数据库系统安全技术框架综述 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/224/2021_2022__E6_95_B0_E6_8D_AE_E5_BA_93_E7_c102_224433.htm 1. 前言 随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、国家安全。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一，本文就安全防入侵技术做简要的讨论。 数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从业人员素质等因素息息相关，因此，从广义上讲，数据库系统的安全框架可以划分为三个层次：⑴网络系统层次；⑵宿主操作系统层次；⑶数据库管理系统层次。 这三个层次构筑成数据库系统的安全体系，与数据安全的关系是逐步紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。下面就安全框架的三个层次展开论述。 2. 网络系统层次安全技术 从广义上讲，数据库的安全首先倚赖于网络系统。随着Internet的发展普及，越来越多的公司将其核心业务向互联网转移，各种基于网络的数据库应用系统如雨后春笋般涌现出来，面向网络用户提供各种信息服务。可以说网络系统是数据库应用的外部环境和基础，数据库系统要发挥其强大作用离不开网络系统的支持，数据库系统的用户（如异地用户、分布式

用户）也要通过网络才能访问数据库的数据。网络系统的安全是数据库安全的第一道屏障，外部入侵首先就是从入侵网络系统开始的。网络入侵试图破坏信息系统的完整性、机密性或可信任的任何网络活动的集合，具有以下特点： a）没有地域和时间的限制，跨越国界的攻击就如同在现场一样方便；b）通过网络的攻击往往混杂在大量正常的网络活动之中，隐蔽性强；c）入侵手段更加隐蔽和复杂。 计算机网络系统开放式环境面临的威胁主要有以下几种类型：a)欺骗（Masquerade）；b)重发(Replay)；c)报文修改(Modification of message)；d)拒绝服务(Deny of service)；e)陷阱门(Trapdoor)；f)特洛伊木马(Trojan horse)；g)攻击如透纳攻击（Tunneling Attack）、应用软件攻击等。这些安全威胁是无时、无处不在的，因此必须采取有效的措施来保障系统的安全。 从技术角度讲，网络系统层次的安全防范技术有很多种，大致可以分为防火墙、入侵检测、协作式入侵检测技术等。⑴防火墙。防火墙是应用最广的一种防范技术。作为系统的第一道防线，其主要作用是监控可信任网络和不可信任网络之间的访问通道，可在内部与外部网络之间形成一道防护屏障，拦截来自外部的非法访问并阻止内部信息的外泄，但它无法阻拦来自网络内部的非法操作。它根据事先设定的规则来确定是否拦截信息流的进出，但无法动态识别或自适应地调整规则，因而其智能化程度很有限。防火墙技术主要有三种：数据包过滤器(packet filter)、代理(proxy)和状态分析(stateful inspection)。现代防火墙产品通常混合使用这几种技术。⑵入侵检测。入侵检测(IDS-- Instrusion Detection System)是近年来发展起来的一种防范技术，综合采用了统计技术、规则方法

、网络通信技术、人工智能、密码学、推理等技术和方法，其作用是监控网络和计算机系统是否出现被入侵或滥用的征兆。1987年，Derothy Denning首次提出了一种检测入侵的思想，经过不断发展和完善，作为监控和识别攻击的标准解决方案，IDS系统已经成为安全防御系统的重要组成部分。 入侵检测采用的分析技术可分为三大类：签名、统计和数据完整性分析法。 ①签名分析法。主要用来监测对系统的已知弱点进行攻击的行为。人们从攻击模式中归纳出它的签名，编写到IDS系统的代码里。签名分析实际上是一种模板匹配操作。 ②统计分析法。以统计学为理论基础，以系统正常使用情况下观察到的动作模式为依据来判别某个动作是否偏离了正常轨道。 ③数据完整性分析法。以密码学为理论基础，可以查证文件或者对象是否被别人修改过。 IDS的种类包括基于网络和基于主机的入侵监测系统、基于特征的和基于非正常的入侵监测系统、实时和非实时的入侵监测系统等。 ⑶协作式入侵监测技术 独立的入侵监测系统不能够对广泛发生的各种入侵活动都做出有效的监测和反应，为了弥补独立运作的不足，人们提出了协作式入侵监测系统的想法。在协作式入侵监测系统中，IDS基于一种统一的规范，入侵监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. 宿主操作系统层次安全技术 操作系统是大型数据库系统的运行平台，为数据库系统提供一定程度的安全保护。目前操作系统平台大多数集中在Windows NT 和Unix，安全级别通常为C1、C2级。主要安全技术有操作系统安全策略、安全管理策略、数据安全等方面。 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、加密数据的恢复代理以及其它安全选项[7]。具体可以体现在用户账户、口令、访问权限、审计等方面。 用户账户：用户访问系统的"身份证"，只有合法用户才有账户。 口令：用户的口令为用户访问系统提供一道验证。 访问权限：规定用户的权限。 审计：对用户的行为进行跟踪和记录，便于系统管理员分析系统的访问情况以及事后的追查使用。 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。针对不同的操作系统、网络环境需要采取的安全管理策略一般也不尽相同，其核心是保证服务器的安全和分配好各类用户的权限。 数据安全主要体现在以下几个方面：数据加密技术、数据备份、数据存储的安全性、数据传输的安全性等。可以采用的技术很多，主要有Kerberos认证、IPSec、SSL、TLS、VPN（PPTP、L2TP）等技术。 4. 数据库管理系统层次安全技术 数据库系统的安全性很大程度上依赖于数据库管理系统。如果数据库管理系统安全机制非常强大，则数据库系统的安全性能就较好。目前市场上流行的是关系式数据库管理系统，其安全性功能很弱，这就导致数据库系统的安全性存在一定的威胁。 [1] [2] 下一页 