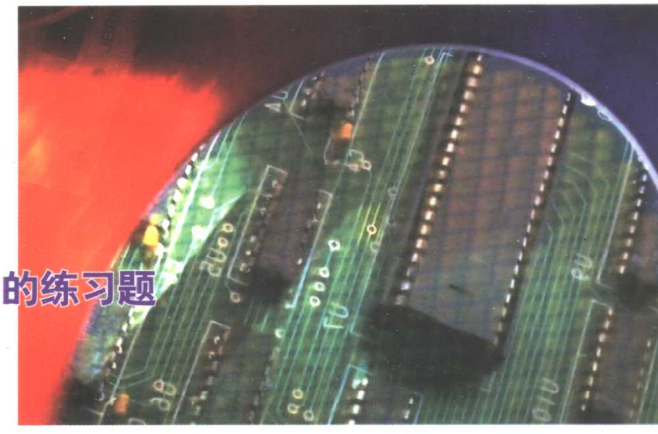
计算机工程师丛书

JI SUAN JI GONG CHENG SHI CONG SHU

# 计算机网络安全与加密技术

李海泉 李 健 编著

- 清晰而系统的基本概念
- 典型的安全防范措施
- 全新的网络安全解决方案
- 实用的加密程序
- 翔实的技术参数
- 每章末给出了本章小结和综合性的练习题



科学出版社
SCIENCE PRESS


# 计算机网络安全与加密技术

李海泉　李　健 编著

科学出版社

2001

## 内 容 简 介

本书共17章和5个附录，分别介绍了计算机网络概述，计算机网络的安全，局域网的安全，Windows NT的安全，Internet防火墙，网络计算机安全，计算机的防电磁泄漏，软件安全与加密技术，操作系统的安全，数据库的安全与加密，计算机网络数据加密与认证，PGP数据加密系统，文件传输安全，电子邮件安全，Web站点的安全，计算机病毒的检测与消除，计算机网络的安全评估，以及PGP命令及其用法，防火墙产品简介，监察和入侵检测工具，内部弱点扫描工具和美国计算机安全评估标准等附录。全书深入浅出，结构合理，层次清晰，有一定的理论深度和较高的实用价值。

本书可作为计算机工程、信息工程、信息系统与信息管理等专业的技术人员的参考书，也可作为高等院校相关专业教材，还可以作为工程技术人员进修教材。

**图书在版编目（CIP）数据**

计算机网络安全与加密技术/李海泉，李健编著. -北京：科学出版社，2001

（计算机工程师丛书）

ISBN 7-03-007970-1

Ⅰ.计… Ⅱ.①李…②李… Ⅲ.①计算机网络-安全技术②计算机网络-加密-技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2000）第81395号

JS489/20

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

北京双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2001年3月第 一 版 开本：787×1092 1/16

2001年3月第一次印刷 印张：35 1/2

印数：1—5 000 字数：810 000

**定价：55.00元**

**(如有印装质量问题,我社负责调换<环伟>)**

# 出版前言

1998年，科学出版社推出了第一批计算机工程师丛书，这些书包括：

《电脑软故障修复技术》

《主机和外设电源故障检修》

《多媒体电脑故障快捷检修技术》

《主机板的实用维修技术》

《外存储设备故障诊断与维护》

《打印机故障诊断与维护》

《显示器故障诊断与维护》

《现代计算机网络技术与应用——设计·开发·管理·维护》

这些书的起点适中，注重跟踪新技术，兼顾通用性，为技术人员提供了极具实用价值的实测数据和电路图等资料。在写作方法上，注意以典型实例带原理，培养读者能够举一反三，触类旁通地解决实际问题的能力。

“计算机工程师丛书”的特色是：全面性、系统性、新颖性、实用性、启发性和可操作性。更注重内容选取立足现在，着眼未来，急用户所需，相对持久的阅读和参考价值。因而，这套书面世后受到广大读者的欢迎，至今销售不衰。该套书被中国计算机管理与维护委员会评为优秀畅销书。

两年前预测，在2000年我国计算机的拥有量将突破1000万台。事实上，据有关部门统计，我国目前计算机的拥有量已达6000万台。这个惊人的增长数字，反映了计算机和网络技术的普及速度迅猛。特别是Internet使人们能够共享世界资源，从根本上改变了人们的生活、工作方式。计算机和网络把世界推向了信息与知识的新时代，人们越来越意识到赖以生存和发展的重要条件是一个人获取信息、处理信息和更新知识的能力，而学会操作、使用计算机和网络是增长能力的重要途径。

既然计算机和网络技术是人们赖以生存和发展的重要工具，那么，计算机设备和网络设备及系统的性能稳定将直接关系到人们的工作、生活质量。由此而引发三个方面的思考：

(1) 大量的计算机设备需要维护和维修，确保计算机无故障运行；一旦发生故障，要迅速、准确地诊断故障的性质和部位，予以快速排除。

(2) 网络就像人体的血脉，它运营、处理着保障社会活力的信息流。一旦网络不畅，出现网络安全问题，将对单位、行业、社会造成巨大影响。网络的维护要防患于未然，并能及时排除网络故障。

(3) 6000万台电脑的拥有量，意味着有高出6000万若干倍的人在使用电脑。那么，学会使用电脑的技巧，掌握软故障的排除方法，势在必行。

鉴于上述，科学出版社组织有关作者编写了计算机工程师的第二批图书，这些书包括：

《电脑应用技巧与软故障修复实战技法》

《主流计算机硬件实用技术》

《微型计算机系统故障诊断与维护》

《主机板实用维修技术》

《票据打印机的原理 使用与维修》

《光盘驱动器原理 设计与维修》

《计算机网络安全与加密技术》

《网络信息安全技术》

其中，《电脑应用技巧与软故障修复实战技法》、《主机板实用维修技术》是修订版。

“计算机工程师丛书”第二批图书秉承了第一批图书的写作风格和内容选取宗旨，更注重结合新的技术产品和作者实践经验的总结，强调高技术含量和有的放矢地举例，把“全面性、系统性、新颖性、实用性、启发性、可操作性”的写作特色落实到每一章节的策划之中。每位作者根据图书的读者定位，精心安排全书结构，指导读者掌握技术的重点和难点。初级水平的读者，可以获得更新、更全的技术知识，有一定实践经验的读者，阅读本套书能让技术水平更上一层楼。

首批“计算机工程师丛书”面世后，得到广大读者的好评，市场检验证明，“计算机工程师丛书”的写作宗旨具有持久的生命力。顺应读者需求，第二批计算机工程师丛书面世了，我们期望它如作者、出版者所愿，成为读者的良师益友。

由于时间紧，书中难免有不完善之处和错误疏漏，敬请批评，指正。

我们欢迎热心的读者为“计算机工程师丛书”后续出版提出希望和要求；欢迎有更多的人加盟“计算机工程师丛书”的作者队伍。

E-mail：wantshulan@sohu.com

科学出版社

计算机图书业务部

2000．11．6

# 序 言

随着 Internet 和局域网的迅速发展和广泛应用，信息高速公路的建立，正在对科学技术、经济和文化带来巨大的推动和影响，也改变着人们的工作、学习和生活方式。计算机网络可以使信息的获取、传递、存储、处理和应用更加快捷、更加方便。然而，在人们热衷和沉醉于 Internet 和局域网及其 E-mail、Web 和 FTP 中的时候，千万不要忽视日益严重的计算机网络的安全问题。来自网络、软件、工作人员和环境等内外的安全威胁，黑客攻击、病毒干扰和破坏、计算机犯罪，不仅使计算机及网络中的信息被窃取、泄漏、修改和破坏，还会使网络设备、计算机设备遭受威胁和破坏，使系统瘫痪。因此，计算机网络的安全是一项综合的系统工程，应引起我们的高度重视。为保证计算机网络的安全，计算机科学技术及应用、信息工程、软件工程、信息管理与信息系统、金融信息管理、会计信息管理等专业科技人员和计算机安全人员，以及大专院校相应专业的师生，必须系统、深入地学习和研究计算机网络的安全技术与方法。

李海泉教授任中国计算机学会维护与管理专业委员会副主任、中国计算机学会外部设备专业委员会委员、中国计算机学会名词审定与编辑出版委员会委员、中国电子学会计算机工程与应用分会维护专业委员会副主任等职务。他先后完成了多个国防科技和国家八·五国防科研项目，获得多个部级科技进步奖；发表过 158 篇学术论文，编著并出版了 15 本专著、8 种大专院校教材，获得多部“优秀科技著作奖”、“优秀教材奖”。1997 年 3 月编著并出版了《计算机系统的安全技术与方法》一书，经多年教学使用，反映良好，先后获得省教委“优秀教材奖”和本学会“优秀科技著作二等奖”。今年，李教授在原著作基础上，按教学需要，根据多年教学和科研实践经验，又参考了国内、外的有关学术著作，编著了《计算机系统安全技术》和《计算机网络安全与加密技术》两本书。《计算机网络安全与加密技术》一书具有以下特点：

1．本书全面、系统地介绍了计算机网络的安全技术与加密方法，反映了该学科的发展方向，适合我国计算机网络发展的需求，在计算机网络安全方面属国内领先水平。

2．所介绍的技术和方法，具有一定的先进性和实用性。如

Internet 安全、局域网安全、Windows NT 的安全、防火墙技术、抗电磁干扰、防电磁泄漏、计算机实体安全、软件和数据安全与加密、E-mail、FTP、Web 安全、安全运行与安全管理、病毒的诊断、消除和预防，以及计算机网络安全评估。因此，本书不会因为计算机及网络产品的更新换代，而失去应用价值。

3. 本书实用性强。本书内容广泛，深入浅出，简明实用，可操作性强。所介绍的技术和方法很实用，并有可参考的程序和借鉴的实用工具，所选用的实例典型，可直接参考、使用，并举一反三、触类旁通。

4. 本书编写独具风格。每章开头有内容提要，引导读者学习原理方法。每章末有内容小结和习题与思考题，帮助读者复习、巩固所学内容。本书最后有参考文献，帮助读者深入研究。最后有五个附录，提供了测试、分析和需要的工具，可供实践中参考。

5. 本书可作为计算机科学技术及其应用、信息工程、软件工程、信息管理与信息系统、银行信息管理、会计信息管理和计算机安全等专业的科技人员作为工具性参考书，也可以作为大专院校相应专业教材，还可供研究生学习和参考。

中国计算机学会计算机维护与管理专业委员会

编辑出版委员会

2000 年 10 月

# 前 言

Internet的发展和应用水平已成为衡量一个国家政治、经济、军事、技术实力的标志。Internet改变着人们的工作、学习和生活方式。发展网络技术是国民经济现代化建设不可缺少的必要条件。网络将使信息的获取、传递、存储、处理和利用更加有效、更加迅速。可以预见，在不久的将来，人们的日常生活和工作对Internet的依赖程度将超过现在对电话和汽车的依赖程度。

然而，在人们热衷和沉醉于Internet及其E-Mail、Web和FTP中的时候，千万不要忽视日益严峻的Internet的安全问题。Internet上的黑客和不法之徒无须“飞檐走壁”、“穿墙入室”，即可轻意地取走你的机密文件，窃取你的银行存款，破坏你的企业账目，公布你的隐私信函，篡改、干扰和毁坏你的数据库，甚至直接破坏你的磁盘或计算机，使你的网络瘫痪或崩溃。人们对Internet及其部件的依赖程度越高，可能遭受的侵害和损失就越大。因此，我们必须充分认识和了解这些风险，采取切实有效的措施，防范风险，加强安全，减少危害和损失，保证计算机网络资源的安全，保护信息的安全。为此，我们编著了《计算机网络安全与加密技术》一书。

本书共分17章和5个附录。书中仔细分析了各个组成部分的安全风险、威胁和攻击，介绍了其安全技术和方法，给出了相应的加密程序及其应用。本书资料翔实，深入浅出，结构合理，层次清晰。每章前面有内容提要，章末有内容小结。全书最后有参考文献，可供读者复习巩固和深入研究。书中融入了作者多年对计算机安全研究和网络安全研究的心血和经验，有一定的理论深度和很高的实用价值。

本书由李海泉教授编著了第一、二、五、六、七、八、九、十一、十二、十四、十五、十六、十七章和附录一～四，由李健和李海泉一起编著了本书第三、四和十章，由李健编写了第十三章和附录五。全书最后由李海泉教授进行整理和统编。本书编写中得到了中国科学院软件所黄昌夺教授和中国计算机学会网络专业委员会委员、西安交通大学计算机博士生导师郑宗淇教授的支持和帮助；西北大学计算机科学系卞雷教授审阅了全书手稿，提出了宝贵的意见。西安石油大学计算机系李刚、张莉、程德玉、朱艳、万芳、吕凯元、孙雅冰等

同学帮助完成了书稿抄写工作，李刚等人帮助完成了绘图和部分书稿打印工作。此外，本书的撰写还得到了西安石油大学计算机系和有关教研室的关心和支持。在此一并表示感射。

本书可作为计算机科学技术及应用、信息工程、软件工程、信息管理与信息系统、金融信息管理、会计信息管理、计算机信息安全等专业的科技人员的工具性参考书，还可作为大专院校上述专业教材和科技人员进修教材，并可供上述专业的研究生学习和参考。

由于作者水平有限，错误和缺点在所难免，欢迎读者和计算机界同行批评、指正。

李海泉　李　健

2000 年 6 月

# 目 录