Broadview®
www.broadview.com.cn

安全技术大系

网络安全概论

李涛 编著

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

安全技术大系

国家自然科学基金
教育部博士点基金 资助项目

网络安全概论

李涛 编著

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

内 容 简 介

本书全面系统地介绍了网络安全的概念、原理及体系架构，详细论述了密码技术、公钥基础设施(PKI)、特权管理基础设施（PMI)、网络层安全性问题，以及 Web、电子邮件、数据库安全和操作系统的安全性问题，并对最新的防火墙技术、网络攻击技术和黑客入侵检测技术、计算机取证技术以及数据备份与恢复技术进行了全面的阐述。

本书取材新颖，内容丰富，可作为高等学校计算机、信息技术类本科生、研究生教材，亦可供网络安全领域专业科研人员参考使用。

图书在版编目（CIP）数据

网络安全概论 / 李涛编著. —北京：电子工业出版社，2004.11
（安全技术大系）
ISBN 7-121-00374-0

Ⅰ.网... Ⅱ.李... 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（2004）第 095707 号

责任编辑：孙学瑛
印　　刷：北京天竺颖华印刷厂
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
经　　销：各地新华书店
开　　本：787×980　1/16　印张：31　字数：623 千字
印　　次：2004 年 11 月第 1 次印刷
印　　数：5000 册　　定价：42.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。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。

序

随着网络经济和网络社会时代的到来，Internet 将会进入一个无处不有、无所不在的境地。经济、文化、军事和社会活动将会强烈地依赖计算机网络，作为国家重要基础设施的网络的安全和可靠性问题已成为世界各国共同关注的焦点。而 Internet 原有的跨国界、无主管性、不设防、缺乏法律约束性，为各国带来机遇的同时也带来了巨大的风险。

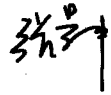
在信息网络已成为国家重要基础设施的情况下，信息战将是一种跨国界、隐蔽性、低花费和跨领域（军事、经济、社会、资源）的无硝烟的战争。其高技术性和战争情报的不确定性给信息战的防御带来了较大的难度。美国国防部专门组织了“信息战执行委员会”研究国家信息战的战略，并对所属网络和 Internet 网点进行了大量的攻击演练。国家级金融支付中心、证券交易中心、空中管制中心、电信网管中心、铁路调度中心、军事指挥中心等必将成为信息战的主要攻击目标。我国在信息化进程中对此必须早有准备。

近年来，随着 Internet 的发展，利用网络安全的脆弱性，黑客在网上的攻击活动每年正以 10 倍的速度增长。形形色色的黑客攻击者是一个各怀鬼胎的复杂群体，把网上任何漏洞和缺陷作为靶子，无孔不入。如：修改网页进行恶作剧，非法进入主机破坏程序，窜入银行网络转移资金，窃取网上信息兴风作浪，进行电子邮件骚扰，阻塞用户和窃取密码等等。政府、军事和金融网络更是他们攻击的主要目标。

网络安全是一门新兴的交叉性学科，综合运用了数学、物理、生物、通讯及计算机技术等诸多学科的基础理论和最新研究成果，同时还涉及政治、法律、军事等复杂层面。显然，若没有长期、系统、深入的研究和应用实践，要全面论述网络安全的理论与技术是不可能的。

《网络安全概论》是李涛教授及其所领导的计算机网络与安全研究所多年来潜心网络安全理论与技术的研究成果，对网络安全的各个层面进行了全面的论述。本书选材新颖、内容翔实、覆盖面广，既详细论述了网络安全的基础理论，同时又对网络安全的应用技术及研究前沿进行了准确的评价。全书层次结构清晰，行文流畅，篇、章相对独立，阅读容易。

《网络安全概论》是近年来网络信息安全领域中一本难得的好书，可作为大学计算机专业教材，为我国的网络安全专业人才的培养提供了有力的支持。



中国科学院院士

前 言

网络安全关系到国家安全。网络安全的理论及其应用技术的研究，不仅受到学术界以及工业界的关注，同时也受到各国政府的高度重视。为了本国的利益，美国等西方发达国家将网络安全技术及产品视为如同核武器一样的秘密技术，立法限制其向我国出口，换句话说，凡出口到我国的网络安全产品均是不安全的。为保障我国网络基础设施的安全，国家安全部、公安部等明确要求使用国产的网络安全产品来确保我国网络的安全。

然而，由于种种原因，目前我国有关网络安全技术及其产品的研发与美国等西方发达国家相比尚有一定的距离。正因为如此，我们更应加倍努力，迎头赶上。

在这种背景下，为促进我国网络安全技术的进步，在国家自然科学基金、教育部博士点基金的资助下，笔者结合自己多年来在网络安全研究中的心得，特编拙著，以期抛砖引玉，为我国的网络安全事业尽一点微薄之力。

全书共四篇 13 章。第一篇论述了网络安全的基础理论，共 3 章：第 1 章阐述了网络安全面临的威胁、网络安全服务和网络安全的基本模型；第 2 章就网络安全的基础——密码技术和信息隐藏技术进行了较为详细的讨论；第 3 章全面论述了公钥基础设施 PKI 的定义、内容和服务，同时介绍了特权管理基础设施 PMI。

第二篇讨论了网络安全的应用，共 3 章：第 4 章着重阐述了安全电子邮件的工作模式、相关的一些协议、标准和评估准则；第 5 章探讨了 IP 层的安全问题，重点阐述了 IPSec 协议的体系结构、原理和应用方式，同时就 VPN 技术以及下一代 IP 规范 IPv6 进行了讨论；第 6 章讨论了 Web 安全的实现方法，并详细阐述了 SSL、TLS、SET 等 Web 安全实现技术，最后就 SSL/TLS 的开放源码软件包 OpenSSL 进行了讨论。

第三篇就操作系统以及数据库安全问题进行了专题讨论，共 2 章：第 7 章分析了操作系统的安全机制，阐述了安全操作系统的设计原则、方法，并探讨了 Windows、UNIX、Linux 操作系统的一些安全漏洞；第 8 章阐述了数据库安全，讨论了常用的数据库安全措施，并介绍了数据库加密、DBMS 隐通道审计等前沿内容，随后分析了流行数据库 ORACLE 的安全性。

第四篇详细论述了网络安全的防护技术，共 5 章：第 9 章阐述了防火墙技术，包括防火墙的定义、功能、体系架构及其实现技术；第 10 章探讨了几种常见的网络攻击技术，包括扫描技术、拒绝服务攻击、缓冲区溢出攻击、嗅探器攻击等，并简要阐述了计算机病毒的特点、分类及防治办法；第 11 章就入侵检测技术进行了讨论，包括基于专家系统、神经网络、人工免疫等最新的 IDS 技术，并详细分析了 Linux 下的一个入侵检测系统——snort，剖析了其基本原理及实现技术；第 12 章探讨了网络安全的前沿技术——计

算机取证，详细阐述了计算机取证的原则、方法、步骤等，简要介绍了常用的取证工具，并阐述了证据分析的方法；第 13 章讨论了数据备份和恢复技术，并就目前的热门技术——容灾系统进行了讨论，详细介绍了容灾等级的定义，容灾计划的制订步骤等。

笔者非常感谢杨频副教授（博士）、赵辉博士、刘念博士、张建华博士、赵奎博士、胡晓勤博士，以及研究生甘玲、杨立、王健、浦海挺、李敏榆、廖竣锴、丁菊玲、仰石、肖康等人的努力。他们为本书收集了大量的文献、资料，并进行了细致的整理工作。笔者还要特别感谢研究生刘莎、郭京、王丹丹、刘颖娜、杨进、漆莲芝、周念念、王丽辉、杜雨、卢正添、王志明对本书进行了繁琐的校对工作，为本书的最后出炉作出了贡献。

由于书稿涉及许多新的内容和研究领域，尽管笔者已经尽了最大的努力，但仍感问题难免，望各位同仁不吝赐教，以利再版修订，为我国的网络安全事业共同出力。

笔　者

目　录