基于数据库管理安全的研究

万绪江 刘晓东 李洋

(辽宁省人工影响天气办公室,辽宁 沈阳 110016)

摘 要:从数据库安全的内涵出发,针对目前数据库面临的安全威胁,分析了影响数据库安全的因素,提出了数据库系统的安全体系三个层次结构。重点论述了这三个层次的数据库安全控制所采取的技术手段和措施,并在此基础上设计了一种新型数据库安全防护模型,使之能够实现数据库多层安全控制技术协作与管理,更可靠地保证数据库的安全;展望了数据库安全研究的方向。

关键词:数据库安全;访问控制;推理控制;组合优化;安全模型

中图分类号:TP393.07 **文献标识码**:A **文章编号**:1673-503X(2009)05-0057-05

1 引言

随着网络和信息技术的快速发展和日益普及,信息化成为现代企事业生存的必要条件。信息共享是网络数据库应运而生广泛应用的基础。越来越多的企事业单位数据相继地保存在开放的数据库中,在为用户提供服务的同时也给数据库数据带来了极大的安全隐患,若数据库安全无法保证,就会造成严重后果。因此,有效地保证数据库的安全已成为数据库研究领域重要课题之一。近年来,全国各省市都加大了对网络安全[1-4]和数据库安全[5-8]等研究的力度,特别是在入侵检测[9-10]、角色访问控制[11]、指纹[12]和人脸识别[13]上均投入很大,结合本地的服务要求和网络安全情况,采取:访问控制——口令法;入侵检测——特征库法;数据库加密[14-18]——对称与非对称加解密法;数据库备份——恢复法,但数据安全仍有失保障。针对目前数据库面临的安全威胁,本文重点概述了保证数据库安全所采用的技术方法和必要的措施,提出建立新型数据库安全防护模型,对病毒特征库、入侵特征库、内容过滤特征库、垃圾邮件特征库等统一进行格式化和归并处理,并采用标签的方式转发到不同模块的处理引擎进行组合优化和分项处理[19-20],利用防火墙(FW)和虚拟专用网(VPN)技术支持,使其各司其职、相互制约,基本实现了分析处理引擎的一体化设计,可大大提高多个功能模块并行运行的工作效率,降低数据库安全风险,减少整个系统的安全漏洞,从而保证数据的安全存储和正常运行。

2 数据库系统安全控制概述

数据库系统安全控制是指为数据库系统建立的安全保护措施,以保护数据库系统软件和其中的数据不因偶然或恶意的原因而遭到破坏、更改和泄露。目前,数据库系统安全与网络安全、操作系统安全及协议安全一起构成了信息系统安全的4个最主要的研究领域。

2.1 数据库安全的定义

数据库安全就是保证数据库信息的保密性、完整性、一致性和可用性,以防止非法用户使用所造成数据的泄漏、更改或破坏。

2.2 数据库安全的问题

数据库安全主要分为物理上和逻辑上的问题。物理上的是指计算机软硬件故障或错误导致的数据丢失等问题。解决物理上的问题,常用备份和恢复的策略;逻辑上的问题主要指对信息未被授权的存取操作。分为三类:(1)信息泄漏:包括直接和非直接(通过推理)地对数据的存取;(2)非法数据修改:由操作人员的失误或非法用户的故意修改引起;(3)拒绝服务:通过独占系统资源导致其他用户不能访问数据库。

3 数据库安全技术措施

数据库安全依赖自身内部安全机制、应用环境、外部网络环境等。从整体上讲,保证数据库安全需要做好网络系统层、宿主操作系统层、数据库管理系统层的安保问题。它们从外到内构成了数据库三层安全体系。以下论述三个层次安保关系。

3.1 网络系统层

网络系统是数据库应用的外部环境和基础,是外部入侵数据库安全的第一道防线。网络系统层的安全防范技术有多种,大致可以分为防火墙、入侵检

收稿日期:2009-07-14;**修订日期**:2009-09-01。

作者简介:万绪江,男,1962年生,工程师,主要从事网络安全和雷达技术保障工作。

测、协作式入侵检测、数字签名与认证技术等。

(1)防火墙(FW)。系统的第一道防护屏障,监控可信任网络与不可信任网络之间的访问通道,拦截来自外部的非法访问并阻止内部信息的外泄。防火墙技术主要有三种:数据包过滤器、代理、状态分析。现代防火墙产品通常具有复合技术。

(2)入侵检测(IDS)。综合采用了统计技术、规则方法、网络通信技术和人工智能、密码学、推理等技术及方法,通过监控网络和计算机系统可鉴别是否出现被入侵或滥用的征兆,它已经成为监控和识别攻击的标准解决方案,是安全防御系统的重要组成部分。IDS 的种类包括基于网络和基于主机的入侵检测系统、基于特征的和基于非正常的入侵检测系统、实时和非实时的入侵检测系统等。

(3)协作式入侵检测技术。独立的入侵检测系统不能够对广泛发生的各种入侵活动都作出有效的检测和反应。为弥补独立运作的缺陷,提出了协作式入侵检测系统。在协作式入侵检测系统中,IDS 基于一种统一的规范,入侵检测组件之间自动地交换信息,并且通过信息的交换得到了对入侵的有效监测,可以应用于不同的网络环境。

3.2 宿主操作系统的安全技术

宿主操作系统是数据库的运行平台,能够为数据库提供第二道安全保护。宿主操作系统的安全控制方法主要采用隔离控制、访问控制、信息加密和审计跟踪。主要安全技术有以下三种:

(1)操作系统安全策略用于配置本地计算机的安全设置,包括密码策略、账户锁定策略、审核策略、IP 安全策略、用户权利指派和加密数据的恢复代理以及其他安全选项。

(2)安全管理策略是指网络管理员对系统实施安全管理所采取的方法及策略,其核心是保证服务器的安全和分配好各类用户的权限。

(3)数据安全主要表现为:数据加密技术、数据备份、数据存储的安全性和数据传输的安全性等。可采用的主要有 SSL、TLS、IPSee、Kerberos 认证和 VPN(PPTP、L2TP)等技术。

3.3 数据库管理系统层安全技术

数据库安全性很大程度上取决于数据库管理系统(DBMS)。DBMS 层次安全技术主要是用来解决前面两道防御已被突破的情况下如何继续保障数据库的数据安全,这就要求 DBMS 必须配有一套强有力的安全机制。当前 DBMS 所采用的数据库安全技术主要有以下五种。

3.3.1 访客身份认证

(1)身份认证是 DBMS 提供的最外层安全保护措施,目的是防止非法用户访问 DBMS,包括身份验证和身份识别。通过身份验证来核实访问者的身份,阻止未授权用户的访问。而通过身份识别,可以防止用户的越权访问。身份验证是由系统提供一定的方式让用户标识自己的身份,并将其保存在系统内部。每次用户请求进入系统时,须向系统提供自己身份信息,由系统对用户身份的合法性进行鉴别,通过鉴定后才能登录系统。目前,身份验证采用最常用、最方便的方法是设置口令法。近年来,一些更加有效的身份验证技术迅速发展起来,如智能卡技术和物理特征(指纹、虹膜等)认证技术及数字签名技术等具有高强度的身份验证技术已日渐成熟。

(2)身份识别是以数据库授权为基础,只有经过数据库授权和验证的用户才是合法的用户。数据库授权技术包括授权用户表、用户授权表和系统的读出/写入规则及自动查询修改技术。授权用户表包含授权用户的各项信息,只有与用户表内各项信息完全相符的用户才是授权用户;每个用户有各自事先规定的权限,当授权用户进入时,通过用户权限表赋予用户相应权利;系统的读出/写入规则可以调用数据库的安全规则;自动查询修改技术具有自动查询修改控制功能来防止用户访问数据库中未授权的部分。

3.3.2 数据存取操作控制

访客的身份认证是定义和控制用户对数据库数据的存取访问权限,以确保只授权给有资格的用户访问数据库,防止和杜绝对数据库中数据的非授权访问,是对已经进入数据库系统内部的用户的访问控制,是数据安全保护的前沿屏障。为了实现数据安全,当主体访问客体时,就要进行存取控制合法性检查,检查该用户(主体)是否有资格访问这些数据对象(客体),具有哪些访问权限(如建、读、增、删、改等操作)。若用户的操作请求超出了数据字典中定义的权限,系统将会自动拒绝。

数据存取操作控制的主要类型有三种:

(1)自主访问控制(DAC) 是将存取操作决定权留给产生信息的信息主,是基于存取者身份或所属工作组来进行存取控制的一种手段,具有某种存取特权的存取者可以向其他存取者传递该种存取许可;DAC 允许使用者在没有系统管理员干涉的情况下对它们所控制的对象进行权限修改。

(2)强制访问控制(MAC) 是系统强制主体服从访问控制政策的一种多级访问控制策略,其基本思想:每个主体和客体都有既定的安全属性,它要求所有客体遵守由主体建立的规则,主体对客体是否能执行特定操作取决于二者安全属性之间的关系。

MAC 的所有权限由系统管理员分配,用户不能改变自身或其主/客体的安全属性。

(3)基于角色存取控制(RBAC) 核心思想是安全授权和角色相联系,用户首先要成为相应角色的成员,才能获得该角色对应的权限。角色可以根据工作用户的责任和资格来分配,用户可以轻松地进行角色转换。而随着新应用和新系统的增加,角色可以分配更多的权限,也可以根据需要撤销相应的权限。应用表明,将管理员权限局限在改变用户角色,比赋予管理员更改角色权限更安全。普遍认为 RBAC 比 DAC 和 MAC 更具发展前景。

RBAC 是 DAC 和 MAC 在应用范围、有效性和灵活性上的拓展,利用 RBAC96 模型就可以实现多种 DAC 和 MAC。由于使用了角色继承、约束、角色管理、授权管理等机制,使得存取控制实现和管理更加灵活。目前对 RBAC 的支持主要在应用层,而对 RBAC 的研究已拓展到面向对象数据库、动态数据库和 XML 知识库领域。

3.3.3 原始数据加密

高度敏感数据除采用以上安全性措施之外,还需采用数据加密技术,以强化数据存储的安全保护。数据加密是防止数据库中数据泄露的有效手段,是数据库安全的最后一道重要安全防线。数据库加密的基本思想就是根据加密算法将原始(明文)转换为一种难以直接辨认的密文存储在数据库中,查询时将密文取出解密后得到明文,从而达到信息隐藏的目的,即使黑客窃取了关键数据,也难以得到所需的信息。另外,数据库加密后,不需要了解数据内容的系统管理员不能见到明文,也大大提高了关键数据的安全性。数据加密主要有对称密钥加密技术(常采用 DES 或 IDEA 加密算法)和公开密钥加密技术(常采用 RSA 加密算法)。根据数据库的实际情况,数据库加密宜采用以记录的字段数据为单位进行加/解密、以公开密钥“一次一密”的加密方法来进行。

数据库可以在三个不同层次实现对数据库数据的加密。这三个层次分别是 OS、DBMS 内核层和 DBMS 外层。在 OS 层对数据库文件进行加密。在 DBMS 内核层实现加密,是指数据在物理存取之前完成加/解密工作。这种方式势必造成 DBMS 和加密器(硬件或软件)之间的接口需要 DBMS 开发者的支持,优点为加密功能强,也几乎不会影响 DBMS 的功能;其缺点是在服务器端进行加/解密运算,加重了数据库服务器的负载。比较实际的做法是将数据库加密系统作为 DBMS 的一个外层工具。采用这种加密方式时,加/解密运算可以放在客户端进行,其优点是不会加重数据库服务器的负载并可实现网上传输加密;缺点是加密功能会受限制。

3.3.4 逻辑推理控制

逻辑推理控制就是防止用户通过间接的方式获取本不该获取的数据或信息。应对统计推理的技术主要有两种方法,即数据扰动:事先对需要进行统计的敏感数据进行加工;查询控制:控制可以查询的记录数,常常应用在统计数据库中。

3.3.5 审计跟踪与攻击检测

审计是在数据库系统运行期间,系统自动跟踪用户的全部操作并记录在日志文件中。记录内容包括:用户名,密码,用户的 IP 地址,操作类型(输入、删除、修改)和操作日期,所涉及到的数据等。若发现系统的数据遭到破坏,可根据日志记录分析调查、追究责任,或者从日志中判断密码是否被盗,以便修改密码,重新分配权限,确保系统的安全。攻击检测则是根据审计数据分析检测内部和外部攻击者的攻击企图,再现导致系统现状事件,追查有关责任者,以分析发现系统安全漏洞,改进增强系统的安全强度。

4 建立新型数据库安全防护模型

4.1 新型数据库安全防护模型结构及其作用

新型数据库安全防护模型在安全防护的基础上建立起来,集访问控制、入侵检测、数据库加密和数据库备份等优化组合的多个功能模块于一身。该模型通过对病毒特征库、入侵特征库、内容过滤特征库和垃圾邮件特征库等统一进行格式化和归并处理,采用标签的方式转发到不同模块的处理引擎进行组合优化和分项处理,利用防火墙(FW)和虚拟专用网(VPN)技术支持,实现了分析处理引擎的一体化设计,提高了多个功能模块并行运行的工作效率,降低了数据库风险,减少了系统的安全漏洞,保证了系统安全和数据库的正常运行。如图 1 所示。

在用户对数据发出存取请求和安全服务时进行严格筛选,对管理员精细划分[21]为:数据库管理员(DBA)主要负责数据库的建立、维护及自主存取控制;数据库安全管理员(SA)主要负责强制存取控制;数据库审计员(DA)主要负责数据库系统的跟踪审计活动。建立健全各项规章制度,做到数据库管理人员的权限划分和界定,及时更新行为知识库和统一特征库的内容。使之成为相互制约、权责明晰的集约化管理模式。

4.2 VPN 技术安全种类

目前,VPN 主要采用四项技术保证安全。这四项技术分别是隧道技术(Tunneling)、加解密技术(En-

cryption & Decryption)、密钥管理技术(Key Management)和使用者与设备身份认证技术(Authentication)。

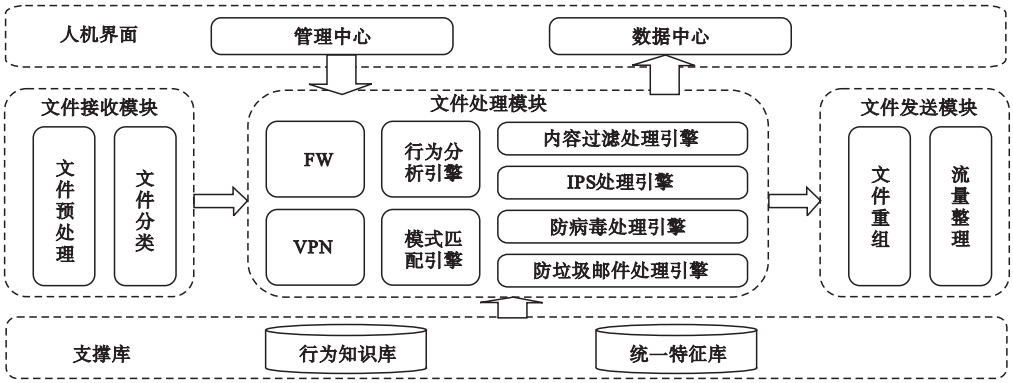

图1 新型数据库安全防护模型

4.2.1 隧道技术

隧道技术是VPN的基本技术类似于点对点连接技术,它在公用网建立一条数据通道(隧道),让数据包通过这条隧道传输。隧道是由隧道协议形成的,分为第二、第三层隧道协议。第二层隧道协议是先将各种网络协议封装到PPP中,再将整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准,由IETF融合PPTP与L2F而形成。第三层隧道协议是把各种网络协议直接装入隧道协议中,形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec等。IPSec(IP Security)是由一组RFC文档组成,定义了一个系统来提供安全协议选择、安全算法,确定服务所使用密钥等服务,从而在IP层提供安全保障。

4.2.2 加解密技术

加解密技术是数据通信中一项较成熟的技术,VPN可直接利用现有技术。

4.2.3 密钥管理技术

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种。SKIP主要是利用Diffie-Hellman的演算法则,在网络上传输密钥;在ISAKMP中,双方都有两把密钥,分别用于公用、私用。

4.2.4 使用者与设备身份认证技术

使用者与设备身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

5 数据库安全研究展望

随着数据库技术与分布式技术、面向对象技术、并行处理技术、多媒体处理、人工智能和模糊技术等技术的结合,在未来一段时间内数据库安全技术的主要研究方向表现在以下几个方面:

(1)访问控制的研究。包括自主访问控制(DAC)、强制访问控制(MAC),特别是基于角色存取控制(RBAC)的研究。

(2)隐蔽信道问题。包括如何通过信息流控制和推理控制等其他安全控制机制来彻底检测与消除的研究。

(3)数据库的审计跟踪。目前,粒度较细的审计很耗时间和空间,如何改进审计机制或者是否有可以借助高效率的自动化审计工具与DBMS集成研究。

(4)多级安全数据库语义的研究和DBMS的多级安全保护体制的研究。

(5)数字水印在数据库安全应用中的研究。

6 结语

安全技术不是相互独立的,而是彼此依赖,相互支持的。访问控制的正确性依赖于安全的识别和鉴别机制,安全的识别和鉴别机制也是审计跟踪的基础,而为了具有安全的识别和鉴别机制,有必要采用加密技术等。数据库系统作为数据管理的载体[22-23],它是计算机网络信息系统的核心部分,其安全性、实时性和可用性有着相当重要的位置。本文从数据库安全性角度出发,分析了影响数据库安全的诸多因素,重点论述了数据库安全控制的技术方法和技术手段。在此基础上设计了新型数据库安全防护模型。由于模型采用模块化结构设计[24],各子模块功能相对独立,所以数据库安全防护工作基本得到保障。该模型具有良好的安全性、实时性、完整性、可用性、移植性和扩充性,各子功能模块还有待于进一步完善。

参考文献

[1] 林闯,肖岩平,王元卓,等. 网络保护质量研究[J]. 计算机学报,2008,31(10):1667-1678.

[2] 李向宁,郝克刚,赵克. 一种新的业务过程管理模型

[J]. 计算机学报,2008,31(1):104 - 111.
[3] 梁彬,侯看看,石文昌,等. 一种基于安全状态跟踪检查的漏洞静态检测方法[J]. 计算机学报,2009,32(5):899 - 909.
[4] 曾彬,张大方,黎文伟,等. 面向网络行为特征分析的网络监测系统设计及实现[J]. 计算机科学,2009,36(1):86 - 91.
[5] 周水庚,李丰,陶宇飞,等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报,2009,32(5):847 - 861.
[6] 周傲英,金澈清,王国仁,等. 不确定性数据管理技术研究综述[J]. 计算机学报,2009,32(1):1 - 16.
[7] 蔡涛,鞠时光,牛德姣. 基于免疫安全存储设备 IBSSD 的研究与实现[J]. 计算机科学,2009,36(1):101 - 105.
[8] 郭文宏,范学峰. 面向 Web 结构化信息处理的汉语知识库构建研究[J]. 计算机科学,2009,36(1):201 - 204.
[9] 唐莞菁,汪卫,王智慧,等. 一种多级安全数据模型中的多实例语义[J]. 计算机研究与发展,2007,44(增刊):238 - 243.
[10] 吕高锋,孙志刚,卢锡城. 域间 IP 欺骗防御服务净化机制[J]. 计算机学报,2009,32(3):552 - 563.
[11] 董理君,余胜生,杜敏,等. 一种基于环境安全的角色访问控制模型研究[J]. 计算机科学,2009,36 (1):51 - 55.
[12] 梅园,曹国,孙怀江,等. 一种新的指纹奇异点快速检测方法[J]. 计算机学报,2009,32(5):1037 - 1045.
[13] 严严,章毓晋. 基于视频的人脸识别研究进展[J]. 计算机学报,2009,32(05):878 - 886.
[14] 肖飞,王运琼,李映松,等. 基于光盘映像文件的 CD - ROM 数据加密与解密方法[J]. 计算机科学,2009,36(5):299 - 301.
[15] 吴海,陈巍,卢炎生. 一种嵌入式移动实时数据库的并发控制策略[J]. 计算机科学,2009,36(2):155 - 158.
[16] 韩卫,张艳苏. MIS 中数据库安全性研究[J]. 计算机工程,2002,28(6):34 - 37.
[17] 应乐年,汪卫,施伯乐. 一种安全数据库多级安全模型与外键引用研究[J]. 计算机应用与软件,2009,7(26):146 - 150.
[18] 陈珂,苗付友,熊焰. 基于 RSA 的代理环签名方案[J]. 计算机科学,2009,36(2):132 - 136.
[19] 伏晓,蔡圣闻,谢立. 网络安全管理技术研究[J]. 计算机科学,2009,36(2):15 - 20.
[20] 傅建明,余乔莉,杨灿. 基于数据场的网络安全风险融合模型[J]. 计算机科学,2009,36(5):72 - 75.
[21] 胡文启,徐军,张伍荣. 网管实战宝典[M]. 清华大学出版社,2008:132 - 171.
[22] 侯乃学,袁健,万绪江. 汉字 DBASE - Ⅲ 关系数据库在气象科研管理上的应用[J]. 辽宁气象,1988 (4):36 - 38.
[23] 万绪江,孟挺,王英华,等. 职工教育管理系统[J]. 辽宁气象,1992 (4):42 - 43.
[24] 班显秀,白乐生,万绪江,等. 在微机上制作动画的方法及其实际应用——"沈阳化学突发事故模拟演示"简介[J]. 辽宁气象,1990 (3):29 - 30.

Study on database management security

WAN Xu-jiang　LIU Xiao-dong　LI Yang
(Weather Modification Office in Liaoning Province, Shenyang 110016, China)

Abstract: Based on the consideration of current database security, factors influencing database security were analyzed. Three hiberarchy security system frameworks of database system were brought up. Technological measures controlling three hiberarchy frameworks security of database system were discussed. A new database security protection model was designed based on the above-mentioned. Thus, multilayer security control cooperation and management of database can be realized, and it can ensure the database security. Finally, the future tasks on database security were discussed.

Key words: Database security; Access control; Reasoning control; Combination and optimization; Security model