高等学校计算机专业教材精选·网络与通信技术

网络安全基础教程

许 伟 廖明武 等编著

清华大学出版社

高等学校计算机专业教材精选·网络与通信技术

网络安全基础教程

许 伟 廖明武 等编著

清华大学出版社
北京

内 容 简 介

本书详细介绍了网络安全的基础知识与典型应用，共分为9章，主要内容包括网络安全概论、计算机病毒防范、数据加密、防火墙技术、计算机安全管理、局域网安全管理、广域网安全管理、网络安全规划和网络安全实施。在每一章中，不仅讲解了基本原理，还尽量让读者能够动手操作一些实践项目，让读者有思考和练习的空间。

本书在编写过程中，介绍了实用的和最新的技术，做到通俗易懂、图文并茂；并且本书采用循序渐进的方式，结合实际案例，有助于读者上机练习。

本书可作为大专院校相关课程教材，也可作为网络安全爱好者的自学参考书。

图书在版编目（CIP）数据

网络安全基础教程 / 许伟，廖明武等编著. —北京：清华大学出版社，2009.6
（高等学校计算机专业教材精选·网络与通信技术）
ISBN 978-7-302-19312-8

I. 网… II. ①许…②廖… 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 008761 号

责任编辑：战晓雷　王冰飞
责任校对：梁　毅
责任印制：李红英
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：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.5　**字　数**：483 千字
版　　次：2009 年 6 月第 1 版　　**印　　次**：2009 年 6 月第1 次印刷
印　　数：1～4000
定　　价：27.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：023125-01

出版说明

我国高等学校计算机教育近年来迅猛发展，应用所学计算机知识解决实际问题，已经成为当代大学生的必备能力。

时代的进步与社会的发展对高等学校计算机教育的质量提出了更高、更新的要求。现在，很多高等学校都在积极探索符合自身特点的教学模式，涌现出一大批非常优秀的精品课程。

为了适应社会的需求，满足计算机教育的发展需要，清华大学出版社在进行了大量调查研究的基础上，组织编写了《高等学校计算机专业教材精选》。本套教材从全国各高校的优秀计算机教材中精挑细选了一批很有代表性且特色鲜明的计算机精品教材，把作者们对各自所授计算机课程的独特理解和先进经验推荐给全国师生。

本系列教材特点如下。

(1) 编写目的明确。本套教材主要面向广大高校的计算机专业学生，使学生通过本套教材，学习计算机科学与技术方面的基本理论和基本知识，接受应用计算机解决实际问题的基本训练。

(2) 注重编写理念。本套教材作者群为各校相应课程的主讲，有一定经验积累，且编写思路清晰，有独特的教学思路和指导思想，其教学经验具有推广价值。本套教材中不乏各类精品课配套教材，并力图努力把不同学校的教学特点反映到每本教材中。

(3) 理论知识与实践相结合。本套教材贯彻从实践中来到实践中去的原则，书中的许多必须掌握的理论都将结合实例来讲，同时注重培养学生分析、解决问题的能力，满足社会用人要求。

(4) 易教易用，合理适当。本套教材编写时注意结合教学实际的课时数，把握教材的篇幅。同时，对一些知识点按教育部教学指导委员会的最新精神进行合理取舍与难易控制。

(5) 注重教材的立体化配套。大多数教材都将配套教师用课件、习题及其解答，学生上机实验指导、教学网站等辅助教学资源，方便教学。

随着本套教材陆续出版，相信能够得到广大读者的认可和支持，为我国计算机教材建设及计算机教学水平的提高，为计算机教育事业的发展做出应有的贡献。

清华大学出版社

前　言

在当前的网络社会中，各行各业对计算机的依赖性日益增强，越来越多的人在使用Internet，有些人还要将办公室、家庭与远程工作空间的计算机相连接，许多人的计算机中存储着关于个人、公司甚至国家机密的重要信息，所以，网络安全已经成为一个日益重要的课题。美国联邦调查局（Federal Bureau of Investigation，FBI）报告显示，危害性网络安全攻击数量在逐年上升。计算机攻击的扩散以及对网络和对远程访问依赖程度的不断增长，促成了对诸如防火墙和虚拟专用网（VPN）等系统需求的增长。同样，也促成了社会对网络安全专业人员的需求，各种组织需要配备能够统筹掌握安全软件与硬件的专业人员。

我国计算机安全防护能力尚不发达，政府、企业团体和个人计算机用户的安全意识都不强，计算机很容易受到内部窃贼、计算机病毒和网络黑客的攻击，这些攻击往往具有极大的风险性。重要数据、文件的滥用、泄露、丢失和被盗，不仅会给国家、企业和个人造成巨大的经济损失，而且严重危及到国家安全和社会稳定。如何保护计算机中的信息不被非法获取、盗用、篡改和破坏，已成为令人关注和亟待解决的问题。

近年来，我们对于网络和信息安全方面不是没有作为，应该说有关部门、专业公司和专业人士也投入了较大的精力对付这类问题，也解决了很多问题。但是，网络安全是一个不断变化发展的领域，网络攻击和防卫在不断的博弈中。起初，在20世纪90年代，信息安全问题主要以简单病毒的形式出现，那时病毒的变化、产生和传播是缓慢的。后来，进入21世纪后，随着互联网用户的增长，互联网以及作为其通用协议的TCP/IP被广泛接纳，这就为越来越多的攻击传播途径提供了作用平台。这不仅产生了对更多更强大的防御机制的需求，同时也相应提供了入侵对象和入侵者。就防病毒产业而言，这种猫鼠游戏过程既提高了攻击工具，也提高了防御工具的复杂性水平。互联网的普遍特性也使其变为一个具有很多目标的环境，而且它还为攻击者提供了若干可以发起攻击的地方。在安全前景改变的同时，围绕安全展开的讨论课题也在发展和变化。

伴随着网络和信息安全这项产业的成熟，我们正在目睹这个概念完全和根本上被公开。各公司正在逐步提高安全意识和对安全事务的响应。比如说微软公司，曾经一度由于他们的安全状况而被人们嘲笑，现在，他们已经是安全响应上真正的先驱。现在微软的产品在发布之后，会不断地提供针对安全问题的补丁。

本书详细介绍了信息安全领域的各个方面，主要内容有：网络安全概论、计算机病毒防范、数据加密、防火墙技术、计算机安全管理、局域网安全管理、广域网安全管理、网络安全规划和网络安全实施。在每一章中，不仅讲解了基本原理，还尽量训练读者动手操作项目，让读者有思考和练习的空间。

本书具有完善的知识体系，对知识的讲解细致详尽，循序渐进，通俗易懂，能逐步提高读者的使用能力，巩固学习技能。

另外，本书注重实践、强调实用。每章课后的练习题，由简单到复杂，完全覆盖了该章涉及的重要知识。

本书主要面向希望了解网络安全基础知识的读者。虽然本书是一本基础书，但要求读者是熟练的计算机用户，经常使用计算机工作或学习，能够熟练使用电子邮件和 Web 浏览器，了解基本的术语。读者应该具备基本的计算机知识，但不需要系统学习计算机专业的课程。

本书由清华大学许伟、廖明武老师主编，李腾和王雷博士也参加了编写和修改。参加本书编写工作的还有李伟、郭涛、冯哲、韩毅、马以辉、邓卫、邓凡平、周云、董武、郑晓蕊、陈占军、倪泳智、黄虹、吕巧珍、裘蕾、金颖、王嘉佳、吴建伟、宋雁、何晓刚、段涛、马丽娟、郭翔、朱晓林、陈磊、李建锋、刘延军、刘子瑛、徐英武、魏宇、赵远锋等人。

本书在编写过程中，参考了许多与网络安全知识相关的杂志和书籍，对于这些文章的作者和书籍编者在此表示衷心的感谢！网络安全本身是一个新兴的事物，许多的理论、实践仍在探索之中，再加上编者学识有限或编写的疏漏，如存在错误和不妥之处，请读者批评指正。

作　者

2009 年 2 月

目　录

第 1 章　网络安全概论

教学提示

计算机网络的广泛应用，为人们的生产、生活、工作、娱乐等带来了方便，同时由于技术原因和人为因素，也为人们带来了诸多安全隐患。

本章首先回顾了计算机网络技术的发展和应用情况，然后提出当前网络安全所面临的挑战，并对网络安全所涉及的内容进行了简要说明，提出了解决网络安全问题的总体思路，最后强调了网络安全的重要性和紧迫性。

通过对本章的学习，应当对网络安全问题以及解决网络安全问题的方法有一个初步的认识，为进一步学习相关知识奠定一个良好的基础，并认清做好网络安全工作的重要意义。

教学重点

- 理解网络安全所面临的挑战。
- 掌握网络安全的内容。
- 掌握网络安全问题的解决思路。
- 理解网络安全的重要性和紧迫性。

1.1　计算机网络的发展和应用

计算机技术与通信技术相结合，使计算机网络技术得以产生和发展。

1．网络技术的发展

最初的计算机网络是一台主机通过导线连接若干个远程的终端，这种网络称为面向终端的计算机通信网。它是以单个主机为中心的星形网，效率不高，功能有限。这就是第一代网络。

1969 年 12 月在美国诞生了阿帕网络（ARPANET），它以通信子网为中心，许多主机和终端设备在通信子网的外围构成一个用户资源子网，通信子网不再使用电话通信的电路交换方式，而采用了数据通信的分组交换方式，大大提高了通信效率，降低了通信费用。这就是第二代计算机网络。

国际标准化组织（ISO）于 1977 年提出了著名的开放系统互连参考模型，简称 OSI/RM，从此以后，就开成了第三代计算机网络，其中，最引人注目的就是 Internet 的飞速发展。

进入 20 世纪 90 年代，计算机网络的发展更加迅速，出现了宽带综合业务数字网（B-ISDN），这就是第四代计算机网络。

我国在 1989 年建成第一个用于数据通信的公用分组交换网，1993 年建成新的覆盖全国的中国公用分组交换网（CHINAPAC），同年 3 月，我国启动金桥工程、金卡工程、金关工程等一系列“金”字工程，计算机网络是这些工程中的重要组成部分。1995 年邮电部投资建成中国公用计算机互联网（CHINANET），提供 Internet 业务。

2．网络技术的应用

计算机网络通常应用于以下几个方面。

1）数据通信

它使分布在不同位置的计算机与计算机可以进行通信，互相传送数据，方便地进行信息交换。例如，使用电子邮件、视频会议等。

2）资源共享

这是计算机网络最具有吸引力的功能，在网络范围内，用户可以共享软件、硬件、数据等资源，而不必考虑用户以及资源所在的位置。

3）实现分布式计算

由于有了计算机网络，许多大型信息处理问题可以借助于分散在网络中的多台计算机协同完成，解决单机无法完成的信息处理任务。特别是分布式数据库管理系统，它使分散存储在网络不同系统中的数据，使用时好像集中存储和集中管理那样方便。

4）提高计算机系统的可靠性和可用性

网络中的计算机可以互为后备，一旦某台计算机出现故障，它的任务可由网中其他计算机取而代之。当网中计算机负荷过重时，网络可将新任务分配给较空闲的计算机去完成，提高了每台计算机的可用性。

1.2 网络安全所面临的挑战

计算机网络的出现，从很大程度上改变了人们进行信息交流的方式，以前需要大量书信用很长时间才能解决的问题，今天可以通过电子信息来迅速解决，不但大大降低了成本，而且效率得到了很大的提高。当然，计算机网络在带给方便、高效的同时，也存在一定程度上的安全问题，需要认真对待，否则，我们可能会蒙受各种程度的损失。

1.2.1 网络内部安全挑战

网络内部安全挑战是指内部人员因工作需要或者外部人员因有机会直接在一个特定网络内部进行操作而造成的安全威胁。

1．网络硬件安全挑战

网络硬件安全挑战是指因为计算机网络的硬件设备故障所造成的安全问题。网络硬件设备是计算机网络正常使用的基础，要让计算机网络正常、稳定、高效运行，那么合理选择硬件设备、合理规划并搭建网络系统、正确配置运行参数都是必不可少的。好在随着计算机技术和网络技术的不断发展和进步，计算机网络硬件设备本身的稳定性和可靠性都有了很大程度的提高，发生故障的几率已经很小了，目前的挑战主要是如何合理规划并搭建网络以及正确配置网络硬件的运行参数了，这两项对于一个大型的网络系统是至关重要的。

2．网络软件安全挑战

网络软件安全挑战是指系统中所安装和使用的软件没能提供预定功能或者提供了错误的功能。其中最明显的例子就是操作系统，操作系统应该提供一个安全的操作环境，因为各个方面的原因可能使操作系统存在各种各样的漏洞。同样数据库系统也是一样，可能因

为考虑不周而出现漏洞，使得原本安全的系统变得不安全了。

病毒程序和木马程序通常是附在正常的程序或者文件之中进行传播，它们所提供的功能是客户所不需要的，属于错误的功能。

3．人为安全挑战

人为安全挑战分为两种类型，第一种是无意造成的安全威胁，第二种是有意造成的安全威胁。两者的操作结果都是因出现了错误的操作而导致不希望的后果，但前者不是操作者本意的表示，比如操作者不小心误操作将自己计算机或者文件服务器上的文件删除了。而后者正好是操作者本意的表示，比如离职的职员出于对公司的不满，将自己计算机或者其他计算机上的有用文件删除了。

这两种情况虽然结果是一样的，但是性质却是完全不同的。对于无意造成的安全威胁相对比较容易解决，而对于有意造成的安全威胁需要采取多种措施才能有较好的效果，这将是本书在后面将要讨论的话题。

1.2.2　网络外部安全挑战

网络外部安全挑战是指来自外部网络（外部网络是指除了用户可控的局部网络以外的网络，如 Internet 网）的安全威胁，包括两种情况，一种是在使用网络服务时引入的安全问题，因为只有在连接网络并使用网络服务时才会发生，所以称为被动攻击，如下载文件资料时引入病毒、木马等有害程序；另一种是来自外部的黑客攻击，因为只要和外部网络处于连接状态，即使没有进行任何操作仍然可能受到攻击，所以称为主动攻击，即利用系统安全漏洞非法进入计算机系统进行非法操作，如破坏系统资源或者窃取资料。

1．被动攻击

被动攻击的特点是目标性不明确，在攻击发生之前并没有确定某个具体的计算机为目标，只是把有害程序放置在一个特定的位置，通常是一个网站上，当访问者访问网页时，如果访问者的计算机安全性不够高的话，有害程序就会直接下载到访问者的计算机上，并在适当的时候被激活，从而对访问者计算机进行非法操作。也有的将有害程序放置在网页上，然后引诱访问者去点击，从而将有害程序下载到访问者的计算机上。还有将有害程序藏匿在资料文件中，等访问者下载资料文件的同时将有害程序一起下载。

2．主动攻击

主动攻击的特点是具有明确的目标，通常使用的方式是通过扫描工具对某个特定的网络范围进行扫描，对扫描得到的计算机再逐个进行试探性攻击，找出安全性比较弱的计算机进行攻击，从而达到破坏目标计算机系统或窃取目标计算机上资料的目的。

1.3　网络安全的内容

网络安全主要包括三个方面的内容，即计算机安全、局域网安全以及广域网安全。计算机是网络中的一个非常重要的组成部分，其负责存储、计算、发送以及接收数据信息，所以保证计算机的安全是网络安全的一个重点。除了要保证单台计算机的安全，还要考虑整个网络系统的安全，对于一个网络系统，通常是一个完整的系统，其中某些部分出现问题，可能会危及整个网络系统的安全运行。对于 Internet 网的使用也存在多种网络安全问题，

需要我们在使用之前做好安全防范工作，将网络安全风险减小到最低。

1.3.1 计算机安全

计算机安全是指单台计算机范围内的安全，通常包括系统安全和数据安全两个方面，系统安全是基础，数据安全是目的。这是网络安全最基本的内容，没有计算机范围内的安全，也就不可能有网络范围的安全。

1. 系统安全

系统安全是指计算机系统能够正常、稳定、高效地提供其功能。系统安全的问题来自多个方面，可能是病毒、木马程序、黑客攻击、人为破坏、硬件故障等。具体体现在以下几个方面。

（1）补丁安全。通常的操作系统和其他系统软件都容易出现安全漏洞，给病毒、木马程序、黑客等以可乘之机，注意随时对系统进行升级并尽可能安装最新的补丁程序是防止安全漏洞被利用的最有效方法。

（2）配置安全。包括系统中账户的建立、密码的设置、注册表访问权限的控制、控制面板访问权限的管理以及文件系统的安全配置等，通过对系统自身的安全系统进行合理的配置，可以大大提高系统的安全性。

（3）系统备份。系统的安全威胁是来自多个方面的，只要一个方面没有考虑到就可能影响系统的正常运行，甚至使系统停止运行。如果重新配置系统需要很长的时间，最有效的方法就是有计划地对系统进行备份，在必要的时候通过恢复备份的方式来解决系统问题。

（4）杀毒。计算机病毒和木马程序是威胁计算机系统安全的两个至关重要的因素，因为病毒和木马程序通常都是隐藏在后台，不易被发现，只有遭到破坏以后才会被发现，而且两者的破坏性都可能很大，所以对病毒和木马程序的防范决不能掉以轻心。

2. 数据安全

数据安全是指用户存储在计算机上的数据信息不被非法查看、修改、移动和删除。数据安全威胁主要来自三个方面，一方面是系统安全被突破以后带来的数据安全威胁；第二方面是人为操作带来的数据安全威胁，第三方面是硬件故障带来的数据安全威胁。要做好数据安全工作，必须同时注意到这三个方面的威胁。具体体现在以下几个方面。

（1）文件安全。对计算机上的文件操作进行监控审计，对文件操作进行记录，并对必要的文件提供自动备份和恢复的功能，以便审计时及时发现和找出非法文件操作的原因，及时采取措施防止非法的文件操作造成文件资料的泄密、破坏，提高文件安全性。

（2）外设接口安全。计算机提供多种接口是为了使用上的方便，但是如果没有合理的规划和管理，这些接口可能成为数据安全的一大隐患。特别是具有将计算机上的数据拷贝带出的接口，如软驱、刻录机、打印机、USB 接口的存储设备等。

（3）打印安全。打印文件是日常工作和生活中常见的一件事情，但是如果有人将不应该打印的重要文件资料打印出来带到不应该带去的地方就麻烦了，比如软件源代码、工程项目文件、客户资料等。

（4）刻录安全。刻录光盘是一种常用的系统备份或者数据备份方式，最重要的原因是该方式简单，而且成本很低。但是如果没有合理的管理，可能导致非法将计算机中的文件进行刻录，从而导致信息泄密。