

ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防 从入门到精通

手机安全篇 · 全新升级版

明月工作室 高翔◎编著

超值赠送

黑客攻防全能视频+计算机硬件管理超级手册+Windows文件管理高级手册+Linux命令应用大全

以下人群请勿翻阅本书:

1. 自以为很牛，对黑客不屑一顾的人
2. 心存侥幸，认为黑客离自己很远的人
3. 习惯黑客攻击，总是折腾他人的人
4. 号太多，习惯被盗号的人
5. 不差钱，不怕被盗刷的人
6. 我不是Boss，对交易安全漠不关心的人

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

ATTACK

黑客攻防 从入门到精通

手机安全篇 · 全新升级版

明月工作室 高翔◎编著

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了手机安全方面的相关知识。

全书主要内容有14章,分别为认识黑客与智能手机攻防、智能手机操作系统——iOS、智能手机操作系统——Android、智能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、DOS攻击、手机游戏安全攻防、QQ账号及电子邮件攻防、智能手机加密与性能优化、移动追踪定位与远程控制技术、保护移动支付安全、揭秘针对智能手机的攻击方式与安全防范、平板电脑的攻防技巧。

本书语言简洁、流畅,内容丰富、全面,适用于一般智能手机用户、对移动设备感兴趣的人员、对移动设备维护的人员阅读和学习,也可以作为各大计算机培训机构的辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通.手机安全篇:全新升级版/高翔编著. — 北京:北京大学出版社,2016.12
ISBN 978-7-301-27735-5

I. ①黑… II. ①高… III. ①黑客—网络防御②移动电话机—安全技术
IV. ①TP393.081②TN929.53

中国版本图书馆CIP数据核字(2016)第269933号

书 名: 黑客攻防从入门到精通(手机安全篇·全新升级版)

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者: 明月工作室 高翔 编著

责任编辑: 尹 毅

标准书号: ISBN 978-7-301-27735-5

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> 新浪微博: @北京大学出版社

电子信箱: pup7@pup.cn

电 话: 邮购部62752015 发行部62750672 编辑部62580653

印 刷 者: 北京大学印刷厂

经 销 者: 新华书店

787毫米×1092毫米 16开本 21.5印张 462千字

2016年12月第1版 2016年12月第1次印刷

印 数: 1-4000册

定 价: 49.00元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究

举报电话: 010-62752024 电子信箱: fd@puppkuedu.cn

图书如有印装质量问题,请与出版部联系,电话: 010-62756370

前言 · 全新升级版

从2003年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，电子商务、网络游戏、视频网站、社交娱乐等百花齐放。计算机技术及通信技术的进一步发展，持续推动中国互联网用户新一轮的高速增长，到2008年已经达到2.53亿户，首次大幅度超过美国，跃居世界首位。

从2009年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为民众重要的消费渠道。当前，“互联网+”的战略布局与工业4.0的深度发展，使得国家经济发展、民众工作生活都与网络安全休戚相关，因此，一个安全的网络环境是必不可少的。

当前最大的一个问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就为不法分子提供了大量的可乘之机。这些不法分子借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产带来了非常大的威胁。

为提升广大民众对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护，我们策划了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（手机安全篇·全新升级版）》分册。

丛书书目

- 黑客攻防从入门到精通（全新升级版）
- 黑客攻防从入门到精通（Web技术实战篇）
- 黑客攻防从入门到精通（Web脚本编程篇·全新升级版）
- 黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）
- 黑客攻防从入门到精通（加密与解密篇）
- 黑客攻防从入门到精通（手机安全篇·全新升级版）
- 黑客攻防从入门到精通（应用大全篇·全新升级版）
- 黑客攻防从入门到精通（命令实战篇·全新升级版）
- 黑客攻防从入门到精通（社会工程学篇）



本书特点

- 内容全面：本书首先介绍了黑客的相关知识和移动设备中各主流操作系统的特点，为全书的学习奠定了一定的基础。后面的章节中以Android和iOS两大操作系统为主线分别介绍了无线通信技术、木马和病毒、移动跟踪定位等知识。本书在攻防实验的操作中涵盖了移动攻防所需的各种攻防工具，适合各个层面、不同基础的读者阅读。
- 与时俱进：本书主要适用于Android和iOS两大操作系统，并且包含了Android6.0及iOS 9版本的相关知识。虽然手机操作系统版本升级较快，但本书中的知识适用于手机各种版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行介绍，从而加深读者对该知识点的理解。
- 适合阅读：本书摒弃了大量枯燥文字叙述的编写方式，采用图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步，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。



读者对象

- 普通智能手机用户。
- 移动攻防爱好者。
- 移动安全研究人员。
- 移动攻防零基础读者。
- 移动设备维修人员。
- 无线通信爱好者。
- 移动应用开发人员。
- 大中专院校相关学生。



本书结构及内容

本书一共有14章，内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

第1章 认识黑客与智能手机攻防

第2章 智能手机操作系统——iOS

第3章 智能手机操作系统——Android

第4章 智能手机病毒与木马攻防

第5章 无线通信技术之蓝牙

- 第6章 无线通信技术之Wi-Fi
- 第7章 DOS攻击
- 第8章 手机游戏安全攻防
- 第9章 QQ账号及电子邮件攻防
- 第10章 智能手机加密与性能优化
- 第11章 移动追踪定位与远程控制技术
- 第12章 保护移动支付安全
- 第13章 揭秘针对智能手机的攻击方式与安全防范
- 第14章 平板电脑的攻防技巧



超值赠送资源

1. 黑客攻防全能视频

为了读者能全面地了解黑客方面的知识从而有效地防御黑客的不法入侵行为，本书特赠送全能教学视频，视频内容包括社会工程学、黑客攻防入门、信息的扫描与嗅探、木马与病毒的防范、系统漏洞防范、远程控制术、加密与解密、数据备份与恢复、移动网络安全等内容。

2. 其他赠送资源

- Windows系统安全与维护手册
- 计算机硬件管理超级手册
- Windows文件管理高级手册
- (140个) Windows系统常用快捷键大全
- (157个) Linux基础命令手册
- (136个) Linux系统管理与维护命令手册
- (58个) Linux网络与服务器命令手册
- 黑客攻防命令手册

我们已将赠送内容上传百度网盘，在浏览器中输入下载链接，打开链接后，在如下图所示的文本框中输入提取码便可下载赠送资源。下载链接：<http://pan.baidu.com/s/1eSfvxDK>，提取码：ez6a。

提示

读者也可加入QQ群，在群文件中下载“资源下载地址列表”文档，直接复制链接和密码，下载多媒体视频。（注意：我们会在群文件中共享一些赠送资源，如百度网盘链接失效，请加入QQ群下载资源。）



后续服务

本书由高翔编著，胡华、闫珊珊、王栋、宗立波、马琳、赵玉萍、栾铭斌等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过E-mail或QQ群与我们联系。

投稿邮箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857



郑重声明

本丛书对大量计算机及移动端的攻击行为进行了曝光，可帮广大读者做好安全防范工作。

请本丛书广大读者注意：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是违法的！



第 1 章 认识黑客与智能手机攻防	1
1.1 丰富多彩的黑客文化	2
1.1.1 黑客的由来	2
1.1.2 手机黑客的由来	3
1.1.3 黑客守则	3
1.1.4 黑客常用攻击方式	4
1.2 黑客必备技能	5
1.2.1 英语阅读能力	5
1.2.2 使用黑客工具	6
1.2.3 具备编程技能	6
1.2.4 熟悉网络协议和工作原理	6
1.3 智能手机攻防基础	6
1.3.1 智能手机主流操作系统	6
1.3.2 智能手机漏洞简介	8
技巧与问答	9
 第 2 章 智能手机操作系统——iOS	13
2.1 iOS 操作系统的发展历程	14
2.1.1 iOS 的发展回顾	14
2.1.2 iOS 最新版本	18
2.1.3 iOS 用户界面	19
2.2 从底层剖析 iOS	20
2.2.1 iOS 的系统架构	20
2.2.2 iOS 开发语言	20
2.3 刷新 iOS 操作系统——刷机	21
2.3.1 什么是刷机	21

2.3.2	iPhone 刷机教程.....	22
2.4	iOS 系统的数据备份与恢复	23
2.4.1	使用 iCloud 备份和恢复用户数据	23
2.4.2	使用 iTunes 备份和还原用户数据	25
2.4.3	使用 91 助手备份和还原用户数据	28
2.5	越狱让 iOS 更加完美	32
2.5.1	认识越狱	32
2.5.2	越狱的利与弊	33
2.6	苹果攻击案例	34
2.7	被用于 iOS 操作系统的攻击方式与防范技巧	37
2.7.1	Ikee 攻击与防范技巧	37
2.7.2	中间人攻击与防范技巧	38
2.7.3	恶意应用程序攻击与防范	40
2.7.4	利用应用程序漏洞攻击与防范	41
	技巧与问答	43

第 3 章 智能手机操作系统——Android..... 46

3.1	Android 操作系统的发展历程	47
3.1.1	Android 操作系统的发展回顾	47
3.1.2	Android 最新版本	49
3.1.3	Android 最新版本新特性	49
3.2	分层认识 Android 系统	50
3.2.1	认识系统分层	50
3.2.2	系统架构分层的优势	50
3.2.3	Android 操作系统的基本架构	51
3.2.4	应用程序层	52
3.2.5	应用程序框架层	52
3.2.6	系统运行库层	53
3.2.7	Linux 核心层	54
3.3	Android 安全模型	55
3.4	Android 组件的基本功能	56
3.4.1	活动	56
3.4.2	服务	57
3.4.3	广播接收器	57
3.4.4	内容提供者	58

3.5 使用备份保护数据	58
3.5.1 手动备份	59
3.5.2 利用91助手备份	62
3.6 Android系统刷机	65
3.6.1 Android系统刷机常识	65
3.6.2 Android系统刷机教程	67
3.7 Android系统获取Root权限	68
3.7.1 Root原理简介	69
3.7.2 获取Root权限的优点与缺点	69
3.7.3 获取Root权限的方法	70
3.7.4 避免一键Root恶意软件的危害	72
3.8 认识Android模拟器	73
3.9 Android平台常见恶意软件及病毒的分类	74
3.9.1 ROM内置类恶意软件/病毒	74
3.9.2 破坏类恶意软件/病毒	74
3.9.3 吸费类恶意软件/病毒	75
3.9.4 窃取隐私类恶意软件/病毒	76
3.9.5 伪装类恶意软件/病毒	76
3.9.6 云更新类恶意软件/病毒	77
3.9.7 诱骗类恶意软件/病毒	78
技巧与问答	78

第4章 智能手机病毒与木马攻防 81

4.1 认识手机病毒	82
4.1.1 手机病毒术语	82
4.1.2 手机病毒的组成	82
4.1.3 手机病毒的特点	83
4.2 认识手机木马	85
4.2.1 手机木马的组成	85
4.2.2 手机木马的分类	86
4.2.3 手机木马攻击的原理	87
4.3 常见的手机病毒	89
4.3.1 常见手机病毒之一——短信病毒	89
4.3.2 常见手机病毒之二——钓鱼王病毒	90
4.3.3 常见手机病毒之三——手机骷髅病毒	91

4.3.4	常见手机病毒之四——同花顺大盗	92
4.3.5	常见手机病毒之五——手机僵尸病毒	93
4.3.6	常见手机病毒之六——卡比尔病毒	94
4.3.7	常见手机病毒之七——老千大富翁	95
4.3.8	常见手机病毒之八——QQ盗号手	96
4.4	手机病毒与木马的危害和防范	97
4.5	网络蠕虫的危害及防范	99
4.5.1	认识网络蠕虫	99
4.5.2	网络蠕虫的危害	100
4.5.3	网络蠕虫的防范	101
4.6	杀毒软件的使用	102
4.6.1	腾讯手机管家	102
4.6.2	百度手机卫士	104
4.6.3	360手机卫士	106
	技巧与问答	107

第5章 无线通信技术之蓝牙..... 110

5.1	蓝牙基础知识简介	111
5.1.1	认识蓝牙	111
5.1.2	蓝牙的起源与发展	111
5.1.3	蓝牙的工作原理	112
5.1.4	蓝牙的体系结构	113
5.1.5	蓝牙的相关术语	114
5.1.6	蓝牙4.2的新特征	114
5.1.7	蓝牙4.2的发展前景	115
5.2	蓝牙设备的配对	116
5.2.1	启动蓝牙适配器	116
5.2.2	搜索周围开启蓝牙功能的设备	117
5.2.3	使用蓝牙进行设备间的配对	118
5.2.4	两台设备传递文件测试效果	119
5.3	蓝牙通信技术应用实例	122
5.3.1	让家居生活更便捷	122
5.3.2	让驾驶更安全	122
5.3.3	增强多媒体系统功能	123
5.3.4	提高工作效率	123

5.3.5 丰富娱乐生活	124
5.4 蓝牙攻击方式与防范	124
5.4.1 典型的蓝牙攻击	125
5.4.2 修改蓝牙设备地址	125
5.4.3 利用蓝牙进行DOS攻击	125
5.4.4 蓝牙的安全防护	126
技巧与问答	126

第6章 无线通信技术之 Wi-Fi 129

6.1 Wi-Fi基础知识简介	130
6.1.1 Wi-Fi的通信原理	130
6.1.2 Wi-Fi的主要功能	130
6.1.3 Wi-Fi的优势	132
6.1.4 Wi-Fi与蓝牙互补	133
6.1.5 Wi-Fi无线网络的建立	134
6.2 无线网络的安全加密	139
6.2.1 使用WEP加密	139
6.2.2 使用WPA-PSK安全加密算法加密	140
6.2.3 禁用SSID广播	140
6.2.4 基于MAC地址的媒体访问控制	141
6.3 智能手机Wi-Fi连接方式	143
6.3.1 Android手机Wi-Fi连接	143
6.3.2 iPhone手机Wi-Fi连接	144
6.4 Wi-Fi技术的应用	146
6.4.1 网络媒体	146
6.4.2 日常休闲	146
6.4.3 掌上设备	147
6.4.4 客运列车	147
6.5 无线路由器设置教程	147
6.5.1 认识无线路由器	147
6.5.2 无线路由器基础设置	148
6.5.3 无线加密	150
6.5.4 禁用DHCP功能	151
6.5.5 修改Wi-Fi连接密码	151
6.5.6 关闭SSID广播	152
6.5.7 设置IP地址和MAC地址的绑定	152

6.6 使用软件破解 Wi-Fi 密码的方法及防范措施	154
6.6.1 手机版“Wi-Fi 万能钥匙”破解 Wi-Fi 密码	154
6.6.2 PC 版“Wi-Fi 万能钥匙”破解 Wi-Fi 密码	156
6.6.3 防止“Wi-Fi 万能钥匙”破解密码	158
6.7 Wi-Fi 攻击方式	158
6.7.1 Wi-Fi 攻击之一——钓鱼陷阱	159
6.7.2 Wi-Fi 攻击之二——陷阱接入点	159
6.7.3 Wi-Fi 攻击之三——攻击无线路由器	159
6.7.4 Wi-Fi 攻击之四——内网监听	160
6.7.5 Wi-Fi 攻击之五——劫机	160
6.8 Wi-Fi 安全防范措施	161
技巧与问答	162

第 7 章 DOS 攻击 165

7.1 DOS 攻击概述	166
7.1.1 什么是 DOS 攻击	166
7.1.2 DOS 攻击原理	166
7.2 DOS 攻击方式的分类	167
7.3 DOS 攻击方式举例	168
7.3.1 DOS 攻击之一——SYN 泛洪攻击	168
7.3.2 SYN Cookie Firewall 防御 SYN 泛洪攻击	168
7.3.3 DOS 攻击之二——IP 欺骗攻击	170
7.3.4 DOS 攻击之三——UDP 洪水攻击	170
7.3.5 DOS 攻击之四——ping 洪流攻击	171
7.3.6 DOS 攻击之五——teardrop 攻击	172
7.3.7 DOS 攻击之六——Land 攻击	172
7.3.8 DOS 攻击之七——Smurf 攻击	172
7.3.9 DOS 攻击之八——Fraggle 攻击	173
7.4 DDOS 攻击揭密	173
7.4.1 什么是 DDOS 攻击	173
7.4.2 DDOS 攻击原理	174
7.4.3 DDOS 攻击与 DOS 攻击的区别	174
7.5 揭密对手机进行 DOS 攻击的方式	175
7.5.1 手机 DOS 攻击之一——蓝牙泛洪攻击	175
7.5.2 手机 DOS 攻击之二——蓝牙劫持攻击	175

7.5.3 手机DOS攻击之三——非正常的OBEX信息攻击	175
7.5.4 手机DOS攻击之四——非正常的MIDI文件攻击	176
7.5.5 防御DOS攻击的措施	176
技巧与问答	176

第8章 手机游戏安全攻防 179

8.1 手机游戏存在的风险	180
8.1.1 风险一——手机游戏病毒	180
8.1.2 风险二——手机账号密码采用明文传输	180
8.1.3 风险三——游戏权限滥用	181
8.1.4 风险四——手机游戏二次打包	181
8.2 手机游戏正确的下载途径	182
8.2.1 通过官网下载	182
8.2.2 第三方软件下载	183
8.3 手机游戏必备常识	185
8.3.1 收费游戏的计费原理及漏洞	185
8.3.2 手机游戏卡顿原因	186
8.3.3 手机游戏加速技巧	187
8.3.4 将手机游戏移动到内存卡	189
8.3.5 卸载后及时删除手机数据包	190
8.4 手机游戏安全防护措施	191
技巧与问答	192

第9章 QQ账号及电子邮件攻防 195

9.1 QQ黑客工具的使用和防范	196
9.1.1 “啊拉QQ大盗”的使用和防范	196
9.1.2 “雨点QQ密码查看器”的使用与防范	199
9.1.3 “QQExplorer”的使用与防范	202
9.2 增强QQ安全性的方法	203
9.2.1 方法一——定期更换密码	203
9.2.2 方法二——申请QQ密保	204
9.2.3 方法三——加密聊天记录	207
9.3 手机电子邮件攻击与防范	208
9.3.1 电子邮件攻击简介	208

9.3.2	电子邮件系统的工作原理	209
9.3.3	电子邮件攻击方式	209
9.4	电子邮件攻击防范措施	210
9.4.1	根据IP地址判断邮件来源	210
9.4.2	软件过滤垃圾邮件	211
9.4.3	避免使用公共Wi-Fi发送邮件	212
9.4.4	谨慎对待陌生连接和附件	212
9.4.5	通过日常行为保护电子邮件	212
9.5	利用密码监听器监听邮箱密码	212
9.5.1	密码监听器的使用方法	213
9.5.2	查找监听者	214
9.5.3	防止网络监听	215
	技巧与问答	215

第10章 智能手机加密与性能优化 218

10.1	设置手机锁屏密码	219
10.1.1	密码锁屏设置	219
10.1.2	图案锁屏设置	220
10.1.3	PIN锁屏设置	221
10.2	个人隐私加密	223
10.3	智能手机省电小常识	227
10.3.1	常识一——调整屏幕显示	227
10.3.2	常识二——优化系统	229
10.3.3	常识三——管理后台程序	232
10.3.4	常识四——使用省电程序	233
10.3.5	常识五——合理使用飞行模式	235
10.3.6	常识六——关闭手机触屏音效和振动	236
10.4	智能手机连接互联网	236
10.4.1	Android智能手机网络接入点设置	236
10.4.2	iPhone智能手机网络接入点设置	238
10.5	智能手机优化软件	239
10.5.1	360手机卫士	239
10.5.2	腾讯手机管家	242
10.5.3	百度安全卫士	244
	技巧与问答	246

第 11 章 移动追踪定位与远程控制技术 250

11.1 移动定位基础知识简介	251
11.1.1 移动定位的分类	251
11.1.2 移动定位技术的现状	251
11.2 常用的定位技术	252
11.2.1 GPS 定位	252
11.2.2 A-GPS 定位	252
11.2.3 基站定位	253
11.2.4 Wi-Fi 定位	254
11.2.5 RFID、二维码定位	255
11.3 移动定位的应用	256
11.3.1 应用一——紧急救援和求助	256
11.3.2 应用二——汽车导航、车辆追踪、舰队追踪	257
11.3.3 应用三——基于位置和事件的计费系统	257
11.3.4 应用四——移动性管理及系统优化设计	257
11.3.5 应用五——移动黄页查询、防止手机盗打	258
11.3.6 应用六——通过定位技术追踪手机	258
11.4 手机远程控制计算机	258
11.4.1 Android 手机远程控制计算机	259
11.4.2 iPhone 手机远程控制计算机	265
11.5 手机位置追踪	267
11.5.1 Android 手机位置追踪	267
11.5.2 iPhone 手机位置追踪	270
技巧与问答	273

第 12 章 保护移动支付安全 276

12.1 移动支付简介	277
12.1.1 什么是移动支付	277
12.1.2 移动支付的特点	277
12.1.3 移动支付的模式	277
12.2 移动支付存在的风险	278
12.3 加强移动支付安全	279
12.3.1 加强手机银行安全	279
12.3.2 加强个人网上银行安全	280
12.4 警惕钓鱼网站	280

12.5 支付宝安全性能提升	283
12.5.1 加强支付宝PC端安全防护	283
12.5.2 加强支付宝手机端安全	293
12.6 手机安全软件的使用	295
12.6.1 开启腾讯手机管家安全支付	295
12.6.2 开启360手机卫士支付保护	300
技巧与问答	303

第 13 章 揭秘针对智能手机的攻击方式与安全防范 305

13.1 智能手机的攻击方式	306
13.1.1 方式一——通过下载软件攻击	306
13.1.2 方式二——利用红外或蓝牙攻击	306
13.1.3 方式三——通过发送短信攻击	307
13.1.4 方式四——利用系统漏洞攻击	307
13.1.5 方式五——制造手机炸弹攻击	308
13.2 智能手机防范攻击技巧	308
13.2.1 技巧一——关闭蓝牙功能	308
13.2.2 技巧二——保证手机软件下载的安全性	309
13.2.3 技巧三——不轻信怪异短信，不接乱码电话	309
13.2.4 技巧四——安装手机卫士软件	310
13.2.5 技巧五——对手机数据定期备份	310
技巧与问答	311

第 14 章 平板电脑的攻防技巧..... 313

14.1 认识平板电脑	314
14.1.1 平板电脑操作系统	314
14.1.2 平板电脑的优缺点	316
14.2 针对平板电脑的攻击方式	317
14.3 平板电脑的防范技巧	318
14.3.1 及时更新平板电脑操作系统	318
14.3.2 锁定SIM卡	320
14.3.3 屏幕锁定	322
14.3.4 安装平板电脑安全软件	324
技巧与问答	326