高等职业教育“十二五”规划教材
高职高专计算机网络系列教材

Computer Network
Security Techn

计算机网络安全技术（第三版）

叶忠杰　主编

科学出版社

高等职业教育“十二五”规划教材

高职高专计算机网络系列教材

计算机网络安全技术

（第三版）

叶忠杰　主编

陈月波　戎　成　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、技术和实际操作技能，主要包括计算机网络安全概论、信息加密技术基础、局域网安全技术基础、Internet 服务安全技术及应用、网络防火墙技术与应用、黑客攻击及防范技术、病毒及其防范技术、数字认证与 VPN 技术和计算机网络安全管理与评估等内容。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、实用技术，了解设计和维护网络系统安全的基本手段、方法及技术，并能实际解决网络安全的基本问题。

本书内容丰富、结构合理、通俗易懂、注重实用，适合作为高职高专院校相关专业的计算机网络安全课程教材及教学参考用书，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. —3 版. —北京：科学出版社，2013
（高等职业教育“十二五”规划教材·高职高专计算机网络系列教材）
ISBN 978-7-03-036565-1

Ⅰ.①计… Ⅱ.①叶… Ⅲ.①计算机网络-安全技术-高等职业教育-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 018579 号

责任编辑：孙露露 郭丽娜 / 责任校对：马英菊
责任印制：吕春珉 / 封面设计：耕者设计工作室

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

北京路局票据印刷厂印刷

科学出版社发行 各地新华书店经销
*
2013 年 2 月第 三 版 开本：787×1092 1/16
2013 年 2 月第一次印刷 印张：18 3/4
字数：425 000

定价：32.00 元

（如有印装质量问题，我社负责调换<路局票据>）
销售部电话 010-62134988 编辑部电话 010-62135763-8212

前　言

《计算机网络安全技术》自2003年首版以来，一直受到广大师生和读者的喜爱，不仅使编者深感压力与责任，也是本书继续改版的动力。感谢这些年来本书的所有参与者，特别是教材编写者的辛勤劳动和敬业精神，感谢使用本书的师生和读者对本书提出的大量宝贵意见和建议。

计算机网络安全技术日新月异，新思路、新技术、新产品层出不穷。旧系统还在不断出现新问题，新系统安全问题依旧存在，新应用带来新的安全问题。所以，为了持续保持计算机网络系统的强壮性、可靠性，就必须不断地学习新的理论与吸收新的技术，及时发现新的问题并予以解决。《计算机网络安全技术（第三版）》以通用、实用、易用见长，及时纳入了新知识、提供了新方案，如新增关于移动互联网、移动终端安全的知识与技术等。

近几年来，有关计算机网络安全方面的教材不断涌现，这些教材各有特点，为各层次各类型读者提供了宝贵的资料，也指导和帮助着国内计算机网络安全技术的应用与研究。

本书有以下三个方面的主要特点。

第一是定位明确。本书定位于非信息安全类专业的计算机网络安全课程，编写理念追求：体系基本完整，理论不求深入；注重知识概念，强调深入浅出；注重实际应用，突出能力训练。

第二是通俗易懂。计算机网络安全的理论性、知识性、技术性较强，本书以清晰的思路、合理的体系、通俗的语言，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。

第三是注重实用。学习本书可使读者方便地掌握计算机网络安全的基本概念，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，熟悉使用常见安全技术解决基本安全问题。在内容选取上，力求反映计算机网络安全的新问题、新技术和新应用，满足构造计算机网络安全的基本需要。

本书在前两版的基础上，整合和增加了部分内容，具体共分9章，内容主要包括计算机网络安全概论、信息加密技术基础、局域网安全基础技术、Internet服务安全技术及应用、网络防火墙技术与应用、黑客攻击及入侵检测、病毒及其入侵检测、数字认证与VPN技术和网络安全管理与评估等。本书的第1～3章由浙江交通职业技术学院的叶忠杰编写，第4章和第8章由浙江交通职业技术学院的戎成编写，第5章和第7章由浙江金融职业学院的陈月波编写，第6章和第9章由台州职业技术学院的沈文华编写。为了方便教学，本书配有电子课件，读者可到网站（www.abook.cn）上下载或发邮件至主编邮箱zj-ye@163.com索取。

编者在向读者推荐本书的同时，也深感计算机网络安全技术的博大精深、日新月异，以编者的现有水平很难在本书中给予全面、准确和及时反映，书中难免会有疏漏甚至错误，在此恳请读者和专家批评指正。

编　者

2012年6月

目　录

第1章

计算机网络安全概论

学习指导

教学目标

本章主要介绍计算机安全、网络安全与信息安全的概念及相互关系；分析了近几年信息安全的严峻形势，随着移动互联网的异军突起，移动互联网安全成为网络安全的新领域；最后，简单分析了 OSI、TCP/IP 及我国的计算机网络安全体系结构。

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全面的了解，以利于后续具体内容的学习。

要点内容

计算机安全、网络安全及信息安全的概念。

计算机网络安全形势。

移动互联网安全问题。

安全服务与安全机制。

网络安全体系结构。

能力要求

掌握计算机安全、网络安全、信息安全的基本概念。

了解计算机安全、网络安全、信息安全三者之间的关系。

了解移动互联网安全与网络安全的关系。

掌握安全服务、安全机制及其关系。

了解网络安全体系架构。

1.1 计算机网络安全概述

1.1.1 计算机安全

当今社会是技术高速发展的信息社会，人类的一切活动均离不开信息，而计算机系统是实现对信息进行收集、分析、加工、处理、存储传输等操作的主体部分。可是计算机系统并不安全，它潜伏着严重的不安全性、脆弱性和危险性。攻击者经常利用计算机存在的缺陷对其实施攻击和入侵，窃取机密资料，导致计算机系统的瘫痪等，给社会造成巨大的经济损失，甚至危害到国家和地区的安全。因此计算机的安全问题关系到人类生活与生存，必须给予充分重视并设法解决。

1. 计算机安全的概念

计算机安全中的“安全”一词对应的英文是“security”，含义有两方面：一方面是指安全的状态，即免于危险；另一方面是指对安全的维护，即安全措施和安全机构。

国际标准化委员会有关计算机安全的定义是“为数据处理系统所采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。美国国防部对国家计算机安全的定义是“安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息”。我国公安部计算机管理监察司的定义是“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害”。

从上述定义中可看出，计算机安全不仅涉及技术问题、管理问题，还涉及有关法学、犯罪学、心理学等问题。可以用四部分来描述计算机安全这一概念，即实体安全、软件安全、数据安全和运行安全。而从内容来看，包括计算机安全技术、计算机安全管理、计算机安全评价与安全产品、计算机犯罪与侦查、计算机安全法律、计算机安全监察、计算机安全理论与政策。

2. 计算机面临的威胁

计算机面临的威胁主要有：电磁泄露、雷击等环境构成的威胁；软硬件故障和工作人员误操作等人为或偶然事故构成的威胁；利用计算机实施盗窃、诈骗等违法犯罪活动的威胁；网络攻击和计算机病毒构成的威胁；信息战的威胁等。

（1）环境构成的威胁

计算机的所在环境主要是场地与机房，会受到下述各种不安全因素的威胁。

电磁波辐射：计算机设备本身就有电磁辐射问题，也会受到外界电磁波的辐射和干扰，特别是自身辐射带有信息，容易被他人接收，造成信息泄露。

辅助保障系统：水、电、空调中断或不正常会影响系统运行。

自然因素：火、电、水、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲

等带来的危害。这些危害有的会损害系统设备，有的则会破坏数据，甚至损毁整个系统和数据。

（2）计算机的软硬件故障

电子技术的发展使电子设备出现故障的概率在几十年里一降再降，许多设备在它们的使用期内根本不会出错。但是由于计算机和网络中的电子设备往往极多，故障还是时有发生。器件老化、电源不稳、设备环境等很多问题会使计算机或网络的部分设备暂时或者永久失效。这些故障一般都具有突发的特点。

软件是计算机的重要组成部分，由于软件自身的庞大和复杂性，错误和漏洞的出现是不可避免的。软件故障不仅会导致计算机工作异常甚至死机，它所存在的漏洞还会被黑客利用来攻击计算机系统。

（3）人为的无意失误

人为的无意失误包括程序设计错误、误操作、无意中损坏和无意中泄密等。例如，操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会对计算机安全造成威胁。

（4）人为的恶意攻击

人为的恶意攻击包括主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重放、乱序、冒充等）。被动攻击是指在不干扰网络信息系统正常工作的情况下进行侦收、截获、窃取、破译和业务流量分析及电磁泄露等。这些人为的恶意攻击属于计算机犯罪行为，实施攻击的主要有以下几种。

1）雇员：人数最多的计算机罪犯由那些最容易接近计算机的人，即雇员构成。有时，雇员只是设法从雇主那里盗窃某种东西——设备、软件、电子资金、专有信息或计算机时间；有时，雇员可能出于怨恨而行动，试图“报复”公司。

2）外部用户：除雇员外，有些供应商或客户也可能有机会访问公司的计算机系统，例如，使用自动柜员机的银行客户。像雇员一样，这些被授权的用户可能获取秘密口令，或者找到进行计算机犯罪的其他途径。

3）黑客与非法侵入者：有些人认为这两类人相同，其实不然。黑客获取对计算机系统未经授权的访问，是因为这种行为有趣和具有挑战性。而非法侵入者则往往出于恶意，他们可能企图窃取技术信息，或者往系统中放置他们所谓的“炸弹”——一种破坏性计算机程序。

4）犯罪团伙：犯罪团伙可以像合法的商业人员一样使用计算机及网络，但是为了达到其非法的目的，如跟踪赃物或非法赌债而实施网络犯罪；另外，有的犯罪团伙使用计算机和打印机伪造支票、驾驶证等证件而实施犯罪。另外，伪造者使用计算机和打印机伪造支票、驾驶证等证件。

（5）计算机病毒与恶意软件

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义：“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”计算机病毒是一种高技术犯罪，具有瞬时性、动态性和随机性；不易取证，风险小破坏大，从而刺激了不法

分子的犯罪意识和犯罪活动；是某些人恶作剧和报复心态在计算机应用领域的表现，也是目前对计算机（尤其是 PC）的主要威胁之一。

恶意软件是恶意植入系统破坏和盗取系统信息的程序。恶意软件的泛滥是继病毒、垃圾邮件后互联网中的又一个全球性问题。恶意软件的传播严重影响了互联网用户的正常上网，侵犯了互联网用户的正当权益，给互联网带来了严重的安全隐患，妨碍了互联网的应用。特洛伊木马就是一种恶意软件。该程序看上去有用或无害，但却包含了旨在利用或损坏运行该程序的系统的隐藏代码。特洛伊木马和蠕虫都是典型的恶意软件。

1.1.2 网络安全

网络安全吗？这是人们本来就有的疑问，但现实的问题是网络有多不安全？

根据 Nielsen-NetRatings 公布的最新全球互联网指数显示，亚太地区的网络活动带动全球互联网的成长。以区域计算，亚太地区的互联网使用者的浏览页数为全球之冠。既然人们一天使用网络的时间这么久，还时常必须利用它来传递个人或公司的重要信息（如把写好的新产品上市计划书传给项目小组成员），处理与个人金钱有关的交易（如在网上书店购书或进入网上银行进行转账），因此网络的安全问题更是每一个人所必须重视的议题。

网络安全涉及上至国家安全下至普通百姓的计算机数据的保护，因此网络安全防范将会是每一个网络系统设计人员和管理人员的重要任务或职责。

1. 网络为什么不安全

要了解网络安全，必须要先了解网络为什么不安全。基本上，不同的人对网络安全的定义不同，一般上网的使用者关心的是连接上任何一台服务器时，客户端的计算机会不会被入侵或资料会不会被窃取；而网站管理员则集中精力在处理服务器端的网络安全问题，如何避免或延缓非法入侵者的阻断攻击行为或如何保护网站使用者资料不被窃取；进行信息流通的企业、经营电子商店的企业和上网消费的使用者所关心的则是如何有效运用安全的交易平台与加密解密技术，来避免文件资料被窃取以及网络诈欺等行为的发生。概括来说，造成网络不安全的主要原因可以分为以下四大类。

（1）软件本身设计不良或系统设计上的缺陷

1）软件本身设计不良，也就是俗称的软件有漏洞。例如，Internet Explorer 的早期版本，因为其本身设计上的疏忽，使得别人很容易就可以取得一些关于使用者的重要信息。这也就是为什么常会在 Microsoft Windows Update 网站上看到某软件的修正程序的原因。利用这些漏洞，要在网站内窃取资料或是植入后门程序等，都不是很困难的事。

2）系统设计上的缺陷。应用程序或系统毕竟是人编写出来的，无论软件设计师考虑的多严密，系统管理多严谨，实际应用在充满陷阱和恶意入侵的互联网中时，仍难免会让非法侵入者有机可乘。因此，在架设时要特别针对这些地方做补强，并配合其他防护措施，以确保网络的安全性。

ActiveX 带来的缺陷。ActiveX 控件是一种内嵌在 Web 网页中的组件，当使用者浏览网页时便会被激活。在许多情况中，可将 Web 的浏览器安全设定设置为“高”，来停止执行这些 ActiveX 控件。非法侵入者或病毒制造者以及其他恶意人士可能会使用

ActiveX 恶意程序代码来攻击计算机。

（2）网络防护不够严谨

除了互联网与计算机系统本身的安全威胁外，经营者对互联网认识的不足往往也会让系统出现安全漏洞。例如，在公司的网站和内部网络间没有架设防火墙，或是企业经营者由于不了解网络技术，听信网络供货商的建议，认为只要装设防火墙便可安全无忧，而忽略其他安全上的问题。

事实上，防火墙对于单纯的网络安全应用或许足够，但并非绝对安全，尤其是当网站服务越来越多时，必须与内部营运系统连接，否则将导致门户大开，安全漏洞也将接踵而至。另外，在 Windows 操作平台上作为资源共享的密码认证与存取权限过于宽松，任何人都可以通过“网络邻居”找到设置共享的 PC，进而任意读写别人的共享磁盘。

（3）网络威胁

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。

1）自然灾害、意外事故。

2）人为行为，如使用不当、安全意识差、内部和外部的信息泄密、信息丢失等。

3）黑客行为，由于黑客的入侵或干扰，造成非法访问、拒绝服务、计算机病毒、非法链接等。

4）电子间谍活动，如信息流量分析、信息窃取、信息战等。

5）网络协议中的缺陷，如 TCP/IP 协议的安全问题等。

（4）使用者的习惯及方法不正确

使用计算机时，应谨慎设定管理员密码。很多网管人员在设定 UNIX 中的 Root 与 Windows 中的 Administrator 的密码时，通常采用简单、好记的密码，如 abcd、1234、1111 或公司名称等，这如同没有设置保护系统的第一层使用者认证一样；而系统管理者的读写权限又较一般使用者大，一旦被入侵，后果不堪设想。很多人习惯将账号或密码写在便利贴上，并将其贴在计算机屏幕上，或轻易地把账号与密码告知他人，这就造成了计算机系统的安全隐患。

勿轻易开启来历不明的档案。有些用户收到来历不明的人寄的邮件附件时，无安全意识，随意打开。有些附件是计算机的隐身病毒，一旦执行，重要档案便被删除。有时则是档案本身藏有特洛伊木马程序，当使用者正在观看很有趣的动画时，入侵者早已将木马程序轻松地放进要入侵的系统中，通过这个程序便可以从远程掌控被入侵的计算机，只要连接网络，非法入侵者便随时可以把联网系统中重要的信息窃取到其硬盘中。

对于任何一家机构而言，雇员是必不可少的。但同时，雇员也是计算基础设施安全的最大威胁。因为大多数雇员没有意识到其在线行为的危险性。终端用户总是禁不住各种病毒附件的“诱惑”，为了获取浏览速度，雇员甚至关闭防火墙或者将登录密码保存在

计算机中。为了确保网络安全，这里列出十种常见危险的网络行为。

1）浏览不明邮件附件。

2）安装未授权应用。

3）关闭或禁用安全工具。

4）浏览不明 HTML 或文本消息。

5）浏览赌博、色情或其他非法站点。

6）公开自己的登录密码、令牌或智能卡信息。

7）重要的文档没有加密。

8）随意访问未知、不可信站点。

9）随意填写 Web 脚本、表格或注册页面。

10）频繁访问聊天室或社交站点。

上面四类情况，每一种都有可能是系统被入侵或资料被盗取的原因。预防胜于治疗，用户应及时排查，对症下药，防堵可能的安全死角。

2. 网络安全的含义

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，凡是涉及网络中信息的保密性、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，避免其他人或竞争对手利用窃听、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、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中有不同的解释。

1）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。

2）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。

3）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。

4）网络上信息内容的安全，即我们所讨论的狭义的“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。其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，网络安全要求通过各种计算机、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。

3. 网络安全的实现

为了实现网络的安全性，不仅靠先进的技术，还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。

1）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。

2）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。

3）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。

1.1.3 信息安全概述

前面简单分析了计算机安全和网络安全的概念，计算机系统承担信息的存储和处理功能，网络系统承担信息的传输功能，所以说计算机安全和网络安全的目标是完美实现信息安全。

实现信息安全取决于每个联网国家、企业和公民采取的安全措施。为防范高技能的网络犯罪，必须培育全球信息安全文化。这不仅需要良好的监管和立法，还需要敏于察觉威胁，并制定出基于信息通信技术的严厉对策。

对我国来讲，需要提升网络普及水平、信息资源开发利用水平和信息安全保障水平。抓住信息技术转型的机遇，基本建成国际领先、多网融合、安全可靠的综合信息基础设