信息安全系列教材

数据库安全

主　编　刘　晖　彭智勇
副主编　林　欣　李石君　燕彩蓉

WUHAN UNIVERSITY PRESS
武汉大学出版社

国家“十一五”863计划(2006AA12Z210)
东华大学研究生教材专项基金(2007005)

信 息 安 全 系 列 教 材

数据库安全

主 编 刘 晖 彭智勇
副主编 林 欣 李石君 燕彩蓉

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

数据库安全/刘晖,彭智勇主编;林欣,李石君,燕彩蓉副主编.—武汉:武汉大学出版社,2007.10
信息安全系列教材
ISBN 978-7-307-05866-8

Ⅰ.数… Ⅱ.①刘… ②彭… ③林… ④李… ⑤燕… Ⅲ.数据库系统—安全技术—高等学校—教材 Ⅳ.TP311.13

中国版本图书馆 CIP 数据核字(2007)第 149381 号

责任编辑:黄金文 夏炽元 责任校对:黄添生 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)
印刷:湖北新华印务有限公司
开本:787×1092 1/16 印张:28.375 字数:678 千字
版次:2007 年 10 月第 1 版 2007 年 10 月第 1 次印刷
ISBN 978-7-307-05866-8/TP·279 定价:41.00 元

信息安全系列教材

编　委　会

何明星，西华大学数学与计算机学院副院长，教授
代春艳，重庆工商大学计算机科学与信息工程学院
陈　龙，重庆邮电大学计算机科学与技术学院，副教授
杨德刚，重庆师范大学数学与计算机科学学院
黄同愿，重庆工学院计算机学院
郑智捷，云南大学软件学院信息安全系主任，教授
谢晓尧，贵州师范大学副校长，教授

华　东

徐炜民，上海大学计算机工程与科学学院，教授
楚丹琪，上海大学教务处，副教授
孙　莉，东华大学计算机科学与技术学院，副教授
李继国，河海大学计算机及信息工程学院，副教授
张福泰，南京师范大学数学与计算机科学学院，教授
王　箭，南京航空航天大学信息科学技术学院，副教授
张书奎，苏州大学计算机科学与技术学院，副教授
殷新春，杨州大学信息工程学院副院长，教授
林柏钢，福州大学数学与计算机科学学院，教授
唐向宏，杭州电子科技大学通信工程学院，教授
侯整风，合肥工业大学计算机学院计算机系主任，教授
贾小珠，青岛大学信息工程学院，教授
郑汉垣，福建龙岩学院数学与计算机科学学院副院长，高级实验师

中　南

钟　珞，武汉理工大学计算机学院院长，教授
赵俊阁，海军工程大学信息安全系，副教授
王江晴，中南民族大学计算机学院院长，教授
宋　军，中国地质大学（武汉）计算机学院
麦永浩，湖北警官学院信息技术系副主任，教授
亢保元，中南大学数学科学与计算技术学院，副教授
李章兵，湖南科技大学计算机学院信息安全系主任，副教授
唐韶华，华南理工大学计算机科学与工程学院，教授
杨　波，华南农业大学信息学院，教授

内容简介

本书比较系统全面地介绍了数据库安全的基本理论、重要模型、关键机制、解决方案、实现架构、演化历程、发展趋势和典型应用。全书从数据和数据库管理员、数据库设计人员、应用开发人员角度出发深入阐述数据安全管理、安全语义、访问控制、安全策略、多级安全DBMS、推理通道检测与控制、安全数据挖掘、隐私保护、SQL注入、数据库木马等专题，对比介绍了十几种安全数据库原型系统与产品，提供了八个典型的数据库及其应用系统安全案例。

本书共有十二章内容。首先采用软件工程方法介绍了数据库有关人员的职责任务，剖析了RDBMS的功能、组件、流程，概括了关系数据模型的特征，归纳了数据库分析设计的过程，并从三个维度考察不同数据库的联系与区别。随后，通过层级安全体系结构描述安全特征、服务、机制、API之间的关联与不同，借助多层面多形式的威胁模型刻画安全语义，说明攻击树的构造，定义攻击模式的构成。详细介绍了十几种典型的MAC、DAC、RBAC访问控制模型。在对比介绍十几种安全策略后，举例说明如何使用SQL执行安全策略与授权，涉及查询修改、递归授权、安全SQL扩展、安全策略可视化等内容。MLS/DBMS部分介绍了多级体系结构、多级关系数据模型、多实例、并发事务处理、隐蔽通道分析等问题，总结了MLS/DBMS的设计准则。推理通道检测和消除无法采用其他技术解决，本书详细介绍了典型的推理问题，检测方法和消除机制。最后，本书还用相当的篇幅介绍了数据挖掘安全、隐私保护、SQL注入、数据库木马等内容。

本书注重数据库安全问题的演化历程、发展趋势，在不同章节概括性介绍了有关研究专题的背景知识，应用驱动，发展过程，便于读者分析把握科学事物的客观规律。本书关注数据库安全问题在现实应用中的合理解决，对比性地介绍了近二十种安全数据库原型系统与产品，包括Oracle、Sybase、Informix、Teradata、Ingres等。另外，所列举的八个典型安全数据库应用系统涉及移动商务的安全事务、安全电子政务、安全工作流、安全知识管理、安全P2P、数据仓库多维访问控制与审计、医疗数据库隐私保护、安全数据中心等热门议题。

本书通俗易懂，注重知识与技术的可操作性和参考价值，可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书，特别可用做信息安全、计算机及其他信息学科本科生高年级或硕士研究生的教材。同时，也可以用做计算机信息安全职业培训的教材。

序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前 言

你可能非常精通数据库，但是，你不一定了解数据库安全。

数据库安全包括数据库系统安全和数据库应用系统安全。由于人们倾向于使用数据库系统管理各种数据构造应用程序，数据库安全问题非常普遍。在处理有关安全问题时，人们或者把解决方案聚焦在数据库系统，或者把防护机制归结在应用代码，这些都是失之偏颇的。实际上，数据库系统无法解决全部数据库安全问题，应用系统也必须借助数据库系统简化安全方案。

数据库安全的内容一直在不断发展变化。在数据库系统产品问世的初期，人们主要考虑访问控制。而现在，人们更加关心通过推理通道，借助数据挖掘，依靠网络攻击，利用木马病毒等方式窃取机密。隐私保护问题也引起社会不同人士越来越多的关注。与此同时，随着数据库技术的扩展、计算机网络通信技术的更替、组织机构的虚拟化协同运作，传统的数据库安全问题也发生了深刻变化，需要增强可配置性、移动性、伸缩性、适应性、移植性、协商性。前沿的数据库应用系统也相继对数据品质、数据完整性、数据资产版权、数据库可存活性提出了更高的要求。

虽然人们对于数据库安全问题的研究与应用从来没有停止过，但是，国内外相关的书籍却并不多。以往的有关书籍或多或少具有这样一些特点：专注于某种数据库产品的安全机制；忽略数据库系统以外的安全方案；将数据库安全作为数据库的一个高级专题简单介绍；没有涉及数据库安全的最新发展。这种状况不利于人们学习掌握、研究应用数据库安全的有关原理与技术。有幸的是，Bhavani Thuraisingham 于 2005 年 5 月出版了 *Database and Application Security* 一书，被国外同行誉为“有关数据安全最为权威的一本书”。本书在借鉴该书总体构思的基础上，遴选了大量权威研究应用成果。

本书共十二章，除第一章绪论外，其余章节围绕数据库安全问题的不同方面展开。主要选取了数据管理、安全语义、访问控制、安全策略、多级安全数据库管理系统、MLS/DBMS 原型系统和产品、推理通道检测与控制、数据挖掘及其安全、隐私保护、安全数据库应用系统、SQL 注入攻击与防范、数据库木马等专题。

数据管理专题总结归纳了数据库及其应用系统的一些基本原理、模型、机制、术语、发展趋势等内容，提供数据管理方面的背景知识。安全语义专题从信息安全的语义出发阐述数据库安全丰富、多学科、多层次的语义，在深入介绍数据库安全各种技术细节内容之前，建立起一个系统化、完整、正反互补的安全图景。访问控制专题深入详细地介绍了十几种典型的强制访问控制、自主访问控制、角色访问控制模型。模型采用了严格的形式化方法说明，文字描述部分可以降低理解难度和理解歧义。安全策略专题从安全策略及其执行机制，安全策略可视化角度揭示数据库安全问题，对于数据库应用系统的研发至关重要。

多级安全数据库管理系统专题深入说明了 MLS/DBMS 所遵循的规范标准，所依据的数

学基础，设计与实现过程中的主要问题。MLS/DBMS 原型系统和产品专题介绍了 MLS/DBMS 发展历程中具有影响的原型系统和商业产品，在总结各自特性的同时，从多种角度对比了它们在设计理念、实现方式的异同。推理控制专题介绍了推理通道的典型形式、定义与描述、检测与消除算法、分布式系统结构。数据挖掘及其安全问题专题在简要介绍数据挖掘知识基础上探讨了数据挖掘对于信息安全的积极促进作用，随后着重论述了如何有效防止通过数据挖掘获取敏感知识。数据库隐私专题探讨了隐私与数据库隐私保护的话题。

安全数据库应用系统专题收集了八个具有代表性的数据库应用系统，重点说明了这些应用系统对数据库安全问题的考量和解决。这些数据库应用系统具有代表性，也是目前主要的发展趋势。数据库安全其他问题专题重点介绍了 SQL 注入攻击与防范以及数据库木马。

本书由东华大学、武汉大学、西安交通大学的专家学者合作完成。各专题配有思考题，适合中高级数据库、信息安全从业人员参考使用。本书按照本科生高年级专业教材形式编写，也可以作为研究生专业教材使用。其中，全书的选题和大纲由刘晖(东华大学)、彭智勇(武汉大学)提出。第一章、第三章、第八章、第十一章由刘晖编写。第二章、第十二章由林欣(东华大学)编写。第四章由彭智勇、任毅(武汉大学)编写。第五章由李石君(武汉大学)、林欣（东华大学）编写。第六章由李石君、韦俊银(东华大学)编写。第七章由刘晖、朱爱玲(东华大学)编写。第九章、第十章由燕彩蓉(西安交通大学)编写。全书由刘晖、彭智勇负责统稿审定。

本书的研究和编写工作受到武汉大学承担的国家“十一五”863 计划《空间数据水印技术及其服务体系的研究与开发》(编号：2006AA12Z210)以及东华大学研究生教材专项基金（2007005）的资助。

在本书组织编写的过程中，受到武汉大学张焕国教授，东华大学王以刚教授、乐嘉锦教授、孙莉教授，武汉大学出版社黄金文编辑的热情帮助。在此谨向他们表示衷心的感谢。

由于时间和水平有限，难免出错，恳请读者批评指正，使本书得以改进和完善。

作　者

2007 年 7 月 26 日于上海

信息安全系列教材书目

密码学引论（普通高等教育“十一五”国家级规划教材）	张焕国等
计算机网络管理实用教程	张沪寅等
网络安全	黄传河等
信息安全综合实验教程	张焕国等
信息隐藏技术实验教程	王丽娜等
信息隐藏技术与应用	王丽娜等
网络多媒体信息安全保密技术	王丽娜等
信息安全法教程	麦永浩等
计算机病毒分析与对抗	傅建明等
网络程序设计	郭学理等
操作系统安全	贾春福等
模式识别	钟　珞等
密码学教程	张福泰等
信息安全数学基础	李继国等
计算机取证技术	陈　龙等
电子商务信息安全技术	代春艳等
信息安全基础	武金木等
网络伦理	徐云峰
网络安全	丁建立等
数据库安全	刘　晖等

目 录