计算机系列教材

计算机系统安全

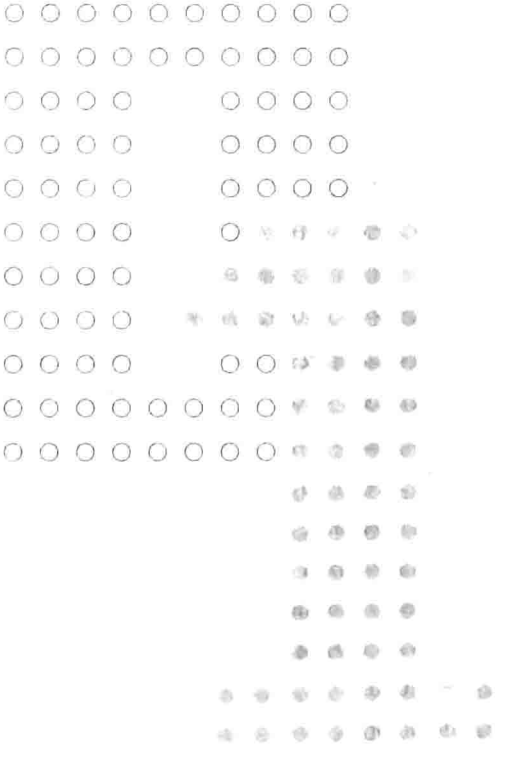
李章兵 编著

清华大学出版社

计算机系列教材

李章兵 编著

计算机系统安全



清华大学出版社
北京

内 容 简 介

计算机系统安全是信息安全的关键内容之一，它已成为计算机信息系统的核心技术，也是网络安全的重要基础和补充。本书是作者在长期信息安全教学和科研的基础上编写而成的，书中系统地阐述计算机系统安全的理论、技术和方法，全面讲述计算机系统安全基础（信息系统及其威胁，安全体系结构与模型、标准）、恶意代码、数据加密与保护、访问控制、信息认证技术、操作系统安全、软件保护与数字版权管理、黑客、数据库安全、防火墙、入侵检测与防御、数字取证技术等方面的内容，涵盖了计算机技术与密码学理论。

本书概念清晰，表达深入浅出，内容新颖翔实，重点突出，理论与实践相结合，实用性强，易学易懂。

本书可作为信息安全、计算机、网络工程等相关专业的高年级本科生或研究生教材，也可供相关专业的教学、科研和工程从业人员参考。

图书在版编目(CIP)数据

计算机系统安全/李章兵编著. --北京：清华大学出版社，2014
计算机系列教材
ISBN 978-7-302-36552-5

Ⅰ. ①计… Ⅱ. ①李… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 112343 号

责任编辑：张　玥　顾　冰
封面设计：常雪影
责任校对：时翠兰
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**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
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：清华大学印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：31.75　　**字　　数**：773 千字
版　　次：2014 年 9 月第 1 版　　**印　　次**：2014 年 9 月第1 次印刷
印　　数：1～2000
定　　价：59.00 元

产品编号：058756-01

《计算机系统安全》 前言

计算机在政治、军事、金融、商业等部门的应用越来越广泛，社会对计算机系统的依赖也越来越大，安全可靠的计算机系统应用已经成为支撑国民经济、关键性基础设施以及国防的支柱，信息安全在各国都受到了前所未有的重视。“信息安全＋国土安全＝国家安全”正逐渐得到社会的认同。我国成立了国家计算机网络应急处理协调中心 CNCERT(http://www.cert.org.cn)、国家计算机病毒应急处理中心 CVERC(http://www.antivirus-china.org.cn)、国家计算机网络入侵防范中心(http://www.nipc.org.cn)、信息安全国家重点实验室(http://www.is.ac.cn)等一批国家级信息安全机构。许多高校及科研院所开设了信息安全专业以及“信息安全导论”、“计算机系统安全”等相关课程。

计算机系统安全是信息安全的关键内容之一，它已成为计算机信息系统的核心技术，也是网络安全的重要基础和补充。学习计算机系统安全，密码学是理论基础，恶意代码和黑客是重要的威胁源，必须掌握其原理和技术，操作系统安全、数据库安全、软件保护和数字版权管理是核心，访问控制、防火墙、入侵检测与防御以及数字取证是实现计算机系统安全的重要技术和保障。

本教材从计算机系统安全的角度出发，结合多年来“信息安全导论”的教学经验，根据教学需要不断充实改进内容，突出了计算机系统安全的概念、原理、技术和应用实例，反映了信息安全的最新进展。第 1 章介绍计算机信息系统与所面临的威胁、计算机系统安全概念、体系结构、安全模型、安全等级标准、信息资产风险评估等基础知识。第 2 章介绍计算机病毒、蠕虫、后门、木马、僵尸网络、恶意移动代码等恶意代码的原理和防范，并对反病毒原理与技术加以介绍。第 3 章介绍密码学基础知识、对称密码、公钥密码、密钥管理、新型密码、信息隐藏与水印、数据与版权保护等。第 4 章详细介绍认证需要的杂凑函数、数字签名以及消息认证、身份认证和实用的认证系统和协议。第 5 章介绍访问控制的模型、策略和实现，以及授权与审计跟踪等知识。第 6 章从进程、内存、文件系统和应用程序的角度，介绍操作系统的安全、安全 OS 的设计理论、Windows 安全、UNIX 安全以及设备安全等。第 7 章介绍软件的保护、破解和逆向的原理和技术，以及数字版权管理(DRM)技术。第 8 章详细介绍黑客及其信息收集类、入侵类、欺骗类、拒绝服务类的攻击，以及木马植入和网络钓鱼技术。第 9 章简介数据库系统及其安全概念，阐述数据库的管理系统安全、数据安全(关联推理和隐私保护)和应用系统安全等原理和技术。第 10 章介绍防火墙的基本知识、体系结构、过滤原理与技术、网闸以及防火墙的配置与管理等。第 11 章介绍入侵检测的概念、原理、技术、实现和蜜罐技术以及 IDS 的部署和产品，并介绍和比较了入侵防御系统原理和技术。第 12 章从计算机犯罪和电子证据概念入手，介绍计算机数字取证的原理和技术、证据分析以及反取证技术等。

本书概念清晰，理论和实践并重，重点突出。偏重实践的书缺乏理论深度，而偏重理论的书很难提高学生进一步学习的兴趣。本书注重从原理和实践双重角度阐明计算机系统安全的知识，教会学生一些处理问题的原理和具体方法并用于实践中，帮助加深对比较抽象和枯燥的理论的理解。

本书选材合理，内容翔实、全面、新颖、深入浅出。重点阐述恶意代码、访问控制、信息认证、操作系统、数据库、软件保护与数字版权等计算机系统安全的基本概念，特别侧重阐述恶意代码这把“威胁之剑”的使用和铸造、黑客攻击等的原理和技术。在防御方面阐述防火墙、入侵检测、数字取证等理论和技术知识。密码学作为信息安全的基础，本书阐述其基本理论，摒弃过时和不过关的内容。总之，本书全面反映了近几年计算机系统安全领域的新发展。

作为“网络安全”的基础，交叉内容较少。密码学、黑客、防火墙和入侵检测等理论和技术也是计算机系统安全需要的知识，但侧重于方法、部署和管理，需要的网络专业知识较少。对于开设了密码学的学生，第3、4章的部分内容可以选择讲授。

本书参考了大量的RFC文档(http://www.ietf.org/rfc.html)、美国国家标准技术研究所出版物(http://csrc.Nist.Gov/publications)，也希望读者在学习的过程中查阅参考。

虽然经过多次修改，鉴于水平有限，书中错漏难免，欢迎读者批评指正。本书参考了大量相关书籍，引用了许多来自于互联网的资料和PPT，但多数资料没有版权信息，无法一一列在参考文献中，敬请作者谅解。

本书不仅适合信息安全专业的本科高年级学生学习，也适合计算机相关专业的其他本科学生和工程技术人员学习和参考，可以作为“信息安全导论”、“信息安全基础”、“计算机系统安全”等相关课程的教材。

本书的编写过程受到湖南省科技计划(2011FJ4300、2012FJ3047)和湖南省教育厅科研项目(11C0533)的资助。感谢北京邮电大学杨义先教授、武汉大学彭国军、王丽娜教授在信息安全领域给予的指导和支持。感谢湖南科技大学计算机科学与工程学院徐建波教授、知识处理与网络化制造、湖南省重点实验室刘建勋教授的支持，感谢钟小勇、汪丰兰、娄宇、许梁茜、李佳、宋佳静、符婷、赖朝刚等人的资料整理和绘图。感谢清华大学出版社对本书出版的支持与帮助。

作　者

2014.2

FOREWORD

《计算机系统安全》目录

第1章　计算机系统安全概述

1.1　信息系统与信息安全

1.1.1　信息化及信息系统

1. 信息与信息化

“信息”一词在英文、法文、德文、西班牙文中均是“information”，日文中为“情报”，我国台湾称之为“资讯”，我国古代用的是“消息”。20世纪40年代，香农(C. E. Shannon)给出了信息的明确数学定义：信息是用以消除随机不确定性的东西(信息是肯定性的确认；确定性的增加)，并提出信息量的概念和信息熵的计算方法，从而奠定了信息论的基础。这一定义被人们视为经典性定义并加以引用。

控制论创始人维纳(Norbert Wiener)认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”。它也被作为经典性定义加以引用。我国著名的信息学专家钟义信教授认为“信息是事物存在方式或运动状态，以这种方式或状态直接或间接的表述”。美国信息管理专家霍顿(F. W. Horton)给信息下的定义是：“信息是为了满足用户决策的需要而经过加工处理的数据。”简单地说，信息是经过加工的数据，或者说信息是数据处理的结果。

根据近年来人们对信息的研究成果，科学的信息概念可以概括为：信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

信息是资源和财富。信息化的程度已经成为衡量一个国家或企业综合技术水平、综合能力的主要标志。从全球范围来看，发展信息技术和发展信息产业也是当今竞争的一个制高点。信息技术和信息产业正在改变人们传统的生产、经营和生活方式，信息已成为社会发展的重要战略资源。

林毅夫等指出：“所谓信息化，是指建立在IT产业发展与IT在社会经济各部门扩散的基础之上，运用IT改造传统的经济、社会结构的过程”。

信息化在改变社会、促进发展的同时，给国家的安全也带来了挑战，常规武器、核武器等离开了信息的精确制导，也就变成了瞎子，因此现代战争中出现了争夺信息控制权的信息战。下面是一些名人对信息化的评价。

美国著名未来学家阿尔温·托尔勒：“谁掌握了信息，控制了网络，谁将拥有整个世界。”

美国前总统克林顿：“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

江泽民：“信息革命是人类第三次生产力的革命，四个现代化，哪一化也离不开信息化。”