高速公路联网收费系统数据安全性的需求及解决方案

作者： 单位： 时间：2007-05-23 点击： 次

摘 要：

关键词：

马丽香
（山西省交通职业技术学院，山西，太原）

摘要：随着我国高速公路的快速发展，高速公路联网收费系统的数据量越来越大，本文对高速公路联网收费系统的运营参数、实时数据、统计分析数据和图像数据的安全性进行了分析，并提出了解决高速公路联网收费系统数据安全的方案。

关键词：高速公路；联网收费；数据安全

高速公路在一个国家的综合运输体系和经济发展中占据举足轻重的地位，我国高速公路经过17年的持续快速发展，目前高速公路通车里程已经接近4万公里，通车里程居世界第二，促进了国民经济和区域经济的持续发展，产生了广泛的经济效益与社会效益。

目前，高速公路普遍采用了高速公路联网收费系统进行收费管理。采用联网收费系统可以最大限度地堵塞收费漏洞，提高收费服务水平和工作效率，减轻收费员工作强度，方便收费结算，规范收费管理；可以对路费、通行券、票据、设备等进行严格管理。联网收费系统和高速公路收费管理的各个环节都有关联，在收费管理过程中会产生大量的数据，这些数据是高速公路管理的一种重要资产，对高速公路收费管理起着越来越重要的作用。

按目前联网收费较为普遍的模式来看，联网收费系统一般由省收费结算中心、省内联网各高速管理公司、收费分中心、收费站四个层次组成。联网收费系统产生的数据可分为四类：系统运营参数、实时数据、统计分析数据和图像数据。

① 系统运营参数包括路网统一时钟、费率表、通行卡黑名单、预付卡黑名单、收费站站名表、系统编码数据表和常规表更新时间表等。

② 实时数据包括入口车道的原始过车记录、出口车道的原始收费记录和实时监视需要的收费站车流量、收费信息。

③ 图像数据包括车道对违章车辆、纠纷车辆以及军警车、公务车、紧急车等特殊车辆进行抓拍的照片图像。图像数据在入口对车辆进行抓拍，并存储在收费站服务器中。抓拍图像数据定期上传到高速公路联网收费管理中心。

④ 统计分析数据包括收费站日通行费的拆账日报表、入口车道收费统计数据、出口车道收费统计数据、日通行费拆分汇总表等。

目前，联网收费系统的管理员对收费系统网络的安全和操作系统的安全、病毒防护等方面已经逐渐关注起来，而联网收费数据的安全性目前还没有得到足够的重视，还没有和网络、系统的安全性等同起来，并且大多数管理员对数据库不熟悉，认为只要把网络和操作系统的安全搞好了，所有的应用也就安全了，对数据安全问题关心太少或忽略数据安全，这就使联网收费数据的安全问题更加严峻。

如果数据库系统中存在安全漏洞和不当配置，通常会造成严重的后果，而且都难以发现。高速公路联网收费系统普遍使用SQL Server数据库，SQL Server数据库是属于“端口”型的数据库，任何人都能够用分析工具对数据库进发起试图连接，进而绕过网络或操作系统的安全机制闯入收费系统、破坏和窃取收费系统数据资料，甚至破坏整个收费系统。

对SQL Server的安全管理可分为3个层次，即账户、数据库的管理与连接特定数据库的权限和使用者对所连接数据库的操作权限。

1、在数据库账户安全方面，可以采用以下安全策略：

① 使用WINDOWS系统认证模式。

使用WINDOWS系统认证模式来连接到SQL SERVER。WINDOWS认证模式是WINDOWS认证和SQL Server认证的结合，用户通过使用一个现成的WINDOWS用户帐号连接到SQL服务器，这样可以防止SQL Server被一些受限的WINDOWS用户的攻击。SQL Server服务器也会被WINDOWS强制安全机制保护，如更加强壮的证明协议和强制性的口令复杂性。

② 使用安全的密码策略。

数据库帐号的密码不能过于简单，对于sa更应该注意，同时不要让sa帐号的密码写于应用程序或者脚本中，还应该养成定期修改密码的好习惯。数据库管理员应该定期查看是否有不符合密码要求的帐号。比如使用下面的SQL语句：

```
Use master
```

```
Select name,Password from syslogins where password is null
```

③ 使用安全的帐号策略。

由于SQL Server不能更改sa用户名称，也不能删除这个超级用户，所以，我们必须对这个帐号进行最强的保护，如使用一个非常强壮的密码，不要在数据库应用中使用sa帐号，只有当没有其它方法登录到 SQL Server 实例（例如，当其它系统管理员不可用或忘记了密码）时才使用 sa。数据库管理员应当新建立一个拥有与sa一样权限的超级用户来管理数据库。

安全的帐号策略还包括不要让管理员权限的帐号泛滥。如果数据库管理员不希望操作系统管理员来通过操作系统登陆来接触数据库的话，可以在帐号管理中把系统帐号“BUILTINAdministrators”删除。不过这样做的结果是一旦sa帐号忘记密码的话，就没有办法来恢复了。

2、在数据库安全管理方面，可以采用以下安全策略：

① 安装最新版本的SERVICE PACK。

管理员应该经常查看Microsoft's Security Bulletin(微软安全公告)并下载安装最新的SERVICE PACK，尽量减少安全漏洞。比如蠕虫病毒可以利用安全漏洞对数据库服务器造成很多破坏。

② 用安全基准分析器（如MBSA）来评估服务器的安全性。

MBSA是一个用来扫描微软产品中包含的不安全设置的工具，包括了SQL SERVER。它可以在本地机上运行或者通过网络运行。它能够测试出SQL SERVER中的问题，如空口令或弱口令、权限过多等问题。

③ 加强数据库日志的记录。

在实例属性中选择“安全性”，将其中的审核级别选定为“全部”，这样在数据库系统和操作系统日志里面，就详细记录了所有帐号的登录事件。管理员应该定期查看SQL Server日志，检查是否有可疑的登录事件发生。

④ 管理扩展存储过程。

SQL Server为了适应通用的需求，包含了大量的系统存储过程，但多数应用中根本用不到多少系统的存储过程，所以应当删除不必要的存储过程，因为有些系统存储过程能很容易地被人利用起来提升权限或进行破坏。

扩展存储过程xp_cmdshell是进入操作系统的最佳捷径，是数据库留给操作系统的一个大后门。如果不需要xp_cmdshell，使用如下SQL语句可以屏蔽：

```
use master
sp_dropextendedproc 'xp_cmdshell'
```

在需要这个存储过程的时候，可以用这个语句恢复过来：

```
sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll'
```

其它如OLE自动存储过程（会造成管理器中的某些特征不能使用）、注册表访问的存储过程（能够读出操作系统管理员的密码）等也应当进行检查，对不需要的进行屏蔽。

3、在数据库连接安全方面，可以采用以下安全策略：

① 使用协议加密。

SQL Server使用Tabular Data Stream协议来进行网络数据交换，如果不加密的话，所有的网络传输都是明文的，包括密码、数据库内容等等，这是一个很大的安全威胁。有可能被人利用在网络中截获到他们需要的东西，包括数据库帐号和密码。所以，在条件容许情况下，最好使用SSL来加密协议。

② 隐藏数据库TCP/IP端口。

在数据库实例属性中选择TCP/IP协议的属性，选择隐藏 SQL Server 实例。如果隐藏了 SQL Server 实例，数据库将禁止对试图枚举网络上现有的 SQL Server 实例的客户端所发出的广播作出响应，这样就不能用1434来探测服务器的TCP/IP端口。

③ 修改TCP/IP使用的端口。

更改数据库实例默认的1433端口。在实例属性中选择网络配置中的TCP/IP协议的属性，将TCP/IP使用的默认端口变为其他端口。

④ 拒绝来自1434端口的探测。

由于1434端口探测没有限制，能够被别人探测到一些数据库信息，而且还可能遭到DOS攻击让数据库服务器的CPU负荷增大，所以对操作系统来说，在IPSec过滤拒绝掉1434端口的UDP通讯，可以尽可能地隐藏SQL Server。

⑤ 对网络连接进行IP限制。

SQL Server数据库系统本身没有提供网络连接的安全解决办法，但是Windows操作系统提供了这样的安全机制。使用操作系统自己的IPSec可以实现IP数据包的安全性。方法是对IP连接进行限制，只保证可信的IP能够访问，也拒绝其他IP进行的端口连接，把来自网络上的安全威胁进行有效的控制。

4、对数据库的操作权限方面，可以采用以下安全策略：

很多数据库应用只是用来做查询、修改等简单功能的，所以管理员应当根据实际需要分配帐号，并赋予仅仅能够满足应用要求和需要的权限。SQL Server存取权限有select、insert、update、delete、exec和dri，其中exec与dri分别表示对预存程序的执行权限和对表格有效性的验证权限。比如，只要查询功能的，那么就使用一个简单的public帐号能够select就可以了。

管理员应当决定哪些用户需要查看数据、哪些用户需要更新数据，然后分配合适的许可。不要随便赋予用户各种权限。

以上主要介绍了一些提高联网收费系统数据安全性的一些方案，当然，更主要的还是要加强内部的安全控制和管理员的安全培训，而且数据安全性问题是一个长期的解决过程，还需要进行更多的安全管理工作。此外，还应该采取其它如数据库的备份（包括磁

带备份、双机热备份、手工备份）、病毒防护、防入侵、防泄漏、数据加密、制订操作规程等措施共同保证联网收费系统数据的安全性。这些不在本文的讨论范围内。

参考文献：

[1] 刘伟铭, 王哲人, 郑白涛. 高速公路收费系统理论与方法[M] . 人民交通出版社, 2000

[2] 田保慧. 高速公路计算机收费系统管理软件的开发. 公路与汽运，2005,(11):153-158

[3]金凌,钱钢. 高速公路联网收费系统的信息安全. 计算机工程，2003，（10）:124-125

上一篇：重锤击实在高填方路基中的应用

下一篇：利用软基土填筑路堤的施工方法