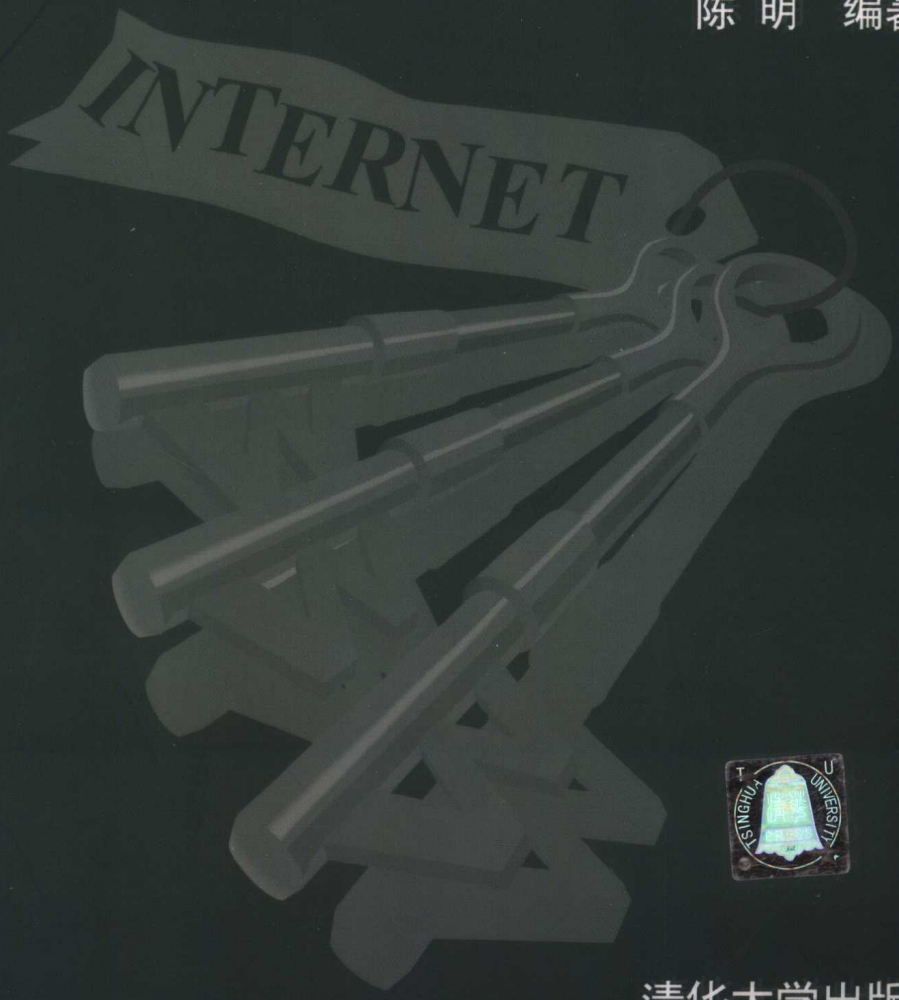
实用计算机网络技术丛书

网络安全

教程

陈明 编著



清华大学出版社

网络安全

实用计算机网络技术丛书

网络安全教程

陈　明　编著

清华大学出版社
北　京

内 容 简 介

本书全面、系统地介绍了当前网络安全方面的有关内容，主要包括网络安全概述、网络安全基础、TCP/IP基础、数据加密技术、网络攻击、检测与防范技术、软件安全漏洞及相关专业的计算机病毒与反病毒、防火墙技术、虚拟专用网技术及Web服务的安全性等内容。本书可作为大学计算机网络教材，也可作为计算机网络工程技术人员的参考书。

图书在版编目(CIP)数据

网络安全教程/陈明编著. —北京：清华大学出版社，2004.4
ISBN 7-302-08151-4

Ⅰ.网… Ⅱ.陈… Ⅲ.计算机－安全技术－教材 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2004)第013351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：冯志强
封面设计：品位数码
印 刷 者：北京密云胶印厂
装 订 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**：14.75　**字数**：362千字
版　　次：2004年4月第1版　2004年4月第1次印刷
书　　号：ISBN 7-302-08151-4/TP·5889
印　　数：1～4000
定　　价：22.00元

总　　序

计算机科学与技术的产生与发展是20世纪科学发展史上最伟大的事件之一，计算机网络技术的出现是计算机应用的又一里程碑，计算机网络的发展对人类的政治、经济和文化将产生深远的影响。十几年前，Sun公司提出了“网络就是计算机”的著名理念，在此之后，计算机网络得到了飞速发展，走过了从局域网、广域网到因特网的普及的道路。今天，随着对等计算和网格计算的兴起，网络不仅成为充当连接不同计算机的桥梁，更应成为扩展计算能力、提供公共计算服务的平台。

计算机网络技术是计算机技术和通信技术的融合和交集，因此，涉及的基础是广泛的，包括的内容是丰富的。涉及的主要内容包括信息基础设施、三网合一、因特网服务等。信息基础设施的内容包括物理网、主干网、宽带接入方式、网络安全应急响应服务、高性能网络体系结构等；三网合一是指通信网、广播网和计算机网络技术紧密结合，实现统一网络，主要内容包括数字电视系统、IP电话、多媒体网络规划等；因特网服务主要包括电子业务和电子商务、应用基础设施提供商AIP、互联网数据中心和应用服务提供商等。

这次推出的6本网络教程(《局域网络教程》、《广域网络教程》、《网络设备教程》、《网络协议教程》、《网络设计教程》和《网络安全教程》)是网络技术的重要组成部分，主要介绍网络构建方面所涉及的技术。对于较高层次透明的分布式系统没有介绍和讨论，对于基于网络环境下的各种类型的网络计算也没有涉及。

《局域网络教程》主要内容包括局域网络概述、数据通信基础、局域网络的物理介质、网络体系结构、经典局域网络、高速以太网络、光纤分布数据接口、异步传输模式、光纤通道无线局域网络、城域网络、网络操作系统、网络安全和局域网络应用等。

《广域网络教程》主要内容包括广域网络通信基础、点对点选择、X.25网、综合业务服务网、帧中继、光纤通道、异步传输模式、数字数据网、广域网络路由、广域网络方案设计等。

《网络协议教程》主要内容包括计算机网络概述、数据通信基础、网络协议和服务概述、计算机网络体系结构、物理层协议、数据链路层协议、网络层协议、运输层协议、高层协议、简单网络管理协议SNMP等。

《网络设备教程》主要内容包括网络设备概述、调制解调器、网络接口卡、集线器、网桥、交换机、路由器、网关、网络存储系统、网络服务器、网络打印设备。

《网络安全教程》主要内容包括网络安全概述、网络安全的基本概念、网络基础与TCP/IP详解、数据加密技术、网络攻击检测技术、网络攻击技术、计算机病毒与反病毒、防火墙技术、虚拟网技术、Web安全、软件安全漏洞等。

《网络设计教程》主要内容包括网络分析与设计基础、网络分析与设计过程、网络需求分析、通信规范、逻辑网络设计、物理网络设计、网络测试、运行与维护等。

本套书是基于大专院校计算机专业和相近专业的教材而编写的，它们与计算机学科的科技参考书和专著不同，主要特点如下：

- 注重了全书的完整性、系统性、层次性。
- 考虑到计算机网络技术的飞速发展，注重了对新技术、新方法的吸收和融合，增强了实用性和现代性。
- 语言简洁，定义明确，对较困难和较繁琐问题的介绍深入浅出，增强了可理解性。
- 每章都附有小结和习题，便于学习总结和自测。
- 本书在理论上处于中等水平，因此，不仅适用于高等院校的教材，也适用于网络培训教材。
- 在各本教程中，尽量减少内容重复，但保证每本教程的内容完整性。
- 采用了原理和应用相结合的介绍方法，保证了教材应用的广泛性。
- 书中结构为积木状，各章相对独立，增强了全书的开放性和独立性。

由于作者水平有限，书中不足之处在所难免，敬请广大读者批评指正。

前　言

随着计算机网络的广泛使用和网络之间信息传输量的急剧增长，一些机构和部门在得益于网络加快业务运作的同时，其上网的数据也遭到了不同程度的破坏，或被删除或被复制，数据的安全和自身的利益受到了严重的威胁。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。从本质上来讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

本书是一本网络安全教程，主要内容包括：网络安全概述、网络安全基础、TCP/IP 基础、数据加密技术、网络攻击、检测与防范技术、软件安全漏洞、计算机病与反病毒、防火墙技术、虚拟专用网技术及 Web 服务的安全性等。

在网络安全概述一章中，介绍了网络安全的重要性、网络安全现状、网络安全面临的主要威胁等；在网络安全基础一章中，介绍了网络安全的定义、网络安全等级、网络安全层次、网络安全目标、网络安全策略、网络安全标准、网络安全方案等；在 TCP/IP 基础一章中，介绍了网络基础知识、TCP/IP 详解等；在数据加密一章中，介绍了数据加密概述、数据加密标准、国际数据加密算法、单向函数、单向 Hash 函数、公开密钥码体制、RSA 算法、密钥管理、通信加密、加密数据存储、硬件加密与 Clipper 加密芯片、加密技术的应用等；在网络攻击、检测与防范技术一章中介绍了网络攻击技术、网络攻击检测技术、网络安全防范技术、黑客攻击与防范、软件安全漏洞等；在软件安全漏洞一章中，介绍了应用软件中的陷门防范、操作系统的安全漏洞与防范、数据库的安全与防范、TCP/IP 协议的安全与防范、网络软件与网络服务的漏洞等；在计算机病毒一章中，介绍了计算机病毒的分类症状、危害、计算机病毒的发展的新技术、反病毒技术、反病毒软件产品、我国反病毒行业的发展、计算机病毒发展的新趋势等。在防火墙技术一章中，介绍了防火墙概念、防火墙的工作方式、防火墙基本组件、防火墙的体系结构及组合形式、防火墙的主要技术、防火墙分类、防火墙设计、防火墙的安全标准、防火墙攻击技术等；在虚拟专用网技术一章中，介绍了 VPN 概念、VPN 的划分、远程访问虚拟网、虚拟拨号专用网、VPN 设计工具、VPN 基本技术等；在 Web 服务的安全性一章中，介绍了 Web 服务所面临的两类安全威胁、防御措施、网络安全协议等。

在本书的编写过程中，我的研究生王秀文、王永、陈清夷、刘庆、宋晓艳、孙丽丽、高雁、赵旭霞和徐东燕等参加了资料的搜集和整理工作。

由于作者水平有限，书中不足之处在所难免，敬请读者批评指正。

陈 明

目　录

第 1 章　网络安全概述

1.1　网络安全的重要性

安全性是互联网技术中最关键且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·利文伙同朋友从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 1100 万美元。

1996 年初，美国旧金山的计算机安全协会与联邦调查局联合进行了一次调查统计，结果显示，有 53% 的企业曾受到过计算机病毒的侵害，42% 的企业计算机系统在过去的 12 个月中曾经被非法使用过。而五角大楼的一个研究小组宣称：美国一年中遭受的网络攻击达 25 万次之多。

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。

根据美国联邦调查局的调查，美国每年因为网络安全所造成的经济损失超过 1.7 亿美元。75% 的公司报告财务损失是由于计算机系统的安全问题造成的。约 59% 的损失可以进行定量估算，平均每个公司损失 40.2 万美元。

我国的网络安全研究虽然起步较晚，但黑客入侵计算机的水平已经和国际“接轨”。1996 年 2 月，刚开通不久的 Chinanet 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。

1997 年 4 月 23 日，美国西南贝尔互联网络公司的某个 PPP 用户侵入中国互联网络信息中心的服务器，破译了该系统的 shutdown 账户，把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。

一连串的网络非法入侵改变了中国网络安全犯罪“空白”的历史。1998 年中国破获电脑黑客案件近百起，利用计算机网络进行的各类违法行为在中国正以每年 30% 的速度激增。黑客的攻击方法已经超过了计算机病毒的种类，总数达到上万种。中国 95% 与 Internet 相连的网络管理中心都遭到过黑客的攻击或侵入，银行、金融和证券机构往往是黑客攻击的重点。针对银行、证券等金融领域的黑客犯罪案件总涉案金额已高达数亿元，针对其他行业的黑客犯罪案件也时有发生。

黑客的威胁见诸报道的已经屡见不鲜，然而内部工作人员的疏忽甚至充当间谍对网络

安全也已构成更大的威胁。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危险。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撰改网站主页、拒绝服务等攻击，但当攻击者的技术达到了某个层次后，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，摧毁网络节点，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，网络安全的目标是能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”(TISFC)，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、英、法、德、荷)共同提出了“信息技术安全评价通用准则”(CC for IT SEC)。CC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用于系统安全的评测的国际标准，它仍然缺少综合解决信息的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Internet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，可以植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收集、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的自杀功能；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，通过惟一识别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，根据预先的设定收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。1977年美国颁布使用的国家数据加密标准由于密码分析和攻击手段的