# Web 应用系统的安全性设计

张国和,徐骏善
(南京理工大学 机械工程学院,江苏 南京 210094)

**摘 要**:探讨了 Web 应用系统的安全问题,阐述了防火墙技术、身份验证技术、ASP.NET 程序安全性设计、数据加密技术等实现 Web 应用系统安全性设计的技术。

**关键词**:Web 应用系统;防火墙;身份验证;ASP.NET;数据库

**中图分类号**:TP393 **文献标识码**:A **文章编号**:1674-7720(2010)21-0085-03

## Design the security of the Web application system

ZHANG Guo He, XU Jun Shan
(School of Mechnical Engineering, Nanjing University of Science & Technology, Nanjing 210094, China)

**Abstract**: The security of Web application system is mainly discussed in this paper, and then the technology to achieve system security through firewall technology, authentication technology, ASP.NET application security design, and data encryption in the database is elaborated.

**Key words**: Web application system; firewall; authentication; ASP.NET; database

随着 Internet 的飞速发展,Web 服务的应用越来越广泛,企业信息系统的应用领域由传统的、小型业务系统逐渐向大型的、关键业务系统转变[1]。企业信息系统中的数据,包括业务处理信息、技术资料信息,以及涉及企业高层发展计划和企业决策信息,其中大部分信息极其重要且具有保密性质。伴随着社会信息化建设大步推进,人们对企业信息系统的使用依赖性也越来越强。因此企业信息系统出现任何故障或被破坏,都会对用户、企业乃至整个行业产生不可估量的影响。

本文以徐工筑路机械有限公司(以下简称徐工筑路)备件管理系统项目为背景,由于此系统是在徐工筑路企业内外 Internet/Intranet 范围内设计使用,系统安全性问题关系到备件管理系统的正常运行,以及企业的业务能否正常展开,因此徐工筑路备件管理系统的安全性设计就显得尤为重要了。

## 1 系统面临的安全威胁

徐工筑路备件管理系统的安全威胁主要表现在非授权访问系统、伪用户登录系统、破坏数据的完整性、干扰备件管理系统正常运行等方面。它们主要利用以下途径:备件管理系统自身存在的漏洞、备件管理系统安全体系的缺陷、徐工筑路员工薄弱的安全意识及尚未健全的管理制度。备件管理系统的安全威胁主要有人为威胁和自然威胁。而人为威胁都是有目的的恶意攻击,攻击有主动和被动之分,因此可以将人为威胁分为主动性攻击和被动性攻击两大类。这些攻击对徐工筑路备件管理系统安全有着直接或潜在的破坏和威胁[2]。

### 1.1 主动性攻击

主动攻击是指那些攻击者未经徐工筑路许可截获或篡改公司信息,冒充公司拒绝或中止某些用户对系统使用的行为。这方面攻击往往是对数据通道中正在传输的数据单元进行更改、删除、延迟、拷贝重发或插入、合成或伪造等各种恶意处理行为,并以更改报文流、拒绝报文服务、伪造连结初始化等形式实现攻击者的险恶用心。主动攻击通常易于探测但却难于防范,因为攻击者可以通过多种不同方法发起攻击。

### 1.2 被动性攻击

被动攻击主要是指攻击者通过监听网络上传递的信息流,从而截获信息内容的行为。这类攻击仅仅为了获得信息流的长度、传输频率等数据要素,它不像主动攻击有直接恶意的破坏,而只是观察和解析出贯穿于一条连接通道上传输的数据单元所含的信息(包括用户数据的内容,或协议控制信息),但不篡改或破坏数据单元的信息。攻击者正是通过这种看似“无恶意”的攻击行为

来了解熟悉正在通信的双方详情,以便用其他方法达到窃取或破坏备件管理系统和企业资源的间接性攻击目的。因此,在信息发送者或接收者发现机密信息被泄漏之前,要发觉这种攻击是很困难的。然而通过对机密信息进行加密可以避免被动攻击的发生。

从上述分析可以看出备件管理系统所受到的攻击可能是多方面的,攻击形式也是多种多样的,而且往往是多种攻击同时存在。如何防范这些非法攻击是一项复杂而艰巨的任务,需要通过各种安全服务措施和健全企业机制来实现。

## 2 对系统的安全措施

为了保证备件管理系统的安全运行,保护企业计算机的硬件、软件和系统数据不因偶然或恶意的原因而遭到破坏、更改或泄漏,本备件管理系统采用以下安全措施。

### 2.1 使用防火墙技术

防火墙技术是一种建立在现代通信网络技术和信息安全技术基础上的网络应用安全技术,越来越多地被应用在专用网络与公用网络的互联环境之中,尤其是以接入 Internet 网络使用最为广泛[3]。

防火墙是指设置在不同网络(如可信任的企业内部网和不可信的外部公共网)或网络安全域之间的一系列器件的组合。防火墙是不同网络或网络安全域之间信息的唯一出入口,它能根据企业的安全政策(允许、拒绝、监测)控制出入网络的信息流,且本身还具有较强的抗攻击能力。防火墙可提供信息安全服务,是实现网络和信息安全的基础设施。在逻辑上,防火墙既是一个分离器、限制器,也是一个分析器,能够有效地监控内部网和因特网之间的任何活动,保证内部网络的安全[3]。

徐工筑路备件管理系统在使用防火墙技术主要体现在两个方面:

(1)企业网络级防火墙,用来防止整个企业内部安全网络出现外来非法不可信网络的入侵。属于这类的有分组过滤和授权服务器,分组过滤检查所有流入本企业网络的信息,拒绝所有不符合企业事先制定好的一套准则的数据,而授权服务器则是检查系统使用用户的登录是否合法。

(2)企业应用级防火墙,企业从应用程序入手来进行备件管理系统的接入控制。通常使用应用网关或代理服务器来区分各种应用。如徐工筑路公司只允许通过访问万维网的应用,而阻止 FTP 应用的通过。

### 2.2 应用系统的安全性

本系统可供徐工筑路的备件中心、备件代理商、市场部、特约维修站、服务部及销售部等多个部门员工同时使用,因此在系统安全性设计方案上,可采用角色管理和系统用户身份验证的安全策略。

(1)角色管理

角色管理将系统不同模块权限和对象权限整合成一个集合,即角色。通过对系统功能模块的划分,不同的模块对不同的角色有着不同的访问权限控制。从而限制了那些没有该功能模块访问权限的用户访问该功能模块。本系统将操作用户分为 7 类角色:仓库管理员、备件系统管理员、服务处处长、服务系统管理员、特约维修站总经理、特约维修站信息接待处理员及销售系统管理员。

(2)系统用户身份验证

身份验证技术是目前广泛使用的企业信息系统的安全技术之一,它通过使用用户向系统出示自己身份证明、系统核查使用用户身份证明的有效性两个过程判明和确认通信双方的真实有效身份。

本备件管理系统主要依靠 Internet 信息服务(IIS)的身份验证技术和 Windows NT 文件访问系统的安全性,如图 1 所示。使用用户的访问请求首先从网络客户进入 IIS,IIS 可以选择使用基本的、简要的或集成的 Windows 身份验证技术对客户进行身份验证,如果客户通过了身份验证,那么 IIS 将根据验证后的结构生成新的对 ASP.NET 的请求后提交给 ASP.NET 应用程序服务器。之后 ASP.NET 应用程序使用从 IIS 传递来的访问标记模拟原始提出请求的客户,并验证该用户在配置文件中所给定的访问权限。最后通过验证,应用程序通过 IIS 返回所请求的页面[4]。此方案依赖了 Windows 集成的账户验证功能,同时可以尽量减少备件管理系统对 ASP.NET 程序本身在安全性方面的编程量,大大简化了备件管理系统设计过程中的工作量。

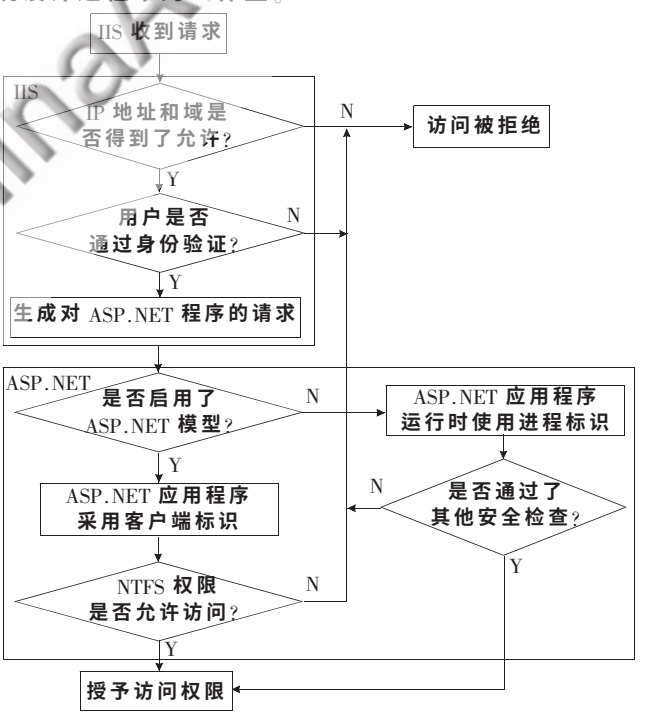


图 1 Windows 验证方案图

### 2.3 ASP.NET 程序的安全性

在备件管理系统的程序设计过程中为了减少因程序设计漏洞而带来的安全性问题,在程序设计中采取如下措施来增加 ASP 脚本的安全性。

(1)防止 SQL 注入攻击,在编程的时候要禁止用户输入非法的危险字符,如单引号('或'),or,and,、,*,<,>,空格等危险字符[5];同时在客户端和服务器端都要对用户输入的信息进行验证;同时在编写程序过程中尽量使用存储过程技术,使用存储过程不仅可以防止某些类型的 SQL 注入式攻击,还可以提高 SQL 语句的执行速度;在程序出现异常的情况下,程序会自动跳转到固定的页面,而不是将错误信息显示给用户,这样可以防止部分别有用心的用户。

(2)在本备件管理系统中,由于访问权限的不同,用户可以访问的页面也不同,为了防止用户直接从网页的地址栏中输入链接地址进入某个超出该用户权限的页面,而出现越权的操作,如图 2 所示。用户登录后输入选择角色并输入密码,验证通过进入导航页面,同时系统记录下该用户的角色。用户在访问页面时,系统将同时记录用户请求的路径,并进入数据库对其进行判断,如果该用户的角色具有访问此页面的权限,则进入要访问的页面,否则进入错误提示页面。用户点击重新登录后将重新返回到登录页面,从而避免了用户采用直接输入网址的方式访问超出其权限的页面。由于系统不能够检测登录的账号是否被他人冒用,所以采取当用户长时间不在系统中进行操作时(本备件管理系统设置为 20 min),用户在系统中的 Session 值过期,从而该登录的账号失去了再次使用系统的权利,必须重新登录系统。这样可以防止用户离开计算机时被他人冒名使用。

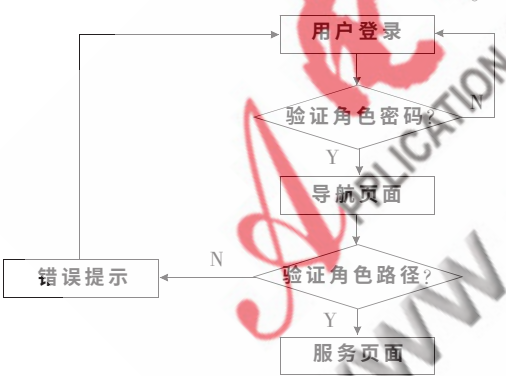


图 2 权限验证流程图

(3)本备件管理系统中具有文件的上传和下载功能,在上传文件时为了防止有些用户上传恶意文件破坏系统,因此需要在上传时对文件类型进行判断。除非是指定的文件类型外,其他的文件均不予上传,尤其是以.asp,.aspx 或.exe 等结尾的文件。

### 2.4 数据库中数据加密技术

由于系统应用程序的关键信息和数据都存储在数据库中,所以数据库的安全性就显得尤为重要。在信息系统的开发过程中,加密技术是一种很常用的安全技术。它把重要的数据通过技术手段变成乱码(加密)后再传送信息,即通过将信息编码为不易被非法入侵者阅读或理解的形式来保护数据的信息,到达目的地后再用相同或不同的手段还原(解密)信息。根据加密密钥和解密密钥在性质上的不同,在 ASP.NET 应用中提供了两种加密算法,即对称加密算法和非对称加密算法[6]。

(1)对称加密是加密和解密使用相同密钥的加密算法。它的优点是保密程度较高、计算开销小、处理速度快、使用方便快捷、密钥短且破译困难。由于持有密钥的任意一方都可以使用该密钥解密数据,因此必须保证密钥不被未经授权的非法用户得到。在对称加密技术中广泛使用的是 DES 加密算法。

(2)非对称加密是加密和解密使用不同密钥的加密算法。它使用了一对密钥:一个用于加密信息;另一个用于解密信息,通信双方无需事先交换密钥就可以进行保密通信。但是加密密钥不同于解密密钥,加密密钥是公之于众,谁都可以使用;而解密密钥只有解密人知道,这两个密钥之间存在着相互依存关系:即用其中任一个密钥加密的信息只能用另一密钥进行解密。它只可加密少量的数据。在非对称加密算法中普遍使用的是 RSA 加密算法。

基于上述分析,并结合徐工筑路备件信息网的特点,采用 RSA 与 DES 混合加密体制的方式实现数据信息的加密。可以用对称加密算法(DES 加密算法)加密较长的明文,用非对称加密算法(RSA 加密算法)加密数字签名等较短的数据,这样既保证了数据的保密强度,又加快了系统运算速度。

本文通过对信息系统安全威胁及系统安全的防护措施的分析[7],使用户能够最大限度地保障 Web 应用系统的安全,并通过必要的安全措施,将可能发生的风险控制在可接受的范围之内。

参考文献

[1] 唐俊,赵晓娟,贾逸龙.企业信息系统安全体系结构的研究[J].微计算机信息,2010(26):43-45.
[2] 瞿微. 基于 Web 的企业售后服务系统设计与加密技术研究[D].武汉:华中科技大学,2006.
[3] 彭继卫.浅谈计算机网络中信息系统的安全防范[J].中国新技术新产品,2009(1):23.
[4] 罗晓光.企业机械有限公司销售管理系统的设计与开发[D].南京:南京理工大学,2008.
[5] 金永涛. 基于.NET 框架的 Web 应用系统安全问题研究[J].北华航天工业学院学报,2009(12):1-3.
[6] 李海泉,李健.计算机网络安全与加密技术[M].北京:科学出版社,2001.
[7] 许晓冯.Web 应用系统的安全威胁及其防护[J].信息化研究,2009(35):1-3.

(收稿日期:2010-04-06)

作者简介:
张国和,男,1984 年生,硕士研究生,主要研究方向:企业信息化。