全国高职高专规划教材

计算机网络安全技术

叶忠杰　主编

陈月波　马云芳　副主编

科学出版社

北　京

内 容 简 介

本书介绍了计算机网络安全的基本知识和技术，包括计算机网络安全概论、信息加密技术、局域网络的安全、网络操作系统安全技术与应用、防火墙技术与应用、数字签名技术与 CA 认证技术、Internet 安全技术、计算机病毒与网络安全、网络黑客攻防技术、计算机网络的安全评估等内容。通过这些内容，使读者能够掌握计算机网络安全的基本概念和应用技术，了解设计和维护安全网络系统的基本手段与常用方法。

本书适合作为大专院校相关专业的教材，也可供各行各业从事计算机网络应用和管理的读者阅读和参考。

图书在版编目(CIP)数据

计算机网络安全技术/叶忠杰主编.—北京：科学出版社，2003
（全国高职高专规划教材）
ISBN 7-03-011989-4

Ⅰ.计… Ⅱ.叶… 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(2003)第 065814 号

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 8 月第 一 版 开本：787×1092 1/16
2004 年 2 月第二次印刷 印张：16 1/2
印数：5 001—8 000 字数：372 000
定价：22.00 元
（如有印装质量问题，我社负责调换〈路通〉）

全国高职高专规划教材编委会名单

主　任　俞瑞钊

副主任　陈庆章　周必水　刘加海

委　员　（以姓氏笔画为序）

王　雷　王筱慧　方　程　方锦明　卢菊洪　代绍庆

吕何新　朱　炜　刘向荣　江爱民　江锦祥　孙光弟

李天真　李永平　李良财　李明钧　李益明　余根墀

汪志达　沈凤池　沈安衢　张　元　张学辉　张锦祥

张德发　陈月波　陈晓燕　邵应珍　范剑波　欧阳江林

周国民　周建阳　赵小明　胡海影　秦学礼　徐文杰

凌　彦　曹哲新　戚海燕　龚祥国　章剑林　蒋黎红

董方武　鲁俊生　谢　川　谢晓飞　楼　丰　楼程伟

鞠洪尧

秘书长　熊盛新

本书编写人员名单

主　编　叶忠杰

副主编　陈月波　马云芳

撰稿人　叶忠杰　陈月波　马云芳　邱　勋

前　言

Internet的建设与发展给整个社会的科学、技术、经济与文化带来了巨大的推动和冲击，同时也给计算机网络工作者带来了新的挑战。Internet/Intranet的安全技术是一项长期的、综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的规划。

随着Internet/Intranet技术的广泛应用，网络安全面临重大挑战。事实上，资源共享和信息安全历来就是一对矛盾，而计算机网络体系结构中的开放性决定了网络安全问题是先天存在的，TCP/IP框架基本上是不设防的。随着Internet的飞速发展，计算机网络资源共享进一步加强，随之而来的是安全问题日益突出，黑客攻击肆虐全球。同时，目前人们也开始重视来自网络内部的安全威胁。

近几年来，有关计算机网络安全的书籍逐渐增多，有翻译国外的著作，也有国内专家自己编著的，这些书各有各的特点，为各层次读者提供了宝贵的资料，也指导着国内计算机网络安全技术的应用与研究。

本书的主要特点有以下三个方面。

首先是通俗易懂。计算机网络的技术性很强，网络安全的技术也比较晦涩难懂，这可能是初学者的共同心理。本书紧紧抓住“入门”这个中心，以通俗的语言和清晰的叙述方式，向读者介绍计算机网络安全的基本理论、基本知识和常用技术。同时，由于网络安全方面的许多资料是翻译过来的，因此，往往对同一个事物有不同的表述方法，常使读者感到困惑，针对这一问题，本书在查阅多方资料的基础上，尽量使其趋于一致。

其次是注重实用。阅读本书，可使读者掌握计算机网络安全的基本概念，并了解设计和维护网络及其应用系统安全的基本手段和方法。本书在编写形式上比较多地介绍方法，突出应用的需求，尽量避开原理性的介绍和一些基本数学理论内容，力争反映网络安全技术的最新发展，主要是想满足构造安全的网络应用系统的实际需要。

第三是资料新颖。计算机应用技术和网络技术的发展是非常迅速的，为了使本书能反映较新的理论和技术，我们参阅了大量的国内外最新的资料，力图尽量靠近新知识、新技术的前沿。

由于本书着眼于网络安全技术的应用，故未涉及计算机网络安全环境的部分内容。

全书共分10章。本书的第1、2、5、10章由叶忠杰编写，第4、6、8章及第9.3.2节由陈月波编写，第3、9章（除9.3.2节外）由马云芳编写，第7章由邱勋编写。

本书适合作为大专院校相关专业的教材，也可供各行各业从事计算机网络应用和管理的读者阅读和参考。笔者在向读者推荐本书的同时，也感到计算机网络安全技术的博大精深和迅速发展，以我们现有的水平很难在本书中全面、准确和及时反映，因此书中会有疏漏之处，在此恳请读者和有关专家批评指正。邮件地址：yezhongjie@zjvtit.edu.cn。

编　者

2003年6月

目　录

第 1 章　计算机网络安全概论

本章要点

网络技术的应用正在日益普及，电子商务、电子政务都是以网络为基础的新兴领域。伴随网络技术应用领域的扩展，网络安全已引起人们极大的关注。本章主要介绍以下内容：

- 网络安全的概念及涵义
- 网络安全的特征与安全威胁
- 网络分层模型及各层的安全性
- 安全网络的体系结构模型
- OSI 体系结构的安全机制与安全服务
- 网络安全体系结构模型分析

通过本章的学习，读者应该对网络安全的威胁、网络安全的重要性和安全网络框架模型有一个全面的印象，以利于后续具体内容的学习。

读者应记住一句话："安全并非是一件产品，而是一个完整的过程。"

本章难点

信息安全构架。

1.1　网络安全概述

网络安全是一个关系到国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题，也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学科。网络安全的重要性已有目共睹。特别是随着全球信息基础设施和各个国家的信息基础逐渐形成，国与国之间变得"近在咫尺"，信息电子化已成为现代社会的一个重要特征。信息本身就是时间，就是财富，就是生命，就是生产力。因此，各国开始利用电子空间的无国界性和信息战来实现其以前军事、文化、经济侵略所达不到的战略目的。另外，由于网络的快速、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（即在 Internet 上开展金融服务）成为网络时代必不可少的一个产物。但是科技进步在造福人类的同时，也带来了新的危害。事物总是辩证统一的，福兮祸焉，祸兮福焉。从某种意义上讲，计算机网络的产生就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽（如计算机网络犯罪）相伴而来。计算机网络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。比如，如何解决网络安全问题？如何解

决由于信息网络化、商务电子化后给社会带来的不稳定因素？实际上，由于信息密集的金融业电子化后，使得国际上资金流动、清算的速度加快，巨额资金操纵、洗钱等非法金融行为变得非常便利，这样极有可能爆发国家甚至世界级的金融危机。1998 年发生的亚洲金融危机很大程度上是由于金融电子化。大量事实表明，确保网络安全已经是一件刻不容缓的大事，否则悔之晚矣！有人预计，未来计算机网络安全问题比核威胁还要严重，因此，解决网络安全课题具有十分重要的理论意义和现实背景。

1.1.1 网络安全案例

1. 国外计算机网络出现的安全问题案例

生活在今天的人们，常常听到关于黑客的故事，这些都是一些有着传奇色彩的故事。

1988 年 11 月 2 日，美国 6000 多台计算机被病毒感染，致使 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即做出反应，国防部成立了计算机应急行动小组。这次事件中遭受攻击的有 5 个计算机中心和 12 个区节点，连接着政府、大学、研究所和拥有政府合同的约 25 万台计算机。这次病毒事件，计算机系统直接经济损失达 9600 万美元。

1991 年 5 月，在 Biscay 海湾发生了一起由于网络系统被攻破造成的沉船事故。由于欧洲气象预报中心的计算机系统被网络黑客侵入并进行破坏，导致气象预报卫星不能正常工作，致使一场暴风雨的预报失误，酿成了这起不该发生的沉船事故。

1993 年 6 月，美国一家医院链接到网络上的一些测试数据结果被黑客侵入后，许多被测者误认为自己患上了癌症。

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，通过电子转账方式，从 CITYBANK 银行在纽约的计算机主机里窃取了 1100 万美元。

2. 我国计算机互联网出现的安全问题案例

1996 年 2 月，刚开通不久的 Chinanet 受到攻击，且攻击得逞。

1996 年秋，北京某 ISP 与其用户发生矛盾，此用户便攻击该 ISP 的服务器，致使服务中断了数小时。

1997 年初，北京某 ISP 被黑客成功侵入，并在清华大学的“水木清华”BBS 站的“黑客与解密”讨论区张贴有关如何免费通过该 ISP 进入 Internet 的文章。

1998 年 6 月 16 日，黑客侵入了上海某信息网的 8 台服务器，破译了网络大部分工作人员的口令和 500 多个合法用户的账号和密码，其中包括两台服务器上超级用户的账号和密码。同年 8 月 22 日，江西省中国公用多媒体信息网（169 网）被电脑黑客攻击，整个系统瘫痪。

事实上，我们知道的网络入侵事件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，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。据

专家估计，每公开报道一次网络入侵事件的背后，有近 500 例是不被公众所知晓的。可以说，现在的 Internet 上，没有任何事情是可以绝对相信的。

今天，网络和主机是否易受攻击（Vulnerable）成了网络世界最受关注的事情和最时髦的话题之一。网络的安全不只是研究者的课题，已变成全球 Internet 使用者和建设者最关注的话题。

1988 年以前，大部分入侵者使用的方法主要是猜口令、利用系统的配置不当以及系统上软件本身的漏洞。到了 1994 年，在这些方法的基础上，增加了新的方法，如通过读操作系统源代码的方法来获取系统的漏洞，并以此展开对系统的攻击。一些网络黑客编写的攻击站点的工具软件，在 Internet 上也公开发布，这就给网络安全带来了更严峻的挑战。

面对越来越严重的危害计算机网络的种种威胁，必须采取措施来保证计算机网络的安全。但是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，大部分是把安全机制建立在物理安全上。随着网络的互联程度的扩大，这种安全机制对于网络环境来讲形同虚设。同时，目前网络上使用的协议，如 TCP/IP 协议，在制定之初也没有把安全考虑在内，所以网络协议本身就是不设防的。TCP/IP 协议中存在很多的安全问题，不能满足网络安全要求。另外，网络的开放性和资源共享也是安全问题的一个主要根源，解决这个问题主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

网络的安全措施一般要分为三类：逻辑上的、物理上的和政策上的。面对危害计算机网络安全的种种威胁，仅仅利用物理上和政策上的手段是十分有限和困难的，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，例如，安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其保密性（Secrecy）和完整性（Integrity）；防止非法用户（或程序）的侵入，限制网络上用户（或程序）的访问权限，保证信息存放的私有性（Privacy）。除了私有性和完整性之外，一个安全的计算机网络还必须考虑通信双方的身份真实性（Authenticity）和信息的可用性（Available）。

网络安全就是要保证网络上存储和传输信息的安全性。为了解决这个问题，国内外很多研究机构在这方面做了很多工作，主要有数据加密、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡（存储卡、加密存储卡、CPU 卡）、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

1.1.2　计算机安全和网络安全的含义

计算机安全的主要目标是保护计算机资源免受毁坏、替换、盗窃和丢失。计算机资源包括计算机设备、存储介质、软件、计算机数据等。

网络安全从其本质上来讲就是网络上的信息安全，它涉及的领域相当广泛。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。下面给出网络安全的一个通用定义。

网络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，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可连续、可靠、正常地运行，网络服务不中断。

从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望保存在计算机系统上的用户信息不受其他非法用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现陷阱、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，它们希望对非法的、有害的、涉及国家或商业机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对机构造成经济损失。

从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，因此，必须对其进行控制。

网络安全在不同的应用环境有不同的解释。

运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄露干扰他人或受他人干扰，本质上是保护系统的合法操作和正常运行。

网络上系统信息的安全，包括用户口令鉴别、用户存取权限控制、数据存取权限，存储方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

网络上信息传播安全，即信息传播后果的安全性，主要是信息过滤。它侧重于防止和控制非法、有害的信息进行传播。避免公用通信网络上大量自由传输的信息失控。本质上是维护道德、法律和国家利益。

网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。因此，网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。

1.1.3 安全网络的特征

1. 保密性

信息不泄露给非授权的用户、实体或进程。数据保密性是保证只有授权用户可以访问数据，而限制其他用户对数据的访问。数据保密性分为网络传输保密性和数据存储保密性两个方面。就像电话可以被窃听一样，网络传输也可以被窃听，解决的办法是对传

输数据进行加密处理。数据存储保密性主要通过访问控制来实现的，管理员对数据进行分类，分成敏感型、机密型、私有型和公用型等几类，对这些数据的访问加以不同的访问控制，如经理可以访问所有数据，一些技术人员除了敏感型数据以外都能进行访问，一般职员只能访问私有型数据和公司型数据。这种访问控制许多安全型操作系统都能做到，如 UNIX、Windows NT 等操作系统，但 Windows 95 和 DOS 等操作系统不具有这种功能。

保证数据保密性的一个容易被忽视的环节是人的安全意识。一个黑客可能会收买一个职员，或欺骗一个职员，从而获得机密数据，这是一种常见的攻击方式，被称为社会工程（Social Engineering）。

2. 完整性

数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。数据的完整性的目的是保证计算机系统上的数据和信息处于一种完整和未受损害的状态，这就是说数据不会因有意或无意的事件而被改变或丢失，数据完整性的丧失直接影响到数据的可用性。

影响数据完整性的因素很多，有人为的蓄意破坏，有人为的无意破坏，有软、硬件设备的失效，还有自然灾害等。但可以通过访问控制、数据备份和冗余设置来实现数据的完整性。

3. 可用性

可被授权实体访问并按需求使用的特性，即当需要时能否存取和访问所需的信息，例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。Internet 蠕虫就是依靠在网络上大量复制并且传播，它占用大量 CPU 处理时间，导致系统越来越慢，直到网络发生崩溃，用户的正常数据请求不能得到处理，这就是一个典型的“拒绝服务”攻击。数据不可用也可能是由软件缺陷造成的，如微软的 Windows 总是有缺陷被发现。

4. 不可否认性

不可否认性也称不可抵赖性，在信息交互过程中，确信参与者的真实同一性，即所有参与者都不能否认和抵赖曾经完成的操作和承诺，利用信息源证据可以防止发信方不真实地否认已发信息，利用提交接收证据可以防止收信方事后否认已经接收的信息。数字签名技术是解决不可否认性的重要手段之一。

5. 可控性

可控性是人们对信息的传播路径、范围及其内容所具有的控制能力，即不容许不良内容通过公共网络进行传输。

1.1.4　网络的安全威胁与安全网络的实现

1. 网络的安全威胁

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上

存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。如果因为安全因素使得信息不敢放进像 Internet 这样的公共网络，那么办公效率及资源的利用率都会受到影响。任何事物总要辩证地看待，一方面，网络提供了资源的共享性、用户使用的方便性，通过分布式处理提高了系统效率和可靠性；另一方面，正是这些特点增加了网络受攻击的可能性。对网络的威胁来自很多方面，并且随着时间的变化而变化。网络威胁是指对网络构成威胁的用户、事物、想法、软件等，网络威胁利用系统暴露的要害或弱点，导致信息的保密性、完整性和可用性程度下降，造成不可估量的经济和政治损失。威胁有两种：无意的和有意的，无意的威胁包括人为操作错误、设备故障、自然灾害等很多不以人的意志为转移的事件；有意的威胁包括窃听、计算机犯罪等人为的破坏。当前主要的威胁来自以下几个方面。

- 自然灾害、意外事故。
- 人为行为，比如使用不当、安全意识差等。
- 黑客行为，由于黑客的入侵或侵扰，造成非法访问、拒绝服务、计算机病毒、非法链接等。
- 内部泄密和外部的信息泄密、信息丢失。
- 电子间谍活动，比如信息流量分析、信息窃取等。
- 信息战。
- 网络协议中的缺陷，例如 TCP / IP 协议的安全问题等。

2. 安全网络的实现

为了实现网络的安全性，不仅靠先进的技术，而且也要靠严格的安全管理、安全教育和法律规章的约束，具体如下。

- 先进的网络安全技术是网络安全的根本保证。用户对自身面临的威胁进行风险分析和评估，决定其所需要的安全服务种类，选择相应的安全机制，然后综合先进的安全技术，形成全方位的安全系统。
- 严格的安全管理。各使用计算机网络的机构、企业和单位应建立相应的网络管理办法，加强内部管理，建立合适的网络安全管理系统、安全审计体系，提高整体网络的安全意识。
- 制定严格的法律规范体系。计算机网络是一种现代高科技的新生事物，法律规范相对滞后。许多行动无法可依、无章可循，因此导致了一段时间内对计算机犯罪处置的无序状态。因此，必须完善相应的法律和规范，同时严格执行，坚决打击这些犯罪活动，保护国家机密和用户的合法权益，使犯罪分子慑于法律规范，不敢轻举妄动。

1.2 网络安全体系结构

计算机网络中各站点要进行通信、交换信息、共享网络资源、完成分布处理，就必须规定各站点共同遵守的通信协议。为此，国际标准化组织（ISO）制定了开放系统互