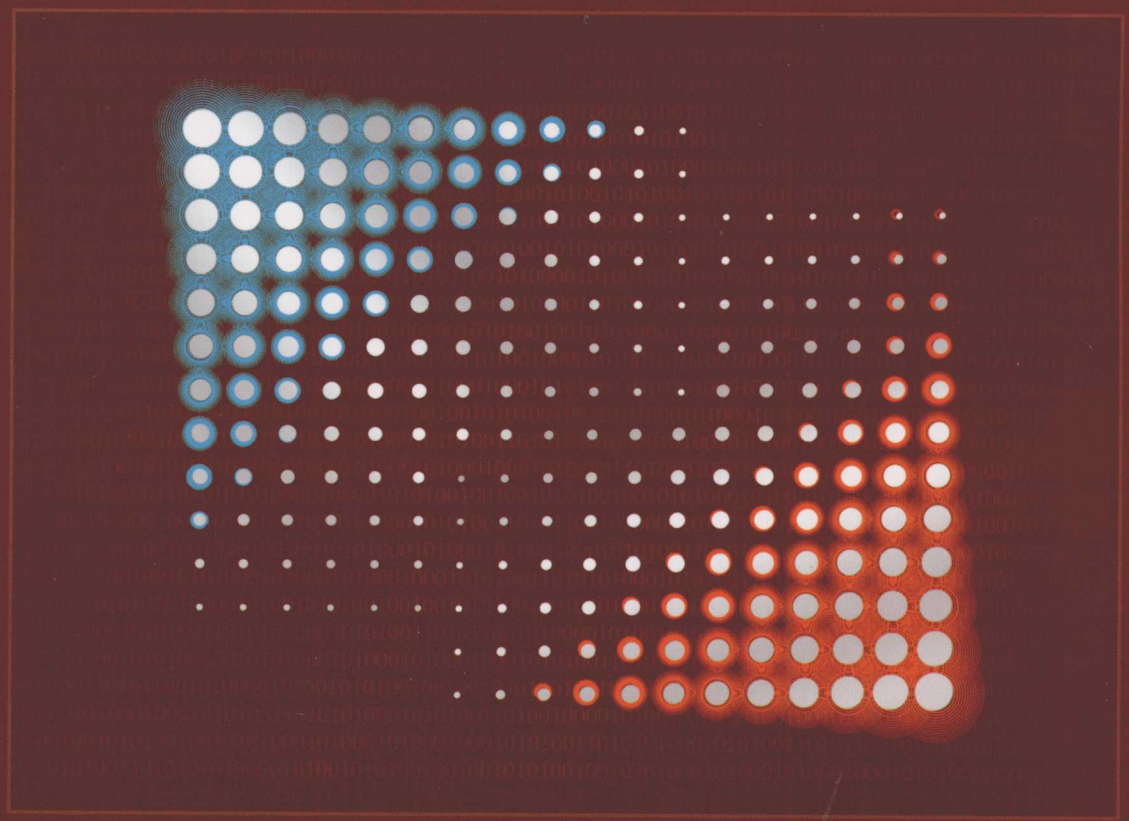
新编计算机类本科规划教材

网络信息安全

蒋天发 编著　　周迪勋 主审



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

新编计算机类本科规划教材

网络信息安全

蒋天发　编著
周迪勋　主审

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

内 容 简 介

本书重点阐述网络信息安全的基础理论和基础知识，侧重论述安全技术的选择策略，安全保密的构建方法和实现技能。本书共14章，主要内容包括：网络信息安全概论、物理安全与Internet服务安全、网络信息密码技术、数字签名与认证技术、网络安全协议、无线网络安全机制、网络信息的访问控制与防火墙技术、入侵检测技术、网络数据库安全与备份技术、病毒防范技术、远程控制与黑客入侵、信息隐藏与数字水印技术、网络安全测试工具及其应用、网络信息安全实验及实训指导等。本书配有免费电子教学课件。

本书内容丰富，结构合理，可作为普通高等院校和高等职业技术学校信息安全、计算机及相关专业课程的教材，也可供从事网络信息安全方面工作的工程技术人员参考。

图书在版编目(CIP)数据

网络信息安全/蒋天发编著.—北京：电子工业出版社，2009.1
新编计算机类本科规划教材
ISBN 978-7-121-07882-8

I. 网… II. 蒋… III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆CIP数据核字(2008)第184000号

责任编辑：王 纲
印 刷：北京季蜂印刷有限公司
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：20.25 字数：518.4千字
印 次：2009年1月第1次印刷
印 数：4000册 定价：29.50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。

前　言

计算机网络应用的发展和普及，给人们的生活与学习方式、生产方式和思维方式带来了巨大的变化，将人类带入到信息化与网络化时代，而网络信息安全的重要性日益突出。网络信息安全不仅影响到网络信息社会的个人生活，而且也影响到电子商务、电子现金支付、数字货币、网络银行、网上证券、电子政务等政治和经济活动。针对这种情况，大多数高等院校都开设了网络信息安全方面的课程。

在2005年，为了贯彻落实教育部《关于进一步加强信息安全学科、专业建设和人才培养工作的意见》（教高[2005]7号）文件精神，加快信息安全学科与教材建设，促进网络信息安全人才的培养，作者根据自己的教学经验和科研成果，编写了《网络信息安全》讲义，并在本校2004级、2005级和2006级本科教学中进行使用，每次学生选修“网络信息安全”课程的人数都达到或超过了学校教务处规定160人，这说明使用《网络信息安全》讲义的效果很好。现在，在《网络信息安全》讲义基础上，针对普通高等院校和高等职业技术学校信息安全、计算机及相关专业课程的教学特点，将相关理论、专业知识与工程技术相结合，编写了《网络信息安全》这本书。本书力求紧跟国内网络信息安全技术的前沿领域，全面、通俗、系统反映网络信息安全的理论和实践。

全书共分14章，主要内容包括：网络信息安全概论、物理安全与Internet服务安全、网络信息密码技术、数字签名与认证技术、网络安全协议、无线网络安全机制、网络信息的访问控制与防火墙技术、入侵检测技术、网络数据库安全与备份技术、病毒防范技术、远程控制与黑客入侵、信息隐藏与数字水印技术、网络安全测试工具及其应用、网络信息安全实验及实训指导等。全书内容丰富，结构合理，可以作为普通高等院校和高等职业技术学校信息安全、计算机及相关专业课程的教材，也可供从事网络信息安全方面工作的工程技术人员参考。

本书由中南民族大学计算机科学学院蒋天发教授编著，武汉理工大学（原网络中心主任）周迪勋教授主审。作者已主持、参加和完成国家自然科学基金项目（编号：40571128）和国家民委重点科研项目（编号：MZY02004）等10项，已将其部分科研成果总结编入本书内容，所以本书是网络信息安全课题组全体成员多年来集体智慧的结晶。参加本书编写与整理工作还有作者在读的硕士研究生王理（访问控制与防火墙）、黄芳（网络安全协议）、张继华（无线网络安全）、李招钗（入侵检测）、张一帆（密码学与网络数据库安全）、李杨（物理安全与病毒防治）、熊祥光（数字签名与认证）、刘永奎（远程控制与黑客入侵）、彭欢（网络安全测试）、周立（实训指导）、腾召荣（实训指导）。还编入了已毕业的研究生柳春华（基于MA的入侵检测）、王强（误用检测）、王涛（网络视频传输安全）、柳晶（基于DCT视频水印）、何淼（基于置乱图像水印）、曹文波（基于混沌图像水印）与博士生彭川（基于离散余弦变换图像水印）的在校研究成果，以及课题合作者武汉理工大学崔巍（教授）、中南民族大学计算机科学学院的雷建云（副教授）、熊志勇（副教授）、贴军（副教授）、周熠（副教授）、何秉娇（副教授）、姜卓睿（讲师）的研究成果。在本书编写过程中，还得到了中南民族大学计算机科学学院孟博（信息安全博士后）、中国软件评测中心（CSTC）蒋巍（网络与硬件评测工程师）和电子工业出版社段丹辉（策划编辑）的指导与帮助。

在本书的策划和编写过程中，参阅了国内外有关的大量文献和资料（包括网站），从其中得到启示；同时也得到了中南民族大学有关领导、同事、朋友及学生的大力支持与帮助。在此致以衷心的感谢！

由于网络信息安全的技术发展非常快，本书的选材和编写还有一些不尽如人意的地方，加上笔者学识水平和时间所限，书中难免存在缺点和谬误，敬请同行专家及读者指正，以便进一步完善提高。作者联系方式：jkx89jtf@scuec.edu.cn。

编　者

目　录

第1章　网络信息安全概论

本章提要

本章首先阐述网络信息安全的重要意义，指出信息安全是国家安全的重要基础；然后简要介绍本课程的主要内容：物理安全与 Internet 安全、网络信息密码技术、数字签名与认证技术、网络安全协议、无线网络安全机制、网络信息的访问控制与防火墙技术、入侵检测技术、网络数据库安全与备份技术、病毒防范技术、远程控制与黑客入侵、信息隐藏与数字水印技术、网络安全测试工具及其应用，以及网络信息安全实验及实训指导；最后从社会学科的角度讨论网络信息安全中的非技术因素。

1.1　网络信息安全的重要意义

21 世纪是知识经济时代，网络化、信息化已成为现代社会的一个重要特征。在这个新时代里，网络信息与我们息息相关。网络信息安全是一个涉及网络技术、通信技术、密码技术、信息安全技术、计算机科学、应用数学、信息论等多种学科的边缘性综合学科。网络信息安全是国家安全的重要基础，因为网络信息在国民经济建设、社会发展、国防和科学研究等领域的作用日益重要。实际上，网络的快速普及与发展、客户端软件多媒体化、协同计算、资源共享与开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。确保网络信息安全至关重要，没有网络信息的安全就谈不上网络信息的应用。当今，由于计算机互联网络的迅速发展和广泛应用，打破了传统的时间和空间的局限性，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。计算机网络和通信是促进信息化社会发展的最活跃的因素。然而，任何事物的发展都具有两重性。由于计算机互联网络的国际化、社会化、开放化、个性化的特点，使得它在向人们提供网络信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。网络信息安全问题已威胁到国家的政治、经济和国防等领域。这是因为对互联网络的非法侵入或人为的故意破坏，将会轻而易举地改变互联网络上的应用系统或导致网络瘫痪，从而使得网络用户在军事、经济、政治上造成无法弥补的巨大损失。因此，很早就有人提出了“信息战”的概念，并将信息武器列为继原子武器、生物武器和化学武器之后的第四大武器。网络信息的泄漏、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等对网络信息安全已构成重大威胁。如果这些问题不解决，国家安全就会受到威胁，电子政务、电子商务、网络银行、网络科研、远程教育和远程医疗等都将无法正常开展，个人的隐私也得不到保障。

计算机网络的广泛应用已经对经济、文化、教育、科技的发展产生了重要影响，许多重要的信息、资源都与网络相关。客观上，几乎没有一个网络能够免受安全问题的困扰。依据 Financial Times 曾经做过的统计，平均每 20 秒就有一个网络遭到入侵，而安全又是网络发展的根本。网络信息安全是近 20 年来特别是近几年来迅速发展起来的新兴学科，由于其战略地位十分重要，各国都给予了极大的关注和投入。我国网络信息安全研究在这些年来取得了长足的进步，但是由于起步较晚、投入不足、研究力量分散，总体来说与发达国家相比还存在着较大差距。

网络信息安全体系结构和网络安全协议的研究更是薄弱环节。面对激烈的网络信息战的对抗和冲突,面对日益增强的计算能力和人类智慧,网络信息安全理论与技术面临着空前的挑战和机遇。目前,国内外网络信息安全现状表现为以下几方面。

①普遍受到重视。计算机网络为其信息安全提供了更大的用武之地,保证网络和信息安全是进行网络应用及电子商务的基础。例如,网上订票由于转款上的问题,存在很多不便。

②政府大力扶持。各国政府关于网络信息安全的技术扶持都非常强。我国进口的信息技术没有密码技术。美国政府严格控制密码技术出口。我国严禁进口,甚至禁止国外密码产品在中国展览。我国政府已经充分意识到网络信息安全的重要性,党和国家领导人为此多次做出重要的指示。国家"973"计划、国家"863"计划和国家自然科学基金已将网络信息安全理论与技术列为"十五"期间我国高新技术的重大研究课题。

③国际网络与其信息安全产业界发展迅速。如防火墙行业发展非常迅速。

④学术活跃。学术界关于安全密码的研究非常活跃。

⑤标准化、国际化。很多电信安全协议如通信协议都有安全标准,但密码技术还没有国际标准。我们必须在吸取国外信息安全的先进管理、理论和技术的基础上,奋发努力、勇于开拓、不断创新,独立自主地发展我国的网络信息安全技术。

网络安全问题的解决,除了必要的技术手段之外,世界各国也正在寻求各种法律手段,以立法的形式强制性地建立保护网络安全的法规。我国已经出台了《中华人民共和国计算机信息系统安全保护条列》、《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》、《计算机信息系统保密管理暂行规定》、《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理的规定》、《中国教育和科研计算机网暂行管理办法》、《关于规范"网吧"经营行为加强安全管理的通知》、《关于互联网中文域名管理的通告》等法律和法规,为我国的计算机网络信息安全提供了法律的保证。我们必须从国家和民族的最高利益出发,在国家主管部门统一组织下,集中力量开展网络信息安全研究,特别要加强对网络信息安全发展战略、网络信息安全理论、密码理论和技术、网络信息安全平台、网络安全芯片、网络安全操作系统、入侵检测与反击技术、网络信息安全检测和监控技术、电磁泄漏技术及病毒防治等方面的研究,确立自主的、创新的、整体的网络信息安全理论体系,构筑我国自主的新网络信息安全系统。

1.2 网络信息安全的主要内容

现代网络技术的广泛应用大大地提高了人类活动的质量和效率,但如同许多新技术的应用一样,网络技术也是一柄人类为自己锻造的双刃剑,善意的应用将造福于人类,恶意的应用则将给社会带来危害。所以,在考虑网络信息安全的保障总体规划上,不仅要在网络信息安全技术上统筹计划,还要强调网络信息保障研究跨学科的性质;更重要的是加强网络信息安全教育与管理,强调其系统规划和责任,重视对网络信息系统使用的法律与道德规范问题,将法律、法规和各种规章制度融合到网络信息安全解决方案之中。总之,网络信息安全保障和网络信息安全的本质在于思想观念上的主动防御而不是被动保护;网络信息安全保障涉及管理、制度、人员、法律和技术等方面。因此,我们要解决网络信息安全的基本策略是综合治理。网络信息安全研究所涉及的内容相当广泛,本书侧重地对下列问题进行讨论和介绍。

1. 网络信息的物理安全

保证计算机网络信息系统中各种设备的物理安全是整个网络信息系统安全的前提，物理安全就是指以物理方法对网络信息系统的设备和线路采取安全措施与保密，即保护计算机网络设备、设施和其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误或错误而导致的破坏。物理安全历来受到广泛重视，国内外已经制定了许多标准和规范。物理安全所涉及的内容相当广泛，主要包括以下四个方面。

(1) 环境安全

环境安全是对计算机网络信息系统所在环境的安全保护，例如灾难保护和区域保护等，具体要求请参见国家标准 GB50173—93《电子计算机机房设计规范》、GB2887—89《计算站场地技术条件》、GB9361—88《计算站场地安全要求》。

(2) 媒体安全

媒体安全包括媒体数据的安全和媒体本身的安全，即指对媒体的安全保管(包括媒体的防盗、防毁、防霉和防砸等)，目的是保护存储在媒体上的信息。

(3) 设备安全

设备安全是指对计算机网络信息系统设备的安全保护，如设备防电磁信息辐射泄漏、防止线路截获、防盗、防毁、抗电磁干扰，以及电源保护等。

(4) 计算机网络临界点安全

计算机网络临界点安全包括内外网络互联的设备、防火墙、无线网络设备、VPN 设备等。

近年来，因特网安全性已成为不可忽视的首要问题。为了提高安全性，人们做了大量研究，提出了各种方案，如数据加密、数字签名、身份认证、防火墙、内容过滤等，但收效不大。总体来说，因特网不安全因素来自三个方面：外在不安全环境、缺乏系统安全标准和因特网内在特性——先天不足。上述三方面中最重要的是第三个方面，因特网设计之初的目的是提供广泛互联、互操作、资源共享，侧重点不是安全，所以它是威胁网络安全、导致网络不可信任的根本原因。

2. 网络信息密码技术

密码是网络信息安全的基础，密码技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机交叉的一门新兴学科。随着计算机网络和计算机通信技术的发展，网络信息密码技术得到了前所未有的重视并迅速地发展和普及起来。密码作为运用于军事和政治斗争的一种技术，历史悠久，无论是在古希腊时代还是在现代都发挥了非常重要的作用。现代密码学不仅用于解决信息的保密性，而且也用于解决信息的完整性、可用性、可控性和不可抵赖性等方面。可以说，密码是保护网络信息安全的最有效的手段，密码技术也是保护网络信息安全的关键技术。过去密码的研制、生产、使用和管理都是在封闭的环境下进行的。20 世纪 70 年代以来，随着经济、社会和信息技术的发展，密码应用范围日益扩大，社会对密码的需求愈加迫切，密码研究领域不断拓宽，密码研究也从专门机构扩展到社会和民间，密码技术得到了空前发展。

密码技术是保障信息安全的最基本、最核心的技术措施和理论基础。密码技术不仅在保护国家秘密信息中具有重要的、不可代替的作用，而且广泛应用于诸如电子邮件、政府信息上网、网上招生录取、网上购物、网络银行、数字化网络电视、网络远程教育、远程合作诊断等领域中。常见密码的破解方法有唯密文攻击法、已知明文攻击法和选择密文攻击法。到目前为止，已经公开发表的各种加密算法多达数百种。若以密钥为分类标准，可将密码系统分为对称密

码（又称为单钥密码或私钥密码）系统和非对称密码（又称为双钥密码或公钥密码）系统；若以密码算法对明文的处理方式为标准，则可将密码系统分为序列密码系统和分组密码系统。在私钥密码体制中，发送方和接收方使用同一个秘密密钥，即加密密钥和解密密钥是相同或等价的。除了以代换密码和转轮密码为代表的古典密码之外，比较著名的私钥密码系统有：美国的 DES(Data Encryption Standard)及其各种变形 Triple DES，GDES，NewDES，欧洲的 IDEA，日本的 FEAL-N，LOK1-91，Skipjack，RC4，RC5 等。

在公钥密码体制中，接收方和发送方使用的密钥互不相同，即加密密钥和解密密钥不相同，加密密钥公开而解密密钥保密，而且几乎不可能由加密密钥推导出解密密钥。比较著名的公钥密码系统有：RSA 密码系统、椭圆曲线密码系统 ECC、背包密码系统、McEliece 密码系统、Diffe-Hellman 密码系统、零知识证明的密码体制和 ELGamal 密码等。

在“密码管理”方面主要讨论密码的生成、空间、发送、验证、更新、存储密钥的管理机制。其中密码的生成是算法安全性的基础；非线性密钥空间可假定能将选择的算法加入到防窜改模块中，要求有特殊保密形式的密钥，从而使能偶然碰到正确密钥的可能性降低；在密钥发送时需要分成许多不同的部分，然后用不同的信道发送，即使截获者能收集到密钥，仍可保证密钥安全性；密钥验证需要根据信道类型判断是发送者传送或是其他人伪装发送者传送；密钥更新可采用从旧密钥中产生新密钥的方法改变加密数据链路的密钥。

3. 数字签名与认证技术

随着 Internet 的发展与应用的普及，一方面除了需要保护用户通信的私有性和秘密性，使非法用户不能获取、读懂通信双方的私有信息和秘密信息之外；另一方面，在许多应用中还需要保证通信双方的不可抵赖性和信息在公共信道上传输的完整性。数字签名(Digital Signatures，DS)、身份认证和信息认证等技术可以解决这些问题。

数字签名的概念最早由 Whitfield Diffie 和 Martin Hellman 于 1976 年提出，其目的是使签名者对电子文件也可以进行签名且无法否认，验证者无法篡改文件。简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。

基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、DES/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准(Digital Signature Standard，DSS)。数字签名技术是不对称加密算法的典型应用。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在公钥与私钥管理方面，数字签名应用与加密邮件 PGP(Pretty Good Privacy)技术正好相反。在数字签名应用中，发送者的公钥可以很方便地得到，但发送者的私钥则需要严格保密。

数字签名通过一套标准化、规范化的软硬结合的系统，使持章者可以在电子文件上完成签字、盖章，与传统的手写签名、盖章具有完全相同的功能。数字签名主要解决电子文件的签字盖