高等学校计算机科学与技术教材

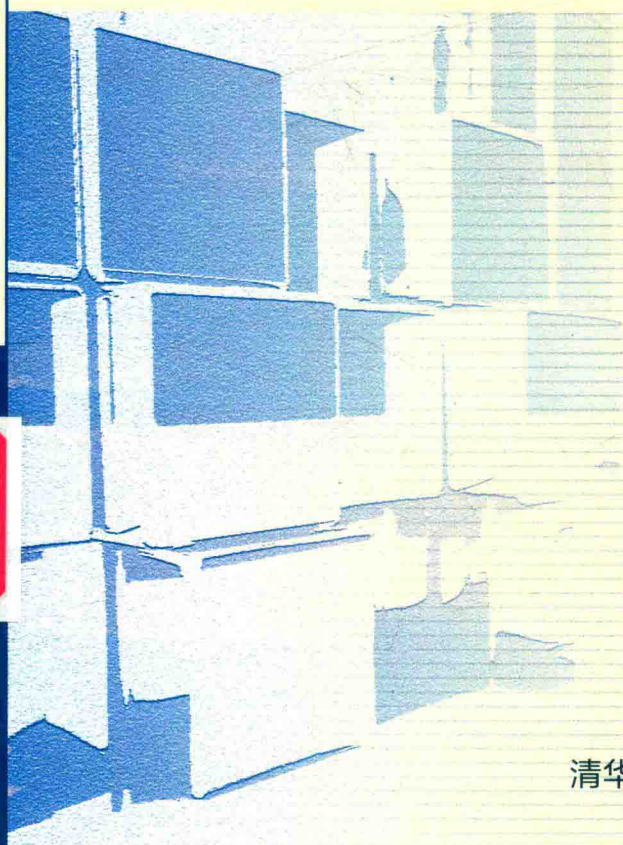
计算机网络安全教程

（第3版）

COMPUTER Science and Technology

□ 石志国　尹 浩　臧鸿雁　编著

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精练，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

计算机网络安全教程

（第3版）

石志国　尹　浩　臧鸿雁　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

第 3 版在第 2 版的基础上参考了很多读者的意见，做了大量修整，使之更加适合高校教学和自学的需要。本书利用大量的实例讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起，适量增加了理论部分的分量，同时配备了实验指导书。

全书从网络安全体系上分成四部分。第一部分：计算机网络安全基础，介绍网络安全的基本概念、实验环境配置、网络安全协议基础及网络安全编程基础。第二部分：网络安全攻击技术，详细介绍了攻击技术“五部曲”及恶意代码的原理和实现。第三部分：网络安全防御技术，操作系统安全相关原理、加密与解密技术的应用、防火墙、入侵检测技术、VPN 技术，以及 IP 和 Web 安全相关理论。第四部分：网络安全综合解决方案，从工程的角度介绍了网络安全工程方案的编写。

本书可以作为高校及各类培训机构相关课程的教材或者参考书。本书涉及的源代码、所有软件和授课幻灯片等教学支持信息，可以从出版社网站 http://www.bjtup.com.cn 下载。

图书在版编目（CIP）数据

计算机网络安全教程 / 石志国，尹浩，臧鸿雁编著. —3 版. —北京：北京交通大学出版社：清华大学出版社，2019.10

ISBN 978-7-5121-3929-9

Ⅰ. ①计… Ⅱ. ①石… ②尹… ③臧… 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（2019）第 209679 号

计算机网络安全教程

JISUANJI WANGLUO ANQUAN JIAOCHENG

责任编辑：谭文芳

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://www.bjtup.com.cn

印 刷 者：北京鑫海金澳胶印有限公司

经　　销：全国新华书店

开　　本：185 mm×260 mm　印张：22.25　字数：566 千字

版　　次：2019 年 10 月第 3 版　2019 年 10 月第 1 次印刷

书　　号：ISBN 978-7-5121-3929-9/TP・880

印　　数：1～5 000 册　定价：49.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。

投诉电话：010-51686043，51686008；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

第 3 版在第 2 版的基础上，参考了很多读者的意见，做了大量修整和扩充，使之更加适合高校教学和自学的需要。本书利用大量的实例讲解知识点，将安全理论、安全工具与安全编程三方面内容有机地结合到一起，每章最后都配有大量的习题，用来检查教学和学习的效果。

与之前版本的比较

2004 年初，《计算机网络安全教程》（第 1 版）出版，目的是解决网络安全技术教学的迫切需要。该版综合了作者在北京大学计算机研究所部分研究内容、清华大学计算机系部分教学内容，以及网络信息安全国际认证考试的部分内容，在第 1 版的写作过程中还得到了当时三院院士王选老师的支持和指导。本书出版以来，受到了广大读者，特别是高校师生的认可和欢迎，同时，很多读者也提出了很多中肯的批评和改进意见。当前，网络安全是计算机相关领域中的一门重要学科，很多高校和研究机构都设置了网络信息安全本科专业，以及网络信息安全方向的硕士点和博士点。

2007 年初对本书第 1 版做了一次全面的更新，出版了《计算机网络安全教程》修订版，在保证第 1 版整体结构的情况下，对内容进行了全面的扩充和修正，一个主要的特点是理论性的增强，主要做了如下 6 方面的调整。

（1）增强了书的理论性并全面阐述了网络安全两个重要的概念：恶意代码和 Web 安全。添加了两章，将全书扩充为 12 章。分别为：第 7 章恶意代码和第 11 章 IP 安全与 Web 安全。

（2）修正了部分内容不规范，图表不清楚的问题。

（3）全面扩充了拒绝服务攻击及分布式拒绝服务攻击的分类和原理。

（4）增加了安全操作系统的机制与原理。

（5）增加了数字签名、数字水印和公钥基础设施 PKI 的相关内容。

（6）为了检查教学及自学的效果，每章都重新设计了选择题、填空题以及问答题，并在书后给出选择题和填空题的参考答案。

2010 年，通过网络向读者征集了很多修改意见，并进行了修改，出版了本书第 2 版。针对读者意见较多的恶意代码一章，进行重写，其他章节同时进行了修改和完善。在没有增加篇幅的前提下，主要做了如下 4 个方面的调整。

（1）重新编写恶意代码这一章，重点介绍了常见的 PE 病毒、脚本病毒、U 盘病毒，以及网络蠕虫的原理与实现，并用程序展示了各种病毒的传染方法。

（2）修正了部分内容不规范的问题。例如：RSA 算法中，公钥是 e，私钥是 d。这是一个大家都默认的规则，而且在教材中后面是 e，d，前面是 a，b，内容不严谨；等等。

（3）增加了部分原理介绍。例如：端口扫描的原理、克隆账户的原理，以及操作系统漏洞的原理等。

（4）因为学习过程中还是以实验为主，本版配套了实验指导，并设计了 10 个实验，同时优化了相关的配套资料。

2019 年，针对书中部分陈旧的内容，在原有内容上进行了修改和补正，主要做了如下调整。

（1）更新了近期的网络安全事件及网络立法情况。

（2）修改 OSI 参考模型和 TCP/IP 参考模型比较；修改部分 IP 协议描述；增加 IPv6 协议发展情况。

（3）完善 Windows 窗口概念；编程步骤、编程工具介绍。

（4）补充黑客和骇客对比，完善“黑客守则十三条”，补充后门和网络安全扫描概述。

（5）完善社会工程学攻击的主要方式，SMB 协议版本，WebDAV 远程溢出攻击手段，增加 DDOSIM-Layer 攻击软件。

（6）tlntadmn 命令描述，木马与后门对比。

（7）补充恶意代码历史，恶意代码传播手段，宏病毒描述。

（8）UNIX 与 Linux 系统补充。

（9）密码学发展近况，RSA 加密技术补充，数字水印特性。

（10）防火墙功能及局限性补充，防火墙分类，入侵检测完善。

（11）IPSec 协议完善，VPN 技术修改，OpenSSL 漏洞。

本书结构

每一章前面设计了“本章要点”，因为每一章内容都比较庞杂，所以要注意本章要点，重点掌握提及的内容。每一章后面设计了适量的习题，主要是针对本章重点、难点进行训练。附录提供了选择题和填空题的答案，可以对照检查自己的学习效果。

本书导读

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、信息论等多种学科的综合性科学。全书从三个角度介绍计算机网络安全技术：计算机网络安全理论、网络安全攻防工具和网络安全编程，这三方面内容均来自实际的工程以及课堂的实践，并通过网络安全攻防体系结合在一起。从网络安全攻防体系上，全书分成 4 部分，共 12 章。

第 1 部分：网络安全基础

第 1 章　网络安全概述与环境配置：介绍信息安全和网络安全的研究体系、研究网络安全的意义、评价网络安全的标准及实验环境的配置。

第 2 章　网络安全协议基础：介绍 OSI 参考模型和 TCP/IP 协议组，实际分析 IP，TCP，UDP，ICMP 协议的结构，以及其工作原理、网络服务和网络命令。

第 3 章　网络安全编程基础：介绍网络安全编程的基础知识，C 和 C++的几种编程模式，以及网络安全编程的常用技术，如 Socket 编程、注册表编程和驻留编程等。

第 2 部分：网络攻击技术

第 4 章　网络扫描与网络监听：介绍黑客和黑客攻击的基本概念，如何利用工具实现网络踩点、网络扫描和网络监听。

第 5 章　网络入侵：介绍常用的网络入侵技术，如社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

第 6 章　网络后门与网络隐身：介绍网络后门和木马的基本概念，并利用四种方法实现网络后门；介绍利用工具实现网络跳板和网络隐身。

第 7 章　恶意代码：介绍恶意代码的发展史，恶意代码长期存在的原因；介绍常见恶意代码的原理，并用程序实现常见的 PE 病毒、脚本病毒、U 盘病毒等。

第 3 部分：网络防御技术

第 8 章　操作系统安全基础：介绍 UNIX、Linux 和 Windows 操作系统的特点，着重介绍安全操作系统的原理，介绍 Windows 操作系统的安全配置方案。

第 9 章　密码学与信息加密：介绍密码学的基本概念，DES 加密算法的概念及如何利用程序实现，RSA 加密算法的概念及实现算法，PGP 加密的原理及实现。

第 10 章　防火墙与入侵检测：介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集；介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵检测。

第 11 章　IP 安全与 Web 安全：介绍 IPSec 的必要性，IPSec 中的 AH 协议和 ESP 协议，密钥交换协议 IKE 及 VPN 的解决方案等。

第 4 部分：网络安全综合解决方案

第 12 章　网络安全方案设计：从网络安全工程的角度介绍网络安全方案编写的注意点及评价标准。

致谢

本书出版 10 多年来，首先要感谢很多老师和同学提出了批评和改进意见，这些意见非常贴切和真诚，我也会尽全力通过网页和电子邮件等方式为读者提供更为周到的服务。其次要感谢很多在网上提出修改意见的读者，感谢他们在提出意见的同时，还勇敢地在网上留下自己的真实联系方式。

在编写过程中，得到众多老师的指导和帮助，感谢众多专家为本书提供了大量详尽的编程资料，并为本书解决了很多编程方面的问题。尤其要感谢的是北京交通大学出版社的编辑谭文芳老师，10 多年来她稳定的支持是本书能及时更新的关键。

图书支持

本书可以作为高校及各类培训机构相关课程的教材或者教学参考书，也可以作为网络

第 3 部分 网络防御技术

第 4 部分 网络安全综合解决方案

第 1 部分

网络安全基础

1

本部分包括 3 章：

☑ **第 1 章　网络安全概述与环境配置**

☑ **第 2 章　网络安全协议基础**

☑ **第 3 章　网络安全编程基础**

所谓教育，是忘却了在校学的全部内容之后剩下的本领。

——阿尔伯特·爱因斯坦（Albert Einstein）

对一切来说，只有热爱才是最好的老师，它远远胜过责任感。

——阿尔伯特·爱因斯坦（Albert Einstein）

不是所有能计算的都有价值，不是所有有价值的都能被计算。

——阿尔伯特·爱因斯坦（Albert Einstein）

第 1 章　网络安全概述与环境配置

本章要点

- 介绍网络安全研究的体系、研究网络安全的必要性
- 研究网络安全的社会意义，目前与计算机网络安全有关的法规
- 评价一个系统或者应用软件的安全等级
- 为了能顺利完成本书介绍的各种实验，最后较为详细地介绍实验环境的配置

1.1　信息安全概述

网络安全是信息安全学科的重要组成部分。信息安全是一门交叉学科，广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

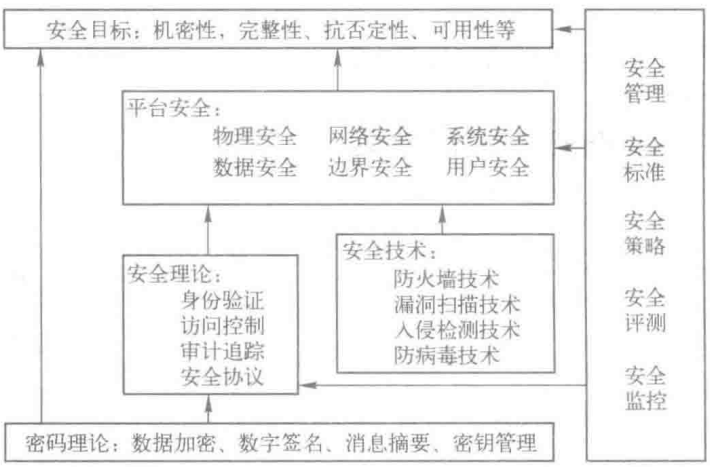


图 1-1　信息安全研究内容及关系

信息安全研究大致可以分为基础理论研究、应用技术研究、安全管理研究等。基础研究包括密码研究、安全理论研究；应用技术研究则包括安全实现技术、安全平台技术研究；安全管理研究包括安全标准、安全策略、安全测评等。

1.1.1　信息安全研究层次

信息安全大致从总体上可以分成 5 个层次：安全的密码算法、安全协议、网络安全、系统安全和应用安全，层次结构如图 1-2 所示。

近年来，随着 TPM（trusted platform module，可信平台模块）技术的发展，硬件系统

和软件系统协作的安全性，逐步成为信息安全领域的研究热点。

图 1-2　信息安全的层次

1.1.2　信息安全的基本要求

信息安全的目标是保护信息的机密性、完整性、抗否认性和可用性，也有的观点认为是机密性、完整性和可用性，即 CIA（confidentiality integrity availability）。

1．机密性 confidentiality

机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

2．完整性 integrity

完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

信息的完整性包括以下两个方面。

（1）数据完整性：数据没有被未授权篡改或者损坏。

（2）系统完整性：系统未被非法操纵，按既定的目标运行。

3．可用性 availability

可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。

除了这三方面的要求，信息还要求真实性，即个体身份的认证，适用于用户、进程、系统等；要求可说明性，即确保个体的活动可被跟踪；要求可靠性，即行为和结果的可靠性、一致性。

1.1.3　信息安全的发展

20 世纪 60 年代倡导通信保密措施，20 世纪 60 年代到 70 年代，逐步推行计算机安全，20 世纪 80 年代到 90 年代信息安全概念被广泛提出，20 世纪 90 年代以后，开始倡导信息保障（information assurance，IA）。信息保障的核心思想是对系统或者数据的 4 个方面的要求：保护（protect），检测（detect），反应（react）和恢复（restore），结构如图 1-3 所示。

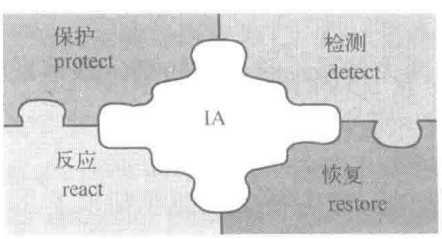


图 1-3　信息保障的结构

利用 4 个单词首字母表示为：PDRR，并称为 PDRR 保障体系。其中：

保护（protect）指采用可能采取的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。