库和配置数据库的数据存储，以 IIS 6.0 提供的 ASP.NET 2.0 为支持的服务器场环境中。而网站集是由顶级网站及其所属的子网站组成，每个子网站又可以包含自己的子网站以及列表和库等内容。图 1 即为 SharePoint 门户体系结构[3]的示意图。

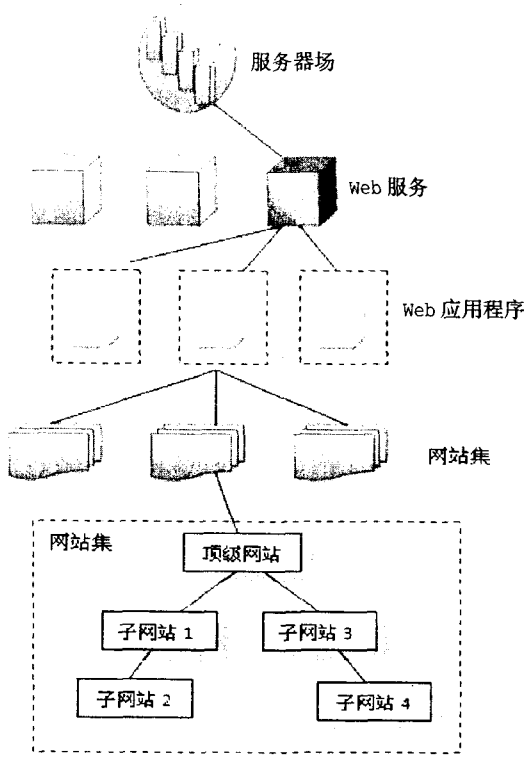

图 1 SharePoint 门户体系结构图

1.2 基于角色的访问控制

2000 年，Ravi Sandhu 等人提出了基于角色的访问控制(Role - Based Access Control，RBAC)的标准模型，其基本思想是根据组织中不同的职责创建角色，适当的访问操作权限被封装在角色中，然后将角色指派给用户，具有相应角色的用户才能够访问信息资源。由于实现了用户与访问权限的逻辑分离，从而方便了权限的管理。

RBAC 模型[4]由三个实体组成，分别为：用户、角色、权限。三者之间的关系如图 2 所示。在 RBAC 模型中，角色对应于一组权限的集合，不同的角色对应的权限集合中包含的权限是不同的，两者之间是多对多的关系，可用二元组：{角色，权限}来表示；用户和角色之间也是多对多的关系，一个用户可以分配多种角色，同一角色可以包括多个用户，可用二元组：{用户，角色}表示[5]。

图 2 RBAC 中的实体关系图

2 SharePoint 中的 RBAC 体系

SharePoint 门户提供了完整的基于角色的访问控制体系，该体系是基于 SharePoint 门户自身的体系结构和基于角色的访问控制模型，并进行相应的扩展来实现的。

2.1 SharePoint 中的 RBAC 组成

在 SharePoint 中，基于角色的访问控制(RBAC)体系由三个部分组成，分别为：用户、权限级别、安全对象[6]。其中用户包括单个的用户和用户组；权限级别对应于角色，是指一组权限的集合，只能够在网站级别进行定义；安全对象指的是对用户指定角色后进行操作的目标，根据 SharePoint 门户的体系结构，安全对象可以划分为不同的范围。上述三部分之间的关系如图 3 所示[3]。

由图 3 可知，为用户分配权限可以分为两种：针对特定的安全对象，将特定的角色指派给用户组，然后将用户添加到分配了角色的用户组中；或者针对特定的安全对象，直接将角色分配给用户。

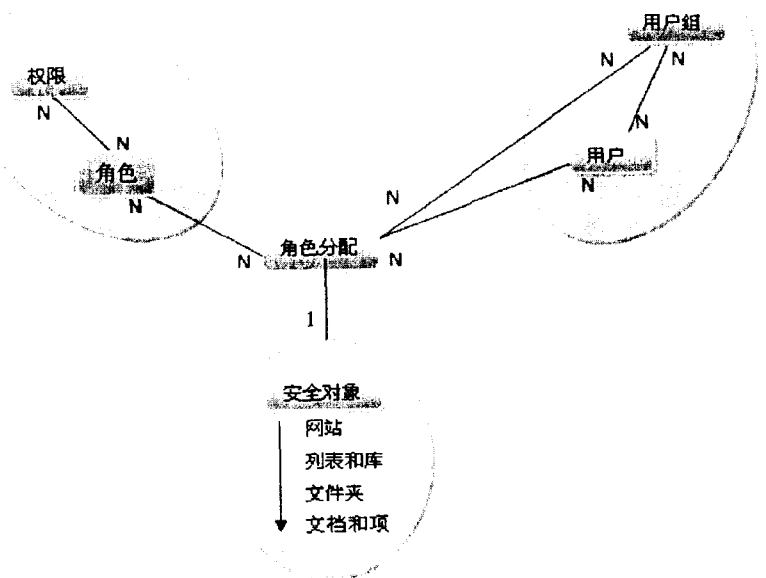

图 3 SharePoint 中的访问控制模型

2.2 SharePoint 中的权限继承管理

SharePoint 门户体系是树状结构的,具有良好的层次性和逻辑性[7]。因而用户在各个层次的网站中可以拥有不同的角色,这些角色之间既可以保持相对的独立,也可以存在一定的继承关系。

结合图 1 中的 SharePoint 门户体系结构图,来阐述其中的权限继承管理。一个网站集对应于一个门户,由一个顶级网站和若干个子网站组成。图 1 中的子网站 1,2,3,4 均为顶级网站的子网站。

SharePoint 门户中各个网站间的权限继承关系如下:

(1)子网站 1 从顶级网站继承权限:子网站 1 会继承顶级网站中定义的角色,但不能定义新的角色,除非断开继承;对顶级网站中角色进行更改会影响子网站 1;用户在顶级网站中拥有的角色适用于子网站 1;只能在顶级网站中来进行用户的添加和删除管理。

(2)子网站 2 从子网站 1 继承权限:与子网站 1 类似,子网站 2 会继承顶级网站中定义的角色,但不能定义新的角色,除非断开继承;对顶级网站中角色进行更改会影响子网站 1 和 2;用户在顶级网站中拥有的角色适用于子网站 1 和 2;只能在顶级网站中来进行用户的添加和删除管理。

(3)子网站 3 断开从顶级网站的继承:子网站 3 继承顶级网站中定义的角色,并且可以定义新角色;用户在顶级网站中拥有的权限不适用于子网站 3;可以恢复继承。

(4)子网站 4 从子网站 3 继承权限:子网站 4 继承子网站 3 中定义的新角色和顶级网站定义的角色,但不能定义新的角色;用户在顶级网站中的权限同样不适用于子网站 4,在子网站 3 中的权限适用于子网站 4;可以断开继承,然后定义新角色。

上述四种情况的用户权限继承关系同样适用于具体的网站,但只有在网站级别才能定义新的角色。由图 3 所知,每个具体的网站自上而下分别包括列表和库、文件夹、列表项和文档。

2.3 安全策略

安全策略也是基于角色的,是一个 Web 应用程序级别的权限控制策略,其优先级要高于网站级的权限控制。如果想临时限制某用户对门户网站的访问操作权限,而又不想在门户中对该用户具有的权限一一进行更改,可以在 Web 应用程序级别对其应用安全策略,来禁止该用户的访问权限。安全策略作为普通的访问控制策略的一个补充,可以方便对用户的特殊权限进行有效的控制。

除此之外,还可以在 Web 应用程序级别来禁止某些权限的使用,从而有效地控制角色中的权限组成。这样,即便用户对应的角色中包含该权限,也不会发挥作用。

2.4 规划门户的 RBAC 体系

SharePoint 门户中,可以直接对单个的用户授予某个角色,也可以将角色授予某个用户组,然后将用户加入到该用户组中。应当根据门户的应用规模,去制定相应的体系。对于用户数特别大的门户,应当尽量避免针对具体用户授予角色,而是将用户添加到特定的用户组中,从而提高门户的易维护性和灵活性。

鉴于 SharePoint 门户中的权限继承关系,在规划门户体系结构的时候,应当充分利用权限的继承性。将非敏感数据存放到上层网站中设置宽松的访问权限,将敏感数据存放到下层网站中,并断开继承,单独进行紧密权限的分配。

3 SharePoint 与 NTFS 的对比及扩展

在 Windows 操作系统中,NTFS 磁盘提供了许多数据管理功能,可以通过 NTFS 权限设置用户对文件的使用权限,其基本原理也是基于角色的访问控制[8]。NTFS 权限体系中的"权限"对应于 RBAC 模型中的"角色",而"细项权限"对应于 RBAC 模型中的"权限"。而 NTFS 使用的是活动目录中的用户和安全组,可以将权限授予用户或者安全组。表 1 对 SharePoint 和 NTFS 中的权限体系进行了比较[7,9]。

表 1　SharePoint 和 NTFS 中的权限体系比较

	SharePoint 中的 RBAC 体系	Windows 中的 NTFS 体系
继承性	具有继承性,并且可断开继承	具有继承性,可以断开继承
累加性	具有累加性。用户对某个安全对象的有效权限是其所有权限来源的总和	具有累加性。用户的有效权限为其所有权限的总和
覆盖性	不具有覆盖性。没有"拒绝"权限的存在;文档权限不能覆盖文件夹的权限,而是两者进行累加	具有覆盖性。"拒绝"权限会覆盖所有其他的权限。文件权限会覆盖文件夹的权限
角色的定义	只能在网站级别进行角色的定义,不能对文档库、列表及以下的安全对象定义角色	可以针对 NTFS 磁盘、文件夹和文件分别进行权限(对应于角色)的定义
组的嵌套	SharePoint 中的用户组之间不具备嵌套性	NTFS 基于活动目录的安全组,可以进行嵌套

通过上表的比较,可以发现 SharePoint 的 RBAC 体系有它的优点和不足。其中 SharePoint 中的用户组之间不具备嵌套性,可以通过 Windows Server 操作系统的活动目录[8]进行弥补。基于活动目录的 SharePoint 内网门户,可以实现安全组之间的嵌套,然后再将嵌套的安全组添加到 SharePoint 的用户组中,从而变相地实现 SharePoint 用户组的嵌套。

(下转第 202 页)

2)信息包的重放:攻击者窃听传输过程中的信息包,假冒 RADIUS Server,向 NAS 作出响应,用于重放攻击,因此是否可防重放攻击是协议安全的一个重要因素。

3)加密算法:如果攻击者不能直接得到密钥的信息,就会考虑攻击算法来破解用户口令,由上面的流程中可以看出,User - Password,Access - Accept 及 Response - Auth 会成为攻击者的切入点。

因此,RADIUS 协议的安全性是影响认证系统能否安全认证、安全授权和安全计费的关键问题。从以上的分析可以看出,由于在认证过程中传输的数据容易被窃听,系统易引起重播攻击,而且密码算法的弱点使得用户口令及 NAS 和 RADIUS 服务器间共享密钥的保护成为关键。因此就要从体系结构上进行合理设计,同时,在服务管理策略上,从数据传输、认证计费流程设计等方面都采取了相应的改进措施,以尽可能地弥补 RADIUS 协议在安全性上的缺陷。

5 结束语

基于 RADIUS 的 AAA 计费和认证管理系统能够为网络时代提供安全可靠和高效的网络服务,这些都是由它合理的体系结构和特点以及开放性和可扩展性所决定的。

文中研究了 RADIUS 协议的认证机制以及在 Linux 环境下 RADIUS 服务器的配置方法,同时它的缺陷也是不容忽视的,文中对 RADIUS 协议的安全性作了分析。对那些对用户的控制、计费与管理要求较高的网络来说,可以考虑从协议自身进行优化扩展以提高其安全性,这些还都有待于进一步研究。

参考文献:

[1] 李 倩. AAA 认证协议的分析[J]. 北京工商大学学报,2006,24(4):45 - 47.

[2] Rigney C, Willens S, Rubens A, et al. Remote Authentication Dial in User Service (RADIUS)[S]. RFC 2865,2000.

[3] Rigney C. RADIUS Accounting[S]. RFC 2866,2000.

[4] 张 琪,喻占武,李 锐,等. 基于 AAA 服务的协议分析与比较[J]. 计算机应用研究,2007(2):296 - 298.

[5] 黄永锋,王 滨,许晓东. RADIUS 在 802.1x 中的应用[J]. 计算机工程与设计,2006,27(5):798 - 801.

[6] 兰丽娜,石瑞生. RADIUS 协议安全机制研究及改进办法初探[J]. 信息安全与通信保密,2007(6):118 - 120.

[7] 鄢野春,佘 望,聂为清,等. 利用 RADIUS 进行 FTTH 宽带网络认证[J]. 计算机技术与发展,2006,16(5):310 - 312.

[8] 梁 根. 基于 RADIUS 的校园网认证管理系统的研究与实现[J]. 计算机技术与发展,2006,16(6):43 - 44.

(上接第 165 页)

4 结束语

通过对 SharePoint 中的 RBAC 体系进行研究,使我们熟悉了 SharePoint 门户的层次结构,以及基于该层次结构的权限继承与管理,可以通过结合网站层次结构和权限继承原理[3],来优化 SharePoint 门户的权限分配管理。除此之外,还可以结合操作系统的活动目录数据库,来对 SharePoint 用户组的嵌套功能进行扩展。

由于 SharePoint 采用了层次式结构的网站架构,从而实现了文档和列表项级别的权限管理,即条目级的权限。每个文档和列表项都包含若干个属性,甚至可以扩展现有的类来实现属性的权限管理,从而实现完整的基于角色的访问控制体系,构筑安全的门户网站。

参考文献:

[1] 崔松健. 基于 WebLogic 的企业门户安全设计[J]. 实验科学与技术,2005(1):43 - 45.

[2] 景栋盛,杨季文. 一种基于任务和角色的访问控制模型及其应用[J]. 计算机技术与发展,2006,16(2):212 - 214.

[3] PattisonT, Larson D. Inside Microsoft Windows SharePoint Services Version 3.0[M]. USA: Microsoft Press,2007.

[4] Osborn S,Sandhu R,Munawer Q. Configuring role based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security,2000,3(2):123 - 132.

[5] 孟庆荣. 协同编辑中访问控制模型的设计与实现[J]. 计算机技术与发展,2007,17(2):72 - 74.

[6] 任善全,吕 强,钱培德. 基于角色的权限分配和管理中的方法[J]. 微机发展(现更名:计算机技术与发展),2004,14(12):65 - 66.

[7] English B. Microsoft Share Point Server 2007 Administrator's Companion[M]. USA: Microsoft Press,2007.

[8] 戴有炜. Windows Server 2003 用户管理指南[M]. 北京:清华大学出版社,2007.

[9] 覃章荣,王 强,欧镇进,等. 基于角色的权限管理方法的改进与应用[J]. 计算机工程与设计,2007,28(6):1282 - 1284.