Computer Network Security: Theory and Practice

计算机网络安全的理论与实践

王 杰

高等教育出版社
HIGHER EDUCATION PRESS

计算机网络安全的理论与实践

王 杰

高等教育出版社

内容提要

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，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。这两条主线相互交织，形成维护网络安全的防御体系，缺一不可。本书以此为指导思想，用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。

本书内容包括网络安全概论，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，实用网络安全协议及无线网安全协议，防火墙原理，抗恶意软件，万维网安全和入侵检测系统。本书还包括相当数量的实际操作练习。

本书可作为高等院校本科高年级学生和一年级研究生的“计算机网络安全”教材，亦可作为计算机工作者和系统管理人员的参考书和自修读物。

图书在版编目(CIP)数据

计算机网络安全的理论与实践 / 王杰编著. —北京：
高等教育出版社,2006.10
ISBN 7-04-020141-0

Ⅰ.计... Ⅱ.王... Ⅲ.计算机网络-安全技术-
高等学校-教材 Ⅳ.TP 393.08

中国版本图书馆 CIP 数据核字(2006)第 108675 号

出版发行	高等教育出版社	购书热线	010-58581118
社　址	北京市西城区德外大街 4 号	免费咨询	800-810-0598
邮政编码	100011	网　址	http://www.hep.edu.cn
总　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　刷	唐山市润丰印务有限公司	畅想教育	http://www.widedu.com
开　本	787×1092　1/16	版　次	2006 年 10 月第 1 版
印　张	14.25	印　次	2006 年 10 月第 1 次印刷
字　数	270 000	定　价	26.40 元

物 料 号　20141-00

作者简介

王杰(原名王洁)，1961年8月生于广州，祖籍湖南。1982年和1984年分别获得中山大学计算数学理学学士和软件工学硕士学位，毕业后留校任教。1986年获美国波士顿大学校长奖学金赴美，1990年获波士顿大学计算机科学哲学博士学位。现任美国马萨诸塞大学罗威尔分校计算机科学系教授和网络与信息安全中心主任。曾任美国第一联合银行总部网络安全顾问，并在北卡罗来纳州议会的技术委员会做过数字签名和网络身份诈骗的专题报告，协助该州议会制定数字签名的法规。主要研究方向为平均计算复杂性理论、网络与系统安全、应用算法以及无线传感器网络通信。多次获得美国自然科学基金会及美国IBM公司和英特尔公司的资助。曾发表论文78篇，著书一本，编书两本。

郑重声明

策划编辑　刘　英

责任编辑　焦建虹

封面设计　王　晔

责任绘图　杜晓丹

版式设计　范晓红

责任校对　王效珍

责任印制　毛斯璐

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，如何不断地采取最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和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和自修读物。

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省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。比如互联网也称为因特网和网际网，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。又比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，或寄到作者的通讯地址: 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), 美国马萨诸塞大学罗威尔分校

2006 年 5 月

目　录

第 1 章　网络安全概论

网络安全的目的是保障人们在日常生活和商业活动中能自由地享受计算机网络所带来的好处而不殃及自身利益。网络安全的任务是看家护院，即照看好连网计算机系统和保护好存储于连网计算机内的数据及在网络中传输的数据。互联网是公共网，任何单位和个人均可通过简单的手续和少量的费用将自己的计算机和网络设备连到互联网而成为互联网的一部分。因为互联网通信主要是通过他人所控制的网络设备接收和传递数据，所以任何人均可设法读到他人在网上传递的数据或利用网络侵入他人的计算机系统。也就是说，任何单位和个人都可以成为攻击者和被攻击对象。即使我们不想攻击别人，我们的连网计算机仍可能被他人利用而变成攻击工具。孙武子曰：知己知彼，百战不殆。为看好自家门户，首先应对可能遭受打击的目标和攻击手段以及攻击者的背景与动机有一个全面且正确的认识。

1.1　网络安全的任务

网络安全的主要任务是维护数据的机密性、完整性和不可否认性，并协助提供数据的可用性。数据的概念在这里是广义的，它指任何可以用计算机执行和处理的对象，包括源程序、可执行代码、各种制式的文件、数码音乐、数码图像和数码电影。数据应只能被合法用户读取和修改。未经许可的任何单位或个人不能读取和修改数据。我们把未经许可的单位和个人统称为第三者。

与中央处理器、内存、硬盘和网络带宽等资源一样，数据也是一种资源。数据也称为信息。

数据有两种状态，一种是传输状态，一种是存储状态。因此，数据的机密性和完整性主要体现在如下两个方面。

1. 维护网传数据的机密性和完整性

机密性是指保证数据在网络传输过程中不会被第三者读取，完整性是指保证数据在网络传输过程中不会被第三者修改或伪造。

2. 维护存储数据的机密性和完整性

机密性是指不允许第三者通过网络非法进入连网计算机系统读取存储在其中的数据，完整性是指不允许第三者通过网络非法进入连网计算机系统修改存储在

其中的数据或存入伪造数据。

数据的不可否认性是指数据的合法拥有者无法向任何人抵赖自己是这个数据的拥有者。不可否认性也称为不可抵赖性。

数据的可用性是指连网计算机系统的各种资源不会被第三者通过网络协议缺陷或既有漏洞阻碍合法用户的使用。比如，当计算机系统受病毒感染后能及时发现并消除病毒，服务器在遭受服务阻断攻击时不致瘫痪。

协议缺陷和既有漏洞是指通信协议、应用软件和系统软件中含有可被第三者利用的意外成分，它可能是协议中的某些步骤不完善，软件中的某些语句含有副作用，或是系统的设置不严谨。

网络安全的主要指导思想是防御。网络安全的防御应是全面的，但同时又是被动的，因为人们在遭受攻击前通常不知道谁将是攻击者和攻击者将在哪里发起攻击。当受到攻击后，即使能及时发现和确认攻击者的计算机系统，我们也不能擅自采取以夷治夷的方针反击攻击者的计算机系统，因为这样做可能是违法的。有关这些问题的探讨涉及法律条文，不在本书论述范围之内。所以，虽然兵法认为进攻是最好的防御，但主动进攻的策略在网络安全领域并不适用。对网络安全而言，*纵深防御*乃是最有效的防御手段。纵深防御的目的是在网络通信系统内外建造一个多层次的交叉防御体系，利用各种有效和合法的手段层层抵御可能来犯之敌。

网络安全是信息安全的重要组成部分。除了网络安全之外，信息安全还包括安全政策、安全审核、安全评估、可信赖操作系统、数据库安全、安全软件、入侵应变、计算机法检、灾难恢复和安全培训等领域。在后面的章节中会提到其中一些领域中的某些方面，但这些领域的详细讨论不在本书范畴之内。

1.2　基本攻击类型和防范措施

网络安全有下列几种基本攻击类型和防范措施。任何已知的网络攻击形式大都是由这些基本攻击类型组成的，可能是其中一种类型或是几种类型的排列组合。

1.2.1　监听

监听的目的是从网络通信中窃取数据。例如，将一个路由器连接到互联网上，便可用监听软件读取所有经过此路由器的数据包。监听软件也称为数据包嗅探或网络嗅探。监听软件可从网上下载。比如，TCPdump 和 Ethereal (参见习题 1.3) 是两个可免费下载且广泛使用的监听软件。监听软件也可根据 TCP/IP 开放程序按照自己的需要编写。编写这样的软件并非难事。不过，这种形式的监听就像守株待兔，因为监听者不知道想监听的数据是否会从此路由器经过。

有目标的监听其难度较大，首先要知道想监听的数据将经过哪些路径，然后设法在这些路径中安插自己的网络设备或设法控制某些已在这些路径上的路由器。在别人的通信路径中安插自己的网络设备虽然不容易，但却是能够做到的，比如可