普通高等教育“十一五”国家级规划教材

高等学校计算机科学与技术教材

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

信息与网络安全

□ 程光　张艳丽　江洁欣　编著

清华大学出版社　●　北京交通大学出版社

普通高等学校“十一五”国家级规划教材
高等学校计算机科学与技术教材

信息与网络安全

程 光 张艳丽 江洁欣 编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书是针对计算机和信息安全专业教学而编写的教材。通过该教材的学习，学生可以掌握计算机网络安全的基本概念，了解网络设计、维护及应用系统安全的基本手段和常用方法。

全书共14章，分为四个部分。第一部分概述信息与网络安全相关知识；第二部分分五章讲述信息安全技术相关内容，包括常规加密技术、DES数据加密标准，公钥加密技术，基于加密技术的数字签名、身份鉴别等网络安全应用，以及信息隐藏技术等；第三部分分四章介绍网络安全相关技术，这部分内容包括网络安全的防御技术和相关的网络安全协议等；第四部分分四章介绍信息与网络检测的相关实用技术，包括入侵检测技术、信息获取技术、安全信息取证和逆向工程等。

本书适合作为“信息与网络安全”课程的教材，也可供相关技术人员作为参考用书。

图书在版编目(CIP)数据

信息与网络安全/程光，张艳丽，江洁欣编著. —北京：清华大学出版社；北京交通大学出版社，2008.6
（高等学校计算机科学与技术教材）
普通高等学校“十一五”国家级规划教材
ISBN 978－7－81123－309－4

Ⅰ.信…　Ⅱ.①程…　②张…　③江…　Ⅲ.电子计算机－安全技术－高等学校－教材　Ⅳ.TP309

中国版本图书馆CIP数据核字(2008)第063091号

责任编辑：谭文芳
出版发行：清华大学出版社　邮编：100084　电话：010－62776969　http://www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010－51686414　http://press.bjtu.edu.cn
印 刷 者：北京东光印刷厂
经　　销：全国新华书店
开　　本：185×260　印张：20.5　字数：525千字
版　　次：2008年6月第1版　2008年6月第1次印刷
书　　号：ISBN 978－7－81123－309－4/TP·417
印　　数：1～5 000册　定价：32.00元

前　言

本书是普通高等教育“十一五”国家级规划教材。

随着互联网渗透到人们社会经济生活的各个方面，由于信息与网络的安全导致的损失日益加剧，信息与网络安全问题也越来越被人们所重视，已成为信息化建设的核心问题。鉴于目前信息与网络安全的重要性，培养和提高未来计算机专业人员信息和网络安全的基础理论和实践技能，已成为目前计算机专业教学的重点课程之一，不少高校已经开设信息与网络安全相关课程和专业。

由于互联网技术的快速发展，信息和网络安全技术有较强的时效性，而目前的教材不能很好地涵盖新的理论和技术，因此，有必要编写面向计算机和信息安全专业本科生的“信息与网络安全”教材。通过该教材的学习，学生可以掌握计算机网络安全的基本概念，并了解网络设计、维护及其应用系统安全的基本手段和常用方法。

本书作者一直参加“CERNET 华东北地区网络中心”和“江苏省计算机网络重点实验室”的建设和管理，具有长期从事计算机网络方面的研究和开发经历，以及多年管理运行区域性 IP 网络的经验；参加和主持过各类相关的国家级课题，开展过网络管理、网络安全体系结构、网络数据安全机制等方面的研究，具有丰富的网络理论、管理和使用经验；连续多年在东南大学进行了“信息与网络安全”等相关课程的教学工作，具有丰富的信息与网络安全教学经验。本书的主要内容已经作为讲义连续 4 年在课堂上先后对 800 多名本科学生进行了讲授，对学生展开课程设计和生产实践都有一定帮助。

本书主要面向全国计算机专业和信息安全专业本科教学而编写。教材主要从先进性、实用性和培养学生多学科综合能力、解决实际问题等几个方面着手，力求通过科研和教学实践，不断完善该学科知识体系结构和内容，使该课程知识更为系统化和实用化，更能适合目前我国信息与网络安全工作和科研的需要。本教材从加密理论、安全协议、安全应用等几个大方向，强调本课程与专业间的逻辑关系，并以目前常见的安全问题实例为分析依据，使教材具有新颖性、知识性和实用性等特点。

本书主要特色体现在以下三个方面。

1. 技术方法的成熟与先进相互结合和补充，理论与实践相结合

本书涉及的内容和技术方法立足于学科前沿，且其理论和实践方法紧密联系信息与网络安全现状。每一章都包含相关理论与技术工具和习题，通过相关工具的学习和习题的完成，能帮助读者更深刻地理解所学习的知识，并学会使用现有的工具解决网络应用过程中所遇到的各类实际问题。

2. 取材先进，内容、体系具有创新性

本书在内容安排上，力求在全面的基础上突出实用性，强调教学与科研、理论和实际的紧密联系，注重书本知识与信息和网络安全的具体应用相结合。同时保留具有探索性、有待完善的国内外研究理论和应用研究方面的知识，力求达到丰富教学内容、加强基础知识教育

和拓宽学生思路，以及培养学生自主思考问题能力的培养目标。

3. 前瞻性

本书不仅对专业的基础理论进行归纳总结，而且对专业的发展趋势及当前热点问题进行了介绍，具有前瞻性。既可满足本科教学也可供专业的技术人员参考。

本书共14章，分为4个部分。第一部分概述信息与网络安全相关知识。第二部分（第2~6章）讲述信息安全技术相关内容，包括常规加密技术，DES数据加密标准，公钥加密技术，基于加密技术的数字签名、身份鉴别等网络安全应用，以及信息隐藏技术等。第三部分（第7~10章）介绍网络安全相关技术，这部分内容主要介绍网络安全的防御技术和相关的网络安全协议等。第四部分（第11~14章）介绍信息与网络检测的相关实用技术，包括入侵检测技术、信息获取技术、安全信息取证和逆向工程等。

本书由程光担任主编。第1~6章、第11~12章由程光编写，第7~10章由张艳丽、程光共同编写，第13、14章由江洁欣、程光共同编写。本书最后由程光进行统稿。

由于信息与网络安全内容发展很快，无法确保将这个领域中的精华全部荟萃。加上作者的水平有限，书中内容有不当之处，敬请广大读者批评指正。

程　光

2008年5月于东南大学

目　录

第 1 章　信息与网络安全概述

本章要点

- ☑ 信息与网络安全现状
- ☑ 常见的网络攻击方法
- ☑ 网络安全威胁和攻击
- ☑ 安全政策和机制
- ☑ 安全标准和组织

我们现在生活在各种类型的电子信息和网络环境中，如：办公室和家庭的个人计算机；数据库服务器，如数据库、Web 服务器；电话系统；移动电话；便携式设备，如笔记本、PDA（Personal Digital Assistant，个人数字助理）、GPS（Global Positioning System，全球定位系统）；无线通信网络；公用信息系统，如银行 ATM 系统；有线电视系统；汽车和家庭设备中内嵌式系统；智能卡系统；等等。在享受网络丰富的信息资源给用户带来了极大方便的同时，计算机病毒、黑客入侵及木马控制、垃圾邮件等也给互联网的运行系统、基于互联网的重要应用系统和广大互联网用户带来了越来越多的麻烦。因此，保证互联网的健康发展，信息与网络安全是首先要解决的问题。

网络安全面临着多个方面的挑战：

- 保护大量不同的安全系统；
- 保护不同系统之间的接口；
- 不同的系统具有不同的安全目标和需求；
- 攻击者寻找系统中最薄弱的环节进行攻击；
- 需要保护系统中每个环节的安全性；
- 维护系统的稳定性；
- 控制系统安全维护的代价等。

另外，在网络防御方面，人们所要面临的安全问题往往是难以预测的，因此需要网络安全人员保持警惕，以使信息网络风险降低至最小程度。同时反病毒措施落后于病毒的发展速度已经是不争的事实，因此仅仅依靠给系统打补丁、安装网络防火墙等常规措施，将使用户长期处于被动地位。

1.1　信息与网络安全现状

1.1.1　互联网的重要性

图 1-1 所示为互联网应用与时间的关系，它表明互联网变得越来越重要，对人们的生活影

响也越来越大。互联网开始仅仅提供信息交流的工具，如发送、接收电子邮件，然后逐渐发展成为信息发布的平台，再发展成和人们生活密切相关的电子交易平台。另外，互联网的应用也越来越复杂，最初的 E-mail 应用不涉及任何安全问题，只是简单的数据收发；现在的电子交易涉及很多网络安全技术，如加密、鉴别、访问控制、数据签名，等等。

图 1-1 互联网应用和时间的关系

图 1-2 是 Internet 软件联盟（Internet Software Consortium，ISC）2007 年 7 月根据 DNS（Domain Name System，域名系统）服务器中主机数据，统计的全球互联网主机的数量。1993 年 1 月全世界互联网主机是 1 313 000 台，到 2008 年 1 月发展到有 541 677 360 台，互联网主机的发展速度以指数方式递增。互联网主机的增加，使得互联网能够影响更多人的生活和工作，同时互联网的安全也愈加重要。

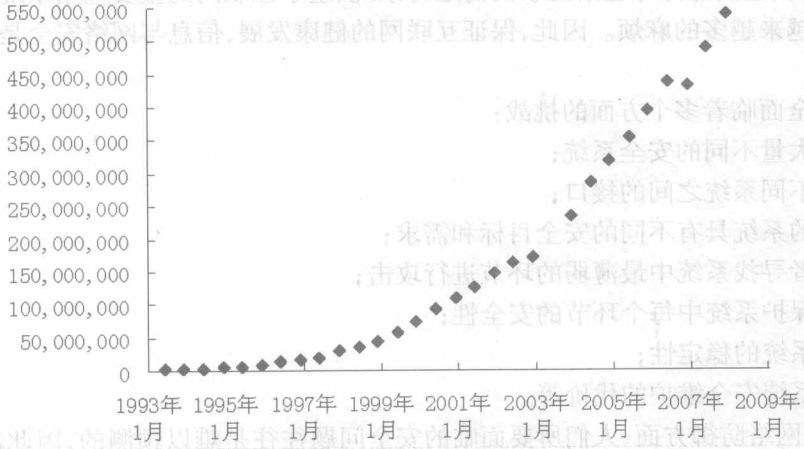

图 1-2 Internet 软件联盟统计的全球互联网主机数量

1.1.2 我国互联网现状

根据中国互联网络信息中心（China Internet Network Information Center，CNNIC）的调查分析，截至 2007 年 12 月 31 日，中国网民的数量已经达到 2.1 亿（见图 1-3），位居世界第二，是仅次于美国（2.15 亿）的网民规模。比 2006 年年末新增了 7300 万网民。2007 年中国网民年增长率达到 53.3%，步入新一轮的快速增长阶段。