

21st CENTURY

实用规划教材

21世纪全国高职高专
计算机系列实用规划教材

实训型教材系列

计算机网络

安全技术

主 编	王其良	高敬瑜
副主编	吴冬燕	范荣真
主 审	宣仲良	曾瑶辉

内容特点:

- 本书全面介绍了计算机网络安全的基础知识
- 本书主要以网络安全技术实训为主，以操作应用软件来引导学生学习
- 本书既可供计算机专业学生使用，也可供对网络安全技术感兴趣的读者参考使用



北京大学出版社
PEKING UNIVERSITY PRESS

TP393.08
165

21 世纪全国高职高专计算机系列实用规划教材

计算机网络安全技术

主 编	王其良	高敬瑜
副主编	吴冬燕	范荣真
参 编	顾 桢	
主 审	宣仲良	曾瑶辉



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书全面介绍了计算机网络安全的基础知识。全书共9章,包括:网络安全概述、操作系统安全、信息加密技术、数字签名与CA认证技术、防火墙技术与配置、网络病毒与防治、黑客攻击与防范、Web服务安全、电子商务网络安全。

本书主要以网络安全技术实训为主,以操作应用软件来引导学生学习,可供计算机专业学生使用,也可供对网络安全技术感兴趣的读者参考使用。

图书在版编目(CIP)数据

计算机网络安全技术/王其良,高敬瑜主编. —北京:北京大学出版社,2006.8

(21世纪全国高职高专计算机系列实用规划教材)

ISBN 7-301-10887-7

I. 计… II. ①王… ②高… III. 计算机网络—安全技术—高等学校:技术学校—教材
IV. TP393.08

中国版本图书馆CIP数据核字(2006)第078396号

书 名: 计算机网络安全技术

著作责任者: 王其良 高敬瑜 主编

责任编辑: 刘 丽

标准书号: ISBN 7-301-10887-7/TP·0887

出 版 者: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> <http://www.pup6.com>

电 话: 邮购部 62752015 发行部 62750672 编辑部 62750667 出版部 62754962

电子信箱: pup_6@163.com

印 刷 者: 世界知识印刷厂

发 行 者: 北京大学出版社

经 销 者: 新华书店

787毫米×1092毫米 16开本 19.75印张 450千字

2006年8月第1版 2006年8月第1次印刷

定 价: 28.00元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究

举报电话: 010-62752024

电子邮箱: fd@pup.pku.edu.cn

21世纪全国高职高专计算机系列实用规划教材

专家编审委员会

主任 刘瑞挺

副主任 (按拼音顺序排名)

陈玉国 崔锁镇 高文志 韩希义

黄晓敏 魏 峥 谢一风 张文学

委员 (按拼音顺序排名)

安志远 丁亚明 杜兆将 高爱国 高春玲 郭鲜凤

韩最蛟 郝金镇 黄贻彬 季昌武 姜 力 李晓桓

连卫民 刘德军 刘德仁 刘辉珞 栾昌海 罗 毅

慕东周 彭 勇 齐彦力 沈凤池 陶 洪 王春红

闻红军 武凤翔 武俊生 徐 红 徐洪祥 徐受容

许文宪 严仲兴 杨 武 易永红 于巧娥 袁体芳

张 昕 赵 敬 赵润林 周朋红 訾 波

信息技术的职业化教育

(代丛书序)

刘瑞挺/文

北京大学出版社第六事业部组编了一套《21世纪全国高职高专计算机系列实用规划教材》。为此，制订了详细的编写目的、丛书特色、内容要求和风格规范。在内容上强调面向职业、项目驱动、注重实例、培养能力；在风格上力求文字精练、图表丰富、脉络清晰、版式明快。

一、组编过程

2004年10月，第六事业部开始策划这套丛书，分派编辑深入各地职业院校，了解教学第一线的情况，物色经验丰富的作者。2005年1月15日在济南召开了“北大出版社高职高专计算机规划教材研讨会”。来自13个省、41所院校的70多位教师汇聚一堂，共同商讨未来高职高专计算机教材建设的思路和方法，并对规划教材进行了讨论与分工。2005年6月13日在苏州又召开了“高职高专计算机教材大纲和初稿审定会”。编审委员会委员和45个选题的主、参编，共52位教师参加了会议。审稿会分为公共基础课、计算机软件技术专业、计算机网络技术专业、计算机应用技术专业4个小组对稿件逐一进行审核。力争编写出一套高质量的、符合职业教育特点的精品教材。

二、知识结构

职业生涯的成功与人们的知识结构有关。以著名侦探福尔摩斯为例，作家柯南道尔在“血学的研究”中，对其知识结构描述如下：

- ◆ 文学知识——无；
- ◆ 哲学知识——无；
- ◆ 政治学知识——浅薄；
- ◆ 植物学知识——不全面。对于药物制剂和鸦片却知之甚详。对毒剂有一般了解，而对于实用园艺却一无所知；
- ◆ 化学知识——精深；
- ◆ 地质学知识——偏于应用，但也有限。他一眼就能分辨出不同的土质。根据裤子上泥点的颜色和坚实程度就能说明是在伦敦什么地方溅上的；
- ◆ 解剖学知识——准确，却不系统；
- ◆ 惊险小说知识——很渊博。似乎对近一个世纪发生的一切恐怖事件都深知底细；
- ◆ 法律知识——熟悉英国法律，并能充分实用；
- ◆ 其他——提琴拉得很好，精于拳术、剑术。

事实上，我国唐朝名臣狄仁杰，大宋提刑官宋慈，都有类似的知识结构。审视我们自己，每人的知识结构都是按自己的职业而建构的。因此，我们必须面向职场需要来设计教材。

三、职业门类

我国的职业门类分为 18 个大类：农林牧渔、交通运输、生化与制药、地矿与测绘、材料与能源、土建水利、制造、电气信息、环保与安全、轻纺与食品、财经、医药卫生、旅游、公共事业、文化教育、艺术设计传媒、公安、法律。

每个职业大类又分为二级类，例如电气信息大类又分为 5 个二级类：计算机、电子信息、通信、智能控制、电气技术。因此，18 个大类共有 75 个二级类。

在二级类的下面，又有不同的专业。75 个二级类共有 590 种专业。俗话说：“三百六十行，行行出状元”，现代职业仍在不断涌现。

四、IT 能力领域

通常信息技术分为 11 个能力领域：规划的能力、分析与设计 IT 解决方案的能力、构建 IT 方案的能力、测试 IT 方案的能力、实施 IT 方案的能力、支持 IT 方案的能力、应用 IT 方案的能力、团队合作能力、文档编写能力、项目管理能力以及其他能力。

每个能力领域下面又包含若干个能力单元，11 个能力领域共有 328 个能力单元。例如，应用 IT 方案能力领域就包括 12 个能力单元。它们是操作计算机硬件的能力、操作计算机软件包的能力、维护设备与耗材的能力、使用计算机软件包设计机构文档的能力、集成商务计算软件包的能力、操作文字处理软件的能力、操作电子表格应用软件的能力、操作数据库应用软件的能力、连接到互联网的能力、制作多媒体网页的能力、应用基本的计算机技术处理数据的能力、使用特定的企业系统以满足用户需求的能力。

显然，不同的职业对 IT 能力有不同的要求。

五、规划梦想

于是我们建立了一个职业门类与信息技术的平面图，以职业门类为横坐标、以信息技术为纵坐标。每个点都是一个函数，即 IT(Professional)，而不是 IT+Professional 单纯的相加。针对不同的职业，编写它所需要的信息技术教材，这是我们永恒的主题。

这样组合起来，就会有 $IT((328)*(Pro(590)))$ ，这将是一个非常庞大的数字。组织这么多的特色教材，真的只能是一个梦想，而且过犹不及。能做到 $IT((11)*(Pro(75)))$ 也就很不容易了。

因此，我们既要在宏观上把握职业门类的大而全，也要在微观上选择信息技术的少而精。

六、精选内容

在计算机科学中，有一个统计规律，称为 90/10 局部性原理(Locality Rule)：即程序执行的 90% 代码，只用了 10% 的指令。这就是说，频繁使用的指令只有 10%，它们足以完成 90% 的日常任务。

事实上，我们经常使用的语言文字也只有总量的 10%，却可以完成 90% 的交流任务。同理，我们只要掌握了信息技术中 10% 频繁使用的内容，就能处理 90% 的职业化任务。

有人把它改为 80/20 局部性原理，似乎适应的范围更广些。这个规律为编写符合职业教育需要的精品教材指明了方向：坚持少而精，反对多而杂。

七、职业本领

以计算机为核心、贴近职场需要的信息技术已经成为大多数人就业的关键本领。职业教育的目标之一就是培养学生过硬的 IT 从业本领，而且这个本领必须上升到职业化的高度。

职场需要的信息技术不仅是会使用键盘、录入汉字，而且还要提高效率、改善质量、降低成本。例如，两位学生都会用 Office 软件，但他们的工作效率、完成质量、消耗成本可能有天壤之别。领导喜欢谁？这是不言而喻的。因此，除了道德品质、工作态度外，必须通过严格的行业规范和个人行为规范，进行职业化训练才能养成正确的职业习惯。

我们肩负着艰巨的历史使命。我国人口众多，劳动力供大于求的矛盾将长期存在。发展和改革职业教育，是我国全面建设小康社会进程中一项艰巨而光荣的任务，关系到千家万户人民群众的切身利益。职业教育和高技能人才在社会主义现代化建设中有特殊的作用。我们一定要兢兢业业、不辱使命，把这套高职高专教材编写好，为我国职业教育的发展贡献一份力量。

刘瑞挺教授 曾任中国计算机学会教育培训委员会副主任、教育部理科计算机教学指导委员会委员、全国计算机等级考试委员会委员。目前担任的社会职务有：全国高等院校计算机基础教育研究会副会长、全国计算机应用技术证书考试委员会副主任、北京市计算机教育培训中心副理事长。

本系列教材编写目的和教学服务

本系列教材在遍布全国的各位编写老师的共同辛勤努力下，在编委会主任刘瑞挺教授和其他编审委员会成员的指导下，在北京大学出版社第六事业部的各位编辑刻苦努力下，本系列教材终于与广大师生们见面了。

教材编写目的

近几年来，职业技术教育事业得以蓬勃的发展，全国各地的高等职业院校以及高等专科学校无论是从招生人数还是学校的软、硬件设施上都达到了相当规模。随着我国经济的高速发展，尽快提高职业技术教育的水平显得越来越重要。教育部提出：职业教育就是就业教育，也就是说教学要直接面对就业，强调实践。不但要介绍技术，更要介绍具体应用，注重技术与应用的结合。本套教材的主要编写思想如下。

1. 与发达国家相比，我国职业技术教育教材的发展比较缓慢并且滞后，远远跟不上职业技术教育发展的需求。我们常常提倡职业教育的实用性，但在课堂教学中仍然使用理论性和技术性教材进行职业实践教学。针对这种现状，急需推出一系列切合当前教育改革需要的高质量的优秀职业技术实训型教材。

2. 本套教材总结了目前优秀计算机职业教育专家的教学思想与经验，与广大职业教育一线老师共同探讨，最终落实到本套教材中，开发出一套适合于我国职业教育教学目标和教学要求的教材，它是一套能切实提高学生专业动手实践能力和职业技术素质的教材。

3. 社会对学生的职业能力的要求不断提高，从而催化出了许多新型的课程结构和教学模式。新型教学模式是必须以工作为基础的模仿学习，它是将学生置于一种逼真的模拟环境中，呈现给学生的是具有挑战性、真实性和复杂性的问题，使学生得到较真实的锻炼。

4. 教材的结构必须按照职业能力的要求创建并组织实施新的教学模式。教学以专项能力的培养展开，以综合能力的形成为目标。能力的培养既是教学目标，又是评估的依据和标准。

5. 本套的重点是先让学生实践，从实践中领悟、总结理论，然后再学习必要的理论，用理论指导实践。从这一个循环的教学过程中，学生的职业能力将得到极大的提高。

教学服务

1. 提供电子教案

本系列教材绝大多数都是教程与实训二合一，每一本书都有配套的电子教案，以降低任课老师的备课强度，此课件可以在我们网站上随时下载。

2. 提供教学资源下载

本系列教材中涉及到的实例(习题)的原始图片和其他素材或者是源代码、原始数据等文件，都可以在我们网站上下载。

3. 提供多媒体课件和教师培训

针对某些重点课程，我们配套有相应的多媒体课件。对大批量使用本套教材的学校，我们会免费提供多媒体课件，另外还将免费提供教师培训名额，组织使用本套教材的教师进行相应的培训。

北京大学出版社第六事业部(<http://www.pup6.com>)

前 言

计算机网络成为当前社会发展的重要推动力。社会经济发展、国防信息建设以及与人们生活息息相关的各行各业，对计算机网络的依赖程度都不断增大。计算机网络给人们带来便利的同时，也带来了保证信息安全的巨大挑战。如何使信息不受黑客的入侵，如何保证计算机网络不间断地工作并提供正常的服务，是各个组织信息化建设必须考虑的重要问题。

本书着重于从实训与应用的角度介绍计算机网络安全，使读者了解一般网络安全的基础理论及技术原理，从实训中认识、理解什么是网络安全，并掌握常用的安全应用技术。全书共 9 章，第 1 章主要介绍计算机网络安全的相关概念，计算机网络的安全体系结构。第 2 章主要介绍计算机操作系统的安全基础与防范措施，包括：操作系统的安全机制及安全级别、操作系统安全技术。第 3 章主要介绍信息加密与公钥架构(Public Key Infrastructure, PKI)技术，包括：加密体系；单钥加密和双钥加密算法；链路、节点、端到端加密；公钥架构。第 4 章主要介绍数字签名与 CA 认证技术，掌握个人数字凭证的申请、颁发和使用。第 5 章主要介绍防火墙技术，包括：防火墙体系结构、包过滤防火墙和应用代理防火墙，以及防火墙的应用。第 6 章主要介绍计算机病毒防范技术，包括：计算机病毒的工作原理和分类，计算机病毒的检测和防范技术，各种防治病毒的软件的使用。第 7 章主要介绍网络黑客的攻击与防范，包括：黑客常用的各种攻击工具及攻击步骤、各种常用的防黑客的方法与工具的使用。第 8 章主要介绍因特网中 Web 服务器的安全性，包括 FTP、电子邮件及 Web 可能的攻击技术及其安全保护措施。第 9 章主要介绍电子商务的安全性，包括电子商务的安全需求分析、电子商务采取的安全措施。本书涉及的内容操作性比较强，在学习时，可多安排学生的实训操作课时，加强实训的监督，并要求学生认真写好实训报告。对书中一些理论如需要进一步加深的，应该指导学生参阅相应的参考书。建议本课程的教学时间为 64 学时，其中 32 学时用于授课，32 学时用于实训。第 1 章安排 2 学时，第 2 章、第 3 章、第 4 章分别安排 6 学时，第 5 章、第 6 章、第 8 章、第 9 章分别安排 8 学时，第 7 章安排 12 学时。

本书由王其良，高敬瑜任主编，吴冬燕，范荣真任副主编，顾桢任参编。王其良编写第 1 章以及第 8 章，范荣真编写第 2 章、第 5 章、第 9 章，高敬瑜编写第 3 章、第 4 章，吴冬燕编写第 6 章，顾桢编写第 7 章。本书由苏州职业大学计算机工程系宣仲良主任，保险职业学院信息系曾瑶辉主任担任主审，他们对本书的修改提出了宝贵的意见，在此表示衷心的感谢！

本书是北京大学出版社组织的 21 世纪全国高职高专计算机系列实用规划教材之一，在取材上突出培养和强化学生的实践能力与应用能力，加强了实训内容的编写，在理论上取精而且简单明了。本书特别突出了各项技术的应用性，希望能贴近高职高专学生的学习特

点，从而激发起学习兴趣，在实践中提高其对计算机网络安全应对与控制能力。

网络安全是一门涉及计算机科学、通信技术、密码技术、应用数学等多门学科的交叉学科，同时在上应用上，网络安全技术和产品发展很快，因此这本书的编写思想是，理论讲解简洁化，应用实例新颖化，操作步骤详细化，以实训引导学生理解理论，从而达到应用的目的。当然，在采用本书做实验时，也可根据具体情况采用熟悉的实例。

由于编写水平及时间所限，书中难免有疏漏之处，恳请广大读者和专家批评指正。

编者

2006年2月

目 录

第 1 章 网络安全概述	1	2.2.2 密码安全配置	24
1.1 网络安全的重要性	1	2.2.3 系统安全配置	26
1.2 网络安全现状分析	2	2.2.4 服务安全配置	30
1.3 网络不安全的主要因素	3	2.2.5 注册表配置	33
1.3.1 互联网具有的不安全性	3	2.2.6 数据恢复软件	37
1.3.2 操作系统存在的安全问题	3	小结	40
1.3.3 数据的安全问题	4	习题	40
1.3.4 传输线路的安全问题	4	第 3 章 信息加密技术	41
1.3.5 网络安全管理问题	4	3.1 概述	41
1.4 网络安全的主要威胁	4	3.1.1 数据加密技术	42
1.4.1 人为的疏忽	5	3.1.2 数据加密算法	42
1.4.2 人为的恶意攻击	5	3.1.3 数据加密技术的发展	43
1.4.3 网络软件的漏洞	6	3.2 数据加密标准 DES 与 IDEA	43
1.4.4 非授权访问	6	3.2.1 数据加密标准 DES 思想	43
1.4.5 信息泄漏或丢失	6	3.2.2 IDEA 算法	45
1.4.6 破坏数据完整性	6	3.3 公开密钥算法	45
1.5 计算机网络安全的定义	6	3.3.1 RSA 公开密钥密码系统	46
1.6 网络信息安全特征与保护技术	7	3.3.2 RSA 的实用性	48
1.6.1 信息安全特征	7	3.3.3 RSA 的实用考虑	48
1.6.2 信息安全保护技术	7	3.4 计算机网络的加密技术	49
1.7 网络信息安全机制	8	3.4.1 链路加密	50
1.8 网络安全威胁的发展趋势	10	3.4.2 节点加密	50
小结	12	3.4.3 端到端加密	51
习题	12	3.5 密钥管理与交换技术	55
第 2 章 操作系统安全配置	13	3.5.1 密钥的管理问题	55
2.1 操作系统的安全问题	13	3.5.2 Diffie-Hellman 密钥交换 技术	56
2.1.1 操作系统安全概念	13	3.5.3 RSA 密钥交换技术	56
2.1.2 计算机操作系统安全评估	14	3.6 密码分析与攻击	57
2.1.3 国内的安全操作系统评估	14	3.6.1 基于密文的攻击	58
2.1.4 操作系统的安全配置	17	3.6.2 基于明文的密码攻击	58
2.1.5 操作系统的安全漏洞	17	3.6.3 中间人攻击	59
2.2 操作系统安全配置实验	18	3.7 信息加密解密应用试验	59
2.2.1 用户安全配置	18		

3.7.1 高强度文件夹加密大师 9000 软件的使用	59	5.1.2 网络防火墙的目的与作用	100
3.7.2 日月精华——文件加密软件的使用	62	5.2 防火墙的类型	100
3.7.3 A-Lock 邮件加密软件的使用	63	5.2.1 包过滤型防火墙	100
3.7.4 “我的地盘” 磁盘加密软件的使用	64	5.2.2 IP 级包过滤型防火墙	100
3.7.5 建设部密钥管理流程	66	5.2.3 代理服务器型防火墙	102
小结	70	5.2.4 其他类型的防火墙	103
习题	70	5.3 防火墙设计的安全要求与准则	104
第 4 章 数字签名与 CA 认证技术	71	5.4 防火墙安全体系结构	105
4.1 数字签名原理、种类与方法	71	5.4.1 过滤路由器防火墙结构	105
4.1.1 数字签名原理	71	5.4.2 双宿主主机防火墙结构	105
4.1.2 数字签名的种类	72	5.4.3 主机过滤型防火墙结构	106
4.1.3 数字签名的技术实现方法	74	5.4.4 子网过滤型防火墙结构	107
4.2 鉴别技术与方法	77	5.4.5 吊带式防火墙结构	107
4.2.1 鉴别的概念	77	5.4.6 典型的防火墙结构	108
4.2.2 数据完整性鉴别	78	5.5 创建防火墙步骤	109
4.3 数字凭证	78	5.5.1 制定安全策略	109
4.3.1 CA 认证与数字凭证	78	5.5.2 搭建安全体系结构	109
4.3.2 个人数字凭证的申请、颁发和使用	83	5.5.3 制定规则次序	110
4.4 认证产品及应用	85	5.5.4 落实规则集	110
4.4.1 通用认证中心	85	5.5.5 注意更换控制	110
4.4.2 eCertCA / PKI	86	5.5.6 做好审计工作	111
4.4.3 Kerberos 认证	86	5.6 防火墙配置实验	111
4.5 数字签名与 CA 认证实验	88	5.6.1 Cisco PIX 防火墙的升级和初始配置	111
4.5.1 ChinaTCP 个人控件数字签名系统 1.00 软件的使用	88	5.6.2 Cisco PIX 防火墙网络地址翻译(NAT)配置	116
4.5.2 在中国数字认证网上练习申请数字证书	93	5.6.3 Cisco PIX 防火墙外部访问内部配置	122
小结	98	5.6.4 费尔个人防火墙配置与管理	126
习题	98	小结	132
第 5 章 防火墙技术与配置	99	习题	132
5.1 网络防火墙概述	99	第 6 章 网络病毒与防治	133
5.1.1 网络防火墙基本概念	99	6.1 计算机病毒概述	133
		6.1.1 计算机病毒基本概念	133
		6.1.2 计算机病毒的历史	133
		6.2 计算机病毒的特征及传播方式	135
		6.2.1 计算机病毒的特征	135

6.2.2 病毒的传播方式.....	137	7.5 防黑措施	204
6.3 计算机病毒的分类	137	7.6 常用攻击和防御软件的应用实验	206
6.4 计算机病毒的破坏行为及防御.....	139	7.6.1 “冰河”使用说明	206
6.4.1 计算机病毒的破坏行为.....	139	7.6.2 RegRun 的使用说明.....	214
6.4.2 计算机病毒的防御.....	139	小结	218
6.5 杀毒软件的安装与配置实验.....	140	习题	218
6.5.1 瑞星杀毒软件的安装与配置	140	第 8 章 Web 服务的安全性	220
6.5.2 卡斯基(Kaspersky)杀毒软件的安装和配置.....	148	8.1 Web 服务的安全概述	220
6.6 病毒的查杀实验	154	8.1.1 网络服务概念.....	220
6.6.1 尼姆达(Nimda)病毒的查杀	154	8.1.2 Web 服务的安全威胁	220
6.6.2 冲击波(Worm.Blaster)病毒的查杀	157	8.1.3 防御措施.....	223
6.6.3 红色代码(Code Red)病毒的查杀	159	8.2 Web 服务中的 IE 安全	224
6.6.4 FunLove 病毒的查杀	161	8.3 Web 服务的安全实验	229
6.6.5 CIH 病毒的查杀.....	163	8.3.1 FTP 服务的安全.....	229
6.6.6 求职信(Klez)病毒的查杀.....	165	8.3.2 E-mail 服务的安全	233
6.6.7 红色终结符(RedLof)病毒的查杀	166	小结	250
小结	168	习题	251
习题	168	第 9 章 电子商务的安全性	252
第 7 章 黑客的攻击与防范	169	9.1 电子商务的安全需求.....	252
7.1 网络黑客概述	169	9.1.1 电子商务安全的概念.....	252
7.2 黑客攻击的目的及步骤.....	170	9.1.2 电子商务的安全问题.....	253
7.2.1 黑客攻击的目的.....	170	9.1.3 电子商务的安全需求.....	254
7.2.2 黑客攻击的步骤.....	170	9.1.4 电子商务的安全体系.....	255
7.3 常用的黑客攻击方法.....	172	9.2 电子商务的安全措施.....	255
7.3.1 端口扫描	172	9.3 电子商务安全技术协议.....	256
7.3.2 口令破解	175	9.3.1 SSL——提供网上购物安全的协议.....	256
7.3.3 特洛伊木马	178	9.3.2 SET——提供安全的电子商务数据交换.....	257
7.3.4 缓冲区溢出攻击.....	185	9.4 基于 SSL 协议网站的构建	262
7.3.5 拒绝服务攻击.....	188	9.4.1 证书服务的安装与管理.....	262
7.3.6 网络监听	193	9.4.2 生成 Web 服务器数字证书申请文件.....	265
7.4 攻击实例	195	9.4.3 申请 Web 服务器数字证书	271
7.4.1 网络监听实例.....	195	9.4.4 颁发 Web 服务器数字证书	273
7.4.2 口令破解实例.....	200	9.4.5 获取 Web 服务器的数字证书.....	274

9.4.6 安装 Web 服务器数字证书274	9.4.12 浏览器数字证书的管理 283
9.4.7 在 Web 服务器上设置 SSL278	9.4.13 在浏览器上设置 SSL 285
9.4.8 浏览器的 SSL 配置.....280	9.4.14 访问 SSL 站点..... 286
9.4.9 申请浏览器数字证书.....280	9.5 浦发银行移动证书的申请..... 286
9.4.10 颁发浏览器数字证书.....282	小结 296
9.4.11 获取及安装浏览器 数字证书282	习题 296
	参考文献 298

第 1 章 网络安全概述

本章要点

- 网络安全的概念、现状分析
- 网络不安全的主要因素及其造成的主要威胁
- 网络信息安全特征与保护技术的简述
- 保护网络信息安全采用的技术机制
- 网络安全威胁及相应对抗技术的发展趋势

1.1 网络安全的重要性

安全性是互联网技术中最关键也最容易被忽视的问题。许多组织都建立了庞大的网络体系，但在多年的使用中从未考虑过安全问题，直到网络安全受到威胁，才不得不采取安全措施。随着计算机网络的广泛使用和网络之间数据传输量的急剧增长，网络安全的重要性愈加突出。

1994 年末，俄罗斯黑客弗拉基米尔·利文伙同朋友在圣彼得堡的一家小软件公司的联网计算机上，向美国花旗银行进行了一连串恶性攻击，以电子转账方式，从花旗银行在纽约的计算机主机里窃取了 180 万美元。

1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，美国司法部主页被篡改，还留下大量攻击美国司法政策的文字，此事在当时成为轰动一时的新闻。

1996 年 2 月，刚开通不久的 Chinanet 网站就受到了攻击，且攻击得逞。1997 年初，北京某 ISP 运营商被黑客成功侵入，并在清华大学“水木清华”BBS 的“黑客与解密”论坛张贴如何免费通过该 ISP 进入 Internet 的文章。

据不完全统计，我国的网络安全问题近年来呈逐年上升趋势，1998 年公安部有关部门受理网络犯罪案件仅 80 多起，1999 年增至 400 多起，2000 年剧增为 2700 多起，2001 年增加到 4500 多起，比 2000 年上升约 70%，2002 年又上升到 6600 多起，而且仅 2003 年上半年就有 4800 多起，比同期上升 77.1%。

有关黑客威胁的报道已经屡见不鲜，而内部工作人员的疏忽甚至有意充当间谍对网络安全已构成更大的威胁。内部工作人员能较多地接触内部信息，工作中的任何大意都可能给信息安全带来威胁。无论是有意的攻击，还是无意的误操作，都会给系统带来不可估量的损失。虽然目前大多数的攻击者只是恶作剧似地使用篡改网站首页、拒绝服务等攻击，但当攻击者的技术达到某个层次后，他们就可以窃听网络上的信息，窃取用户密码、数据库等信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，可以删除数据库内容，摧毁网络结点，释放计算机病毒等。

综上所述，网络必须有足够强大的安全措施。无论是局域网还是广域网，无论是单位

还是个人，网络安全的目标是全方位地防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.2 网络安全现状分析

20 世纪 90 年代初，英、法、德、荷 4 国针对传统的 TCSEC(Trusted Computer System Evaluation Criteria)准则只考虑保密性的局限性，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 (nSFC)”，但是该准则中并没有给出综合解决上述问题的理论模型和方案。近年来 6 国 7 方(美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰)共同提出了“信息技术安全评价通用准则”，该准则综合了国际上已有的评审准则和技术标准的精华，给出了框架和原则要求。

然而，作为取代 TCSEC 用于系统安全评测的国际标准，它仍然缺少综合解决信息多种安全属性的理论模型依据。更重要的是，他们的高安全级别的产品对我国是封锁禁售的。

作为信息安全的重要内容，安全协议的形式化方法分析始于 20 世纪 80 年代初，目前主要有基于状态机、模态逻辑和代数工具的 3 种分析方法，但仍有局限性和漏洞，处于发展提高阶段。

由于在广泛应用的因特网上，黑客入侵事件不断发生，不良信息在网上大量传播，所以网络安全监控管理理论和机制的研究就备受重视。黑客入侵手段的研究分析、系统脆弱性检测技术、报警技术、信息内容分级标识机制、智能化信息内容分析等研究成果已经成为众多安全工具软件的基础。

从已有的研究结果可以看出，现在的网络系统中存在着许多设计缺陷和情报机构有意埋伏的安全陷阱。例如在 CPU 芯片中，发达国家利用现有技术条件，可以加入无线发射接收功能，在操作系统、数据库管理系统或应用程序中能够预先安置从事情报搜集、受控激发的破坏程序。通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CPU 的自杀程序；搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过唯一识别 CPU 的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先的设定搜集敏感信息或进行定向破坏。

作为信息安全关键技术的密码学近年来空前活跃。美、欧、亚各洲频繁举行密码学和信息安全学术会议。1976 年美国学者提出的公开密钥密码体制克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，并可用于身份认证，它是当前研究的热点。目前处于研究和发展阶段的电子商务的安全性是人们普遍关注的焦点，它带动了认证理论、密钥管理等方面的研究。随着计算机运算速度的不断提高，各种密码算法面临着新的密码体制，如量子密码、DNA 密码、混沌理论等的挑战。1977 年美国颁布使用的国家数据加密标准越来越不能满足安全需要，美国正在征集 21 世纪使用的新数据加密标准。

我国信息安全研究经历了通信保密及计算机数据保护两个发展阶段，现正进入网络信息安全的研究阶段。虽然通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，所以基于具体产品的增强安全功能的成果很难保证没有漏洞，也很难得到推广应用。现在虽然在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全

网关、黑客入侵检测、系统脆弱性扫描软件等，但是，这些产品安全技术的完善性、规范化和实用性还存在许多不足。特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面与国际水平相比存在很大差距，而且，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络信息安全研究起步晚，与技术先进国家相比有差距，特别是在系统安全和安全协议方面的工作与国外差距较大。在我国研究和建立创新性安全理论及系列算法，仍是一项艰巨的任务。然而我国的网络信息安全研究已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，可以期待取得实质性进展。

1.3 网络不安全的主要因素

计算机网络安全脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。要使网络方便快捷，又要保证安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找支撑点。因此，可以说任何一个计算机网络都不是绝对安全的。

1.3.1 互联网具有的不安全性

最初，互联网仅用于科研和学术组织内，它的技术基础存在不安全性。现在互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性的特征，这就对网络安全提出了挑战。互联网的不安全性主要表现在如下方面。

(1) 网络互联技术是全开放的，使得网络所面临的破坏和攻击来自各方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件设施的攻击。

(2) 网络的国际性意味着网络的攻击不仅来自本地网络的用户，而且可以来自互联网上的任何一台机器，也就是说，网络安全面临的是国际化的挑战。

(3) 网络的自由性意味着最初网络对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，互联网使用的基础协议 TCP/IP(传输控制协议/网际协议)，FTP(文件传送协议)、E-mail(电子邮件)、RPC(远程进程调用)，以及 NFS(网络文件系统)等不仅是公开的，而且都存在许多安全漏洞。

1.3.2 操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给网络安全留下了许多隐患。

操作系统的体系结构造成的不安全性是计算机系统不安全的根本原因之一。操作系统的程序是可以动态链接的，例如：I/O 的驱动程序和系统服务，这些程序和服务可以通过打“补丁”的方式进行动态链接，许多 UNIX 操作系统的版本升级也都是采用打补丁的方式进行的。

这种动态链接的方法容易被黑客所利用，并且也是计算机病毒产生的环境。另外，操作系统的一些功能也会带来不安全因素，例如支持在网络上传输可以执行的文件映像、网络加载程序等。