文章编号:1005－0523(2005)01－0111－04

# NET 服务环境中的身份认证

裴冬菊[1],黄青云[2]

(1.华东交通大学 信息工程学院,江西.南昌 330013;2.江西农业大学 计算机与信息工程学院,江西 南昌 330045)

**摘要**:身份认证是网络安全的重要组成部分,也是.NET 的重要组成部分.本文简要介绍了.NET 服务环境、Web 服务和网络安全,重点阐述了.NET 服务环境中的身份认证技术.

**关 键 词**:.NET 服务环境;WEB 服务;网络安全;身份认证

**中图分类号**:TP39308　　**文献标识码**:A

## 1 引 言

随着网络应用广泛深入到社会生活的各个领域,网络安全已经成为网络界的核心问题.特别是电子商务的兴起,已经对网络信息安全提出了更高的要求.身份认证往往是网络安全的第一道防线,特别是重要的数据和信息被多位用户共享时,对用户真实身份和访问权限的确认显得特别重要.然而实现身份认证的技术有多种,每种技术实现身份认证各有千秋.Web Services(即 Web 服务)技术的出现,信息系统的开发和集成更加简单、广泛,面向 Web 服务的改造势在必行[1]..NET 平台为开发 Web 服务提供了很好的环境.了解.NET 平台下的身份认证就显得更加有必要.

本文首先介绍.NET 服务和 Web 服务,然后阐述网络安全和身份认证的概念和重要性,最后就.NET 服务这一新环境中的身份认证的几种方法一一进行阐述.

## 1 .NET 服务环境和 Web 服务

.NET 是一个平台,是一项革命性的技术框架,是一种将信息、用户、系统和设备连接在一起的软件技术,是 Microsoft 的 XML Web services 的运行平台,基本元素包括:开发工具、服务器、智能设备和 XML WEB Services[2].它提供了前所未有的集成技术,通过 XML Web 服务将许多大小不一的、分散的应用通过互联网连接在一起..NET 服务环境和 WEB 服务并非同一概念.NET 服务环境只是开发和调用 WEB 服务的一个平台,而 WEB 服务是一种自包含、自解释、模块化的应用,能够被发布、定位,并且从 Web 上的任何位置进行调用.Web 服务技术提出不久,但它代表了下一代网络计算和企业应用的必然趋势,可以执行从简单的请求到错综复杂的商业处理过程的任何功能.因此,各大公司在积极参与相应技术领域和规范规定的同时也投入巨大的力量,把企业产品和市场战略向 Web 服务转型.这种转变特别体现在电子商务的应用方面.

## 2 网络安全

网络正逐渐融入社会生活的方方面面,正在改变人们的生活方式、工作方式和思维方式,并已经成为一个国家政治、经济、文化、科技、军事和综合国力的重要标志.在看到网络对社会发展起到的正

**收稿日期**:2004－09－20

**作者简介**:裴冬菊(1976－),女,江西贵溪人,华东交通大学研究生.

面作用的同时,也必须注意到它的负面影响.个别不法分子利用网络从事非法活动.从1986年到现在,网络从各个方面受到攻击,使国家、企业和个人的利益蒙受损失.由此,保证网络的安全势在必行,它已成为信息化社会的一个焦点问题.

网络安全应该包括三个方面的内容:安全攻击、安全机制与安全服务.身份认证认证是网络安全服务的基本服务.它是用来确定网络中信息传送的源结点用户与目的结点用户的真实身份,避免出现假冒、伪装等现象,保证信息的真实性.

## 3 身份认证

身份认证是计算机系统的用户在进入系统或访问不同保护级别的系统资源时,系统确认该用户是否真实、合法和唯一[3].

### 3.1 身份认证的重要性

身份认证是安全技术的一个重要方面,是安全系统中的第一道关卡.用户在访问安全系统之前,首先根据系统设置,提供证书或用户名、密码等,经过身份认证系统识别身份,然后由安全系统根据用户的身份和授权数据库决定用户是否能够访问某个资源.一旦身份认证系统被攻破,那么系统的所有安全措施将形同虚设.黑客攻击的目标往往是身份认证系统,所以身份认证系统的设置对整个系统安全的健壮起决定性作用.

### 3.2 身份认证的各种技术

.NET身份认证验证技术,是Microsoft .NET的一个重要组成部分,是实现网络安全的重要机制之一.在安全的网络通信中,涉及的通信各方必须通过某种形式的身份验证机制来证明它们的身份,验证用户的身份与所宣称的是否一致,然后才能实现对于不同用户的访问控制和记录.

一般身份认证方法的过程是:当用户要求访问提供服务的系统时,系统要求提供该用户的口令,系统接收口令后,将其与系统存储的该用户的口令进行比较,如若相同,则认为是合法用户,否则,认为是非法用户.

这种身份认证方法的缺点在于:

1) 经过加密的口令在传输过程中有可能被截取,由于密文是固定不变的,所以攻击者可以利用截获的密文进行重新攻击.

2) 系统中所有用户的口令以文件形式存储在服务器端,攻击者可以利用系统中存在的漏洞获取系统的口令文件.

3) 只能进行单向认证,即系统可以认证用户,而用户不能对系统进行认证.

4) 没有用户访问控制,这样就可能造成数据泄密,可信度降低和破坏数据库的完整性.

笔者所介绍的身份认证是确定远程用户实际声明的身份的过程.这一远程用户身份认证方法可以用来解决以上问题.

#### 3.2.1 Windows身份认证

Windows身份认证是把身份认证的任务交给IIS(Internet Information Server)处理[4].IIS会向应用程序传递Windows用户账号,以及这个账号发送的、需要进行处理的请求.如果设置IIS要求用户进行登录,那么这个账号表示的就是发出请求的用户.使用Windows身份认证的好处有以下三点:(1)需要完成的工作少;(2)集成了IIS的安全性;(3)集成了Windows客户机.使用Windows进行身份认证的工作方式有:匿名访问、基本认证和Windows综合认证[5].

##### 3.2.1.1 匿名访问

在WEB上,许多工作站不需要提供用户认证.用户可以自由地访问站点,使用站点提供的服务.编程人员和网站管理者将访问这类站点的用户称为匿名用户.与之相同的,许多WEB服务认证认可这种匿名访问.通常默认情况下,一个.NET环境下的WEB服务创建后,自动支持匿名服务.但可以使用IIS来改变服务的认证级别.

利用Windows环境中的IIS来实现将匿名用户转换为应用基础上的特定的用户账号的步骤如下:

1) 打开"我的电脑",选择"控制面板",双击"管理工具".

2) 在管理工具窗口中,双击"Internet服务管理器"图标,进入Internet服务管理窗口.

3) 在Internet服务管理窗口中,展开工作站服务器定位的应用程序文件夹.右击文件夹,选择"属性".

4) 在属性对话框中选择"目录安全性",在目录安全表中,点击编辑按钮,弹出认证模式对话框.

5) 在认证模式对话框中,点击"匿名访问"功能框中的"编辑".Windows将显示一个匿名用户账号对话框,在这个对话框中,可以使用IIS给匿名用户制订一个用户账号.

匿名认证适合于那些不需要安全措施的WEB网页和WEB服务,也适于那些使用安全网络联接机制管理用户名和密码的工作站.

#### 3.2.1.2 基本认证

与匿名访问相反,基本认证需要用户提供合法的用户名和密码.当用户访问需要提供基本认证的基于 Web 服务动态网页时,浏览器会从有关用户名和密码的系统中获取信息.然后,浏览器将数据发送给服务器,接下来服务器决定准许还是拒绝用户访问系统中的 Web 服务.将服务器改为需要基本认证,执行的过程如下:

前几个步骤和将匿名用户转换为应用基础上的特定的用户账号的步骤相同.不同的就在于:在最后一步选择"验证访问"功能框中的基本验证,然后点击"确定".

这时,如果浏览器再一次请求服务器中的 Web 服务,服务器将要求浏览器提供用户的身份确认信息.浏览器发送并获取信息后,Web 服务会显示用户当前注册时所对应的账号的有关信息.如果在服务器上没有与用户登录信息相匹配的用户账号,则服务器将返回 HTTP 401 访问被拒绝的错误信息.

基本认证虽然提供了一个途径,要求用户提供有效的用户名和密码,然而,当一个程序将用户名和密码传给一个需要基本认证的服务器时,这些信息是以简单的文本形式传送的.这些以简单的文本形式传送的用户名和密码很容易被网上黑客监听,所以笔者建议要避免使用基本认证.

#### 3.2.1.3 WINDOWS 综合认证

综合认证最早被称为 WINDOWS NT 局域网管理器,利用散列码技术来保护密码信息.当客户程序连接到一个需要提供综合 WINDOWS 认证的页面上时,WEB 服务器会发送给客户程序一个随机数,客户程序用这个随机数加密密码.然后,客户程序将用户名、域名和加密的密码返回给服务器.接着,服务器将这些信息发送给域控制器,域控制器使用这些信息对用户进行认证.

### 3.2.2 分类认证

分类认证改变了基本认证以纯文本的密码提交方式的不足.要使用分类认证,用户必须拥有 WINDOWS 2000 域服务器.当服务器要求客户程序提供用户认证时,服务器会首先发送给客户程序相关信息,这些信息与用户名和密码结合起来生成一个特殊的结果,编程人员称之为单相无规律的信号.客户程序发送给服务器的不是单纯文本形式的用户名和密码,而是这些无规律的数据.编程人员称之为单向无规律信号是因为监听到这些信号的黑客很难,或者说几乎没有可能使用这些数据推出原始的用户名和密码.因为服务器知道原始的无规律信号,所以可以解析出用户名和密码.如果用户使用的是 WINDOWS 2000 域服务器,则可以使用认证模式对话框选择分类认证.

### 3.2.3 表单认证

在 WEB 上,很多工作站信赖表单认证.通常情况是,表单认证使用 COOKIE 将用户认证信息传递给 WEB 服务器提供安全认证需求.为了使用表单认证,用户必须通过一个加密连接登录到系统.系统认证用户后,返回给用户程序一个标记,客户程序可以用来在整个工作站上不同的页面实现用户认证.如果用户连接到一个身份还未经认证的页面上,服务器将变更请求,转到一个客户程序可以实现的用户认证的页面上.因为客户程序要与工作站进行交互,所以程序将认证标记存储在一个 COOKIE 中.如果客户程序不支持 COOKIE,表单认证将会失败.其中部分代码如下:identify1.aspx(管理人员身份检证程序)

```
<% if cookies("username")<>1 then
response.Redirect("error.asp")
else
cookies("username")=1
end if %>
```

我们可以在任何一个页面通过加上下面的代码就可以利用 identify1.aspx 实现表单认证,避免非法用户使用系统资源.

### 3.2.4 基于证书形式的认证

当创建一个需要提供用户认证的网络应用软件时,服务器程序要求客户程序以一个确认表单的形式提供用户的数字证书.在 Windows 2000 中,我们可将客户证书转换为特定的用户账号.在这种方式下,客户程序不必提交用户名和密码.

使用 IIS,可以指定一个页面或 Web 服务需要用户使用安全通信对话框提交客户证书.用户可以设置浏览器,当远程服务器提示浏览器提交数字证书时,使得浏览器可以自动地提交.如果用户创建自己的客户程序,则可以创建 x509Cretificate 类的一个实例,将文件中存在的证书对象赋予该实例.这样,用户就可以将证书对象赋予给 Web 服务对象.

### 3.2.5 使用 web.config 文件配置安全设置

web.config 文件是 ASP.NET 应用程序配置文件.该文件包含公共语言运行库读取的配置设置,以及应用程序可以读取的设置.ASP.NET 配置系统提供以下好处:

1) 配置信息存储在基于 XML 的文本文件中.您可以使用任何标准的文本编辑器或 XML 分析器来创建和编辑 ASP.NET 配置文件.

2) 多个配置文件(名称都是 Web.config)可以出现在 ASP.NET Web 应用程序服务器上的多个目录中.每个配置文件都将配置设置应用于它自己的目录和其下面的所有子目录.子目录中的配置文件可以提供除从父目录继承的配置信息,还可以重写或修改父目录中定义的设置.

3) 在运行时,ASP.NET 使用分层虚拟目录结构中 Web.config 文件提供的配置信息为每个唯一的 URL 资源计算一组配置设置.然后缓存结果配置设置,以供所有后面的对资源的请求使用.

4) ASP.NET 检测对配置文件的更改并自动将新配置设置应用于受该更改影响的 Web 资源.

5) ASP.NET 配置系统是可以扩展的.您可以定义新配置参数并编写配置节处理程序以对它们进行处理.

6) ASP.NET 通过配置 Internet 信息服务防止对配置文件的直接浏览器访问来保护配置文件不受外部访问.

ASP.NET 资源的配置信息包含在一组配置文件中,每个配置文件都包含 XML 标记和子标记的嵌套层次结构,这些标记带有指定配置设置的属性.这些标记必须是格式正确的 XML,所以标记、子标记和属性是区分大小写的.

在 Web.config 文件中可以设置定制错误消息是否可用;设置应用程序的认证策略,可允许或拒绝用户的访问;设置应用层的跟踪在应用程序的每页中是否打开输出跟踪日志;等等.下面 Web.config 文件示例声明配置<authentication>和<authentication>单元使得用户可以控制对 Web 服务的访问权限:

指定程序使用表单认证:<authentication mode="Forms" loginurl"=/login.aspx"/>

指定只允许名字为"admin"的用户访问:

<authentication> <allow users="admin"/> </authentication>

指定拒绝匿名用户访问:<authentication> <deny users="?"/> </authentication>

## 4 结束语

互联网的发展和信息技术的普及,给人们的工作和生活带来了前所未有的便利.然而,由于互联网所具有的广泛性和开放性,决定了互联网不可避免地存在着信息安全隐患.Web 服务代表了下一代网络计算和企业应用的必然趋势,要开发出新一代的具有安全性的 Web 服务,就有必要了解.NET 服务环境中的身份认证.笔者对本文介绍的各种身份认证验证成功,希望这些认证技术能为读者带来帮助.

**参考文献:**

[1] 李安渝,等.Web Serveices 技术与实现[M].北京:国防工业出版社,2003.

[2] 王兴玲,杨崇俊.基于.Net 平台的地理信息 Web 服务研究与应用[J].计算机工程与应用,2002:6-8.

[3] 董志文,沈国民.计算机网络系统的身份认证技术[J].网络安全,2002:88-91.

[4] Russ Basiura、Richard Conway. 王晓娜,黄开枝译.ASP.NET 安全性高级编程[M].北京:清华大学出版社,2003.

[5] Kris Jamsa.袁 然,邹丰义,等译.NET Web 服务解决方案应用编程[M].北京:电子工业出版社,2003.

# Identification Authentication of NET Services Environment

**PEI Dong-ju[1], HUANG Qing-yun[2]**

(1.School of Information and Eng., East China Jiaotong University, Nanchang 330013;2.School of Computer and Electronic Information, Agricultural University Nanchang, 330046, China)

**Abstract**: Identification Authentication is a crucial part of network security, and it is also very important to .NET. In most part of this article it illustrates the Identification Authentication technologies in .NET environment, and it also briefly introduces the .NET Service、Web Services and network security.

**Key words**: .NET services environment; WEB services; network security; identification authentication