★ 刘会霞　等编著

网络犯罪与信息安全

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络犯罪与信息安全

刘会霞　等编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书以信息安全和网络犯罪侦查取证为主要内容，以帮助学习者防范网络危害为主要目的，不涉及过多和过深的信息安全技术理论和空洞生涩的专业术语。

全书共分 10 章。第 1 章全面介绍信息安全和网络犯罪侦查的基础知识，第 2 章讲解操作系统存在的安全问题和防护方法，第 3 章介绍网络常用服务的安全性问题，第 4 章讲解网络攻击与防御技术，第 5 章介绍防治计算机网络病毒和木马的基本方法，第 6 章讲解信息加密和网络中的密码应用，第 7 章讲解无线网络的安全问题，第 8 章讲解网络犯罪侦查中涉及的问题，第 9 章介绍电子数据取证技术，第 10 章讲解信息安全管理技术。

全书以案例引领的模式编写，学习内容围绕实际工作中出现的问题展开，使读者能够有目的地学习相关知识和技能。

本书可作为高等院校计算机网络安全课程和网络犯罪侦查取证课程的教材，也可作为普通计算机用户学习网络安全防护技能的教科书。

图书在版编目（CIP）数据

网络犯罪与信息安全/刘会霞等编著. —北京：电子工业出版社，2014.9

ISBN 978-7-121-24260-1

Ⅰ. ①网… Ⅱ. ①刘… Ⅲ. ①互联网络—计算机犯罪—高等学校—教材②互联网络—安全技术—高等学校—教材 Ⅳ. ①D914②TP393.08

中国版本图书馆 CIP 数据核字（2014）第 198212 号

策划编辑：施玉新
责任编辑：周宏敏
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：20.75　字数：629 千字
版　　次：2014 年 9 月第 1 版
印　　次：2014 年 9 月第 1 次印刷
定　　价：46.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

21 世纪是信息时代，现今人们利用计算机网络工作学习、游戏娱乐，充分享受计算机网络带来的快乐；同时，人类社会也面临来自网络的威胁。网络病毒、网络攻击、信息盗窃、网络侵权、网络战争等问题，使人们不得不把网络安全提升到国家安全的战略高度予以关注。许多重大黑客事件表明，计算机网络存在严重的安全漏洞，而中国计算机网络的安全防护能力尤其薄弱，据报道，中国 95%以上的与 Internet 相连的主机曾遭受过黑客攻击，2014 年 5 月 26 日至 6 月 1 日，中国大陆被篡改的网站数量达 6092 个，比前一周增长 51.9%。由此可见，作为计算机网络的应用者，如果不了解网络安全防护知识、不具备安全应用防护技能，就很难有效可靠地使用计算机网络，所以普及计算机网络安全知识是大势所趋。

本书是一本以信息安全和网络犯罪侦查基本原理为基础，以网络安全和网络犯罪侦查基本技术为落脚点，以贴近网络安全应用实际内容为对象的计算机网络安全技术基础性教材。书中内容没有涉及过多和过深的信息安全技术理论和空洞生涩的信息安全专业术语，对可操作的内容也尽量列出完整的操作过程，期望对读者提高计算机网络安全防护技能有所帮助。

全书以案例引领的模式编写，学习内容围绕实际工作出现的各种问题，使读者不但可以学会网络安全防护知识和技能，更能实现技能学习与社会应用的无缝对接，达到学以致用的目的。

全书共分 10 章。第 1 章全面介绍信息安全和网络犯罪侦查的基础知识，帮助读者建立网络安全防护理论的整体概念，认识网络犯罪问题。第 2 章讲解操作系统存在的安全问题和防护方法，帮助读者有效保护计算机操作系统和手机系统的安全。第 3 章讲解网络常用服务的安全性问题，帮助读者了解网络应用中存在的安全问题，安全使用网络。第 4 章讲解网络攻击与防御技术，帮助读者了解攻击手段和必要的防护方法。第 5 章介绍防治计算机网络病毒和木马的基本方法，教会计算机用户高效率地查找、清除计算机病毒和木马的技巧。第 6 章讲解信息加密和网络中的密码应用，帮助读者了解信息加密的概念，掌握实用的加/解密技术，有效保护应用环境和信息的安全。第 7 章讲解无线网络的安全问题，帮助读者安全使用无线网络。第 8 章讲解网络犯罪侦查中涉及的问题，帮助读者了解侦查过程涉及的内容和方法。第 9 章介绍电子数据取证技术，帮助读者有效获取电子证据。第 10 章讲解信息安全管理技术，帮助读者了解安全管理涉及的基本内容和方法，树立安全管理的基本理念，学会利用最基本的安全管理方法和技术安全管理网络。

本书由刘会霞、谭建伟、孙莉、李玲玲、秦志红等编写，朱一、王长杰和王勇参与了书中部分

章节的编写工作。全书由刘会霞、谭建伟统稿。河南工程学院李建教授、河南司法警官职业学院王慧斌博士对书稿进行了认真审阅，提出了许多意见和建议，在此深表感谢。

本书作者对书中引用文献和案例的作者表示深深的敬意和由衷的感谢。

由于编者水平有限，编写时间仓促，加之对信息安全和网络犯罪侦查问题的认识、理解存在局限性，本书难免存在错误和不当之处，敬请读者批评指正。

编　者

2014 年 6 月

反侵权盗版声明

目　录

第 1 章　信息安全概述

计算机网络技术的快速发展为信息传递提供了便利条件，也为扩大计算机应用领域提供了基本保障，但是，在计算机网络应用层次不断提高、应用领域不断扩大的同时，安全管理也成为全球共同关注的话题，“斯诺登”曝光美国监听事件更加剧了人们对信息安全的担忧。信息资源在网络环境传播、共享使用的过程中，一些重要的信息可能被网络黑客觊觎而被窃取、篡改，也可能因为攻击行为导致网络崩溃出现丢失，诸如此类问题影响了信息产业正常有序的发展，严重时甚至会造成人类社会的动荡。因此，保证网络安全、有序运行是发挥网络作用的基础，保证信息安全也是应用的前提。2010 年以来，世界各国相继制定和大幅调整网络安全战略，增设专门机构，加大人员和资金投入，最大限度地维护网络信息的安全和利益。

网络犯罪案例

案例 1：罗伯特制作“蠕虫”事件

“蠕虫”病毒的始作俑者是美国康奈尔大学计算机科学系一年级研究生罗伯特• 潘• 莫里斯。罗伯特从小就表现出了超出常人的计算机天分，在康奈尔大学有“孤独的才华横溢的程序专家”的名声。

在 20 世纪 80 年代，苹果 II 型 PC 首次出现病毒，当时人们对计算机病毒并不十分了解，而此时罗伯特心中的目标就是编写一个无害的能够传染尽可能多的计算机的病毒。1988 年 10 月，罗伯特开始了自己的计划，他一面集中精力编写病毒程序，另一方面寻找计算机系统中可以施放病毒程序的漏洞。11 月 2 日美国东部标准时间晚上 7 点 30 分，罗伯特完成了病毒的编写工作，一个小时后，他在麻省理工学院人工智能实验室的计算机上以 RTM 名登录，并下达了病毒执行指令。在罗伯特按下“ENTER”键的瞬间，病毒开始扩散，几分钟之内已在网上肆虐，一台台计算机被感染病毒陷入瘫痪。罗伯特吃完晚饭去检查病毒的进展情况，发现计算机已经毫无反应，他意识到大事不妙，病毒已经失去了控制，这时才想起编写病毒时把复制参数设置错了。

这一事件使互联网上 10%的计算机受到感染，美国的直接经济损失将近 1 亿美元，罗伯特也因此受到控告，被判 3 年缓刑、1 万美元罚款和 400 小时的社区服务。

思考：病毒制作者的行为可能造成什么样的可怕后果？

案例 2：江西卫生厅考试中心数据库被非法操作事件

2008 年 6 月，江西省公安厅网监总队接到江西省卫生厅考试中心报案。称该厅网站的医师资格查询数据库被他人非法操作，有人修改了数据库内容并制作虚假《医师资格证书》牟利。6 月初，有人持假《医师资格证书》到浙江省相关部门办理《行医许可证》，虽经专门机构认定证书是假的，但查询江西省卫生厅网上数据库发现确有其人，于是向江西省卫生厅核实。江西省卫生厅在检查考试中心网站时发现，几个月前该网站曾遭到黑客侵入，数据库被大量篡改，遂向警方报案。

6 月 19 日，江西省公安厅网监总队立案侦查此案。通过对被攻击受控制服务器的现场勘验，民警发现黑客于 3 月 26 日起入侵江西省卫生厅网站，并上传网站后门程序对网站服务器进行控制。经查，黑客是利用境外新加坡的 IP 地址将篡改的数据上传至数据库，手段非常隐蔽，有较高的反追查意识。办案民警经过几天的艰苦侦查，终于将黑客在网上的其他虚拟身份锁定，并最终确定犯罪嫌疑人上网的地点。

6 月 24 日，民警展开抓捕行动，在某租住地将犯罪嫌疑人李某及其同伙 5 人当场抓获，缴获作案用笔记本电脑 4 台，打印机 1 台，各类银行卡 25 张，虚假身份证 13 张，虚假空白医师资格证书 6

本，医师执业证书1本，建造师证书2本。随后，民警又在武汉将另一名主要犯罪嫌疑人王某抓获。

据警方介绍，2007年，就读于南昌某高校计算机专业的李某因毕业论文没有通过，无法取得毕业证书，遂产生贩卖假证的念头，只是苦于网上数据库查不到这些假证。2008年3月，李某发现网上要求办理医师资格证书及毕业证书的信息非常多，于是在网上找到王某，要求王某侵入一些网站，在取得使用权限后交给自己使用，然后通过入侵修改数据—办理假证—贩卖假证—用假证办理从业许可证等环节从中非法牟利。

经查，王某先后入侵江西省卫生厅考试中心网站、湖北省卫生厅网站、贵州人事考试网、四川人事考试网、湖北荆州人事局网站、江苏自考网、辽宁省建设厅网站等10余个网站，并以每个网站管理员权限5000元至8000元的价格卖给李某。李某则对下线收取代理费，每添加一个客户收取1000元至2500元不等。据李某交代，他共添加了包括江西省卫生厅网站在内的网站数据700余个，获利200余万元。据一名受害者反映，为了弄到一个上网可查的假证书，他就花了8000多元。

思考：此案暴露出了网络应用中的哪些不安全问题？危害性有哪些？

案例3：以奥运为名的网络诈骗案

2008年1月4日，南京公安局网络警察支队接到举报，称有人假冒2008年奥运会名义建立网站，实施诈骗活动。南京警方经过缜密调查，于1月28日在海南儋州抓获许某、陈某等9名犯罪嫌疑人。

据该团伙成员交代，2007年12月底，许某和陈某等建立了网站，假冒“系统提示”信息，向众多网络游戏玩家发送中奖消息。当游戏玩家登录他们建立的网站后，中奖页面会显示用户中得18 800元至38 800元不等的“惊喜奖金”及奥运会门票一张，但领奖的前提是向一个银行卡号汇款998元作为手续费。案发时，全国各地共有100多名受害者向涉案银行账户汇款共30余万元。

思考：为什么网络诈骗的危害性比传统形式的诈骗更严重？

案例4：美国加州5名用户指控Facebook违反隐私法事件

据国外媒体报道，2009年8月美国加利福尼亚州5名Facebook用户向奥兰治县法院提起民事诉讼，指控Facebook违反该州隐私法，并在如何使用个人信息方面误导用户。

原告要求Facebook支付赔偿金和诉讼费用，并要求陪审团参与审理。原告诉称，Facebook将用户提交的个人信息提供给第三方，违反了加州隐私与网络隐私法。该网站还在未向用户披露的情况下进行数据挖掘等工作。5名原告分别包括1名专业摄影师、2名13岁以下的儿童、1名原Facebook用户以及1名洛杉矶女演员兼模特。

Facebook发言人巴里• 斯彻内特拒绝对此做出评论，他表示：“我们认为该指控毫无根据，并将积极应诉。”Facebook目前的用户已增长至2亿多，隐私保护方面的问题日益突出。2009年初，由于数万名用户抗议Facebook滥用在该网站上共享的个人信息，该网站宣布调整隐私控制方式，转而让用户选择多种不同的隐私政策。Facebook于2月表示，在采取新的隐私政策前，将允许用户对隐私、内容所有者以及共享方面的调整进行评估、评价和投票。2007年末，Facebook推出了“Beacon”跟踪工具，该工具可以在用户毫不知情的情况下将其行为发布到其他网站，在自由主义草根组织MoveOn和会员的压力、抗议下，网站最终允许用户关闭该工具。

1.1 信息安全的内涵和意义

从社会学的角度看，信息安全是关系国家安全、社会稳定、民族文化继承和发扬的重要问题。从技术的角度看，它又是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，内容广泛且技术复杂，因此也造成了信息安全保障工作的复杂性。

在人类社会信息化建设的进程中，信息安全问题是一项长期而复杂的社会系统工程，既需要管

理者充分运用先进的管理手段和专门技术进行专项治理，也需要应用者提高安全防护意识和安全应用技术，以有效保护应用环节的安全。或许很多人都听说过或知道“信息安全”这一热门词汇，但是“信息安全”究竟涵盖哪些内容？是哪些因素导致了信息应用的不安全？人类社会需要什么样的安全？这些问题未必人人清楚。本节将帮助读者了解信息安全的基本概念，全面或重新认识信息安全。

1.1.1　产生信息危害的原因

只有充分了解发生信息危害的基本原因，才能更好地找出应对策略，从根本上解决信息安全危害问题。

1．危害信息安全的形式

对于网络信息应用领域的“危害”，可以从两个方面理解，一是各种外在或内在因素对网络信息造成的危害，二是利用网络信息对人类社会产生的危害。前者又分为人为与非人为两种，非人为危害主要指自然灾害对网络信息造成的危害，如地震、水灾、火灾、战争等原因出现的网络中断、系统破坏、数据丢失等。人为危害是指对网络信息人为攻击，达到破坏、欺骗、窃取数据等目的。与其他危害相比，计算机应用领域的危害包含有较强的技术性，影响范围较大，由此造成的后果也更为严重。

危害信息安全的表现形式多种多样，危害后果和抑制手段也不尽相同，这里归类列出常见的几种，旨在帮助大家认识出现危害事件的严重性，提高信息安全防护意识。

（1）自然灾害

自然灾害对网络信息造成危害的事件在世界各国时有发生。如果建造机房、安装设备时没有考虑防水、防火、防静电、抗震、避雷等问题，工作环境抵御自然灾害的能力会很差，发生灾害后有可能给网络系统造成灭顶之灾。例如，辽宁某铁路局控制机房因缺乏雷电防护设施曾 3 次遭受雷击，致使控制系统和一些终端设备损坏，严重影响了正常编组运输。日本东京电信局在电缆维护时，工人操作不慎造成火灾，由于缺乏有效的火灾控制手段，大火持续了 16 小时，烧毁了大量的通信设备，导致数家银行和邮局的计算机通信网络中断，银行分布在各地的自动付款机被迫停机，邮局的一些业务只能暂停。

（2）系统漏洞

计算机网络系统本身存在的致命漏洞是威胁信息安全的重要因素。网络系统大型化使控制管理的复杂程度不断增加，隐藏其中的漏洞也越来越多，它们有可能引起网络系统崩溃，也有可能成为渗透网络系统的工具或通道。例如，微软公司曾在 IE 浏览器安全建议书中证实，IE 浏览器存在安全漏洞，由此可能引起零位指针失效或内存失效等错误。思科曾承认它的 Internetwork 操作系统存在处理 IPv6 包的漏洞，若向受影响的思科设备发送特制的 IPv6 包，有可能迫使设备重新启动，导致 DoS 攻击。

（3）操作失误

工作人员缺乏责任心或因专业知识滞后造成操作失误，也会导致意想不到的灾难事件。例如，由于美国防空司令部指挥中心计算机操作员输入数据错误，引起防空警报，最高指挥部随即命令 1000 枚核导弹进入待发状态，核战争一触即发。香港联合交易所工作人员在停电后按停警钟时，意外地按下后备电源的“紧急停止掣”，截断了大堂及自动对盘系统主机的电源，停电使系统停止工作 4 分 58 秒，结果导致收市延误，在延误收市的 4 分 58 秒期间，额外交易 1099 宗，成交额约 1 亿多元。延误时间内交易的合法性引起了巨大争论。

（4）病毒侵袭

计算机病毒的产生和全球性蔓延对信息安全应用构成了严重威胁，且已经造成了巨大的损失，计算机病毒的危害之大，不亚于人类社会发生的瘟疫。台湾大学生陈盈豪制造的“CIH”病毒，首次发作就使全球约 6000 万台计算机受害。“爱虫”病毒发作，全球损失约 100 亿美元。某省财政厅

财务管理系统感染病毒，破坏了3年的财务数据，造成无法挽回的巨大损失。

（5）人为恶意破坏

人为恶意的攻击、破坏是威胁信息安全的重要原因，也是最难控制和防范的危害因素。此种危害的表现形式很多，有对着计算机设备撒尿、浇油漆的物理破坏，有放置逻辑炸弹的应用系统破坏，有格式化磁盘的信息破坏，有篡改信息、盗窃程序数据的个人牟利行为，也有侵入重要、机密信息系统严重危害国家安全的重大事件。

（6）网络欺诈

网络欺诈已成为阻碍应用的重要顽疾，现在的网络不但是滋生欺诈性犯罪的新土壤，花样繁多、数量巨大的网络欺诈内容也严重影响了人们对网络信息的信任度。

（7）网络传黄

在互联网的有害信息中，传播面最为广泛的就是网络色情信息。资料统计显示，互联网上的色情网站有420万之多，占全部网站的12%，色情网页约有3.72亿个，每天色情主题搜索约6800万次，占全部搜索问题的25%。大量的不良信息对青少年网民比例高于世界平均水平的中国，已经产生了严重的恶果，网络也成为引发一系列社会问题的根源。

（8）网络赌博

2009年以来，全国破获了多起网络赌博案件，涉案金额之巨、危害之大令人触目惊心。湖南省赌博案中的涉案金额高达百亿元以上，上海赌博案中的短期投注金额高达66亿元，这其中的大部分投注赌资通过网络流向境外，网络赌博已经成为一种严重的“灾害”，成为危害国家经济建设和社会治安稳定的重要因素。

2. 发生危害信息安全事件的诱因

危害信息安全事件的发生数量居高不下，且逐年增加，说明危害信息安全有较为特殊的诱发原因，值得深究，认清引发危害信息安全事件的原因也有助于开展防范工作。

（1）网络系统本身存在脆弱性缺陷

计算机网络系统本身的脆弱性是诱发危害网络信息安全事件最根本的原因。计算机以高速度、高精度处理信息见长，它有许多其他设备不能比拟的优点，如信息存储密度高、易修改、能共享、网络传递方便等，正是这些优点使计算机备受人们青睐。也正是这些特点使计算机具有先天的脆弱性，高存储密度使处理大量信息成为可能，而在大量信息中隐藏少量非法信息不易察觉，信息一旦丢失损失会很惨重；信息易修改的特性给正常工作带来很多方便，修改后不留痕迹又使犯罪分子有机可乘，使追查犯罪困难重重；网络传递、共享能使人们快速、充分地利用信息资源，但信息传递过程中的电磁泄露、搭线窃听、接收信息对象的甄别困难等问题，又使信息安全控制难以把握。

计算机网络系统的脆弱性和计算机技术的开放性，使针对网络系统的危害易于发生，而防护的薄弱又给了危害行为人可乘之机，所以计算机网络系统的脆弱性不可避免地导致了危害网络安全事件。

（2）网络系统存在管理的复杂性问题

计算机网络系统的功能日益强大，计算机软、硬件的复杂程度随之成倍增长，计算机网络系统的管理也日趋复杂化。正是因为网络和计算机信息系统具有管理复杂性，工作中稍有不慎或管理策略不当，都会使网络系统出现安全隐患，这些不易察觉的安全漏洞，对拥有高技术、法制观念不强、时刻想捞取不法利益者是不小的诱惑，对刻意显示自己才能的人来说也是不可多得的机会。

计算机网络系统管理的复杂性使管理难度增大，同时，保证网络安全的难度也增大。这必然导致网络的安全性相对下降，使非法渗透网络系统更为容易，更多的人有机会、有可能使用计算机网络或针对计算机网络从事非法活动。危害信息安全事件数量的居高不下和网络系统管理复杂性有直接关系。

（3）网络信息的重要性使之成为攻击目标

计算机应用环境逐渐增多，使存储于其中的信息量和信息重要程度相应增加，许多信息和财富