国外计算机科学教材系列

权威作者 经典教材

网络安全

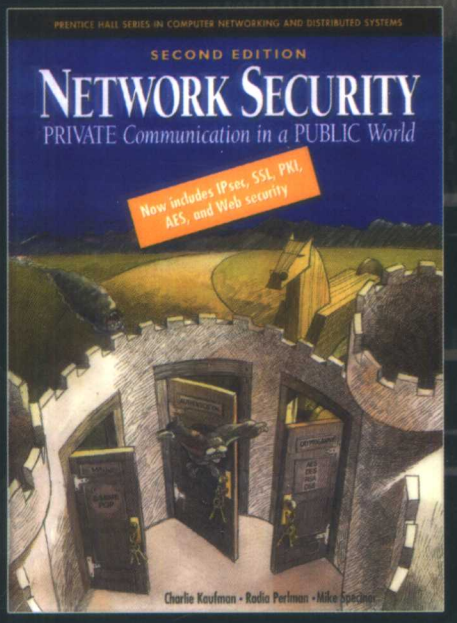
——公众世界中的秘密通信

（第二版）

Network Security

Private Communication in a Public World

Second Edition



Charlie Kaufman
[美] Radia Perlman 著
Mike Speciner

许剑卓 左英男 等译

戴英侠 审校

PRENTICE HALL PTR

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

国外计算机科学教材系列

网络安全
——公众世界中的秘密通信
（第二版）

Network Security: Private Communication in a Public World

Second Edition

Charlie Kaufman
[美] Radia Perlman 著
Mike Speciner

许剑卓 左英男 等译

戴英侠 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书全面阐述了信息安全理论，全书共分五个部分，即密码学、认证、标准、电子邮件以及其他安全机制。其中，第一部分阐述了密码算法的基本原理以及各种经典的和现代的加密算法。第二部分介绍了如何在网络中证明身份、人在向设备证明自己的身份时可能碰到的问题、认证握手协议的细节以及协议可能存在的多种缺陷。第三部分讲述了一系列安全协议（如Kerberos，IPSec和SSL等）以及PKI的一些标准。第四部分讲述了电子邮件安全中的若干问题，列出了与电子邮件相关的几个安全特性，并描述了这些安全特性的具体实现方式。第五部分介绍了防火墙、各种操作系统的安全性问题、浏览网站时所涉及的协议以及对安全实践经验的总结。本书提供了章后习题，书后还给出了大量参考文献。

本书从日常应用入手，以简单易懂的方式阐述了深奥的理论，加之原作者文笔生动幽默，堪称风格独特。本书可作为相关专业高年级本科生和研究生的教学用书以及相关领域专业人员的参考用书。

版权贸易合同登记号　图字：01-2003-0593

图书在版编目（CIP）数据

网络安全：公众世界中的秘密通信（第二版）/（美）考夫曼（Kaufman, C.）等著；许剑卓等译.
-北京：电子工业出版社，2004.9
（国外计算机科学教材系列）
书名原文：Network Security: Private Communication in a Public World, Second Edition
ISBN 7-5053-9945-4

Ⅰ.网…　Ⅱ.①考…　②许…　Ⅲ.计算机网络-安全技术-教材　Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2004）第089447号

责任编辑：刘　静
印　　刷：北京兴华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　　印张：30　字数：845千字
印　　次：2004年9月第1次印刷
定　　价：45.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。
联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

对信息安全的认识是从所需的安全属性开始的，安全属性包括信息的保密性、完整性、可用性以及不可否认性。人们最早意识到的信息安全属性是保密性，即信息仅为授权者所享有，不被泄露给非授权的用户、实体或过程。电报、电话的发明和应用，特别是如今网络通信的普及，使人们获得了远距离交流消息的各种手段。因此，远程通信安全的重要性显得特别突出。密码技术成为安全保密的重要支撑技术，因为报文加密使得第三方难以窃听到所传输消息的真正意义。当然，除了信息的保密性问题以外，还存在完整性（即信息未经授权不能进行更改的特性）问题。此外，当对信息进行存储、处理和传输时，要求整个系统能正常运行。但是，由于种种原因（如发生了拒绝服务攻击、非法滥用资源、计算机病毒侵害、由不熟练导致的误操作、自然灾害等情况），通信系统可能会失去或部分地失去工作能力。这就是可用性（即信息及信息系统可被授权实体访问并按需求使用的安全特性）的安全需求。例如，在授权用户或实体需要信息服务时，信息服务应该可以使用，或者在信息系统部分受损或需要降级使用时，仍能为授权用户或实体提供有效服务。最后，我们还必须提到不可否认性（又称抗抵赖性，即人们不能否认自己的信息行为）的问题。不可否认性分为源发不可否认和接收不可否认，前者用于防止发送者否认自己已发送的数据和数据内容，后者用于防止接收者否认已接收到的数据和数据内容。实现不可否认性的手段与技术有很多，最常用的是数字证书和数字签名。

本书围绕上述各种问题，全面地阐述了安全性。全书共分为五个部分：密码学（第2章至第8章）、认证（第9章至第12章）、标准（第13章至第19章）、电子邮件（第20章至第22章）以及其他安全机制（第23章至第26章）。第一部分深入浅出地阐述了密码算法的基本原理以及经典的和现代的各种加密算法。其中，第2章是必读的，因为这一章的内容对于理解本书的其他内容至关重要。第7章和第8章讲述了密码学背后更深层次的数学原理，这两章对于理解本书的其他内容并无影响，所以读者可以放在最后阅读。第二部分介绍了如何在网络中证明身份、人在向设备证明自己身份时可能碰到的问题、认证握手协议的细节以及协议可能存在的多种缺陷。第三部分讲述了一系列安全协议（如Kerberos, IPSec和SSL等），以及PKI的一些标准。第四部分主要讲述了电子邮件安全中的若干问题，列出了与电子邮件相关的几个安全特性，并描述了这几个安全特性的具体实现方式。最后一部分介绍了防火墙、各种操作系统的安全性问题、浏览网站时所涉及的协议以及对安全实践经验的总结。

本书原作者对密码算法和安全协议等有深入的研究，在很多方面都有独到见解，文笔生动、幽默。他用形象的语言讲述了自己的学术观点，引人入胜。同时，作者对安全的误区和一些错误的观点也给出了一针见血的评述。

本书适合作为高年级本科生或研究生的教材，也可以作为相关领域专业人员的参考书。

本书的第1章到第14章由许剑卓翻译，第15章到第26章由左英男翻译，全书的整理由戴英侠负责。此外，黄英达、左晓栋、代亮、魏军、杨东晓、鲍旭华、李闻和冯萍慧等也参与了翻译工作。

由于译者水平有限，书中难免存在疏漏和不当之处，恳请广大读者和专家批评指正。

致　谢

虽然围绕网络安全问题有着大量的争论，但我们仍感觉到网络安全领域的人士很乐于分享智慧和时间。在向提供帮助的人表示感谢时，我们总是担心可能会漏掉其中的某些人，但是不对任何人表示感谢显然也是不妥的。

Eric Rescorla和Hilarie Orman对本书进行了仔细的审阅并回答了我们提出的很多问题。其他对本书进行审阅并提供帮助的人有：Tom Wu，Kevin Fu，Marshall Ross，Joe Tardo，Joe Pato，Seth Proctor，Timothy Spiller，Tom Rice，Kristen McIntyre，Gary Winiger，Dan Harkins，Peter Memishian，Jeff Schiller，Burt Kaliski，Tony Lauck，Phil Karn，Ron Rivest，Steve Crocker，Steve Kent，John Linn，Steve Hanna，Jim Bidzos，Dave Jablon，Ted Ts'o，Matthew Barnes，Keith McCloughrie，Jeffrey Case，Kathrin Winkler，Philippe Auphelle，Sig Handelman，Phillip Hallam-Baker，Uri Blumenthal，Serge Vaudenay，Boyd Roberts。

如果没有下述几家公司的帮助，我们就无法完成第24章，因为该章涉及的多数是非公开的内容。在此要感谢Iris（Lotus Notes）的Al Eldridge、IBM（KryptoKnight）的Amir Herzberg和Mark Davis、OSF的Walt Tuvell以及微软（LAN Manager和Windows NT安全）的Cliff Van Dyke，他们向我们讲解了各自的系统并及时审阅了我们撰写的内容。虽然我们之中有67%的人所服务的公司生产这一领域的产品，但是本书提供的观点是我们自己的观点，而不是公司的观点。

Prentice Hall的总编Mary Franz在本书的成书过程中一直非常热心地为我们提供帮助。她知道我们在什么时候需要帮忙，也知道什么时候不需要理会我们。她知道有时需要不断地唠叨催促我们，也知道有时只需要深情地望着我们，就足以使我们知道没有及时交稿是多么内疚的事。

虽然这本书让我们的人生中很大一部分时间都变得非常繁忙，但是Ray Perlner让我们对这一创作过程充满了热情。他对本书的创作怀着真切的关心，在我们之间有争论时他提出了非常有用的建议，他帮助我们查找参考文献并审校了本书的部分章节，他还特别喜欢纠正我们用错的代词，其实有时我们故意用错一些代词只是希望能够听到他咯咯的傻笑。Dawn Perlner在本书的编写过程中也提供了大量的帮助，并试图说服很多人（甚至是陌生人）购买本书。

当然还要感谢你，我们的读者。我们欢迎你提出宝贵的建议和批评，当然也非常欢迎你的赞美。我们希望能够定期更新本书的内容，如果你希望我们在本书的新版本中讨论什么题目或者改正哪些错误，都请你告诉我们。通过网站http://www.phptr.com/networksecurity可以与Errata取得联系。

我们现在使用的电子邮件地址是ckaufman@us.ibm.com，radia@alum.mit.edu和ms@alum.mit.edu，但我们发现电子邮件不总是可靠的，并且地址也总是改变。如果无法与我们之中的任何一个人取得联系，你可以和出版商Prentice Hall联系，特别是可以和我们的编辑Mary Franz（mfranz@prenhall.com）联系以获得我们最新的电子邮件地址。

目　录

第二部分　认证

第三部分 标准

第五部分 其他安全机制

第1章 简 介

在一个月黑风高的夜晚，远处传来野狗的嚎叫。Alice突然看到一个闪亮的物体，一个钻石链扣！家里只有一个人能够买得起钻石链扣，肯定是管家偷了主人的钻石链扣！Alice必须马上告知Bob，但是她怎么才能通知Bob而不被管家发现呢？如果打电话给Bob，管家可能会在另一个分机上偷听，如果用信鸽并将消息系到它的脚上，Bob又怎么知道是Alice发送的消息呢？他说不定会以为是Trudy故意陷害管家、因为管家拒绝了她的求爱。

这就是本书要讲解的内容。本书恐怕不会过多地描述Alice和Bob的个性，也不会讲述关于管家的事情。但是，我们将讲解如何通过不安全的信道进行安全的通信。

安全的通信是什么意思呢？Alice必须能够发送只有Bob可以看懂的消息给Bob，即使别人能够看到她发送的消息也无所谓。当Bob接收到消息的时候，他必须能够识别出该消息确实是Alice发送的，而且没有人在Alice发送消息与Bob接收到消息之间篡改消息。

不安全的信道是什么意思呢？在一些词典或其他解释中，Internet被描述为“不安全的信道”。整个世界的每台计算机正在逐步走向互联，人们正在谈论如何连接家里的各种家用电器，这将形成一个美妙的全球网络。多么美好啊！你可以通过电子邮件将信息发送给全世界的任何人。你在斐济度假的时候，可以通过网络发送一个简单的命令控制你的核能源工厂。网络世界是可怕的，侦听者可以窃听网络上的很多连接。信息必须经过包交换机转发，重新配置这些交换机就有可能侦听或修改经过的数据包。

这种状况看起来很让人失望，但是可以利用神奇的数学原理来解决这些问题，特别是利用密码学。利用密码学原理，可以将一串数值转换为密文。密文是一组乱码，只有知道秘密的人才能对其做反向转换。密码学让我们能够伪装数据，使得侦听者虽然能够窃听传输的消息，但却无法获取任何有用的信息。密码学还使得我们能够创建一个无法伪造的消息，并且可以监测出该消息在传输过程中是否被篡改。一种实现这一目的的技术叫数字签名，数字签名是与消息相关联的一个数值，其他人可以检验这一数值，以识别消息发送者的身份。只有发送者能够生成该数字签名。这看起来很让人惊讶，怎么才能做到让你只能检验某个数值而无法生成该数值呢？一个人的手写签名只能是这个人生成的，但可以被其他人所识别。但是，看起来似乎不难生成某个数值，即使这个数值还必须是能够被检验的。理论上讲，可以尝试大量的数值并检验是否为某个人的签名。这样不就可以生成别人的数字签名了吗？但是，由于使用的数值非常大，用这种方法生成签名可能需要花费大量的时间（比如整个宇宙时间的几倍）。所以，数字签名和手写签名有着相同的特性，也就是只能是某个人生成的。但是数字签名比手写签名具有更多有用的特性，因为数字签名取决于消息的内容，如果有人修改了消息的内容，那么签名也就不再是正确的了，这样就可以发现篡改行为。在学习过第2章之后，读者就会很清楚这一点了。

密码学是本书的主要内容，这不是因为密码学本身非常有趣（当然它确实很有趣），而是因为人们希望计算机网络能够具备的安全特性可以通过密码学来实现。