□ 信息安全系列丛书

计算机网络安全的理论与实践

（第2版）

【美】 王 杰

Computer Network Security
Theory and Practice

高等教育出版社
HIGHER EDUCATION PRESS

□ 信息安全系列丛书

计算机网络安全的理论与实践

（第2版）

【美】 王 杰

Computer Network Security Theory and Practice

JISUANJI WANGLUO ANQUAN DE LILUN YU SHIJIAN

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

计算机网络安全的理论与实践/(美)王杰编著. —2 版. —北京：高等教育出版社，2011.6

ISBN 978-7-04-031798-5

Ⅰ.①计… Ⅱ.①王… 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（2011）第 083745 号

策划编辑 刘 英　　责任编辑 刘 英　　封面设计 张雨微　　版式设计 范晓红

责任校对 金 辉　　责任印制 张泽业

出版发行 高等教育出版社
社　　址 北京市西城区德外大街 4 号
邮政编码 100120
印　　刷 三河市华润印刷有限公司
开　　本 787×1092　1/16
印　　张 24.25
字　　数 500 000
购书热线 010-58581118
咨询电话 400-810-0598

网　　址 http://www.hep.edu.cn
　　http://www.hep.com.cn
网上订购 http://www.landraco.com
　　http://www.landraco.com.cn

版　　次 2006 年 10 月第 1 版
　　2011 年 6 月第 2 版
印　　次 2011 年 6 月第 1 次印刷
定　　价 49.00 元

物 料 号 31798-00

第 2 版前言

本书第 2 版是在第 1 版和英文版的基础上修订和补充而成的。它在保持第 1 版的结构和指导思想下增加了以下内容：彩虹表及其在字典攻击中的应用，RC4 序列密码安全性讨论，中国余数定理及其在证明 RSA 算法正确性的应用，漩涡散列函数，OCB 操作模式，无线网状网安全问题，Linux 操作系统中的防火墙设置，微软 Windows 便携式执行格式病毒传播原理及第二代万维网技术的一些安全问题，行为分析入侵检测技术和 Honeynet 计划。第 2 版还充实了第 1 版中的部分章节，包括电子邮件安全协议、无线局域网安全协议和无线个人网安全协议。为便于自学，第 2 版在书后还给出了部分习题的解答。此外，第 2 版对某些英语名词的翻译作了一些修改，比如 phishing 在第 1 版译为钓取，而译为网络钓鱼更为贴切。

第 2 版共分九章。

第 1 章介绍网络安全的概貌。首先讨论网络安全的任务，综述常见的网络攻击类型和防范措施，然后讨论攻击者的分类及定义网络安全模型。

第 2 章介绍对称密钥加密算法和密钥生成算法。首先讨论加密算法的设计要求，介绍 Feistel 分组密码结构，DES 和 AES 标准分组密码加密算法，RC4 序列密码加密算法和讨论它们的完全性，然后介绍分组密码使用模式及密钥生成算法。

第 3 章介绍公钥密码体系和密钥管理方法。首先讨论公钥密码体系的指导思想，介绍 Diffie-Hellman 密钥交换体系，RSA公钥密码体系和椭圆曲线公钥密码体系，然后介绍密钥传递和管理方法。

第 4 章介绍数据认证方法。首先讨论安全散列函数的设计要求，介绍散列函数结构，SHA-512 散列函数，漩涡散列函数，信息认证代码算法，HMAC 算法模式，OCB 操作模式和生日攻击，然后介绍数字签名标准，双签名协议和盲签协议。

第 5 章介绍常用的网络安全协议。首先讨论在网络体系各层配置密码算法的优缺点，介绍公钥基础设施，然后介绍网络层 IPsec 协议、传输层 SSL/TLS 协议、应用层电子邮件安全协议、Kerberos 身份认证协议及安全外壳协议。

第 6 章介绍设置在数据链路层的无线网安全协议。首先介绍无线局域网体系结构，有线隐私等价协议的安全问题和改进后的网络安全存取协议，然后介绍无线个人网蓝牙安全协议，并讨论无线网际网的安全问题。

第 7 章介绍网络周边安全体系。首先讨论防火墙的设计思想，介绍网络层数据包过滤、传输层线路网关、应用层代理服务器和堡垒主机等防火墙技术，然后介绍防火墙设置方案，网址转换技术和在 Linux 操作系统中设置防火墙的基本方法。

第 8 章介绍抗恶意软件的技术。首先讨论计算机病毒和病毒分类，介绍病毒、蠕虫和特洛伊木马传播原理，然后介绍服务阻断攻击，万维网安全性及抗恶意软件方法。

第 9 章介绍入侵检测技术。首先讨论入侵检测的基本思想，介绍网检系统、机检系统、混合系统、特征检测、行为分析和数据挖掘等检测技术，然后介绍诱饵体系。

附录 A 给出部分习题的解答，并特别在第 6 章的习题解答中介绍了一个如何破译无线局域网 WEP 安全协议加密算法的方法，并给出了程序的源代码。

第 2 版的结构与英文版基本相同。英文版的写作得到许多同行的建议和帮助，特别是 Gordan College 的 Stephen Brinton 教授审阅了英文版初稿的第 1~5 章和第 7~8 章，麻省大学罗威尔分校陈冠岭教授审阅了第 6 章，付新文教授提供了不少相关资料和建议，美国银行 (Bank of America) 网络安全工程师 Jared Karro 审阅了全部章节，Worcester Polytechnic Institute 楼文菁教授审阅了第 1~2 章和第 6 章。麻省大学罗威尔分校部分博士研究生和硕士研究生亦对英文版和中文第 2 版的写作提供了帮助，他们是 (按英文和拼音姓氏为序): Anthony Kolodziej、Blake Skinner、Bora Seng、David Einstein、Hengky Susanto、Jeff Brown、Karen Uttecht、Michael Court、Nathaniel Tuck、Ryan Buckley、William Brown、杜春燕、方正、侯强、李楠、李优、刘忠丽、潘娴、杨杰、袁旭。此外，Stephen Brinton、方正、潘娴、杨杰协助提供了习题解答。作者谨在此致以诚挚的谢意。

感谢高等教育出版社编辑刘英博士对本书的编辑加工。

作者在 2008 年秋季和 2009 年秋季用本书英文版给本系研究生讲授计算机网络安全课程，授课用的 PPT 幻灯片可在 `http://www.cs.uml.edu/~wang/NetSec` 网页上找到。

作者在授课的基础上对本书作了进一步修订。尽管如此，本书不妥之处在所难免，恳请读者及采用本书的教师发现错误后通知作者。来信和建议请寄至作者的电子信箱: wang@cs.uml.edu。

王 杰 (J. Wang)，美国麻省大学罗威尔分校

2011 年 1 月

第 1 版前言

网络安全是计算机科学的新分支，也是信息产业的新领域。它的产生源于网络通信的保密需要，它的发展得益于人们为应对侵犯网络通信和连网计算机系统的各种攻击所做出的锲而不舍的努力。随着互联网应用的深入和普及，如何不断地采取更有效的安全措施保护网络通信内容不被窃取、篡改和伪造以及保护连网计算机系统免受侵扰已变得至关重要。除军事和金融通信以外，网络安全如今已成为电子商务、信息管理及资源共享等领域不可缺少的工具和保障，因而也越来越受到政府、商业及家庭计算机用户的重视。毫无疑问，网络安全将继续成为计算机科学研究与应用中一个举足轻重的领域。

互联网是在有线电话网的基础上发展起来的，由于当初在设计互联网通信协议时忽视了安全因素，导致互联网通信存在许多本来可以避免的缺陷和漏洞。为了解决互联网技术中的一系列问题，包括网络安全问题，美国国家科学基金会已号召研究人员探索和开发新一代互联网技术，研究互联网如果从零开始，应该有怎样的体系结构才能更好地适应今后的发展并解决现有的网络安全问题。无论结果如何，维护网络安全的努力将是持续不断的，原因包括以下几点：第一，旧的网络安全机制可能由于计算理论的进展、计算机性能的提高或新技术的产生而不再有效。第二，旧的网络安全问题解决之后，新的网络安全问题又将不断出现。第三，新的应用可能需要新的安全措施加以保护。比如近年来出现的网络安全攻击，特别是对大型企业计算机系统的攻击，已从几年前用蠕虫和服务阻断所进行的撒网式攻击变成更具针对性的攻击了。

经过多年的努力，特别是最近十几年的研究与实践，网络安全已逐渐形成了一些成熟的理论和有效的方法。学习这些理论与方法将为今后研究网络安全和开发安全系统打下良好的基础，同时也为系统安全管理提供牢靠的依据。因此，网络安全已成为美国各大学计算机科学系本科生与研究生的主要课程。中国的大学近年来也开始逐渐重视网络与信息安全的教学。

本书主要围绕着两条主线展开。第一条主线是以计算机密码学为根基而建立起来的各种安全协议和相应的工业化标准，它以加密算法和网络安全协议设计为主导。第二条主线是为弥补通信协议缺陷和系统漏洞而发展出来的防火墙、抗恶意软件和入侵检测等技术，它以网络设置和管理为主导。网络安全的这两条主线相辅相成，缺一不可。遗憾的是，现有的网络安全教材基本上是围绕网络安全的第一条主线展开的。围绕第二条主线展开的书则通常是面向系统管理人员而编写的，不太适合作为教材使用。本书是为弥补这一缺陷所做的一点尝试，其宗旨是以较短的篇幅向读者深入浅出、系统地介绍计算机网络安全理论与实践的主要研究成果和发展动向，使读者在一个学期的学时之内既学到理论知识又学到实用的安全技术。由于篇幅的限制，本书在不影响全局的条件下放弃了一些内容。一本书只能做一本书的事，愿本书能达到预期目标。

本书作为教材，其对象是高等院校修过计算机网络课程的高年级本科生和一年级研究生。本书亦可作为计算机工作者和系统管理人员的参考书或自修读物。

本书对专用英语名词的汉语翻译尽量与大众习惯保持一致，同时也参考了中国台湾和海外华人社团的一些用法。有些名词的汉语翻译虽然有待斟酌，但却已经被广泛使用，故不便改动。如果某个名词存在多种流行译法，本书将尽量采用意译的方法。如互联网也称为因特网或网际网，因特网是音译，网际网是直译，互联网是意译，本书采用互联网这一译法。又如网络协议层次结构的底层有物理层和实体层两种译法，物理层是直译，实体层是意译，本书采用实体层这一译法。为了方便读者阅读，书后附有专用名词汉英对照表。

本书在介绍加密算法时涉及数论及离散概率里的一些熟知的概念和定理，自学的读者如果对算法不予深究可省略这些内容。本书的一部分练习具有一定难度，需要读者有一定的系统编程经验，包括二进制数操作和二进制文件存取及编写网络应用程序的经验。后者主要是指建立在 TCP/IP 通信协议上的套接字编程。这些练习是为以本书为教材的计算机科学系和计算机工程系的学生而设计的。不过，即使不做这些练习，也不会影响读懂本书的任何章节。所以，读者如果只希望对网络安全有全面的了解，但没有时间或不愿花时间编写程序的话，则可跳过这些程序练习。

本书的基本结构如下所述。第 1 章介绍网络安全的研究领域，讨论网络安全所要解决的问题。第 2~4 章介绍网络安全领域的标准常规加密算法，公钥密码体系，密钥的产生、输送与管理方法，公钥证书，数据认证方法。第 5 章介绍实用网络安全协议和无线网安全协议。第 6~8 章介绍防火墙、抗恶意软件和入侵检测系统。标有星号的章节内容较深，故作为本科生教材时可略去。习题分常规、中等难度 (以 * 为记)、较难 (以 ** 为记) 三种级别。本科生应能完成不带星号的习题，研究生应能完成不带星号和带一个星号的习题，学有余力的本科生和研究生可试做带两个星号的习题。带星号的编程练习也可以作为实验设计。有些练习的内容是在

带星号的章节内讲授的，所以虽然不难，也标上了一个星号。

本书是根据作者多年来积累的网络安全教学经验和学生们的反馈，在以前写过的讲义的基础上整理、补充和加工而成的。本书内容除少部分外，均在本系的高年级本科生和研究生的网络安全课程中讲授过。作者在 2006 年春季特别用本书的手稿给本系研究生讲授网络安全课程，并在此基础上对本书手稿做了进一步的加工和修改。尽管如此，本书不妥之处在所难免，恳请读者及采用本书为教材的人员一旦发现错误后尽快通知作者。来信和建议请寄到作者的电子邮箱: wang@cs.uml.edu，或寄到作者的通信地址: J. Wang, Department of Computer Science, University of Massachusetts, Lowell, MA 01854, USA。

作者有幸从 1996 年起一直从事计算机网络安全的本科生与研究生课程的设计与教学，并从 2002 年起组织并参与了本校网络与信息安全中心每周一次的讨论班，在此期间得到许多同事、学生和校外专家的帮助，谨在此表示感谢。感谢在北卡罗来纳州任教时的同事保罗·杜沃 (Paul Duvall) 教授和现在的同事大卫·马丁 (David Martin) 教授的帮助。杜沃教授是美国国家安全局 (NSA) 的密码学专家，马丁教授是计算机保密和软件法检的专家。我从他们那里获益良多。

用母语写此书是我的心愿，感谢高等教育出版社给我这个机会。

斯娃提·古塔 (Swati Gupta) 曾在 2002 年将作者的讲课内容做过详细笔记，刘本渊教授阅读了本书初稿的部分章节，助教杜春燕阅读了本书初稿的全部章节，部分曾在中国受过高等教育的博士研究生和硕士研究生也对本书的写作提供了帮助，他们是余芷君、钟宁、黄蓓 (按姓氏笔画为序)，谨在此致以诚挚的谢意。

写此书所花的时间和精力比约稿时预计的超出了许多。为写此书不可避免地占用了与家人共聚的时间，我对此深怀歉意。感谢妻子赵虹和儿子、女儿的谅解与支持。

愿此书能为中国计算机网络安全的高等教育的普及尽一点力量。

王 杰 (J. Wang)，美国麻省大学罗威尔分校

2006 年 5 月

目 录