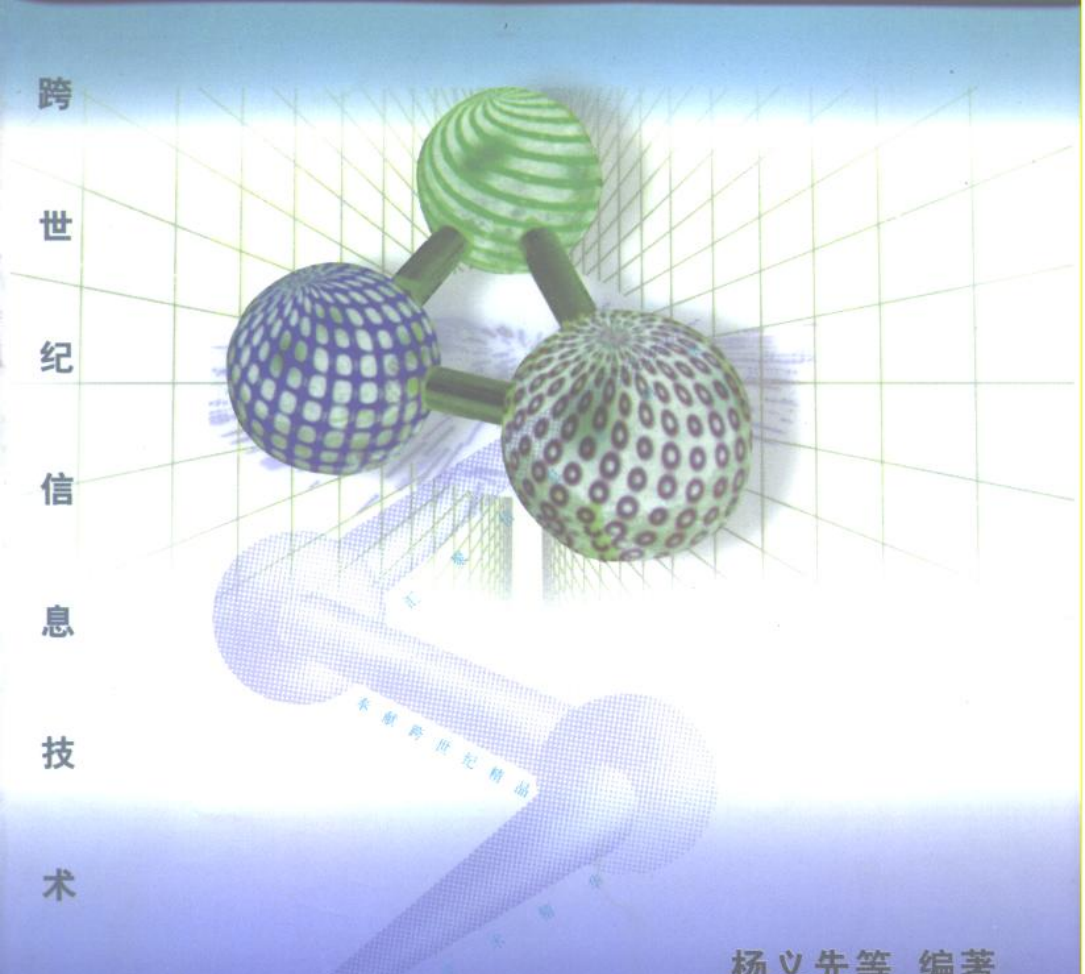
跨世纪信息技术丛书



杨义先等 编著

网络信息安全与保密

WANGLUO XINXI ANQUAN YU BAOMI

北京邮电大学出版社

《跨世纪信息技术丛书》

网络信息安全与保密

杨义先　李名选　编著

北京邮电大学出版社

·北京·

图书在版编目(CIP)数据

网络信息安全与保密/杨义先，李名选编著．－北京：北京邮电大学出版社，1999.11

（跨世纪信息技术丛书）

ISBN 7-5635-0386-2

Ⅰ.网… Ⅱ.①杨… ②李… Ⅲ.①信息网络-安全技术 ②信息网络-保密技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(1999)第 62657 号

网络信息安全与保密

编　　著　杨义先　李名选

责任编辑　周　明

*

北京邮电大学出版社出版发行

新华书店北京发行所发行　各地新华书店经售

河北省高碑店市印刷厂印刷

*

850×1 168 毫米　1/32　印张 6.625　字数 166 千字

1999 年 11 月第 1 版　1999 年 11 月第 1 次印刷

印数：1—10 000 册

ISBN 7-5635-0386-2/TN·173　　定价：10.40 元

• 跨世纪信息技术丛书 •

编 委 会

本书顾问

周　宪　信息产业部电信科学研究院院长

蔡　红　国家保密局副局长

樊守志　北京市安全局局长

吕宾珉　北京市公安局副局长

朱　炎　北京市科委副主任

华平澜　北京市信息化工作办公室副主任

赵祥伟　北京市科委保密处处长

总 序

信息化浪潮如日中天，它描绘出现代化之旅的时代画卷。信息技术如同一架强劲的发动机，不管人们对它的应用持何种态度，我们都不得不跟上它的步伐。信息技术在其应用中所赋有的强渗透性和高附加值，而成为信息时代的核心技术和中坚力量，它影响和决定着现代技术总体的走向。

网络的平民化和商业化为五十年代以来的新信息革命提供了一次转机，这一转机就是八十年代之后，网络逐步取代电脑成为信息社会的技术核心，亦即电脑成为网络的终端，而并非网络作为电脑的外围。这一革命性的变化，同时演绎出现代通信的时代意义：通信不仅仅作为信息传递的手段，它还能在信息存储和转换、信息处理和收发等方面扩展着自身的功能。现代通信向着信息业全面延伸，现代通信的内涵就是信息网络，就是国家或国际的信息基础结构（俗称“信息高速公路”）的技术平台。从这种意义上看，现代通信的技术，正成为信息技术体系中的主导和基质。

北京邮电大学作为国内通信领域著名大学，聚集着一批学识卓越的中青年技术专家，他们作为信息技术某一领域的领衔人物，始终站在信息技术研发活动中的前沿地带。他们把自己在国外或国内获得的最新知识和丰硕成果，把自己对信息技术的深刻理解，连同他们的智慧和热情，凝聚在这套跨世纪信息技术丛书之中，呈现给读者。

纵览这套丛书，这其中有执全光通信领域研究之牛耳的顾畹仪教授对波分多用（WDM）全光通信网作为光纤通信未来发展首选方案的据理力争；有国内外知名的信息安全权威杨义先教授对

网络与信息安全技术前沿及趋势的恢宏论述;有网管及通信软件专家孟洛明教授对现代网络管理技术的通览;有智能网领域成果斐然的杨放春教授对智能化现代通信网的诠释;有目前我国电子商务炙手可热的学者吕廷杰教授对我国实现电子商务软环境及社会影响等给予的引人注目的回答;有光纤通信专家纪越峰教授对综合业务接入技术和光波分复用系统的精辟论述;有 CERNET 专家马严教授对计算机互联网技术及其演进的展望;有刘元安和郭军两位年轻的博士生导师分别对未来移动通信和智能信息技术所作的前瞻性的描述。

我们认为这几位中青年学俊,从他们各自所在的重点研究项目和教学工作中抽出时间来写作这套丛书,其意义丝毫不亚于他们手头的一二个项目。这些年轻的博士生导师不仅仅是最新信息技术的生产者,而且是这些最新知识的整理者和传播者。他们点拨出热门技术中的技术轨道,直叙其来龙去脉,如数家珍,娓娓动听。他们为了整个文稿简捷、生动、明快而不厌其烦地几易其稿,这令我们既感动又宽慰。北京邮电大学出版社为这套丛书的出版倾注了大量的精力,我们谨此致以诚挚的谢意。是为序。

丛书编委会

一九九九年十月

前　言

因特网已遍及世界180多个国家，容纳了60多万个网络，接入了2000多万台主机，为1亿多用户提供了多样化的网络与信息服务。在因特网上，除了原来的电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、静态及视频等通信技术都在不断地发展与完善。在信息化社会中，网络信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络信息系统的依赖也日益增强。

各种各样完备的网络信息系统，使得秘密信息和财富高度集中于计算机中。另一方面，这些网络信息系统都依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

随着网络的开放性、共享性、互连程度的扩大，特别是因特网的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，比如，电子商务、电子现金、数字货币、网络银行等，以及各种专用网的建设，比如金融网等，使得网络与信息系统的安全与保密问题显得越来越重要，成了关键之所在。

现在，几乎每天都有各种各样的黑客故事：1996年8月17日，美国司法部的网络服务器遭到黑客入侵，并将“美国司法部”的主页改为“美国不公正部”，将司法部部长的照片换成了

阿道夫·希特勒，将司法部徽章换成了纳粹党徽，并加上一幅色情女郎的图片作为所谓司法部部长的助手。1994年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国CITYBANK银行发动了一连串攻击，通过电子转帐方式，从CITYBANK银行在纽约的计算机主机里窃取1100万美元。1996年9月18日，黑客又光顾美国中央情报局的网络服务器，将其主页由“中央情报局”改为“中央愚蠢局”。1996年12月29日，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他80多个军方网址。1996年12月29日，美国空军的全球网页完全变了样，其中空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言。1988年11月，美国康乃尔大学的学生Morris编制的名为“蠕虫”的计算机病毒通过因特网传播，致使网络中约7000台计算机被传染，造成经济损失约1亿美元。1998年8月22日，江西省中国公用多媒体信息网（169台）被电脑黑客攻击，整个系统瘫痪。1998年4月25日下午5时30分左右，一神秘的电脑黑客非法侵入中国公众多媒体信息网（CHINANET）贵州站点的WWW主机，将“贵州省情”的WEB页面改换成一幅不堪入目的淫秽画面。1998年6月16日，黑客入侵了上海某信息网的8台服务器，破译了网络大部分工作人员的口令和500多个合法用户的帐号和密码，其中包括两台服务器上超级用户的帐号和密码。1998年10月27日，刚刚开通的，由中国人权研究会与中国国际互连网新闻中心联合创办的“中国人权研究会”网页，被黑客严重篡改。

事实上，我们听到的关于通过网络的入侵只是实际所发生的事例中非常微小的一部分。相当多的网络入侵或攻击并没有被发现。即使被发现了，由于这样或那样的原因，人们并不愿意公开

它，以免公众作出强烈的惊慌失措的反应。绝大多数涉及数据安全的事件从来就没有被公开报道过。据统计，商业信息被窃取的事件以每月260%的速率在增加。然而，据专家估计，每公开报道一次网络入侵，就有近500例是不被公众所知晓的。

现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互连程度的扩大，这种安全机制对于网络环境来讲形同虚设。另外，目前网络上使用的协议，比如TCP/IP协议，在制订之初也没有把安全考虑在内，所以没有安全可言。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

面对如此严重危害网络信息系统的种种威胁和网络安全与保密的重要性，必须采取有力的措施来保证网络信息的安全与保密。网络的安全措施一般分为三类：逻辑上的、物理上的和政策上的。面对越来越严重危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来有效地防范计算机犯罪显得十分有限和困难，因此也应采用逻辑上的措施，即研究开发有效的网络安全技术。

即使是有了非常完备的安全与保密政策法规，有非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但是如果这些知识得不到普及，那么所有努力都是白费。然而，目前国内几乎没有一本科普性的书籍对网络信息系统的安全与保密进行过全面系统的介绍。本书的主要目的之一便是想填补这一空白。

本书是北京邮电大学信息安全中心和北京市科委保密处的全体成员集体智慧的结晶。林晓东博士、邢育森博士、夏光升博士、冯运波博士、李子臣博士、张磊学士、陈文杰学士等为本书提供了丰富的参考文献。特别感谢胡正名教授、钮心忻博士、孙

伟博士、李中献博士、詹榜华博士。他们同心协力，率领北京邮电大学信息安全中心近40位研究人员在网络信息安全与保密研究方面的丰富成果是本书的营养源泉。感谢北京邮电大学出版社将此书选入《跨世纪信息技术丛书》。

由于作者水平有限，书中难免出现各种失误和不当，欢迎大家批评指正。

作　者

1999年9月

目　录

1

网络信息安全与保密综论

2

密码技术简介

3

防火墙技术简介

4

虚拟专用网(VPN)技术简介

5

病毒与反病毒技术简介

6

其他安全与保密技术简介

1 网络信息安全与保密综论

1.1 网络信息安全与保密的内涵是什么?

网络信息安全与保密是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。从技术角度看，网络信息安全与保密是一个涉及计算机科学、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边缘性综合学科。网络信息安全与保密的重要性有目共睹。特别是随着全球信息基础设施和各国信息基础设施的逐渐形成，国与国之间变得“近在咫尺”。网络化、信息化已成为现代社会的一个重要特征。网络信息本身就是时间，就是财富，就是生命，就是生产力。实际上，网络的快速普及、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。

事物总是辩证统一的。科技进步在造福人类的同时，也带来了新的危害。从某种意义上讲，网络信息系统的广泛普及，就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。网络信息系统中的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。网络信息安全与保密便是这些众多新课题中最具代表性的例子。

根据《汉语大词典》（罗竹风主编）的解释，“安全”有两层含义：其一是指“平安，无危险”；其二是指“保护，保全”。“保密”，则指“保守事物的秘密，不使泄漏”。仅仅根据词典的