<<网络安全高级软件编程技术>>

图书基本信息

书名：<<网络安全高级软件编程技术>>

13位ISBN编号：9787302219040

10位ISBN编号：7302219044

出版时间：2010-4

出版时间：清华大学出版社

作者：吴功宜,张建忠,张健,董大凡,许昱玮

页数：391

前言

未来的社会是信息化的社会，计算机科学与技术在其中占据了最重要的地位，这对高素质创新型计算机人才的培养提出了迫切的要求。
计算机科学与技术已经成为一门基础技术学科，理论性和技术性都很强。
与传统的数学、物理和化学等基础学科相比，该学科的教育工作者既要培养学科理论研究和基本系统的开发人才，还要培养应用系统开发人才，甚至是应用人才。
从层次上来讲，则需要培养系统的设计、实现、使用与维护等各个层次的人才。
这就要求我国的计算机教育按照定位的需要，从知识、能力、素质三个方面进行人才培养。
硕士研究生的教育须突出“研究”，要加强理论基础的教育和科研能力的训练，使学生能够站在一定的高度去分析研究问题、解决问题。
硕士研究生要通过课程的学习，进一步提高理论水平，为今后的研究和发展打下坚实的基础；通过相应的研究及学位论文撰写工作来接受全面的科研训练，了解科学研究的艰辛和科研工作者的奉献精神，培养良好的科研作风，锻炼攻关能力，养成协作精神。
高素质创新型计算机人才应具有较强的实践能力，教学与科研相结合是培养实践能力的有效途径。
高水平人才的培养是通过被培养者的高水平学术成果来反映的，而高水平的学术成果主要来源于大量高水平的科研。
高水平的科研还为教学活动提供了最先进的高新技术平台和创造性的工作环境，使学生得以接触最先进的计算机理论、技术和环境。
高水平的科研也为高水平人才的素质教育提供了良好的物质基础。

<<网络安全高级软件编程技术>>

内容概要

本书的作者队伍是由南开大学计算机系、国家计算机病毒应急处理中心的人员组成。
作者在总结多年网络安全科研与教学实践经验的基础上，设计了12个“近似实战”的网络安全软件设计与编程训练的课题。
训练课题覆盖了从密码学在网络通信中的应用，网络端口扫描、网络嗅探器、网络诱骗、网络入侵检测、安全Web、防火墙，到Linux内核网络协议栈程序加固、网络病毒与垃圾邮件的检测与防治技术。
训练课题接近研究的前沿，覆盖了网络安全研发的主要领域与方向。
完成网络安全训练课题的操作系统选择为Linux，完成训练课题不限定任何特殊的硬件环境与编程语言。
通过在Linux环境中完成网络安全软件的设计与编程训练，提高读者研发具有自主知识产权的网络安全技术和产品的能力。
本书可以作为计算机、信息安全、软件工程、通信工程、电子信息及相关专业的硕士与工程硕士研究生、博士研究生的教材或参考书，以及本科计算机专业，信息安全专业高年级学生网络安全教材或参考书，也可作为网络安全高级软件编程人才的培训教材与研发工作参考手册。

作者简介

吴功宜，南开大学信息技术科学学院计算机系教授、博士生导师。
曾任南开大学计算机系系主任、研究生院常务副院长、信息技术科学学院院长。
研究方向：计算机网络与信息系统，网络与信息安全。
从1984年开始为本科生和研究生讲授“计算机网络”等课程；主持和参加完成多项网络与信息安全方向科研项目，发表学术论文50余篇；参加编著和出版的教材、专著、译著共28部。
张建忠，博士，南开大学信息技术科学学院计算机系教授、博士生导师。
多年来承担计算机网络方向本科生及研究生的教学工作，讲授“计算机网络基础”、“网络管理”、“网络安全技术”、“对等计算”等课程。
张健，博士，高级工程师，任国家计算机病毒应急处理中心和计算机病毒防治产品检验中心常务副主任。
自1990年至今一直从事计算机病毒防治研究工作。

<<网络安全高级软件编程技术>>

书籍目录

章节摘录

插图：安全审计研究的内容主要有：网络设备及防火墙日志审计、操作系统曰志审计。
目前防火墙等安全设备具有一定的日志功能，在一般情况下只记录自身的运转情况与简单的违规操作信息。
由于一般的网络设备与防火墙对网络流量分析能力不够强，所以这些信息还不能对网络的安全提供分析依据。
同时，由于一般网络设备与防火墙采用内存记录日志，因此空间有限，信息需要经常地覆盖。
因此没有能力提供足够的分析数据。
这种网络设备与防火墙的设计不能满足安全评测标准的要求。
目前大多数操作系统都提供日志功能，记录用户登录等信息，但是如果要从大量零散的信息去人工分析安全信息是很困难的。
同时，日志被修改的可能性也存在。
因此，目前多数操作系统安全审计方法尚不能满足安全评测标准的要求。
1.3.4 网络防病毒技术研究恶意传播代码（maliciousmobilecode，MMC）是一种软件程序，它被设计成能够从一台计算机传播到另一台计算机，从一个网络传播到另一个网络，目的是在网络和系统管理员不知情的情况下，对系统进行故意地修改。
恶意传播代码包括病毒、木马、蠕虫、脚本攻击代码，以及垃圾邮件、流氓软件与恶意的Internet代码。
病毒程序的名称来源类似于生物学的病毒。
病毒程序是一种专门修改其他宿主文件或硬盘的引导区，来复制自己的恶意程序。
一旦感染病毒，宿主文件就变成病毒再去感染其他的文件。
木马程序又叫做特洛伊木马，是一种非自身复制程序。
它伪装成一种程序，但是程序是什么用户并不知道。
例如，用户从网络上下载并运行了一个游戏程序，但游戏程序的制造者同时将一个木马程序装进了用户的计算机，以便黑客进入并控制该计算机。
木马程序不改变或感染其他的文件。
后门（backdoor）程序是恶意程序中的子程序，它使黑客可以访问本来安全的计算机系统，而不会让用户或管理员知道。

编辑推荐

《网络安全高级软件编程技术)》：计算机科学与技术学科前沿丛书，计算机科学与技术学科研究生系列教材(中文版)

版权说明