中国科学院研究生教学丛书

信息系统的安全

卿斯汉　冯登国　编著

科学出版社
www.sciencep.com

中国科学院研究生教学丛书

信息系统的安全

卿斯汉　冯登国　编著

国家重点基础研究发展规划资助项目(项目编号:G1999035810)
国家自然科学基金项目资助项目(项目编号:60083007)

科学出版社

北京

内 容 简 介

本书为《中国科学院研究生教学丛书》之一。本书系统地介绍了信息系统安全的基本理论和关键技术，书中结合作者近年来的科研工作，力求反映出信息系统安全领域的最新研究成果。全书共分 7 章，主要内容包括：信息系统安全的基本概念和基础知识；密码系统的基本模型；一些有代表性的密码算法和密钥管理技术；美国 21 世纪的密码算法标准——AES；一些有代表性的认证协议；主要的认证协议的形式化分析工具——BAN 逻辑和 SVO 逻辑；安全电子商务协议的基本需求；一些典型的电子商务协议以及对它们的形式化分析；电子商务协议主要的形式化分析工具——Kailar 逻辑；网络安全的基本概念；网络面临的安全威胁；网络安全的服务与机制；防火墙技术；网络攻击与防范；安全操作系统的基本概念；自主存取控制与强制存取控制；最小特权管理；标识与鉴别；审计；可信通路；隐蔽通道；操作系统的安全模型；安全操作系统的设计和开发方法；数据库安全的基本需求；数据库的完整性与可靠性；存取控制；数据库加密和密钥管理的特点；数据库的安全策略和数据库的安全模型；数据库的备份和恢复等。

本书可作为高等学校计算机、信息与通信科学、数学等专业师生的参考教材，对从事上述领域工作的广大科技人员具有重要的参考价值。

图书在版编目(CIP)数据

信息系统的安全/卿斯汉，冯登国编著. —北京：科学出版社，2003
(中国科学院研究生教学丛书)
ISBN 7-03-011414-0

Ⅰ. 信… Ⅱ. ①卿 … ②冯… Ⅲ. 信息系统-安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2003)第 027429 号

责任编辑：鞠丽娜 / 责任校对：朱光光
责任印制：吕春珉 / 封面设计：槐寿明

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
*
2003 年 5 月第 一 版 开本：787×1092 1/16
2003 年 5 月第一次印刷 印张：9 1/4
印数：1—5 000 字数：220 000

定价：18.00 元
(如有印装质量问题，我社负责调换〈环伟〉)

《中国科学院研究生教学丛书》序

在21世纪曙光初露，中国科技、教育面临重大改革和蓬勃发展之际，《中国科学院研究生教学丛书》——这套凝聚了中国科学院新老科学家、研究生导师们多年心血的研究生教材面世了。相信这套丛书的出版，会在一定程度上缓解研究生教材不足的困难，对提高研究生教育质量起着积极的推动作用。

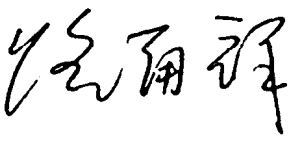
21世纪将是科学技术日新月异，迅猛发展的新世纪，科学技术将成为经济发展的最重要的资源和不竭的动力，成为经济和社会发展的首要推动力量。世界各国之间综合国力的竞争，实质上是科技实力的竞争。而一个国家科技实力的决定因素是它所拥有的科技人才的数量和质量。我国要想在21世纪顺利地实施“科教兴国”和“可持续发展”战略，实现小平同志规划的第三步战略目标——把我国建设成中等发达国家，关键在于培养造就一支数量宏大、素质优良、结构合理，有能力参与国际竞争与合作的科技大军，这是摆在我国高等教育面前的一项十分繁重而光荣的战略任务。

中国科学院作为我国自然科学与高新技术的综合研究与发展中心，在建院之初就明确了出成果出人才并举的办院宗旨，长期坚持走科研与教育相结合的道路，发挥了高级科技专家多，科研条件好，科研水平高的优势，结合科研工作，积极培养研究生；在出成果的同时，为国家培养了数以万计的研究生。当前，中国科学院正在按照江泽民同志关于中国科学院要努力建设好“三个基地”的指示，在建设具有国际先进水平的科学研究基地和促进高新技术产业发展基地的同时，加强研究生教育，努力建设好高级人才培养基地，在肩负起发展我国科学技术及促进高新技术产业发展重任的同时，为国家源源不断地培养输送大批高级科技人才。

质量是研究生教育的生命，全面提高研究生培养质量是当前我国研究生教育的首要任务。研究生教材建设是提高研究生培养质量的一项重要的基础性工作。由于各种原因，目前我国研究生教材的

建设滞后于研究生教育的发展。为了改变这种情况，中国科学院组织了一批在科学前沿工作，同时又具有相当教学经验的科学家撰写研究生教材，并以专项资金资助优秀的研究生教材的出版。希望通过数年努力，出版一套面向21世纪科技发展，体现中国科学院特色的高水平的研究生教学丛书。本丛书内容力求具有科学性、系统性和基础性，同时也兼顾前沿性，使阅读者不仅能获得相关学科的比较系统的科学基础知识，也能被引导进入当代科学研究的前沿。这套研究生教学丛书，不仅适合于在校研究生学习使用，也可以作为高校教师和专业研究人员工作和学习的参考书。

“桃李不言，下自成蹊。”我相信，通过中国科学院一批科学家的辛勤耕耘，《中国科学院研究生教学丛书》将成为我国研究生教育园地的一丛鲜花，也将似润物春雨，滋养莘莘学子的心田，把他们引向科学的殿堂，不仅为科学院，也为全国研究生教育的发展作出重要贡献。



前　言

随着计算机的迅速普及和互联网的飞速发展，经济、信息全球化的趋势已日益明显，它在给我国带来发展机遇的同时，也向我们提出了严峻的挑战。西方发达国家作为全球化浪潮和知识经济的主导者，正在利用信息霸权谋取主宰世界，正在鼓吹和准备信息威慑及“战略信息战”。面向21世纪，信息系统安全已成为世界性问题。没有信息系统安全，就没有完全意义上的国家安全，就没有真正的政治、军事和经济安全。因此，我们要从全球战略的高度来考虑信息系统的安全问题。

本书是一部关于信息系统安全的专著。信息系统安全的内容十分广泛，热点不断变化，作为研究生教材，本书讲述了有关信息系统安全中最为重要的内容，包括：信息系统安全的核心——密码技术；信息系统安全的基础——安全协议；信息系统安全的三大要素——数据库安全、操作系统安全和网络安全；网络安全的第一道屏障——防火墙；网络安全的重要应用——安全电子商务协议等方面。本书不强调多而全，而强调少而精，亦即对所叙述的内容尽量讲得清楚一些。本书包括上述领域的最新研究成果，同时包括作者近年来的科研成果。我们希望，广大读者通过本书能够对信息系统的安全问题有一个较为全面的认识，对信息系统安全的基本理论和关键技术加深理解，并能够解决信息系统中产生的一些实际安全问题。

全书共分7章。第1章主要介绍了信息系统安全的一些基本概念和基础知识，以及本书的组织与编排。第2章主要介绍了密码学的基本概念、密码系统的基本模型、一些有代表性的密码算法、密钥管理技术以及美国的先进加密标准AES。第3章主要介绍了一些有代表性的认证协议，包括：Kerberos协议、Otway-Rees协议、Needham-Schroeder协议、Yahalom协议等，并介绍了主要的认证协议的形式化分析工具——BAN逻辑和SVO逻辑。第4章主要介绍了安全电子商务协议的基本需求；一些典型的电子商务协议以及对它们的形式化分析；电子商务协议主要的形式化分析工具——Kailar逻辑，以及我们针对Kailar逻辑的缺陷所做的改进。第5章主要介绍了网络安全的基本概念、网络面临的安全威胁、网络安全的服务与机制、防火墙技术、网络攻击与防范等。第6章主要介绍了安全操作系统的基本概念、自主存取控制与强制存取控制、最小特权管理、标识与鉴别、审计、可信通路、访问监督器、可信计算基、隐蔽通道、操作系统的安全模型等，并结合我们的工作实践介绍了安全操作系统的设计和开发方法。第7章主要介绍了数据库安全的基本需求，包括：数据库的完整性与可靠性、存取控制、数据库加密和密钥管理的特点、用户身份鉴定、审计等；数据库的安全策略和数据库的安全模型；数据库的备份和恢复。

在本书的写作过程中，得到了中国科学院信息安全技术工程研究中心广大科研人员的支持和帮助，本书涉及的许多科研成果是在他们共同努力下完成的，部分工作人员和研究生还参加了本书的编写和校对工作。在此，我们特别感谢：倪惜珍研究员、刘文清博士、吴文玲副研究员、蒋建春博士、杨雷博士、王贵林博士、贺也平博士、周典萃硕士等。

本书的出版得到中国科学院研究生教材出版基金的资助，在此特表谢意。作者也感谢

科学出版社的责任编辑为本书的顺利出版所付出的辛勤劳动。

本书作为研究生教材，主要的读者对象是高年级本科生、硕士和博士，也可供计算机、信息和通信等相关专业的教学、科研和工程技术人员参考。由于作者的水平和时间有限，不足之处在所难免，敬请广大读者批评指正。

作　者

2003 年 3 月

目　录

第1章 绪 论

信息系统安全是一门既古老又年轻的科学，它既包含密码学这一古老的分支，又包括网络安全这一新兴的学科。本书阐述有关信息系统安全的重要内容，包括：信息系统安全的核心——密码技术；密码学的直接应用——安全协议；信息系统安全的三大要素——数据库安全、操作系统安全和网络安全；以及网络安全的第一道屏障——防火墙等方面。本章主要介绍信息系统安全的一些基本概念和基础知识。

1.1 信息系统和信息安全

随着互联网络的飞速发展，信息作为一种无形的物质资源，其重要性与日俱增。人们逐渐意识到，信息是促进经济增长和社会进步的重要资源。通过构造良好的信息系统，我们才能“耳聪目明”，正确决策，高效地利用能源和物质资源，才能推动社会的文明和进步。计算机信息系统对各种信息进行海量和快速地采集、存储、处理和交换，替代传统的低效人工处理，所以被广泛应用于政治、军事、经济、科研等各行各业，成为重要的工具和手段。到2000年底为止，据不完全统计，我国各领域已经使用的各类计算机信息系统达100余万个，正日益成为各行业、各部门赖以正常运转的不可缺少的有力工具。

计算机信息系统已经渗透到社会的各个方面，许多政府部门、机构、企业，甚至家庭都应用计算机系统存储文件，管理日常事务，参与决策，这些机构都已经计算机化了。这种社会的计算机化产生了一种新的社会资产：计算机资产。计算机资产包括两个部分：一是计算机信息系统资源，包括硬件、软件、系统相关配套设备和设施、相关的文档资料、系统服务、计算机业务人员等。这一部分是信息系统的物质载体。二是计算机系统产生和拥有的信息资源，包括统计数据、机密信息、个人档案、计划、情报、资料等，这一部分是信息系统的本质内容。如果说系统资源是国家的重要物质财富，那么信息资源则是国家的重要战略资源。谁拥有它，谁就掌握了战略主动权。因此，对计算机资产的保护有着重要的战略意义。

在计算机问世之初，计算机的数量还相当少，懂得计算机技术的人又不多，所以那时的计算机应用只有简单的安全性问题。80年代以后，分布式网络日益普及，跨国的计算机网络逐渐建立起来。最明显的例子是Internet在全球的迅速普及和发展。据美国国家科学基金会(U.S. National Science Foundation)的统计，从1995年到2000年，Internet以空前的速度增长，其中商业市场的年增长率达到62.4%；Internet的用户数从3000万增加到6亿以上。与此同时，计算机管理技术、网络中的信息交换控制、程序及资源共享秩序以及计算机使用者应遵循的法律及人们的基本价值观念、道德准则等却未能得到同步提高，这种情况就为今天的计算机犯罪的产生和发展提供了温床。以下是几个计算机犯罪的例子：

1989年3月2日凌晨，3名德国黑客因涉嫌向前苏联出售机密情报被捕，他们在两年

多的时间内，闯入了许多北约和美国的计算机系统，窃取了许多高度机密的信息。

1988年11月2日，美国康奈尔大学的学生罗伯特·莫里斯释放了一个蠕虫病毒，造成Internet网上近6000台主机瘫痪，损失据称高达几千万美元。

法国国防部1996年证实，法国海军行动力量参谋部的计算机所存储的军事机密于1995年7月底被人盗窃。这些军事机密包括几百艘盟军军舰的声音识别码，即海军情报部门分类保存的每艘军舰的特殊的声音，它们可以保证情报部门准确地判定每艘军舰的航行方位。这些军事机密被窃，令法国政府和军事部门大为恐慌。

1996年9月，美国中央情报局的主页被一群远在瑞典的少年黑客改为中央笨蛋局(Central Stupidity Agency)。此前，一名黑客闯入美国司法部网址，将主页上的"司法部"(Department of Justice)改为"非法部"(Department of Injustice)，页面的背景也被换成了德国纳粹党党徽的标志。

2000年初，黑客大举进攻美国和日本等发达国家的网站。例如，2000年1月，日本政府11个省、厅受到黑客攻击。总务厅的统计信息全部删除；外务省主页3分钟受攻击1000余次；最高法院1月26～28日受攻击3000余次。美国一些著名网站也大部分被黑，造成严重损失和社会影响。上述现象引起美国总统克林顿和日本前首相小渊惠三的高度重视。对此，日本首相小渊惠三亲自指挥，采取三大措施：1)通产省成立信息安全对策专门机构；2)2月1日，政府成立黑客特别委员会，首批拨款24亿日元；3)着重研究入侵检测技术、追踪技术、病毒技术和密码技术四大信息安全技术。针对美国网站大面积遭受黑客攻击的严重情况，克林顿总统亲自主持专门会议，即著名的28人会议，其中16人来自跨国信息产业，6人为政府官员，6人来自科研单位。值得注意的是，这是美国政府第一次邀请科研单位人员参加此类会议。会上，克林顿总统进行总结并得出以下结论：1)信息安全靠法制，法制靠技术；2)"黑客事件"是发展中的问题；3)政府应创造保障信息安全的大环境；4)加大信息安全领域的科研投入；5)加强信息安全培训，增强全民信息安全意识；6)建设信息安全示范工程；7)加强政府和企业之间关于信息安全的沟通。最后，克林顿强调，信息安全是国家大事，不单只是企业关注的事情。

2000年10月，黑客入侵微软公司并获取微软新开发产品的机密源代码事件披露，震动了微软公司高层，包括比尔盖茨本人。此案初步定性为工业间谍案，并移交美国联邦调查局处理。世界各大媒体争相报道，有的媒体冠以"黑客太黑，微软太软"大标题，讽刺微软这样著名的公司都无法挡住黑客凶猛的攻势。这一事件无疑将引起大跨国公司的重视，所以要吸取微软公司的教训，不能对信息安全问题掉以轻心。

上述事实说明，计算机犯罪已经渗入到政府机关、军事部门、商业、企业等单位，如果不加以遏制，轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全，所以信息安全已引起许多国家，尤其是发达国家的高度重视，他们不惜在此领域投入大量的人力、物力和财力，以达到提高计算机信息系统安全的目的。

1.2 信息系统安全的概念和基本需求

什么是信息安全(information security)呢？

国际标准化组织ISO对信息安全提出的建议定义是："为数据处理系统建立和采取

的技术和管理的安全保护。保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭受破坏、更改、泄漏”。国内一些学者建议的定义为：“计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭受破坏、更改、泄漏以及系统连续正常运行”。具体地说，信息系统的安全包含以下三个方面的内容：

1）运行系统的安全包括：法律、政策的保护；硬件运行安全；操作系统安全；防止电磁泄漏等；

2）系统信息的安全包括：用户身份认证、存取权限控制、审计跟踪、数据加密等；

3）信息内容的安全主要指意识形态方面的不健康内容或对人类发展、社会稳定不利的内容，如：暴力、反动言论、色情内容等。

众所周知，人们对信息安全的第一需求是保密性，亦即未经授权者不能理解相关信息。实现保密性的基本技术是密码学，密码学由密码编码学和密码分析学两大部分组成。密码编码学是研究速度快且难以破译的密码算法的科学，密码分析学是研究攻破密码算法的方法的科学。这两门科学既相互对立，又相互依存，缺一不可。

人们对信息安全的另一个主要需求是完整性，亦即传输或存储的信息是未经窜改、重放或延迟的原始真实信息。第三个需求是非否认性，亦即消息的发送方不能否认消息的发送，消息的接收方不能否认消息的接收等等。上述两类需求也是很自然的，在网络环境中为互不相识的人们或实体建立信任关系时，必须确认信息的真实性，确认信息真实的发送者和接收者，在提交仲裁时提供不可否认的证据等等。

此外，信息的采集和加工以及信息系统的建立是有代价的。人们希望需要这些信息时即可应用。然而，由于黑客常用拒绝服务式攻击，则可能引起系统效率大大下降或系统瘫痪，计算机病毒也可能引起系统资源破坏或系统崩溃。因此，人们自然而然地提出了信息安全的可用性的需求。

为了实施安全协议，特别是安全的电子商务协议，还有一个重要的需求即公平性的需求。这一需求的含义是，参加协议的任意一方无论在协议执行的哪一个阶段终止协议的执行，所有协议的参与方均处于平等的地位。

最后，人们对信息安全的重要需求是可靠性，亦即保证信息系统能够高质量地持续运行的特性。

如何衡量信息系统的安全性呢？我们可以通过信息系统的安全性衡量标准，4A 的完善程度来衡量。

所谓 4A 系指：用户身份认证(Authentication)、授权(Authorization)、审计(Accountability)和保证(Assurance)。对用户身份进行认证，是指在用户获取信息、访问系统资源之前对其身份标识进行确认和验证，保证用户的合法性。针对不同的用户进行授权，使用户能够以合适的权限合法地访问各种不同的信息及系统资源。审计是对各种信息安全事件的检查、跟踪和记录，提供信息系统中信息安全事件的证明与根据。保证的作用在于能够确保系统安全策略的实施，保证信息被完整、准确地解释，以及在意外故障中保证信息资源不被破坏。

1.3 威胁信息系统安全的途径

对于信息系统安全构成的威胁主要有两类：信息泄漏和信息破坏。

1）信息泄漏：所谓信息泄漏，就是故意或偶然地获得其他用户的信息，特别是敏感的机密信息。

2）信息破坏：由于偶然事故和人为故意破坏信息的正确性、完整性和可用性。例如，各类设备的硬件和软件的偶然性故障；环境条件和自然因素的影响以及操作失误造成的信息破坏。特别严重的是，抱着故意去破坏他人的信息。恶意攻击的目的大致有以下几种：

1）企图获得数据库里的机密信息；

2）企图获得用户的机密信息；

3）修改或破坏文件和信息；

4）获得任意使用计算机系统和数据通信系统的特权，以便长期访问系统。

对信息的人为故意威胁称之为攻击。就攻击的方法而言，它可以归纳为被动攻击和主动攻击两类。对信息的威胁除了上述人为的恶意攻击以外，还可能有各种无意的信息泄漏和信息破坏。如操作不当、编程错误、误用磁盘等等。

另外，对信息系统的威胁还包括对信息系统或计算机网络的实体威胁，主要指对系统的硬件和设备的威胁。例如：

1）人为破坏系统和设备；

2）各种自然灾害；

3）丢失各类媒体；

4）设备故障，包括硬件、电源和其他设备故障；

5）战争破坏和散失等。

应当指出，对实体的威胁不仅造成国家财产的严重损失，更重要的是会造成机密信息的泄漏和破坏。因此，对实体的保护是防止信息威胁的天然屏障。

当前在信息安全领域存在下述主要问题。

1）信息系统的电磁辐射防护问题。关于这个问题，发达国家在60年代初已注意解决。由于技术的进展，现已有人演示了在1000米以内距离即可窃收计算机显示终端的电磁辐射并且复原其信息。因此，防范国内外敌人“窃听”计算机信息是保护国家利益的重要问题。目前，对这一问题的解决主要有两种措施，一是装设电磁屏蔽间，使计算机辐射的电磁波封闭在房间内。一是使用低辐射的计算机产品，增加窃收的难度。目前，国外已有多种型号的产品，但先进产品及其标准对我国保密和禁运。

2）计算机病毒问题。计算机病毒是能将本身复制到其他程序中的一种程序。计算机病毒由两个基本部分组成：传染部分和行动部分。传染部分决定病毒蔓延的速度和侵袭的范围，行动部分决定病毒的危害程度。针对计算机病毒破坏信息系统资源与否，计算机病毒可以分为恶性病毒和良性病毒两类。但是，不论何类病毒都是信息系统正常运行时所不需要的。随着网络的普及和发展，计算机病毒可以通过计算机网络迅速传播，因此带来的危害也越来越大。

3）计算机黑客问题。计算机联网以后，特别是用电话线联网以后，计算机黑客问题就

成了计算机安全的大敌。不法分子采用各种手段(例如长期猜试用户口令)非法进入计算机系统,成为非法用户。越是重要的计算机网络,越是黑客进攻的目标,越要引起我们严密的注意。国防、经济、公安、银行等重要的计算机网建成后必将出现黑客问题。美国国防部的网络和宇航局的网络一直处于黑客不停顿的进攻下,足以引起我们的警惕。防止黑客得逞的主要措施是搞好联网情况下的用户鉴别和存取控制。利用人的生理特征鉴定用户身份是可靠的方法,但费用较高。加密和数字签名等也是常用的方法。

4) 计算机犯罪问题。随着计算机的推广应用,以计算机为主要工具或将计算机作为对象的犯罪案件,即计算机犯罪不断增加,危害程度亦日益严重。例如,英国 1983 年计算机诈骗案的平均金额为 3 万英镑,但 1988 年就增加到 40 万英镑。从我国发现的计算机犯罪案件的情况看,犯罪分子都是内外勾结,因此对内部人员的审查和教育是不容忽视的问题。国外甚至有高层经理和计算机安全顾问进行计算机犯罪的案例,值得我们警惕。此外,在研究信息系统安全技术时,应当开发针对内部人员作案的安全产品。

要保证计算机信息系统的安全性,首先要从技术上入手,构造信息系统的安全壁垒,抵御各种各样的攻击,甚至可以通过某些称之为"蜜罐"的陷井捕获犯罪分子。现在常用的信息安全关键技术有:1)数据加密技术。包括:数据传输加密技术、数据存储加密技术、数据完整性鉴别技术、密钥管理技术;2)智能卡技术;3)防火墙技术;4)安全操作系统技术;5)安全数据库技术;6)入侵检测技术;7)访问控制技术;8)安全 WEB 服务器技术等等。

另外,保证信息系统的安全性还包括很多非技术因素,例如建立与信息安全相关的法律、法规,使黑客慑于法律的威严,不敢轻举妄动。同时,信息系统的使用机构、企业、社团应建立相应的信息安全管理办法,加强内部管理,建立审计和跟踪机制,提高整体信息安全意识,防止诸如"社会工程学"(social engineering)之类的攻击。

总之,对于信息系统的安全,我们应有以下几点认识:

1) 紧迫性:事实已经表明,信息安全是关系到一个国家的生存与发展的重要因素,具有重大的战略意义,确保信息安全可谓刻不容缓,否则,将悔之晚矣!

2) 长期性:信息系统的安全问题完全可以用"魔高一尺,道高一丈"来形容,它是盾与矛,矛与盾之间的无限循环。希望一劳永逸地解决信息系统安全的想法是不切实际,甚至是危险的;

3) 综合治理:信息系统的安全问题不仅仅是一个技术问题,而是一个集技术、管理、法规、道德和教育综合作用为一体的系统工程;

4) 相对性:信息安全总是相对的,它总是与所付出的代价紧密相连。在实际系统中,总是要在信息安全与系统的方便性与易用性之间寻求平衡点。

1.4 本书的组织与安排

本书共分 7 章,从第 2 章起,我们分别阐述信息系统安全中的一些基本理论和关键技术。第 2 章主要介绍了密码学的基本概念、密码系统的基本模型、一些有代表性的密码算法和密钥管理技术。最后,介绍美国的先进加密标准 AES 和美国今年宣布的获胜算法——Rijndael 算法,它将作为美国政府 21 世纪使用的密码算法。第 3 章主要介绍了一些有代表性的认证协议,其中包括实用的认证协议——Kerberos 协议和一些经典的认证