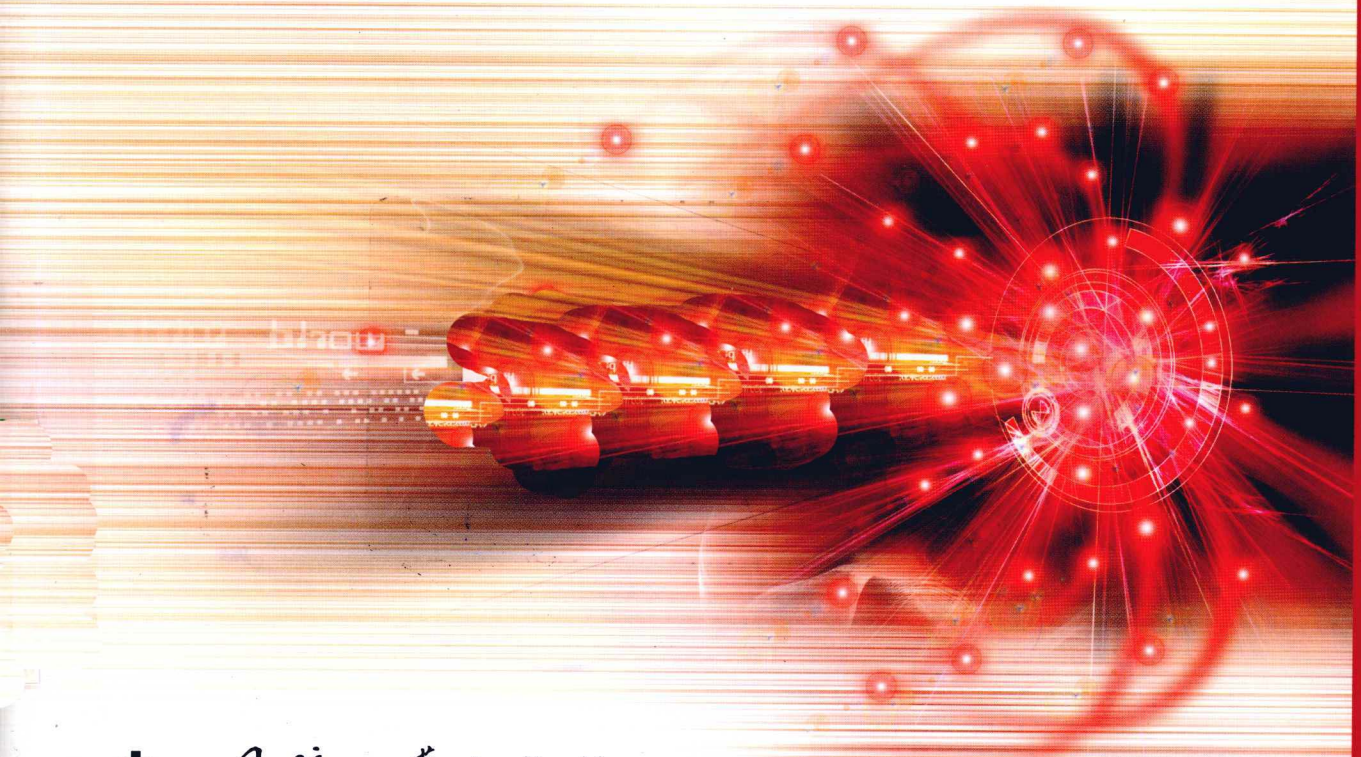
陈 越　寇红召　费晓飞　卢贤玲◎编著

数据库安全

DATABASE SECURITY



国防工业出版社
National Defense Industry Press

内 容 简 介

本书全面介绍了在网络数据共享环境下，保证数据完整性、可用性、机密性和隐私性的数据库安全理论和技术。内容涉及数据库访问控制、XML 与 Web 服务安全、数据库加密技术、数据库审计、推理控制与隐通道分析、数据仓库和 OLAP 系统安全、数据库水印技术、可信记录保持技术、入侵容忍与数据库可生存性和数据隐私保护等。全书基本上反映了近年来数据库安全研究的最新研究成果，提供了详尽的参考文献，并力图指出进一步的研究方向。

本书既可作为计算机科学与技术、信息安全等专业的本科生、研究生课程的教材，也可供广大数据库安全工程技术和管理人员参考。

图书在版编目(CIP)数据

数据库安全／陈越等编著. —北京：国防工业出版社，2011.7

ISBN 978-7-118-07450-5

Ⅰ.①数… Ⅱ.①陈… Ⅲ.①数据库系统—安全技术

Ⅳ.①TP311.13

中国版本图书馆 CIP 数据核字(2011)第 107772 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092　1/16　印张 13¾　字数 308 千字

2011 年 7 月第 1 版第 1 次印刷　印数 1—4000 册　定价 32.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

前　言

随着计算机技术的突飞猛进，数据库作为信息技术中不可或缺的一部分也日显重要。数据库已经融入到日常生活的诸多方面，应用也日益广泛，不仅在传统的商业领域、事务处理领域发挥着重要作用，而且在非传统领域，如商务智能、统计分析、移动通信等领域也正在发挥越来越重要的作用。与此同时数据库技术与网络技术、多媒体技术也逐渐出现融合的趋势。

一方面数据库系统在网络上承担着向用户提供开放式的数据处理服务，另一方面数据库系统也面临着开放式环境所带来的对数据完整性、可用性、机密性、隐私性的各种威胁，如数据不完整、不一致、关键数据丢失、系统意外停止服务、非法与恶意使用数据库等都会对数据库及其支持的上层应用带来灾难性的后果。因此，保证数据库的安全在当前信息技术中占有十分重要的地位和作用。本书就数据库安全方面的理论做出了较为全面翔实的介绍，同时紧跟数据库技术发展前沿，深入浅出地讨论了数据库安全保护的技术与方法。

数据库技术飞速发展，最新科研成果不断涌现，原有的相关图书在内容上不够全面，有些部分也未将最新的研究成果包含其中，为满足从事数据库基础软件研究与开发、数据库应用开发和数据库安全研究的科技工作者的需要，编写了本书。本书的编著是在作者多年从事数据库安全教学和科研的基础上完成的，旨在全面介绍数据库安全的理论、技术和方法，既包含了传统数据库安全的基本内容，也包含了数据库安全领域的最新研究成果。

本书内容主要包括数据库访问控制、XML 与 Web 的安全、数据库加密技术、数据库审计、推理控制与隐通道分析、数据仓库和 OLAP 系统中的安全问题、数据库水印技术、可信记录保持技术、入侵容忍与数据库的可生存性以及数据的隐私保护等。

本书第 1、7、8、10 章由陈越编写，第 2、9、11 章由寇红召编写，第 4 章由费晓飞编写，第 3、5、6 章由卢贤玲编写，全书由陈越负责策划，陈越和费晓飞进行了统稿和校对。编写过程中研究生甄鸿鹄、马慧娟、韩磊磊、邵婧、张英杰等同学也参与了资料搜集整理、专题课题研究等与编写本书相关的工作。本书编写参考了大量的相关文献，在此对这些文献的作者表示感谢，编者仅列出了主要的参考文献，如有纰漏之处敬请谅解。

由于数据库安全涉及的范围很广，其研究也在不断进展中，本书难免存在遗漏和不足之处，敬请读者批评指正。

目　录

第1章 绪 论

随着信息技术的发展，基于网络的分布式信息系统已在政府、企事业单位、军事等部门广泛应用。作为信息管理的主要工具，数据库技术是信息系统的核心和基础，已成为计算机、网络领域最重要的技术之一。数据是组织、机构最重要的战略和运营资产，对个人来说，也是极有价值的信息资源，对数据机密性、完整性、可用性、隐私性造成的破坏以及数据的非法使用不但会影响到单个用户或单个系统，还可能对整个组织、机构造成灾难性的后果；随着信息系统体系结构的不断发展以及新的应用需求的不断出现，数据库技术与网络、面向对象、Web、普适计算、网格、P2P、联机分析处理技术、数据挖掘等技术不断融合，摆脱了单一数据库系统的局限，呈现出开放式、网络化、分布式、智能化等新特征，在这种开放式环境下，数据库系统面临的安全威胁和风险也迅速增大，数据库安全的研究领域迅速扩大，对数据安全的要求不断提升，这些新的领域和新的要求已经超出了现有技术所能解决的范围，数据库安全问题面临诸多挑战；同时，加强数据库的安全性也有利于增强信息系统用户对数据管理基础平台和信息服务的信心，推动信息技术及其应用的健康发展。因此，数据库安全在当前信息技术中占有十分重要的地位和作用，也是众多学者和研究人员研究的热点之一。

本章首先讨论了数据库技术的发展和研究热点问题，介绍了数据库安全的基本概念、风险和需求；简述了数据库安全的策略、模型与机制；介绍了数据库安全的研究新进展。

1.1 数据库技术发展及其研究热点

1.1.1 数据库技术的发展

数据模型是数据库系统的核心和基础。因此，对数据库技术发展阶段的划分应该以数据模型的发展演变作为主要依据和标志。总体说来，数据库技术从开始到现在一共经历了三个发展阶段：第一代是网状、层次数据库系统，第二代是关系数据库系统，第三代是以面向对象数据模型为主要特征的数据库系统。

第一代包括网状和层次数据库系统，是因为它们的数据模型虽然分别为层次和网状模型，但实质上层次模型只是网状模型的特例而已。这两者都是格式化数据模型，都是在20世纪60年代后期研究和开发的，不论是体系结构、数据库语言，还是数据的存储管理，都具有共同特征。

第二代数据库系统支持关系数据模型。关系模型不仅具有简单、清晰的优点，而且有关系代数作为语言模型，有关系数据理论作为理论基础。因此关系数据库具有形式基础好、数据独立性强、数据库语言非过程化等特点，这些特点是数据库技术发展到了第二代的显著标志。目前使用的大多数数据库产品属于关系数据库产品。

第三代数据库系统(面向对象数据库系统)是为了满足新的数据库应用需要而产生的新一代数据库系统。它把面向对象的方法和数据库技术结合起来,可以使数据库系统的分析、设计最大程度地与人们对客观世界的认识相一致。虽然面向对象数据库的研究已经进行了若干年,但目前数据库产品均是在关系数据库编程开发方法中加入了某些面向对象的特征,其本质的数据模型仍是关系数据模型。

鉴于上述情况,本书主要以基于关系数据模型的数据库安全问题作为研究对象。

关系数据库管理系统管理用关系模型组织的数据集合,它主要具有数据结构化、共享性、独立性等特点。数据库管理系统提供了以下三类基本功能。

(1) 数据定义。数据库管理系统提供定义数据类型和数据存储形式的功能。每个记录的每个字段中的信息为一个数据。因记录的信息不同,其数据类型也应不同。通过定义数据类型,可以在一定程度上保证数据的完整性。

(2) 数据操作。数据库管理系统提供多种处理数据的方式。例如:在一张表中查找信息或者在几个相关的表或文件中进行复杂的查找;使用相应的命令更新一个字段或多个记录的内容;用一个命令对数据进行统计,甚至可以使用数据库管理系统工具进行编程,以实现更加复杂的功能。

(3) 数据控制。数据库管理系统对数据提供一定的访问控制功能,从而保证在多个用户共享数据时,只有被授权的用户才能查看或修改数据,某些数据库产品还提供了数据加解密功能。

1.1.2 数据库技术的研究热点

1. Web 数据库

随着万维网(World Wide Web, WWW)的迅速扩展,WWW 上可用数据源的数量也在迅速增长。人们正试图把 WWW 上的数据源集成为一个完整的 Web 数据库,使这些数据资源得到充分利用。

Web 技术的蓬勃发展,使人们已不满足只在 Web 浏览器上获得静态信息,人们需要通过它发表意见、查询数据,甚至进行网上购物,这就需要实现 Web 与数据库的互连。数据库技术发展比较成熟,特别适用对大量的数据进行组织管理,Web 技术具有较佳的信息发布途径,将两者结合起来,充分利用大量已有的数据库信息资源,可以使用户在 Web 浏览器上方便地检索和浏览数据库的内容,这对许多软件开发者来说具有极大的吸引力。所以,开发动态的 Web 数据库已成为当今 Web 技术研究的热点。

Web 数据库技术一般采用三层或多层体系结构,前端采用基于客户机的浏览器技术,通过 Web 服务器及中间件访问数据库。目前,Web 数据库技术主要有 CGI、SAPI、JDBC(Java Database connector)、RAD(Rapid Application Development)和 ASP。

2. XML 支持

由于 XML(eXtended Markup Language——可扩展的标记语言)采用了可存储数据关系和数据属性的层次型树状数据模型,因此,可以将 XML 文档看做是 XML 数据库。

XML 数据库是一种支持对 XML 格式文档进行存储和查询等操作的数据管理系统。在系统中,开发人员可以对数据库中的 XML 文档进行查询、导出和指定格式的序列化。

目前,XML 数据库有三种类型:

（1）XML Enabled Database （XEDB），即能处理 XML 的数据库。其特点是在原有的数据库系统上扩充对 XML 数据的处理功能，使之能适应 XML 数据存储和查询的需要。一般的做法是在数据库系统之上增加 XML 映射层，这可以由数据库供应商提供，也可以由第三方厂商提供。映射层管理 XML 数据的存储和检索，但原始的 XML 元数据和结构可能会丢失，而且数据检索的结果不能保证是原始的 XML 形式。XEDB 的基本存储单位与具体的实现紧密相关。

（2）Native XML Database （NXD），即纯 XML 数据库。其特点是以自然的方式处理 XML 数据，以 XML 文档作为基本的逻辑存储单位，针对 XML 的数据存储和查询特点专门设计适用的数据模型和处理方法。

（3）Hybrid XML Database （HXD），即混合 XML 数据库。根据应用的需求，可以视其为 XEDB 或 NXD 的数据库，典型的例子是 Ozone。用户可以定义自己的标记，用来描述文档的结构。随着 Web 应用的发展，越来越多的应用都将数据表示成 XML 的形式，XML 已成为网上数据交换的标准。所以当前数据库管理系统都扩展了对 XML 的处理，存储 XML 数据，支持 XML 和关系数据之间的相互转换。

由于 XML 数据模型不同于关系模型和对象模型，其灵活性和复杂性导致了许多新问题的出现。在学术界，XML 数据处理技术成为数据库、信息检索及许多其他相关领域研究的热点，涌现了许多研究方向，包括 XML 数据模型、XML 数据的存储和索引、XML 查询处理和优化、XML 数据压缩等。在数据库产品中，IBM 公司在它新推出的 DB2 9 版本中，直接把对 XML 的支持作为其新产品的最大卖点，号称是业内第一个同时支持关系型数据和 XML 数据的混合数据库，无需重新定义 XML 数据的格式，或将其置于数据库大型对象的前提下，IBM DB2 9 允许用户无缝管理普通关系数据和纯 XML 数据。对于传统关系型数据与层次型数据的混合应用已经成为了新一代数据库产品所不可或缺的特点。除了 IBM，Oracle 和微软也同时宣传了它们的产品可以实现高性能 XML 存储与查询，使现有应用更好地与 XML 共存。

3. 数据仓库

数据仓库（Data Warehouse）技术是数据库技术应用和联机事物处理（Online Analysis Processing，OLAP）技术发展深化的结果，是决策支持系统（Decision Support System，DSS）的重要组成部分。其目的是能够更好地存储和处理大规模数据，并能够从这些数据中提取出有用的信息，以供企业更好地决策。数据仓库技术是从数据库技术发展而来的，是面向主题的、集成的、稳定的和随时间变化的数据集合。数据仓库系统（Data Warehouse System，DWS）由三个组成部分，即数据仓库、数据仓库管理系统和数据仓库分析工具。数据仓库用来存放数据。与关系数据库不同的是，在数据仓库中，数据的来源并不局限于单一的数据源，它可以来源于现存的多个数据库。数据仓库中数据的组织也不再是二维表的格式，而是采用多维立方体的结构，这种结构把数据属性分为“维”和“度量”，并增加了旋转、切片和切块、下钻和上卷的操作，以增强对数据仓库的查询功能。数据仓库管理系统用来完成对数据的各种操作，它不仅要完成数据库管理系统的功能，以保持数据的完整性、一致性、安全性、共享性以及分布式处理的能力，而且还支持对数据仓库的操作，包括：支持对多维数据的操作；支持 OLAP；支持异种数据库的互连，并且把来自不同数据源的数据转换成面向主题的格式，以便用户访问和分析，最终做出决策。数据仓库工具是提供

给用户使用的界面视图，以保证用户能够轻易地操纵数据仓库。

4. 数据挖掘

随着计算技术和 Internet 技术的发展，数据资源日益丰富。但是数据资源中蕴涵的知识却至今未能得到充分的挖掘和利用，“数据丰富而知识贫乏”的问题十分严重。近年来兴起的数据挖掘（Data Mining）技术为解决这个问题带来了一线曙光。

数据挖掘是一种从大型数据库或数据仓库中发现并提取出隐藏在其中的信息的一种新技术，它同样也是 DSS 的一个重要组成部分。数据挖掘与 OLAP 不同，OLAP 重在分析数据，而数据挖掘则重在自动从数据中提取人们感兴趣的知识，并把提取出来的知识表示成概念、规则、规律和模式。因此，可以说数据挖掘是一种更加智能化的知识发现行为，它涉及的研究领域也非常广阔，包括归纳学习、机器学习、人工智能、统计分析等。

5. 网格数据管理

简单地讲，网格是把整个网络整合成一个虚拟的、巨大的超级计算环境，实现计算资源、存储资源、数据资源、信息资源、知识资源、专家资源的全面共享。网格环境下的数据管理目标是，保证用户在存取数据时无需知道数据的存储类型（如数据库、文档、XML）和位置。目前，数据网格研究的问题之一是，如何在网格环境下存取数据库，提供数据库层次的服务，因为数据库显然应该是网格中十分宝贵而数据资源。数据库网格服务不同于通常的数据库查询，也不同于传统的信息检索，需要将数据库提升为网格服务，把数据库查询技术和信息技术有机结合，提供统一的基于内容的数据库机制和软件。

1.2 信息安全与数据库安全

信息安全对于我国的信息化建设非常重要，制定正确的信息安全战略、构建全面的信息安全保障体系是信息安全工作的重点。信息安全保护的核心是资产，数据正是组成资产的基本元素，在数据库中存储了大量数据，数据生存期长，维护的要求高，涉及信息在不同粒度的安全，即客体具有层次性和多样性。对于信息安全而言，数据库的防护是如同网络安全一样重要的核心地带。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四个最主要的研究领域。

1.2.1 信息安全技术

国际标准化组织（ISO）对信息安全的定义是：“在技术上和管理上为数据处理系统建立的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露”。

1. 信息安全属性

信息安全是信息系统安全、信息自身安全和信息行为安全的总和，目的是保护信息和信息系统免遭偶发的或有意的非授权泄露、修改、破坏或丧失处理信息能力，实质是保护信息的安全性，即机密性、完整性、可用性、可控性和不可否认性。

机密性：指信息不泄露给非授权实体并供其利用的特性。

完整性：指信息不能被未经授权的实体改变（不被偶然或蓄意地增加、删除、修改、伪造、乱序、重放等破坏）的特性。

可用性：指信息能够被授权实体访问并按要求使用，信息系统能以人们所接受的质量水平持续运行，为人们提供有效的信息服务的特性。

可控性：指授权实体可以对信息及信息系统实施安全监控，控制信息系统和信息使用的特性。

不可否认性：不可否认性是面向通信双方（人、实体或进程）信息真实同一的安全要求的属性，它包括收、发双方均不可否认。不可否认性可以在出现信息安全纠纷时提供调查依据和手段。

2. 信息安全威胁

信息安全威胁是对信息资产（属于某个组织的有价值的信息或资源）引起不期望事件而造成损害的潜在可能性。基本的安全威胁有信息泄露、完整性破坏、业务拒绝/服务拒绝、非法使用。

信息泄露：信息有意或无意泄露给某个非授权的人或实体。例如：利用电磁泄露或搭线窃听等方式截获信息；非法进入主机复制敏感信息；通过分析信息长度、流通频度、流向和流量析出有用的信息而造成信息的丢失或泄露等。

完整性破坏：数据的一致性/完整性被非授权地增加、删除、修改、伪造、乱序、重放而受到损坏（改变数据的价值和存在）。

业务拒绝/服务拒绝：攻击者通过对系统进行过量的、非法的、根本不能成功的访问尝试使系统崩溃或超载，从而导致对信息或其他资源的合法访问被无条件地阻止或访问不畅。

非法使用：某一资源被某个非授权的人或实体使用，或被授权的人或实体以越权的方式使用。例如：假冒或盗用合法用户身份，非法进入信息系统进行违法操作；合法用户以未授权方式进行操作，等等。

3. 信息安全服务

按国家标准 GB/T 9387.2－1995，适合于数据通信环境的安全服务有认证服务、访问控制服务、数据机密性服务、数据完整性服务和不可否认服务等。

认证服务：提供通信对等实体和数据来源的认证。对等实体认证用于两开放系统的同等层中的实体建立连接或数据传输阶段，对对方实体（用户或进程）的合法性、真实性进行确认，以防止假冒。数据源认证服务用于对数据单元的来源提供确认，证明某数据与某实体有着静态不可变关系，但它对数据单元的重复或篡改不提供认证保护。

访问控制服务：用于防止未授权用户非法使用系统资源。这种保护可应用于使用通信资源、读/写或删除信息资源、处理资源的操作等各种类型的对资源的访问。

数据机密性服务：对数据提供保护，防止非授权的泄露。为了防止网络中各个系统之间交换数据被截获或被非法存取而造成泄密，提供密码加密保护。它分为数据保密和通信业务流保密。

数据完整性服务：防止非法实体对数据的修改、插入、删除等。它通过带或不带恢复功能的面向连接方式的数据完整性、选择字段面向连接或无连接方式的数据完整性以及无连接方式数据完整性等服务来满足不同用户、不同场合对数据完整性服务的不同要求。

不可否认服务：也称抗否认服务或抗抵赖服务。其分为两种：①为数据的接收者提供数据的原发证明，以防止发送方在发送数据后否认自己发送过此数据；②为数据的发送者

提供数据交付证明，以防止接收方在收到数据后否认收到过此数据或否认它的内容（伪造接收数据）。

4. 信息安全技术体系

信息安全技术是信息安全保障体系的主要支撑环节，没有技术的支撑，所有的信息安全服务都是纸上谈兵。面向应用的信息安全技术主要包括信息安全支撑技术、安全互连与接入控制、网络计算环境安全和应用安全技术。

信息安全支撑技术是基础，一方面，它直接保护信息的安全特性，如通过加密和认证保护信息的机密性、完整性和不可否认性；另一方面，提供对安全互连与接入、计算环境安全和应用安全技术的支持。主要包括信息保密技术、信息认证技术、授权与访问控制技术和安全管理技术。

安全互连与接入控制是网络安全的关键，主要提供局域网间基于公共网络的逻辑安全互连和实现局域网的接入控制与物理隔离。主要包括虚拟专用网技术、防火墙技术和网络隔离技术。

网络计算环境安全是网络安全的起点，主要是保护与平台相连的终端主机和服务器运行过程和运行状态的安全。主要包括操作系统安全、数据库安全、安全扫描技术、入侵检测技术和病毒及防护技术。

应用安全技术是信息化建设的主要目的，信息是依靠应用系统来提供服务的。常用的应用安全有电子邮件安全技术、Web 安全技术和电子商务安全技术。

1.2.2 数据库安全威胁

根据安全威胁的来源及攻击的性质，可将数据库的安全威胁大致分为以下几类：

1. 逻辑的威胁

非授权访问：即用对未获得访问许可的信息的访问。

推理访问数据：是指由授权读取的数据，通过推论得到不应访问的数据。

病毒：病毒可以自我复制，永久地或是通常是不可恢复地破坏自我复制的现场，达到破坏信息系统、取得信息的目的。

特洛伊木马：一些隐藏在公开的程序内部，收集环境的信息，可能是由授权用户安装的，利用用户的合法的权限对数据安全进行攻击。

天窗或隐蔽通道：在合法程序内部的一段程序代码，特定的条件下如特殊的一段输入数据将启动这段程序代码，从而许可此时的攻击可以跳过系统设置的安全稽核机制进入系统，以实现对数据防范的攻击和达到窃取数据的目的。

2. 硬件的威胁

磁盘故障：在计算机运行过程中最常见的问题就是磁盘故障，它会导致重要数据的丢失。

控制器故障：控制器发生故障，会破坏数据的完整性。

电源故障：电源故障分为电源输入故障和系统内部电源故障，由于系统停电是不可预料的，因而不论处在哪种情况下都有可能使数据受到毁损。

存储器故障：介质、设备和其他备份故障。数据存储在可移动介质上以作备份，恢复工作则包括数据的复制。如果服务器出错、被毁，则存储设备或其使用的介质的任何错误

都会导致数据的丢失。

芯片和主板的故障:芯片和主板的故障会导致严重的数据毁损。

3. 人为错误的威胁

操作人员或系统用户的错误输入,应用程序的不正确使用,都可能导致系统内部的安全机制的失效,导致非法访问数据的可能,也可能导致系统拒绝提供数据服务。

4. 传输的威胁

目前的数据库应用大多是基于网络环境的。在网络系统中,无论是调用任何指令,还是任何信息的反馈均是通过网络传输实现的,因此对数据库而言,就存在着网络信息传输的威胁。

对网络上信息的监听:对于网上传输的信息,攻击者只需要在网络链路上通过物理或逻辑的手段,就能对数据进行非法的截获与监听,进而得到敏感信息。

对用户身份的仿冒:对用户身份仿冒这一常见的网络攻击方式,能对数据库的信息产生严重的威胁。对网络信息篡改的攻击者可能对网络上的信息进行截获并且对其内容增加、删除或改写,使用户无法获得准确、有用的信息或落入攻击者的陷阱。

对信息的否认:某些用户可能对自己发出或接收到的信息进行恶意的否认。

对信息进行重发:"信息重发"的攻击方式,即攻击者截获网络上的密文信息后并不将其破译,而是再次转发这些数据包,以实现其恶意的目的。

5. 物理环境的威胁

自然的或意外的事故如地震、火灾、水灾等导致硬件的破坏,进而导致数据的丢失和损坏。

1.2.3 数据库安全的定义与需求

关于数据库安全,国内外有不同的定义。国外以 C. P. Pfleeger 在"Security in Computing—Database Security PTR, 1997"中对数据库安全的定义最具有代表性,被国外许多教材、论文和培训所广泛应用。他从以下方面对数据库安全进行了描述:

(1) 物理数据库的完整性:数据库中的数据不被各种自然的或物理的问题而破坏,如电力问题或设备故障等。

(2) 逻辑数据库的完整性:对数据库结构的保护,如对其中一个字段的修改不应该破坏其他字段。

(3) 元素安全性:存储在数据库中的每个元素都是正确的。

(4) 可审计性:可以追踪存取和修改数据库元素的用户。

(5) 访问控制:确保只有授权的用户才能访问数据库,这样不同的用户被限制在不同的访问方式。

(6) 身份验证:不管是审计追踪或者是对某一数据库的访问都要经过严格的身份验证。

(7) 可用性:对授权的用户应该随时能进行应有的数据库访问。

本书在 GB 17859—1999《计算机信息系统安全保护等级划分准则》中的《中华人民共和国公共安全行业标准》GA/T 389—2002"计算机信息系统安全等级保护数据库管理系统技术要求"的基础上,给出了数据库安全更加全面的定义。

数据库安全：保证数据库信息的保密性、完整性、可用性、可控性和隐私性的理论、技术与方法。

数据库的安全需求包括以下几个方面：

（1）保密性。指保护数据库中的数据不被泄露和未授权的获取。

（2）完整性。指保护数据库中的数据不被无意或恶意地插入、破坏和删除；也指数据的正确性、一致性和相容性，即保证合法用户得到与现实世界信息语义和信息产生过程相一致的数据，包括数据库物理完整性、数据库逻辑完整性和数据库数据元素取值的准确性和正确性。

（3）可用性。指确保数据库中的数据不因人为的和自然的原因对授权用户不可用。某些运行关键业务的数据库系统应保证全天候（24×7，即每天24小时，每周7天）的可用性。

（4）可控性。指对数据操作和数据库系统事件的监控属性，也指对违背保密性、完整性、可用性的事件具有监控、记录和事后追查的属性。

（5）隐私性。指在使用基于数据库的信息系统时，保护使用主体的个人隐私（如个人属性、偏好、使用时间等）不被泄露和滥用。隐私性是与保密性和完整性密切相关的，但它涉及与使用数据相关的用户偏好、职责履行、法律遵从证明等其他保护需求，如个人不希望其消费习惯、消费偏好等被泄露，企业希望营造一个用户放心的信息环境、维护企业信誉、避免卷入法律纠纷等。

数据库的安全主要应由数据库管理系统（DataBase Management System，DBMS）来维护，但是操作系统、网络和应用程序与数据库安全的关系也是十分紧密的，因为用户要通过它们来访问数据库，况且和数据库安全密切相关的用户认证等其他技术也是通过它们来实现的。

1.3 数据库安全策略、模型与机制

1.3.1 安全策略

数据库的安全策略是指如何组织、管理、保护和处理敏感信息的原则，它包括以下方面。

1. 最小特权策略

最小特权策略是在让用户可以合法存取或修改数据库的前提下，分配最小的特权，使这些信息恰好可以满足用户的工作需求，其余的权利一律不予分配。这种策略是把信息局限在为了工作确实需要的那些人的范围内，可把信息泄露限制在最小范围内，同时数据库的完整性也能得到保证。

2. 最大共享策略

最大共享策略的目的是让用户最大限度地利用数据库信息。但这并不意味着每个人都能访问所有信息，因为它还有一个保密要求。这里只是在满足保密的前提下，实现最大限度的共享。

3. 粒度适当策略

在数据库中，将数据库中不同的项分成不同的粒度，粒度越小，能够达到的安全级别