



信息安全国家重点实验室

信息安全丛书

Database Security

数据库安全

张敏 徐震 冯登国 编著



科学出版社

www.sciencep.com

信息安全国家重点实验室信息安全丛书

数据库安全

张敏 徐震 冯登国 编著

国家重点基础研究发展规划项目(项目编号:G1999055800)

国家杰出青年科学基金资助项目(项目编号:60025205)

科学出版社

北京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。本书是在作者长期从事数据库安全科研和开发工作的基础上撰写而成。本书的内容主要包括三个方面:首先是基本概念、原理的介绍,包括信息安全和数据库安全的概念、背景知识和安全模型;其次对数据库安全技术进行了全面的介绍,包括多级安全数据库的基本原理、典型原型、实现方法,新型数据库安全等;第三还对国内外数据库安全相关的评估和技术标准进行了介绍,包括 TCSEC、TDI、ITSEC、GB17859-1999、GA/T389 等。

本书可作为计算机、信息安全、信息管理系统等专业的本科生、研究生的参考书,也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

数据库安全/张敏,徐震,冯登国编著. —北京:科学出版社,2005

(信息安全国家重点实验室信息安全丛书/冯登国主编)

ISBN 7-03-015469-X

I. 数… II. ①张…②徐…③冯… III. 数据库系统-安全技术
N. TP311.13

中国版本图书馆 CIP 数据核字(2005)第 044004 号

责任编辑:鞠丽娜 刘亚军/责任校树:耿 耘

责任印制:吕春珉/封面设计:王 浩

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005年7月第一版 开本:B5(720×1000)

2005年7月第一次印刷 印张:15 1/2

印数:1 4 000 字数:295 000

定价:25.00元

(如有印装质量问题,我社负责调换<环伟>)

销售部电话:010-62136131 编辑部电话 010-62138978-8002(B106)

《信息安全国家重点实验室信息安全丛书》编委会

顾 问 蔡吉人 何德全 林永年 沈昌祥 周仲义

主 编 冯登国

编 委 (按姓氏拼音字母排序)

陈宝馨	陈克非	戴宗铎	杜 虹	方滨兴
冯克勤	郭宝安	何良生	黄民强	荆继武
李大兴	林东岱	刘木兰	吕诚昭	吕述望
宁家骏	裴定一	卿斯汉	曲成义	王煦法
王育民	肖国镇	杨义先	赵战生	张焕国

序 言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破,形成了巨大的新型生产力。数字化的生活方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地,也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务的各种信息化应用之花,在华夏沃土上竞相开放,炎黄子孙们,在经历了几百年的苦难历程后,在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握,非一朝一夕之功。治水、训火、利用核能都曾经经历了非常漫长的岁月。不掌握好科学技术造福人类的一面,就会不经意地释放出它危害人类的一面。

生产力的发展,为社会创造出许多新的使用价值。但是,工具的不完善,会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样,由于人类认识真理和实践真理的客观局限性而存在许多不完善的地方,从而形成信息系统的漏洞,造成系统的脆弱性,在人们驾驭技能不足的情况下损害着人们自身的利益。

世界未到大同时,社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力,在信息空间也同样存在。在这个空间频频发生的和被有些人利用系统存在的脆弱性运用其“暴智”来散布计算机病毒,制造拒绝服务的事端,甚至侵入他人的系统,盗窃资源、资产,以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展,信息安全成为全社会的需求,信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定,也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现,取决于信息安全是否得以保障。什么是信息安全?怎样才能保障信息安全?这些问题都是严肃的科学和技术问题。面对人机结合和非线性、智能化的复杂信息巨系统,我们还有许多科学技术问题需要认真研究。我们不能在研究尚处肤浅的时候,就盲目乐观地向世人宣称,我们拥有了全面的解决方案;我们也不能因为面对各种麻烦,就灰头土脸,自暴自弃,我们需要的是革命的乐观主义精神、坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的,今天对信息安全的认识,就经历了一个从保密到保护,又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的,它涉及人、社会和技术等因素,因此,仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看,只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段,才能取得良好的效果。

为了推动我国信息化发展的进程,信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中,我们既注重学术水平,又注意其实用价值。本丛书从信息安全保障体系、操作系统安全、数据库安全、网络安全、无线网络安全、网络攻击、密码技术、PKI 技术、信息隐藏、安全协议、安全事件应急响应、量子密码通信等多个角度,分析和总结信息安全的科学问题以及信息安全保障的理论与技术,因此,这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中,以使读者阅读本丛书后在理论、方法、技术上得到新的启发和收获,从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的,今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言,它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力,不断地深化自己的研究,借鉴国外先进的科学技术,结合国情,与时俱进地推出信息安全保障的新理论、新办法和新手段,用我们的智慧保卫我们的信息疆土,使我们的信息家园尽量祥和安宁。

限于作者的水平,本丛书难免存在不足之处,敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003年7月

前 言

信息技术经过多年的发展,已经彻底改变了我们的生活方式。在我们越来越依赖于信息技术的同时,信息安全问题也日益突出。由于信息是当今人类社会的重要战略资源,因此必然要面对越来越多的安全威胁。数据库系统是信息存储和处理的核心环节,它的安全性在整个信息安全体系结构中占据关键位置。数据库系统是当前网络和信息系统的基础平台,也是当今世界最为复杂的应用系统之一。因此解决数据库安全问题是目前最为紧迫的挑战之一。

本书的作者长期从事与数据库安全相关的科研和开发工作,具有坚实的理论基础和丰富的实践经验,为本书的编写奠定了基础。截至目前,国内已经出版了大量信息安全方面的教材和著作,然而其中关于数据库安全方面的却非常零散、不全面,而仅有的少数介绍数据库安全的教材和著作,由于出版日期较早而缺乏最新的研究和开发实践方面的内容。本书不仅吸收了国内外相关论文和著作(已在参考文献中列出)的很多精华,而且有专门的章节介绍作者在相关领域的实际工作,尽量做到理论和实践相结合。

全书分为8章。第1章是绪论,主要介绍信息安全和数据库安全的背景和基本概念;第2章介绍系统安全的核心理论和当前重要的安全模型;第3章至第5章全面介绍多级安全数据库的理论和相关技术,其中第3章给出多级安全数据库的基础知识,包括体系结构、事务处理等,第4章介绍 Seaview 和 Lock Data Views 两个典型的多级安全数据库系统原型,第5章主要介绍多级安全数据库中的推理分析和隐通道技术;第6章介绍一些新型数据库的安全技术和数据库加密技术;第7章介绍国内外与数据库安全相关的评估和技术标准,包括 TCSEC、TDI、ITSEC、GB17859-1999、GA/T389 等;第8章是安全数据库系统设计与实现,介绍作者在信息安全国家重点实验室开发的 LOIS 安全数据库系统的设计,概述了当前主流数据库的安全机制。

本书的编写得到了王宏、李斓、何永忠、雷浩、吕双双、李晓峰、王新刚等几位博士的大力协助。没有他们的鼎力相助,本书的编写和统稿不会如此顺利,在此对他们表示衷心感谢。

本书在写作过程中得到了科学出版社的大力支持以及国家重点基础研究发展规划项目(项目编号:G1999055800)和国家杰出青年科学基金项目(项目编号:60025205)的资助,在此深表谢意。

由于数据库安全技术发展速度快、涉及面广,作者虽然竭尽全力,错误和不足仍在所难免,欢迎读者批评、指正。

目 录

第 1 章 绪论	1
1.1 信息技术与数据库技术	1
1.1.1 信息技术的发展	1
1.1.2 数据库技术的发展	3
1.2 信息安全概述	5
1.2.1 信息安全的必要性	5
1.2.2 信息安全的基本概念	6
1.2.3 安全机制	10
1.2.4 信息安全标准	12
1.3 数据库安全问题.....	13
1.3.1 数据库安全威胁	14
1.3.2 数据库安全需求	15
1.3.3 数据库安全与操作系统安全的关系.....	17
1.4 数据库安全研究的发展.....	19
1.4.1 数据库安全研究的阶段划分	20
1.4.2 萌芽时期	20
1.4.3 初始时期	22
1.4.4 标准化时期	23
1.4.5 多样化时期	24
1.4.6 国内安全数据库的研究和开发工作.....	26
1.5 小结.....	27
第 2 章 安全模型	28
2.1 安全模型概述.....	28
2.2 访问控制矩阵模型.....	29
2.2.1 基本概念	30
2.2.2 访问控制矩阵的基本操作	30
2.2.3 授权管理	32
2.3 取子模型.....	33
2.3.1 基本概念	33
2.3.2 授权管理	33

2.4	动作实体模型	35
2.4.1	基本概念	35
2.4.2	一致性规则	36
2.4.3	传递规则	37
2.4.4	静态图和动态图的互一致性规则	38
2.5	Wood 模型	38
2.5.1	数据库的三级模式	38
2.5.2	基本概念	39
2.5.3	概念级的存取规则	40
2.5.4	外部级的存取规则	40
2.5.5	存取控制流程	41
2.6	Bell-La Padula 模型	41
2.6.1	基本概念	41
2.6.2	基本操作	42
2.6.3	模型公理	42
2.7	BIBA 模型	43
2.7.1	基本概念	43
2.7.2	模型公理	44
2.8	Dion 模型	45
2.8.1	基本概念	45
2.8.2	模型公理	46
2.9	流控制的格模型	47
2.9.1	基本概念	48
2.9.2	格结构的派生	48
2.9.3	隐式数据流和显式数据流	49
2.10	基于角色的访问控制模型	50
2.10.1	RBAC 的历史	50
2.10.2	NIST 的 RBAC 标准	51
2.10.3	RBAC 管理	54
2.10.4	RBAC 约束	55
2.10.5	RBAC 应用	56
2.11	Clark-Wilson 模型	57
2.11.1	基本概念	57
2.11.2	安全策略	57
2.12	多策略模型	58

2.13	Smith-Winslett 模型	60
2.13.1	基本概念	60
2.13.2	安全策略	60
2.13.3	多级关系的访问	61
第 3 章	多级安全数据库基础	64
3.1	多级数据库管理系统体系结构	64
3.1.1	体系结构分类	65
3.1.2	高级运行结构	66
3.1.3	可信主体结构	66
3.1.4	TCB 子集类体系结构	67
3.1.5	完整性锁结构	70
3.2	多级关系数据模型	72
3.2.1	传统关系模型	73
3.2.2	多级关系模型	73
3.3	多级安全数据库事务并发处理	82
3.3.1	传统事务模型与可串行化理论	83
3.3.2	多级并发处理问题分析	87
3.3.3	多级数据库管理系统并发控制机制	90
3.3.4	多级事务	96
第 4 章	多级安全数据库范例	99
4.1	SeaView	99
4.1.1	项目简介	99
4.1.2	系统结构	99
4.1.3	主要实现技术	101
4.2	Lock Data Views	108
4.2.1	项目简介	108
4.2.2	系统结构	108
4.2.3	主要实现技术	109
第 5 章	推理分析与隐通道分析	114
5.1	多级安全数据库中的推理分析	114
5.1.1	推理分析问题	114
5.1.2	推理分析安全	116
5.1.3	推理通道的识别及消除	119
5.2	隐通道分析	121
5.2.1	基本概念	122

5.2.2	隐通道分析的准备	126
5.2.3	识别隐通道的方法	132
5.2.4	评估隐通道的带宽	137
5.2.5	隐通道处理措施	139
第6章	新型数据库系统安全及数据库加密技术	140
6.1	面向对象数据库安全技术	140
6.1.1	面向对象数据库的定义和组成	140
6.1.2	面向对象数据库的数据模型	140
6.1.3	面向对象数据库的主要安全问题	141
6.1.4	面向对象数据库的安全模型和机制	141
6.1.5	小结	146
6.2	数据仓库安全技术	146
6.2.1	数据仓库技术概述	146
6.2.2	数据组织与关键技术	148
6.2.3	安全问题	149
6.2.4	安全措施	149
6.2.5	小结	151
6.3	XML 安全技术	151
6.3.1	XML 加密	152
6.3.2	XML 签名	152
6.3.3	XML 密钥管理规范	152
6.3.4	可扩展访问控制标记语言	153
6.3.5	安全判断提示标记语言	153
6.3.6	XML 访问控制研究	153
6.3.7	XML 数据库及其安全	156
6.4	统计数据库安全技术	156
6.4.1	基本概念	157
6.4.2	统计数据库面临的安全问题	157
6.4.3	防推导技术	159
6.4.4	小结	163
6.5	数据库加密技术	163
6.5.1	数据库加密技术概述	163
6.5.2	数据库加密基本要求	164
6.5.3	数据库加密实现分类	164
6.5.4	关键影响因素	166

6.5.5 局限性	169
第7章 数据库安全评估标准	170
7.1 安全评估标准	170
7.1.1 可信计算机系统评估准则	171
7.1.2 信息技术安全评估准则	174
7.1.3 IT 安全评估的国际准则	176
7.1.4 我国信息安全测评标准	181
7.2 可信数据库管理系统解释	185
7.2.1 TDI 的评估意义	186
7.2.2 TDI 的组成部分	186
7.2.3 TDI 的主要内容	187
7.3 数据库管理系统的保护轮廓	191
7.3.1 DBMS.PP 安全环境及目标	192
7.3.2 DBMS.PP 安全要求	193
7.4 我国数据库管理系统安全评估准则	194
第8章 安全数据库系统设计与实现	196
8.1 信息安全系统开发过程	197
8.1.1 初始分析	198
8.1.2 安全需求分析	199
8.1.3 系统设计	202
8.1.4 编码实现	206
8.1.5 验证和测试	206
8.1.6 形式化方法的应用	207
8.2 LOIS 安全数据库系统	208
8.2.1 Postgre SQL 简介	208
8.2.2 需求分析	213
8.2.3 概要设计	214
8.2.4 详细设计概述	220
8.3 商业数据库安全机制简介	225
8.3.1 Oracle	225
8.3.2 Sybase	229
8.3.3 Informix	232
主要参考文献	233

第 1 章 绪 论

信息技术从 20 世纪 40 年代开始萌芽,经过不断的发展,而今已经彻底改变了人类的生活方式。信息是当今人类社会的重要战略资源,它必然要面对各种各样的安全威胁。在我们越来越依赖于信息技术的同时,信息安全的问题也日益突出。信息安全技术主要研究如何对抗信息安全威胁、保护信息资源。目前,它已成为信息技术的关键组成部分。在信息爆炸的今天,我们绝大多数的信息存储和大量的信息处理都依赖于数据库系统,所以数据库安全对于信息的安全有着至关重要的影响。由于数据库技术应用的普遍性、数据库系统的复杂性、数据及其处理的丰富语义,许多研究者对数据库安全理论和技术进行了广泛而深入的研究,并且该方向仍然是当前的热点之一。

1.1 信息技术与数据库技术

以信息技术为代表的新技术革命对人类社会的发展进程产生了重大影响,信息技术本身也取得了长足的进步。对于信息技术目前还没有一个十分统一的定义,一般认为,信息技术就是获取、处理、传递、储存、使用信息的技术。但从广义上讲,凡是与上述诸方面相关的技术都可以叫做信息技术,一般可分为四类,即感测技术、通信技术、计算机技术和控制技术。所谓感测技术,是指对信息的传感、采集技术;通信技术是传递信息的技术;计算机技术是处理、存储信息的技术;控制技术则是使用与反馈信息的技术。数据库技术是计算机技术的关键组成部分,是信息技术的基础支撑平台之一。历经多年发展,数据库技术已经取得了丰硕的成果,并且随着应用和基础技术的发展在迅速进步。

1.1.1 信息技术的发展

信息技术自诞生以来已逐步显示出其对科技、社会、经济发展的巨大推动力。各国政府认识到其重大作用后纷纷投入力量推动信息技术的发展。美国政府从 20 世纪 50 年代开始就重视对科技和信息加工的投入。第二次世界大战结束后,美国政府通过国家科学基金会重点资助和扶持了对国家的科技进步有重要意义的基础学科以及与政府近期发展目标有关的信息产品和服务,为后来信息产业的发展奠定了坚实的基础。目前,美国是世界上最大的信息产品输出国,其信息技术的使用也是最为普遍的。英国、德国、法国、日本等国家正在努力发展本国的信息产业,

我国也在全力推动信息产业的发展。

1. 美、英、日等国的信息化工作

1993年2月克林顿以国情咨文的形式提出在美国建设信息高速公路的计划,引起了世界各国的强烈反响。信息高速公路是国家信息基础设施的形象比喻,它是现代通信技术和计算机技术融为一体的全国范围内的高速计算机通信网。这一信息网将融合美国现有的各类计算机网络、电话和有线电视网,成为教育、卫生、娱乐、商业、金融等诸多服务的信息载体。为了实施该项庞大的系统工程,美国政府计划投资数百亿美元,兴建覆盖全国的光纤信息网。预计整个网络建成将耗资4000亿美元,历时20年左右。

1995年2月25日西方七国召开了部长会议讨论全球信息化(GII),掀起了信息化与兴建“信息高速公路”的热潮。英国计划在10年内拨资380亿英镑建设信息高速公路。1994年2月英国电信局宣布准备投资100亿英镑在全国建立一个光纤通信网络,向人们提供新闻、商业、金融、教育和娱乐等方面的服务。英国政府还打算建立120个全新的数字化电视台,为今后发展多媒体服务系统奠定基础。德国电信局正在大力建设传输能力为155Mb/s的宽带综合服务数据网,在该网络上,所有的多媒体信息都可以传输。现在德国已建成世界上第一流的通信基础设施,铺设光缆8万公里,连接1460万户家庭。1994年法国政府提出了面向未来的信息计划。该计划要求把现有电话线路同光纤网络连接起来,形成全国范围内的光纤通信网。法国电信公司将每年为该项目投资2000万~2500万法郎。日本政府从1993年开始进行“全国超高速信息网”的建设。该计划拟于2015年将光纤送到日本的每个企业和家庭,总投资约45万亿日元。

到21世纪初期,各发达国家的信息基础设施已经颇具规模,各国的焦点从信息基础设施建设转入关键信息应用,包括电子商务、电子政务等。电子商务的主要推动力来自于商业界,其成功案例不胜枚举,如Amazon, ebay等,而电子政务的推动力来自于各国政府。

为了推动美国电子政务,美国白宫管理与预算办公室在2001年7月18日宣布成立“电子政务特别工作小组”。该特别小组由来自46个政府机构的成员组成,于2001年8月9日正式开始工作。2001年10月3日,总统管理委员会讨论并通过了该小组围绕“为取得电子政务的战略性进展应采取的重点行动”提出的建议。随后,各机构的项目小组会同白宫管理与预算办公室制定了电子政务计划实施框架,并将其列入2003年财务预算。

2000年9月,英国首相布莱尔发起了“英国在线运动”,其内容是让英国人民、企业和政府上网。这项运动有三个主要目标:使英国成为世界上开展电子商务最好的地方;保证在任何地方都能够使用因特网;从网上就可以获得政府的各种服务。

2. 我国信息化的进程

邓小平同志早在1984年就指出：“开发信息资源，服务四化建设”。在世界许多发达国家相继提出自己面向未来的信息计划，加速社会信息化进程的今天，我国既面临着严峻的挑战，又有着不可多得的大好机遇。为此，必须清醒地认识信息社会发展规律，抓住有利时机推动我国社会的信息化进程。1997年4月，国务院在深圳召开了第一次全国信息化工作会议。会议确定了“统筹规划、国家主导、统一标准、联合建设、互联互通、资源共享”的我国信息化建设指导方针。1998年，国务院进行机构改革，在原邮电部、电子工业部的基础上新设信息产业部，负责统筹规划我国的信息化建设、对国家信息产业进行归口管理。

20世纪80年代以来，我国信息产业得到了快速的发展，到2002年，已经占到GDP的5.7%，成为国家重要的支柱产业。经过十几年的发展，我国已经建成了由固定和移动、地面和空间互补、覆盖全国、通达世界的数字化的工业电信网，网络规模居世界首位。截至2003年6月底，电话用户的总数达到4.72亿，9月底超过了5亿。固定和移动平分秋色。互联网达到了6800万用户，联网的计算机达到2570万台，国内的电视机拥有量达到3亿台，其中有有线电视用户达到1亿户。金税工程已经覆盖了80%的纳税企业，电子货币和金融电子化发展的步伐明显的加快，已经实现了各类银行卡在100个大中城市跨行联网通用。四大商业银行在本系统的300多个城市实现了银行卡联网运行和跨地区使用。电子政务建设得到大力推动，特别是在许多城市开展了网上联合审批、网上招标、政府采购、市民综合服务窗口、网上教育培训、网上社会保障、市长邮箱等，对公众的服务信息系统越来越多，深受企业和居民的欢迎。电子政务建设不仅增强了政府的经济调节、市场监管的能力，提高了政府的工作效率，而且还大大提高了政府社会管理和公共服务的能力，提高了政府工作的透明度，促进了政府职能的转变。

1.1.2 数据库技术的发展

数据库技术经过近40年的研究和发展取得了丰硕的成果。数据库应用是数据库技术的发展动力，随着数据库应用领域的扩展，不断有新的数据模型产生，应用对数据库系统的性能、可靠性和安全性的要求也越来越高，正是这些需求在不断地推动数据库技术的发展。数据库管理系统(DBMS)开发技术为数据库技术的发展提供了技术上的支撑，而数据模型是数据库系统的核心和基础，一般对数据库的发展阶段的划分都以它作为主要依据和标志。我们可以将数据库技术的发展大致分为3个阶段。

1. 早期数据库技术

一般将 20 世纪 60 年代后期开始研究、开发的层次数据库系统和网状数据库系统称作第一代数据库。它们分别采用层次和网状数据库模型,实际上层次模型是网状模型的特例。它们具有类似的体系结构、数据库语言 and 数据库存储管理。IBM 公司的 IMS 是比较典型的层次数据库,而美国数据库系统语言协商会(CODASYL)在 DBTG 系列报告中提出了网状模型,在它的思想指引下开发了很多商品化的数据库。这个阶段数据库系统支持三级模式的体系结构,即外模式、概念模式和内模式,具有物理独立性和一定程度的逻辑独立性。虽然在这个阶段有了独立的数据定义语言,但是数据操纵语言需要指定如何访问数据,需要应用程序根据数据库的逻辑模式和物理模式选择存取路径,这样用户使用不便,并且数据独立性和应用程序的一致性都比较差。

2. 关系数据库

20 世纪 70 年代初 IBM 公司 San Jose 实验室的研究员 E. F. Codd 发表了题为“A Relational Model of Data for Large Shared Data Banks”的文章。文中提出了数据库的关系模型,开创了关系数据库理论研究并为关系数据库技术奠定了理论基础。20 世纪 70 年代是关系数据库理论研究和原型开发的时代,在这个阶段 IBM 公司 San Jose 实验室开发的 System R 和 Berkeley 大学开发的 INGRES 是典型的代表。取得的成果主要包括三个方面:奠定了关系模型的理论基础,对关系语言(关系代数、关系演算、SQL 语言和 QBE 等)的研究为 80 年代的数据库语言标准化奠定了基础;在关系数据库管理系统(RDBMS)原型的开发过程中攻克了系统实现中的查询优化、并发控制、故障恢复等一系列关键技术难题。

关系模型建立在严格的数学基础上,概念简单、清晰,易于理解和使用,所以得到了广泛的支持。20 世纪 70 年代末以来涌现了大量优秀的关系数据库产品,如 DB2、ORACLE、INGRES、INFORMIX、SYBASE 等。直到目前关系数据库仍然是应用的主流。当然,在 30 多年的发展过程中,RDBMS 的运行环境发生了巨大的变化。目前,关系数据库的理论和实现技术的研究已经非常透彻,本书中假定读者已经具备这方面的基础知识。

3. 新一代数据库

上述几种数据库对于管理结构简单、操作简单、完全格式化和结构化的数据是非常成功的,这一点可以从它们在传统商务和管理的事务性应用领域的普遍应用得到验证。然而,当今数据库的数据模型日渐丰富,应用领域愈加广泛,新的计算技术层出不穷,数据库技术也向着多个方向迅速发展。

首先,从20世纪80年代以来,关系模型已无法满足新领域的数据库建模需求,人们提出并发展了许多新的数据模型。这些数据模型包括函数数据模型(FDM)、语义数据模型(SDM)、E-R模型、面向对象模型等。其中,比较有影响的数据模型是面向对象模型,基于面向对象模型的数据库称为面向对象数据库,但它还是一种新兴技术远不如关系数据库成熟。

其次,数据库系统在传统商业中的成功很大程度上刺激了数据库系统在其他领域中的应用。这些领域包括CAD/CAM、地理信息系统、知识系统、实时系统等。在这些新的领域,数据库技术需要面对大量的全新需求,包括强有力的数据库建模能力;强有力的数据存储和共享能力;现代事务管理(嵌套事务、协作事务等);时间认知能力;触发器或主动能力等。在强大的需求推动下涌现出了一大批新型数据库,如时态数据库、实时数据库、工程数据库和超媒体数据库等,并且随着应用需求的发展还会有新型的数据库出现。

此外,计算机技术的发展也在推动数据库技术的进步。网络技术的发展导致了分布式数据库的产生,并行技术与数据库结合创造了并行数据库。总的来说,现在已经不能简单地用数据模型作为标准来定义新一代的数据库,数据库已经进入了多样化的时代。

1.2 信息安全概述

信息技术的飞速发展使其影响已深入到现代社会的各个领域。如今信息技术已经成为无时不在、无处不有、无所不用的工具,人类已经进入信息社会。人类社会的经济、政治、军事、文化、教育、科技和其他社会活动越来越强烈地依赖信息资源和信息共享。信息像其他重要的商务资产一样也是一种资产,对一个组织而言具有价值,需要妥善保护。然而信息共享在为人们带来利益、价值和方便的同时,也带来了巨大的风险和隐患,暗藏着极大的危险性甚至毁灭性。这就引发了信息社会最敏感、最具挑战性的核心问题之一——信息安全问题。从某种程度上讲,信息资源共享与信息安全是一对矛盾。目前,信息安全已经成为信息时代的关键和重点。

1.2.1 信息安全的必要性

当今的信息系统日益复杂,其中必然存在系统设计、实现、内部控制等方面的弱点。脆弱性指的是可能被用来侵害系统或系统内信息的任何弱点。系统具有脆弱性就意味着信息资产需要面对各种各样的安全威胁。如果没有采取适当的措施应对系统运行环境中的安全威胁,信息资产可能会遭受巨大的损失。

1988年11月2日,美国康奈尔大学的学生释放了一个蠕虫病毒,造成Internet上近6000台主机瘫痪,经济损失高达几千万美元。美国政府因此立即做出反