

知雨科技 编著

# 黑客

# 攻防大曝光

## 社会工程学、计算机黑客攻防、 移动黑客攻防技术揭秘

### Hacking Revelations:

Social Engineering and the Hacker Attack and Defense  
Technology of Computer and Mobile Phone

#### 内容全面，范例丰富：

本书通过 215 个操作范例，全面揭秘网络安全技术，内容涉及社会工程学、计算机黑客攻防和移动黑客攻防三方面，理论和实践并重。

#### 一步一图，讲解细致：

本书从零起步，步步深入，采用一步一图的方式讲解，便于读者轻松读懂并跟随操作，提高学习效率。

#### 超值配套，轻松入门：

本书配套资源包含 120 分钟多媒体视频和《Windows 10 系统安全与维护手册》电子书等，直观易懂，帮助读者快速掌握黑客攻防技术。



机械工业出版社  
CHINA MACHINE PRESS

网络安全技术丛书

# 黑客攻防大曝光

——社会工程学、计算机黑客攻防、移动黑客攻防技术揭秘

知雨科技 编著



机械工业出版社

本书介绍了社会工程学、计算机与手机安全相关的多方面知识。主要内容分为三部分：第一部分为社会工程学，分为 4 章，介绍了社会工程学基础、信息收集和搜索、个人信息安全、商业信息安全；第二部分为计算机黑客攻防，分为 17 章，介绍了网络安全技术基础、网络钓鱼攻击揭秘、信息的扫描与嗅探揭秘、病毒攻防、木马攻防、密码攻防、计算机后门技术、系统漏洞攻防、网站安全防护、局域网攻防、QQ 安全防护、网络代理与追踪技术、远程控制技术、入侵痕迹清除技术、间谍软件的清除和系统清理、系统和数据的备份与恢复、加强网络支付工具的安全；第三部分为移动黑客攻防，分为 8 章，介绍了移动终端攻防基础、iOS 操作系统、Android 操作系统、手机病毒与木马攻防、无线通信技术之蓝牙、无线通信技术之 Wi-Fi、手机游戏安全、移动支付安全。

本书内容丰富全面，适用于计算机初学者，也适用于计算机维护人员、IT 从业人员以及对黑客攻防与网络安全维护感兴趣的计算机中级用户，各大计算机培训班也可以将其作为辅导用书。

## 图书在版编目 (CIP) 数据

黑客攻防大曝光：社会工程学、计算机黑客攻防、移动黑客攻防技术揭秘 / 知雨科技编著. —北京：机械工业出版社，2017.5  
(网络安全技术丛书)

ISBN 978-7-111-56502-4

I. ①黑… II. ①知… III. ①黑客—网络防御 IV. ①TP393.081

中国版本图书馆 CIP 数据核字 (2017) 第 069778 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策划编辑：王海霞 责任编辑：王海霞

责任校对：张艳霞 责任印制：李 飞

北京机工印刷厂印刷 (三河市南杨庄国丰装订厂装订)

2017 年 5 月第 1 版·第 1 次印刷

184mm×260mm·30.5 印张·749 千字

0001—4000 册

标准书号：ISBN 978-7-111-56502-4

定价：89.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换  
电话服务 网络服务

服务咨询热线：(010) 88361066 机工官网：[www.cmpbook.com](http://www.cmpbook.com)

读者购书热线：(010) 68326294 机工官博：[weibo.com/cmp1952](http://weibo.com/cmp1952)

(010) 88379203 教育服务网：[www.cmpedu.com](http://www.cmpedu.com)

封面无防伪标均为盗版

金书网：[www.golden-book.com](http://www.golden-book.com)

最近 20 年来,我国的计算机技术与实际应用飞速发展,并早已进入了互联网时代;而自 2009 年左右开始,移动互联网兴起,互联网与移动互联网共同营造了双网互联。

在如今这个互联网时代,网络已经成为个人生活与工作中信息获取的重要手段,网络购物也已经成为民众重要的消费渠道。而非专业人员较低的防范意识和计算机技术水平给了不法分子可乘之机,各种网络病毒、木马、流氓软件、间谍软件等纷纷出现,给人们的个人信息安全及财产安全带来了非常大的威胁。为了使计算机网络免受恶意软件、病毒和黑客的攻击,为了使个人隐私不遭到泄密,为了使财产免受损失,我们必须提高自己的防范意识和网络安全技术,做好计算机网络的安全防范工作。

## 本书内容

本书介绍了社会工程学、计算机与手机安全相关的多方面知识。主要内容分为三部分:第一部分为社会工程学,分为 4 章,介绍了社会工程学基础、信息收集和搜索、个人信息安全、商业信息安全;第二部分为计算机黑客攻防,分为 17 章,介绍了网络安全技术基础、网络钓鱼攻击揭秘、信息的扫描与嗅探揭秘、病毒攻防、木马攻防、密码攻防、计算机后门技术、系统漏洞攻防、网站安全防护、局域网攻防、QQ 安全防护、网络代理与追踪技术、远程控制技术、入侵痕迹清除技术、间谍软件的清除和系统清理、系统和数据的备份与恢复、加强网络支付工具的安全;第三部分为移动终端安全,分为 8 章,介绍了移动黑客攻防基础、iOS 操作系统、Android 操作系统、手机病毒与木马攻防、无线通信技术之蓝牙、无线通信技术之 Wi-Fi、手机游戏安全、移动支付安全。

## 本书特色

- 内容全面:本书包含了社会工程学、计算机网络安全和移动终端安全三大领域的知识。
- 易学易懂:本书从零起步,步步深入,通俗易懂,使初学者和具有一定基础的用户都能逐步提高,快速掌握黑客防范技巧与工具的使用方法。

# 黑客

攻防大曝光——社会工程学、计算机黑客攻防、移动黑客攻防技术揭秘

- 实用性强：本书注重理论和实例相结合，并配以大量插图讲解，力图使读者能够融会贯通。
- 案例丰富：本书重点突出，并附有大量的操作实例，读者可以一边学习，一边操练，做到即学即用、即用即得。

## 本书适合人群

- 初、中级计算机用户；
- 电脑爱好者；
- 各行各业关注网络防护的人员；
- 网络管理人员；
- 大、中专院校计算机相关专业学生。

## 本书作者

本书由知雨科技编著，参与编写的具体人员有郑奎国、王叶、丛砚敏、郅朝怡、施亚、朱伟伟、李季、郑林、丁建飞、张阮阮、刘超、方开庆、陈红、宫晨伟、陈伟、高文晖、赵根昌、苗玉珍、竹简、余东航、王彦祥、王清江、杨龙胜、向荣辉、向世军。在此向他们表示感谢！

## 郑重声明

据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，本书内容是帮助广大读者做好计算机与移动终端的安全防护工作。

## 前言

**第 1 章 人人都要懂的社会工程学 / 1**

## 1.1 黑客与社会工程学 / 2

- 1.1.1 社会工程学攻击概述 / 2
- 1.1.2 无法忽视的非传统信息安全 / 2
- 1.1.3 攻击信息拥有者 / 3

## 1.2 揭秘常见的社会工程学攻击手段 / 3

- 1.2.1 环境渗透 / 4
- 1.2.2 引诱 / 4
- 1.2.3 伪装 / 4
- 1.2.4 说服 / 4
- 1.2.5 恐吓 / 4

1.2.6 恭维 / 5

1.2.7 反向社会工程学攻击 / 5

## 1.3 案例揭秘：社会工程学攻击时刻在发生 / 5

- 1.3.1 非法获取用户的手机号码 / 5
- 1.3.2 揭秘网络钓鱼 / 6
- 1.3.3 揭秘如何伪造身份骗取系统口令 / 7

## 1.4 从源头防范黑客攻击 / 7

- 1.4.1 个人用户防范社会工程学攻击 / 8
- 1.4.2 企业或单位防范社会工程学攻击 / 8

## 第 2 章 无所不能的信息搜索 / 11

### 2.1 利用搜索引擎搜索 / 12

- 2.1.1 百度搜索功能及语法应用 / 12
- 2.1.2 企业机密信息是怎样泄露的 / 17

### 2.2 利用门户网站收集信息 / 18

- 2.2.1 门户网站 / 18
- 2.2.2 知名门户搜索 / 19
- 2.2.3 高端门户搜索 / 20

### 2.3 利用综合信息搜索 / 21

- 2.3.1 利用找人网收集信息 / 21
- 2.3.2 利用查询网收集信息 / 22
- 2.3.3 利用人人网和贴吧收集信息 / 24
- 2.3.4 揭秘即时通信软件是怎样泄密的 / 25
- 2.3.5 新浪微博的泄密渠道 / 26

## 第 3 章 个人信息安全 / 27

### 3.1 网站 Cookies 泄密及应对措施 / 28

- 3.1.1 认识 Cookies / 28
- 3.1.2 在 IE 浏览器中清除 Cookies / 28
- 3.1.3 在“Internet 选项”对话框中设置清除网页历史记录 / 30
- 3.1.4 信息安防终极秘籍: index.dat Suite 工具的应用 / 30

### 3.2 用户文件使用记录泄密及安全防范 / 31

- 3.2.1 查看最近使用的项目 / 32
- 3.2.2 搜索最近访问、修改或创建的文件 / 35
- 3.2.3 使用 XYplorer 软件搜索文件 / 37
- 3.2.4 通过应用软件查看历史访问记录 / 37

## 第 4 章 商业信息安全 / 39

- 4.1 揭秘搜集信息的手段 / 40
  - 4.1.1 翻查垃圾 / 40
  - 4.1.2 伪造身份 / 40
  - 4.1.3 设置陷阱 / 41
- 4.2 商业窃密手段曝光 / 41
  - 4.2.1 技术著述或广告展览 / 42
  - 4.2.2 信息调查表格 / 42
  - 4.2.3 手机窃听技术 / 43
  - 4.2.4 智能手机窃密技术 / 43
  - 4.2.5 语音与影像监控技术 / 44
  - 4.2.6 GPS 跟踪与定位技术 / 45

## 第 5 章 网络安全技术基础 / 47

- 5.1 认识进程与端口 / 48
  - 5.1.1 认识系统进程 / 48
  - 5.1.2 关闭和新建系统进程 / 49
  - 5.1.3 端口的分类 / 50
  - 5.1.4 查看端口 / 52
  - 5.1.5 开启和关闭端口 / 53
  - 5.1.6 端口的限制 / 55
- 5.2 常见的网络协议 / 60
  - 5.2.1 TCP/IP 族 / 60
  - 5.2.2 IP / 61
  - 5.2.3 ARP / 62
  - 5.2.4 ICMP / 63
- 5.3 常用的计算机与网络命令 / 64
  - 5.3.1 测试物理网络的 ping 命令 / 64
  - 5.3.2 查看网络连接的 netstat 命令 / 66
  - 5.3.3 工作组和域的 net 命令 / 67
  - 5.3.4 23 端口登录的 telnet 命令 / 70
  - 5.3.5 传输协议 ftp 命令 / 71
  - 5.3.6 查看网络配置的 ipconfig 命令 / 72

## 第 6 章 揭秘网络钓鱼攻击 / 73

- 6.1 认识网络钓鱼攻击 / 74
- 6.2 真网址与假网址：识别假域名注册欺骗 / 75
  - 6.3.1 花样百出的钓鱼邮件 / 76
  - 6.3.2 伪造发件人地址 / 77
  - 6.3.3 邮件前置与诱惑性标题 / 78
- 6.3 揭秘 E-mail 邮件钓鱼技术 / 76
- 6.4 利用 360 安全卫士防范网络钓鱼 / 79



## 第 7 章 揭秘信息的扫描与嗅探 / 81

### 7.1 确定扫描目标 / 82

- 7.1.1 确定目标主机 IP 地址 / 82
- 7.1.2 了解网站备案信息 / 85
- 7.1.3 确定可能开放的端口和服务 / 86

### 7.2 扫描的实施与防范 / 87

- 7.2.1 扫描服务与端口 / 88
- 7.2.2 FreePortScanner 与 ScanPort 等常见扫描工具 / 90
- 7.2.3 用扫描器 X-scan 查本机隐患 / 91

7.2.4 用 SSS 扫描器实施扫描 / 96

7.2.5 用 ProtectX 实现扫描的反击与追踪 / 99

### 7.3 嗅探的实现与防范 / 102

- 7.3.1 什么是嗅探器 / 102
- 7.3.2 捕获网页内容的艾菲网页侦探 / 102
- 7.3.3 使用影音神探嗅探在线视频地址 / 104

### 7.4 运用工具实现网络监控 / 108

- 7.4.1 运用长角牛网络监控机实现网络监控 / 108
- 7.4.2 运用 Real Spy Monitor 监控网络 / 112

## 第 8 章 病毒曝光与防范 / 117

### 8.1 认识病毒 / 118

- 8.1.1 计算机病毒的特点 / 118
- 8.1.2 病毒的三个基本结构 / 118
- 8.1.3 病毒的工作流程 / 119

### 8.2 Restart 病毒与 U 盘病毒曝光 / 120

- 8.2.1 揭秘 Restart 病毒 / 120
- 8.2.2 揭秘 U 盘病毒 / 123

### 8.3 VBS 脚本病毒曝光 / 125

- 8.3.1 揭秘 VBS 脚本病毒生成机 / 125
- 8.3.2 揭秘 VBS 脚本病毒刷 QQ 聊天屏 / 127

### 8.4 宏病毒与邮件病毒防范 / 128

- 8.4.1 宏病毒的判断方法 / 128
- 8.4.2 防范与清除宏病毒 / 128
- 8.4.3 全面防御邮件病毒 / 129

### 8.5 网络蠕虫病毒防范 / 130

- 8.5.1 网络蠕虫病毒实例分析 / 130
- 8.5.2 网络蠕虫病毒的全面防范 / 130

### 8.6 杀毒软件的使用 / 132

- 8.6.1 用 NOD32 查杀病毒 / 133
- 8.6.2 免费的专业防火墙 ZoneAlarm / 134

## 第9章 木马曝光与防范 / 136

### 9.1 认识木马 / 137

- 9.1.1 木马的起源与发展 / 137
- 9.1.2 木马的机体构造 / 137
- 9.1.3 木马的分类 / 138

### 9.2 揭秘木马的生成与伪装 / 139

- 9.2.1 曝光木马的伪装手段 / 139
- 9.2.2 曝光木马捆绑技术 / 140
- 9.2.3 曝光自解压捆绑木马 / 142
- 9.2.4 曝光 CHM 木马 / 144

### 9.3 揭秘木马的加壳与脱壳 / 147

- 9.3.1 曝光 ASPack 加壳 / 147
- 9.3.2 曝光“北斗压缩”多次加壳 / 149
- 9.3.3 使用 PE-Scan 检测木马是否加过壳 / 150
- 9.3.4 使用 UnASPack 进行脱壳 / 151

### 9.4 清除木马 / 152

- 9.4.1 通过木马清除专家清除木马 / 152
- 9.4.2 在 Windows 进程管理器中管理计算机进程 / 155

## 第10章 常用软件加密解密技术 / 157

### 10.1 Excel 文件的加密解密 / 158

- 10.1.1 用 Excel 自带功能加密 / 158
- 10.1.2 用 Passware Kit Basic Demo 解密 Excel 文件 / 160
- 10.1.3 用 AOPR 解密 Excel 文件 / 161
- 10.1.4 用 Excel Password Recovery 解密 Excel 文件 / 162

### 10.2 加密软件 PGP 的使用 / 164

### 10.3 Word 文件的加密解密 / 168

- 10.3.1 用 Word 自带功能加密 / 168
- 10.3.2 Word 密码破解器的使用 / 170
- 10.3.3 “风语者”文件加密器的使用 / 171
- 10.3.4 用 AOPR 解密 Word 文件 / 173

### 10.4 WinRAR 压缩文件的加密解密 / 174

#### 10.4.1 用 WinRAR 加密文件 / 175

#### 10.4.2 用 ARPR 1.53 绿色版解密 RAR 文件 / 176

### 10.5 ZIP 压缩文件的加密解密 / 177

- 10.5.1 用 WinZip 加密文件 / 177
- 10.5.2 使用 ARCHPR 解密 ZIP 文件 / 179
- 10.5.3 利用 ZIP 密码暴力破解工具探测口令 / 180

### 10.6 EXE 文件的加密解密 / 181

- 10.6.1 使用“EXE 文件添加运行密码”加密 EXE 文件 / 181
- 10.6.2 用 EXE 加壳保护工具加密 EXE 文件 / 183
- 10.6.3 用加壳软件 ASPack 加密 EXE 文件 / 184

## 第11章 计算机后门技术 / 186

### 11.1 认识后门 / 187

11.1.1 后门的发展历史 / 187

11.1.2 后门的分类 / 187

### 11.2 揭秘账号后门技术 / 188

11.2.1 使用软件克隆账号 / 188

11.2.2 手动克隆账号 / 190

### 11.3 系统服务后门技术 / 193

11.3.1 揭秘使用 instsrv 创建系统服务后门 / 193

11.3.2 揭秘使用 Srvinstw 创建系统服务后门 / 194

### 11.4 检测系统中的后门程序 / 198

## 第12章 系统漏洞攻防 / 200

### 12.1 系统漏洞基础知识 / 201

12.1.1 认识系统漏洞 / 201

12.1.2 Windows 系统常见漏洞 / 201

### 12.2 Windows 服务器系统 / 202

12.2.1 曝光入侵 Windows 服务器的流程 / 202

12.2.2 NetBIOS 漏洞 / 203

### 12.3 使用 MBSA 检测系统漏洞 / 207

12.3.1 MBSA 的安装 / 207

12.3.2 检测单台计算机 / 209

12.3.3 检测多台计算机 / 210

### 12.4 使用 Windows Update 修复系统漏洞 / 210

## 第13章 网站安全防护 / 213

### 13.1 曝光 SQL 注入攻击 / 214

13.1.1 Domain(明小子)注入工具曝光 / 214

13.1.2 啊 D 注入工具曝光 / 217

13.1.3 对 SQL 注入漏洞的防御 / 221

### 13.2 曝光 PHP 注入利器 ZBSI / 222

### 13.3 曝光 Cookies 注入攻击 / 223

13.3.1 曝光 IECookiesView 注入工具 / 223

13.3.2 曝光 Cookies 注入工具 / 225

### 13.4 曝光跨站脚本攻击 / 226

13.4.1 简单留言本的跨站漏洞 / 226

13.4.2 跨站漏洞 / 229

13.4.3 对跨站漏洞的预防措施 / 233

## 第14章 局域网攻防 / 235

### 14.1 局域网基础知识 / 236

14.1.1 局域网简介 / 236

14.1.2 局域网安全隐患 / 236

### 14.2 常见的几种局域网攻击类型 / 237

14.2.1 ARP 欺骗攻击 / 237

14.2.2 IP 地址欺骗攻击 / 238

### 14.3 局域网攻击工具 / 239

14.3.1 网络剪刀手 Netcut / 239

14.3.2 WinArpAttacker 工具 / 240

### 14.4 局域网监控工具 / 243

14.4.1 LanSee 工具 / 243

14.4.2 网络特工 / 245

## 第15章 QQ 安全防护 / 248

### 15.1 QQ 攻击方式曝光 / 249

15.1.1 QQ 消息“炸弹”攻击 / 249

15.1.2 本地 QQ 密码攻防 / 250

15.1.3 非法获取用户 IP 地址 / 251

15.1.4 查询本地聊天记录 / 251

### 15.2 QQ 安全防护 / 252

15.2.1 保护 QQ 密码 / 252

15.2.2 防范 IP 地址探测 / 254

### 15.3 加密 QQ 聊天记录 / 255

## 第16章 网络代理与追踪技术 / 256

### 16.1 常见的代理工具 / 257

16.1.1 “代理猎手”代理工具 / 257

16.1.2 SocksCap 代理工具 / 260

### 16.2 常见的黑客追踪工具 / 262

16.2.1 曝光使用 NeoTrace Pro 进行追踪 / 262

16.2.2 实战 IP 追踪技术 / 264

## 第17章 远程控制技术 / 265

### 17.1 远程控制概述 / 266

- 17.1.1 远程控制的技术原理 / 266
- 17.1.2 基于两种协议的远程控制 / 266
- 17.1.3 远程控制的应用 / 267

### 17.2 利用“远程控制任我行”进行远程控制 / 268

- 17.2.1 配置服务器端 / 268
- 17.2.2 通过服务端程序进行远程控制 / 269

### 17.3 用 QuickIP 进行多点控制 / 270

#### 17.3.1 安装 QuickIP / 270

#### 17.3.2 设置 QuickIP 服务器端 / 272

#### 17.3.3 设置 QuickIP 客户端 / 273

#### 17.3.4 实现远程控制 / 273

### 17.4 用 WinShell 实现远程控制 / 274

#### 17.4.1 配置 WinShell / 274

#### 17.4.2 实现远程控制 / 276

### 17.5 远程桌面连接与协助 / 278

#### 17.5.1 Windows 系统的远程桌面连接 / 278

#### 17.5.2 Windows 系统远程关机 / 281

#### 17.5.3 区别远程桌面与远程协助 / 283

## 第18章 入侵痕迹清除技术 / 284

### 18.1 黑客留下的脚印 / 285

- 18.1.1 日志产生的原因 / 285
- 18.1.2 为什么要清理日志 / 287

### 18.2 日志分析工具 WebTrends / 287

- 18.2.1 创建日志站点 / 288
- 18.2.2 生成日志报表 / 291

### 18.3 清除服务器日志 / 293

#### 18.3.1 手工删除服务器日志 / 293

#### 18.3.2 通过批处理文件删除服务器日志 / 294

### 18.4 清除历史痕迹 / 295

#### 18.4.1 清除网络历史记录 / 295

#### 18.4.2 使用 Windows 优化大师进行清理 / 298

#### 18.4.3 使用 CCleaner / 299

## 第19章 流氓软件的清除和系统清理 / 303

### 19.1 流氓软件的清除 / 304

19.1.1 清理浏览器插件 / 304

19.1.2 流氓软件的防范 / 305

19.1.3 使用金山清理专家清除  
恶意软件 / 309

### 19.2 间谍软件防护实战 / 310

19.2.1 间谍软件防护概述 / 310

19.2.2 用 Spy Sweeper 清除间谍软件 / 311

19.2.3 通过事件查看器抓住“间谍” / 313

19.2.4 使用 Windows Defender 对计算机  
进行保护 / 317

19.2.5 使用 360 安全卫士对计算机进行  
防护 / 319

19.2.6 AD-Aware 让间谍程序消失无踪 / 322

19.2.7 浏览器绑架克星 HijackThis / 324

## 第20章 系统和数据的备份与恢复 / 328

### 20.1 备份与还原操作系统 / 329

20.1.1 使用还原点备份与还原系统 / 329

20.1.2 使用 GHOST 备份与还原系统 / 331

### 20.2 备份与还原用户数据 / 335

20.2.1 使用驱动精灵备份与还原驱动  
程序 / 335

20.2.2 备份与还原 IE 浏览器的收藏夹 / 337

20.2.3 备份和还原 QQ 聊天记录 / 340

### 20.3 使用恢复工具恢复误删除的 数据 / 342

20.3.1 使用 Recuva 恢复数据 / 342

20.3.2 使用 FinalData 恢复数据 / 346

20.3.3 使用 FinalRecovery 恢复数据 / 350

## 第21章 加强网络支付工具的安全 / 353

### 21.1 加强支付宝的安全防护 / 354

21.1.1 加强支付宝账户的安全防护 / 354

21.1.2 加强支付宝内资金的安全防护 / 357

### 21.2 加强财付通的安全防护 / 359

21.2.1 加强财付通账户的安全防护 / 359

21.2.2 加强财付通内资金的安全防护 / 363

## 第22章 移动终端攻防基础 / 366

- 22.1 智能手机主流操作系统 / 367
  - 22.1.1 Android 操作系统 / 367
  - 22.1.2 iOS 操作系统 / 367
  - 22.1.3 Windows Phone 操作系统 / 368
- 22.2 智能手机漏洞简介 / 368
- 22.3 手机黑客的由来 / 368

## 第23章 iOS操作系统 / 370

- 23.1 iOS 操作系统概述 / 371
  - 23.1.1 iOS 的用户界面 / 371
  - 23.1.2 iOS 的发展历程 / 371
  - 23.1.3 iOS 10 新特性 / 372
- 23.2 iOS 的系统结构与开发语言 / 374
  - 23.2.1 iOS 的系统结构 / 374
  - 23.2.2 iOS 开发语言 / 374
- 23.3 备份和恢复 iPhone/iPad/iPod 数据 / 375
  - 23.3.1 使用 iCloud 备份和恢复用户数据 / 376
  - 23.3.2 使用 iTunes 备份和还原用户数据 / 378
- 23.4 针对 iOS 系统的攻击曝光 / 379
  - 23.4.1 iKee 攻击与防范 / 379
  - 23.4.2 中间人攻击与防范 / 380
  - 23.4.3 恶意应用程序 Handy Light 和 InstaStock 曝光与防范 / 381
  - 23.4.4 具有漏洞的应用程序：iOS 应用程序和第三方应用程序 / 382

## 第24章 Android操作系统 / 384

### 24.1 Android 操作系统概述 / 385

- 24.1.1 Android 的发展历程 / 385
- 24.1.2 Android 7.0 新特性 / 386
- 24.1.3 Android 模拟器的使用 / 387

### 24.2 Android 系统架构 / 388

- 24.2.1 应用程序层 / 389
- 24.2.2 应用程序框架层 / 389
- 24.2.3 系统运行库层 / 389
- 24.2.4 Linux 核心层 / 390

### 24.3 Android 安全模型 / 391

### 24.4 Android 基础应用组件 / 392

- 24.4.1 活动 / 392
- 24.4.2 服务 / 392
- 24.4.3 广播接收器 / 393
- 24.4.4 内容提供者 / 394

### 24.5 Android 手机备份功能 / 394

#### 24.5.1 Recovery 模式 / 394

#### 24.5.2 备份的方法 / 394

### 24.6 Android 系统刷机 / 396

- 24.6.1 Android 系统刷机常见术语 / 396
- 24.6.2 安卓手机刷机方法及步骤 / 397

### 24.7 获取 Android root 权限 / 398

- 24.7.1 获取 root 权限的原理 / 398
- 24.7.2 获取 root 权限的好处以及风险 / 398
- 24.7.3 如何获取 root 权限 / 399

### 24.8 曝光 Android 平台恶意软件及病毒 / 400

- 24.8.1 ROM 内置恶意软件/病毒曝光 / 400
- 24.8.2 破坏类恶意软件/病毒曝光 / 401
- 24.8.3 吸费类恶意软件/病毒曝光 / 401
- 24.8.4 窃取隐私类恶意软件/病毒曝光 / 402
- 24.8.5 伪装类恶意软件/病毒曝光 / 402
- 24.8.6 云更新类恶意软件/病毒曝光 / 403
- 24.8.7 诱骗类恶意软件/病毒曝光 / 404

## 第25章 手机病毒与木马的防范 / 405

### 25.1 常见的手机病毒曝光 / 406

- 25.1.1 安卓短信卧底 / 406
- 25.1.2 钓鱼王病毒 / 407
- 25.1.3 手机骷髅病毒 / 407
- 25.1.4 短信海盗 / 408
- 25.1.5 同花顺大盗 / 409
- 25.1.6 手机僵尸病毒 / 409
- 25.1.7 卡比尔病毒 / 411
- 25.1.8 QQ 盗号手 / 411

### 25.2 手机病毒与木马的危害与安全防范 / 412

- 25.2.1 手机病毒与木马带来的危害 / 412
- 25.2.2 手机病毒与木马的防范措施 / 413

### 25.3 手机杀毒软件的使用 / 414

- 25.3.1 360 手机卫士 / 414
- 25.3.2 腾讯手机管家 / 417
- 25.3.3 金山手机卫士 / 418



## 第26章 无线通信技术之蓝牙 / 420

### 26.1 蓝牙基础知识简介 / 421

- 26.1.1 认识蓝牙 / 421
- 26.1.2 蓝牙的起源与发展 / 421
- 26.1.3 蓝牙的工作原理 / 421
- 26.1.4 蓝牙的体系结构 / 422
- 26.1.5 蓝牙的相关术语 / 423
- 26.1.6 蓝牙 4.2 的新特征 / 423
- 26.1.7 蓝牙 4.2 的发展前景 / 424

### 26.2 蓝牙设备的配对 / 424

- 26.2.1 启动蓝牙适配器 / 425
- 26.2.2 搜索周围开启蓝牙功能的设备 / 426
- 26.2.3 使用蓝牙进行设备间的配对 / 426

### 26.2.4 两台设备传递文件测试效果 / 428

### 26.3 蓝牙通信技术应用实例 / 430

- 26.3.1 让家居生活更便捷 / 430
- 26.3.2 让驾驶更安全 / 431
- 26.3.3 增强多媒体系统功能 / 431
- 26.3.4 提高工作效率 / 432
- 26.3.5 丰富娱乐生活 / 432

### 26.4 蓝牙攻击方式曝光与防范措施 / 433

- 26.4.1 曝光蓝牙的常见漏洞 / 433
- 26.4.2 修改蓝牙设备地址 / 433
- 26.4.3 DoS 漏洞的产生 / 434
- 26.4.4 蓝牙的安全防护 / 434

## 第27章 无线通信技术之Wi-Fi / 435

### 27.1 Wi-Fi 简介 / 436

- 27.1.1 Wi-Fi 的通信原理 / 436
- 27.1.2 Wi-Fi 的主要功能 / 436
- 27.1.3 Wi-Fi 的优势 / 438
- 27.1.4 Wi-Fi 与蓝牙互补 / 438
- 27.1.5 Wi-Fi 无线网络的建立 / 439

### 27.2 无线网络的安全加密 / 442

- 27.2.1 使用 WEP 加密 / 442
- 27.2.2 使用 WPA-PSK 安全加密算法加密 / 442
- 27.2.3 禁用 SSID 广播 / 443

### 27.2.4 基于 MAC 地址的媒体访问控制 / 443

### 27.3 智能手机 Wi-Fi 连接方式 / 445

- 27.3.1 Android 手机 Wi-Fi 连接 / 445
- 27.3.2 iPhone 手机 Wi-Fi 连接 / 446

### 27.4 Wi-Fi 技术的应用 / 448

- 27.4.1 网络媒体 / 448
- 27.4.2 日常休闲 / 448
- 27.4.3 掌上设备 / 449
- 27.4.4 客运列车 / 449

### 27.5 无线路由器设置 / 449