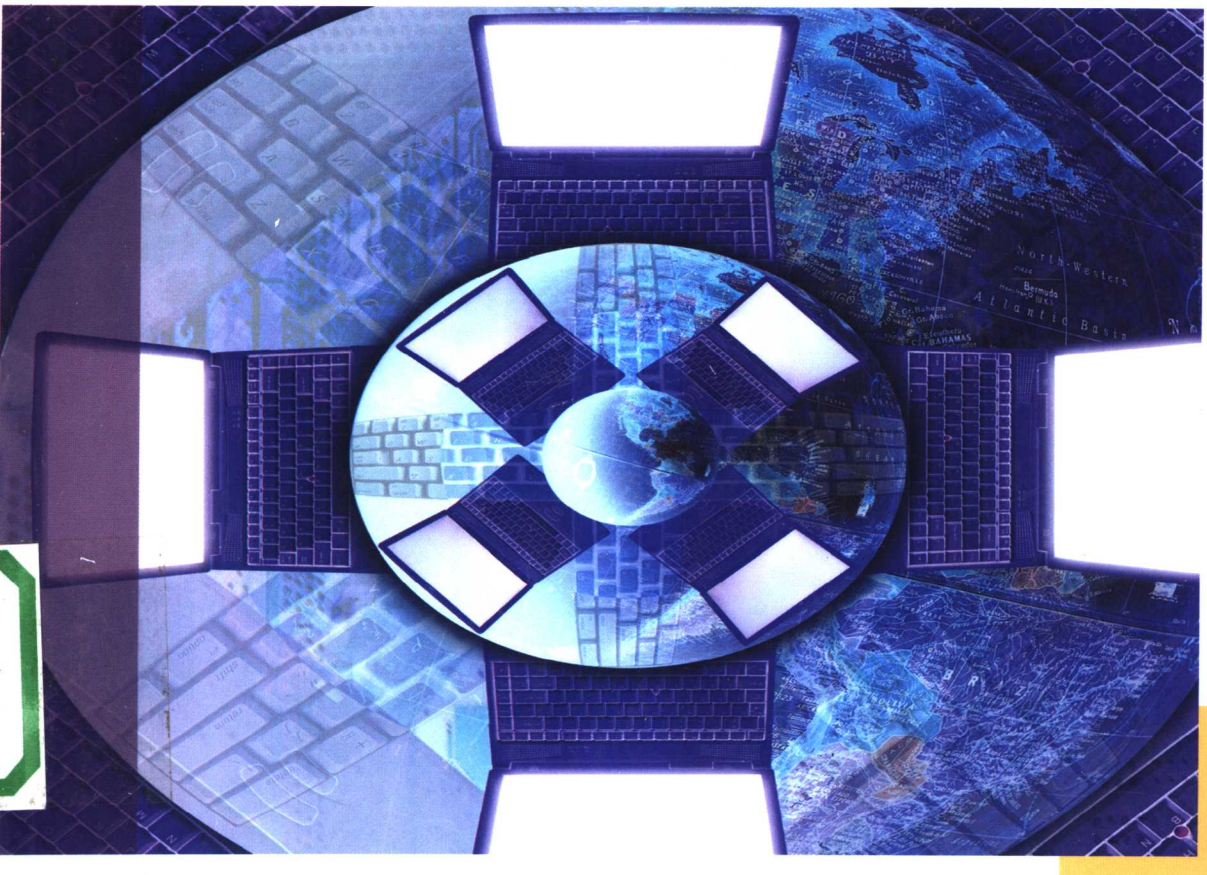
应用型本科人才培养创新教材出版工程

计算机教育核心课程教材

计算机网络安全技术

主　编　潘　瑜
副主编　臧海娟　何　胜



科学出版社
www.sciencep.com

TP393.08
151

●应用型本科人才培养创新教材出版工程

计算机教育核心课程教材

计算机网络安全技术

主　编　潘　瑜

副主编　臧海娟　何　胜

科学出版社

北　京

内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络安全基础知识、计算机网络安全协议基础知识、计算机网络安全编程基础知识、计算机网络操作系统安全基础知识、计算机网络攻击与入侵技术、计算机网络病毒及反病毒技术、计算机网络站点的安全技术、数据加密技术基础知识、防火墙与入侵检测技术、网络安全方案设计等内容。本书概念清晰、层次分明、逻辑性强、面向应用、实验丰富，在强调掌握基础知识的同时，还给出了各种网络安全技术和使用方法。每章都附有典型例题和习题，有利于教师的教学和学生的学习。

本书的内容涵盖了计算机网络安全技术的各个领域，因此既可作为应用型本科院校计算机专业、通信专业、信息专业的教材，也可以供从事计算机网络安全及相关工作的工程技术人员学习参考。

图书在版编目(CIP)数据

计算机网络安全技术/潘瑜主编. —北京：科学出版社，2006

（应用型本科人才培养创新教材出版工程·计算机教育核心课程教材）

ISBN 7-03-016960-3

Ⅰ.计… Ⅱ.潘… Ⅲ.计算机网络-安全技术-高等学校-教学参考资料 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2006)第 014952 号

责任编辑：余 丁/责任校对：包志虹

责任印制：黄晓靖/封面设计：陈 敬

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

*

2006 年 2 月第 一 版 开本：B5(720×1000)

2006 年 2 月第一次印刷 印张：22 3/4

印数：1—4 000 字数：428 000

定价：28.00 元

（如有印装质量问题，我社负责调换〈双青〉）

前　言

目前，应用型本科高等院校“计算机网络安全技术”课程教学已经基本展开。在因特网飞速发展的信息时代，计算机网络安全技术越来越重要。本书作为计算机网络安全技术的教科书，重点介绍了计算机网络安全基础、计算机网络安全协议、计算机网络安全编程、计算机网络操作系统安全、计算机网络攻击与入侵技术、计算机网络病毒及反病毒技术、计算机网络站点安全、数据加密技术、防火墙与入侵检测技术、网络安全方案设计等内容。本书的基本内容是围绕提高读者“计算机网络安全能力”这个主题展开的。

在编写本书时，我们充分考虑了计算机网络安全技术的实际情况，将计算机网络安全领域中相对比较繁杂的部分舍去，而保留了计算机网络安全技术中最常用、最基本的部分。本书思路清晰，分析透彻，实例典型，实验和习题丰富，理论联系实际，力求使读者通过学习能够达到“举一反三、融会贯通”目的。

本书由江苏技术师范学院潘瑜任主编，臧海娟、何胜担任副主编，蒋益峰参与编写。其中第1章、第2章、第4章、第7章和全部附录由潘瑜编写，第9章的9.1～9.5节、第10章由臧海娟编写，第3章、第5章、第8章由何胜编写，第6章、第9章的9.6节由蒋益锋编写。最后由潘瑜统稿成书。

本书在编写过程中得到“21世纪应用型本科教材编委会”和江苏技术师范学院施步洲、王国军、蒋忠芳、周丽琴的大力支持，江苏技术师范学院的韩君为本书做了大量文字录入和排版工作，在此向他们表示衷心地感谢！

本书的出版还得到江苏省教育厅自然科学研究项目02KJB520011和江苏技术师范学院教学改革与研究项目“计算机网络安全技术系列课程的改革与实践”的资助，在此也表示衷心地感谢！

由于编者水平有限，书中难免有疏漏之处，欢迎广大读者批评指正。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章

计算机网络安全概述

学习目标

计算机网络中的安全问题与现实社会中的安全问题一样，是一个永恒的话题，也是一个很难解决的问题。本章从介绍网络安全现状、网络安全面临的威胁和困难入手，引出对网络安全体系结构的描述，讨论了网络安全法规和网络安全评价标准，对读者全面理解网络安全概念很有帮助。

1.1 网络安全概述

1.1.1 网络安全现状

随着计算机网络的普及和计算机网络应用的发展，人类社会对计算机网络的依赖程度日渐加深。计算机网络安全不仅对每个人都有现实意义，而且对一个国家的政治、经济和国防安全也十分重要。由于计算机网络安全的问题没有得到很好的解决，某些企业、金融公司甚至政府部门蒙受过重大损失。

事实上，计算机网络安全问题是现实社会中的各种安全问题在计算机网络这个虚拟社会中的一个映射。现实生活中可能存在的各类问题在计算机网络中也会存在。例如，在真实社会中进行商业活动时可能会遇到商业欺诈：农民朋友可能会买到假种子、假化肥；企业和个人可能会遇到假钞等。同样，基于计算机网络技术的电子商务活动也可能会遇到各种类型的攻击，例如计算机病毒、商业信息窃取、拒绝服务、虚假身份等。但有所不同的是，由于计算机网络的开放性、匿名性和计算机网络技术的复杂性，通过计算机网络进行攻击和破坏比在真实社会中容易得多。例如，在计算机网络中要隐藏身份或冒名顶替要比在真实社会中容易。在计算机网络刚刚流行的时候，很多人都以拥有电子邮件信箱为荣，纷纷把电子邮件地址印在名片上，然而，人们很快就发现，这样做会带来很大的麻烦——每天都会收到大量的无法拒绝的垃圾邮件。因为在计算机网络中发信人可以根据需要不断变更自己的邮件地址、邮件标题，使电子邮件的接收者上当。

计算机网络安全问题涉及数学、计算机技术、通信技术、管理和法律等多个领域。从不同学科的角度出发，会有不同的解决办法，但上述任何一种方法都不可能完全解决计算机网络安全问题，因此必须综合运用上述方法才能解决问题。

在计算机网络安全领域中有一个出现频率很高的词，那就是“黑客”（Hacker），本意是指一些计算机水平很高的程序员，他们可以发现系统中潜在的漏洞，彼此之间经常在计算机网络中相互交换安全信息和安全技术，但从来不对别人的计算机系统进行蓄意破坏。而那些未经授权就进入别人的系统，非法获取信息，对系统进行破坏或对数据进行修改、删除等操作的人，则被称为破坏者（Cracker），这种攻击和破坏活动可能会对系统造成很大的损失。

由于因特网的日益普及，各种网络攻击工具很容易从网站上下载，计算机网络安全所面临的形势与因特网发展初期有很大的不同。现在，即使是一个初学者，利用各种工具软件也能够很容易地对计算机系统进行攻击。虽然目前采取了安全防护措施的机器比以前多了，但是，随着计算机的普及，因特网上不设防的、具有安全漏洞的计算机也越来越多。

因此，在今天，“黑客”已经失去其早期“技术高手”的含义，而成为任何进行攻击活动者的代名词。在本书中，我们把那些进行非授权访问、修改数据，或使系统不可靠、不可用的活动称为攻击活动，而从事这种攻击活动的人统一称为“黑客”。

利用“黑客”手段对计算机网络进行攻击的人有以下四种：

① 第一种人：这些人只是为了提高知名度，他们拥有很多的资源（时间、计算机资源和金钱等），不断地寻找目标，进行各种尝试攻击；

② 第二种人：这些人没有明确的目的，可能会入侵不同的系统，修改服务器的主页，发送大量的垃圾信息；

③ 第三种人：计算机网络安全技术的研究人员为了证明一个计算机系统是不安全的，需要进行模拟攻击，以便找到系统的安全隐患；

④ 第四种人：有计划、有目的地对特定系统进行破坏和攻击的人。

1.1.2 网络安全面临的威胁

网络的互联拓展了计算机应用的空间，但互联技术本身以及计算机系统存在的弱点，也使得所有网络用户因为彼此互联而更容易被攻击。因为我们通过网络已经与现实社会中形形色色的人联结到了一起。

如图 1-1 所示，假设主机 A 和主机 B 是计算机网络中的两个用户，主机 C 是连接在计算机网络上的第三个用户，主机 A 和主机 B 之间正在通过计算机网络进行正常的通信，在这种情况下面临的主要安全问题是：

图 1-1 网络安全示意图

① 主机 C 对主机 A 或主机 B 的非授权访问；

② 主机 C 冒用主机 A 或者主机 B 的

身份对网络上的其他主机进行访问；

③ 主机 C 使主机 A 或主机 B 无法使用网络等。

归纳起来，计算机网络安全面临的风险主要有以下五种：

1. 保密性（Confidentiality）

在计算机网络中通信双方的信息有可能被网络中的第三方获得。

在图 1-1 中，当主机 A 和主机 B 通信时，在不安全的计算机网络环境中，他们的通信内容有可能被第三方主机 C 截取，这可以通过下面四种典型的情况实现：

（1）电磁辐射监听

数据信号的传输通常是一定频率的电信号在金属导体或者无线的环境下传输，或者是通过光脉冲在光纤中传输。而对于前者，总会产生一定的电磁辐射，通过灵敏的仪器获取、分析这些电磁辐射，就可以了解传输的内容。

（2）线路中搭线窃听

这是一种经典的信息获取方法，在通信线路上搭接一根线和一部电话机，就可以知道这根线上通话的内容。如果将电话机换成一个协议分析设备，就可以对传输的信息进行分析、窃听。

（3）共享网络中的信息监听

对于共享以太网、无线网络等，任意一台连接到网络中的计算机，都可以通过运行数据包监听程序（例如 Sniffer Pro 数据包抓包软件），捕获数据包并进行分析。

（4）其他方式

光纤通信虽然不会产生电磁辐射，但攻击者如果可以物理接触到光纤，也可以通过诸如分光器之类的设备监听数据。

“黑客”还可以利用一些伪装技术，设法获得用户的网络数据流量并加以分析。如果“黑客”能够控制计算机网络中的重要设备（如交换机和路由器）时，就可以很容易地得到各种用户数据流量，进行分析。为了确保计算机网络中的通信内容的安全，防止网络中的第三方窃取，必须在发送方对所要传输的信息加密，在接收方进行解密。

2. 认证（Authentication）

所谓认证是指在计算机网络中，进行通信的双方在通信之前需要彼此确认对方就是要通信的对象，而不是假冒的通信对象。

在现实社会中，当对话双方面对面说话时，人们通过识别对方的面孔，能够很清楚要通信的对象是谁；当对话双方通过电话交谈时，人们也基本可以通过识

别对方的声音，知道要通信的对象是谁。但是，在计算机网络这个虚拟社会中，当通信的双方无法真正“看”到或“听”到对方时，不能根据传统的特征识别对方时，如何确保通信的双方不是假冒的对象就成了一个必须严肃对待的问题。

例如，当你在家中的计算机上通过因特网收到一封来自远方的电子邮件，这封邮件说他是你自大学毕业后就没有见过面的老同学，你是相信还是不相信呢？当你收到来自电子银行的邮件，请你填写银行账号和密码，你该怎样做呢？给大家的忠告是在没有进行必要的认证之前，上述的电子邮件都不是100%可信的。

如图1-1所示，如果主机A只允许主机B访问，主机A应该如何确认主机B的身份？如果主机C模仿成主机B与主机A通信，主机A应该怎样识别？是通过IP地址、用户名和口令还是其他信息？对于这些问题，都是需要通过适当的认证来解决的。

3. 完整性（Integrity）

所谓完整性是指信息在传输的过程中无法被篡改，或者即使被篡改了，也可以被接受方发现。在计算机网络中进行数据通信过程中，通信双方在网络上传输的信息有可能被监听，也有可能被篡改。如图1-1所示，即使主机A和主机B之间的数据通信是保密的，主机C虽然无法理解其内容，但主机C仍然可以通过某些方法和工具篡改或破坏主机A和主机B之间的通信的内容。因此，在计算机网络中不仅通信的双方要彼此认证，对双方的通信内容的完整性和不可篡改性也要保证。

4. 不可否认性（Non-repudiation）

所谓不可否认性是指在电子交易过程中，发出信息的一方无法否认其行为。如图1-1所示，在基于计算机网络的电子商务中，如果主机A向主机B发出了一个订单，或者主机A收到了主机B的一笔汇款，如何确保主机A或主机B无法否认在计算机网络上做过上述操作？因此，在基于计算机网络的电子商务活动中确保信息的不可否认性是十分重要的。

5. 可用性（Availability）

所谓可用性是指计算机网络的基础设施、硬件和软件系统等在任何时候都能够可靠运行，并且随时能被所有用户正常使用。由于对国家、企业和个人来说计算机网络的作用越来越重要，人们要利用计算机网络来做各种各样的事情，例如可以利用计算机网络进行人员招聘、广告发布、商业信件收发、合同签订和商品销售等工作。这些商业企业对网络的依存度很高，如果计算机网络服务中断（哪怕只是几个小时），企业的业务也会受到很大的影响。因此，计算机网络的可用

性直接关系到企业的生存。

事实上，所有连接在计算机网络上的计算机都同时扮演着两个角色：网络服务的提供者和网络服务的使用者。当一台计算机通过网络对外提供服务时，自己就处于被攻击的危险中；而当一台计算机通过网络使用外面的服务时，也同样处于被攻击的网络中。来自网络的攻击可能会破坏系统，也可能会使原先提供的网络服务不可用。目前在计算机网络中可能出现的攻击和破坏活动，归纳起来有下面四种：

（1）扫描（Scan）

利用特定的工具和专用的软件，向目标（如指定的网络或指定的主机）发出一些特定的数据包，根据响应的结果进行分析，了解目标网络或目标主机的相关特征，为进一步的攻击做准备。

（2）入侵（Intrusion）

在计算机网络中，利用不同的方法和工具，进行诸如口令猜测、漏洞攻击等活动，一旦侵入目标系统，并获取相应的权限，则可以对目标系统的资源进行非授权访问和其他破坏活动。

（3）拒绝服务（Denial of Service）

在计算机网络中利用专用的工具软件或自己编写的程序，向目标系统发送大量的无用数据包，将目标系统的带宽占满，使得目标系统的服务无法被合法的用户所使用。

（4）滥用（Misuse）

在计算机网络中传播计算机病毒、发布垃圾邮件、扩散有害信息等活动都是对网络的滥用。这些活动也有可能导致目标系统不能够使用。

要解决这些网络安全问题，需要综合运用多种技术手段、管理手段和法律手段。其中，保密性、认证、完整性、不可否认性等问题，主要基于密码算法及其应用。而可用性涉及更多的因素，如访问控制、管理等。因此，我们将在介绍有关攻击的基础上，介绍加密技术及其应用，以及各种常见安全防护手段，说明如何发挥人的作用，通过有效的安全管理，综合各种技术手段，从而达到比较安全的防护效果。

另外，从信息系统面临的威胁来看，最具破坏性的主要来自内部。在内部威胁中，危害性最大的就是内部关键人员为了某种利益从事的攻击、破坏活动。对工作不满、遭到辞退、或者与外部勾结的工作人员，往往更容易获取和破坏内部的关键信息。工作中的漫不经心，也经常会导致各种漏洞。

因此，如果发现了一个攻击者声势很大地对系统进行入侵、破坏，实际上产生的危害并不算大。因为那很可能是一个业余攻击者，使用从网络上获得的攻击工具“练手”。危害最大的是那些不动声色的“专业”攻击者，他们可以长期地

对信息进行窃取、修改，并使自己攻击的活动很隐蔽，不被发现。

综上所述，我们可以对网络安全防护下一个定义：

拒绝未经授权的物理或电子入侵、操作，保证网络和所传信息端到端的完整性，能够抗拒各种类型的破坏，包括电子袭击、物理袭击、人为错误等。

1.1.3 网络安全面临的困难

计算机网络中安全问题与现实社会中的安全问题一样，是一个永恒的问题，也是一个很难解决的问题，在可以预见的未来不会有一个“一劳永逸”的解决方案。这主要是由以下四个方面的原因造成的：

1. 网络攻击与网络防守的不对称性

“黑客”在攻击计算机网络时，通常不会遵守正常计算机网络用户所默认的一些规则，他们会利用操作系统软件或者网络协议上的漏洞达到攻击网络主机的目的。如果我们分析一个“黑客”攻击网络的全过程，可以发现他的攻击行动是经过精心准备的，用于攻击的工具也很容易从因特网上获得。因此，“黑客”攻击的风险低、也很难被追踪。对于网络系统管理员来说，则意味着必须堵住所有可能的漏洞。因特网不断增加的复杂性、协议与应用的不断增多等都使得网络系统管理员进行安全防护的难度加大。

我们也可以把安全问题看成是一条链，最脆弱的一环可以使整个系统崩溃。例如，某个设计得很好的网络安全系统，就因为系统管理员使用了一个简单的“弱口令”，使得整个网络安全设计都变得不安全。

另外，“黑客”的攻击是主动行为，他可以选择一天的任何时候进行，而系统管理员不可能做到每周 7×24 小时都处于积极的防守状态。因此，网络攻击和网络防守是极不对称的，100％网络安全是非常难做到的。

2. 网络安全的动态性

由于计算机网络技术发展非常迅速，随着技术的发展，网络操作系统、网络硬件平台、网络应用软件和网络协议都会发生变化。当用户安装了新的服务器，升级了网络操作系统，采用了新的网络协议，安装了新的应用后，原来存在的一系列安全问题可能会消失，但新的安全问题和安全漏洞可能又会出现。因此，网络安全是动态的，不可能存一个“一劳永逸”的解决方案。对计算机网络安全的攻击与防守来讲，攻击者总是占有优势，因为防守者必须仔细检查和防守每个可能的漏洞，一旦有所疏忽让攻击者找到一个漏洞，系统就可能被攻破。另外，如前所述，实施攻击的“黑客”往往是具有丰富专业知识和经验的计算机网络专业人员，而被攻击者大部分是普通的计算机用户，也许仅仅会操作和使用计算机，

此为试读，需要完整PDF请访问：www.ertongbook.com