# 基于网络的ASP服务平台安全模型的研究

王春风
(盐城工学院 现代教育技术中心,江苏 盐城 224003)

**摘要**:网络化制造ASP服务平台借助Web服务技术,通过浏览器和分布在不同地域的用户进行交互,如何保证Web服务调用的安全是系统开发和部署时应考虑的问题。本文根据网络化制造ASP服务平台的逻辑结构,从开发者的角度提出了针对ASP服务平台的安全模型,并给出了该安全模型的核心设计和实现。

**关键词**:ASP平台;ASP安全模型;资源访问控制
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1671-5322(2007)02-0043-04

网络化制造ASP服务平台是一个大型复杂的集成应用系统,它以Internet为媒介,借助Web服务技术,使处理复杂的业务和数据变得方便可行。但是,对于如何保证用户信息的安全、Web服务调用的安全、数据存储的安全和如何开发出健壮的代码不给黑客留任何漏洞等一系列问题[1]都是系统开发和部署时应该考虑的问题。

由于网络化制造ASP系统是一个新兴的研究课题,目前国内外对该课题的研究,特别是对这么一个复杂系统的安全性研究还没有成熟的成果可以借鉴,作为一个系统开发人员,非常有必要对网络化制造系统中的安全问题花费时间和精力进行深入研究,并在网络化制造ASP服务平台中具体实施。

## 1 ASP服务平台结构

网络化制造ASP服务平台(包括总平台和所有分平台)采用了典型的*N*层架构[2],程序结构分为3个逻辑层,从上到下分别是Web用户界面、业务规则、数据访问,其中还包括了通用组件和Web服务模块,其逻辑结构如图1所示:

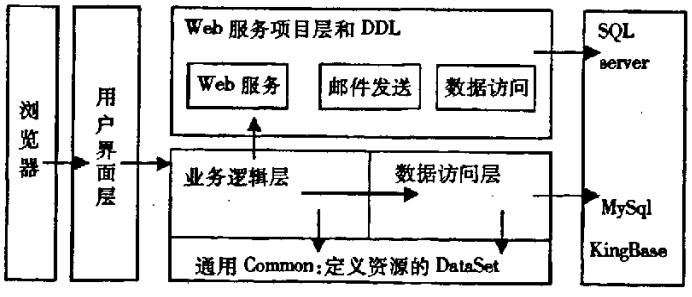


图1 网络化制造ASP服务平台的逻辑结构

Fig. 1 The logistic structure of Networked Manufacturing ASP platform

### 1.1 Web层

Web用户界面的功能包括:管理Web页的呈现和行为、显示数据、捕获数据、数据验证检查、为用户提供任务指南、向"业务外观"发送用户输入、从"业务外观"接收结果、向用户显示错误。

### 1.2 业务逻辑层

业务逻辑项目块包含业务对象本身以及应用于它们的规则。这也是主要业务对象所在的位

收稿日期:2007-01-30
作者简介:王春风(1979-),女,江苏南通人,讲师,硕士,主要研究方向为网络安全、虚拟现实、Internet交互技术。

置。它们实现业务实体或系统对象。系统的业务逻辑将在这些对象中编码,尽管部分业务逻辑可能实际上已在数据库的存储过程和触发器中进行了编码。业务逻辑从"Web 用户界面"接受服务请求,根据编码的业务逻辑处理请求,将处理结果传递回"Web 用户界面"层。如果需要操作数据库数据,则将数据发送到"数据访问"层,或从"数据访问"层中获取数据。平台在与其他子平台交互的时候,业务逻辑层就要与"Web 服务项目"层进行数据交互和信息传递。

### 1.3 数据访层

数据访问项目层为业务规则提供了数据服务,从数据库(或其他数据服务)获取数据或向数据库发送数据的功能。数据访问层还可以封装各种数据库的访问接口,在该平台中数据访问层从业务规则层接收请求,使用存储过程获取或操作数据,并将数据库查询结果返回到业务规则层。

### 1.4 Web 服务和组件

Web 服务使用基于 SOAP 的消息交换来实现防火墙移动数据和在异构系统之间移动数据,以此来实现数据交换和应用程序逻辑的远程调用。网络化制造 ASP 服务平台和位于不同地方的企业分平台和城市分平台交互的时候,大部分是使用 Web 服务来完成的。组件是为平台提供服务的,具有一定通用性能的功能模块,比如加密/解密、服务计费、数据访问、邮件服务等[3]。

从平台的结构来看,系统具有一般的网络程序特点,系统在多种不同的机器上运行。客户端、Web 服务器、数据库服务器和应用服务器。另外,平台结构和功能的复杂性,用户类型的复杂性,每一个细节都会影响到系统高效安全的运行,因此针对该模型提出一个有效的安全模型是很有必要的。

## 2 ASP 服务平台的安全模型

建立平台的安全模型也就是为平台的各种安全问题找到最佳的解决方案,并且要使该安全模型简便、可行和高效,看起来是一个不可分割的整体,ASP 服务平台的安全模型如图 2 所示。

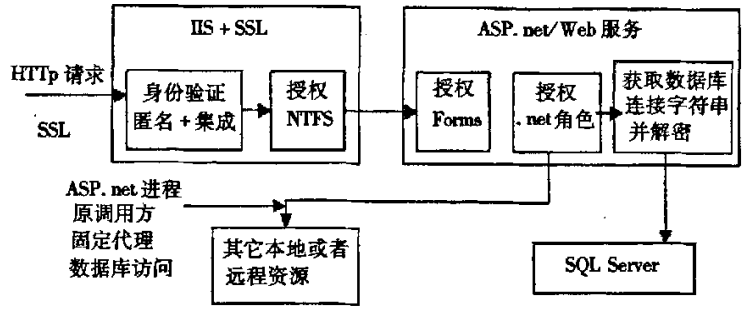


图 2 ASP 服务平台的安全模型

Fig. 2 The security model of Networked Manufacturing ASP platform

从图中可以看出机密信息的传输主要采用 SSL 安全信道,但过多的使用 SSL 会降低系统的性能. 因为在使用 SSL 的过程中,要存取密钥,并且要采用一定的算法对信息进行验证,这是一个复杂的过程。IIS 的验证使用匿名用户 + Windows 集成验证,这样用户在没有登陆系统之前获得的是最小访问权限。在使用系统的时候采用 Forms 验证 + 基于角色的授权,这样就可以灵活控制用户的访问权限。数据库的连接字符串包括其他的重要信息主要采用 DPAPI 加密。

在 Web 服务调用方面,采用 SOAP 验证技术,SOAP 技术也可以用来传递重要的大量的机密信息,这样在某些方面降低了大块信息传输和处理的复杂性,增强了信息传输的安全性。在系统内部,采用了各种验证以及密码存取技术,还有附加码和数字签名等技术,更好地保证了代码的健壮性和系统的可靠性。

## 3 ASP 服务平台安全模型的设计实现

### 3.1 资源访问控制的实现

资源访问,就是当用户请求资源的时候,首先判断用户的 Cookie 是否已经存在,如果不存在,系统读取资源的访问权限,如果允许匿名用户,则就可以访问,如果不允许,则要进行登录。登录成

功后,系统还要对其角色进行验证,因为授权是基于角色的授权,而不是基于用户的授权。

在实现中,角色检查控制是以 web. config 来控制为例,还可以利用编程的方式来进行用户角色的检查,这也就是我们的程序中为何要实现 CustomPrincipal 类的原因。.NET 框架提供了 WindowsPrincipal 和 GenericPrincipal 类,这些类分别实现为 Windows 和非 Windows 身份验证机制提供了基本的角色检查功能。这两个类都实现了 Iprincipal 接口。为了用于授权,ASP. NE T 要求这些对象存储在 HttpContext. User 中。这些类的功能足以满足大多数应用程序方案。应用程序可以调用 Iprincipal. IsInRole 方法来执行编程方式的角色检查。但是基本类的实现并不能满足大型的、角色复杂的 Web 应用程序,为此创建了一个实现 Iprincipal 接口的类 CustomPrincipal 来开发自己的 principal 实现。比如,增加了一个函数 IsInAllRoles,允许您检查特定用户是否为多个角色成员,增加了一个函数 IsInAnyRoles,允许您检查某个用户是否为某几个角色之一,这样判断起来增加了很多灵活性。

### 3.2　脚本注入

脚本注入攻击是通过浏览器使用用户输入框插入恶意标记或脚本代码,比如输入 < Script > , < object > , < applet > , < embed > 等,这个用户输入将保存在数据存储比如数据库或者 cookie 中,当客户读取这个信息时,这种恶意代码就会执行。

当 Web 页面上的一个文本框接收用户输入的字符串作为读者的姓名存入数据库,如果恶意用户输入 < script > alert( " haha!" ); </script > ,这样我们每次查询读者的时候都会执行这个恶意代码。要防脚本注入攻击,首先处理数据输入之前先验证,比如检查所输入的" User Age" 值是否是数值,是否为 16 或者是大于 16 的数值,或者确认用户列仅有诸如 A - Z,a - z,0 - 9 的有效数字和一些特殊的字符。这个时候使用 ASP. NET 验证控件是验证内容的极好的方法,特别是 RegularExpressionValidator 控件在验证用户输入的时候十分方便。使用正则表达式和 RegularExpressionValidator 控件,也可以很好的验证各种数据。

其次,当接收到来自非信任源的不恰当输入时,可以编写函数筛选出诸如[ ] { } 和 & 这样一些特殊字符,这时候可以使用 string 对象的 Replace( )方法。比如我们可以创建一个清理例程进行重用,然后就可以对各种数据使用它。

看看下面的示例:

```
String CleanUpInput (String strInput)
{
strInput = strInput. Replace("[","");
strInput = strInput. Reptace(")"," ");
strInput = strInput. Replace("("," ");
strInput = strInput. Replace(")", "" );
strInput = strInput. Replace("&","");
}
```

还可以采用编码输入内容来预防脚本注入攻击,编码( encoding) 是控制来自用户输入的数据的有效方法。例如, < 字符被翻译成 ⁢ 字符。Server 对象的 HtmlEncode 方法可以用来编码有害字符。编码形成标记的字符可以防止执行这些标记。所以编码用户输入可以防止脚本注入攻击。比如在 Web 页面的 Textl 文本框中输入 < script > alert( " HiThere" ) </script > 然后把它显示在标签 Labell 中:Labell. Text = Server. HtmlEncode( TextI. Text) ;经过编码后的内容就原原本本的显示在 Labell 中 ,而不是运行了 script 脚本。

### 3.3　URL 篡改

URL 篡改是攻击 Web 应用程序的最简单、最通用的方法。如果 ASP. NET 应用程序使用 HTTPGET 方法,而不是 HTTPPOST 方法,那么它就极易受到攻击。因为应用程序使用 HTTP GET 方法向服务器提交信息的时候,可以从 URL 上看到向服务器传送的所有信息,包括所有控件的视图状态信息和其它 HTML 控件信息,用户很容易修改并重新提交这些信息。另外,用户在利用 URL 传送参数的时候,如参数是一些敏感的信息比如用户名,或者极易被恶意用户猜到的信息,比如客户 ID,那么这些信息就很容易被篡改后提交,从而暴露用户的其他敏感信息。由于任何人都可以篡改 URL 参数,编码 URL 是个比较明智的手段。

下面举个简单的编码方法,首先创建两个方法来编码和解码数据。其中的 Encode 和 Decode 语法将获得当前字符的 ASCII 值,并将 5 添加到其中,然后再将新值回传给 ASCII 字符。解码的处理过程正好相反,这里仅列出 encode 方法:

```
Public string encode( string strData)
{
int i, iStringChar;
StringBuilder sbUrl = new StringBuilder( );
```

```
Char ch ;
for( i =0 ;i < strData . Length;i + + )
{
iStringChar = Asc( strDataSubstring( i,1)) +5;
ch = Chr( iStringChar);
sbUrl. Append( ch);
}
Return sbUrl. ToString( );
}
```

在平台系统中,涉及到敏感或者机密信息的时候,一般都采用 SSL 安全通道[4]进行传递,这样就不会遇到上述问题。另外,在不采用 SSL 传输的页面可以采用 Base64 位编码,这种编码是一种定义明确的方法,不是加密,但也可以有效防止 URL 篡改,给用户一种安全感。

## 4 小结

网络化制造 ASP 服务平台是个复杂的集成应用系统,它通过网络为企业提供软件共享、协同商务、资源优化配置、协同设计等服务,目的是提高企业的信息化水平和竞争力,从整体上实现区域资源的优化配置。本文根据网络化制造 ASP 服务的体系结构和特点,分析了系统在当前运行和部署环境下可能面对的安全隐患和安全威胁,并从开发者的角度为平台系统构建了一个安全模型,并提供了该安全模型主要部分的设计和实现。在实现模型采用的各种安全技术,包括资源访问控制、防止脚本注入、防止 URL 篡改及 SSL 安全通信技术等都是当今网络安全系统最热门和最具广泛应用前景的技术。在以后开发类似的复杂的大型集成应用系统的时候,本文中各种技术的设计和实现模型都具有一定的通用性和借鉴意义。

**参考文献:**

[1] 范玉顺,刘飞. 网络化制造系统及其应用实践[M]. 北京:机械工业出版社,2003:25 - 28.
[2] 杨海成,祁国宁. 制造业信息化工程—背景、内容与案例[M]. 北京:机械工业出版社,2003:10 - 14.
[3] 张南平,王伟. 基于. NET 平台的 B/S 应用系统的开发框架[J]. 武汉理工大学学报,2004,26(1):42 - 44.
[4] 张宇. 网络化制造 ASP 服务平台安全性应用研究[D]. 西安:西安交通大学,2005.

# Security Model Research Based on the Networked Manufacturing ASP Platform

WANG Chun - Feng
(Modern Educational Technology Center, Yancheng Institute of Technology, Jiangsu Yancheng 210098, China)

**Abstract**: The Networked Manufacturing ASP Platform especially relies on the Web Service technology, and enables interaction of customers from different regions through browers. How to guarantee the security of Web Service invocation should be considered during the development and deployment of system. The paper is based on the logistic structure of Networked Manufacturing ASP Platform. A security model of Networked Manufacturing ASP Platform is put forward from the developer's perspective, and the vital design and realization of security model is given.

**Keywords**: ASP platform; ASP security model; resource access control