

SQL Server 气象资料数据库的安全管理

刘 军, 郑良璋

(武汉理工大学 计算机学院, 湖北 武汉 430070)

摘 要:现在气象服务与人们生活、工作联系很紧密,气象资料数据的安全性变得非常重要。文中概述气象信息服务系统,对 SQL Server 气象资料数据库的安全机制进行了分析,介绍了身份验证和权限管理两个重要概念,通过 Windows 集成验证模式和混合验证模式两种模式来验证用户身份;通过划分角色来分配权限。最后通过一个管理扩展存储过程实例对 SQL Server 气象资料数据库的安全性进行了分析,从而达到限制他人权限来保护气象资料数据库的安全。

关键词:SQL Server;气象资料;安全;管理

中图分类号:TP309.2

文献标识码:A

文章编号:1005-3751(2006)02-0215-02

Security Management of SQL Server Meteorology Data Database

LIU Jun, ZHENG Liang-zhang

(Department of Computer Science, Wuhan University of Technology, Wuhan 430070, China)

Abstract: Now, meteorology service relate closely to people's life and work. It's very important to the security of meteorology data. This article summarizes service system of meteorology data, analyzes security mechanism of SQL Server Meteorology data database, introduces two important conceptions of authentication and permission. Authenticates users by two modes: Windows authentication and mixed authentication, and grant permissions by roles. Finally, from a case for management of extension procedure, analyzes the security of SQL Server meteorology data database, so that limit others permissions to protect the security of meteorology database.

Key words: SQL Server; meteorology data; security; management

0 引 言

Microsoft SQL Server 是为 Windows NT 设计的,它具有 Windows NT 的许多优点,并且将安全性与 Windows NT 的安全性紧密地结合在一起,可以使用 Windows NT 的用户和组来控制数据库的访问权限。它是一个功能强大的后台数据库管理系统,可以帮助各种规模的企业用来管理数据,以可伸缩性的商业解决方案、强大的数据仓库以及与 Microsoft Office 和 Microsoft BackOffice 的紧密集成为企业提供额外的商业便利^[1]。它是基于 Internet/Intranet 的应用系统,由于互连网络的开放性和通信协议的安全缺陷,以及在网络环境中数据存储和对其访问与处理的分布性特点,网上传输的数据很容易受到破坏、窃取、篡改、转移和丢失。这些危害通常是由网络的攻击引起的,诸如身份窃取 (Identity Interception)、假冒 (Masquerading)、数据窃取 (Data Interception)、否认 (Repudiation)、错误路由 (Misrouting)、拒绝服务 (Denial of Service) 和业务量分析 (Traffic Analysis) 等。另外,用户在操作、管理以及对系统的安全设置上的失误,同样会给网络安全带来危害。这些危害给数据信息的完整性、可用性、隐私性、可靠性带

来了巨大的威胁,对基于 Web 数据库的气象信息服务也构成了危害。因此,安全问题成了任何网络应用系统都必须考虑的主要问题。基于 Web 数据库的气象资料数据库也是如此。

数据库安全在当前数据库技术的发展中扮演着越来越重要的角色。由于数据库在大型软件中占有举足轻重的地位,使得它成为众多黑客攻击的对象,气象资料数据库的安全问题也是如此。如何尽可能地保证气象资料数据库的安全成为人们思考的问题。

文中不是对 SQL Server 安全中的所有问题做泛泛的介绍,而是在介绍几个重要概念和剖析重要机制的基础上,通过分析来阐述气象资料数据库的安全管理。

1 气象信息服务系统概述

气象信息服务系统是基于三层 C/S 模式的网络数据库系统,它以 Web 方式提供对气象信息的共享和利用。系统的三层体系结构可以划分为:表示层、应用逻辑层、数据服务层,其结构模型如图 1 所示。表示层是基于 Web 浏览器的客户端,负责与用户交互,完成基本的规则验证、数据描述和显示,并把用户请求通过调用中间层组件传递给应用逻辑层;应用逻辑层通常为 Web 服务器,执行具体的事务逻辑,并通过 SQL 方式向数据服务层提出数据或其它资源的请求。数据服务层通常为数据库服务器,负责

收稿日期:2005-05-14

作者简介:刘 军(1966—),女,湖北武汉人,硕士,副教授,研究方向为软件工程、网络数据库。

对气象信息数据的存储和管理。

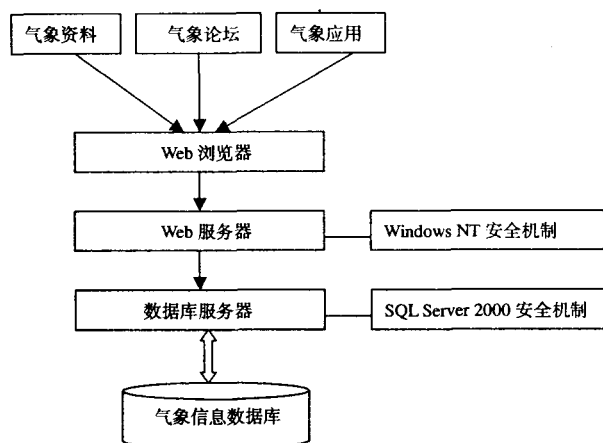


图 1 气象信息服务系统体系结构图

表示层体现了气象信息服务系统的内容体系,包括气象资料共享、气象科研业务、气象科技动态、气象论坛公告、气象百科、气象应用(天气预报、有偿服务、科普教育等)。所有这些气象信息都存储在数据库服务器中。浏览器接受用户的请求,并传递给应用服务器,经过服务器的身份验证后,确认为合法用户的,服务器就向气象信息数据库提出数据查询请求,数据库服务器生成数据查询结果。查询结果按原路径逆向返回,最终以 HTML 的形式呈现给用户。

2 SQL Server 气象资料数据库的安全机制分析

内部安全性关心的是文件系统级的问题,即防止 SQL Server 服务器中的 master 数据库中的 sysxlogins 被在服务器主机有账号的人(合法或窃取的)进行攻击。如果数据目录内容的权限过分授予,使得每个人均能简单地替代对应于那些数据库表的文件,那么确保控制客户通过网络访问的授权表设置正确,对此毫无意义。

外部安全性关心的是从外部通过网络连接服务器的客户的问题,即保护 SQL Server 服务器免受来自通过网络对服务器连接的攻击。你必须设置 SQL Server 授权,使得它们不允许访问服务器管理的数据库内容,除非提供有效的用户名和口令^[2]。

2.1 身份验证

SQL Server 为访问者访问数据库设置了两层身份验证。一是服务器级的验证,访问者需要提供正确的登录信息来连接并登录服务器;二是数据库级的验证,需要提供正确的数据库用户信息来访问数据库。

SQL Server 服务器级身份验证模式有两种:Windows 集成验证模式、混合验证模式。

Windows 集成验证模式是 SQL Server 2000 默认的身份验证模式。在这种模式下,能够登录 Windows 的合法用户和组,都可以连接并登录 SQL Server 2000。这种连接称为信任连接(trust connection)。

混合验证模式是 Windows 集成验证模式和 SQL

Server 验证模式的混合。SQL Server 验证模式中,需要访问者提供登录名称和相应密码,这种连接服务器的方式称为非信任连接(non-trust connection)。

相比之下,数据库级的身份验证远没有服务器级身份验证严格。数据库用户信息不包含密码信息,访问者甚至无须知道他们的数据库用户名就可以访问数据库,当然,这是以访问者是 SQL Server 的合法登录用户为前提的^[3]。

2.2 权限问题

实施安全管理的一个重要步骤是创建用户定义的数据库角色,然后分配权限,完成这一步骤的方法是创建一些名字与全局组名字配套的角色。在气象系统里,可以创建 Meteorology Data Entry Operator, Meteorology Data Entry Managers 这样的角色。创建好角色就可以分配权限,在这个过程中,用标准的 Grant, Revoke 和 Deny 命令去分配权限,须注意的一点是,Deny 权限优于其他的权限,如果用户是 Deny 权限的角色或组的成员,SQL Server 将拒绝用户访问对象。

Web 数据库的终端用户只要有浏览器就能查阅、操作气象信息。为了保证气象信息数据库的安全,必须针对不同用户设置不同的访问权限。访问权限设计原则应该是不给用户不必要的权限。应用系统中不同用户有不同权限,同一用户做不同的操作时所访问的数据也不同。可以采用两种方法分配访问权限。第一,按身份分配权限。例如在气象信息服务中,气象中心领导的权限比基层气象台站的权限高。第二,按角色分配权限。在气象信息服务系统中,以某种身份进行某一项工作就是系统的一个角色,比如高级系统管理员、一般用户等。不同的角色应有不同的权限。系统管理员不但可以浏览数据,还可以更新数据、发布公告、分配权限等。而一般用户只能浏览部分数据。当然,也可以把两者结合起来,即同一个人扮演不同角色时分配不同权限。在气象信息服务系统中,可以建立如下的用户信息表:姓名、密码、工作单位、用户权限类别。

3 管理扩展存储过程

存储过程位于数据库服务器中,是一个 SQL 语句的集合,可包含一个或多个 SQL 语句。其实在多数应用中根本用不到多少系统的存储过程,而 SQL Server 的这么多系统存储过程只是用来适应广大用户需求的,所以请删除不必要的存储过程,因为有些系统的存储过程很容易地被人利用起来提升权限或进行破坏^[4]。

例如:在 Windows 集成验证模式里,气象中心数据库服务器 A 给预报员 B 授权为一般用户,在查询分析器中输入:

```
use master
go
```

(下转第 219 页)

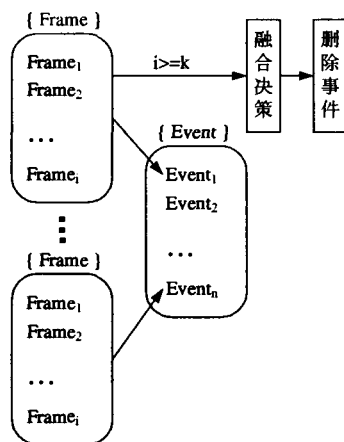


图5 融合中心事件集及其处理

首先将入侵检测探测器按所处位置分为三类:一是被保护主机入侵检测探测器;二是某受保护子网入侵检测探测器;三是其它入侵检测探测器。并设每个探测器参预决策的权重为 m_i , 该事件内不同探测器的总数为 N 。

算法第一步:为每个入侵检测探测器进行参预决策的权重分配。

如果该事件中的目的 IP 地址与受保护主机的目的 IP 地址相同,则 $m_{\text{主机探测器}} = 0.6$, 其余入侵检测探测器 $m_i = 0.4/(N-1)$;

如果该事件中的目的 IP 地址为某一受保护子网的 IP 地址,则 $m_{\text{受保护子网}} = 0.5$, 其余入侵检测探测器 $m_i = 0.5/(N-1)$;

其它情况,则每个入侵检测探测器 $m_i = 1/N$ 。

算法第二步:加权表决法融合。

根据分配好的决策权重和局部判决进行如下计算:

$$\mu_{\text{DDoS}} = \sum m_i * \mu_{i\text{DDoS}} \quad \mu_{\text{worm}} = \sum m_i * \mu_{i\text{worm}}$$

$$\mu_{\text{probe}} = \sum m_i * \mu_{i\text{probe}} \quad \mu_{\text{control}} = \sum m_i * \mu_{i\text{control}}$$

算法第三步:决策。

若融合后的 μ_{DDoS} , μ_{worm} , μ_{probe} , μ_{control} 的最大值小于门限值 $\mu_{\text{阈值}}$, 则将此事件判断为正常, 否则将此事件判断为该最大值对应的攻击行为。

4 结束语

文中提出了一种分布式入侵检测系统的设计与实现, 提出的局部判决、事件关联和融合算法均具有较强的可操作性。文中未能讨论入侵检测响应问题, 读者可参考文献[2]。

参考文献:

- [1] de Boer R C. A Generic Architecture for Fusion - Based Intrusion Detection Systems[D]. [s.l.]: Erasmus University, Rotterdam School of Economics, 2002.
- [2] 郭代飞, 杨义先, 胡正名. 基于大规模网络的自适应入侵响应模型研究[J]. 北京邮电大学学报, 2004, 27(1): 79-83.
- [3] 王 勇, 王行愚, 张瑞霞. 基于 D-S 证据理论的分布式入侵检测方法研究[J]. 计算机工程与应用, 2004(13): 167-169.
- [4] 吕慧勤, 褚永刚, 吕硕望, 等. 入侵检测系统融合机制研究[J]. 网络安全技术与应用, 2003(12): 10-14.
- [5] 罗光春, 卢显良, 张 骏, 等. 基于多传感器数据融合的人侵检测机制[J]. 电子科技大学学报, 2004, 33(1): 71-74.

(上接第 216 页)

```
exec xp_cmdshell 'net user userB password /add'
```

这样数据服务器 A 就增加了预报员 B 用户, 预报员 B 登录数据库服务器 A 后, 在查询分析器中输入:

```
use master
```

```
go
```

```
exec xp_cmdshell 'net localgroup administrators userB /add'
```

后再执行下面的 SQL 语句:

```
exec xp_cmdshell 'net localgroup administrators'
```

发现 userB 已经在 administrators 组中, 意味着预报员 B 已经拥有系统管理员的权限了, 可以执行:

```
use master
```

```
go
```

```
exec sp_dropextendedproc 'xp_cmdshell'
```

这个 SQL 语句是用来去掉 xp_cmdshell 存储过程, xp_cmdshell 存储过程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。另外, 数据库服务器 A 的管理员可以在帐号管理中把系统帐号“BUILTIN\Administrators”删除, 不过这样的后果是一旦 sa 帐号忘记密码的话, 就没有办法恢复了^[5]。

4 结束语

尽管可以利用 SQL Server 气象资料数据库提供的许多工具来管理和配置数据库的安全性能, 但在进行数据库的活动时仍旧可能忽略安全问题。进行数据库活动的过程中暴露出安全漏洞的可能性在很大程度上依旧存在, 文中所讨论的扩展存储过程问题, 它涉及到提升权限的安全问题。加深对安全机制的理解, 可以让人们能够发现那些隐藏的安全漏洞。

参考文献:

- [1] 何培英, 刘雯琳, 徐发山. Web 数据库操作技术[J]. 微机发展, 2003, 13(2): 80-82.
- [2] 樊志平. 数据安全性的实现方法[J]. 微机发展, 2003, 13(12): 53-54.
- [3] 罗远模, 王 珊. SQL Server 数据库系统基础[M]. 北京: 高等教育出版社, 2002.
- [4] Nielsen P. Microsoft SQL Server 2000 宝典[M]. 刘 瑞, 陈微, 等译. 北京: 中国铁道出版社, 2004.
- [5] 周立柱, 冯建华, 孟小峰, 等. SQL Server 数据库原理——设计与实现[M]. 北京: 清华大学出版社, 2004.