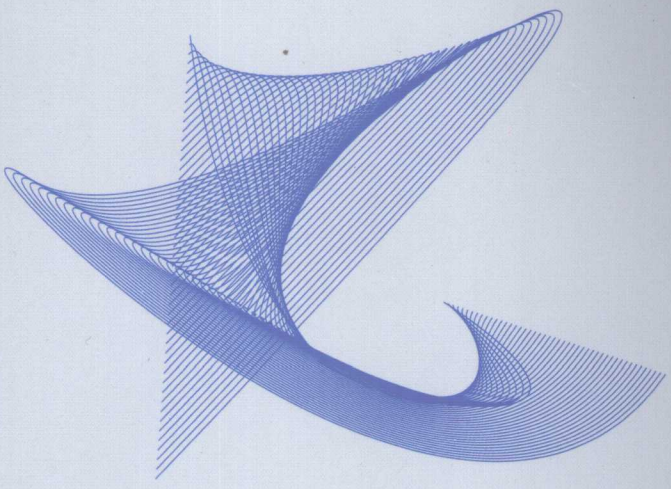
普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全技术概论



冯登国　赵险峰　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全技术概论

冯登国　赵险峰　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书概括地介绍了主要的信息安全技术，包括密码、标识与认证、授权与访问控制、信息隐藏、网络与系统攻击、网络与系统安全防护与应急响应、安全审计与责任认定、主机系统安全、网络系统安全、恶意代码检测与防范、内容安全、信息安全测评、信息安全管理等技术，所介绍的内容涉及这些信息安全技术的基本术语与概念、发展历史与发展趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制、基本实现方法等方面。

本书有助于读者全面了解信息安全技术的基本原理、方法及各项技术之间的关系，适合作为高等学校信息安全专业本科生和相关专业的高年级本科生或研究生的教材，也适合供相关科研人员和对信息安全技术感兴趣的读者阅读。

图书在版编目（CIP）数据

信息安全技术概论/冯登国，赵险峰编著. —北京：电子工业出版社，2009.4
（信息化与信息社会系列丛书. 高等学校信息安全专业系列教材）
普通高等教育“十一五”国家级规划教材
ISBN 978-7-121-08578-9

Ⅰ.信… Ⅱ.①冯… ②赵… Ⅲ. 信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 044867 号

策划编辑：刘宪兰
责任编辑：张 京
印 刷：北京东光印刷厂
装 订：三河市万和装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：16 字数：389 千字
印 次：2009 年 4 月第 1 次印刷
印 数：4 000 册 定价：28.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

总　　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。在做这些工作的过程中，我们愈发认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一个紧迫需求，成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006 年 5 月，我国《2006—2010 年国家信息化发展战略》公布，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版物等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的，是力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑当前国家信息化人才培养的需求、各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师、分期分批出版高质量的信息化教育丛书的

方式，根据当前高校专业课程设置情况，先开发“信息管理与信息系统”、“电子商务”、“信息安全”三个本科专业高等学校系列教材，随后再根据我国信息化和高等学校相关专业发展的情况陆续开发其他专业和类别的图书。

对于新编的三套系列教材（以下简称系列教材），我们寄予了很大希望，也提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争出版一批精品教材，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每一本教材配有一至两位审稿专家。

如今，我们很高兴地看到，在教育部和原国务院信息化工作办公室的支持下，通过许多高校教师、专家学者及电子工业出版社的辛勤努力和付出，“信息化与信息社会”系列丛书中的三套系列教材即将陆续和读者见面。

我们衷心期望，系列教材的出版和使用能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材开始陆续出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、老师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，还是一个初步的尝试。其中，固然有许多的经验可以总结，也难免会出现这样那样的缺点和问题。我们衷心地希望使用系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

曲维枝

2008 年 12 月 15 日

序　言

人类走过了农业社会、工业社会，如今正处于信息社会的伟大时代，“信息社会”这个词语无疑已经家喻户晓，信息化的大潮正席卷着世界的每一个角落。地球两端，万里之隔，人们能通过互联网与亲朋畅快交流，音容笑貌犹如就在眼前，真正是天涯变咫尺；分支机构遍布全球的庞大企业运转有条不紊，各机构协作顺畅，其功能强大的信息系统功勋卓著；分析复杂神秘的生物基因，预测瞬息万变的天气趋势，有了容量惊人的数据库系统和“聪明绝顶”的高性能计算系统，科学家们如虎添翼。总之，人类处处受益于信息化成果并正在信息化这条大道上加速前进，决不会放慢脚步。

然而，阳光之下总会有阴影，人类越依赖于信息系统，信息安全问题就越发凸显。关于信息安全的形形色色的新闻日益频繁地见诸于媒体：某银行数据库数据被窃取导致客户信息泄露，使客户惶惶不安，银行面临信任危机；某计算机病毒大肆泛滥，无数用户系统瘫痪，让相关企业损失惨重；某国军方网络被黑客侵入，军事机密竟被人如探囊取物般轻易窃取……这样的事件一再提示我们，信息安全问题是社会信息化发展进程中无法回避的客观产物，只有主动积极地面对和解决这一问题才能保障信息化的顺利推进，确保经济、社会的稳定乃至国家的安全。

目前，世界各国政府在信息安全领域的重视程度正在不断加大，并纷纷推出了本国的相关标准、规范或法律，大力扶持高校和其他科研机构对信息安全问题的研究，同时采取各种措施促进信息安全领域的人才培养以满足本国信息化建设的需要，为本国的信息产业发展提供中坚力量。特别是一些信息化进程起步较早，水平较高的发达国家，其信息安全领域的研究水平和产业化程度已相当令人瞩目。

我国正处于信息化建设的关键阶段，2006 年发布的《2006—2010 年国家信息化发展战略》更是从战略的高度指出了推进信息化对我国经济建设和国家发展的重要作用，规划出了新时期我国信息化发展的宏伟蓝图。由此可见，我国的信息化建设和信息产业正面临前所未有的机遇和挑战。

正是在这样的时代背景下，信息安全问题越来越引起全社会上下的广泛关注。信息安全领域必须不断提高研究水平以满足经济建设和国家安全的需要，为我国信息化建设的大踏步前进保驾护航，为创建和谐社会，实现可持续发展贡献力量。因此，大量高素质的信息安全人才成为了最急需、最宝贵的资源。

康有为曾经说过："欲任天下之事，开中国之新世界，莫亟于教育"。我们的国家要想不断发展科技，增强国力，开创出我们自己富强文明的"新世界"，必须加大力度进行信息化建设。而要使我国的信息化水平走在世界前列，全面提高信息安全领域教育水平，特别是促进高等学校信息安全专业对相关人才的培养和教育，就成为了成败的关键。高等学校信息安全系列教材的编撰就是希望能够为我国的信息安全领域专业人才的培养、为我国信息化水平的腾飞助一臂之力。

信息安全专业教育有其自身的特点，要求学习该专业的学生能够将系统知识与专业知识有机结合，在注重提升理论高度的同时还要能够把理论知识与工程实践紧密联系起来。本系列教材针对高等学校信息安全专业教育的这些特点，同时根据其知识体系、教育层次和课程设置，规划了教材的内容，增加了实际案例，力争做到既紧跟前沿技术的发展，又不失扎实的基本理论和生动活泼的形式，使学生能够学以致用。本系列教材从不同角度论述和总结了信息安全领域的科学问题，有着较强的适用性，既可作为高等学校信息安全专业和相关专业本科生的教材，也可以作为非信息安全专业的公共教科书，同时还可以作为从事信息安全工作的科研技术人员和管理人员的培训教材或参考书，使其了解信息安全相关关键技术和发展态势。

信息安全科学在不断发展，我们也将会努力使本系列教材适应和紧跟这种发展的节奏，使我们培养的信息安全人才能够与时俱进，用自己的所学共筑我国信息安全的万里长城。

限于作者的水平，本系列教材难免存在不足之处，敬请读者批评指正。

高等学校信息安全专业系列教材编委会

2008 年 10 月

前　言

在古往今来的政治军事斗争、商业竞争等活动中，人们常常希望他人不能获知或篡改某些信息，也常常需要查验信息的可信性，“信息安全”一词就是指实现以上目标的能力或状态。随着存储、处理和传输信息手段的变化和进步，信息安全面临更大挑战，它的内涵也不断延伸。当前，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为危及所存储、处理或传输的数据，或者危及由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。其中，可用性指能够保障数据和服务的正常使用；机密性指能够确保数据的传输和存储不受未授权的浏览，甚至不暴露保密通信的事实；完整性指能够确保数据是完整的，在被篡改的情况下能够发现篡改；非否认性指能够保证信息系统的操作者或信息的处理者不能否认其行为或处理结果；真实性指能够确保人、进程或系统等身份或信息、信息来源的真实；可控性指能够保证掌握和控制信息与信息系统的基本情况，可对它们的使用实施授权、审计、责任认定、传播源追踪和监管等控制。

顾名思义，信息安全技术是指保障信息安全的技术，它主要包括对信息的伪装、验证和对信息系统的保护等方面。信息安全技术由来已久，相关内容较多地出现在了古代东、西方的文字记载中，但它仅在第二次世界大战以后才获得了长足的发展，由主要依靠经验、技艺逐步转变为主要依靠科学，因此，信息安全是一个古老而又年轻的科学技术领域。当前，随着社会信息化程度的提高，许多国家和地区采取了有力的措施推进信息安全技术与相关技术的发展，信息安全的研究与开发显得更加活跃，人们关心的信息安全问题已经从早期的机密性扩大到以上全部 6 个属性，形成了较为复杂的信息安全技术体系。信息安全技术主要包括以下 5 类：核心基础安全技术（包括密码技术、信息隐藏技术等）、安全基础设施技术（包括标识与认证技术、授权与访问控制技术等）、基础设施安全技术（包括主机系统安全技术、网络系统安全技术等）、应用安全技术（包括网络与系统攻击技术、网络与系统安全防护与应急响应技术、安全审计与责任认定技术、恶意代码检测与防范技术、内容安全技术等）、支撑安全技术（包括信息安全测评技术、信息安全管理技术等）。

由于信息安全面临的问题较多，在方法上涉及数学、物理、微电子、通信、计算机等众多领域，有着覆盖面广的技术体系和丰富的科学内涵，因此要全面阐述、把握它并非易

事。尤其是，随着信息技术的发展，近十年来信息安全技术体系发生了一些较显著的变化，因此，它的概貌也有必要得到新的描述。为了帮助在校学生、相关研究人员和感兴趣的读者全面了解信息安全技术的基本原理、方法及各项技术之间的关系，本书概括地介绍了主要的信息安全技术，依次为密码技术、标识与认证技术、授权与访问控制技术、信息隐藏技术、网络与系统攻击技术、网络与系统安全防护与应急响应技术、安全审计与责任认定技术、主机系统安全技术、网络系统安全技术、恶意代码检测与防范技术、内容安全技术、信息安全测评技术、信息安全管理技术，所介绍的内容涉及这些技术的基本术语与概念、发展历史与发展趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制、基本实现方法等方面。本书每章配有论述与思考题，以供巩固之用。

本书是作者在长期从事科研与教学的基础上编写的。本书的编写得到了国家自然科学基金项目（编号：60673083、60573049）的支持。在一些内容的讨论和数据、参考资料的提供方面，编写工作也得到了信息安全国家重点实验室相关科研、教学人员和研究生的帮助，他们包括吴文玲研究员、连一峰副研究员、苏璞睿副研究员、张立武高工、张敏高工和博士生夏冰冰、邓艺、王蕊等，作者在此一并向他们表示感谢。

作者感谢本书的审核专家蔡吉人院士提出的建设性和指导性意见，还要感谢电子工业出版社的刘宪兰编辑在本书成稿过程中给予的各种支持和帮助。

作者希望本书的出版能为信息安全技术与观念在我国的普及尽微薄之力！

作　　者

2008 年 12 月 31 日

目　　录

第1章 绪　论

盗“天火”的普罗米修斯

无恃其不来，恃吾有以待也；无恃其不攻，恃吾有所不可攻也。

——《孙子兵法》

内容提要

信息安全在古代就已经受到了学者、军事家和政治家的重视。当前，随着社会信息化程度的提高，信息安全面临诸多挑战，因此信息安全的研究与开发显得更加活跃，许多国家和地区采取了有力的措施推进信息安全技术与相关技术的发展。信息安全面临的问题较多，在方法上涉及数学、物理、微电子、通信、计算机等众多领域，有着系统的技术体系和丰富的科学内涵，要全面地把握它并非易事。本章主要介绍信息安全的基本概念和发展历程，并从信息安全威胁和需求分析中，引出信息安全技术体系的基本框架和网络环境下的信息安全模型。

本章重点

- 信息安全的基本概念和发展历程
- 信息安全威胁和需求
- 信息安全技术体系
- 网络环境下的信息安全模型

1.1 什么是信息安全

信息安全问题在人类社会发展中从古至今都存在。在政治军事斗争、商业竞争甚至个人隐私保护等活动中，人们常常希望他人不能获知或篡改某些信息，并且也常常需要查验所获得信息的可信性。普通意义上的信息安全是指实现以上目标的能力或状态。例如，人们在工作中常提到：系统的信息安全怎样、有没有信息安全保障等。信息安全自古以来一直受到人们的重视。我国春秋时代的军事家孙武（公元前 535 年—不详）在《孙子兵法》中写道："能而示之不能，用而示之不用，近而示之远，远而示之近。"这显示了孙武对军事信息保密的重视。古罗马统治者 Caesar（公元前 100 年—公元前 44 年）曾使用字符替换的方法传递情报，例如，将 a、b、c 等分别用 F、G、H 等来表示，这反映了他对通信安全的重视。随着人类存储、处理和传输信息方式的变化和进步，信息安全的内涵在不断延伸。当前，在信息技术获得迅猛发展和广泛应用的情况下，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据或由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。以上这 6 个属性刻画了信息安全的基本特征和需求，被普遍认为是信息安全的基本属性[1][2]，其具体含义如下。

（1）可用性（Availability）。即使在突发事件下，依然能够保障数据和服务的正常使用，如网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等。

（2）机密性（Confidentiality）。能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

（3）完整性（Integrity）。能够保障被传输、接收或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或者篡改的位置。

（4）非否认性（Non-repudiation）。能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

（5）真实性（Authenticity）。真实性也称可认证性，能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。

（6）可控性（Controllability）。能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制。

1.2 信息安全发展历程

顾名思义，信息安全技术是指保障信息安全的技术，具体来说，它包括对信息的伪

装、验证及对信息系统的保护等方面。由于对信息和信息系统的保护与攻击在技术上是紧密关联的，因此，对受保护信息或信息系统的攻击、分析和安全测评技术也都是信息安全技术的有机组成部分。另外，为了达到信息安全目的，一般需要对人或物进行相应的组织和管理，其中也包含一些非技术的成分。

虽然信息安全技术由来已久，但仅在第二次世界大战以后它才获得了长足的发展，由主要依靠经验、技艺逐步转变为主要依靠科学，因此，信息安全是一个古老而又年轻的科学技术领域。纵观它的发展，可以将其划分为以下四个阶段[3]。

1）通信安全发展时期

从古代至 20 世纪 60 年代中期，人们更关心信息在传输中的机密性。最初，人们仅以实物或特殊符号传递机密信息，后来出现了一些朴素的信息伪装方法。在我国北宋年间，曾公亮（999 年—1078 年）与丁度（990 年—1053 年）合著的《武经总要》反映了北宋军队对军令的伪装方法，按现在的观点，它综合了基于密码本的加密和基于文本的信息隐藏：先将全部 40 条军令编号并汇成码本，以 40 字诗对应位置上的文字代表相应编号，在通信中，代表某编号的文字被隐藏在一个普通文件中，但接收方知道它的位置，这样可以通过查找该字在 40 字诗中的位置获得编号，再通过码本获得军令。在古代欧洲，代换密码和隐写术得到了较多的研究和使用[4]。德国学者 Trithemius（1462 年—1516 年）于 1518 年出版的《多表加密》（Polygraphia）记载了当时欧洲的多表加密方法，该书被认为是密码学最早的专著，它反映了当时欧洲在代换密码的研究上已经从单表、单字符代换发展到了多表、多字符代换；Trithemius 于 1499 年还完成了世界上第一部信息隐藏的专著——《隐写术》（Steganographia），但该书于 1606 年才得以出版，它记载了古代欧洲人在文本中进行信息隐藏的方法。自 19 世纪 40 年代发明电报后，安全通信主要面向保护电文的机密性，密码技术成为获得机密性的核心技术[4]。在两次世界大战中，各发达国家均研制了自己的密码算法和密码机，如二战中的德国的 ENIGMA 密码机、日本的 PURPLE 密码机与美国的 ECM 密码机，但当时的密码技术本身并未摆脱主要依靠经验的设计方法，并且由于在技术上没有安全的密钥或码本分发方法，在两次世界大战中有大量的密码通信被破解。以上密码被普遍称为古典密码。1949 年，Shannon 发表论文“保密系统的信息理论”[5]，提出了著名的 Shannon 保密通信模型，明确了密码设计者需要考虑的问题，并用信息论阐述了保密通信的原则，这为对称密码学建立了理论基础，从此密码学发展成为一门科学。

2）计算机安全发展时期

计算机安全发展时期跨越 20 世纪 60 年代中期至 80 年代中期。计算机的出现是 20 世纪的重大事件，它深刻改变了人类处理和使用信息的方法，也使信息安全包括了计算机和信息系统的安全。20 世纪 60 年代出现了多用户操作系统，由于需要解决安全共享问题，人们对信息安全的关注扩大为“机密性、访问控制与认证”，但逐渐注意到保障可用性。1965—1969 年，美国军方和科研机构组织开展了有关操作系统安全的研究。