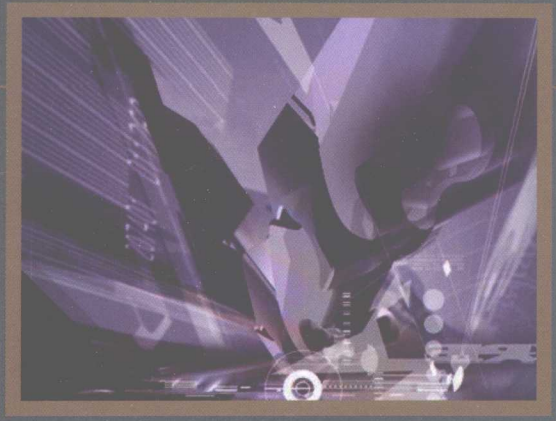
高等学校计算机科学与技术教材

网络安全技术

□ 丰继林　高焕芝　主编



- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

清华大学出版社　●　北京交通大学出版社

高等学校计算机科学与技术教材

网络安全技术

丰继林　高焕芝　主　编

清华大学出版社
北京交通大学出版社

·北京·

内 容 简 介

本书在内容安排上充分考虑理论与实践相结合的原则，注重培养学生的网络安全应用技能。

本书将网络安全所涉及的相关内容归纳为14章，内容安排上从基本概念入手，由浅入深，让初学者一步步掌握知识点，最后通过工程实例将所学知识综合运用，加深理解。本书具体内容包括网络安全概论、网络安全协议、操作系统安全技术、数据库安全技术、信息加密技术、数字签名技术和CA认证技术、网络病毒防范技术、网络攻击与防范技术、防火墙技术、入侵检测技术、VPN技术、无线网安全技术、电子商务安全技术及网络安全评估。

本书突出实用性、系统性，从网络安全管理者的角度详细讲解了网络安全可能面临的各种安全威胁、网络安全防御及网络安全评估的应用实战技术。每章都配有相应的习题和实训题目，帮助读者对书中内容进行学习验证，具有很强的实践性。

本书可作为应用型本科和高职高专计算机类专业教材，以及非计算机专业的网络安全普及教材，也可以作为网络安全爱好者的自学教材及网络安全管理员的辅助参考资料。

图书在版编目（CIP）数据

网络安全技术/丰继林，高焕芝主编. —北京：清华大学出版社；北京交通大学出版社，2009.8

ISBN 978-7-81123-753-5

Ⅰ.网…　Ⅱ.①丰…　②高…　Ⅲ.计算机网络-安全技术　Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2009）第135309号

责任编辑：杨正泽

出版发行：清华大学出版社　邮编：100084　电话：010-62776969　http://www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010-51686414　http://press.bjtu.edu.cn

印 刷 者：北京东光印刷厂

经　　销：全国新华书店

开　　本：185×260　印张：25.75　字数：660千字

版　　次：2009年9月第1版　2009年9月第1次印刷

书　　号：ISBN 978-7-81123-753-5/TP·519

印　　数：1～4 000册　定价：38.00元

前　言

随着网络应用领域的拓宽和网络攻击技术的快速发展，网络安全问题已经成为网络用户面临的最大挑战。如何能在网络的海洋中安全翱翔，成为每个网络爱好者必须要思考的问题。可见对网络安全相关知识的了解对于目前的网络用户来说已经极其重要，作为大学生，尤其是计算机专业的学生，网络安全知识更为重要。

本书针对各类院校专科、应用型本科学生的特点组织编写。以培养网络安全管理方面的应用型人才为目标，将重点放在对网络安全基础知识的了解和各种网络安全技术的应用之上，将理论、技术、应用融为一体，同时也兼顾到教材的先进性、实用性和可读性。

本书将网络安全所涉及的各个知识领域做了详细的归纳总结，并以工程案例为导线，将理论知识融入到工程案例中，便于学生的理解掌握。

本书内容主要包括网络安全的基础知识，如网络安全的概念、特性、发展趋势、常见网络协议的安全、操作系统的安全和数据库的安全；各种常用的网络安全技术，如信息加密技术、数字签名技术、病毒防范技术、攻击与防范技术、防火墙技术、入侵检测技术、VPN技术、无线网技术及电子商务安全技术；网络安全的评估标准，以便于对网络进行安全的评估工作。

本书由丰继林、高焕芝担任主编，其中第1、2章由丰继林编写，第3、4章由庞国莉编写，第5、6章由王小英编写，第7、8章由高焕芝编写，第9、10章由李芳编写，第11、12章由陈小娟编写，第13、14章由张兵编写。由高焕芝进行初稿通稿，丰继林进行最后的修改和定稿。

本书在编写过程中得到各界人士的大力支持，在此对给予帮助和支持的同仁表示深深的感谢。

由于编者水平有限，本书肯定有不少内容和形式上的不妥之处，恳请读者指正。同时希望读者能够经常与编者交流教学和学习经验，编者的电子信箱是 ghzygc_1976@163.com。

编　者

2009年9月

目　录

第1章

网络安全概论

教学目标

本章主要掌握网络安全的含义、网络安全威胁，了解OSI安全服务、OSI安全机制和OSI安全服务的层配置，掌握网络安全体系结构的基本模型。学完本章将对网络安全从宏观上有较好的把握。

教学要求

知识要点	能力要求
网络安全的含义	掌握网络安全的基本概念
网络安全威胁	掌握网络安全面临的威胁
OSI安全服务	了解OSI安全服务
OSI安全机制	了解OSI安全机制
OSI安全服务的层配置	了解OSI安全服务的层配置
网络安全体系结构模型	掌握网络安全体系结构模型

网络安全是什么？每个接触计算机的人都会这么问？在这里将详细给大家介绍网络安全的概念、特征及常遇到的网络安全威胁，网络安全体系结构及模型等知识，让大家对网络安全有一个初步的认识和理解。

1.1 网络安全概述

以Internet为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要因素，而Internet所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在两个方面。

① 开放性的网络，导致网络的技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如，任何具有不良企图的黑客可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的攻击不仅仅来自本地网络用户，它可以来自Internet上的任何一台主机，也就是说，网络安全所面临的是一个国际化的挑战。

② 自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而不受任何的法律限制。

开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得人们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力，同时人们又要面对网络开放带来的数据安全的新挑战和新危险。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的重要事情之一。

1.1.1 网络安全案例

安全性是互联网技术中最关键也最容易被忽视的问题。许多组织都建立了庞大的网络体系，但在多年的使用中从未考虑过安全问题，直到网络安全受到威胁，才不得不采取安全措施。随着计算机网络的广泛使用和网络之间数据传输量的急剧增长，网络安全的重要性愈加突出。

1994 年末，俄罗斯黑客弗拉基米尔·利文伙同朋友在圣彼得堡的一家小软件公司的联网计算机上，向美国花旗银行进行了一连串恶性攻击，以电子转账方式，从花旗银行在纽约的计算机主机里窃取了 180 万美元。

1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，美国司法部主页被篡改，还留下大量攻击美国司法政策的文字，此事在当时成为轰动一时的新闻。

1996 年 12 月 29 日，黑客入侵美国空军的全球网网站并将其主页肆意修改，其中有关美国空军介绍、新闻发布等内容被替换成了一段黄色录像，并且声称美国政府所说的一切都是谎言，迫使美国国防部一度关闭了近 80 多个军方网站。

1996 年 2 月，刚开通不久的 Chinanet 网站就受到了攻击，且攻击得逞。

1997 年初，北京某 ISP 运营商被黑客成功侵入，并在清华大学“水木清华”BBS 的“黑客与解密”论坛张贴如何免费通过该 ISP 进入 Internet 的文章。

2002 年 2 月，Yahoo 网站和 ZDNet 遭遇分布式拒绝服务攻击。

2003 年，冲击波（Blaster）至少攻击了全球 80%的 Windows 用户。

2005 年，中国台湾地区一名 38 岁无业男子，破解了中国台湾地区 40 多家网络银行的虚拟硬盘，取得上千笔资料，并冒充银行服务人员发送网络钓鱼 E-mail，到处散播伪造的第二代金融卡驱动升级程序。

2006 年 10 月，成都电子科技大学职业教育学院电子商务专业 03 级在校大学生宋某在成都市利用互联网多次搜索他人身份证号码和招商银行卡卡号，并通过身份证测试银行卡密码，测试成功后，通过网上消费的方法，窃得苏州某高校在校 44 名大学生发放奖学金的银行卡内的存款 51 619.12 元。

2007 年 6 月 21 日，美国国防部长亲口证实，五角大楼的一个非保密电子邮件系统一天前遭受黑客攻击，迫使国防部 1 500 个电子邮件账户脱机停用，以至于美国众议员兰吉在国土安全委员会听证会上忧心忡忡地说：“这说明什么？这意味着恐怖分子或其他国家能入侵美国国土安全部的数据库，篡改姓名以便让他们能进入我国，而我们甚至根本上不晓得他们已经得逞！”

2007 年 9 月 2 日，美国宣布，美国政府招聘人员的专用网站遭受黑客入侵，大约 14.6 万名用户的数据被盗取，以至于该网站随即被迫关闭。

2008 年据不完全统计，我国的网络安全问题近年来呈逐年上升趋势，1998 年公安部有

关部门受理网络犯罪案件仅 80 多起，1999 年增至 400 多起，2000 年剧增为 2 700 多起，2001 年增加到 4 500 多起，比 2000 年上升约 70%，2002 年又上升到 6 600 多起，而且仅 2003 年上半年就有 4 800 多起，比同期上升 77.1%。

有关黑客威胁的报道已经屡见不鲜，而内部工作人员的疏忽甚至有意充当间谍对网络安全已构成更大的威胁。内部工作人员能较多地接触内部信息，工作中的任何大意都可能给信息安全带来威胁。无论是有意的攻击，还是无意的误操作，都会给系统带来不可估量的损失。虽然目前大多数的攻击者只是恶作剧似地使用篡改网站主页、拒绝服务等攻击，但当攻击者的技术达到某个层次后，他们就可以窃听网络上的信息，窃取用户密码、数据库等信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，可以删除数据库内容，摧毁网络节点，释放计算机病毒等。

综上所述，网络必须有足够强大的安全措施。无论是局域网还是广域网，无论是单位还是个人，网络安全的目标是全方位地防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.1.2　网络安全的含义

网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的机密性、完整性及可使用性受到保护。要做到这一点，必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件，如终端、调制解调器、数据链路的功能仅仅能被那些被授权的人访问。网络的安全问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控性的相关技术和理论都是网络安全的研究领域。机密性指确保信息不暴露给未授权的实体或进程。完整性则意味着只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改。可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。可控性表示可以控制授权范围内的信息流向及行为方式。可审查性指对出现的网络安全问题提供调查的依据和手段。

网络安全的具体含义随观察者角度不同而不同。从用户（个人、企业等）的角度来说，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、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者角度说，希望其网络的访问、读写等操作受到保护和控制，避免出现“后门”、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，制止和防御黑客的攻击。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，避免给国家造成损失。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威胁，必须对其进行控制。

1.1.3　网络安全的特征

要保证网络安全，最根本的就是保证网络安全的基本特征发挥作用。因此，下面先介绍信息安全的 5 大特征。

1. 保密性

保密性指确保信息不暴露给未授权的实体或进程。

2. 完整性

完整性指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

3. 可用性

可用性指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。比如网络环境下的拒绝服务，破坏网络和有关系统的正常运行等都属于对可用性的攻击。

4. 不可否认性

不可否认性指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

5. 可控性

可控性指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

1.1.4 网络安全威胁

网络安全威胁是指实体对网络资源的保密性、完整性和可用性在合法使用时可能造成的危害。这些可能出现的危害，是某些别有用心的人通过一定的攻击手段来实现的。网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听或篡改等。

网络安全威胁主要有以下 4 种。

① 截获（Interception）：攻击者从网络上窃听他人的通信内容。

② 中断（Interruption）：攻击者有意中断他人在网络上的通信。

③ 篡改（Modification）：攻击者故意篡改网络上传送的通信内容。

④ 伪造（Fabrication）：攻击者伪造网络上的通信内容并进行传送。

上述 4 种威胁可划分为被动攻击和主动攻击两大类，截获信息的攻击称为被动攻击；中断、篡改和伪造信息的攻击称为主动攻击。

对网络安全威胁较大的还有如下 4 种恶意程序，分别为计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹。

美国基础设施保护中心（NIPC）做了一个统计，近几年，平均每个月出现 10 种以上新的攻击手段。深圳市安络科技有限公司（CNNS）特地组织安全专家对近几年的网络安全威胁，尤其是最近出现的新攻击手段进行分析，从图 1-1 可以看出，基于各种攻击机制的各种现成攻击工具越来越智能化，也越来越傻瓜化。虽然大多数的攻击手法都惊人的相似，无非是蠕

虫、后门、rootkits 和 DoS 等，但这些手段都体现了强大的威力。攻击手段的新变种与以前出现的相比，更加智能化，攻击目标直指互联网基础协议和操作系统。同时，黑客工具应用起来也越来越简单，使很多新手也能轻易使用黑客工具，而且，对攻击者入侵技术的要求越来越低。

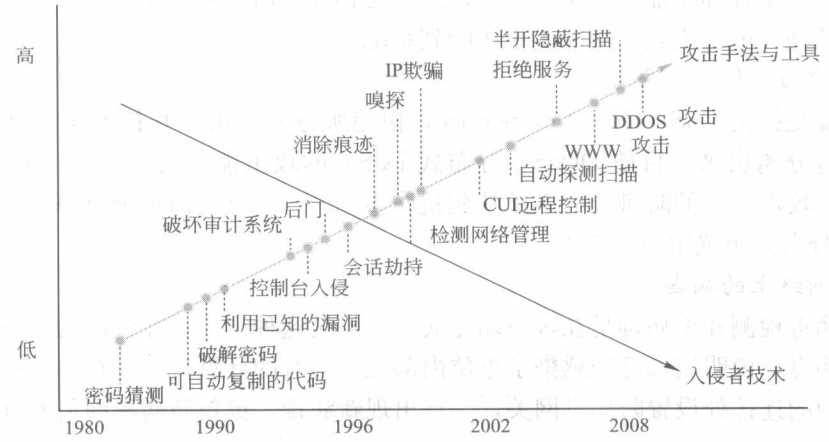


图 1-1　攻击手法与入侵者技术对比图

病毒技术与黑客技术的结合对信息安全造成更大的威胁。近年来，流行的计算机病毒无一例外地与网络结合，同时具有多种传播方法和攻击手段，一旦爆发即在网络上快速传播，难以遏制，加之与黑客技术的融合，潜在的威胁和损失更巨大。从发展趋势来看，现在的病毒已经由从前的单一传播、单种行为，变成依赖互联网传播，具有电子邮件、文件传染等多种传播方式，集黑客、木马等多种攻击手段于一身的广义的“新病毒”。

今后恶意代码、网络安全威胁和攻击机制的发展将具有以下特点。

① 与互联网更加紧密地结合，利用一切可以利用的方式（如邮件、局域网、远程管理、即时通信工具等）进行传播。

② 所有的病毒都具有混合型特征，集文件传染、蠕虫、木马、黑客程序的特点于一身，破坏性大大增强。

③ 扩散极快，而且更加注重欺骗性。

④ 利用系统漏洞将成为病毒有力的传播方式。

⑤ 无线网络技术的发展使远程网络攻击的可能性加大。

⑥ 各种境外情报、谍报人员将越来越多地通过信息网络渠道搜集情报和窃取资料。

⑦ 各种病毒、蠕虫和后门技术越来越智能化，并呈现整合趋势，形成混合性威胁。

⑧ 各种攻击技术的隐秘性增强，常规手段不能识别。

⑨ 分布式计算技术用于攻击的趋势增强，威胁高强度密码的安全性。

⑩ 一些政府部门的超级计算机资源将成为攻击者利用的跳板，网络管理安全问题日益突出。

网络安全技术的发展是多维、全方位的，主要有以下几方面。

1）物理隔离

物理隔离的思想是不安全就不联网，要绝对保证安全。在物理隔离的条件下，如果需要进行数据交换，就如同两台完全不相连的计算机，必须通过软盘等媒介，从一台计算机向另一台计算机复制数据，这也被形象地称为“数据摆渡”。由于两台计算机没有直接连接，就