普通高等教育“十一五”国家级规划教材

张　永　范通让　主编

计算机信息安全实践教程

21世纪计算机科学与技术实践型教程

丛书主编　陈明

清华大学出版社

普通高等教育“十一五”国家级规划教材

张 永 范通让 主编

计算机信息安全实践教程

清华大学出版社
北京

21世纪计算机科学与技术实践型教程
丛书主编 陈明

内 容 简 介

本书首先从计算机信息安全典型案例入手，着重介绍信息安全面临的威胁种类、信息安全技术体系、信息安全防护等级、信息安全相关技术和信息安全职业标准等知识，具有比较鲜明的特点。全书共分为10章，在章节组合和内容选取上，对一些比较抽象的原理部分做了弱化，相关技术都从案例操作进行导入，有比较强的可操作性。

本书对信息安全职业和职业能力做了比较全面的介绍，对一些有代表性的标准、规范做了重点介绍，这些知识都非常有利于培养从业人员的职业素养。

本书在内容组织方面，具有图文并茂、与实际生活联系紧密的特点，将比较抽象的专业知识尽可能地用浅显易懂的叙述呈现出来，十分符合现代读者的阅读习惯。

本书适合作为应用型本科、高职高专院校计算机信息安全相关专业的教材，也可供计算机信息安全技术爱好者自学使用。

图书在版编目（CIP）数据

计算机信息安全实践教程/张永，范通让主编. --北京：清华大学出版社，2016
21世纪计算机科学与技术实践型教程
ISBN 978-7-302-42269-3

Ⅰ. ①计… Ⅱ. ①张… ②范… Ⅲ. ①电子计算机－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第283787号

责任编辑：谢　琛　薛　阳
封面设计：何凤霞
责任校对：焦丽丽
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 装 者：三河市中晟雅豪印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：15.75　　**字　　数**：363千字
版　　次：2016年3月第1版　　**印　　次**：2016年3月第1次印刷
印　　数：1～2000
定　　价：34.50元

产品编号：061714-01

《21世纪计算机科学与技术实践型教程》

编辑委员会

《21世纪计算机科学与技术实践型教程》

序

21世纪影响世界的三大关键技术：以计算机和网络为代表的信息技术；以基因工程为代表的生命科学和生物技术；以纳米技术为代表的新型材料技术。信息技术居三大关键技术之首。国民经济的发展采取信息化带动现代化的方针，要求在所有领域中迅速推广信息技术，导致需要大量的计算机科学与技术领域的优秀人才。

计算机科学与技术的广泛应用是计算机学科发展的原动力，计算机科学是一门应用科学。因此，计算机学科的优秀人才不仅应具有坚实的科学理论基础，而且更重要的是能将理论与实践相结合，并具有解决实际问题的能力。培养计算机科学与技术的优秀人才是社会的需要、国民经济发展的需要。

制订科学的教学计划对于培养计算机科学与技术人才十分重要，而教材的选择是实施教学计划的一个重要组成部分，《21世纪计算机科学与技术实践型教程》主要考虑了下述两方面。

一方面，高等学校的计算机科学与技术专业的学生，在学习了基本的必修课和部分选修课程之后，立刻进行计算机应用系统的软件和硬件开发与应用尚存在一些困难，而《21世纪计算机科学与技术实践型教程》就是为了填补这部分空白。将理论与实际联系起来，使学生不仅学会了计算机科学理论，而且也学会了应用这些理论解决实际问题。

另一方面，计算机科学与技术专业的课程内容需要经过实践练习，才能深刻理解和掌握。因此，本套教材增强了实践性、应用性和可理解性，并在体例上做了改进——使用案例说明。

实践型教学占有重要的位置，不仅体现了理论和实践紧密结合的学科特征，而且对于提高学生的综合素质，培养学生的创新精神与实践能力有特殊的作用。因此，研究和撰写实践型教材是必需的，也是十分重要的任务。优秀的教材是保证高水平教学的重要因素，选择水平高、内容新、实践性强的教材可以促进课堂教学质量的快速提升。在教学中，应用实践型教材可以增强学生的认知能力、创新能力、实践能力以及团队协作和交流表达能力。

实践型教材应由教学经验丰富、实际应用经验丰富的教师撰写。此系列教材的作者不但从事多年的计算机教学，而且参加并完成了多项计算机类的科研项目，他们把积累的经验、知识、智慧、素质融于教材中，奉献给计算机科学与技术的教学。

我们在组织本系列教材过程中，虽然经过了详细的思考和讨论，但毕竟是初步的尝试，不完善甚至缺陷不可避免，敬请读者指正。

本系列教材主编　陈明

2005年1月于北京

前　言

信息安全相关技术对现代信息社会的重要意义不言而喻，世界各国都对其十分重视。小到个人信息安全保障，大到亿万用户的企业级商业信息系统，甚至国家级的信息安全保障，都离不开信息安全技术的支撑。

然而如果将信息安全的相关技术和从业人员标准进行具体化，我们会发现这实际上是一个非常繁杂的体系，信息安全技术几乎是包罗万象的，对从业人员的技术等级要求也是参差不齐的，一个有志于在此行业进行从业的人员，在开始进行学习的时候几乎无法下手。对信息安全初级的从业人员来说，在实际工作当中对技术等级的要求并非高不可攀，职业素养才是更加重要的一环，它要求从业人员具有安全意识，知晓安全标准，遵守安全规范以及具有常规的安全技术等。上述要求无论是对初级从业者还是高级技术人员都同样适用。

本书依照现代学生的认知特点，遵从行业人员的素质规范要求，从大家比较熟悉的信息安全典型案例展开，逐次递进，符合人们的认知规律。全书共 10 章，主要包括信息安全技术概述、物理层安全技术、加密与解密技术、操作系统安全技术、数据库系统安全技术、网络安全技术、应用安全技术、病毒木马和间谍软件以及容灾与备份等。此外，本书还对信息安全职业与职业能力做了比较详细的介绍。全书各章节紧密联系实际，对相关技术介绍均具有比较强的可操作性，体现了典型的应用职业特色。

本书由南京信息职业技术学院计算机与软件学院张永、石家庄铁道大学范通让任主编，南京信息职业技术学院计算机与软件学院的闫冰和任俊新、南京市玄武中等专业学校沈斌任副主编，参与本书编写的还有史律、章春梅、许丽婷、王莉和马秀芳等资深一线教师。

在此书的编写过程中，还得到了北京西普阳光教育科技有限公司产品技术总监林雪纲博士的诚挚帮助与指导，对他的无私贡献和宝贵建议表示真诚的感谢。

本书的编写参考了大量的书籍、期刊以及互联网上的资源，为此，我们向有关的作者、编者和译者表示真诚的感谢。

还要感谢清华大学出版社的相关编辑、出版人员，是他们的辛勤工作才使本书得以出版。

由于计算机信息安全技术的变化日新月异，新事物层出不穷，加之编者水平所限，书中疏漏之处在所难免，恳请读者不吝批评指正。

编　者

2015 年 6 月

目　　录

第 1 章　计算机信息安全概述

➢ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 查找信息安全的典型案例；
- 了解信息安全所面临的威胁类型；
- 查找信息安全技术体系方面的知识；
- 了解信息安全的防护等级。

➢ **本章教学目标**

本章的教学目标是：

- 了解信息安全所面临的各种威胁及其表现形式；
- 了解信息安全体系和防护等级方面的基本知识。

➢ **本章教学要点**

本章的教学要点包括：

- 信息安全面临的威胁种类；
- 计算机信息安全技术体系；
- 信息安全防护等级及其分类标准。

➢ **本章教学建议**

本章内容采用案例引导模式进行教学。

关于计算机信息安全，一般人听起来都会感觉很神秘，谈起来有些玄之又玄的样子。年轻人往往会非常好奇那些黑客的世界到底是什么样子，是否跟“黑客帝国”的电影所表现的那样玄妙而又难以理解呢？其实，信息安全跟每个人都息息相关，我们的日常生活，几乎天天都面临着信息安全方面的挑战。生活在信息时代的我们，电子信息交互流动已经成为一种生活常态，信息安全所面对的威胁前所未有。普通用户需要懂得一些信息安全方面的知识来保护自己，而专业用户需要更加精深的专业知识来为社会提供信息安全服务。无论是中国还是全世界，大家对信息安全的重视已上升到一个极高的层面。

1.1　计算机信息安全典型案例

本节介绍一些曾经发生过的信息安全方面的典型案例，通过这些案例，能够帮助大家初步建立信息安全的意识。

1.1.1 棱镜门

2013 年 6 月，美国前中央情报局(CIA)职员爱德华·斯诺登(见图 1.1)将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并告之媒体何时发表。按照设定的计划，2013 年 6 月 5 日，英国《卫报》先扔出了第一颗舆论炸弹：美国国家安全局有一项代号为“棱镜”(PRISM)的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。2013 年 6 月 6 日，美国《华盛顿邮报》披露称，过去 6 年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果和雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料(见图 1.2)。美国舆论随之哗然，世界为之震惊。

图 1.1 爱德华·斯诺登

图 1.2 “棱镜”计划示意图

这项代号为“棱镜”的高度机密行动此前从未对外公开。这是一起美国有史以来最大的监控事件，其侵犯的人群之广、程度之深让人咋舌。

2013 年 6 月 7 日，在加州圣何塞视察的美国总统奥巴马做出回应，公开承认该计划。在秘密项目披露之前，斯诺登已经离开美国，后经辗转，避难于俄罗斯。在此之后斯诺登又披露多项与“棱镜门”有关的秘密文件，美国政府在斯诺登持续爆料和国内国际对监控计划出现越来越多质疑声的巨大压力下，被迫主动解密与斯诺登泄露的“棱镜”网络监控计划及电话监听计划这两大秘密情报监控项目相关的多份文件。

经解密的资料显示，“棱镜”计划监控的对象和范围远超想象，几乎涵盖全世界各国，

侵害人民生活的每个层面。“棱镜”事件曝光之后，与此有关的苹果、思科、微软、谷歌和Facebook等公司纷纷发表声明，力证自己“清白”；欧盟各国感到“震惊”和“愤怒”；俄罗斯和中国等国家分别发表评论。几乎可以说是全球鼎沸，事件产生的影响至今余波未息。

1.1.2　病毒

2003年8月11日，全球爆发了著名的“冲击波”(Worm Blaster)病毒，该病毒利用在2003年7月21日公布的RPC漏洞进行传播，攻击Windows 2000\XP\Server 2003\NT4.0计算机系统。在短短的一周之内，“冲击波”病毒至少攻击了当时全球80%的Windows用户，使他们的计算机无法工作并反复重启(见图1.3)。大量企业用户也未能幸免。据事后统计，“冲击波”病毒及其变种在全球所造成的损失高达几百亿美元。“冲击波”蠕虫病毒原型的编写者至今仍未被发现，美国联邦调查局(FBI)仅仅逮捕了一个编写病毒变种“冲击波B”的18岁青年杰弗里·帕森(见图1.4)，西雅图一家地方法院判定帕森18个月有期徒刑。

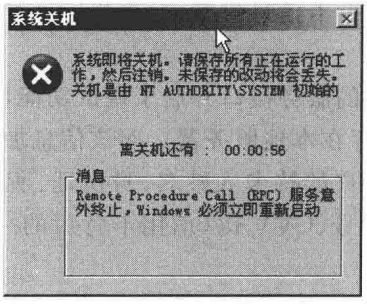

图1.3　“冲击波”病毒感染表现

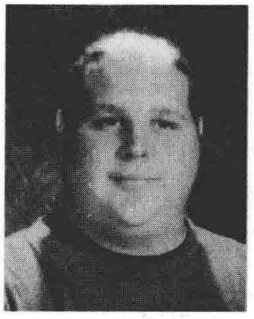

图1.4　杰弗里·帕森

1.1.3　黑客入侵

2011年7月29日，韩国通信委员会声称，黑客(见图1.5)袭击了韩国一家门户网站(Nate)和一家博客网站(Cyworld)，导致3500万名用户的信息泄露。被泄露的信息有姓名、账号(ID)、电子邮件地址、手机号码、密码以及身份证号码。这是韩国历史上遭到的最大规模的网络攻击。

1.1.4　木马盗号

2014年3月，有病毒团伙利用马航事件通过QQ和邮件传播盗号木马(见图1.6)，在盗取QQ密码后实施更多诈骗行为。此类盗号木马采用压缩包的形式，伪装成热门新闻事件最新进展、真相等，文件名包括“2014马航失联报道”等，通过QQ文件或邮件的方式传播，利用网民的好奇心，诱使其点击下载。一旦此类木马程序点击运行，就会弹出假冒的QQ“重新登录”窗口，诱使网民输入自己的QQ账号和密码，并将其发送到木马作者搭建的服务器上，不法分子盗取QQ后，会以冒充好友借钱等多种方式实施诈骗。

图 1.5 黑客(hacker)

图 1.6 木马盗号

1.1.5 电子交易

2014 年 3 月 22 日 18 点 18 分,一个编号为 54302 的漏洞报告被曝光在互联网安全问题反馈平台乌云(wooyun.org)之上,发布者是乌云的核心白帽子黑客“猪猪侠”。这份报告表明,携程网的一个漏洞会导致大量用户银行卡信息泄露,而这些信息可能直接引发盗刷等问题。

漏洞报告指出,携程将用于处理用户支付的服务接口开启了调试功能,使所有向银行验证持卡所有者接口传输的数据包均直接保存在本地服务器。而该信息加密级别并不够高,可以被黑客轻易获取。泄露的信息包括用户的持卡人姓名、身份证、所持银行卡类别(例如,招商银行信用卡、中国银行信用卡)、卡号、CVV 码(信用卡背后的一组数字)以及用于支付的 6 位密码。

3 月 23 日,携程网给出关于此事件的详细解释,“携程的技术开发人员为了排查系统疑问在线上环境开启支付调试功能,留下了临时日志,因疏忽未能及时删除,目前,这些信息已经删除。经过排查,仅漏洞发现者做了测试下载,共涉及 93 名存在风险的携程用户。没有接到携程电话通知的用户,个人信息是安全的。”

虽然此次事件由于漏洞被及时发现所以没有造成非常严重的直接损失,但是它确实表明这样一个严峻的现实:随着电子交易的普及和便捷,越来越多的人依赖电子交易完成商务活动,而这些敏感信息一旦造成泄露,后果简直是难以估量的。

1.1.6 手机入侵

2014 年 9 月 7 日,中央电视台新闻频道曝光了一款手机上的间谍软件(见图 1.7),看似正常的办公软件,实际上却能在用户不知情的情况下盗取隐私信息,甚至网银。据测试,该款软件图标就是正常的移动办公文件表格,而一旦安装点击,手机里的联系人和短信信息立即会被传到黑客指定的邮箱。短信、联系人姓名和电话分毫不差地被黑客所窃取。该病毒另一个可怕之处在于,它不仅可以获取

图 1.7 手机间谍软件

最新的短信和联系人信息，而且还能拦截用户手机接收到的有关提示短信。这样银行等金融机构发给用户的提示短信等重要信息，就可能被这款病毒软件劫持，取得了这些信息的不法分子可以在用户完全不知情的情况下，窃取用户银行卡中的钱财。

随着我国手机网民数量的持续增长，网民使用手机上网的比例已经超过使用电脑上网的比例，智能手机已经成为最大的上网通道。由于手机中存在大量的隐私资料和敏感信息，一旦泄漏就可能给用户造成巨大损失。不法黑客也看到了这一点，基于智能手机的各类病毒、跟踪定位程序、监听程序和间谍软件等层出不穷，给用户造成了巨大的危害。

1.1.7　数据损坏灾难

2008年3月19日，美国威斯康辛数据中心被火烧得一塌糊涂（见图1.8）。根据事后统计，这次大火烧掉了75台服务器、路由器和交换机，当地大量的站点都瘫痪。该数据中心属于当地一家名为Camera Corner/Connecting Point的公司所有，该公司主营网站托管和其他IT服务。

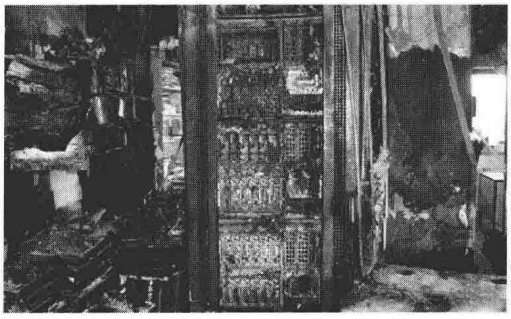

图1.8　火烧威斯康辛数据中心

这次事故给当地网站带来了巨大损失。耗时10天的修缮和重新部署，才使得这些网站得以上线。

由于现代信息社会严重依赖于保存在电子设备中的各种数据，所以有些重要的数据一旦损坏，会造成广泛而严重的后果。

自计算机系统广泛应用以来，发生过的数据损坏灾难不计其数，尤其是一些重大的自然灾害，例如地震、飓风和洪水等具有毁灭性的破坏力。

1.1.8　内部人员泄密

据媒体报道，国内某电信运营商的第三方合作公司技术人员，因个人利益驱使，在处理技术服务期间勾结内部员工，利用工作之便潜入电信运营商办公内网，非法下载几百万条核心数据并出售牟取暴利。

近年来，信息安全泄密事件频频发生，有信息系统被黑客从外部攻破的，也有内部人员过失泄密或主动窃密的。在许多情况下，内部人员造成的泄密危害要比黑客从外部侵入造成的危害高得多。近年来比较典型的内部人员泄密事件还包括中国人寿80万份意外险保单信息泄露事件和圆通快递百万客户信息泄露事件等。