

长达5小时互动教学多媒体光盘辅助教学

光盘互动快乐学

旗讯中文 编著

黑客攻击与防卫

- 18课阶梯式教学，循序渐进，层层深入
- 直观便捷，多媒体教学光盘让你易学易会
- 揭秘黑客入侵手法，慧眼识破伪装伎俩
- 网络技巧零点起步，轻松迈进黑客大门

9 787894 760791 >

电脑报电子音像出版社出版

书盘互动快乐学



黑客攻击与防卫

作者：周建、王洪、孙建
主编：王洪、孙建

本书共分10章，主要介绍黑客攻击与防卫的相关知识。第1章介绍黑客攻击与防卫的发展概况；第2章介绍黑客攻击与防卫的法律法规；第3章介绍黑客攻击与防卫的常用工具；第4章介绍黑客攻击与防卫的常用技术；第5章介绍黑客攻击与防卫的常用漏洞；第6章介绍黑客攻击与防卫的常用漏洞利用；第7章介绍黑客攻击与防卫的常用漏洞利用；第8章介绍黑客攻击与防卫的常用漏洞利用；第9章介绍黑客攻击与防卫的常用漏洞利用；第10章介绍黑客攻击与防卫的常用漏洞利用。



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

这是一本学习网络安全的入门教材，通过生动的图片，详细的步骤，丰富的提示讲述了电脑黑客的常见行为，即使电脑基础为零的读者也能迅速把握黑客的伎俩。在黑客攻防的案例中，我们还对关键的技术问题，做出了必要的说明和解答，真正让初学者提高网络安全意识，做好切实有效的防范。

读者在还可以配合交互式多媒体自学光盘边学边练，从而提高学习网络安全只是的兴趣和爱好，快速成为网络应用高手。

声明：使用网络技术攻击他人计算机属于违法行为，读者请勿模仿本手册中介绍的方法对他人计算机进行恶意攻击，否则后果自负！

版权所有 盗版必究
未经许可 不得以任何形式和手段复制和抄袭

手 册 名：黑客攻击与防卫

编 者：旗讯中文

技术编辑：何 磊

封面设计：陈 敏

出版单位：电脑报电子音像出版社

地 址：重庆市双钢路3号科协大厦

邮 政 编 码：400013

对外合作：(023)63658933

发 行：电脑报经营有限责任公司

经 销：各地新华书店、报刊亭

C D 生 产：四川省釜山数码科技有限公司

文 本 印 刷：重庆华林印务有限公司

开 本 规 格：787mm×1092mm 1/16 17.5 印张 300 千字

版 号：ISBN 978-7-89476-079-1

版 次：2009 年 1 月第 1 版 2009 年 1 月第 1 次印刷

定 价：29.80 元(1CD+配套手册)

电脑上手，就这18课

对于初学电脑者而言，一本易学、易会的入门指南往往令其事半功倍。《书盘互动·快乐学》系列将用户最需要掌握的电脑应用以专辑的方式独立成册，每本专辑均按18课时安排内容，方便读者把握学习过程和进度。此外，还大量采取人性化版式设计，图文混排，用图文穿插的形式让读者在每个步骤中清楚地知道操作方法和技巧，使读者能在第一时间对需要掌握的知识有直观的了解，并且获得轻松愉快的阅读体验。这就是我们的最终目的——“快乐学电脑，无痛苦入门”。

系列特色

人性化体验

从读者、学习者角度出发，体贴入微的版式设计与讲解流程，让读者在轻松愉快的体验中阅读。

直观图解

大量图片、标注和技巧讲解，直观易懂，一目了然。从标题到目录再到正文，从颜色体系到段落排版，从装帧到各种内容小元素，无处不在的细节元素，均形成了一种快捷学习氛围和环境。

内容精选

针对初学读者经常用到的几个方面，从入门、打字、办公到装机，再到操作系统，涵盖了日常生活中电脑使用的主要方面。

循序渐进

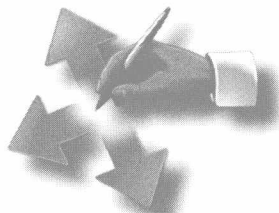
按照使用流程安排章节，带领读者层层深入，避免学习时前后翻阅无所适从的麻烦。学习其中课程，逐步进步、逐步提高。由慢到快，电脑技能就可以上一个新的台阶。

多媒体光盘

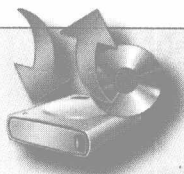
提供长达300分钟的超值多媒体互动配套光盘，情景教学，边学边看，学习更快速有趣。

适用读者群

- (1) 长期困惑于电脑难学的入门者
- (2) 无电脑操作经验的初学者
- (3) 电脑基础培训班学员
- (4) 在校或即将进入工作岗位的学生
- (5) 中老年电脑学习者
- (6) 想高效、轻松掌握电脑应用的读者



“轻轻松松学电脑，快快乐乐巧入门”，就在《书盘互动·快乐学》！



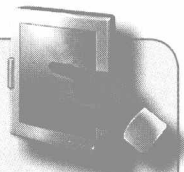
多媒体互动视频教学光盘 使用说明

超过 300 分钟的视频教学，体验坐在家中上课的感觉

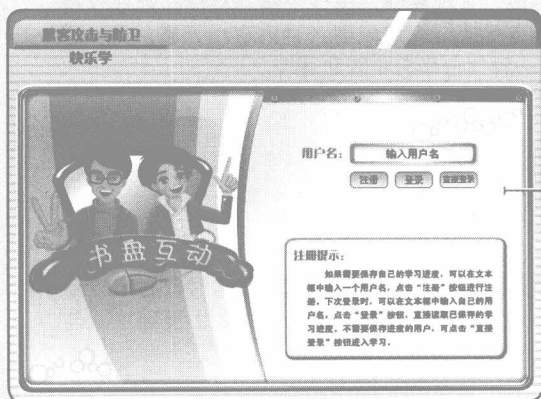
情景化视频教学 + 操作演示 + 交互 + 轻松快乐学习模式

光盘运行方式

将本光盘放入光驱，几秒钟后光盘自动运行。如果没有自动运行，可在桌面双击“我的电脑”图标，在打开的窗口中右击光盘所在的盘符，在弹出的快捷菜单中选择“自动播放”命令，即可启动光盘程序。

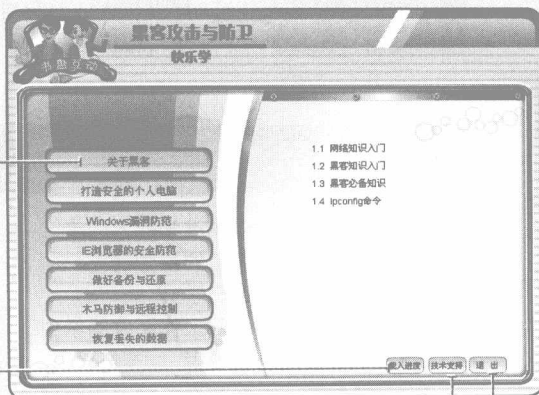


光盘操作方式



光盘运行后会自动播放一段片头动画，播放完毕后或单击鼠标即可进入光盘运行的主界面。在主界面中为用户提供了两种登录选择，如果需要保存自己的学习进度，可以在文本框中输入一个用户名，点击“注册”按钮进行注册。下次登录时，可以在文本框中输入自己的用户名，点击“登录”按钮，直接读取已保存的学习进度。不需要保存进度的用户，可选择“直接登录”按钮进行学习。

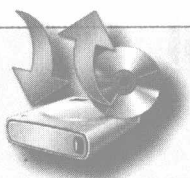
将鼠标指针移到菜单上并单击，在右侧窗格中即可显示出相应的知识点目录，选择相应的知识点进入视频教学模式。



载入学习进度

上网求助或阅读

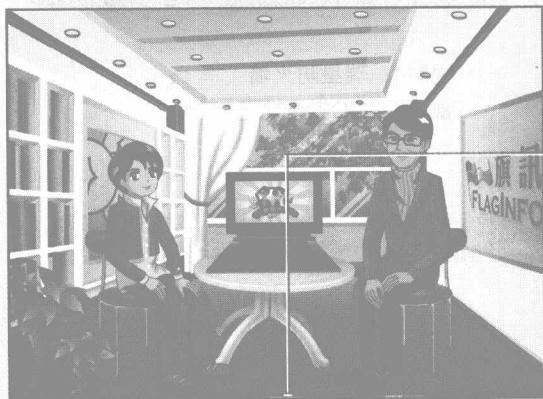
退出光盘



多媒体互动视频教学光盘 使用说明

超过 300 分钟的视频教学，体验坐在家中上课的感觉

光盘运行界面



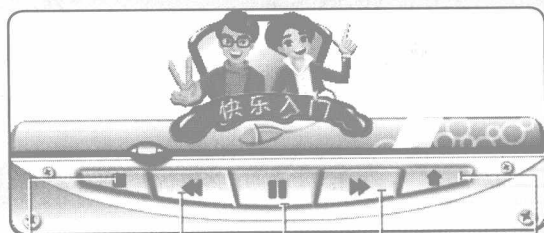
进入视频教学模式后，系统会自动进行讲解。单击界面最下方的小三角按钮，即可开启控制面板。在面板中可以对视频内容进行控制。

练习模式



控制视频教学播放

控制音量



停止

快退

播放/暂停

快进

返回

单击“练习”按钮进入练习模式，界面将自动缩小到只有一个文本框和播放按钮的控制界面，此窗口可以拖动到屏幕任意位置，读者可以根据讲解边学边练。单击“返回”按钮将切换到播放界面。

光盘索引

关于黑客

视频1: 网络知识入门

视频2: 黑客知识入门

视频3: 黑客必备知识

视频4: Ipconfig命令

打造安全的个人电脑

视频1: 使用Windows防火墙

视频2: 设置Windows XP安全登录

视频3: 瑞星杀毒软件

视频4: 瑞星防火墙

视频5: QQ安全防范

Windows漏洞防范

视频1: NetBIOS漏洞防御

视频2: IPC\$漏洞的防范

视频3: Outlook Express漏洞欺骗

IE浏览器的安全防范

视频1: 防范网页攻击

视频2: 防范网页泄密

视频3: 防范恶意代码攻击

做好备份与还原

视频1: 使用系统还原点备份与恢复系统

视频2: 驱动程序的备份还原

视频3: 备份和恢复聊天记录

视频4: 备份注册表

视频5: 恢复注册表

视频6: “文件和设置转移向导”备份数据

视频7: “文件和设置转移向导”恢复数据

木马防御与远程控制

视频1: 木马克星ipamor

视频2: 木马清除工具Trojan Remover

视频3: Dame Ware远程控制

视频4: QQ远程控制技术

恢复丢失的数据

视频1: 使用BadCopy Pro恢复数据

视频2: 使用Easy Recovery修复与恢复文件

视频3: 使用Final Data修复与恢复文件

第1课 黑客世界——正确理解黑客

1.1 什么是黑客	2
1.2 恶意入侵者的危害	4
窃取密码	4
使计算机或系统感染病毒	4
记录按键	4
恶意入侵者的危害	4
后门操作	5
形成僵尸网络	5
监听电子邮件	5
1.3 黑客文化	6
1.4 黑客与法律	8

第2课 黑客基础 I ——必备的基础知识

2.1 黑客入侵过程	12
攻击前奏	12
实施攻击	13
巩固控制	13
继续深入	13
2.2 网络身份证——IP地址	14
什么是IP地址	14
IP地址分类	15
查找对方IP地址	15
2.3 被黑客利用的通道——端口	18
什么是端口	18
按性质区分端口	18
按提供的服务方式区分端口	19
常见端口	19
查看对方的端口	20
2.4 黑客是怎样破解账号与密码的	21
2.5 黑客的高级入侵方式	22
拒绝服务攻击	22
分布式拒绝服务攻击	23
DDoS攻击对Web站点的影响	23

第3课 黑客基础 II ——局域网基础

3.1 局域网知识	26
什么是局域网	26
局域网的构成	26

网络操作系统	27
局域网的几种工作模式	27
3.2 路由基础知识	29
什么是“路由”	29
路由器的原理	29
路由器的作用	30
设置家庭路由器	30
网络中的网关	31

第4课 黑客基础Ⅲ——基本命令使用

4.1 Ping命令的使用	34
Ping检测网络故障	34
Ping命令的常用参数选项	36
4.2 Netstat 命令的使用	38
4.3 IPConfig命令的使用	40
4.4 Tracert命令的使用	42
Tracert使用方法	42
如何设置到目标地址最大跳跃数	43
如何解决网速变慢故障	43

第5课 黑客的耳目——扫描器搜索目标

5.1 极速扫描器	46
5.2 X-Scan综合扫描器	47
锁定扫描的目标范围	47
设置X-Scan扫描的模块	48
X-Scan参数设置	50
使用X-Scan扫描网络	51
扫描结果分析	52
5.3 个人服务扫描器	53
5.4 用MBSA检查Windows系统的安全	54
5.5 扫描目标主机开启的端口	55

第6课 黑客的猎犬——嗅探器捕获信息

6.1 Sniffer Portable	58
6.2 Iris嗅探器	59
Iris基本使用	59
Iris简单应用实例	60

6.3 艾菲网页侦探	62
6.4 网络欺骗的应对与防范	63
什么是网络欺骗	63
网络欺骗的主要技术	63
欺骗空间技术	64
增强欺骗质量	65

第7课 打开盒子的钥匙——系统与文档的解密

7.1 清除BIOS密码	68
万能密码法	68
Debug大法	68
使用NU的RESCUE工具软件	69
FlashBios命令	69
放电大法	70
7.2 清除Windows 2000登录密码	71
本地清除密码	71
远程清除密码	72
7.3 清除Windows XP登录密码	74
删除SAM文件	74
利用LC4从SAM文件中找密码	75
妙用密码重设盘	75
万能钥匙ERD Commander	77
7.4 清除屏幕保护密码	79
重启法	79
硬件冲突法	79
查看数据法	79
7.5 EFS加密和解密	80
EFS加密原理	80
EFS密码恢复步骤	81
关于EFS解密的疑难解答	82
加强EFS的安全	83
7.6 找回Office密码	85
使用Office Password Remover 恢复Word密码	85
使用WORD97/2000/XP密码查看器找回密码	86
使用Excel Password Recovery轻松找回Excel文档密码	87
7.7 找回压缩文件密码	90
找回WinZIP加密密码	90
WinRAR压缩文件的破解	91
7.8 解密被加密的光盘	92
使用File Monitor检测加密光盘	92
抓取镜像文件的IsoBuster	93
7.9 获取FTP站点用户名密码	95

第8课 看好系统的后门——基于认证的入侵

8.1 IPC\$认证的相关知识	98
什么是IPC?	98
关于Windows操作系统的默认共享	98
命令提示符中的命令介绍	99
8.2 IPC\$认证连接实例	100
8.3 远程命令相关知识	102
8.4 IPC\$认证连接实例	103
编写BAT文件	103
与目标主机建立IPC\$连接	103
拷贝文件至目标主机	104
通使远程主机执行hack.bat文件	104
验证账号是否成功建立	105
8.5 IPC\$空连接漏洞	106
漏洞描述	106
漏洞带来的影响	106
通过IPC\$空连接获取信息实例	106
8.6 IPC\$认证漏洞的安全解决方案	108
删除默认共享	108
禁止空连接进行枚举攻击的方法	109
关闭Server服务	109
8.7 黑客利用Telnet入侵实例	110
实例一	111
实例二	112
8.8 Telnet高级入侵分析和防范	114
AProMan简介	114
instsrv简介	114

第9课 遥控你的电脑——远程控制技术

9.1 远程控制基础知识	120
远程控制的原理	120
远程控制的实现	120
远程控制的应用	121
远程控制安全性	121
9.2 使用DameWare进行远程控制	122
启动DameWare	122
DameWare功能预览	122
连接远程主机	123
远程执行命令	124

修改系统参数并远程控制系统	125
9.3 使用PCanywhere进行远程控制	128
设置被控端	128
设置主控端	129
设置网络连接	130
远程连接	131

第10课 你的聊天他知道——QQ攻击与防范

10.1 QQ密码破解方式	134
黑客盗取	134
木马盗取	134
10.2 本地破解QQ原理	136
本地破解的奥秘	136
本地破解的原理和方法	136
10.3 QQ密码在线探测	138
10.4 木马盗取QQ	139
QQ简单盗	139
QQ流感大盗	140
QQ盗号王	142
10.5 QQ炸弹攻击	143
飘叶千夫指	143
碧海青天QQ大使	144
QQ细胞发送器	145
10.6 避开攻击保护密码的八个小技巧	147

第11课 内部防范——局域网安全攻击与防范

11.1 使用代理破除限制	152
什么是代理服务器	152
局域网使用代理上网	152
11.2 突破网关限制的常用工具	154
SocksCap32	154
Socks2HTTP	154
E-BorderClient	155
File Gateway	155
11.3 局域网网络执法官	156
选择嗅探驱动程序	156
网络用户管理	156
11.4 局域网全面控制工具NetSuper	157

11.5 局域网内BT下载提速	159
使用端口映像	159
本机上安装端口映射器	160

第12课 木马屠城——木马植入与防范

12.1 木马攻击流程	164
木马的构成	164
配置木马	164
运行木马	165
信息反馈	165
木马连接	165
传播木马	165
远程控制	166
12.2 常用木马类型	167
12.3 木马植入方法	169
木马传播途径	169
木马伪装方法	169
常用木马伪装配置	170
12.4 木马连接与远程控制	173
连接木马服务端	173
客户端的远程控制	174
12.5 网页木马入侵与防范	175
网页木马的准备	175
网页伪装木马	175
12.6 专杀工具清除木马病毒	176
Trojan Remover清除木马	176
The Cleaner清除木马	177
木马克星IParmor	178
12.7 手工揪出藏在系统中的木马	181
网络尖兵工作原理	181
检查任务管理器中的进程	181
检查启动项、注册表、ini文件、服务	182
检查系统文件夹	182
检查开放的端口	182
注意捆绑的木马	183
手动清除木马	183

第13课 深入核心——篡改Windows注册表

13.1 什么是注册表脚本	186
13.2 编写注册表脚本	188

13.3 注册表脚本应用实例.....	190
登录Windows时显示消息文字	190
修改Windows的常用设置选项	191
让“运行”、“注销”和“关机”消失	192
让“运行”、“注销”和“关机”回到从前	193
关闭随OE和系统而启动的Messenger	194
13.4 恶意JavaScript脚本的编写	195
什么是JavaScript?	195
语法标记	195
在Html文档中嵌入JavaScript	196
JavaScript脚本操作注册表	196
13.5 JavaScript脚本篡改注册表	198
修改IE标题栏	198
在右键加进网页链接	198
IE设置项变灰（不可用）	199
把主页加入Windows启动	199

第14课 见招拆招——注册表入侵与防范

14.1 形形色色的访客	202
日常操作中对注册表的访问	202
软件安装中对注册表的访问	204
危险的注册表启动	205
注册表的远程入侵实例	206
14.2 恶意代码修改注册表的防范	209

第15课 有备无患——系统与重要数据的备份与恢复

15.1 Windows的备份与还原	214
系统工具备份	214
系统工具还原	215
15.2 Ghost系统备份与恢复	217
保存镜像	217
使用镜像还原	218
15.3 一键恢复精灵系统备份与恢复	221
启动备份功能	221
设置用户密码	221
还原操作系统	223
15.4 误删除分区、格式化数据恢复	224
使用Final Data恢复数据	224
使用EasyRecovery恢复数据	226
15.5 Ghost误操作的恢复	228

第16课 亡羊补牢——病毒防治与清除

16.1 中毒的症状	232
16.2 清除Autoun闪存病毒	234
16.3 清除AV终结者	236
揭秘“AV终结者”	236
彻底清除“AV终结者”	237
如何预防“AV终结者”	238
16.4 清除熊猫烧香	239
熊猫症状分析	239
狡猾的病毒	239
初战告捷	240
狂扫穷寇	240
防“病”于未然	241

第17课 防黑于未然——信息安全保卫战

17.1 谁是网络世界的救世主	244
17.2 捕获不请自来的“客人”	247
准备工作	247
进程伪装型后门的歼灭	249
服务欺骗型后门的战役	250
最艰难的寻找：Ring 0后门	251
清理不受欢迎的附属产品	252

第18课 防范黑客——系统服务速查

18.1 利用进程了解你的系统	256
18.2 常用Windows系统进程列表	257
18.3 揭露进程伪装术	259
18.4 进程树的妙用	261
18.5 封杀进程的另类方法	262
封杀对方机器进程	262
定时封杀本机进程	262
封杀不可见窗口的进程	262

Lesson

1

黑客世界——正确理解黑客

“黑客”是一个神秘而特殊的群体，从最初屈指可数的几位黑客，到今天网上的黑客泛滥成灾，黑客真正的定义和精神宗旨已难觅踪影。黑客究竟经过了怎样的一个发展过程，又有多少黑客前辈让我们缅怀？本课将为读者介绍黑客的发展、行为、精神以及法律范畴，让读者了解黑客，并正视网络安全问题。



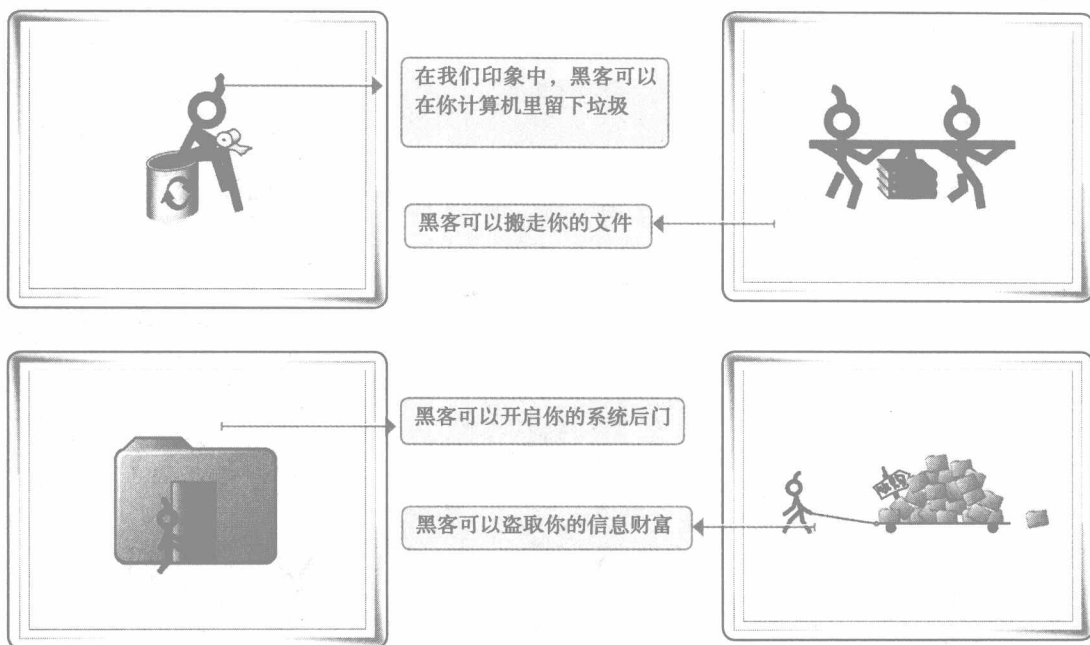
本课导读

- 1.1 什么是黑客
- 1.2 恶意入侵者的危害
- 1.3 黑客文化
- 1.4 黑客与法律

什么是黑客

如今，大多数电脑用户或多或少都听说过“黑客”一词，由于媒体的宣传，“黑客”的名声已经非常恶劣了。“黑客”一词让人们联想到那些怀有恶意的人，他们攻击普通用户、诈骗勒索一些企业、窃取信息，甚至摧毁经济或者侵入军用计算机系统。无可否认，网络上确实有很多心怀不轨的黑客，但从黑客发展历程来看，这些破坏者只是黑客群体中很小的一部分，下面我们来大致了解一下黑客发展史。

电脑黑客这个词是在上世纪 60 年代中期首次出现的。黑客一般是程序员——那些忙忙碌碌写代码的人。黑客们是些理想家，他们总能找到用电脑的新方法、总能编出别人做不出来的程序。他们是计算机业界的先锋，小到应用程序大到操作系统他们都能开发。



小知识：按照这个定义的话，比尔·盖茨、史蒂夫·乔布斯、史蒂夫·沃兹尼亚克都算是黑客了——他们看到了计算机的潜能，并创造性地实现了这些潜能。

这些黑客的一个统一特征就是，他们有着强烈的好奇心，有时候甚至是有些偏执。不仅以自己开发新程序的能力而自豪，并且还以能够弄明白其他程序或系统的原理为荣。

如果程序有 bug——代码缺陷，黑客们会开发并发布一些称为补丁的程序来解决此类问题。