刘启原 刘 怡 编著

数据库与信息系统的安全

数据库丛书

科学出版社

数据库丛书

数据库与信息系统的安全

刘启原　刘　怡　编著

科学出版社

2000

内 容 简 介

在现代信息系统中，安全问题已经上升到了一个非常重要的地位，而系统安全、数据库安全，以及网络安全等问题已经融合成为一系列不可分割的问题。本书系统地介绍了信息系统安全问题的概念、原理、典型的技术方法以及成熟而有影响的涉及安全的产品。本书共分十一章，第一、二章是引言及安全问题的概述，第三章介绍安全问题的理论基础——安全模型；第四章介绍安全的标准；第五章介绍安全数据库设计中所考虑的问题；第六、七章介绍安全系统实践中特别重要的密码学和攻击检测两个问题；第八章简单讨论了数据仓库的安全问题；第九章到第十一章研究的是网络安全、Java安全以及病毒对抗等问题。为了使读者更全面地掌握有关的内容，本书附录部分介绍了较多的各方面的材料。

本书可供信息系统的策划者和设计者参考，也可作为高等院校信息系统相关专业的教学参考书。

图书在版编目(CIP)数据

数据库与信息系统的安全/刘启原 编著. -北京：科学出版社，2000
（数据库丛书）
ISBN 7-03-007765-2

Ⅰ.数… Ⅱ.刘… Ⅲ.①数据库系统-安全技术②信息系统-安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(1999)第 30856 号

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717

新蕾印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

2000年1月第一版 开本：787×1092 1/16
2000年1月第一次印刷 印张：21
印数：1—3 000 字数：477 000

定价：32.00元

（如有印装质量问题，我社负责调换〈兰各〉）

《数据库丛书》是我国数据库专家学者团结协作，合力撰写的一套系列著作。它比较全面地反映了国际数据库技术的丰富内容与最新发展，和我国数据库科技工作者多年来的主要研究成果，具有较高的理论水平和学术价值。

数据库是计算机科学技术中发展最快的领域之一，也是应用最广的技术之一。是计算机信息系统与应用系统的核心基础。相信《数据库丛书》的编撰出版，必将有益于推动我国数据库技术的研究与发展，促进我国数据库技术的普及与提高，加快数据库应用的推广与深入，为我国社会经济信息化作出贡献。

张效祥

九六年六月

《数据库丛书》编委会

序

数据库是计算机领域发展最快的学科之一，因为它既是一门非常实用的技术，也是一门涉及面广、研究范围宽的学科。因此，它吸引了理论研究、系统研制和应用开发等不同方面众多的学者、专家和技术人才致力于其研究和实践。

数据库系统所管理、存储的数据是各个部门宝贵的信息资源。在信息化时代来临、Internet高速发展的今天，信息资源的经济价值和社会价值越来越明显。建设以数据库为核心的信息系统和应用系统，对于提高企业的效益、改善部门的管理、改进人们的生活均具有实实在在的意义。正因为数据库技术与经济、社会的发展和信息化建设有着密切的关系，这门学科才获得了巨大的源动力和深厚的应用基础。

数据库系统已从第一代网状、层次数据库系统发展到第二代关系数据库系统和第三代以面向对象为主要特征的数据库系统。数据库技术与网络通信技术、面向对象技术、并行计算技术、多媒体技术、人工智能技术等互相渗透，互相结合，成为当前数据库技术发展的主要特征。它使数据库领域中新的技术内容层出不穷，新的学科分支不断涌现，形成了新一代数据库系统的大家族。与传统的数据库相比，当今数据库的整体概念、技术内容、应用领域，甚至某些原理都有了重大的发展和变化。

面对如此丰富的学术内容和技术方法，如此广阔的研究方向和应用领域，从事数据库研究、开发和应用的科技人员，攻读数据库方向的研究生都迫切希望有一套丛书能系统而全面地介绍数据库学科的多个分支和相关领域。

《数据库丛书》的编写宗旨是把当前数据库学科各个分支的最新学术成果介绍给读者，以促进国内的学术研究；同时，又介绍数据库技术的发展过程，各分支之间的内在联系及在数据库大家族中的位置，以促进数据库和计算机科学的其它领域技术的结合。

本丛书由各分册组成，包括《数据库进展》、《分布式数据库》、《分布式数据库管理系统实现技术》、《并行关系数据库管理系统引论》、《数据仓库技术与联机分析处理》、《知识库系统》、《特种数据库技术》等。本丛书的每一分册涉及数据库学科的一个或几个分支。其中《数据库进展》则与其他分册有所不同，是本丛书的总纲、指南和补充，是给本丛书穿针引线、铺垫基础，从而使丛书成为一个各部分既相互独立又相互联系的整体。

《数据库丛书》是开放的，故丛书的分册将随着数据库学科的发展而不断补充。

本丛书各分册的主编和作者，多是长期从事数据库各分支领域研究工作的专家、学者。他们学术造诣高深，实践经验丰富，书中许多内容是他们长期研究的成果。本丛书不仅反映了国际数据库技术的最新成果和发展方向，也展示了我国数据库工作者的学术成果和研究深度，具有较高的理论水平和学术价值。它的出版是我国数据库学术界的一件大喜事。我向本丛书的所有作者和编委的辛勤工作表示崇高的敬意。

萨师煊

1998年1月

前　言

社会的信息化进程在90年代呈现出飞速发展的势头，构成了人类社会90年代的独特风景线。90年代以来，我国信息产业蓬勃发展。90年代中期，国家制定了以"三金"工程("金桥工程"、"金税工程"、"金卡工程")为代表的信息工程战略规划。此外，正在建立的国家宏观决策支持网络系统、国家海关信息系统("金关工程")、国家科研教育信息系统、农业综合管理及信息服务系统、医药卫生信息服务系统等都将使我国国民经济信息化进一步发展。

数据库技术是构建信息系统的核心技术，社会的信息化加速过程是数据库技术继70年代之后获得蓬勃发展的又一次历史性的机遇，不论是计算机单机，还是计算机网络，甚至是周边智能设备构成的更加广泛意义上的网络，应当说，其发展的直接动力都是信息处理。现代信息处理技术从科学计算领域扩展出来之后，一发不可收拾，迅猛地渗透到几乎所有领域，已经形成了专门的信息处理技术领域；世界经济的发展主流从工业经济转向信息经济，已经出现了"知识经济"这一新名词；IT这个新的词汇的产生标志着信息产业的形成。知识和信息成为社会发展的、马力强大的新动力。信息资源与其它自然资源一样，受到了人们越来越多的重视，很多国家投入巨资来开发这一决定人类未来发展前途的宝藏。

信息技术的普及和信息高速公路的建设热潮为信息资源的开发和共享创立了良好的基础。由于信息资源的开发，人们可借助信息技术和远程通信技术，随时随地获取各种所需要的信息，提高决策的准确性和客观性，以便在变化和竞争的环境中掌握主动权并争取优势。

信息产业具有高投入、高产出、高风险的特点。高风险的特点不仅表现在投入的风险回报上，也表现在信息系统的脆弱和易遭攻击上，即较小代价的攻击成功，可能造成对方的损害程度可以非常严重。例如已经出现了核电站的控制系统(也是一种信息处理系统)被攻击者引爆的可能性。社会生活中还有各种可能的经济犯罪。因此，信息系统的安全性问题随着信息化进程而变得日益敏感和重要。

在当代激烈的国际经济和社会发展竞争中，经济实力和军事实力的竞争成为国力竞争的主要领域。正在信息化的社会对信息基础设施的建设和信息资源开发，对信息服务的快捷性、准确性、全面性，特别是信息的安全性，都提出了越来越高的要求。在信息资源开发和信息服务领域中的国际竞争、市场争夺和相互渗透也日趋激烈。信息对抗成为世界各国特别是发达国家尤为关心的问题。信息的安全显然是国家安全、国防安全的不可忽视的必要前提，也是21世纪中与每个社会成员密切相关的最重要的问题之一。有人预言，信息安全保密将是21世纪世界十大热门课题之一。因此，数据库和信息系统的安全问题成为十分重要的问题。因此，总结数据库和信息系统领域的安全研究工作的成果，总结这一领域内最前沿的技术和产品，对信息系统安全领域的发展趋势进行一些探讨，应该是很有必

要的，这也就是编写本书的初衷和基本目的。本书在选材方面，注意了全面、系统，取材较新，对大专院校的学生和信息系统的设计者、实现者的需要特别加以考虑。

本书共分十一章。涉及一些理论基础的内容集中在第三章“安全模型”和第六章“密码学与信息保密”中。为了使用户对数据库安全技术的实际进展有一个比较客观的了解，本书介绍了国产数据库系统 COBASE 的安全设计，这就是第五章“典型数据库安全设计分析”。伴随着分布系统和网际网的迅速发展，同时受到多层次客户服务器体系结构的影响，数据库技术已经不再是一门独立的学科，不能脱离网络、操作系统等周边环境来讨论安全问题。值得一提的是第七章“攻击检测”，虽然篇幅不大，但是在现代实用的信息系统中，攻击检测系统作为安全的最后一道防线，受到用户的严重关注，它也是技术和产品上发展最为活跃的一个领域，例如对病毒的对抗（也是一种攻击检测技术）。如果有可能，编著者希望能在本书再版时增补这方面的内容。

本书得到中国人民大学王珊教授的大力支持，王珊教授和她的研究生帮助校阅了全文，并且对本书的编写提出了很多中肯的建议；人民大学和中软总公司的许多同志对本书的编写也给予了多方面帮助。在此一并向这些朋友们表示衷心的感谢。

由于水平有限，书中一定会有很多不当之处，敬请批评指正。

目　录

第一章　引言 …… 1
1.1　信息化进程 …… 1
1.2　信息在世界性竞争中的地位 …… 2
第二章　安全问题概论 …… 4
2.1　信息安全学概述 …… 4
2.2　数据库安全涉及问题 …… 16
2.3　安全控制 …… 32
2.4　安全与保密 …… 35
第三章　安全模型 …… 40
3.1　引言 …… 40
3.2　哈里森-罗佐-厄尔曼存取矩阵模型 …… 41
3.3　取-予模型 …… 44
3.4　动作-实体模型 …… 48
3.5　贝尔-拉帕丢拉模型 …… 58
3.6　基于角色的存取控制(RBAC)模型 …… 62
3.7　伯巴模型 …… 67
3.8　第昂模型 …… 70
3.9　安全数据视图模型(SEA VIEW) …… 73
3.10　贾让第-沙胡模型 …… 83
3.11　斯密司-温斯莱特模型 …… 91
3.12　基于信息流控制的格模型(The lattice model for flow control) …… 96
3.13　对安全模型的讨论 …… 100
第四章　安全有关的标准 …… 102
4.1　数据库安全相关标准的发展 …… 102
4.2　TCSEC/TDI 安全标准 …… 104
4.3　简短的结语 …… 114
第五章　典型数据库安全设计分析 …… 116
5.1　可信 COBASE 的体系设计 …… 116
5.2　强制存取控制的实现 …… 118
5.3　COBASE 发展考虑 …… 125
第六章　密码学与信息保密 …… 127
6.1　密码学基础 …… 127
6.2　密码技术 …… 130

6.3 数字签名 …… 139
6.4 密码和认证技术相关标准 …… 146
6.5 数据库加密 …… 150
6.6 网络通信中的密码技术 …… 159
6.7 加密软件 …… 160
第七章 攻击检测 …… 167
7.1 引言 …… 167
7.2 攻击检测技术和理论 …… 168
第八章 数据仓库的安全问题 …… 190
8.1 数据仓库概述 …… 191
8.2 数据仓库中的安全问题 …… 192
第九章 网络安全问题 …… 195
9.1 网络信息系统安全概论 …… 195
9.2 网络操作系统 …… 202
9.3 网络管理和网络安全 …… 207
9.4 防火墙和网络安全 …… 215
9.5 电子商务的安全问题 …… 220
9.6 电子邮件安全 …… 223
9.7 NDS 的安全 …… 227
9.8 Intranet 与客户/服务器体系结构的安全问题 …… 229
9.9 公用分组交换网及其它网络的通信安全 …… 231
9.10 企业网络建设及其安全问题 …… 236
第十章 Java 语言及其安全性问题 …… 242
10.1 Java 概览 …… 242
10.2 Java 语言的特点 …… 243
10.3 Java 的安全问题 …… 245
10.4 ActiveX 安全模型 …… 251
第十一章 信息安全和病毒问题 …… 253
11.1 引言 …… 253
11.2 病毒技术 …… 253
11.3 病毒检测技术 …… 256
11.4 病毒清除技术和产品 …… 258
附录 …… 263
一、OMG 白皮书 …… 263
二、病毒及相关防护软件 …… 276
三、安全产品分类 …… 297
四、计算机犯罪有关法律条款 …… 299
五、安全数据库产品 …… 300

六、安全有关词汇表 …… 316
七、安全研究领域大事记 …… 320
参考文献 …… 322

第一章 引 言

1.1 信息化进程

90年代以来，我国信息产业蓬勃发展。90年代中期，国家制定了以“三金”工程为代表的信息工程战略规划，主要为“金桥工程”、“金税工程”、“金卡工程”等。此外，正在建立的国家宏观决策支持网络系统、国家海关信息系统(“金关工程”)、国家科研教育信息系统、农业综合管理及信息服务系统、医药卫生信息服务系统等都将使我国国民经济信息化进一步发展。

“七五”以来，我国信息产业投入资金100亿元，培训人员35 000人，并建成了卫星通信网。此外，国家经济信息系统、邮电通信系统、公安系统、民航旅客服务系统、国家统计信息系统、气象系统、电网监测调度系统、财税系统、科技情报系统、海关/经贸服务系统、新闻信息管理系统及办公自动化系统的建立和建成，对国民经济和社会发展都产生了重大的影响。我国电子信息服务业正在兴起，已有800多个公用数据库，与世界12个大型信息系统联网。

1990～1995年，信息产业总产值由50亿元增加到500亿元，平均年增长率58.5%，占世界产业的比例从0.3%提高到0.8%。全国从事信息产业产品开发、生产、营销、维护、服务及咨询企事业单位为15 000家，从业人员约30万人；制造业千余家，从业人员10万人；软件千余家，从业人员8万人；服务业13 000家，从业人员12万人；研究开发机构50余家。已形成的集团有18家，其中销售额在10亿元以上的有58家，进入全国百强企业的有18家，年销售额200亿元，占本行业的40%，初步形成了一定规模经济。我国信息产业正在实现从内销导向转为出口导向的重大转变，信息产品正在走向国际市场，开始具备了在国际市场上的竞争能力。

信息产业具有高投入、高产出的特点，并已在推进我国现代化建设的历史进程中产生了巨大的经济和社会效益；但同时也应当看到，信息产业还具有高风险的特点，一旦决策失误，则会遇到严重的挫折。因此，世界各国，特别是发达国家，在发展信息产业方面，都充分重视其高风险的问题，从政策到资金的支持都有明显的政府行为色彩。

美国政府从50年代开始就重视对科技和信息加工业的投入。美国政府每年用于科技开发超过1 000亿美元，超过了欧共体为此项投入的总和。美国是世界上最大的信息产业国和信息产品输出国，其产品在本国和国外的利用率大大高于其它国家，同时美国还利用其在技术、资金和市场上的优势，不断收买其它国家的特别是发展中国家的信息产品，以占领更多的国外市场。二战结束后，美国政府通过国家科学基金会，重点资助和扶持对国家的科技进步有重要意义的基础科学和与政府近期发展目标有关的二次信息产品和服务，为信息产业的发展奠定了坚实的基础。在过去的10多年里，美国联机数据库的数量增长了近11倍，信息产业工作者、联机服务和网关的数量也增加了10倍多。

欧洲国家也在努力发展本地区的信息产业。80年代初，欧共体国家在布鲁塞尔成立

了欧洲信息提供者协会(EURIPA),联合开发欧洲的信息资源,促进欧洲的信息产业的发展和信息交流活动。同时,欧共体国家欧洲科技信息联机网络(EURONET DIANE)投入商业运行,使欧洲地区有了自己的联机网络,逐步占领了本地区的信息市场。

Internet 在全球的普及,使数据库的开发不仅具有巨大的经济效益和明显的社会效益,同时还具有深远的政治意义。不但各发达国家在 Internet 的发展上投入了巨大的资金和人力,发展中国家也都非常重视 Internet 的发展和利用。例如新加坡政府为了抗衡西方国家新闻媒介对新加坡的负面报道,于 1995 年 2 月通过 Internet 网络,将大型数据库 SINGAPORE INFORMAP 输入 Internet,向全球网络用户介绍新加坡的发展成就。新加坡在电子版本的政府年报中提供有关新加坡的历史、人民、政府及经济发展的事实和数据,并决心将这一工作长期进行下去。日本为了解决在国际信息互换中输入国的被动地位,从 1994 年开始通过 PC 通信网络 ASAHI NET 向世界发送有关日本文化信息,除发送旅游观光指南外,还介绍本国的社会和文化,以便于加强国际间的相互了解。

1.2 信息在世界性竞争中的地位

信息技术的普及和信息高速公路的建设热潮为信息资源的开发和共享创立了良好的基础。由于信息资源的开发,人们可借助信息技术和远程通信技术,随时随地获取所需要的各种信息,提高决策的准确性和客观性,在变化和竞争的环境中掌握主动权并争取优势。世界经济的发展主流从工业经济转向信息经济,已经出现了"知识经济"的新名词,知识和信息成为社会发展的、马力强大的新动力。信息资源与其它自然资源一样,受到了人们越来越多的重视,很多国家投入巨资来开发这一决定人类未来发展前途的宝藏。美国未来学者阿尔文·托夫勒在对 21 世纪进行的前瞻研究《力量转移——临近 21 世纪时的知识、财富和暴力》一书中,对知识、信息的占有权和使用权给予了这样一段评论:"今天的信息战所以日趋激烈化,部分地是由于人们日益认识到,信息虽然对于新经济至关重要,但却不服从适用于其它资源的规则……信息是取之不尽,用之不竭的"。托夫勒使用了"信息战"的词眼来强调未来社会对信息的重视、依赖和争夺,因为他认为信息是 21 世纪最重要的资源,信息的安全问题自然成为信息社会的重要话题。托夫勒对信息安全问题举了几个精彩的例子:电子时代的投票箱里发生的切尔诺贝利事件或三里岛事件(失控);在政治家据以作出重大决策的数据库为他人所操纵的时候,能够保证他们的决策不会出现有利于敌对方的错误(扭曲)吗?……

在当代激烈的国际经济和社会发展竞争中,经济实力已经逐渐取代军事力量而成为竞争的主要领域,正在信息化的社会对信息基础设施的建设和信息资源开发,对信息服务的快捷性、准确性、全面性,特别是信息的安全性,都提出了越来越高的要求。在信息资源开发和信息服务领域中的国际竞争、市场争夺和相互渗透也日趋激烈。信息对抗成为世界各国特别是发达国家尤为关心的重大问题。从中可以看到,信息产业的的确确是关系国家、民族重大战略利益的产业,绝对不能掉以轻心。

下列数字可以充分说明信息化进程对社会发展的巨大而深远的影响:计算机平均性能每年增长 50%。从 1946 年第一台数字机诞生以来,计算机性能已提高了将近 5 个数量级。估计到 21 世纪初,硬件性能将会比 90 年代初提高 100 多倍。计算机硬件、软件和网

络技术蓬勃发展，万亿次巨型计算机将投入使用，下世纪整个世界将置于计算机网络覆盖之下。与此相匹配，将出现每秒 10 亿位的网络技术。技术手段的迅猛发展带来的是人类社会形态的翻天覆地的变化。我们已经真正站在了 21 世纪——信息世纪的门槛上了。人类社会生活的方方面面、角角落落无一遗漏地、全面地渗透着信息化进程的深刻影响。在 21 世纪，占有信息就等于占有了财富，占有信息就等于占有了权力。信息的重要性在人类文明进程中终于达到了质变的地步，社会对信息的利用程度越深，对信息的依赖程度也就越深，信息的安全问题也就必然越重要。信息的安全问题必然成为新世纪的重大问题而为愈来愈多的有识之士所认识，也必将受到全社会愈来愈广泛的注意。

在经济与社会信息化的时代，信息化已经引发了新的一轮革命。社会活动中，无论是经济领域还是政治领域，现在已经没有人再怀疑计算机信息处理的能力，技术进步为社会带来的翻天覆地的变化，可以说是日新月异，无处不在；以军事领域为例，最突出的进展是发展出了崭新的信息战理论，加速了 C4I 系统的一体化。这是信息化对国防现代化的具有时代特征的影响。以信息技术为核心的现代科技把先进的技术与完善的军事学说及与之相适应的军事组织结合起来，形成了使武器发挥最大作用的真正的军事技术革命。信息化进程大大增强了收集、处理和近于实时地传送信息的能力；信息技术与常规精确打击能力相结合，将深刻地影响到进攻和防御军事行动的实施；在军事演习等方面，信息技术拓展了高级模拟的范围，提高了演习、训练系统的设计、测试及战术发展能力。可以毫不夸张地说，信息技术为武器装备的新发展提供了空前的机遇，引发了一场涉及整个军事领域的军事技术革命。信息战正在成为军事家们不得不面对的新概念，信息的安全显然是国家安全、国防安全的不可忽视的必要前提，也是 21 世纪社会生活中与每个社会成员密切相关的最重要的问题之一。

第二章　安全问题概论

2.1　信息安全学概述

现代信息系统的飞速发展是以计算机以及以计算机为核心的计算机网络系统的飞速发展为标志的。信息系统规模化发展势头强劲，这从一个侧面预示了信息革命的到来，同时也深刻反映了当今社会对信息系统的巨大依赖性。

信息化的社会在尽力追逐信息系统的时空性能，高速计算机、高速网络逐步民用化、商用化、家用化，也确实带来了巨大的收益。但是，对于国家军事情报、政府机关的机密文件、企业公司内部计划以及个人的隐私等敏感信息，现有的多数系统还不能做到提供足够的信息安全保护。事实上，现代的计算机信息系统并不安全，它存在很大的不安全性、脆弱性和危险性。

2.1.1　信息安全和数据库安全的必要性

在现代信息社会中，信息是人类最宝贵的资源。对企业来讲，信息是企业的生命，关系到企业的发展，甚至关系到企业的生死存亡。正因为信息在人类社会活动、经济活动中起着越来越重要的作用，信息的安全就日益成为关系成败的关键要素，日益引起人们越来越深刻的重视。

最近几年来，有关信息系统的安全问题的讨论逐渐增多，大多数计算机用户、公司等在建立自己的管理信息系统或信息决策系统时，对于系统的安全给予了越来越多的关注。研究与安全性相关的问题也变得日益突出。

新形势下，计算机系统的安全问题应该得到足够的重视，正在形成一门新学科——信息安全学。所谓信息系统安全，是指为信息处理系统建立和采取的技术和管理的安全保护措施，以保护计算机系统中的硬件、软件及数据，防止其因偶然或恶意的原因而使系统或信息遭到破坏、更改或泄露。信息系统安全的内容包括了计算机安全技术、安全管理、安全评价和安全产品、计算机犯罪与侦察、计算机安全法律、安全监察，以及计算机安全理论与策略。概括起来，计算机系统的安全性问题被区分为三大类，即技术安全类、管理安全类和政策法律类。技术安全是指计算机系统本身实现中，采用具有一定的安全性质的硬件、软件来实现对于数据及其所含数据或信息的安全保护，能够在整个系统中，在一定程度甚至完全可以保证系统在无意或恶意的软件或硬件攻击下仍能使得系统内的数据或信息不增加、丢失、泄露。除技术安全之外的，诸如硬件意外故障、场地的意外事故、管理不善导致的数据介质的物理丢失等安全问题，视为管理安全。而政策法律类则指有关政府部门建立的一系列的与计算机犯罪有关的法令、法规。本文将集中讨论技术安全类问题。

保密作为一个传统概念，在现代社会得到更深入、更广泛的认识和理解，这与社会的信息化程度是密切相关的。当今社会正向着信息化方向飞速发展，信息作为一种特殊的资源而存在，社会生活越来越依赖于科学技术的发展，同时也越来越依赖于对各种信息的获

得。信息的重要性骤增，这样，研究信息安全问题、解决信息安全问题从而保护系统信息促进了可信系统的形成与发展。

计算机系统或信息处理系统的安全技术同时涉及软件技术和硬件技术。在计算机使用的早期，特别在微机或小型系统中，人们的安全意识相对淡薄得多，一般至多为系统加一道口令。而现在的信息处理系统中，尤其是在网络环境下，不仅要采用口令来进行基本的用户识别，还要为不同实体进行标记，在各个接口间进行验证等。

造成系统不安全的因素有很多，既有系统的稳定性或可靠性不足、环境干扰或自然灾害等客观因素，也有人员工作失误、操作不当等，但对系统的不安全影响最大的是人为的攻击破坏，其中包括人为的非授权存取与破坏、计算机病毒等。目前，各种人为破坏已遍及军事、司法、政府机关、交通、通信、金融等社会的方方面面，造成了巨大的损失，并且许多后果是惊人的。比如：在海湾战争中，“沙漠盾牌”行动计划甚至被网络黑客所捕捉；美国司法机关受到攻击，原告的讼词被窃取等。

计算机系统所受的安全攻击包括来自外界的蓄意攻击闯入或无偿使用资源（即免费搭车等，本文在介绍隐蔽信道时将进一步介绍这一概念）。这些攻击大多采用匿名注册、请求拒绝、特洛伊木马（Trojan Horse）及网络蠕虫（Worm）等手段来达到非法侵入或消耗系统资源而使系统性能降低甚至瘫痪。例如，在 Internet 中，Email 蠕虫可以导致电子邮件系统瘫痪。如果蠕虫侵入军事指挥通信系统，则可能使得整个指挥系统失灵，灾难性后果是可以想像的。在网络环境中，不同场地设备的使用使得网络硬件也成为网络“黑客”的一个有效的攻击点。“黑客”可以通过网络通信设备，从合法用户的通信过程中截获信息并予以破解，进而进行对信息的修改或加载。

为降低进而消除对系统安全的攻击，尤其是弥补原有系统在安全保护方面的缺陷，安全领域的专家经过长期的研究，在计算机安全技术方面逐步发展建立了一系列系统安全可信的标准。

2.1.2 历史与动态

信息安全的研究伴随人类社会的发展走过了漫长的历程。其应用领域不断拓宽，研究方法不断有所突破，是一门古老而又年轻的学科。信息安全是一个内涵极其丰富的概念，信息安全问题不仅涉及到计算机系统本身的技术问题、管理问题，还涉及法律学、犯罪学、心理学、经济学、应用数学、计算机基础科学、计算机病毒学、加密学、审计学等相关学科。同时，信息安全又是一门技术，越来越多的人在研究和应用这一技术，并使这一技术形成产品、形成产业。

纵观信息安全研究的历史，大致可以分为三个阶段：一是计算机诞生前的保密学（以通信安全保密为主）研究；二是计算机诞生后的计算机系统的安全保密研究；三是近年随着全球信息高速公路日渐成熟，大范围的信息系统广泛建立，社会信息化迅猛进展，形成了对信息系统的安全保密研究。这三个阶段的研究相互衔接、互相渗透。通信安全保密是计算机和信息系统安全保密的基础；计算机安全研究是现代信息系统安全研究的重要内容；信息系统安全保密研究实际上综合了前面两者的研究，并构成了新的研究体系。这三个阶段体现了递进的研究层次，前者是后者的基础和前提，后者对前者具有反馈和激励作用。通信安全保密是基础研究层次，计算机安全保密问题是中间研究层次，信息系统安全

则是最高研究层次。

随着信息系统的广泛建立和规模化，使计算机的应用形式上升为网络形态。这种网络化的信息系统在系统内纵向贯通，在系统间横向渗透，构成了集通信、计算机和信息处理于一体的庞大而复杂的系统，成为现代社会运转所不可缺少的基础。人们意识到，不能再从单个安全功能、单个网络来个别地考虑安全问题，而必须从体系结构上全面而系统地考虑安全保密。因此，安全保密的研究应着力于系统这个层次，把信息系统作为安全保密研究的对象。但是，由于研究对象的空前复杂性，信息系统安全保密研究目前还没有系统的理论，整个研究还期待着质的突破。

战争是信息安全研究的另一个重要的激励因素，未来战争除了与传统战争的"物质"性相同而外，对信息、情报的依赖程度与日俱增，信息、情报在战争中的作用也越来越重要；信息安全问题的重要性已经上升为关系战争胜负乃至于国家根本利益的高度，信息安全是信息战的一个组成部分。

信息安全又是社会稳定安全的必要前提条件，随着信息攻击和信息犯罪的增多，社会对信息安全的重视程度显然也达到了空前的高度。信息系统安全无误地运转变得空前重要，已经引起了各国政府和研究机构的高度重视。

从 70 年代开始，现代信息系统安全研究开始结出累累硕果。1971 年，Lampson 提出了存取监控器的设想。其思想是所有主体必须根据系统存取授权表来实现对客体的存取，对客体的每次存取以及授权的改变都必须通过存取监控器。存取监控器是一个重要的存取控制抽象模型，为保护思想的实现提供了基本的理论，也为系统的审计监控提供了前提。

1972 年，Schell 提出了安全内核的概念。1974 年，Mitre 证实了构筑安全内核的可能性。安全内核的提出是信息安全保密研究的一个重要成果。安全内核方法是用有条理的设计过程代替智力游戏，从而构筑安全的计算机系统，进而为信息系统的开发建立安全的平台提供了理论基础。许多的现代操作系统都采用了安全内核的概念，包括"八五"、"九五"期间开发的国产系统软件平台 COSA 就是采用安全内核、系统多态的思路开发的。1978 年，Gudes 等人提出了数据库的多级安全模型，把计算机安全保密研究扩展到数据库领域。1988 年，Denning 提出了数据库视图技术，为实现最小泄露提供了技术途径。

进入 80 年代，许多国家颁布了计算机犯罪法，成立了信息安全机构、防治计算机病毒协会等等。1984 年国际标准化组织(ISO)公布了信息处理系统参考模型，并提出了信息处理系统的安全保密体系结构(ISO－7498-2)。国际信息处理联合会(IFIP)于 1984 年成立了信息安全技术委员会，即 TC11，专门研究信息安全问题。该委员会每年召开一次国际会议，讨论信息安全政策、技术、管理和控制等问题。在 1984 年的国际信息处理联合会(IFIP)安全保密年会上，Fugini 提出了办公信息系统的安全管理方法。其它的国际性会议有国际计算机和通信安全与保护大会、国际信息安全计算机病毒专题会议、世界数据安全会议等。欧洲共同体与欧美各国都有相应的会议和常设机构。我国自 1986 年 7 月第一次在青岛举行全国信息安全技术交流会以后，至今已召开了 10 多次会议。

80 年代中期，开始出现分布式系统的应用。1985 年，Voydock 和 Kent 提出了高级网络协议的安全保密问题。1986 年，Nessett 提出分布式系统的安全保密问题，使信息系统安全保密研究的范围不断扩大，并逐渐走向深入。虽然在方法和技术上没有什么突破，但