普通高校本科计算机专业特色教材精选·网络与通信

# 计算机网络安全

沈鑫剡　编著

清华大学出版社

普通高校本科计算机专业特色教材精选·网络与通信

# 计算机网络安全

沈鑫剡　编著

清华大学出版社
北京

## 内 容 提 要

这是一本既注重网络安全基础理论，又着眼培养读者解决网络安全问题能力的教材，书中详细讨论了加密算法、报文摘要算法、认证协议等网络安全基础理论，黑客攻击方法和过程，目前主流的网络安全技术，如以太网安全技术、安全路由、信息流管制、VPN、防火墙、入侵防御系统和安全无线局域网等，以及这些防御黑客攻击技术的原理和案例，安全网络的设计方法和过程，安全应用层协议及应用等。

本教材的最大特点是将计算机网络安全理论、目前主流网络安全技术和安全网络的设计过程有机地集成在一起。让读者既能掌握完整、系统的计算机网络安全理论，又具备运用主流网络安全技术实现安全网络的设计能力。

本教材以通俗易懂、循序渐进的方式叙述网络安全知识，并通过大量的例子来加深读者对网络安全知识的理解，内容组织严谨、叙述方法新颖，是一本理想的计算机专业本科生的计算机网络安全教材，也可作为计算机专业研究生的计算机网络安全教材，对从事计算机网络安全工作的工程技术人员，也是一本非常好的参考书。



**图书在版编目（CIP）数据**

计算机网络安全/沈鑫剡编著. —北京：清华大学出版社，2009.9
（普通高校本科计算机专业特色教材精选·网络与通信）
ISBN 978-7-302-20397-1

Ⅰ. 计… Ⅱ. 沈… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 101089 号

**责任编辑**：袁勤勇　徐跃进
**责任校对**：李建庄
**责任印制**：杨　艳

**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
**社　总　机**：010-62770175　　**邮　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质　量　反　馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn

**印 刷 者**：北京密云胶印厂
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185×260　　**印　张**：19　　**字　数**：451 千字
**版　　次**：2009 年 9 月第 1 版　　**印　次**：2009 年 9 月第 1 次印刷
**印　　数**：1～3000
**定　　价**：26.00 元

# 出版说明

INTRODUCTION

在我国高等教育逐步实现大众化后，越来越多的高等学校将会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为此，教育部已经启动了“高等学校教学质量和教学改革工程”，强调要以信息技术为手段，深化教学改革和人才培养模式改革。如何根据社会的实际需要，根据各行各业的具体人才需求，培养具有显著特色的人才，是我们共同面临的重大问题。具体地说，培养具有一定专业特色的和特定能力强的计算机专业应用型人才则是计算机教育要解决的问题。

为了适应21世纪人才培养的需要，培养具有特色的计算机人才，急需一批适合各种人才培养特点的计算机专业教材。目前，一些高校在计算机专业教学和教材改革方面已经做了大量工作，许多教师在计算机专业教学和科研方面已经积累了许多宝贵经验。将他们的教研成果转化为教材的形式，向全国其他学校推广，对于深化我国高等学校的教学改革是一件十分有意义的事情。

清华大学出版社在大量调查研究的基础上，决定组织编写一套“普通高校本科计算机专业特色教材精选”。本套教材是针对当前高等教育改革的新形势，以社会对人才的需求为导向，主要以培养应用型计算机人才为目标，立足课程改革和教材创新，广泛吸纳全国各地的高等院校计算机优秀教师参与编写，从中精选出版确实反映计算机专业教学方向的特色教材，供普通高等院校计算机专业学生使用。

本套教材具有以下特点：

1. 编写目的明确

本套教材是在深入研究各地各学校办学特色的基础上，面向普通高校的计算机专业学生编写的。学生通过本套教材，主要学习计算机科学与技术专业的基本理论和基本知识，接受利用计算机解决实际问题的基本训练，培养研究和开发计算机系统，特别是应用系统的基本能力。

2. 理论知识与实践训练相结合

根据计算学科的三个学科形态及其关系，本套教材力求突出学科的理论与实践紧密结合的特征，结合实例讲解理论，使理论来源于实践，又进一步指导实践。学生通过实践深化对理论的理解，更重要的是使学生学会理论方法的实际运用。在编写教材时突出实用性，并做到通俗易懂，易教易学，使学生不仅知其然，知其所以然，还要会其如何然。

3. 注意培养学生的动手能力

每种教材都增加了能力训练部分的内容，学生通过学习和练习，能比较熟练地应用计算机知识解决实际问题。既注重培养学生分析问题的能力，也注重培养学生解决问题的能力，以适应新经济时代对人才的需要，满足就业要求。

4. 注重教材的立体化配套

大多数教材都将陆续配套教师用课件、习题及其解答提示，学生上机实验指导等辅助教学资源，有些教材还提供能用于网上下载的文件，以方便教学。

由于各地区各学校的培养目标、教学要求和办学特色均有所不同，所以对特色教学的理解也不尽一致，我们恳切希望大家在使用教材的过程中，及时地给我们提出批评和改进意见，以便我们做好教材的修订改版工作，使其日趋完善。

我们相信经过大家的共同努力，这套教材一定能成为特色鲜明、质量上乘的优秀教材。同时，我们也希望通过本套教材的编写出版，为“高等学校教学质量和教学改革工程”作出贡献。

清华大学出版社

# 前言

PREFACE

目前计算机网络安全教材是百花齐放，各有特色，但总体上可以分成三类，第一类着重讨论加密、认证算法及其他安全协议，这一类教材的特点是比较详细地讲述网络安全理论，尤其对各种算法和协议做了深入讨论，但缺乏和当前主流安全技术的结合，很难让读者学以致用。第二类主要讨论黑客攻击手段和防御技巧，这一类教材不介绍系统、完整的网络安全理论，有点像黑客攻防大全。第三类把操作系统安全机制、应用程序安全机制和网络安全机制放在一起讨论，当然，所有内容都是浅尝辄止。这三类教材虽然侧重点不同，但有着同样的问题，一是不对当前主流网络安全技术进行深入讨论，二是不在具体网络环境下讨论安全网络的设计方法和过程，对许多问题只是空对空地介绍一些基本概念和方法，没有具体结合目前面临的网络安全问题。因此，难以培养读者解决网络安全问题的实际能力。

对于一本真正以实现将读者领进计算机网络安全知识殿堂为教学目标的教材，一是必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力。二是必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论这些安全技术的实现原理，让读者知其所以然，也让读者具备用主流网络安全技术解决实际网络安全问题的能力。三是需要在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程，给读者提供解决实际网络安全问题的方法和思路，解决读者学以致用的问题。

作为计算机网络安全教材，应该着重讨论和网络有关的安全问题，与操作系统及应用程序有关的安全问题应该在《操作系统》和《算法与程序设计》课程中予以解决，因为离散地讨论一些安全问题会降低该教材的系统性和连贯性，同时，不和整个操作系统结构和程序设计环境结合来讨论操作系统和应用程序安全问题的解决机制，也不利于读者理解、掌握。计算机网络安全教材不可避免地会涉及黑客攻击和防御，但必须从网络总体结构出发，讨论防御黑客攻击的技术，而不是逐个列出攻击手段和防

御方法，将教材变成黑客攻防大全，背离了教材着重于基本理论、基本技术和基本方法的宗旨。

本教材的特色在于：一是为读者提供完整、系统的网络安全理论；二是详细讨论当前主流网络安全技术，并结合网络安全理论讨论这些安全技术的实现原理；三是在实际网络环境下给出运用当前主流安全技术设计安全网络的方法和过程；四是通过构建防御黑客攻击的网络安全体系，讨论运用网络安全技术全方位防御黑客攻击的方法；五是通过门户网站这样的技术给出了精确控制网络资源访问过程的方法。

全书内容安排如下：第 1 章概论，着重讨论了目前存在的安全问题、解决安全问题的基本方法和构建网络安全体系的必要性。 第 2 章黑客攻击机制，详细讨论了黑客攻击类型、主要攻击步骤及运用网络安全技术防御黑客攻击的基本思路。 第 3 章网络安全基础，详细讨论了加密算法、报文摘要算法、认证协议、IP Sec 等网络安全基础理论。 第 4 章安全网络技术，详细讨论了几种广泛应用的网络安全技术及这些网络安全技术防御黑客攻击的机制。 第 5 章无线局域网安全技术，详细讨论了 WEP 安全机制及存在的安全缺陷，802.11i 安全机制解决无线局域网通信安全的原理。 第 6 章虚拟专用网络，详细讨论了第 2 层和第 3 层隧道实现数据跨公共分组网络安全传输的方法和过程。 第 7 章防火墙，详细讨论了无状态分组过滤器、有状态分组过滤器及堡垒主机对网络资源访问过程实施严格控制的机制。 统一访问控制动态配置网络资源访问控制策略的机制。 第 8 章入侵防御系统，详细讨论了主机入侵防御系统和网络入侵防御系统防御黑客攻击的机制。 第 9 章网络管理和监测，详细讨论了网络管理系统的安全问题和解决方法，监测网络安全状态的机制。 第 10 章安全网络设计实例，详细讨论了运用主流网络安全技术、防火墙、入侵防御系统、网络综合监测系统设计一个实现预定安全目标的安全网络的过程。 第 11 章应用层安全协议，详细讨论了 Web 安全机制、电子邮件安全传输协议和门户网站精致控制网络资源访问过程的机制。

在教材编写过程中，解放军理工大学工程兵工程学院计算机应用教研室的俞海英、伍红兵、胡勇强、魏涛和龙瑞对教材内容提出了许多很好的建议和意见，其他同事也给予了很多帮助和鼓励，在此向他们表示衷心的感谢。 作为一本无论在内容组织、叙述方法还是教学目标都和传统计算机网络安全教材有一定区别的新教材，错误和不足之处在所难免，殷切希望使用该教材的老师和学生批评指正，也殷切希望读者能够就教材内容和叙述方式提出宝贵建议和意见，以便进一步完善教材内容。 作者 E-mail 地址为：shenxinshan@163.com。

作　者

2009 年 7 月

# 目录

CONTENTS

# 第1章 概 述

CHAPTER

进入信息社会，信息已经成为一种非常重要的资源，它的安全与否已经影响到个人、企业，甚至国家的根本利益。在信息技术领域，信息是一种用二进制表示的数据，它通过信息采集系统存储到计算机中，由计算机进行处理，通过网络在计算机间相互传输。信息安全要求信息在采集、存储、处理和传输过程中不被破坏、窃取和篡改。但信息流动过程中的每一个环节都存在安全问题，存在计算机中的信息有可能被人盗用，侵入计算机的病毒可能破坏整个系统，经过网络传输的信息可能被窃取或篡改，因此，信息安全由计算机安全和网络安全组成，计算机安全负责信息存储和处理过程中的安全事务，主要防止病毒和非法访问。网络安全负责信息传输过程中的安全事务，主要防止用户非法接入，窃取或篡改传输过程中的信息。承担计算机安全功能的实体主要是操作系统和应用程序，当然还有一些用于保护计算机信息资源的实用程序，因此，计算机安全问题通常是操作系统和应用程序的安全问题，目前，大量黑客攻击都是针对操作系统和应用程序的漏洞进行的。但随着互联网的普及和发展，计算机之间为了共享信息资源，用网络互联，这种情况下，网络已经成为病毒的主要传播途径，黑客也常常通过网络远距离窃取存储在某个计算机中的信息，如此，网络安全除了保障信息安全传输外，还须包括阻断病毒传播和黑客非法访问的途径的功能。因此，网络安全在信息安全中占有极其重要的地位，它不仅包含保障信息安全传输的功能，而且还具有识别病毒和正常信息，识别正常访问和黑客攻击，识别授权用户和非授权用户，分类信息资源并对不同信息资源设置相应访问控制策略等功能。但网络安全不承担操作系统和应用程序应该有的安全功能，因此，完整的信息安全系统应该由安全的操作系统、安全的应用程序和安全的网络组成。

## 1.1 信息安全和网络安全

### 1.1.1 信息处理时的安全问题

计算机是信息的终端设备，承担着信息采集、处理和存储的功能，信息

处理时的安全问题实际上就是计算机安全问题，目前，计算机最大的安全问题就是病毒、非法访问和拒绝服务攻击。

**1. 病毒**

病毒是一种具有自复制能力并会对系统造成巨大破坏的恶意代码，它首先隐藏在某个实用程序中，隐藏过程可以由实用程序设计者完成，或者通过病毒感染该实用程序的过程完成。当某个计算机下载该实用程序并运行它时，将运行隐藏在其中的恶意代码，即病毒，病毒将感染其他文件，尤其是可执行文件，并接管一些系统常驻软件，如鼠标中断处理程序。如果病毒接管了鼠标中断处理程序，当鼠标操作激发该中断处理程序时，将首先激发病毒程序，病毒程序可以再次感染其他文件，并视情况执行破坏操作，如清除所有硬盘中的文件。当感染了病毒的实用程序被其他计算机复制并执行时，病毒将蔓延到该计算机。

对于单台计算机，病毒传播主要通过相互复制实用程序完成，对于接入网络的计算机，从服务器下载软件、下载主页、接收电子邮件等操作都有可能感染病毒。接入网络的计算机一旦感染病毒，安全将不复存在，存储在计算机中的信息将随时有可能被破坏，机密信息将随时外泄，非授权用户随时有可能通过远程桌面这样的工具对计算机进行非法访问。

**2. 非法访问**

非法访问是指非授权用户通过远程登录或远程桌面等工具访问计算机的资源，造成非法访问的原因有病毒、操作系统和应用程序漏洞等。特洛伊木马病毒可以将通过网络接收到的命令作为特权用户输入的命令发送给命令解释程序，从而达到访问系统资源的目的。操作系统和应用程序漏洞可以使普通用户获得特权用户的访问权限，从而使非授权用户访问到本不该访问的资源。

**3. 拒绝服务攻击**

一种类型的拒绝服务攻击利用操作系统或应用程序的漏洞使系统崩溃，从而使系统无法继续提供有效服务，如缓冲器溢出就是利用应用程序不对需要处理的数据长度进行检测的漏洞，导致应用程序的缓冲器溢出，因而影响系统的正常运行，甚至崩溃，从而使系统无法继续提供有效服务。

另一种类型的拒绝服务攻击是消耗掉某个计算机的有效资源，使其没有用于对正常用户提供有效服务所需要的资源。如攻击者向某个计算机发送大量 IP 分组，以此消耗掉计算机的接入带宽，导致正常用户请求服务的 IP 分组无法到达该计算机，因而无法获得服务。还有 SYN 泛洪攻击，通过用大量无效的 TCP 连接建立请求消耗掉计算机的 TCP 会话表资源，从而使计算机没有用于和正常用户建立 TCP 连接的 TCP 会话表资源。

**4. 计算机安全问题的应对措施**

一部分计算机安全问题是由操作系统或应用程序的漏洞引起的，解决这些安全问题的方法是及时为漏洞打上补丁，因此，必须有一套保障所有终端系统都能及时通过补丁软件消除已发现漏洞的机制，最大限度地避免系统遭到攻击。及时发现操作系统和应用程序的漏洞，并通过下载补丁软件予以修补并不是网络安全的范畴，但目前，由于网络中系统众多，各个系统的管理、应用人员的计算机水平又都参差不齐，要求所有系统的管理人

员都能及时发现系统所安装的操作系统和应用程序的漏洞，并通过下载补丁软件予以修补是比较困难的，因此，需要在网络中安装监测系统，由网络监测系统对所有系统安装的操作系统和应用程序进行监测，获取它们的类型和版本号，检测它们是否修补了已发现的漏洞，并对有安全问题的系统进行提醒。安装网络监测系统是一种通过网络安全机制来解决网络中所有系统因为操作系统和应用程序的漏洞而引发的安全问题的方法。

一部分计算机安全问题是需要网络安全机制予以解决的，如拒绝服务攻击，需要网络中的监测设备能够及时检测出这种异常信息流，并对其流量予以管制。网络安全机制也可以识别出含有病毒的信息流，并阻断其网络传播途径。

### 1.1.2 信息传输时的安全问题

目前，信息通过网络进行传输，信息传输时的安全问题毋庸置疑是网络安全问题，它涉及非法接入、信息窃取、源地址欺骗和拒绝服务攻击等，这些安全问题基本上由网络安全机制解决。

**1. 非法接入**

每个企业都有内部网络，或许这样的内部网络也和 Internet 相连，但只允许企业内部人员访问企业内部网络的资源。所谓非法接入是指非企业内部人员连接到了企业内部网络并获得访问内部网络资源的途径。攻击者实现非法接入的手段很多，如通过笔记本计算机直接接入企业内部网络的某个以太网交换机端口，通过远程拨号接入方法接入企业内部网络，利用无线局域网接入企业内部网络等。

**2. 信息窃取**

如果攻击者非法接入企业内部网络，或者信息需要经过公共传输网络进行传输，传输的信息很容易被拦截、窃取和篡改。如攻击者通过修改路由器路由表，将信息发送给攻击者的终端。攻击者通过类似集线器这样的共享式传输设备连接到内部网络的某条主干传输通路上等。这样，经过网络传输的信息有可能被攻击者截获，攻击者可以窃取这些信息，甚至篡改后继续转发给原始目的终端。

**3. 源地址欺骗**

源 IP 地址是信息发送者的一个重要标识符，接收者常用 IP 分组的源 IP 地址来确定信息发送者的身份。为了控制信息流动，也常对允许交换信息的子网进行限制，因此，IP 分组的源和目的 IP 地址也是确定信息是否允许经过路由器转发的依据。攻击者为了达到非法访问的目的，或是为了躲避责任，常用本不存在的，或是其他合法用户的 IP 地址，作为自己发送的 IP 分组的源 IP 地址。

**4. 拒绝服务攻击**

网络中路由器的缓冲器和路由表空间，结点之间链路的带宽都是用于保证信息正常传输的资源，拒绝服务攻击通过消耗掉这些资源，使网络无法正常传输信息，导致传输过程中的信息被阻塞，甚至丢弃。如攻击者通过发送包含大量无用路由项的路由消息给路由器，使路由器的路由表溢出，导致路由器无法正常转发 IP 分组。如大量被攻击者控制的终端同时向某个子网发送大量信息，导致通往该子网的路径因为阻塞而无法正常转发有用信息。

**5. 传输安全问题的应对措施**

防护攻击者非法接入的方法是构建一个能够阻断非法接入途径的内部网络，如以太网的接入认证机制、安全端口机制、无线局域网的安全机制等。防止信息窃取、篡改的最好办法是加密和报文摘要技术。防止源地址欺骗的方法是除了源 IP 地址，还采用数字签名来标识信息发送者，同时，通过测试接收 IP 分组的端口是否连接通往源 IP 地址所确定的发送者的路径来判别 IP 分组源 IP 地址的真伪。防止拒绝服务攻击的机制有信息流管制、有效信息鉴别及过滤等机制。

### 1.1.3 电子交易时的安全问题

随着电子商务的开展和普及，各种电子交易平台出现在网络中，人们开始通过网络实现购物、交易和缴费等活动。这种情况下，电子交易的安全性直接决定电子商务的发展和普及。电子交易的安全性涉及计算机安全和信息传输安全，但除了计算机安全和信息传输安全外，还存在其他安全问题，如通过伪造的某个银行网站，骗取登录用户的银行卡卡号和密码，从而实现非法目的的案例，这就要求提供一种能够对双方身份的真实性进行鉴别的机制。另外，攻击者可能在某次正常电子交易时截获用户请求购物的消息，虽然，加密和报文摘要技术使攻击者无法窃取和篡改该消息，但攻击者经过一段时间后，再次重发该消息，导致购物网站以为该用户将再一次进行购物，造成用户的损失，这就要求提供能够鉴别重复请求消息的机制，解决这些安全问题也是网络安全的范畴。

## 1.2 信息安全目标

信息安全目标是实现信息的适用性、保密性、完整性、不可抵赖性和可控制性等。

### 1.2.1 适用性

适用性是信息被授权实体访问并按需使用的特性。通俗地讲，就是做到有权使用信息的人任何时候都能使用已经被授权使用的信息，信息系统无论在何种情况下都要保障这种服务；而无权使用信息的人，任何时候都不能访问到没有被授权使用的信息。

实现信息适用性的安全目标要求保障计算机系统的适用性和网络系统的适用性，计算机系统不因病毒和拒绝服务攻击而崩溃。网络系统不因拒绝服务攻击而发生阻塞、路由器崩溃。电子交易过程中能够正确鉴别交易双方的身份，并对交易请求进行重复性检测。

### 1.2.2 保密性

保密性是防止信息泄露给非授权个人或实体，只为授权用户使用的特性。通俗地讲，信息只能让有权看到的人看到，无权看到信息的人，无论在何时，用何种手段都无法看到信息。

实现信息保密性的安全目标要求计算机系统能够严格控制信息访问过程，防止非授权用户的非法访问。网络系统能够严格控制非授权用户接入网络，按照安全等级划分子