

# 办公局域网数据库安全访问技术应用

李水莲

(连云港财经高等职业技术学校, 江苏 连云港 222003)

**【摘要】**科技飞速发展,人们的生活离不开网络。网络对企业办公来说非常重要,已经成为不可缺少部分,办公局域网的建立方便了企业各个部门之间的沟通。局域网安全关系到企业的利益。由于网络很复杂,存在很多安全隐患,所以办公局域网的建立需要具有能够识别安全风险的能力,应用有效的数据库安全访问技术能够实现企业稳定经营,本文从办公局域网存在的安全风险出发研究数据库安全访问技术的应用,供读者参考。

**【关键词】**办公局域网;风险;数据库安全访问技术;应用

**【中图分类号】**TP393.1 **【文献标识码】**A **【文章编号】**1673-1891(2014)02-0080-03

企业为了方便经营会建立办公局域网,办公局域网的数据库安全关系到企业的稳定经营,局域网中数据库安全是网络信息安全的重要组成部分,局域网数据库安全访问技术需要按照客户的要求以及安装角度的分析,以便确定数据库安全访问技术的应用,保证企业局域网的安全,实现企业的稳定发展。

## 1 办公局域网数据库系统存在的安全隐患

办公局域网数据库在使用中存在很多安全隐患,笔者分析了很多关于办公局域网安全隐患的资料,总结出安全隐患主要表现在以下几个方面:(1)局域网数据库经常受到病毒的威胁,由于网络已经普及,计算机病毒逐渐泛滥,病毒不断扩散。办公室局域网数据库新系统被病毒侵害以后会给局域网造成很大的破坏,企业的有用信息丢失,给企业的经营造成一定的麻烦。(2)来自于黑客的威胁。某些计算机高手出于某种动机,对网络进行恶意攻击,窃取相关数据,影响企业的经营。(3)工作人员长时间的工作,出现粗心大意,一旦疏忽就可能会造成局域网数据库系统信息外漏,影响到单位局域网的安全。(4)办公局域网数据库自身也存在漏洞,局域网数据库系统在设计之初肯定会存在一些细小的漏洞,虽然看起来微不足道,但是一旦变成黑客攻击的目标,对办公室的局域网会产生很大的威胁。(5)应用程序本身也存在漏洞,应用程序中软件资源存在隐患,相互通信的程序也存在隐患。(6)网络结构本身,以及合作单位都存在一定的风险<sup>[4]</sup>。这些风险的存在都会影响到办公局域网数据库的安全访问,对企业的发展的稳定性也产生很大的影响。

## 2 局域网数据库安全访问相关技术分析

网络数据库安全访问技术涉及两个层次的内容:第一层次是系统运行的安全性,也就是系统的

硬件层次。第二层次是系统信息的安全性,也就是数据库加密技术以及口令鉴别技术。这两个层次的应用是办公局域网数据库安全访问技术的重要内容。

### 2.1 角色的访问控制技术 RBAC

分析这种角色访问技术需要了解 RBAC 的原理,工作人员需要经过授权才能获得,权限需要和角色对应。角色和权限是相互映射的<sup>[1]</sup>。访问方式可以简化控制权,使系统的执行保护策略具有很大的灵活性,也能够按照实际情况重新改编角色。

### 2.2 NET Framework 技术

Framework 访问技术需要在一个综合环境中,包括用户的创建、配置、运行和其他应用程序。这种程序的构成包括:数据库语言运行、Framework 共享数据对象类别库以及 ASP.NET 的相关内容。关于 NET Framework 包含 Web 的应用模型,也能够提供 Web 服务框架和相关的服务内容以及相关的服务。

Framework 技术与角色的访问控制技术,与两种技术的应用能够起到一定的安全保证。

## 3 局域网数据库安全访问系统的设计

### 3.1 关于系统架构的设计

局域网数据库的安全访问技术的应用包含了三个部分的内容:表示层、数据访问层和数据层。共同构成了局域网数据库访问系统的框架,其构建设计见图1。

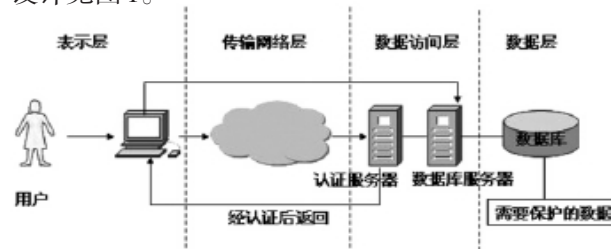


图1 局域网数据安全防卫系统的架构设计示意图

收稿日期:2014-02-20

作者简介:李水莲(1980-),女,江苏徐州人,讲师,硕士,研究方向:计算机教学。

网络数据库的安全访问系统需要和认证服务器联系在一起,系统的每个架构层次能够承担不同的功能,数据库的安全访问控制,在每个层次中都有体现,需要结合相关的安全策略和系统的构成组件才能满足数据库访问机制的应用。所谓的表示层是用户和系统之间的交互信息的借口,数据访问层也是用户和数据库之间的核心构成部分负责逻辑计算和数据控制方面的内容<sup>[3]</sup>。在控制过程中涉及到数据的人身和加密。数据层是数据的存储、封装和调用功能。系统的构架和设计是系统性的工程,需要加强这方面的设计。

### 3.2 数据库安全访问技术的应用

办公室的客户端需要提供相互设计的界面,局域网的数据安全访问系统要借助 Windows,在 NET 中实现用户相互认证,用户的认证需要提供规范化的用户认证,系统的服务器会接受相关要求,并且做出响应。另外,系统还会对输入的信息进行有效过滤,有效的避免了恶意代码进行 SQL 形成的注入,造成系统出现危险。系统的稳定性也能够有效的增强。

其次,局域网的数据流包含数据本身的同时,还包含连串的字符信息以及密码,如果不进行处理在局域网中传输很容易出现资料外泄,对系统进行加密是非常重要的。最后,角色的安全访问机制是安全技术的重要组成部分,可以通过认证服务器完成任务,安全技术要求通过授权的用户才能够访问局域网<sup>[4]</sup>。

## 4 局域网中数据安全访问技术的应用

### 4.1 关于表示层设计的应用

数据安全访问的第一层屏障是表示层设计,表示层设计负责用户信息的接收、过滤以及提交过程是接触窗体实现的。采用树状排列的形式显示出用户名的应对角色。包括了用户登录的 ID,用户名、登录时间、有关权限。重要部分的设计过程需要用户发出数据连接的申请要求,局域网中允许这个请求之后,由 NET 对用户的要求进行审查,用户通过认真核对以后利用用户名和密码就可以登录到窗体中。

系统针对用户提供的密码,需要按照局域网的要求验证相关的匹配信息。系统通过验证以后,本身可以创建一个 COOKIE 直接反馈到用户端。如果角色端出现数据段就可以防止用户发出的请求,重复获取相关角色内容。当用户被确定在最初界面时,事件处理的程序能够创建 Iprincipal,保护对象

存在 HttpContext 中。用户可以按照分配角色的不同控制界面的操作。系统中涉及到 SQL 的注入式攻击的防范,系统中的语句可以通过存储过程,使用 Parameters 集合,用户可以不用管输入什么样的字符,都可以进行文本处理<sup>[5]</sup>。

### 4.2 关于数据访问层的应用

网络数据安全涉及到系统访问层的设计,数据访问本身需要加密和解密。加密处理有三种形式:字符串的加密、用户密码加密以及验证用户信息的加密。系统通过 Secret 类别中的 Encrypt 对相关数据进行加密,并且将密文传输到认证服务器中。认证服务器对信息进行算法计算,结合随机数后按照一定的算法返回到数据中,具体流程见图 2。

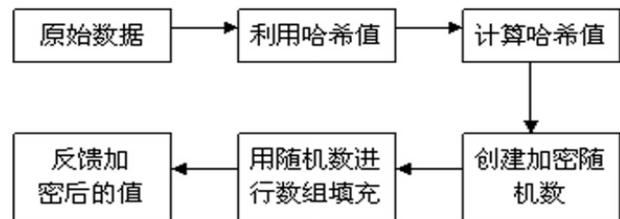


图2 加密算法流程示意图

数据访问层的认证设授权需要和数据库中的 User-Role 的表象信息联系在一起,操作中在 User-Role 表中完成操作。确定用户等级以后,系统会针对不同的等级进行不同管理,系统管理员具有更改系统角色的能力。

### 4.3 系统数据层的应用

数据层在安全访问层数据方面,安全访问系统对数据库系统的功能涉及到角色的验证以及权限的划分。认证的数据库包含了用户信息表、用户登录表、角色表以及权限表等。数据表的存储是数据的关键功能,主要原理在于,能够在 Auth 的数据库中处理相关信息,以便获得信息的角色,资源和权限等相关数据,可以通过数据层处理,实现 SQL Server 的自定义存储过程。

## 5 局域网数据库安全访问技术控制系统的运用

一方面,为了维护对数据库的安全访问要在适当的时机更改数据库密码,更改后的密码要保存在数据库中。当需要建立数据连接的时候,系统能够自动处理对应的密码,通过解密才可以与系统进行连接<sup>[6]</sup>。密码的维护系统自身能够完成对密码的加密。从以上的分析方式出发对密码系统加密涉及三种类型:定时器类 TimeCtr、加解密类 DES3、密码更改类 PSD A O。他们的数据关系图如图 3 所示。

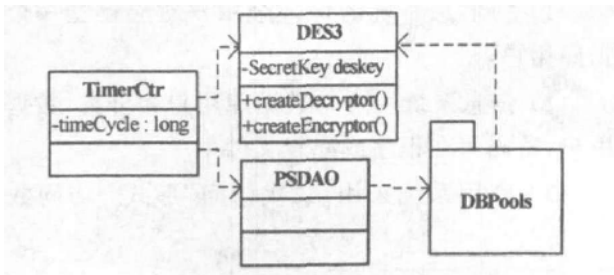


图3 密码更改核心类图

另一方面,为了保证网络的正常运行,要求对安全数据网管进行验证,认证客户端发出信息传递到服务器中,认证信息由 URL 和随机的字符串构成。为了保证系统的安全。服务器的一端会随时向客户发出更改秘钥和随机字符,更改完成以后要

解决分布式在其中存在的问题,保证系统的稳定性更强。完整身份验证以后,可以从数据连接池中找出符合要求的连接。创建新的连接需要对局域网进行二次访问,利用算法解密其中存在的密码,得到数据连接以后,放入到数据中返回到应用系统中,实现系统的稳定性。这种局域网的连接形式能够保证网络构成的稳定性<sup>[1]</sup>。

### 6 结束语

文中从技术角度分析了办公室局域网数据安全,提出了局域网数据库安全设计的方式,总结了这种技术的应用方法,对保证办公室局域网数据库安全具有很重要的作用,对企业的发展具有长远意义。

#### 注释及参考文献:

- [1]曲幸生.B/S方式三层结构管理信息系统分析与设计[D].长安大学,2013.
- [2]刘义理.分布式数据库安全框架研究[D].同济大学,2012.
- [3]靳桂珍.浅谈局域网络系统的数据库安全[J].活力,2009(10):163.
- [4]骆轶姝.数据库权益管理模式及应用研究[D].东华大学,2011.
- [5]冯朝胜.数据库加密系统研究[D].四川师范大学,2010.

## Application Security Office LAN Database Access Technology

LI Shui-lian

(Lianyungang Vocational Technology Academy of Finance and Economics, Lianyungang, Jiangsu 222003)

**Abstract:** With rapid development of science and technology, people's life cannot leave the network. Network is very important for enterprise office, has become an indispensable part. The establishment of the office LAN is convenient for the communication between different departments. LAN security is related to the interests of the enterprise. Because the network is very complex, there are a lot of potential safety problems, so the establishment of the office LAN needs to identify the ability of security risks, application of effective database security access technology can achieve stable operation enterprise, this article discusses the application of the database secure access technology from the office LAN for the security risks for reader reference.

**Key words:** office LAN; risk; the database security access technology; application