Computer

计算机网络安全与防护

Network Security and Protection

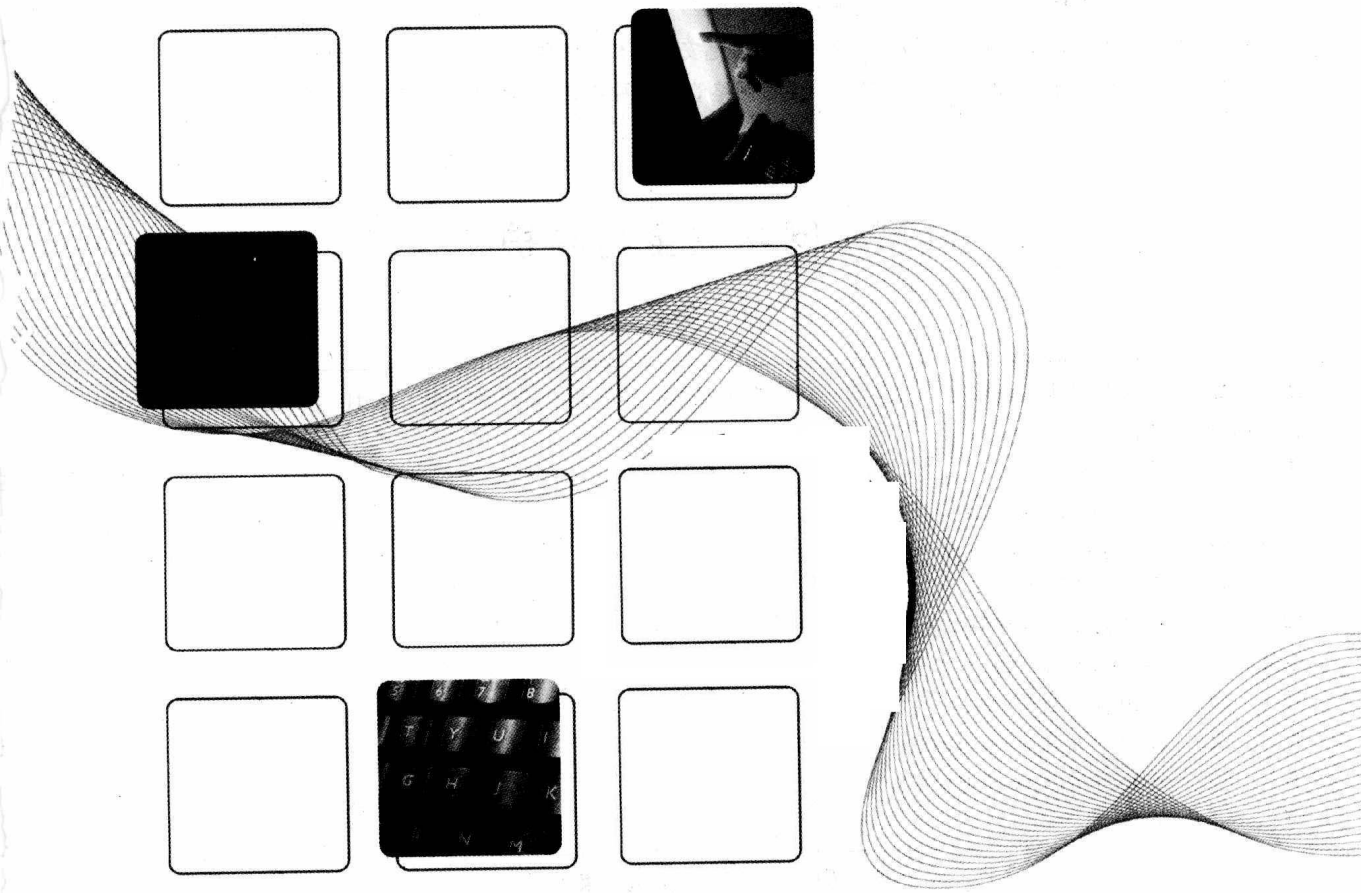
张 靖 编著

电子科技大学出版社

计算机网络安全与防护

Computer Network Security and Protection

张 靖 编著



电子科技大学出版社

图书在版编目（CIP）数据

计算机网络安全与防护 / 张靖编著. -- 成都：
电子科技大学出版社, 2010. 8
ISBN 978-7-5647-0591-6

Ⅰ. ①计… Ⅱ. ①张… Ⅲ. ①计算机网络－安全技术
Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2010）第 159255 号

内 容 提 要

本书共 16 章，主要内容有计算机网络安全概述、网络安全管理及技术基础、密码技术、数据备份和恢复、网络安全隔离、网络接入认证、无线网络安全、IPv6 安全问题、典型网络应用安全保障、系统安全防护、检测和恢复技术、网络安全风险分析和评估、信息系统安全保障等。本书面向应用，在强调相关基础知识的同时，阐述和介绍了网络安全管理和防护技术的基本原理、方法、措施以及案例，加强了理论和实践的结合。

本书既可供从事计算机网络、网络管理、信息安全及相关工作的专业人员学习、研究参考，也可作为理工专业高年级本科生、研究生学习网络管理、网络安全方面的教材或者参考书。

计算机网络安全与防护

张 靖 编著

出　　版： 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑： 周清芳
责任编辑： 周清芳
主　　页： www.uestcp.com.cn
电子邮箱： uestcp@uestcp.com.cn
发　　行： 新华书店经销
印　　刷： 成都蜀通印务有限责任公司
成品尺寸： 185mm×260mm　　**印张** 21　　**字数** 520 千字
版　　次： 2010 年 8 月第一版
印　　次： 2010 年 8 月第一次印刷
书　　号： ISBN 978-7-5647-0591-6
定　　价： 48.00 元

前　言

我国网民数量已经超过 3 亿，互联网用户数高居世界第一。同时，互联网普及率达到 22.6%，总带宽 625Gbps，IP 地址 1.8 亿个，手机上网用户 1.17 亿……数据大幅增长的背后是信息网络与国民经济的联系日益紧密，购物、交友、获取等信息都可通过网络进行，但随之而来的是网络与信息安全问题日益突出。

随着网络技术的不断发展和应用普及，网络受到破坏和攻击的行为日渐增多，一些系统和资源也越来越频繁地被侵入、修改、盗取等，在众多单位部门和普通百姓日益依赖网络时，却发现网络如此脆弱，发现网络安全的保障体系、运行机制、技术保障，甚至管理都有很多漏洞、缺陷，网络的安全管理和技术保障越来越得到重视，并已成为衡量一个信息系统是否完善、安全的重要标志。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论、管理等多种学科的综合性学科。有关网络管理、网络技术等的文献资料、书籍很多，涉及的专业知识面很广，也有相当的复杂程度。实际上，网络安全与人、设备、环境、政策、技术等因素相关，网络安全除了加强主动预防技术，还要增强评估、监测、恢复等手段。本书根据网络安全存在的问题和技术处理需要，把网络安全相关专业的管理、技术等知识内容比较系统地衔接起来，有利于读者学习、理解、掌握和进一步地深入实践和研究。

自 2001 年开始，作者为计算机科学与技术专业的本科生开设了《计算机网络》、《网络管理》、《网络安全》专业课，2005 年开始承担公安部、人事部信息网络安全专业技术人员继续教育培训《信息网络安全管理》、《信息网络安全技术》、《互联网信息内容安全管理》和《互联网上网服务营业场所安全管理》的授课，并担任主讲教师。作者一直负责校园网的建设、管理和研究工作，本书的内容编排以多年来授课为基础，并融合了工作经历和科研成果，本着“实用、完整、理论联系实际”的原则，与众多从事网络安全工作和研究的同仁一起分享自己的感受。

本书共分 16 章，第 1 章主要介绍网络安全的形势、网络安全概述以及网络攻击；第 2 章介绍网络安全的基本概念和网络攻击技术；第 3 章介绍加（解）密码基本原理和密码技术；第 4 章介绍数据备份和恢复的原理以及相关技术；第 5 章介绍网络管理的概念、功能、结构、协议等基本内容；第 6 章介绍网络安全的常见技术以及手段；第 7 章介绍网络隔离与安全交换，通过逻辑隔离或物理隔离技术，将网络分割成不同的通信域，以达到网络信息高度安全的目的；第 8 章介绍网络终端接入认证技术；第 9 章介绍典型网络应用的安全

技术以及保障措施；第 10 章介绍无线局域网络的安全；第 11 章介绍蜜罐技术原理和蜜网技术；第 12 章介绍 IPv6 出现的安全问题以及安全措施；第 13 章介绍信息系统的防护和检测、网络端口扫描和漏洞检测以及响应、恢复技术；第 14 章介绍安全风险分析评估、安全审计的概念和方法；第 15 章介绍信息系统安全保障概念、目标、体系、内容、策略等内容；第 16 章以校园网为例介绍了一个网络安全管理和技术保障的实例，重点介绍了校园网的主要安全内容、安全策略和安全保障技术、措施。

本书编著工作得到了四川机电职业技术学院刘松青老师和攀枝花学院杨晓为、周伟、张翔、张杰、冯霞等老师的大力帮助，他们对本书提出了很多宝贵的意见，在此特别致谢。

由于作者水平有限，时间仓促，书中不足之处甚至错误在所难免，恳请读者批评指正，作者表示衷心感谢。

张　靖

2010 年 6 月

目 录

第1章 概 述

1.1 网络安全形势

网络日益普及的今天，互联网已逐步成为人们生活和工作中必不可少的组成部分。网络涉及国家的政府、军事、文教等诸多领域。其中，存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息。通过网上的协同和交流，人的智能和计算机快速运行的能力汇集并融合起来，创造了新的社会生产力，交流、学习、医疗、消费、娱乐、安全感、安全环境、电子商务、网上购物等满足着人们的各种社会需要。然而，与此同时，网络社会与生俱来的不安全因素，如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等各种人为攻击也无时无刻不在威胁着网络的健康发展。基于网络的威胁潜伏在每一个角落。

互联网自21世纪初，在世界各国都得到了前所未有的发展，尤其在中国，可谓是突飞猛进。我们可以看到随着互联网的快速发展，虚拟与现实生活越来越难以割裂，政府、企业发展都与互联网的发展息息相关，个人的生活、工作也越来越依赖于计算机网络，互联网的发展给整个世界的发展带来了一次伟大的革命。人与人、国与国之间距离在不断缩小，从“地球村”到“世界是平的”一说，都意味着人类越来越意识到互联网的含义。越来越多的人发现，随着互联网的发展，他们能够找到更多的合作对象和竞争对手，地球上的各个知识中心都将被统一到了单一的全球网络中。但不幸的是，随着网络发展而衍生出来的网络安全问题也时刻威胁着“地球村”的“村民”们，例如计算机病毒、流氓软件、间谍软件等。由于Internet的开放性和超越组织与无国界等特点，使它在安全性上也同样存在着开放性和无国界性，因此，给网民带来了严重的安全隐患问题。那么，何为网络安全威胁，网络安全威胁到底会给社会带来怎样的后果呢？

网络安全关系政治、经济、军事、科技和文化等国家信息安全。据有关报道，2000 年美国发生网上恐怖事件，短短几天内电子商务网站、股市网站等损失达 12 亿美元；2001 年日本东京国际机场航管由于红色代码病毒导致的系统失灵，影响巨大，造成几百架飞机无法起降、千人行程受阻；2003 年，美国银行的 ATM 网络遭到入侵，损失惨重，2005 年的 4 000 多万张卡用户信息被盗，并被植入特洛伊木马，假冒消费，由此导致用户巨大的财产损失，这是美国最大的窃密事件……由于这些事件的不断发生，人们对网络安全的认识也在不断深入，对信息安全防护能力、隐患发现能力、网络应急反应能力以及对抗能力的要求也在不断提升。因此，网络的安全问题就显得更加关键和重要。

据统计，在全球范围内，由于信息系统的脆弱性而导致的经济损失，每年达数亿美元，并且呈逐年上升的趋势。据美国《金融时报》报道，现在平均每 20 秒就发生一次入侵计算

机网络的事件；超过1/3的互联网防火墙被攻破。中国工商银行、中国银行、中国建设银行等金融机构先后成为黑客们模仿的对象，设计了类似的网页，通过网络钓鱼的形式获取利益，而这一现象正在以每个月73%的数字增长，使很多用户对网络交易的信心大减。在历史上，由于网络的不安全而给军队带来损失的案例也是不计其数。海湾战争前，美军将带有“病毒”的计算机通过法国卖给伊拉克军队。海湾战争初期，美军就对伊军实施了“病毒”战，使其防空指挥控制系统失灵，指挥文书只能靠汽车传递，在整个战争中都处于被动挨打的局面。同样，网络的不安全也影响了人们的生活，对构建和谐社会产生了阻碍。尊重隐私权是每个公民应有的权利，但侵犯信息隐私权的事件在网络上大量存在。网络一旦遭到非法攻击，网络操作系统中的用户全称、电话号码和办公地点等信息，就可能被复制或篡改，网民的基本信息就得不到保障。

1.2 我国网络安全形势

我国互联网基础设施和重要信息系统整体上运行基本正常，没有出现造成严重影响或后果的大规模网络安全事件。但是，网络攻击的频次、种类和复杂性均比往年大幅增加，遭入侵和受控计算机数量增多，潜在威胁和攻击力继续增长，信息数据安全问题日益突出，网络安全形势依旧严峻。

2008年国家互联网应急中心（CNCERT）接收和自主监测的各种网络安全事件数量与2007年上半年同期相比有较为显著的增加。其中，垃圾邮件事件和网页恶意代码事件增长较快，网页恶意代码同比增长近一倍；网页篡改事件和网络仿冒事件也有大幅增长，同比增长分别是23.7%和38%，其中，涉及国内政府机构和重要信息系统部门的网页篡改事件、涉及国内外商业机构的网络仿冒事件是2008年上半年事件监测和处置的重点。

网页篡改事件特别是我国大陆地区政府网页被篡改事件呈现大幅增长趋势。统计显示，2008年上半年我国大陆地区被篡改的.gov.cn网站数量比2007年上半年增加41%，共计2 242个，占被篡改网站总数的比例达到7%，而.gov.cn域名仅占.cn域名总数的2.3%，这说明.gov.cn网站遭受黑客攻击的可能性相对较高。2008年5月1日，我国颁布施行《政府信息公开条例》，该《条例》的推行对政府信息化建设提出了新的要求，同时也对电子政务信息系统的网络安全提出更高的要求。由于政府网站整体安全水平较低，往往是黑客攻击的重要目标，因此，作为政府对外形象的窗口、发布权威信息和与公众开放交流的平台，电子政务信息系统的网络安全管理成为各级部门必须高度重视的问题。

我国大陆地区感染木马和僵尸网络的主机数量巨大。据CNCERT的监测数据显示，2008年前5个月监测到的感染木马和僵尸网络的主机数量缓慢波动上涨，但在6月份出现跳跃式增长。这一现象跟CNCERT加强监测力度和扩大监测范围有关，但更令人担忧的原因则是攻击者似乎在北京奥运会前夕加紧活动，图谋通过网络攻击干扰数字奥运的顺利举行。

造成木马和僵尸网络产生和扩散的一大途径是恶意代码的肆虐传播。2008年上半年，CNCERT通过技术平台共捕获约90万个恶意代码，比2007年同期增长62.5%。其中，新的恶意代码样本8.9万个，与2007年同期基本相近；通过国内外合作渠道接收到恶意代码样本49.6万个。综合各种来源数据并从中去掉重复的恶意代码样本，2008年上半年实际新增恶意代码样本数达52.9万个。数据合作方包括国内外主要的反病毒厂商、CERT 组织和安全机构。