高等职业教育“十一五”规划教材

高职高专计算机网络系列教材

计算机网络安全与实训

耿　杰
方风波　◎主编

科学出版社
www.sciencep.com

高等职业教育“十一五”规划教材

高职高专计算机网络系列教材

计算机网络安全与实训

耿　杰　方风波　主编

科学出版社

北　京

内 容 简 介

计算机网络安全已经引起了社会的普遍关注，成为当今网络技术的一个重要研究课题，也是学校教学的重要课程之一。

全书共分 9 章，通俗地阐述了网络所涉及的安全问题，主要内容包括：计算机网络安全知识、数据安全、网络通信安全、操作系统安全、防火墙技术、网络病毒及其预防、黑客攻击与防范、Web 安全技术。

本书遵循“理论知识以够用为度，重在实践应用”的原则编写，书中提供了大量的操作实例，帮助读者掌握计算机网络安全的基本原理与技术。

本书适合高职高专计算机及相关专业学生使用，也可作为计算机网络安全的培训教材，对从事信息安全的人员也是一本基础实践参考书。

图书在版编目（CIP）数据

计算机网络安全与实训/耿杰，方风波主编. —北京：科学出版社，2006
（高等职业教育“十一五”规划教材·高职高专计算机网络系列教材）
ISBN 7-03-017396-1

Ⅰ.计… Ⅱ. ①耿… ②方… Ⅲ. 计算机网络-安全技术-高等学校：技术学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2006）第 060555 号

责任编辑：孙露露 赖文华 / 责任校对：都 岚
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
佳海彩色印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2006 年 8 月第 一 版 开本：787×1092 1/16
2006 年 8 月第一次印刷 印张：12 3/4
印数：1—3 000 字数：283 000

定价：18.00 元

（如有印装质量问题，我社负责调换〈环伟〉）
销售部电话 010-62136131 编辑部电话 010-62138978-8003

中国科学院教材建设专家委员会

高职高专

本书编写人员

主　编　耿　杰　方风波

副主编　汤钦林　王巧莲　黄鹤鸣

参　编　（按姓氏笔画排序）

刘自昆　胡　氢

前　言

近年来，随着计算机技术和 Internet 建设的普及与发展，计算机网络安全问题逐步成为人们关注和讨论的焦点。计算机网络应用已深入到社会的各个领域，人类对计算机网络的依赖性越来越大。随之而来的是计算机网络安全问题。普及计算机网络安全知识已从法律上、技术上确保计算机网络的安全，成为保护我国计算机网络安全的头等大事。鉴于此，高职高专计算机及其相关专业的学生开设计算机网络安全技术课是十分必要的。

本书遵循“理论知识以够用为度，重在实践应用”的原则编写。全书共分 9 章，通俗地阐述了网络所涉及的安全问题及各种相关的安全技术。主要内容包括计算机网络安全知识、数据安全、网络通信安全、操作系统安全、防火墙技术、网络病毒及其预防、黑客攻击与防范，以及 Web 安全技术。

第 1 章是计算机网络安全概述，内容包括计算机网络安全简介、网络安全面临的威胁及原因、网络安全机制。第 2 章是加密技术，介绍了数据加密标准 DES 等常见的加密算法，同时详细介绍了加密技术的典型应用——数字签名的实现方法。第 3 章是网络通信安全，介绍了网络通信的安全性、网络通信存在的安全威胁等。第 4 章是操作系统安全，主要以 Windows 2000 Server 为例，讲述了操作系统的安全机制、安全管理及安全应用。第 5 章是防火墙技术，内容包括防火墙的简介、类型、配置，防火墙的选购和使用，常见的防火墙产品介绍。第 6 章是入侵检测系统，内容包括入侵检测系统的简介、类型、配置、选购和使用，以及常见的入侵检测系统。第 7 章介绍了计算机网络病毒的检测、防范和清杀的常用技术。第 8 章是黑客的攻击与防范，主要介绍了常用的黑客攻击方法及常用的防黑措施。第 9 章介绍 Web 安全，包括 Web 技术简介、Web 服务器安全、Web 浏览器安全等。

本书叙述准确，深入浅出。书中提供了大量的网络安全技术实训，读者通过实训项目的操练，可以掌握计算机网络安全的基本原理与技术，进而增强实际问题的处理能力。为方便教学，本书配有电子课件，“思考与练习”部分的答案也在其中，可到科学出版社网站（www.sciencep.com）下载。该书适合高职高专计算机及其相关专业学生使用，也可作为计算机网络安全的培训教材，对从事信息安全的人员也是一本基础实践参考书。

本书在编写过程中得到了许多专家和同仁以及科学出版社编辑给予的大力支持，在此向他们表示最真挚的感谢！

由于作者水平有限，书中不免有疏漏和不足之处，欢迎广大读者批评指正。主编邮箱：ruopiao97121@163.com（耿杰），ffbm@163.com（方风波）。

目　录

第1章　计算机网络安全概述

本章学习目标

- 掌握网络安全的定义。
- 掌握网络面临的各种安全威胁。
- 了解产生网络安全威胁的原因。

本章要点内容

- 网络安全的定义。
- 网络面临的安全威胁及原因。
- 网络的安全机制。

本章学前要求

- 了解数据库原理，了解网络程序设计语言及基本编程方法。
- 掌握操作系统、计算机网络的基础知识。

随着网络技术的不断发展，网络在人们生活中已经占有一席之地，为人们的生活带来了极大方便。然而，网络也不是完美无缺的，它在给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等问题严重威胁着网络的安全。目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 网络安全简介

目前，Internet 几乎覆盖了世界各地，容纳了数十万个网络，为几十亿用户提供了形式多样的网络与信息服务。除了广泛应用的 Web 网页、E-mail、新闻论坛等文本信息的交流与传播之外，网络电话、网络传真、视频等通信技术都在迅猛地发展。在信息化社会中，计算机网络将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络的依赖日益增强。人们依靠计算机网络系统接收和处理信息，实现相互间的联系和对目标的管理、控制。通过网络交流信息、获得信息已成为现代信息社会的一个主要特征。网络正改变着人们的工作方式和生活方式。

科技进步在造福人类的同时，也带来了新的危害。随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络的重要性和对社会的影响越来越大，随之相伴的是由于网络的脆弱性，利用计算机网络犯罪的情况越来越严重，已经严重地危害着社会的发展和国家的安全。

1996 年 8 月 14 日，美国发生一起计算机病毒入侵计算机网络的事件，几千台计算机被病毒感染，Internet 不能被正常访问。政府不得不立即做出反应，国防部成立了计算机快速行动小组。这次病毒事件导致的直接经济损失达 1 亿多美元。

1994 年底，俄罗斯黑客弗拉米尔与其同伙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。

2001 年，某用户与南京 ISP 发生矛盾后便攻击该 ISP 的服务器，致使服务中断了几个小时。

2003 年 3 月 21 日，黑客侵入了江苏某信息网的多台服务器，破译了密码数据库，获得了网络工作人员的口令和 300 多个合法用户的帐户与密码，并将这些密码和口令公布于众。

事实上，上面这些网络入侵事件只是我们知道的实际所发生的事例中非常微小的一部分，有相当多的网络入侵或攻击并没有被发现，或者出于各种各样的原因未被公开。据统计，商业信息被窃取的事件以每月以 260%的速度增加。社会上每公开报道一次网络入侵事件的背后，有无数例是不被公众所知的。

面对越来越严重的计算机网络安全的威胁，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设计的开始都忽略了安全问题。即使考虑了安全问题，大部分都是把安全机制建立在物理安全上。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很脆弱。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，保证其保密性和完整性；防止非法用户的侵入，限制网络上用户的访问权限，保证信息存放的私有性。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的真实性和信息的可用性。

计算机网络安全的目的是要保证网络上数据存储和传输的安全性。国内外很多研究机构为了解决这个问题做了大量的工作，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、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。

1.2　计算机网络安全

1.2.1　计算机网络安全的定义

计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因自然和人为的因素而受到破坏、更改和泄露。网络安全主要包括物理安全、软件安全、信息安全和运行安全等 4 个方面。

1. 物理安全

物理安全包括硬件、存储媒体和外部环境的安全。硬件是指网络中的各种设备和通信线路，如主机、路由器、服务器、工作站、交换机、电缆等；存储媒体包括磁盘、光盘等；外部环境则主要指计算机设备的安装场地、供电系统。保障物理安全，就是要保护这些硬件设施能够正常工作而不被损害。

2. 软件安全

软件安全是指网络软件以及各个主机、服务器、工作站等设备所运行的软件的安全。保障软件安全，就是保护网络中的各种软件能够正常运行不被修改、破坏和使用。

3. 信息安全

信息安全是指网络中所存储和传输数据的安全，主要体现在信息隐蔽性和防修改的能力上。保障信息安全，就是保护网络中的信息不被非法修改、复制、解密、使用等，也是保障网络安全最根本的目的。

4. 运行安全

运行安全指网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。保障运行安全，就是通过对网络系统中的各种设备运行状况进行监测，发现不安全因素时，及时报警并采取相应措施，消除不安全状态以保障网络系统的正常运行。

网络安全的目的是为了确保网络系统的保密性、完整性和可用性。保密性要求只有授权用户才能访问网络信息；完整性要求网络中的数据保持不被意外或恶意地改变；可用性指网络在不降低使用性能的情况下仍能根据授权用户的需要提供资源服务。

1.2.2 网络安全的特征

由于网络安全受到威胁的多样性、复杂性及网络信息、数据的重要性，在设计网络系统的安全时，应该努力达到安全目标。一个安全的网络具有下面五个特征：可靠性、可用性、保密性、完整性和不可抵赖性。

（1）可靠性

可靠性是网络安全最基本的要求之一，是指系统在规定条件下和规定时间内完成规定功能的概率。如果网络不可靠，经常出问题，这个网络就是不安全的。目前，对于网络可靠性的研究主要偏重于硬件可靠性方面。研制高可靠性硬件设备，采取合理的冗余备份措施是最基本的可靠性对策。但实际上有许多故障和事故，与软件可靠性、人员可靠性和环境可靠性有关。如人员可靠性在通信网络可靠性中起着重要作用。有关资料表明，系统失效中很大一部分是由人为因素造成的。

（2）可用性

可用性是网络面向用户的基本安全要求。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的，多方面的，有时还要求时效性。网络必须随时满足用户通信的要求。从某种意义上讲，可用性是可靠性的更高要求，特别是在重要场合下，特殊用户的可用性显得十分重要。为此，网络需要采用科学合理的网络拓扑结构，必要的冗余、容错和备份措施以及网络自愈技术、分配配置和负荷分担、各种完善的物理安全和应急措施等，从满足用户需求出发，保证通信网络的安全。

（3）保密性

保密性指防止信息泄漏给非授权个人或实体。信息只为授权用户使用，保密性是对信息的安全要求。它是在可靠性和可用性的基础上，保障网络中信息安全的重要手段。对于敏感用户信息的保密，是人们研究最多的领域。由于网络信息会成为黑客、计算机犯罪、病毒、甚至信息战的攻击目标，已受到了人们越来越多的关注。

（4）完整性

完整性也是面向信息的安全要求。它是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等操作破坏的特性。它与保密性不同，保密性是防止信息泄漏给非授权的人，而完整性则要求信息的内容和顺序都不受破坏和修改。用户信息和网络信息都要求完整性，例如涉及金融的用户信息，如果用户账目被修改、伪造或删除，将带来巨大的经济损失。网络中的网络信息一旦受到破坏，严重的还会造成通信网络的瘫痪。

（5）不可抵赖性

不可抵赖性也称作不可否认性，是面向通信双方（人、实体或进程）信息真实的安全要求。它包括收发双方均不可抵赖。随着通信业务的不断扩大，电子贸易、电子金融、电子商务和办公自动化等许多信息处理过程都需要通信双方对信息内容的真实性进行认同，为此，应采用数字签名、认证、数据完备、鉴别等有效措施，以实现信息的不可抵赖性。

网络的安全不仅仅是防范窃密活动，其可靠性、可用性、完整性和不可抵赖性应作为与保密性同等重要的安全目标加以实现。我们应从观念上，政策上做出必要的调整，全面规划和实施网络信息的安全。

1.3　网络安全面临的威胁

1.3.1　网络内部威胁

1. 计算机系统的脆弱性

计算机系统的脆弱性主要来自计算机操作系统的不安全性，在网络环境下，还来源于网络通信协议的不安全性。计算机系统有其自身的安全级别，有关安全级别的定义我们将在后面详细讨论。有的计算机操作系统属于 D 级，这一级别的操作系统根本就没有安全防护措施，它就像一个门窗大开的屋子，如 DOS、Windows 3.x、Windows 95 等操作系统，它们只能用于一般的桌面计算机系统，而不能用于安全性要求高的服务器的操作系统。UNIX 系统和 Windows NT 达到了 C2 级别，其安全性远远强于 Windows 95 操作系统，而且主要用于服务器上。但这种操作系统仍然存在着安全漏洞，因为这两种系统中都存在超级用户，UNIX 中是 root，而 Windows NT 中是 Administrator，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者，这样系统就面临着巨大的危险。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会存在超级用户带来的问题。现在很多操作系统都使用静态口令，但口令还是有很大的破解可能性，而且不好的口令维护制度会导致口令丢失。口令丢失也就意味着安全系统的全面崩溃。

世界上没有能长久运行的计算机系统，计算机系统可能会因硬件故障或软件原因而停止运行或运行错误，或被入侵者利用并造成损失。硬盘故障、电源故障和主板芯片故障等都是人们应经常考虑的硬件故障问题。软件原因可能存在于操作系统中，更多的是存在于应用软件中。

2. 网络内部的威胁

对网络内部的威胁主要是来自网络内部的用户，这些用户试图访问那些不允许使用的资源和服务器。可以分为两种情况：一种是有意的安全破坏，入侵者的攻击和计算机犯罪就是属于这一类。这是计算机网络所面临的最大威胁，此类攻击还可以分为主动攻击和被动攻击两种情况，主动攻击是指计算机网络的内部用户以各种方式有选择地破坏

信息的有效性和完整性，而被动攻击则是在不影响网络正常工作的情况下，进行信息截获、窃取、破译等，目的是为了获得重要机密信息。

第二种是由于用户安全意识差造成的无意识的操作失误，使得系统或网络误操作或崩溃。如操作员安全配置不当造成的安全漏洞或隐患，用户安全意识不强，用户口令选择不慎或不恰当，用户将自己的账号保护不严或与别人共享等都会对网络安全带来威胁和隐患，或者被非法入侵者加以利用，从而造成对系统的危害。

1.3.2 网络外部威胁

除了受到来自网络内部的安全威胁外，网络还受到来自外界的各种各样的威胁。网络系统受到的威胁是多样的，因为在网络系统中可能存在许多种类的计算机和操作系统，采用统一的安全措施是不容易的，也是不可能的，而对网络进行集中安全管理则是一种好的方案。

安全威胁主要可以归结为物理威胁、网络威胁、身份鉴别、编程、系统漏洞等方面。

1. 物理威胁

物理安全是指保护计算机硬件和存储介质等设备和工作程序不遭受损失。常见的物理安全威胁有偷窃、垃圾搜寻和间谍活动等。物理安全是计算机系统和网络操作系统安全的最重要的方面。

办公室的计算机是偷窃者的主要目标之一。由于计算机或网络服务器中存储的数据信息的价值远远超过设备的价值，计算机偷窃行为对用户的损失可能成倍于被偷的设备的价值。因此必须采取严格的防范措施以确保计算机设备不会被偷窃。入侵者可能会潜入计算机房，偷取计算机或计算机里的机密信息，也可能化装成计算机维修人员，趁管理员不注意时，进行偷窃。当然也可能是内部职员窃取他们不应该看到的信息，并把信息散布出去或卖给商业的竞争对手。

千万不要小看了搜寻垃圾，在商业竞争中，有些人专门会搜寻对手扔下的垃圾，但这种人所需要的是一些机密信息。办公室的工作人员可能会把一些打印错误的文件扔进废纸篓，而没有对其做任何安全处理，如不把这些文件销毁，那么这些文件就有可能落到那些竞争对手的手中。

间谍活动是人们不能忽略的一种因素，现在商业间谍很多，而且一些商业机构可能会为击败对手而采取任何不道德的手段，有时政府机关也有可能卷入这种间谍活动当中。

2. 网络威胁

计算机网络的发展和使用对数据信息造成了新的安全威胁。在计算机网络上存在着电子窃听，分布式计算机系统的特征是各种分离的计算机通过一些媒介相互连接在一起，进行相互通信，而且局域网一般是广播式的，只要把网卡模式设置成混合模式，网络上人人都可以收到发向任何人的信息。当然，也可以通过加密来解决这个问题，但目前，强大的加密技术还没有在网络上广泛使用，况且加密也是有可能破解的。