.NET环境下基于RBAC的Web应用程序访问控制

宋 昕,夏 辉,王学通
(西安理工大学 计算机科学与工程学院,陕西 西安 710048)

摘 要:文中从目前Web应用系统的变化趋势及其面临的安全问题出发,提出一种基于RBAC模型的访问控制方案。该方案以.NET环境为平台,以角色为中介,把用户和Web资源联系起来。在为Web资源分配角色的同时给用户分配角色,这样具有一定角色的用户就可以访问到该角色所许可的资源,从而实现了基于角色的访问控制。该方案简化了访问控制的操作,具有较大的灵活性,使系统的安全性得到提高。最后,给出了结论并指出需进一步研究的问题和改进方法。

关键词:RBAC;.NET;访问控制
中图分类号:TP393 **文献标识码**:A **文章编号**:1005-3751(2006)04-0218-03

Access Control of Web Application Based on RBAC model in .NET Environment

SONG Xin, XIA Hui, WANG Xue-tong
(Computer Science & Engineering College, Xi'an University of Technology, Xi'an 710048, China)

Abstract: According to the ever-changing trend of Web application systems and the security problems they face, provides a RBAC-based access control implementation for Web applications. With roles sitting in the middle of users and Web resources, users and Web resources are both allocated to different roles by using .NET platform, so a user with certain roles can access resources with the same ones. This kind of flexible implementation simplifies the operation of access control and promotes the system security. At the end of this paper, conclusion and improvements are given.

Key words: RBAC; .NET; access control

0 引 言

随着万维网进一步的应用与发展,人们对它所提供的服务提出了更高的要求。在早期人们使用万维网来共享与交流超文本信息,这也是Tim BL在CERN设计HTML时的初衷,即通过浏览器访问Web服务器中存放的超文本信息和资源。这种信息共享方式得到了迅速的发展,使用者也越来越多,慢慢的一些更高的需求也提了出来,比如:Web技术从最早期的静态网页技术发展到动态网页技术。而需求没有就此停止,现在人们除了通过浏览器来访问信息资源外,还希望通过它完成一些类似应用程序的功能,比如电子商务网站和游戏网站,人们在这些网站上浏览信息的同时还完成了其他的功能,如填写用户信用卡信息在线购买商品,进行分布式网络游戏等等。因此Web应用提供的服务发生了变化,提供给用户的资源越来越多,而且资源本身并不是对所有用户都开放的,与此同时,服务的消费者不再仅仅是单一的网站浏览用户,他们还可能是网站的一般会员、高级会员,甚至是在线管理员等等。由于资源的多样性和用户的多样性就要求在资源和用户之间建立访问控制关系,以便对系统进行更好的组织和管理。

收稿日期:2005-08-02
作者简介:宋 昕(1977-),男,陕西人,助教,硕士,研究方向为计算机网络及应用。

1 RBAC模型

早在20世纪70年代就有人在多用户系统中对用户访问权限管理的问题进行了研究,即如何控制用户对资源的访问,他们把这称之为RBAC(Role-Based Access Control,基于角色的访问控制)。1996年Ravi S. Sandhu等人提出了通用的RBAC模型[1]。此模型有3个实体:用户、角色和访问权限(如图1所示)。其核心思想是:受保护资源的访问权限与角色相联系,而给用户分配各种角色;用户与所要求访问的资源之间没有直接关系,若用户要访问某一资源,那他必须具有可访问此资源的角色。

图1 RBAC模型

在RBAC中,引入了"角色"这一重要概念。所谓角色,就是一个或者一群用户在系统内可执行的操作的集合。例如,一个网站访问者的角色可以有一般浏览者、一般会员、高级会员、网站管理员、栏目管理员等,而这些角

色又可对网站的结构、内容、以及访问者进行增、删、查、改等操作。由于用户的角色不同,所拥有的访问权限显然也各不相同。RBAC 根据用户在系统内所处的角色进行访问授权与控制。也就是说,传统的访问控制直接将用户和所访问的资源相联系,而 RBAC 在中间加入了角色,通过角色沟通用户与资源。一个用户可经授权而拥有多个角色,一个角色可由多个用户使用;每个角色可执行多种操作,每个操作也可由不同的角色执行。而且在实际生活中,一旦一个用户的角色被设定后,角色改变并不频繁。相比之下在 Web 系统中,由于系统的组织结构或者功能经常变化,用户对受保护资源的存取权限变化更频繁。如果让用户直接与访问权限相联系,那么访问权限的维护量大而复杂。但是如果系统将用户与其具有的角色相联系,则这种关系相对而言更持久,维护工作更系统化。这样的授权管理与针对个体的授权相比较,可操作性和可管理性都要强很多。因此通过角色这一中介极大地简化了对用户和访问权限的管理。

2　实　现

按照 RBAC 模型,要对 Web 上的应用程序进行访问控制,首先要将各种实体信息(用户、角色、访问权限)和实体之间相互关系信息表示出来。

用户信息和用户角色信息比较清楚,是一些用户代号、密码、角色代号和角色名称,这些信息可以直接存放在数据库中。但受保护的资源如何表示?它们与角色之间的关系又如何表示?事实上,在 Web 中对一定资源的访问都可以通过 URL 来进行[2],因此可以用 URL 来表示资源,而且对资源(URL)的访问权限只有两种,即允许或者拒绝。因此,可以建立图 2 中 ProtectedURLs 数据表,表的第一个字段描述了受保护的资源,即 URL;另一个字段中描述角色,如果一个 URL 可被多个角色访问,则角色和角色之间用逗号分开,比如如下记录:

URL	RoleID
Http://MySite/Default.asp	1,2,3

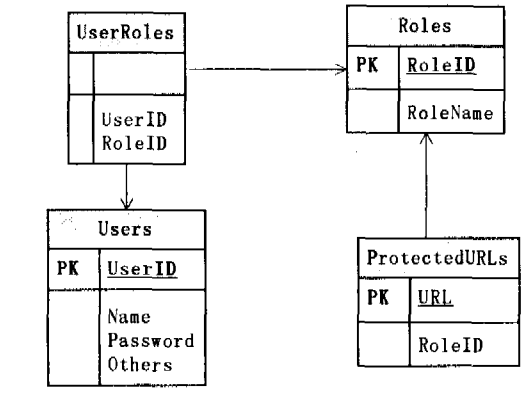

图 2　用户、角色、URL 信息表

通过增加或删除 RoleID 字段中的角色代号(1,2,3)来允许或拒绝特定角色对特定 URL(Http://MySite/Default.asp)的访问。

这样定义以后就可以按照用户所具有的角色信息来判断他是否有访问资源的(URL)的权力。将所有在 Web 应用中使用的访问控制信息存放到数据库中,以便通过这些信息实施对用户访问的控制,故建立以下数据表(如图 3 所示)。

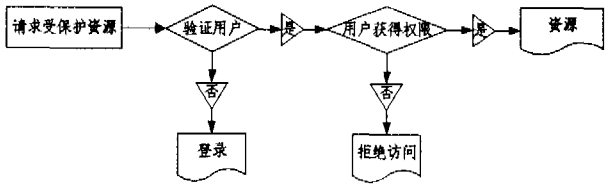

图 3　基于 RBAC 的访问过程

基于角色访问控制的各种所需信息通过以上 4 个数据表已经表示出来,接下来就是如何在服务器和客户端读取和使用这些信息,从而对用户的访问需求进行判断。ASP.NET 和.NET Framework 联合 IIS 为 Web 应用程序安全提供了一个基础,它的明显优势在于,不必再编写自己的安全架构。.NET Framework 已提供了 3 种不同类型的身份验证方式:Windows 身份验证、Passport 身份验证、和窗体身份验证[3]。文中所采用的就是通过窗体身份验证方式(即一组模块和类:FormsAuthenticationModule, FormsAuthentication, FormsIdentity, FormsAuthetication Ticket)对数据库中的用户信息作出判断,并将用户信息填写入 cookie 存放在客户端。当用户再次访问受保护资源时浏览器会自动提供这些 cookie,服务器端的验证程序再根据这些 cookie 对用户进行验证。用户访问 Web 应用程序的过程如下[4]:

(1)用户对资源(URL)的访问请求被发送到 Web 服务器。

(2)用户提供 ID、密码,这些凭证由身份验证应用程序进行验证。根据用户提供凭证的方式分为两种情况:若用户初次访问,则用户标识还未被确认,所以这个用户会被定向到一个登录页面,以便用户输入凭证信息,若凭证有效则将用户 ID 存放到服务器端的 HttpContext.User 对象中,同时向客户端发送一个包含用户 ID 的 cookie。若用户是再次访问,则用户 ID 信息已经在客户端的 cookie 中,这个 cookie 会自动由浏览器提交到服务器上进行验证。

(3)服务器首先根据用户的 ID 查找出用户的角色,然后根据用户所访问的 URL 查找此 URL 许可的访问角色,最后将这两个角色(或角色集合)进行对比若相同(或交集不为空)则用户可以访问资源,同时填写第二个 cookie,这个 cookie 主要包含用户的角色信息。否则,用户访问被拒绝。

(4)被拒绝的访问用户要么被提示用被请求资源的合适凭证进行登录,要么被重定向到一个"访问被拒绝"的 Web 页面。

上述过程中使用了用户 ID cookie 和角色 cookie。第一个 cookie 的作用在于不必使用户在同一段时间内反复

登录,如果用户在某个时间段,每访问一次受保护资源都要登录一次会使用户感到非常厌倦,而且系统运行的效率也不高。第二个 cookie 作用在于减少对服务器通过用户 ID 查找用户角色的次数,提高运行效率。

3 关键技术

Web 应用通过 HTTP 协议进行通信,而 HTTP 协议是无连接的应用层协议,因此要在 Web 上实现应用程序的访问控制,如何让服务器知道用户的身份就成了一个需要解决的问题。而在上文的实现过程中使用了 cookie,通过 cookie 存放用户身份并保持用户和服务器之间的联系。但使用 cookie 传递信息安全性很差,主要表现在 3 个方面[5]:

* 如果 cookie 明文传递,那么就有可能在传输过程中被其他人窃听;

* cookie 一般存放在用户的硬盘上,容易被非法用户进行拷贝;

* 如果非法用户通过假冒某个服务器站点来接受用户的 cookies,以后他就可以使用这些收集到的 cookies 来对那些应该接收这些 cookies 的站点发动攻击。

由此可见,要在 Web 上实现基于角色的访问控制,其中一个必要的前提是所传递的 cookie 必须是安全的,因此为了保证上述过程的安全实现,需要做如下改进:

(1)在 Web 服务器上安装 SSL,以防止他人在 cookie 传递过程中进行窃听。

(2)将上述两个 cookie 加密后再发给客户端浏览器。

(3)利用 ASP.NET 提供的功能,将 cookie 存放到浏览器的内存中,这样可以防止他人从硬盘上拷贝 cookie。

以上改进很好地保证了 cookie 在客户端与服务器之间传递时的安全,其中(2)和(3)利用 ASP.NET 提供的类可以方便地实现。

4 结束语

基于角色的访问控制机制为管理用户与受保护资源提供了便利。文中从 Web 应用目前的发展状况与需求出发,分析了 Web 应用所需要的访问控制方式,并在此基础上采用 RBAC 模型,实现了在.NET 环境下的 Web 应用程序访问控制。

参考文献:

[1] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based access models[J]. IEEE Computer, 1996, 29(2): 38-47.

[2] Barkley J F, Cincotta A V, Ferraiolo D F, et al. Role Based Access Control for the World Wide Web[A]. Proc of 20th NIST-NCSC National Information Systems Security Conference, National Institute of Standards and Technology[C]. Baltimore, Maryland, U.S.A.: [s.n.], 1997.

[3] 李敏波. ASP.NET 1.1 高级编程[M]. 北京:清华大学出版社,2005.

[4] Gaster B, Kent D, Sabbadin E, et al. ASP.NET 安全性高级编程[M]. 北京:清华大学出版社,2003.

[5] Park J S, Sandhu R, Gail-Joon Ahn. Role-Based Access Control on the Web[J]. ACM Transactions on Information and System Security, 2001, 4(1): 37-71.

(上接第 217 页)

显得极为重要。

本系统通过 VPN 实时地将这些数据写入到证据库中保存起来,被传送的数据一旦写入证据库,就使用 MD5 对存储的数据进行数字签名,使这些原始数据具有不可篡改性。

使用 VPN 通道提供强壮的认证和加密通信的优点在于:

①数据在传送前首先通过 VPN 认证,保证信息在传送过程中不被窃取;

②数据在传送前就已加密,因此没有任何明文数据在网络中传送;

③数据送达到证据库后,进行解密,以明文形式存储下来,同时使用 MD5 加密算法进行数字签名,以防数据被篡改。

5 结束语

计算机取证是网络诉讼的核心,是当前计算机犯罪案件侦查的关键技术。本系统将计算机取证与入侵检测结合起来,采用基于协议分析的入侵检测方法,提高了入侵检测效率及数据分析能力,有助于解决动态取证的实时性;通过实时检测,根据入侵行为的类型,及时采取相应的响应措施,可以将入侵损失降到最低;同时系统采取了较全面的安全机制,以确保收集到的入侵证据的真实性、准确性及不可篡改性,使其成为有效的法庭证据。该系统是动态计算机取证的一种较好的解决方案。

参考文献:

[1] 钟秀玉,凌 捷. 计算机动态取证的数据分析与研究[J]. 计算机应用与软件,2004(9):26-27.

[2] 张 斌,李 辉. 计算机取证——有效打击计算机犯罪[J]. 网络安全技术与应用,2004(7):59-61.

[3] 唐正军,李建华. 入侵检测技术[M]. 北京:清华大学出版社,2004.208-211.

[4] 丁菊玲,刘晓洁,李 涛,等. 基于人工免疫的网络入侵动态取证[J]. 四川大学学报(工程科学版),2004,36(5):108-111.

[5] Kumar G. Classification and detection of computer intrusion [D]. Purdue University, 1995.

[6] 黄 文,文春生,欧红星. 分布式网络系统日志的安全性研究[J]. 零陵学院学报,2004,25(3):66-68.