21世纪计算机科学与技术系列教材（本科）

网络安全技术及应用

主　编　龙冬阳
副主编　王常吉　肖德琴

华南理工大学出版社

21世纪计算机科学与技术系列教材(本科)

网络安全技术及应用

主　编　龙冬阳

副主编　王常吉　肖德琴

编　委　(按笔划为序)

王晓明　王常吉　龙冬阳　肖德琴

凌　捷　郭艾侠　谢赞福

华南理工大学出版社

·广州·

内容简介

本书主要介绍网络安全技术及其应用。首先从网络出发，介绍基于密码体制的Kerberos认证技术和以X.509数字证书为基础的PKI体制的网络身份认证技术，重点介绍网络安全协议IPSec协议的体系结构，同时也简单讨论了无线网络安全问题。针对网络攻击技术，介绍了口令破解、缓冲区溢出攻击、网络扫描器扫描、拒绝服务攻击及欺骗攻击技术；针对系统防御主要介绍了网络病毒防治、防火墙技术、入侵检测技术等防御技术。最后介绍了安全工程及信息安全管理技术。

本书可作为计算机、数学、通信、信息系统管理专业本科生教材，也可作为相关领域工程技术人员的参考资料。

图书在版编目(CIP)数据

网络安全技术及应用/龙冬阳主编. —广州：华南理工大学出版社，2006.2
(21世纪计算机科学与技术系列教材(本科))
ISBN 7-5623-2226-0

Ⅰ.网… Ⅱ.龙… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2005)第051219号

总 发 行：华南理工大学出版社(广州五山华南理工大学17号楼，邮编510640)
发行部电话：020－87113487 87111048(传真)
Email：scutc13@scut.edu.cn **http**://www.scutpress.com.cn
责任编辑：欧建岸 ouja2@163.com
印 刷 者：湛江日报社印刷厂
开 本：787×960 1/16 **印张**：25.75 **字数**：520千
版 次：2006年2月第1版第1次印刷
印 数：1～3 000册
定 价：35.50元

编 委 会

总 序

放眼五洲风云，惊心世界科技。进入21世纪才短短几年，但科技进步更加日新月异。以信息科技为核心的高新技术的发展，极大地改变了人们的生产、生活方式和国际经济、政治关系，以经济为基础、科技为先导的综合国力竞争更为激烈。在这样激烈的竞争中，我们清醒地看到，我国生产力和科技、教育还比较落后，实现现代化，实现中华民族的伟大复兴还有很长的路要走。而在这方面，党中央已经明确提出，开发人力资源，加强人力资源能力的建设，是关系到我国发展的重大问题。培养和造就一代年轻人才，是一项紧迫而重大的战略任务。

培养和造就一代年轻人才，靠什么？靠教育，靠对年轻一代进行德智体美劳全方位的教育。培养一代掌握当前科技核心信息技术（计算机科学技术即是其重要分支）的人才，就要靠更加精心、更加有力度的教育。

而在计算机科学的教育中，除了教师、设备之外，重要的条件是教材。教师、设备、教材三者互为补充，构成计算机科学教育不可或缺的要素。在某种意义下，教材还可以认为是前导性的。惟其如此，计算机器协会（ACM）在1968年，当美国许多大学刚刚设立计算机科学系的时候，就集中了全美国计算机科学的权威教授、专家和各主要大学的代表，制定了计算机科学教育的基本框架、课程设置以及各门课程的基本内容和大纲。美国那个时期的课程设置和教材，几乎无一例外都是根据“课程表68”的思想形成和编写的。而后电气与电子工程师学会（IEEE）也参与了制定计算机科学教育的计划。作为迎接新世纪的重要举措，他们一起推出了反映当代计算机科学前沿知识和全面要求（所谓全面要求，指它不仅讨论了专业知识的内容，还讨论了知识产权、计算机病毒防范、伦理道德、职业规范、社会影响等问题）的ACM和IEEE“课程表2001”。在众多的学科门类中，对于青年一代的教育予以如此重视的，除计算机科学外，大概无第二个了。这既反映了计算机科学（包括作为其总体的信息科学技术）的核心地位，也反映了教材在教育中的特殊地位。

也就在1968年，当年的图灵奖获得者理·W·汉明（R·W·Hamming）

走向图灵奖讲演台时谈到:“我们需要为我们的学生到2000年时做准备,那时他们许多人即将达到他们事业的顶峰。”我们也要立足现在,把教育的目标放到30年后,我们现在的教育也要为到2035年时我们的学生做准备,那时他们许多人即将达到他们事业的顶峰。根据我国发展的规划,这也就是我国进入建国100周年倒计时的时刻,就是我们要实现中华民族全面复兴的时候,就是我国在综合国力要名列世界前茅的时候,因此我们现在就要为这一个宏伟目标作准备。

任重而道远。我国现在还很难说已经有了能和上面所述ACM和IEEE“课程表2001”在思路上、在内容上相符的教材。我们认为,在教材建设上,借鉴和采用个别的外文教材是可以的和无碍的,但是如同整个教育必须走我们自己的路一样,在教材建设上我们也一定要走自己的路。

广东省作为经济大省强省,现在明确提出要成为教育强省。作为在广东的计算机科学工作者,我们深感自己在发展我国特别是广东省的计算机科学教育中责任重大。因此,我省计算机学会与华南理工大学出版社共同组织了全省各高等院校计算机专业骨干教师编写这套《21世纪计算机科学与技术本科系列教材》,希望这套教材能为计算机专业提供优秀的教学用书。这套教材以培养未来人才为目标,以ACM和IEEE“课程表2001”为指导,结合我国计算机教育实际情况,以着力提倡创新精神和提倡实践动手能力为主线,注重教材内容的系统性、科学性和准确性以及文字的流畅性、可读性。

我们虔诚希望我们的努力能切切实实推动我国,特别是广东省计算机教育水平上一个台阶。

姜云飞

韩国强

苏运霖

2003年9月

前 言

在信息化社会中，信息是一种重要的战略资源，因特网已经成为世界各国获取经济、军事和科技情报的重要场所。信息高速公路为跨国搜集各种战略信息提供了新的途径，国际上围绕信息的获取、使用和控制的竞争愈演愈烈。“谁掌握了信息，控制了网络，谁就将拥有整个世界。”国家的信息获取能力，以及在社会生产生活领域中的“制信息权”，将成为国家在21世纪的生存与发展竞争中能否占据主动的关键。网络与信息安全成为当今信息化社会最关键的领域之一，因而要加速网络信息安全技术的研究、构建我国21世纪的网络信息安全保障体系、有效地保障国家安全、社会稳定和经济持续发展，就必须培养大量的从事网络信息安全技术研究的专门人才。因此，网络与信息安全技术已成为当代计算机专业、数学专业及电子与通信专业等专业研究生、本科生和IT技术人员的必修课。基于这种迫切性，受广东省计算机学会委托，由中山大学、暨南大学、广东工业大学、华南农业大学及广东技术师范学院等高校的多名教师联合编写了这本教材。

本书共分10章。

第1章介绍网络信息安全的一些基本概念，包括信息安全的5个基本属性：保密性、完整性、可用性、可控性和不可否认性，简单讨论常见的网络安全威胁及典型的网络攻击，同时还涉及网络安全服务，主要由安全服务、安全机制、安全模式及安全分析等内容组成；最后介绍了一些安全标准和制定安全标准的国际化组织以及建立信息安全保障体系的相关问题。

第2章介绍密码学的基本概念及技术，包括古典密码体制、单钥密码体制（如DES和AES）、公钥密码体制（如RSA）、散列（Hash）函数（如MD5）、数字签名以及密钥管理等内容。

第3章介绍基于单钥密码体制的Kerberos认证协议和以X.509数字证书为基础的PKI体制的网络身份认证技术。

第4章介绍IP层的安全协议，特别是IPSec协议的体系结构和它的基本原理。我们也讨论了电子邮件加密技术——PGP的设计原理，它是Internet安全的重要应用。作为IPSec协议的体系结构的应用，主要介绍IPSec在Windows 2000操作系统中的实现。最后还介绍了SSL协议与TLS传输层安全协议。

第5章介绍计算机病毒的特征与原理、计算机病毒的预防与清除，以及宏病毒、邮件病毒、特洛伊木马病毒、网络炸弹等几种常见的计算机病毒。

第6章介绍几种常用的网络攻击技术，包括其原理及工具，以及其防御手段。重点讲述网络攻击的步骤、口令破解问题和缓冲区溢出攻击技术。同时也介绍两

种信息收集工具:扫描器和 Sniffer。最后讨论了拒绝服务攻击 DoS 和欺骗攻击技术。

第 7 章从防火墙的基础知识、设计原理、设计实例、面临的攻击等方面进行了较为详细的介绍,最后还给出防火墙具体的安装、配置方法及使用实例。

第 8 章介绍入侵检测系统的基本概念和入侵检测系统设计原理及实施规则,还对目前常用的若干入侵监测工具如 RealSecure、Cisco Secure IDS、Autonomous Agents for Intrusion Detection、金诺网安入侵检测系统 KIDS 和瑞星入侵检测系统 RIDS－100 等进行了详尽的介绍。

第 9 章简单介绍了无线网络的基础知识。主要分析无线网络中的不安全因素,提出相应的解决措施,并介绍了无线网络的基本结构及其设计方法,最后探讨无线网络的攻击和防护。

第 10 章分 5 个层面对信息安全工程进行讨论。先讨论信息安全管理体系框架,然后分析风险评估和应急响应方法,之后讨论灾难备份与恢复的一些措施,再对安全攻防进行分析,最后对物理安全进行了讨论。

本书每一章后都附有适当的练习题,重点在网络信息安全的基本概念与方法,有些分析题是探讨性的,并没有所谓的"标准答案"。对于学习者来说,做一定的练习就如同上机编程实现某一个密码算法一样是必不可少的重要环节。

本书由中山大学龙冬阳教授主编。龙冬阳教授编写第 1 章、第 6 章及第 9 章,暨南大学王晓明教授编写第 2 章,中山大学王常吉副教授编写第 3 章,广东工业大学凌捷教授编写第 4 章,华南农业大学郭艾侠老师编写第 5 章,华南农业大学肖德琴副教授编写第 7 章和第 10 章,广东技术师范学院谢赞福副教授编写第 8 章。本书的出版是各位作者共同辛勤劳动的结果,没有大家的合作,就没有这本《网络安全技术及应用》。

罗少贤与关展鹏为本书做了大量的工作。同时本书的编写得到了国家自然科学基金(项目编号:60273062)和教育部留学回国人员启动基金的资助,在此一并表示感谢。

由于水平所限,书中难免有错漏,欢迎读者批评指正。将意见发送到电子邮箱 issldy@zsu.edu.cn。

龙冬阳

中山大学计算机科学系

2006 年 1 月

目　录

1 引 论

本章主要介绍网络安全的一些基本概念，包括信息安全的5个基本属性：保密性、完整性、可用性、可控性和不可否认性，简单讨论常见网络安全威胁及典型的网络攻击，同时还涉及网络安全服务的内容，主要由安全服务、安全机制、安全模式及安全分析等内容组成，最后介绍一些安全标准和制定安全标准的国际化组织以及建立信息安全保障体系的相关问题。

1.1 信息化与安全

信息社会的到来与信息技术的应用，使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入崭新的信息化时代。在信息化社会中，一个国家、一个地区、一个单位乃至一个家庭和个人，如果没有好的信息基础设施，他在现代信息社会的激烈竞争中就会落后，甚至失败。

Internet为人类交换信息，促进科学、技术、文化、教育、生产的发展，提高生活质量提供了极大的便利。由于网络的全球性、开放性、无缝连通性、共享性和动态发展，使任何人都可以自由接入Internet。因此难免有人采用各种攻击手段进行破坏活动，试图穿透别人的系统，窃取重要情报、捣毁电子邮箱、散布破坏性信息、倾泻信息垃圾、进行网络欺诈、施放病毒和发动“黑客战”等活动，对国家、单位和个人的信息安全构成极大的威胁。

网络信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题。信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是21世纪初世界各国奋力攀登的制高点。网络信息安全问题倘若不能妥善解决，将会全方位地危及我国的政治、军事、经济、文化和社会生活的各个方面，使国家处于信息战和高度经济风险的威胁之中。

1.2 信息安全基本概念

随着信息技术的发展与广泛应用，信息革命所带来的变革已深入人们日常生活和每个企业行为之中。特别是通信技术与计算机技术的结合带动了计算机通信网络的飞速发展，Internet不断普及，人们的消费观念和整个商务系统也都发生了