北京市高等教育精品教材立项项目

高等院校信息与通信工程系列教材

计算机通信信息安全技术

王景中 徐小青 编著

清华大学出版社

高等院校信息与通信工程系列教材

计算机通信信息安全技术

王景中 徐小青 编著

清华大学出版社
北 京

内容简介

本教材是作者在多次讲授计算机安全课程的基础上，参考国内外相关文献编写而成的。全书共分10章，分别介绍了计算机通信信息安全基本概念、计算机病毒、密码技术、计算机系统安全、信息安全服务、防火墙技术、安全管理与审计、信息安全协议、安全工具以及信息安全基础设施。

本教材适合于高等院校计算机科学与技术、电子信息工程、通信工程以及相关专业信息安全课程的教学，也可以作为有关工程技术人员的参考书。

图书在版编目(CIP)数据

计算机通信信息安全技术/王景中，徐小青编著. －北京：清华大学出版社，2006.3
(高等院校信息与通信工程系列教材/陈俊亮主编)
ISBN 7-302-12268-7

Ⅰ. 计…　Ⅱ. ①王… ②徐…　Ⅲ. 计算机通信－安全技术－高等学校－教材
Ⅳ. ①TN91 ②TP309

中国版本图书馆CIP数据核字(2005)第153534号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
责任编辑：陈国新
印 装 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：27.25　**字数**：642千字
版　　次：2006年3月第1版　2006年3月第1次印刷
书　　号：ISBN 7-302-12268-7/TP·8020
印　　数：1～4000
定　　价：36.00元

出版说明

信息与通信工程学科是信息科学与技术的重要组成部分。改革开放以来，我国在发展通信系统与信息系统方面取得了长足的进步，形成了巨大的产业与市场，如我国的电话网络规模已位居世界首位，同时该领域的一些分支学科出现了为国际认可的技术创新，得到了迅猛的发展。为满足国家对高层次人才的迫切需求，当前国内大量高等学校设有信息与通信工程学科的院系或专业，培养大量的本科生与研究生。为适应学科知识不断更新的发展态势，他们迫切需要内容新颖又符合教改要求的教材和教学参考书。此外，大量的科研人员与工程技术人员也迫切需要学习、了解、掌握信息与通信工程学科领域的基础理论与较为系统的前沿专业知识。为了满足这些读者对高质量图书的渴求，清华大学出版社组织国内信息与通信工程国家级重点学科的教学与科研骨干以及本领域的一些知名学者、学术带头人编写了这套高等院校信息与通信工程系列教材。

该套教材以本科电子信息工程、通信工程专业的专业必修课程教材为主，同时包含一些反映学科发展前沿的本科选修课程教材和研究生教学用书。为了保证教材的出版质量，清华大学出版社不仅约请国内一流专家参与了丛书的选题规划，而且每本书在出版前都组织全国重点高校的骨干教师对作者的编写大纲和书稿进行了认真审核。

祝愿《高等院校信息与通信工程系列教材》为我国培养与造就信息与通信工程领域的高素质科技人才，推动信息科学的发展与进步做出贡献。

北京邮电大学

陈俊亮

2004 年 9 月

前　言

随着信息时代的到来，信息安全越趋重要。计算机网络、数据通信、电子商务、办公自动化等领域都需要解决信息安全问题。社会对信息安全技术的需求也越来越迫切。为了满足社会的需要，各高等院校计算机科学与技术、通信工程以及电子信息类本科专业相继开设了有关信息安全方面的课程。为了满足本课程的需要，笔者本着内容全面、知识结构合理的原则编写了本教材。

本教材是作者在多次讲授计算机安全课程的基础上，参考国内外相关文献编写而成的。在编写过程中，力求突出重点，注重知识点结合，强调基本概念和基本方法，深入介绍安全协议。

本教材共分 10 章。第 1 章对计算机通信信息安全所涉及的基本概念、研究内容、安全服务、安全标准、安全的作用等进行了概括性的介绍，使读者通过本章的学习，对本课程所研究的内容有所了解，激发学习兴趣。第 2 章详细讲解了计算机病毒的组成结构、基本概念和基本原理，介绍了一些基本的研究方法，使读者建立基本的概念，增强对计算机病毒的认识，掌握计算机病毒的诊断方法，此外，本章还具体分析了几种病毒实例。第 3 章讲解了计算机通信信息安全所涉及的密码技术，重点介绍了对称密码体制和非对称密码体制，并且具体分析了典型的对称密码算法 DES 和典型的非对称密码算法 RSA。第 4 章讲解了计算机系统漏洞、操作系统安全、数据库系统安全以及用户程序安全，使读者了解到任何计算机软件系统都存在漏洞，在开发软件系统时，应该尽量减少漏洞，降低不安全因素的影响。第 5 章详细介绍了认证、访问控制、机密性、完整性以及不可否认性等基本的安全服务。第 6 章介绍了防火墙基本知识，重点介绍了包过滤技术和代理服务技术，并且简单介绍了 Firewall-1 等防火墙产品。第 7 章介绍了安全管理的概念和协议以及安全审计的方法，并详细介绍了入侵检测技术。第 8 章介绍了安全体系结构的概念，详细介绍了 IPSec 安全协议和 TLS 安全协议，使读者对安全协议有一个比较深入的了解。第 9 章介绍一些实用的安全工具，包括清除病毒工具、扫描工具以及入侵检测工具等。第 10 章介绍了信息安全基础设施的基本概念，简要介绍了 X.509 模式和 SPKI 模式。每一章都有小结和习题。

本书是北京市高等教育精品教材立项项目，适合作计算机科学与技术、电子信息工程、通信工程以及电子信息类本科专业信息安全相关课程的教材，也可以作为有关工程技术人员的参考书。

本教材由王景中、徐小青编写，由王景中统稿。本书编写过程中，得到了汪国洋、陈浩、赵志英、杨广华、杨志延、王艳芳、周文刚、郝斌和潘耀都的大力支持和帮助，在此表示衷心感谢。由于作者水平有限，书中难免出现不当之处，敬请读者批评指正。

编　者

2005 年 9 月

目　录

第1章 绪 论

计算机技术与通信技术的有机结合，形成了信息时代无所不在的计算机通信网络。计算机网络是两台以上具有自治功能的计算机通过传输媒体连接在一起，在通信协议的作用下，实现信息传输、信息共享和信息处理的系统集合。

计算机网络为人们的工作、学习和生活等诸多社会活动提供了十分方便、快捷的手段。特别是因特网的出现，在某种程度上使我们的社会活动发生了根本的转变。通过计算机网络，人们不出家门就能了解世界各地的新闻，浏览世界著名图书馆的图书资料，随时随地通过网络欣赏电影、音乐、电视连续剧，收集所需要的各个方面的信息；足不出户就能购买商品，管理自己的银行存款，进行股票交易，在家里完成自己的工作任务，并且随时与工作单位保持联系。计算机网络的飞速发展和应用也加快了各种新技术、新知识、新文化的传播，涉及到社会、政治、军事、经济、文化、医疗、社会保障、交通、通信、商务、生产、学习、交流和日常生活等各个领域，极大地影响着社会、团体、个人自身内部以及相互之间关系的思维方式、行为方式和观念的变化。

计算机网络为我们所提供的各种功能和帮助，都是以网络服务的形式提供的。为了提供这些服务，一方面需要完善的计算机网络基础设施，该设施由网络硬件和通信软件构成，由此构成网络服务的信息存储、处理以及传输平台，另一方面需要完善的保障体系，该体系体现计算机通信网络的信息安全特性，由它保证安全地实现信息传输、信息共享和信息处理。如果没有通信信息的安全保证，那么从计算机网络中得到的服务是非常有限的，而且其服务质量也无法保证。

从网络组成方面来讲，计算机网络由用户资源子网络和通信子网络构成。用户资源子网由用户终端以及网络接口设备构成。它主要完成信息的收与发、信息处理等功能，直接向用户提供服务。通信子网主要由信息传输媒体、传输设备、路由设备等构成，主要完成信息传输的功能。因此，这里所强调的计算机网络是一个计算机通信信息网络，它不但涉及用户终端上直接为用户提供的功能，也涉及到传输媒体、传输设备中的信息传输功能。

本书叙述的信息安全问题贯穿于整个网络的各个方面，涵盖于信息存储、处理和传输各个过程之中。

1.1 信息安全

本节首先介绍信息概念的发展，然后介绍有关信息的定义和特性，最后给出信息安全的概念。

1.1.1 信息概念的发展

信息的概念以及人们对它的认识是随着社会的发展而逐步建立起来的。在早期的人类活动中，人们对信息的认识比较模糊，对信息和消息的含义没有明确界定。到了20世纪中期以后，现代信息技术的飞速发展及其对人类社会的深刻影响，迫使人们开始探讨信息的准确含义。信息概念的形成也经历了一个较长的历史。

1928年，哈特雷(L. V. R. Hartley)将信息定义为选择通信符号的方式，并且用“选择的自由度”来计量这种信息的大小。这个定义是以具体的通信过程为依据给出的。他认为在通信过程中，任何通信系统的发信端总有一个字母表(或符号表)，发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符号序列的过程。

1948年，香农(C. E. Shannon)指出，“一个实际的消息是从可能的消息集合中选择出来的，而选择消息的发信者又是任意的，因此，这种选择就具有随机性”。他认为，通信系统所处理的信息在本质上都是随机的，因此可以运用统计方法进行处理。在此基础上他推导出信息测度的数学公式，发明了编码的三大定理，为现代通信技术的发展奠定了理论基础。

1948年，维纳(N. Wiener)以控制论为基础对信息进行定义，他把信息定义为“人们在适应外部世界，并且使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称”。他还认为，“接收信息和使用信息的过程，就是适应外部世界环境的偶然性变化的过程，也是我们在这个环境中有效地生活的过程”。维纳的信息定义包含了信息的内容与价值，表示出信息的动态特性，揭示了信息的功能与范围。

1975年，意大利学者朗高(G. Longo)提出“差异就是信息”的观点。他指出，“信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身”。目前，这个观点被普遍接受。很显然，“有差异就是信息”的观点是正确的，但是“没有差异就没有信息”的说法却不够确切。例如，我们碰到两个长得一模一样的人，他们之间看上去没有什么差异，但会马上联想到“双胞胎”这样的信息。可见，“差异就是信息”也有其局限性。

1.1.2 信息的定义

由于信息概念本身的复杂性、发展的曲折性以及应用的广泛性，目前仍然没有统一的定义。在当今的信息社会，信息渗透到这个社会的各个领域、各个行业以及我们日常生活的各个角落。在不同的领域，对信息有着不同的定义，信息的定义多达上百种，它们都从不同角度、不同层次揭示了信息的特征与性质，但也都有这样或那样的局限性。信息作为物质世界的三大组成要素之一，其定义的适用范围是非常宽的。

在通信领域对信息的研究有着悠久的历史，人们普遍接受的信息定义是，信息是事物运动的状态与方式，是事物的一种属性。信息科学是通信理论研究的最重要的内容之一。在通信领域，主要涉及到电路、信号、消息与系统，其实它们都是信息的载体。信息不同于消息，消息只是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息

可以用文字或图像来表述。信息不同于情报，情报通常是揭示秘密的、专门的、新颖的一类信息；可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是逻辑化的信息，并非所有的信息都是知识。

1.1.3 信息的性质

信息是高度抽象的，我们可以把信息的性质描述为，信息来源于物质，但不是物质本身；信息也来源于精神世界，但又不限于精神的领域。信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，它们主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共事性、可传递性、可变换性、可转化性和可伪性等。

1.1.4 信息的功能

我们说信息具有一般物质的属性，它的功能就是信息属性的体现。相对于信息的本质属性和一般属性，信息的功能也可分为两类。第一类功能是信息的基本功能，用于维持和强化世界的有序性；第二类功能是信息的社会功能，表现为维系社会的生存，促进人类文明的进步和人类自身的发展。具体来看，信息的功能主要表现在以下五个方面。

第一，信息是宇宙万物有序运行的内在依据。信息源于物质的运动，早在生命现象出现之前，自然界中无机物之间、无机物及其周围环境之间就存在着相互作用，存在着运动、变化的过程，因而也存在着信息的运动过程。可以说，缺少物质的世界是空虚的世界，缺少能量的世界是死寂的世界，缺少信息的世界则是混乱的世界。

第二，信息是人类认识世界和改造世界的媒介，它实现人类与自然界的沟通。人类通过自己的感觉器官，从物质世界中感知和提取信息；通过大脑的加工，以信息的形式输出，作用于物质世界，达到改造客观世界的目的。信息始终是这个过程的媒介物。

第三，信息是社会生存与发展的动力。信息交流是人类社会活动赖以形成、维系和发展的根本保证。由于社会内部的信息交流，使后人可以在前人的肩膀上起步。因此，信息本身也是社会前进与发展的基石，是人类进化的动力。

第四，信息是智慧之源，是人类的精神食粮。人的思维和智慧是信息过程的产物，不能想像没有信息的生活。

第五，信息是管理的灵魂。管理一直是人类的一项经常性的社会活动，是一个有序化的过程。管理主体向管理客体传递信息，监督客体的运行状态，收集反馈信息，不断地做出调整行为，以保证目标的实现。管理最重要的职能之一是决策。决策就是选择，而选择意味着消除不确定性，意味着需要大量、准确、全面而且及时的信息。

1.1.5 信息技术

人类认识世界和改造世界的过程，是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。信息是抽象的，但是，在这个过程中，每一步都需要专门的技术对信息进行作用，这些技术是具体的。