PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全“十一五”规划教材

信息安全概论

XINXI ANQUAN GAILUN

郝玉洁　刘贵松
秦　科　晏　华　编著
秦志光　主审

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全"十一五"规划教材

信息安全概论

郝玉洁　刘贵松　秦　科　晏　华　编著

秦志光　主审

电子科技大学出版社

图书在版编目（CIP）数据

信息安全概论/郝玉洁等编著. —成都：电子科技大学出版社，2007.8

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-221-1

Ⅰ. 信… Ⅱ. 郝… 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（2007）第 124448 号

内 容 提 要

本书为普通高等学校信息安全“十一五”规划教材之一，内容丰富，涵盖了当前在信息安全领域的主要研究内容，是信息安全专业的入门教材。主要包括：计算机系统实体安全、密码学基础与应用、系统与网络安全、病毒防御技术等领域的基础知识。每章的习题可帮助初学者了解信息安全领域的全貌，掌握基本的计算机安全技术。

本书既可以作为信息安全或计算机专业的本科生、研究生教材，也可以作为相关领域专业技术人员的参考用书。

普通高等学校信息安全“十一五”规划教材

信息安全概论

郝玉洁 刘贵松 秦 科 晏 华 编著

秦志光 主审

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：曾　艺

责任编辑：曾　艺

主　　页：www.uestcp.com.cn

电子邮件：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都蜀通印务有限责任公司

成品尺寸：185mm×260mm　　印张　19　字数　463　千字

版　　次：2007 年 8 月第一版

印　　次：2007 年 8 月第一次印刷

书　　号：ISBN 978-7-81114-221-1

定　　价：30.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

秦志光　李建平　周明天

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由8本理论教材和2本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。

唐远炎

二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际IEEE SMC机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际SCI检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际SCI检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

随着我国社会信息化进程的发展，计算机网络及信息系统在社会生活中的作用越来越重要，在政府机构、企事业单位及社会团体中的影响也越来越明显。信息化水平的提高标志着社会的进步和发展，极大地方便了人们的学习、工作、生活，也带来了巨大的发展机遇，但由于信息系统本身的脆弱性和日益呈现的复杂性，信息安全的问题不断暴露，不仅涉及了个人隐私，也对整个国家的安全与公民的利益产生了极大的威胁，因此，信息安全问题已经成为整个社会关注的重点之一，在这个大环境之下，信息安全专业人士的社会需求量也逐年增加。为了满足社会需求，我们撰写的《信息安全概论》教材本着培养信息安全专业人才为目标，是信息安全或计算机专业了解和学习信息安全理论与技术的入门教材。

本教材分十一章，第一章概括介绍了信息安全目前的研究内容、典型的信息安全模型和信息安全体系结构，介绍了国内外信息安全的标准化发展情况。第二章主要介绍了计算机实体的安全保护措施，如可靠与容错的技术、防止电磁干扰的技术等。其主要目的是通过环境和实体的安全技术达到计算机系统的物理安全。第三章密码学概论是信息安全技术的基础，教材中后续章节的安全实用技术都是密码技术的应用与发展。因此，在第三章中，我们以密码学发展的过程为线索，介绍了古典与现代的密码学算法思想以及应用这些思想的软硬件加密技术。第四、五、六章是密码学思想的应用成果，主要是消息认证、数字签名、访问控制与身份认证技术，是实现操作系统安全和数据完整性的首选技术，是保证主机安全的主要手段。第七章 PKI 技术也称为公共密钥基础设施，它以非对称密钥技术为基础，以数字证书为媒介，为用户建立起一个安全、可信的网络环境，是目前为止既能实现用户身份认证，又能保证互联网上所传输数据安全的唯一技术。本章重点介绍了 PKI 的体系结构、证书机制以及认证过程等。第八章介绍了操作系统安全机制，主要是内存保护机制、文件保护机制、恶意病毒防御机制与安全操作系统设计的基本思想。第九章介绍了计算机软件安全技术思想。第十章专门介绍了计算机病毒的分类、特点，通过对计算机病毒的一些典型案例的分析，建立计算机病毒的常规防御技术。第十一章重点介绍了网络安全的常规技术、防御与攻击技术、入侵检测技术等。

全书由郝玉洁、刘贵松、秦科、晏华共同编著完成。在教材的撰写中，作者力求以通俗的语言将自己在教学一线的多年积累展示给读者，使读者学习之余能有更多的收获，了解信息安全的思想和设计技术，以指导今后的工作。

由于作者水平有限，书中难免有各种错误和问题，恳请读者谅解，也希望专家和读者批评指正。

郝玉洁

2007 年 3 月

目录

第 1 章　概述

第 2 章　计算机系统的实体安全

第 3 章 密码学概论

第 4 章 消息认证与数字签名

第 5 章 身份认证

第 6 章 访问控制

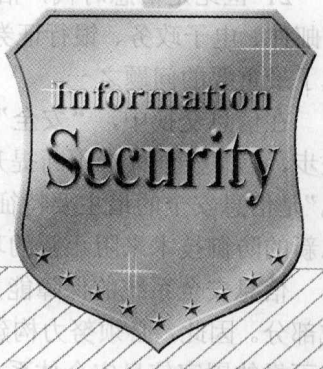
第 7 章 PKI 技术

第 8 章 计算机操作系统的安全

第 9 章　计算机软件安全性

第 10 章　计算机安全与恶意程序

第 11 章 网络安全



第1章

概　述

信息安全技术是一门综合交叉学科，它要综合利用数学、物理、通信和计算机诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、完整的、协同的解决方案。涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络内信息的保护方法以实现系统内信息的安全、保密、真实和完整。随着信息技术的发展与应用，信息安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

21 世纪是信息时代，信息的传递在人们日常生活中变得非常重要。如：电子商务、电子邮件、电子政务、银行证券等，无时无刻不在影响着人们的生活。这样信息安全问题也就成了最重要的问题之一。

在信息交换中，“安全”是相对的，而“不安全”是绝对的，随着社会的发展和技术的进步，信息安全标准不断提升，因此信息安全问题永远是一个全新的问题。“发展”和“变化”是信息安全的最主要特征，只有紧紧抓住这个特征才能正确地处理和对待信息安全问题，以新的防御技术来阻止新的攻击方法。

信息安全系统的保障能力是 21 世纪综合国力、经济竞争实力和民族生存能力的重要组成部分。因此，必须努力构建一个建立在自主研究开发基础之上的技术先进、管理高效、安全可靠的国家信息安全体系，以有效地保障国家的安全、社会的稳定和经济的发展。

1.1 信息安全的目标

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，使信息服务不中断。 也可以说，所谓信息安全，一般是指在信息采集、存储、处理、传播和运用过程中，信息的自由性、秘密性、完整性、共享性等都能得到良好保护的一种状态。这两种对信息安全的定义，目标是保持一致的，但侧重点不同，前者注重动态的特性，后者注重的是静态的特性。

早期计算机网络的作用，是共享数据并促进大学、政府研究和开发机构、军事部门的科学研究工作。那时制定的网络协议，几乎没有注意到安全性问题。在人们眼里，网络是十分安全可靠的，没有人会受到任何伤害，因为许可进入网络的单位都被认定为可靠的和可以信赖的，并且已经参与研究和共享数据，大家在网络中都得各种服务。然而，当 1991 年美国国家科学基金会（NSF）取消了互联网上不允许商业活动的限制后，越来越多的公司、企业、商业机构、银行和个人进入互联网络，利用其资源和服务进行商业活动，网络安全问题就凸现出来。每个厂商都有一些不能为外人或竞争者知道的信息和数据，如特定的单证、交易金额、销售计划、客户名单等，他们不希望外部用户访问这些信息和数据。但是，计算机窃贼或破坏者却千方百计闯入互联网络和主计算机，盗用数据、破坏资源、制造事端。有时，善意的用户也可能会在网络中偶然获取到厂商暴露的信息和数据，尤其是在某些计算机系统缺乏安全保障措施时，计算机网络安全技术应运而生，以满足这种发展中的需要，使得网络用户在获取同全球网络连接的好处的同时，保证其专用信息及资产的安全。

在因特网大规模普及之后，特别是在电子商务活动逐渐进入实用阶段之后，网络信息安

全更是引起人们的高度重视。网络交易需要大量的信息，包括商品生产和供应信息（商品的产地、产量、质量、品种、规格、价格等）；商品需求信息（消费者的个人情况、购买倾向、购买力的增减、消费水平和结构的变化等）；商品竞争信息（同行业竞购和竞销能力、新产品开发、价格策略、促销策略、销售渠道等）；财务信息（价格撮合、收支款项、支付方式等）；市场环境信息（政治状况、经济状况、自然条件特别是自然灾害的变化等）。这些信息通过合同、货单、文件、财务核算、凭证、标准、条例等形式在买卖双方以及有关各方之间不断传递。为保证整个交易过程的顺利完成，必须保证上述信息的完整性、准确性和不可修改性。由于网络交易信息是在因特网上传递的，因此，相对于传统交易来说，网络交易对信息安全提出了更高、更苛刻的要求。

危及网络信息安全的因素主要来自两个方面。一是由于网络设计和网络管理方面的原因，无意间造成机密数据暴露；二是攻击者采用不正当的手段通过网络（包括截取用户正在传输的数据和远程进入用户的系统）获得数据。对于前者，应当结合整个网络系统的设计，进一步提高系统的可靠性；对于后者，则应从数据安全的角度着手，采取相应的安全措施，达到保护数据安全的目的。

一个良好的网络安全系统，不仅应当能够防范恶意的无关人员，而且，应当能够防止专有数据和服务程序的偶然泄露，同时不需要内部用户都成为安全专家。设置这样一个系统，用户才能够在其内部资源得到保护的安全环境下，享受访问公用网络的好处。

1.2 信息安全的研究内容

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性、可控性和占有性的相关技术和理论都属于信息安全的研究领域。这些内容的具体要求是：

（1）保密性　确保信息不暴露给未授权的实体或进程。保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

（2）完整性　是指信息在存储或传输时不被修改、破坏，不出现信息包的丢失、错位等，即不能被未授权的第三方修改。完整性要求只有得到允许的人才能修改数据，并且能够辨别数据是否已被修改，它是信息安全的基本要求。破坏信息的完整性是影响信息安全的常用手段，因此，要保证数据的一致性，就必须防止数据被非法用户篡改。

（3）可用性　包括对静态信息的可得到和可操作性及对动态信息内容的可见性。可用性要求得到授权的实体在需要时可以方便地访问数据，而使攻击者不能占用所有资源去阻碍授权者的工作。它保证合法用户对信息和资源的使用不会被不正当地拒绝，需要的服务可以满足。

（4）真实性　是指信息的可信度，主要是指对信息所有者或发送者的身份的确认，对信息的来源进行判断，对伪造来源的信息予以鉴别。

（5）实用性　是指信息加密的密钥不可丢失（不是泄密）。因为丢失了密钥的信息也就丢失了信息的实用性，成为垃圾。

（6）占有性　是指存储信息的节点、磁盘等信息载体被盗用，导致对信息的占用权的丧失。

（7）可控性　可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。

（8）可审查性　对出现的网络安全问题提供调查的依据和手段。

目前，在信息安全领域人们关注的焦点主要集中在以下几个方面：

①密码理论与技术；

②安全协议理论与技术；

③安全体系结构理论与技术；

④信息对抗理论与技术；

⑤网络安全与安全产品。

1.2.1 密码理论与技术

密码技术是信息安全的核心技术。如今，计算机网络环境下信息的保密性、完整性、可用性和抗抵赖性，都需要采用密码技术来解决和保证。密码体制分为对称密码（又称为私钥密码）和非对称密码（又称为公钥密码）两种。公钥密码在信息安全中担负起密钥协商、数字签名、消息认证等重要角色，已成为最核心的密码体制。

当前，公钥密码的安全性概念已经被大大扩展了。像著名的 RSA 公钥密码算法、Rabin 公钥密码算法和 ElGamal 公钥密码算法都已经得到了广泛应用。但是，有些公钥密码算法在理论上是安全的，可是在实际应用中并非安全。因为在实际应用中不仅需要算法本身在数学证明上是安全的，同时也需要算法在实际应用中也是安全的。比如，公钥加密算法根据不同的应用，需要考虑选择明文安全、非适应性选择密文安全和适应性选择密码安全三类。数字签名根据需要也要求考虑抵抗非消息攻击和选择消息攻击等。因此，近年来，公钥密码学研究中的一个重要内容——可证安全密码学正是致力于这方面的研究。

公钥密码在信息安全中担负起密钥协商、数字签名、消息认证等重要角色，已成为最核心的密码。目前密码的核心课题主要是在结合具体的网络环境、提高运算效率的基础上，针对各种主动攻击行为，研究各种可证安全体制。其中引人注目的是基于身份（ID）密码体制和密码体制的可证安全模型研究，目前已经取得了重要成果。这些成果对网络安全、信息安全的影响非常巨大，例如公钥基础设施（PKI）将会更趋于合理。在密码分析和攻击手段不断进步、计算机运算速度不断提高以及密码应用需求不断增长的情况下，迫切需要发展密码理论和创新密码算法。

当前，密码学发展面临着挑战和机遇。计算机网络通信技术的发展和信息时代的到来，为密码学提供了前所未有的发展机遇。在密码理论、密码技术、密码保障、密码管理等方面进行创造性思维，去开辟密码学发展的新纪元是我们的追求所在。

1.2.2 安全协议理论与技术

安全协议的建立和完善是安全保密系统走上规范化、标准化道路的基本因素。一个较为完善的内部网和安全保密系统，至少要实现加密机制、验证机制和保护机制。

安全协议的研究主要包括两方面内容，即安全协议的安全性分析方法研究和各种实用安全协议的设计与分析研究。安全协议的安全性分析方法主要有两类，一类是攻击检验方法，一类是形式化分析方法，其中安全协议的形式化分析方法是安全协议研究中最关键的研究问题之一，它的研究始于20世纪80年代初，目前正处于百花齐放、充满活力的状态之中。许多一流大学和公司的介入，使这一领域成为研究热点。随着各种有效方法及思想的不断涌现，这一领域在理论上正在走向成熟。

从大的方面讲，在协议形式化分析方面比较成功的研究思路可以分为三种：第一种思路是基于推理知识和信念的模态逻辑；第二种思路是基于状态搜索工具和定理证明技术；第三种思路是基于新的协议模型发展证明正确性理论。目前，已经提出了大量的实用安全协议，具有代表性的有：电子商务协议、IPSec协议、TLS协议、简单网络管理协议（SNMP）、PGP协议、PEM协议、S-HTTP协议、S/MIME协议等。实用安全协议的安全性分析特别是电子商务协议、IPSec协议、TLS协议是当前协议研究中的另一个热点。

典型的电子商务协议有SET协议、iKP协议等。另外，值得注意的是Kailar逻辑，它是目前分析电子商务协议的最有效的一种形式化方法。

为了实现安全IP，Internet工程任务组IETF于1994年开始了一项IP安全工程，专门成立了IP安全协议工作组IPSEC，来制定和推动一套称为IPSec的IP安全协议标准。其目标就是把安全集成到IP层，以便对Internet的安全业务提供底层的支持。IETF于1995年8月公布了一系列关于IPSec的建议标准。IPSec适用于IPv4和下一代IP协议IPv6，并且是IPv6自身必备的安全机制。但由于IPSec还比较新，正处于研究发展和完善阶段。

在安全协议的研究中，除理论研究外，实用安全协议研究的总趋势是走向标准化。我国学者虽然在理论研究方面和目前已有协议的分析方面做了一些工作，但在实际应用方面与国际先进水平相比还有一定的差距，当然，这主要是由于我国的信息化进程落后于发达国家的原因。

1.2.3 安全体系结构理论与技术

安全体系结构理论与技术主要包括：安全体系模型的建立及其形式化描述与分析，安全策略和机制的研究，检验和评估系统安全性的科学方法和准则的建立，符合这些模型、策略和准则的系统的研制（比如安全操作系统，安全数据库系统等）。

20世纪80年代中期，美国国防部为适应军事计算机的保密需要，在20世纪70年代的基础理论研究成果计算机保密模型（Bell&La padula模型）的基础上，制订了“可信计算机系统安全评价准则”（TCSEC），其后又对网络系统、数据库等方面作出了系列安全解释，形成了安全信息系统体系结构的最早原则。至今美国已研制出符合TCSEC要求的安全系统（包括安全操作系统、安全数据库、安全网络部件）多达100多种，但这些系统仍有局限性，还没有真正达到形式化描述和证明的最高级安全系统。20世纪90年代初，英、法、德、荷四国针对TCSEC准则只考虑保密性的局限，联合提出了包括保密性、完整性、可用性概念的“信息技术安全评价准则”（ITSEC），但是该准则中并没有给出综合解决以上问题的理论模型和方案。近年来六国七方（美国国家安全局和国家技术标准研究所、加、英、法、德、