普通高等教育“十一五”国家级规划教材
教育部普通高等教育精品教材

工业和信息化“十三五”高职高专人才培养规划教材

计算机网络安全技术 第4版

Network Security Technology

石淑华 池瑞楠 ◎ 主编

历经市场考验： 累计 **33** 次印刷，销量超过 **10** 万册

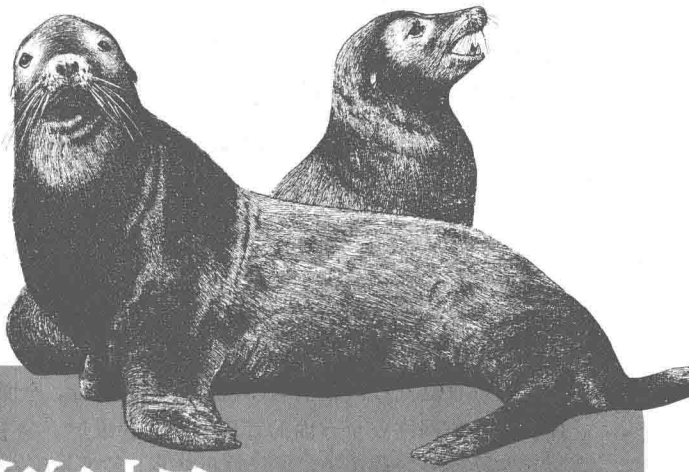
内容精心编排： 应用能力培养为核心，职业技能提升为重点

教学资源丰富： PPT 课件 + 教学大纲 + 教案 + 教学进度表 + 习题答案

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材
教育部普通高等教育精品教材

工业和信息化“十三五”高职高专人才培养规划教材



计算机网络安全技术（第4版）

Network Security Technology

石淑华 池瑞楠 ◎ 主编

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

计算机网络安全技术 / 石淑华，池瑞楠主编. -- 4版. -- 北京 : 人民邮电出版社，2016.8
工业和信息化“十三五”高职高专人才培养规划教材
ISBN 978-7-115-42647-5

Ⅰ. ①计… Ⅱ. ①石… ②池… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第123127号

内 容 提 要

本书根据高职院校的教学特点和培养目标，全面介绍了计算机网络安全的基本框架、基本理论，以及计算机网络安全方面的管理、配置和维护。全书共 7 章，主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、计算机病毒、数据加密技术、防火墙技术、Windows Server 的安全及 Web 应用安全。本书注重实用，以实验为依托，将实验内容融合在课程内容中，使理论紧密联系实际。

本书可作为高职高专计算机及相关专业的教材，也可作为相关技术人员的参考书或培训教材。

◆ 主　　编　石淑华　池瑞楠
责任编辑　桑　珊
执行编辑　左仲海
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：19.5　　2016 年 8 月第 4 版
字数：446 千字　　2016 年 8 月北京第 1 次印刷

定价：49.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

第4版 前 言 FOREWORD

本书的第1版自2005年出版以来，受到广大师生的欢迎，被许多高职院校选用，并分别于2008年、2012年再版，累计重印30多次，总发行超过100000册。2008年我们的“计算机网络安全技术”课程被评为省级精品课程，2012年第3版的教材也被评为“国家级精品教材”。在这几年里，我们在教学中不断积累、总结。这次改版保留原版教材特色，全面更新了教材各章节的内容，及时反映计算机网络安全领域的新技术、新成果，以在内容上更贴近最新计算机网络安全技术的发展。原版保留了以下方面。

（1）注重基础理论。我们根据行业企业发展需要和完成职业岗位实际工作任务所需要的知识、能力，组织了教材的理论体系结构，改版保留了前3版教材中的经典理论内容。

（2）注重实际操作。我们一直强调对学生动手实践能力的培养，在教材中设计了很多针对性的实验和案例，改版保留了前3版教材中大量的实验内容。

随着时间的推移，网络安全技术在不断发展，所以我们对教材进行了全面修订，力争体现以下特色。

（1）注重知识的更新。计算机网络安全技术领域的一个典型特点就是技术更新速度较快。这次改版增加了各种技术相关的新资讯和数据，并增加了很多新的知识。例如，第1章中增加了新内容和新软件，第7章的结构做了很大的变动，知识更加全面。

（2）注重培养学生动手能力和知识的巩固。本书理论“以必需、够用为度”，特别注重实践环节，每章中都增加了大量的实验案例，通过大量的配图使得实验操作步骤尽量详尽；同时增加了课后的习题，注重巩固学生的理论知识。

对于书中提到的一些工具软件，读者可以在Internet上自行下载。本书还配有PPT课件、教学大纲、习题答案等教学资源，任课教师可登录人民邮电出版社教育社区（www.ryjiaoyu.com）免费下载，或者到我们的精品课程网站（http://jpkc.szpt.edu.cn/2008/wlaqjs/）免费下载。

本书由石淑华和池瑞楠老师编写，并由石淑华统稿、审定。在本书的编写过程中，深圳职业技术学院网络技术专业的王隆杰、梁广民、张立涓、杨名川、邹润生、刘平等老师在实验和绘图方面也做了很多工作，在此一一表示感谢！

由于编写水平有限，时间仓促，书中难免有不妥和错误之处，恳请广大读者批评指正。编者邮箱为 sshua@szpt.edu.cn。

编者

2016年4月

目录 CONTENTS

第 1 章 计算机网络安全概述

本章简要介绍了网络安全领域中的问题，讲解了网络系统安全的重要性及网络系统脆弱性的原因。同时，本章给出了网络安全的定义，介绍了信息系统安全的发展历程。本章的重点是培养读者的兴趣，使读者的学习有一个良好的开端。

职业能力要求

- 掌握网络安全行业的基本情况，了解网络安全行业的新技术；培养良好的职业道德。
- 具有认真负责、严谨细致的工作态度和工作作风，具备良好的团队协作和沟通交流能力。
- 具有良好的自学能力，对新技术有学习、研究精神，具有较强的动手操作能力。

学习目标

- 了解网络安全的重要性。
- 掌握网络安全的定义。
- 了解网络安全的发展历程。

1.1 网络安全简介

1.1.1 网络安全的重要性

随着信息科技的迅速发展及计算机网络的普及，计算机网络深入到国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着，计算机网络资源共享进一步加强，信息安全问题日益突出。

据中国互联网络信息中心（China Internet Network Information Center，CINIC）最新发布的中国互联网络发展状况统计报告显示，截至 2015 年 12 月底，中国网民规模达到 6.88 亿，互联网普及率为 50.3%。中国手机网民规模达 6.20 亿，占比由 2014 年的 85.8%提升至 90.1%，如图 1-1 所示。

网民基数大，受到的威胁数量就不容小觑。单从病毒这一威胁来看，腾讯公司的互联网报告中统计出的 2015 年新增病毒样本就接近 1.5 亿个，图 1-2 所示为 2012 年到 2015 年新增病毒数量的统计图。病毒的总数量还是非常庞大的。各种计算机病毒和网上黑客对

Internet 的攻击越来越猛烈，网站遭受破坏的事例不胜枚举。

图 1-1　中国网民数量统计

腾讯2015年互联网安全报告

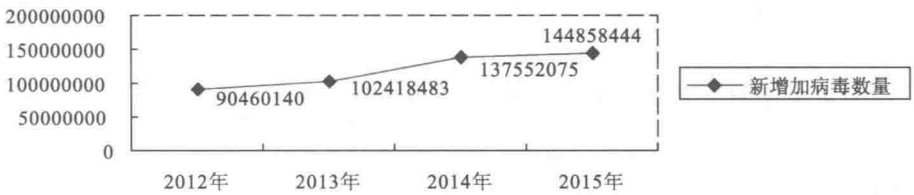


图 1-2　新增加病毒统计（2012～2015 年）

互联网在我国政治、经济、文化及社会生活中发挥着越来越重要的作用。作为国家关键基础设施和新的生产、生活工具，互联网的发展极大地促进了信息流通和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。随着互联网的影响日益扩大、地位日益提升，维护网络安全工作的重要性日益突出。

网络系统出现故障会影响国计民生。1992 年，美国联邦航空管理局的一条光缆被无意间挖断，所属的 4 个主要空中交通管制中心关闭 35 小时，成百上千航班被延误或取消。2008 年 3 月，英国伦敦希斯罗机场第五航站楼的电子网络系统在启用当天就发生故障，致使五号航站楼陷入混乱。

2015 年信息泄露是信息安全中影响最大的因素，其中数量最大的 4 起事件分别为：美国人事管理局 2 700 万政府雇员及申请人信息泄露；美国第二大医疗保险公司 Anthem 8 000 万客户及员工信息泄露；婚外恋网站 Ashley Madison 3 700 万用户信息泄露；意大利间谍软件公司 Hacking Team 被黑，包含多个零日漏洞、入侵工具和大量工作邮件及客户名单的 400G 数据被传到网上任意下载。这 4 起信息泄露事件的影响面各有不同：美国人事管理局（The Office of Personal Mangement，OPM）把这次事件上升到国与国之间网络战争的政治影响；Anthem 主要事关客户个人保险号和病历；Ashley Madison 则主要为隐私和道德问题。这些信息的泄露涉及许多个人的信息安全。

除了民生，信息安全与国家安全息息相关，涉及国家政治和军事命脉，影响国家的安

全和主权。一些发达国家，如英国、美国、日本、俄罗斯等，把国家网络安全纳入了国家安全体系。

2013年的“斯诺登”事件对全世界产生的影响是巨大的。爱德华·斯诺登曾是美国中情局（Central Intelligence Agency，CIA）职员，其通过英国《卫报》和美国《华盛顿邮报》披露了棱镜计划。棱镜计划（PRISM）是一项由美国国家安全局（National Security Agency，NSA）自2007年开始实施的绝密电子监听计划。许可的监听对象包括任何在美国以外地区使用参与计划公司服务的客户，或是任何与国外人士通信的美国公民。国家安全局在PRISM计划中可以获得的数据包括电子邮件、视频和语音交谈、影片、照片、VoIP交谈内容、档案传输、登入通知，以及社交网络细节。监听对象还包括其他国家政要，监听范围之广，令人震惊。NSA直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头都参与其中，为他们挖掘各大技术公司的数据提供便利。

NSA曾与加密技术公司RSA达成了1000万美元的协议，要求在移动终端广泛使用的加密技术中放置后门。RSA此次曝出的丑闻影响非常巨大，作为信息安全行业的基础性企业，RSA的加密算法如果被安置后门，将影响到非常多的领域。

RSA客户遍及各行各业，包括电子商贸、银行、政府机构、电信、宇航业、大学等。超过7000家企业，逾800万用户（包括财富500强中的90%）均使用RSA SecurID认证产品保护企业资料，而超过500家公司在逾1000种应用软件安装有RSA BSafe软件。据第三方调查机构显示，RSA在全球的市场份额达到70%。

斯诺登揭露的可能是美国对外信息安全战略中的冰山一角，但是足够引起其他国家的重视，引发其他国家开始思索：如何摆脱对美国软件、硬件的依赖，发展自主知识产权的安全产品。

信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防空间，称为Cyber-Space，是国际战略在军事领域的演进。这对我国网络安全提出了严峻的挑战。我们国家对信息安全的建设也非常重视，加快建设我国网络安全保障体系。

2016年我国在第十三个五年规划纲里列出了未来5年中国计划实施的100个重大工程及项目，其中明确与信息安全相关的项目有：量子通信与量子计算机、国家网络空间安全和构建国家网络安全和保密技术保障体系。

1.1.2 网络脆弱性的原因

1. 开放性的网络环境

正如一句非常经典的语句所说：“Internet 的美妙之处在于你和每个人都能互相联接，Internet 的可怕之处在于每个人都能和你互相联接。”

网络空间之所以易受攻击，是因为网络系统具有开放、快速、分散、互联、虚拟、脆弱等特点。网络用户可以自由访问任何网站，几乎不受时间和空间的限制。信息传输速度极快，因此，病毒等有害信息可在网上迅速扩散和放大。网络基础设施和终端设备数量众多，分布地域广阔，各种信息系统互联互通，用户身份和位置真假难辨，构成了一个庞大

而复杂的虚拟环境。此外，网络软件和协议存在许多技术漏洞，让攻击者有了可乘之机。这些特点都给网络空间的安全管理造成了巨大的困难。

Internet是跨国界的，这意味着网络的攻击不仅仅来自本地网络的用户，也可以来自Internet上的任何一台机器。Internet是一个虚拟的世界，所以无法得知联机的另一端是谁。图1-3所示为网上非常出名的一幅图片，图片阐述的含义是虚拟环境中不知对方是谁。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络安全面临的是一个国际化的挑战。

图1-3 网上图片

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构想，因此，任何一个人、团体都可以接入，网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，也可能是对网络通信协议及应用的攻击；可能是对软件的攻击，也可能是对硬件的攻击。

2. 协议本身的脆弱性

网络传输离不开通信协议，而这些协议也有不同层次、不同方面的漏洞，针对TCP/IP等协议的攻击非常多，在以下几个方面都有攻击的案例。

（1）网络应用层服务的安全隐患。例如，攻击者可以利用FTP、Login、Finger、Whois、WWW等服务来获取信息或取得权限。

（2）IP层通信的易欺骗性。由于TCP/IP本身的缺陷，IP层数据包是不需要认证的，攻击者可以假冒其他用户进行通信，此过程即IP欺骗。

（3）针对ARP的欺骗性。ARP是网络通信中非常重要的协议。基于ARP的工作原理，攻击者可以假冒网关，阻止用户上网，此过程即ARP欺骗。近一年来ARP攻击更与病毒结合在一起，破坏网络的连通性。

（4）局域网中，以太网协议的数据传输机制是广播发送，使系统和网络具有易被监视性。在网络上，黑客能用嗅探软件监听到口令和其他敏感信息。

3. 操作系统的漏洞

网络离不开操作系统，操作系统的安全性对网络安全同样有非常重要的影响，有很多网络攻击方法都是从寻找操作系统的缺陷入手的。操作系统的缺陷有以下几个方面。

（1）系统模型本身的缺陷。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来弥补。

（2）操作系统程序的源代码存在Bug（漏洞）。操作系统也是一个计算机程序，任何程序都会有Bug，操作系统也不会例外。例如，冲击波病毒针对的就是Windows操作系统的RPC缓冲区溢出漏洞。那些公布了源代码的操作系统所受到的威胁更大，黑客会分析其源代码，找到漏洞进行攻击。

（3）操作系统程序的配置不正确。许多操作系统的默认配置安全性很差，进行安全配置比较复杂，并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确地

配置这些功能，也会造成一些系统的安全缺陷。

Microsoft 公司在 2010 年发布了 106 个安全公告，修补了 247 个操作系统的漏洞，比 2009 年多 57 个。漏洞的大量出现和不断快速增加补丁是网络安全总体形势趋于严峻的重要原因之一。不仅仅操作系统存在这样的问题，其他应用系统也一样。例如，微软公司在 2010 年 12 月推出 17 款补丁，用于修复 Windows 操作系统、IE 浏览器、Office 软件等存在的 40 个安全漏洞。在我们实际的应用软件中，可能存在的安全漏洞更多。

4. 人为因素

许多公司和用户的网络安全意识薄弱、思想麻痹，这些管理上的人为因素也影响了安全。

1.1.3 网络安全的定义

国际标准化组织（International Organization for Standardization，ISO）引用 ISO 74982 文献中对安全的定义：安全就是最大程度地减少数据和资源被攻击的可能性。

《计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念："计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。"

从本质上讲，网络安全是指网络系统的硬件、软件和系统中的数据受到保护，不因偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

欧共体（欧洲共同体为欧盟前身）对信息安全给出如下定义："网络与信息安全可被理解为在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输的数据，以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。"

网络安全的具体含义会随着重视"角度"的变化而变化。例如，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、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说，希望对本地网络信息的访问、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，从而制止和防御网络黑客的攻击。从安全保密部门的角度来说，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、对国家造成巨大损失。从社会教育和意识形态的角度来说，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.1.4 网络安全的基本要素

网络安全的目的如图 1-4 所示：保障网络中的信息安全，防止非授权用户的进入，以及事后的安全审记。

图 1-4 网络安全的目的