

## 第八章 数据的加密与解密

### 8.1 BIOS的密码设置与清除

BIOS (Basic Input Output System) 即基本输入/输出系统, 它实际上是被固化到计算机主板上的 ROM 芯片中的一组程序, 为计算机提供最低级的、最直接的硬件控制。和其它程序不同的是, BIOS 是储存在 BIOS 芯片中的, 而不是储存在磁盘中, 由于它属于主板的一部分, 因此大家有时就称呼它一个既不同于软件也不同于硬件的名字“Firmware”(固件), 它主要用于存放自诊断测试程序 (POST 程序)、系统自举装入程序、系统设置程序和主要 I/O 设备的 I/O 驱动程序及中断服务程序。

#### 8.1.1 BIOS 密码设置方法

如果你不希望别人用自己的电脑, 可设置 BIOS 的密码功能给电脑加一把“锁”。BIOS 版本虽然有多个, 但密码设置方法基本相同。现以 Award 4.51 PG 版本为例。在计算机启动过程中, 当屏幕下方出现提示: “Press DEL to enter SETUP”时按住 Del 键便可进入。

方法是: 开机时, 当屏幕下方出现提示“Press DEL to enter SETUP”时按住 Del 其中与密码设置有关的项目有:

“BIOS FEATURES SETUP”(BIOS 功能设置)

“SUPERVISOR PASSWORD”(管理员密码)

“USER PASSWORD”(用户密码)

选择其中的某一项, 回车, 即可进行该项目的设置。选择管理员或用户密码项目后回车, 要求输入密码, 输入后再回车, 提示校验密码, 再次输入相同密码, 回车即可。需要注意的是, 进行任何设置后, 在退出时必须保存才能让设置生效。(保存方法是: 设置完毕后选择“SAVE & EXIT SETUP”或按 F10 键, 出现提示“SAVE to CMOS and EXIT (Y/N) ?”此时按下“Y 键”, 保存完成。)

具体设置分以下几种方法:

设置方法 1: 单独设置“SUPERVISOR PASSWORD”或“USER PASSWORD”其中的任何一项, 再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“Setup”, 保存退出。这样, 开机时按 Del 键进入 BIOS 设置画面时将要求输入密码, 但进入操作系统时不要求输入密码。

设置方法 2: 单独设置“SUPERVISOR PASSWORD”或“USER PASSWORD”其中的任何一项, 再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“System”, 保存退出。这样, 不但在进入 BIOS 设置时要求输入密码, 而且进入操作系统时也要求输入密码。

设置方法 3: 分别设置“SUPERVISOR PASSWORD”和“USER PASSWORD”, 并且采用两个不同的密码。再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“System”, 退出保存。这样, 进入 BIOS 设置和进入操作系统都要求输入密码, 而且输入其中任何一个密码都能进入 BIOS 设置和操作系统。但“管理员密码”和“用户密码”有所区别: 以“管理员密码”进入 BIOS 程序时可以进行任何设置, 包括修改用户密码。但以“用户密码”进入时, 除了修改或去除“用户密码”外, 不能进行其它任何设置, 更无法修改管理员密码。由此可见, 在这种设置状态下, “用户密码”的权限低于“管理员密码”的权限。

#### 8.1.2 BIOS 密码的破解

如果我们遗忘 BIOS 密码该怎么办呢? 不要着急, 以下几招可以帮助你。对于用户设置的这两种密码, 我们的破解方法是有所区别的:

### （一）破解“USER PASSWORD”

#### 方法一：Debug 法

在遗忘密码之后只需在 DOS 状态下启动 Debug，然后输入如下命令即可手工清除密码：

```
_o 70 16  
_o 71 16  
_q
```

另外，不熟悉 Debug 的用户也可下载一个专门破解 CMOS 密码的工具软件 Cmospwd。然后在 DOS 启动该程序，它会将用户的 CMOS 密码显示出来（Cmospwd 支持 Acer、AMI、AWARD、COMPAQ、DELL、IBM、PACKARD BELL、PHOENIX、ZENITH AMI 等多种 BIOS），使用非常方便。

#### 方法二：软件破解

现在有很多检测系统或开机密码的软件，最常见的有 BiosPwds、Cmospwd 等。其中 BiosPwds 是其中比较优秀的一个，可以检测出 BIOS 版本、BIOS 更新日期、管理员密码、CMOS 密码、密码类型等，而且使用方法简单，单击窗口中的“获取密码”按钮即可显示出 BiosPwds 所检测到的所有信息。

但是由于软件破解密码时，是对 BIOS 编码过的密码进行逆向解码，所以有时也许会发现程序的密码和真实的密码并不相同，这也属于正常现象，所以这一招有时会不灵的。

#### 方法三：自己编制文件破解

进入 MS-DOS 环境，在 DOS 提示符号下输入 EDIT 并回车（若你发现按 EDIT 出现错误，就是说你没有 edit.com 这个文件，请看下一条方法），输入：

```
ALT+179 ALT+55 ALT+136 ALT+216 ALT+230 ALT+112 ALT+176 ALT+32 ALT+230  
ALT+113 ALT+254 ALT+195 ALT+128 ALT+251 ALT+64 ALT+117 ALT+241 ALT+195
```

注：输入以上数据先按下 ALT 键，接着按下数字键盘里（按键盘上面那一排数字键是没有作用的）的数字键，输完一段数字后再松开 ALT 键，然后再按下 ALT 键。在操作过程中，屏幕上会出现一个乱字符，我们不用管它。然后在“file”菜单下选择“save”，保存为 Cmos.com 文件，接着退出到 MS-DOS 环境下，找到 cmos.com 这个文件，看看他是否是 20 个字节，若不是就说明你输入错了，须重新输入。确认后，直接运行 cmos.com，屏幕上应该没有任何提示信息，然后重新启动计算机即可清除 CMOS 里的密码，当然，CMOS 里的其它设置也会同时被清除，这就需要我们重新设置了。

#### 方法四：DOS 下破解

这个方法直接在 MS-DOS 环境下便可完成，在 MS-DOS 环境下输入：COPY CON CMOS.COM 后回车，继续输入如下十个字符：ALT+176 ALT+17 ALT+230 p ALT+176 ALT+20 ALT+230 q ALT+205 <空格>，然后按“F6”键，再按回车保存，运行 Cmos.com 文件后，重新开机即可。

### （二）破解“SUPERVISOR PASSWORD”

#### 第一招：通用密码

每个主板厂家都有主板设置的通用密码，以便于提供技术支持之用。如果我们知道了该主板的通用密码，那么无论是开机，还是进行 CMOS 设置都可以“穿墙而入”。

需要注意的是各主板厂家出于某些原因，不同时期主板的通用密码会有所不同，因此这一招并不能通行天下，我们只有多尝试几次，是否有用就要看运气了。

Award BIOS 通用密码：j256、LKWPETER、wantgirl、Ebbb、Syxz、aLLy、AWARD?SW、AWARD\_SW、j262、HLT、SER、SKY\_FOX、BIOSTAR、ALFAROME、lkwpeter、589721、awkard、h996、CONCAT、589589。

AWI BIOS 通用密码：AMI、BIOS、PASSWORD、HEWITT RAND、AMI\_SW、

LKWPETER、A.M.I。

### 第二招：CMOS 放电

目前的主板大多数使用纽扣电池为 BIOS 提供电力，也就是说，如果没有电，它里面的信息就会丢失了。当它再次通上电时，BIOS 就会回到未设置的原始状态，当然 BIOS 密码也就没有了。

我们先要打开电脑机箱，找到主板上银白色的纽扣电池。小心将它取下，再把机箱尾部电源插头拔掉，用金属片短接电池底坐上的弹簧片，大概隔 30 秒后，再将电池装上。

此时 CMOS 将因断电而失去内部储存的信息，将它装回，合上机箱开机，系统就会提示“CMOS Checksum Error-DeFaults Loaded”，那就是提示你“CMOS 在检查时发现了错误，已经载入了系统的默认值”，BIOS 密码破解成功。

### 第三招：跳线短接

如果主板的 CMOS 芯片与电池整合在了一块，或者是电池直接被焊死在了主板上，还有就是我们用了第二招“CMOS 放电法”，结果没起作用，那么我们就要用跳线短接这一招了。

打开机箱后，在主板 CMOS 电池附近会有一个跳线开关，在跳线旁边一般会注有 RESET CMOS（重设 CMOS）、CLEAN CMOS（清除 CMOS）、CMOS CLOSE（CMOS 关闭）或 CMOS RAM RESET（CMOS 内存重设）等字样，用跳线帽短接，然后将它跳回就行了。

由于各个主板的跳线设置情况不太一样，所以在用这一招的时候，最好先查阅主板说明书。还要注意，在 CMOS 放电或者清除 CMOS 中的数据时，不要在系统开机的情况下进行，建议断掉电脑电源。

### 8.1.3 BIOS 的保护技巧

BIOS 升级失败或病毒发作（如 CIH）及其他一些原因会导致 BIOS 出现故障，这就要求我们采用适当的方法对 BIOS 进行保护。

(1)保护Boot Block块：BIOS中的Boot Block引导块是BIOS中的一个单独区域，专门负责在BIOS遭受破坏时使用ISA显卡和软驱启动系统。用户在升级BIOS时通常不会修改这个区域。

当升级出现问题时，我们就能利用这个 Boot Block 引导块重新启动计算机并对系统进行恢复了。不过值得注意的是，这个 Boot Block 引导块并非不能修改，BIOS 升级程序在适当的条件下也可对该部分内容进行刷新！许多用户在对 BIOS 进行升级时并没有注意这一点，而是对 BIOS 中的所有信息进行升级，从而给升级失败之后的修复带来了很大的麻烦。其实，BIOS 升级程序大多提供了跳过 Boot Block 引导块的功能，如 Awdflash 就提供了一个“/SB”参数，用户在升级 BIOS 时，只需加上“/SB”参数就可以保护芯片原来的 Boot Block 块不被修改。这样万一在整个升级过程有什么失误，用户还可以借助 Boot Block 引导块对 BIOS 进行恢复。

(2) 将 BIOS ROM 中的信息备份下来：对于 Awdflash 而言，系统已经提供了一个专门用于备份原有 BIOS 信息的“/SY”参数，用户只需执行“Awdflash BIOS 文件名/pn/sv”命令，它就会将原有的 BIOS 备份下来。

### 8.2 Windows 的密码设置与破解

在使用 Windows 的时候，我们为了安全，要作用户安全设置：

#### 1. 禁用 Guest 账号

在计算机管理的用户里面把 Guest 账号禁用。为了保险起见，最好给 Guest 加一个复杂的密码。你可以打开记事本，在里面输入一串包含特殊字符、数字、字母的长字符串，然后把它作为 Guest 用户的密码拷进去。

#### 2. 限制不必要的用户

去掉所有的 Duplicate User 用户、测试用户、共享用户等等。用户组策略设置相应权限，

并且经常检查系统的用户，删除已经不再使用的用户。这些用户很多时候都是黑客们入侵系统的突破口。

### 3. 创建两个管理员账号

创建一个一般权限用户用来收信以及处理一些日常事物，另一个拥有 Administrators 权限的用户只在需要的时候使用。

### 4. 把系统 Administrator 账号改名

大家都知道，Windows 2000 的 Administrator 用户是不能被停用的，这意味着别人可以一遍又一遍地尝试这个用户的密码。尽量把它伪装成普通用户，比如改成 Guesycludx。

### 5. 创建一个陷阱用户

什么是陷阱用户？即创建一个名为“Administrator”的本地用户，把它的权限设置成最低，什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。这样可以让那些 Hacker 们忙上一段时间，借此发现它们的入侵企图。

### 6. 把共享文件的权限从 Everyone 组改成授权用户

任何时候都不要把共享文件的用户设置成“Everyone”组，包括打印共享，默认的属性就是“Everyone”组的，一定不要忘了改。

### 7. 开启用户策略

使用用户策略，分别设置复位用户锁定计数器时间为 20 分钟，用户锁定时间为 20 分钟，用户锁定阈值为 3 次。

### 8. 不让系统显示上次登录的用户名

默认情况下，登录对话框中会显示上次登录的用户名。这使得别人可以很容易地得到系统的一些用户名，进而做密码猜测。修改注册表可以不让对话框里显示上次登录的用户名。方法为：打开注册表编辑器并找到注册表项“HKLMSoftwareMicrosoftWindows TCurrentVersionWinlogonDont-DisplayLastUserName”，把 REG\_SZ 的键值改成 1。

我们还要注意密码安全设置：

#### 1. 使用安全密码

一些公司的管理员创建账号的时候往往用公司名、计算机名做用户名，然后又把这些用户的密码设置得太简单，比如“welcome”等等。因此，要注意密码的复杂性，还要记住经常改密码。

#### 2. 设置屏幕保护密码

这是一个很简单也很有必要的操作。设置屏幕保护密码也是防止内部人员破坏服务器的一个屏障。

#### 3. 开启密码策略

注意应用密码策略，如启用密码复杂性要求，设置密码长度最小值为 6 位，设置强制密码历史为 5 次，时间为 42 天。

#### 4. 考虑使用智能卡来代替密码

对于密码，总是使安全管理员进退两难，密码设置简单容易受到黑客的攻击，密码设置复杂又容易忘记。如果条件允许，用智能卡来代替复杂的密码是一个很好的解决方法。

#### 8.2.1 Windows 98 密码的设置与破解

关于用户密码，很多人都存在一个误区，即认为用户密码就是开机密码。事实上 Windows 在默认的情况下，是没有开机密码的。那么用户密码是用来干什么的呢？是用来保护“个性”的。系统允许设置多个用户，其目的并不是为了保护用户的隐私。而是为每一个用户保存了一组系统外观的配置，以适应不同用户不同的使用习惯，只不过要输入密码而已。所以这个密码根本起不到保密的作用，只是个摆设罢了。

用户密码可以在控制面板的“密码”或“用户”工具中设置：在控制面板中，双击“用

户”图标，点击“新建”按钮，会出现“添加用户”窗口，点击“下一步”按钮，输入新添加的用户名，然后点击“下一步”，在出现的窗口中输入新用户密码，接着点击“下一步”按钮，会出现“个性化设置”窗口，选择你需要的项目（不选也可以），然后再次点击“下一步”按钮，就可以为本机添加一个新用户。用同样的方法给每个可以使用此机器的用户建立一个用户名，然后你就可以输入密码了，当然也可以留到用户登录后自己修改密码。

对 Windows 有点了解的人都知道在 Windows 98 系统中，这个密码系统是毫无安全性可言的。它在开机或更换用户登陆时启动，输入正确的密码后就可以使用系统，但是即使不知道密码也可以用 ESC 键跳过登陆程序，直接进入系统。这时我们可以通过更改注册表，来强制用户在开机时必须输入用户名和密码才能进入 Windows。实现方法：点击“开始”菜单中的“运行”，输入 regedit，打开注册表编辑器，依次打开到 HKEY\_LOCAL\_MACHINE\Network\Logon，然后新建一个 DWORD 值，将其命名为“Mustbevalidated”，值改为 1，就可以了。

和 Windows 98 不同，Windows 2000 在这一方面作了很大的改进，如果把系统设定为：用户必须输入用户名和密码才能使用本机，那么如果不输入正确的用户名密码就不能进入系统；同时将用户分为管理者、用户和来宾三类，各有其不同的权限。这为规范管理计算机用户提供了手段。

另外，熟悉 Windows 98 系统的用户都知道，有关用户密码信息都存贮在 Windows 目录下扩展名为“.pwl”的文件中。这里告诉你一个简单而有效的保护方法：单击“开始”→“运行”，输入 sysedit 命令，打开“系统配置实用程序”。选中关于文件 System.ini 文件。这时你会发现其列表项中有一项标题为[Password Lists]的项，这就是有关用户密码文件的链接记录，其中 HUT=C:\WINDOWS\HUT.PWL（等号前的“HUT”为用户名，等号后为该用户密码文件的存放路径及文件名）。知道了这点，我们就可以对其进行修改，以便任意指定文件。比如，你可以事先将源文件 HUT.PWL 改名并复制到另一目录中，如在 DOS 方式下，执行命令：COPY C:\WINDOWS\HUT.PWL C:\WINDOWS\SYSTEM\S1.DAT。而后再将 System.ini 中密码文件的存放路径改为 HUT=C:\WINDOWS\SYSTEM\S1.DAT。这样，就没有人再能轻松地找到你的密码文件了。

如果遗忘 Windows 的用户密码会怎么样呢？放心，这不会影响系统的启动，但它将导致用户无法进入自己的个人设置，因此破解 Windows 的启动密码以找回丢失的“个性”也是很有必要的。为此，我们可删除 Windows 安装目录下的\*.PWL 密码文件及 Profiles 子目录下的所有个人信息文件，然后重新启动 Windows，系统就会弹出一个不包含任何用户名的密码设置框，我们无需输入任何内容，直接单击“确定”按钮，Windows 密码即被删除。另外，将注册表 HKEY\_LOCAL\_MACHINE\Network\Logon 分支下的 UserProfiles 修改为“0”，然后重新启动 Windows 也可达到同样的目的。

### 8.2.2 Windows98 系统平台的安全策略

Windows 98 系统平台的安全策略就是保证系统程序和应用程序的正常运行，用户文件数据的安全、完整和保密，程序及数据的备份和故障恢复。

#### 一、系统安装时的安全策略

##### 1. 划分硬盘分区

安装时要考虑的重要一点就是硬盘的划分。通常用户的硬盘容量是比较大的，一般几 G 至几十 G 不等，如果只设定一个硬盘 C，所有的软件及数据都放在一起，C 盘负荷较重，容易发生故障；有些病毒专门破坏 C 盘文件及数据，如 CIH 病毒；而且 C 盘出现异常及瘫痪后，会造成数据丢失，不易恢复。为便于日后的使用和维护，需将硬盘进行分区，将一个物理硬盘分成几个逻辑硬盘，如 C、D、E、F，安装时将系统程序和应用程序及常用数据放在 C 盘，D 盘存放重要数据及备份，E 盘等也作相应安排，这样做便于安全策略的实施。如

果硬盘容量较小可分成 C 和 D，分区的设置可以在安装之前通过 FDISK 实现，也可在安装之后通过 PMagic9x 等软件实现。

## 2. 设置密码

如果一台机器只是单一用户使用，设置开机密码是一种简单有效的安全措施。如果一台机器多人使用，就需设置多用户密码，安装 windows98 系统时，通过“控制面板”中的“密码”及“用户”设置实现。先设置管理员的用户及密码，重新启动计算机后，以“管理员”身份进入 windows 98，通过控制面板中的“用户”向导提示，设置用户名和密码。这样，不同的用户在一台机器上实现了自己的桌面系统，可设置相应的使用权限。

## 二、系统运行中的安全策略

### 1. 系统软件的安全

系统软件安装完毕后，要时常进行清理维护工作，如磁盘扫描、磁盘碎片整理、优化系统、删除临时及垃圾文件，目的是清除隐患、提高系统效率。也可使用 windows 优化大师、硬盘碎片整理等工具软件。应用软件的安全应用软件有很多，用户应尽量使用正版件，许多盗版软件系统不完整，含有缺陷和病毒，也不要任意从网上下载软件，随意安装。软件删除时也要注意方法，有些软件可直接删除目录及图标；有些通过自带的卸载程序；有些则需通过“控制面板/添加删除程序”来完成。不恰当的安装和卸载程序会造成系统故障。

### 2. 浏览器的安全

浏览器也需进行安全设置，以 IE5 为例，用户可在“浏览器/工具/Internet 选项/安全”中设置“Internet”及“本地 Intranet”选项，进行自定义安全设置。使用时不访问可疑网站，不浏览可疑网页，出现异常时及时关闭浏览器，定时清理历史记录和临时文件夹，还要依靠个人防火墙实时监测，保证系统安全。

### 3. 电子邮件的安全

电子邮件的使用使人们感受到信息交流的快捷方便，但也给人们带来了一些麻烦，广告邮件肆意散发，垃圾邮件满天飞；邮件炸弹造成邮件服务器故障，电子邮箱无法使用；病毒经由邮件传播，干扰破坏邮箱的使用。

为了保证邮箱的正常使用，可采取以下措施，对于广告邮件和垃圾邮件，可建立相应的邮件规则，设置为拒收或直接删除；为防止邮件炸弹，不开启邮件的预览功能，不打开可疑邮件，直接将其删除；为防邮箱爆满，不使用邮件的“自动回复”功能，根据邮箱容量对大邮件进行过滤删除。安装邮件实时监测程序，查杀有毒邮件。

### 4. 病毒的检测和防范

系统在使用时经常遇到病毒的威胁，病毒的传播机制不断更新，危害越来越大，用户应安装防病毒程序，定时升级，经常检测系统，对外来光盘和软盘认真查毒，设置实时检测，防范病毒的感染和入侵。

### 5. 注册表的管理

注册表是 windows 98 的有效管理工具，很多故障通过修改注册表能够排除，例如：限制和规定用户使用权限，防止用户非法进入，IE 浏览器的故障排除等。当然，这要求对注册表比较熟悉，注册表可以通过导出和引入进行备份和恢复。

## 三、数据的备份和恢复

### 1. 系统文件和数据的备份

对硬盘分区表、引导扇区等关键数据要作相应备份，制作引导盘并妥善保管，以备系统维护和修复时使用。更进一步，可利用 GHOST 软件进行整个 C 盘的镜像工作，方法是经由 GHOST 引导盘启动或 windows98 启动时的 DOS 命令方式，运行 GHOST 软件，依次执行 local→partition→to image，按提示将 C 盘整个内容镜像到 D 盘或其他盘。以后系统出现故障时可迅速恢复 C 盘系统。GHOST 软件不仅可镜像某个逻辑硬盘，而且可克隆整个物理硬盘，

为系统的维护带来了极大方便。

## 2. 用户文件和数据备份

用户的文件和数据一般都存放在默认的相应目录下，例如：Office 文件放在 C:\>My Documents 目录下；Outlook Express 邮件内容放置在 C:\>Windows\Application Data\Identities\{02c31A..... }\Microsoft\Outlook Express 目录下；Foxmail 邮件内容放置在 C:\>Program Files\Foxmail 目录下；浏览器的收藏夹位于 C:\>windows\Favorites；历史记录存放在 C:\>indows\history，了解了这些，备份时只需将相应的子目录拷出，日后恢复时拷回即可。

对于其他的文件，用户也可建立相应的目录存放。重要数据和文件要有规律地进行备份，不能只放在机器中，要有多个备份，备份时要分门别类，必要时刻录到光盘。

### 8.2.4 Windows 2000/XP 登录加密方法

操作系统的安全现状令人堪忧，为图省事，许多人仅仅设置简单密码甚至不设防，而导致门户洞开，让敌人长驱直入，为所欲为。

Windows 2000/XP 自带的“本地安全策略”是一个不错的系统安全管理工具，通过对账户、密码、安全选项的合理设置，可以实现高安全性的系统登录。下面就以 Windows XP 为例介绍一下最主要的设置内容。

#### 1. 锁定无效登录

为了防止他人进入电脑时，反复用猜测密码的方式登录，我们可以锁定无效登录，当密码输入错误达设定次数后，便锁定此账户，在一定时间内不能再以该账户登录。设置方法是：进入控制面板，依次展开“管理工具”→“本地安全策略”，出现“本地安全设置”窗口（如图 8-1），在左侧列表中打开“账户策略”→“账户锁定策略”，在右边双击“账户锁定阈值”，在弹出的设置对话框中输入无效登录的次数（一般设 3 次为宜），确定后系统自动将锁定时长和计数器清零的时长设置为“30 分钟”，我们也可以打开这两个策略修改时间。经过以上设置，就能够阻止那些靠猜密码登录的非法用户了。

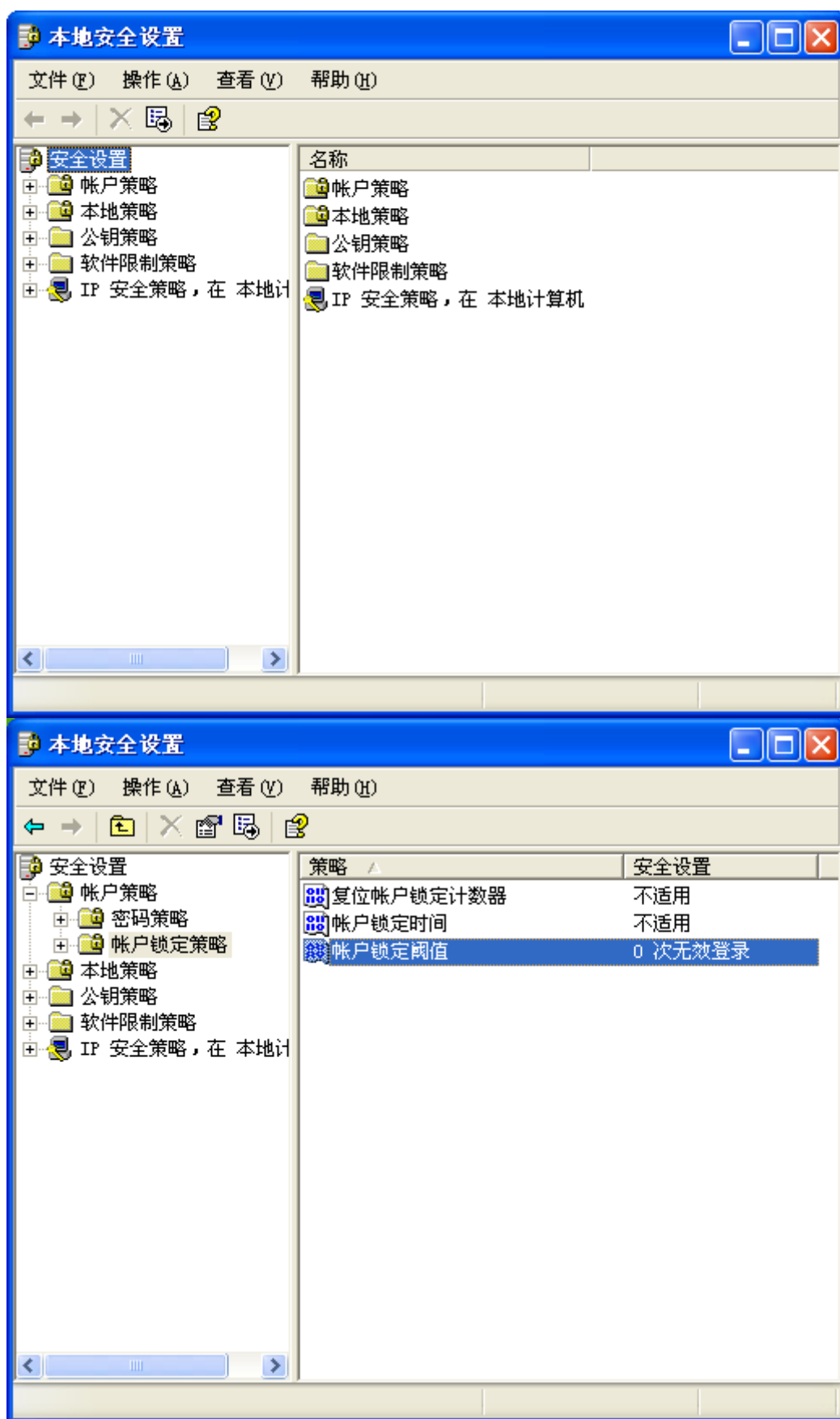


图 8-1 本地安全策略

## 2. 加强密码安全



为了让各账户的密码相对安全、不易被破解，我们可设置密码策略，加强密码的安全性，最有效的方法是增加密码的长度和复杂性，并定期更改密码。设置方法是：展开“账户策略”→“密码策略”，打开“密码长度最小值”，设置最少字符数为 8 位以上，接着打开“密码必须符合复杂性要求”，设置为“已启动”，还可打开“密码最长存留期”设置密码能使用的天数。经过以上三项设置后，凡新建账户或老账户更改密码时，系统会要求使用 8 位以上同时包含英文字母、数字或标点的密码，并且必须按设定的时间定期更改密码，密码的安全性将大大增强。

### 3. 设置账户保密

默认情况下，在系统登录框中会保留上次登录的用户名，这方便了该用户的登录，但却留下了安全隐患，特别是对管理员账户，暴露账户名称是一件非常危险的事情，因为不良企图者只需输入密码便可尝试登录，甚至使用专门的工具来攻破此账户。我们可以将上次登录账户隐藏起来，设置方法是：展开“本地策略”→“安全选项”，在右边找到“在登录屏幕上不要显示上次登录的用户名”，双击打开此策略，将其设置为“已启用”。进行此项设置后，系统启动或注销后，登录框中用户名为空，这样，必须输入完整有效的用户名和密码才能登录。

当我们忘记了密码的时候怎么办呢？有下面几种方法：

方法一：如果你不用管本来系统中包含的任意帐号，而且有两个操作系统的话，可以使用另外一个操作系统（能访问 NTFS，不然的话使用其他工具来访问 NTFS）启动，然后删除 C:\WINNT\system32\config 目录下的 SAM 文件，即帐号密码数据库文件。然后重新启动，这时管理员 administrator 帐号就没有密码了。当然，也可以取下硬盘换到其他机器上来删除 SAM 文件。

方法二：使用一个 DOS 启动盘，使用 NTFSDOS（网络上可以下载到）工具，这个工具可以从 DOS 下写 NTFS 分区的内容。然后到系统目录，比如 C:\WINNT\system32，下修改 logon.scr 为 logon.scr.bak，拷贝一个 command.com（2000 可以用 cmd.exe）文件更名为 logon.scr。这样启动机器后等待 15 分钟，本应该出现的屏幕保护现在变成了命令行模式，而且是具有 administrator 权限的，通过这个就可以修改密码或者添加新的管理员帐号了。完成过后再把屏幕保护程序的名字改回去。

方法三：制作并使用 Linux boot disks，这个启动盘可以访问 NTFS 文件系统，并且可以读取注册表并重写帐号密码。只需要根据其启动后的提示一步一步做就是了。成功率非常高。

方法四：可以使用一些第三方的密码恢复软件。

1. 使用 NTAccess（<http://www.sunbelt-software.com/product.cfm?id=265>）工具。这个工具可以绕过系统 syskey 的保护。该工具可以重新设置 NT、2000、XP 的密码通过使用经过 NTAccess 修改过的启动盘。

2. Passware Kit 也提供一个工具用来恢复系统密码。同样，这个工具也支持各种 NT 系统，具体介绍可以参考它的介绍。

3. 使用 O&O Bluecon 2000 使用办法和上面的这些第三方软件差不多。这里不详细介绍了。

#### 8.2.4 堵住 Windows 2000 系统登录时的漏洞

可能有些人知道，在 Windows 2000 的登录界面里，的确可以通过切换输入法，在“全拼”输入的“帮助”选单里选择“输入法入门”，右击窗口中的“选项按钮”，选择“跳至 URL”，在随后出现的对话框中输入想去的路径，就可以看到资源管理器的界面，也许因为我所使用的是 Windows 2000 的中文服务器版本，实际操作中并不能打开文件夹，但确实可以任意设置文件夹乃至硬盘分区的共享权限，从而使操作者可以通过网络完全控制装有

Windows 2000 操作系统的电脑上的所有数据资源。如果是服务器安装了 Windows 2000，那么后果更是不堪设想。

经过测试，不仅是“全拼”输入法存在这个问题，“郑码”输入法也存在这个问题。问题不仅是在“帮助”选单里的“输入法入门”中，在“帮助”选单里的“操作指南”里同样也存在。怎么办呢？

堵住漏洞有两招：

方法一：由于漏洞是出在“操作指南”和“输入法入门”的“选项按钮”上，如果我们能使这一功能不发挥作用，不就把这一漏洞堵住了吗？事实上，“操作指南”和“输入法入门”所对应的是我们所熟悉的与“.hlp”文件相似的另外一种类型的帮助文件，它的后缀名为“.chm”，而“选项按钮”是“.chm”文件所独有的。

我们在“WINNT（Windows 2000 的系统目录）\HELP”目录下找到了与这一漏洞相关的几个“.chm”文件，分别是“winime.chm”（输入法操作指南）、“winpy.chm”（全拼输入法帮助）和“winzm.chm”（郑码输入法帮助，这里的“郑”字被误写成了“政”字）。将这几个文件从“WINNT\HELP”目录中移走（包括将其删除）或是更名，那么再回到登录界面，我们会发现“操作指南”和“输入法入门”已经不起作用，Windows 2000 的登录漏洞也就被堵住了。而且去掉这几个帮助文件，对整个 Windows 2000 的使用并无影响。

方法二：当我们启动 Windows 2000 并成功登录后，按住“ALT+CTRL+DEL”组合键，选择“锁定计算机”将计算机锁定，再按下“Ctrl+Shift”组合键时，就不能进行输入法的切换了，这也就是我所说的第二种解决方法。不过使用这一方法的读者一定要记住，启动 Windows 2000 后，务必要先登录，再锁定计算机，千万别忘了。

### 8.2.5 增强 Windows 2000 的安全性

作为新一代的企业级网络系统，Windows 2000 在安全特性方面的设计注重了三个方面：

1. 对于基于 Internet 的新型企业的支持：帮助它们突破原有的企业网络和 Internet 的界限，满足移动办公、远程工作，和随时随地接入全球数字神经系统（Internet）进行通信和电子商务的需要。新一代的 Ex tranet 应用由此应运而生。

2. 微软在 Windows 2000 中提供的是一个安全性框架，并不偏重于任何一种特定的安全特性；即微软不是提供给用户一个锤子，让用户去找合适的钉子去敲。新的安全协议、加密服务提供者或者第三方的验证技术，可以方便地结合到 Windows 2000 的“安全服务提供者接口”（SSPI，Security Service Provider Interface）中，供用户选用。

3. Windows 2000 意识到用户对于向下兼容的需要，完全无缝地对 Windows NT 4.0 的网络提供支持，提供对 Windows NT 4.0 中采用的 NTLM（NT LAN Manager）安全验证机制的支持。用户可以选择依照自己的步调迁移到 Windows 2000 中对替代 NTLM 的 Kerberos 安全验证机制。

任何事物都有一定之规，系统管理员只有建立一套严密的安全规则，才能有效保障操作系统的稳定运转。本文就 Windows2000 操作系统的安全策略设计进行概要分析，旨在让大家从宏观角度了解系统管理员都应在哪些方面执行必要的安全配置，然后根据实际环境再在各个环节分别扩展，最终创建一个安全的 Windows 2000 服务器。下面我们来看看 Windows 2000 的安全策略：

#### 1. 确认所有磁盘分区的格式都为 NTFS

我们都知道，NTFS 分区磁盘具备高强度的访问控制机制，它能够有效地保护数据不被泄漏与篡改，这是其它格式的分区所不具备的，比如 FAT、FAT32 或者 FAT32x。所以，首先我们要确保服务器上的每个分区都被创建为 NTFS 格式。对于已经成为 FAT 格式的分区，我们可以使用“convert”程序完整地将其转换为 NTFS 格式。有一点提醒大家，当使用“convert”程序时，被转换的磁盘驱动器将被设置为对 Everyone 的 Full 控制权限，这将是非常危险的。

要解决这个问题，我们可以使用 Windows NT Server Resource Kit 中提供的“fixacls”软件，它能够帮助我们为驱动器重新配置更为合理的权限。

### 2. 确认“Administrator”帐号具有一个强健的口令

Windows 2000 允许我们设置口令的长度可达 127 位。通常情况下，长口令要比短口令强健，包含多种字符类型（指口令中包含字母、数字、标点符号或者非打印 ASCII 码）的口令要比单一字符类型口令（指口令全部是数字或者全部是字母）强健。所以，要实现最大的保护工作，就要为“Administrator”帐号创建至少 9 位长度的口令，并使口令的前 7 位中至少包含一个标点符号或者非打印字符（非打印字符是按住 ALT 键再输入小键盘数字产生的特殊字符）。而且，如果一个系统管理员管理着多个服务器，那么各服务器的“Administrator”帐号口令不应该相同。

### 3. 禁止不需要的服务

安装完 Windows 2000 Server 后，我们就应该禁止掉该服务器不承担任何的网络服务程序。特别要考虑的是，服务器是否需要运行任何 IIS 服务组件，是否需要运行文件和打印机共享服务。另外，除非特别需要，我们也不要再在服务器上安装其他应用程序。比如说，不要安装电子邮件客户端程序、office 产品等等。总之，不是必须运行的程序，不安装。

### 4. 禁止或删除不需要的用户帐号

我们应该经常查看用户帐号列表，将不怎么使用的帐号坚决禁止，或者干脆删除掉。比如，禁止 Guest 帐号。

### 5. 合理设置文件、目录和注册表的访问权限

根据具体需求，建议对 Windows 2000 安装后默认文件、目录以及注册表访问权限进行修改。

### 6. 删除所有不需要的文件共享

建议删除系统中所有不必要的文件共享服务，降低信息暴露风险。

### 7. 限制注册表不被匿名访问

默认情况下，注册表可以被远程访问。但我们要限制远程访问的用户，一般情况下只开放 administrators 的远程访问权限。要实现这个目的，需要修改注册表，步骤如下：

(1)添加下列 key: \HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg。

(2)选择 winreg，点击安全（Security）菜单，再点击权限（Permissions）。

(3)设置 Administrator 的权限为完全控制（Full Control），并确认列表中没有其他用户或组，点击确定（OK）。

通过以上对注册表键值的安全许可设置，就控制了哪些用户或组可以远程访问注册表内容。

### 8. 限制 LSA 信息不被匿名访问

LSA 是 Local Security Authority 的缩写，即本地安全颁发机构，它的功能是负责在本地计算机上处理用户登录与身份验证。LSA 的信息非常重要，我们应该限制匿名用户对 LSA 的访问。要实现这个目的，需要修改注册表，步骤如下：

(1)创建键值\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous

(2)赋值为 1，类型为 REG\_DWORD

### 9. 设置强健的口令策略

对于口令的设置管理，我们应该做到：

(1)最小口令长度至少为 8。

(2)建立适合的最小口令使用期限，一般在 1—7 天。

(3)建立适合的最大口令使用期限，一般不超过 42 天。

(4)设置口令的历史保持次数至少为 6，就是说，当前设置的口令不能与最近 6 次中的任何一次相同。

#### 10. 设置用户帐号锁定策略

用户帐号锁定就是指当一个帐号登录失败的次数超过 administrator 设定的次数，该用户帐号将被自动禁止使用，直到 administrator 再次启用它。建议将这个次数设置为 3—5 之间。Windows NT 资源工具箱 (Resource Kit) 中有一个程序 passprop.exe，它可以帮助我们与管理工具中不能访问的帐号进行设置，比如要为 administrator 帐号设定锁定策略，就执行下面的命令：

```
passprop /adminlockout
```

#### 11. 重新配置 Administrator 帐号

Administrator 即超级用户，它的权限至高无上，重要性毋庸置疑，同时也是被攻击最多的对象。我们要对安装后默认的 Administrator 帐号重新配置，从而达到最大的安全性。建议采取如下措施：

(1)为 administrator 重新起名，最好是不起眼的名字，比如：myadminok，mygod 等等。

(2)再次创建一个 administrator 帐号，但不分配任何权限，以达到诱骗目的。同时经常查看事件日志文件，检查是否有使用这个帐号的企图，从而及早发现攻击隐患。

(3)使用 passprop 程序为真正的 administrator 帐号设置帐号锁定策略。

(4)禁止本地计算机的 administrator 帐号。

#### 12. 安装防病毒软件并及时更新

计算机病毒的危害日益加重，我们必须在服务器上安装防病毒软件，并做到及时更新。及时安装最新版本的 SP 和 Hotfixes 补丁程序。强烈建议及时跟踪 Microsoft 公司发布 SP 以及 hotfixes 的消息，从而根据具体环境，在机器中安装最新的 SP 及 hotfixes 补丁程序。微软公司的产品补丁分为 2 类：SP (Service Pack) 和 HotFixes。SP 是集合一段时间发布的 HotFixes 的大补丁，一般命名为 SP1、SP2，一段时间才发布一次。HotFixes 是小补丁，它位于当前 SP 和下一个 SP 之间，是为解决微软网站上最新安全告示 (Security bulletin) 中的系统漏洞而发布的，一般命名为“MS 年份-序号”，比如 MS01-044 表示 2001 第 44 个 HotFixes。

### 8.3 文件的加密与解密

为了保护个人的隐私和重要数据，我们可以把重要文件加密，但是，有的时候，我们忘记了密码，所以我们也要知道怎么样解密。本节就是介绍文件的加密和解密。

#### 8.3.1 利用文件夹属性进行文件夹加密

(1)选中要加密的文件夹。

(2)从“查看”菜单中选择“自定义文件夹”选项，从向导中一步一步选择。

(3)运行到第三步时将出现 PRONTPAGE 窗口，从源文件<head>...</head>之间加入以下代码：

```
<script language="javascript">
loop ( )
function loop ( )
{
x=""
while (x!="你要输入的密码")
{x=prompt ("想要进入请输入密码！")}
alert ("密码正确，请进！")
}
```

</script>

然后点击保存，将会返回到向导中，点击完成就可以了。当然，我们还可以用专门的软件进行文件夹加密。

万一，我们忘记了密码怎么办呢？其实很简单，WinRAR 就可以实现。现在有许多朋友需要给自己的文件夹加密，而大部分文件夹加密都是把待加密文件夹变成一个系统文件夹（如控制面板）从而来保护文件夹。如超级兔子魔法设置就有这个功能。

我们打开 WINRAR，可以看到已用文件夹加密软件加密过的文件夹下的所有文件。再到那个被加密文件夹处看看，也可以看到，而且还是有密码的。被加密的文件夹在这里暴露无遗。

由此看来，那些被加密软件伪装的天衣无缝的文件夹，在 WinRAR 下就得全部显出原形。

### 8.3.2 利用 NTFS 文件系统加密数据

我们会将自己有价值的信息放到计算机上。不幸的是，骗子也能知道。在我们家中及公司的电脑里，可能有敏感的公司和客户信息，或者是个人银行存款支付报告书，而我们想确保这些信息的安全。Windows XP 中的 NTFS 文件系统具有以前 Windows® 95、Windows 98 或 Windows Me 所不具备的几点安全优势，其中之一就是 NTFS 文件系统先进的加密文件系统（EFS）安全功能。

利用 EFS，即可选择对文件和文件夹进行加密。这样，即使有人能访问文件（例如通过偷窃有文件副本的膝上机或磁盘），他们仍无法对文件进行解密，因此也就看不到信息。出于安全的考虑，EFS 中包含多层加密。每个文件都有唯一的文件加密密钥。必须使用该加密密钥才能解密文件的数据。该密钥也进行了加密，且仅对得到数据使用授权的人可用。EFS 与文件系统组合在一起，使文件更难于被攻破，而管理却更加简便。选择进行文件加密后，数据加密和解密的实际过程就成为完全透明的，不需要您任何东西。

加密单个文件时，必须决定是否加密包含该文件的文件夹。如果选择加密文件夹，则所有以后添加到文件夹中的文件和子文件夹都将进行加密。如果是加密文件夹，则还须选择是否加密其中现有的所有文件和子文件夹。

解密文件夹时，将由您确定是否解密其中的所有文件和子文件夹。如果选择仅解密文件夹，则其中的文件和子文件夹仍将处于加密状态。但新的文件和子文件夹将不会自动进行加密。

打开 Windows 资源管理器。（单击开始，指向所有程序，再指向附件，然后单击 Windows 资源管理器。）右键单击要加密的文件或文件夹，然后单击属性。在常规选项卡上，单击高级。选中加密内容以便保护数据复选框。注意，压缩的文件或文件夹不能再进行加密。如果对压缩文件或文件夹进行加密，则该文件或文件夹将进行解压缩。标记为“系统”属性的文件是不能加密的，而位于系统根目录结构中的文件也不能进行加密。

要解除密码，打开 Windows 资源管理器。右键单击加密的文件或文件夹，然后单击属性。在常规选项卡上，单击高级。清除加密内容以便保护数据复选框。

从系统安全角度来看，为需要保护的文件或文件夹对象设置用户访问权限和许可，基本上可以有效地保护数据，但经常出现的安全问题是：未被授权的用户可以使用 Windows 2000 之外的操作系统或忽略 NTFS 权限的程序来入侵文件或文件夹对象。此时，入侵者甚至可以获得文件或文件夹对象所在物理驱动器的访问和控制权，在其上安装其他的操作系统，并以管理员的身份访问该驱动器上的任何数据。为了防止上述安全问题，Windows 2000 提供了内置的加密文件系统（Encrypting File System，简称 EFS）。EFS 文件系统不仅可以阻止入侵者对

文件或文件夹对象的访问，而且还保持了操作的简捷性。我们来看看加密与解密操作：

加密文件系统通过为指定 NTFS 文件与文件夹加密数据，从而确保用户在本地计算机中安全存储重要数据。由于 EFS 与文件集成，因此对计算机中重要数据的安全保护十分有益。

#### 1. 加密操作

(1) 利用 Windows 2000 资源管理器选中待设置加密属性的文件或文件夹（如文件夹为“Windows 2000”）。

(2) 单击鼠标右键，选择“属性”，启动“Windows 2000 属性”对话框窗口。

(3) 单击“常规”选项卡中的“高级”按钮，启动“高级属性”对话框。

(4) 选择“压缩或加密属性”框中的“加密内容以便保护数据”复选框，单击“确定”按钮，即可完成文件或文件夹的加密。

#### 2. 解密操作

(1) 利用 Windows 2000 资源管理器选中待设置加密属性的文件或文件夹（如文件夹为“Windows 2000”）。

(2) 单击鼠标右键，选择“属性”，启动“Windows 2000 属性”对话框窗口。

(3) 单击“常规”选项卡中的[高级]按钮，启动“高级属性”对话框。

(4) 清除“高级属性”对话框“压缩或加密属性”框中的“加密内容以便保护数据”复选框中的“√”。

注意：

1. 不能加密或解密 FAT 文件系统中的文件与文件夹。

2. 加密数据只有存储在本地磁盘中才会被加密，而当其在网络上传输时，则不会加密。

加密文件或文件夹的操作

加密文件与普通文件相同，也可以进行复制、移动以及重命名等操作，但是其操作方式可能会影响加密文件的加密状态。

#### 1. 复制加密文件

(1) 在 Windows 2000 资源管理器中选中待复制的加密文件（如 Windows 2000）。

(2) 用鼠标右键单击加密文件，选择“复制”。

(3) 切换到加密文件复制的目标位置，单击鼠标右键，选择“粘贴”，即可完成。

#### 2. 移动加密文件

(1) 在 Windows 2000 资源管理器中选中待复制的加密文件（如 Windows 2000）。

(2) 用鼠标右键单击加密文件，选择“剪切”。

(3) 切换到加密文件待移动的目标位置，单击鼠标右键，选择“粘贴”，即可完成。

注意：对加密文件进行复制或移动时，加密文件有可能被解密，尤其要注意的是，加密文件复制或移动到 FAT 文件系统中时，文件自动解密，所以建议对加密文件进行复制或移动后应重新进行加密，一定要小心备份证书，要不然重装后自己都打不开。

### 8.3.3 用压缩软件加密文件及破解方法

除了用来压缩文件，我们还常常把 WinRAR 当作一个加密软件来使用，在压缩文件的时候设置一个密码就可以达到保护数据的目的了。正因为如此，专门针对 WinRAR 密码的破解软件也是遍地开花。密码的长短对于现在的破解软件来说，已经不是最大的障碍了。那么，怎样才可以让 WinRAR 加密的文件比较安全呢？

我们知道，现在的破解软件在破解加密文件密码的时候总要指定一个 Encrypted File（目标文件），然后根据字典使用穷举法来破解密码。但是如果我们将多个需要加密的文件压缩在一起，然后为每一个文件设置不同的密码，那破解软件就无可奈何了。假设现在有一个重要文件，需要给它加密保存，我们就可以这样做：

1. 按照常规的方法把它压缩并且设置一个密码；

2. 准备一个其他文件（当然这个文件小一点最好了，因为我们只是利用它来迷惑破解

软件而已);

3. 在 WinRAR 的工作窗口中打开我们第一步已经压缩好的加密文件, 在“命令”菜单中选择“添加文件到压缩文件”菜单选项; 如图 8-3 所示:



图 8-3 WINRAR 运行窗口

4. 在弹出的“添加文件名和参数”对话框中选择“文件”窗口, 如图 8-4 所示:

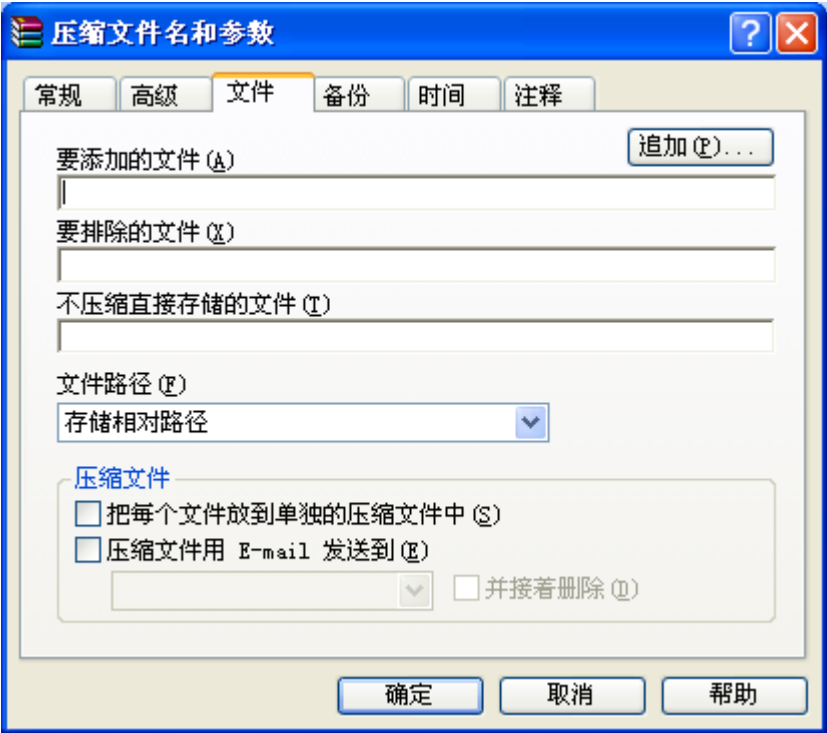


图 8-4 文件窗口

然后, 单击“追加”按钮, 把我们准备的“其他文件”比如“G:\英语学习\沪江坐着听 PC 复读机.doc”, 点击“确定”按钮即完成了。

5. 在“高级”选项卡标签中点击“设置密码”按钮设置一个不同的密码, 然后开始压缩即可。如图 8-5, 6 所示:

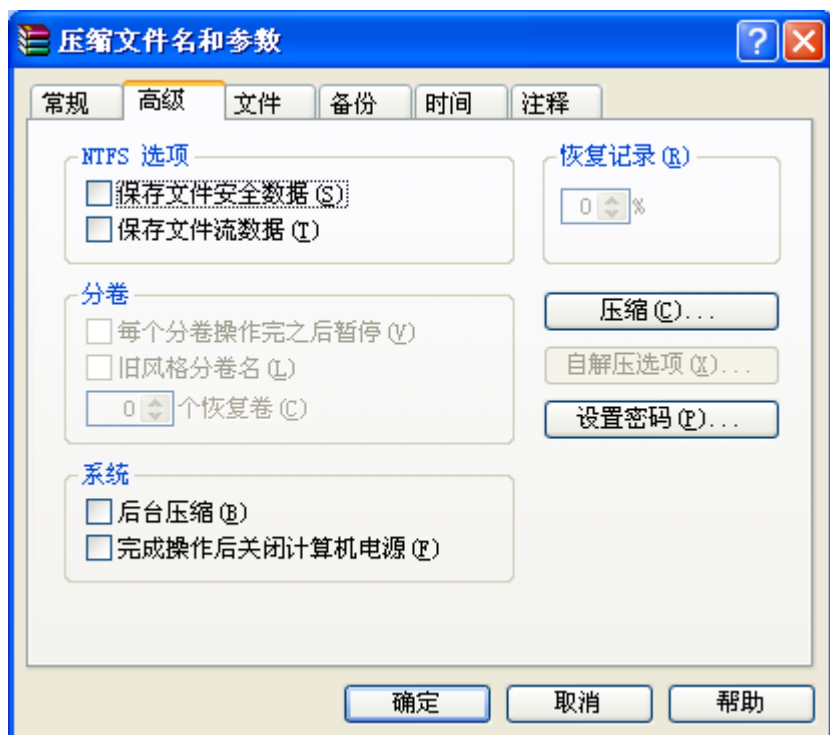


图 8 — 5 高级窗口

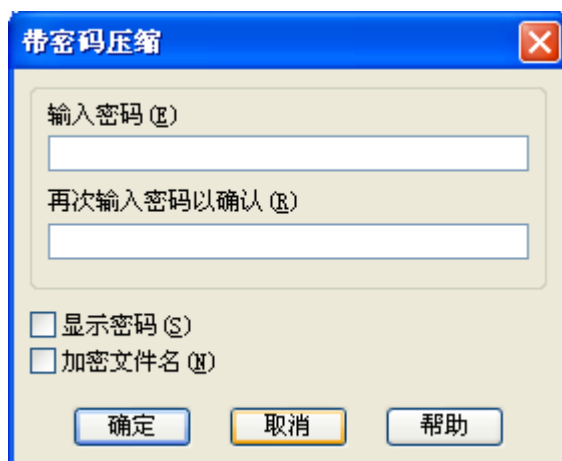


图 8 — 6 输入密码

好了，现在两个密码已经设置完成了（如果添加了多个文件，也可以给每个文件设置不同的密码，如果你担心自己会忘记，只设两个密码也可以达到目的）。我们可以试着打开压缩文件看看，是不是每一个文件名的右上角都有一个表示加密的星号呢？打开其中不同的文件都需要相对应的密码，使用破解软件是得不到正确密码的。但是，如果大家自己也忘记了密码，所以在设置这样的密码的时候，最好有自己便于记忆的规律可循。实在不行，我们可以使用第三方软件，比如我的密码（MyPassWord）V3.10 来帮助记忆密码。

我们再看一则技巧，我们平时在使用压缩软件对文件进行压缩的时候，通常还会加上密码以防止他人私自打开查看。但是这样一来，每压缩一次文件，就要手工输入一次密码，很麻烦。有没有更好的办法呢？我们可以通过简单的设置，在每次压缩文件的时候让压缩软件自动对其进行加密。

运行 WinRAR 后，选择菜单栏中的“选项→设置”，在“设置”窗口中选择“压缩”选项，如图 8 — 7 所示：



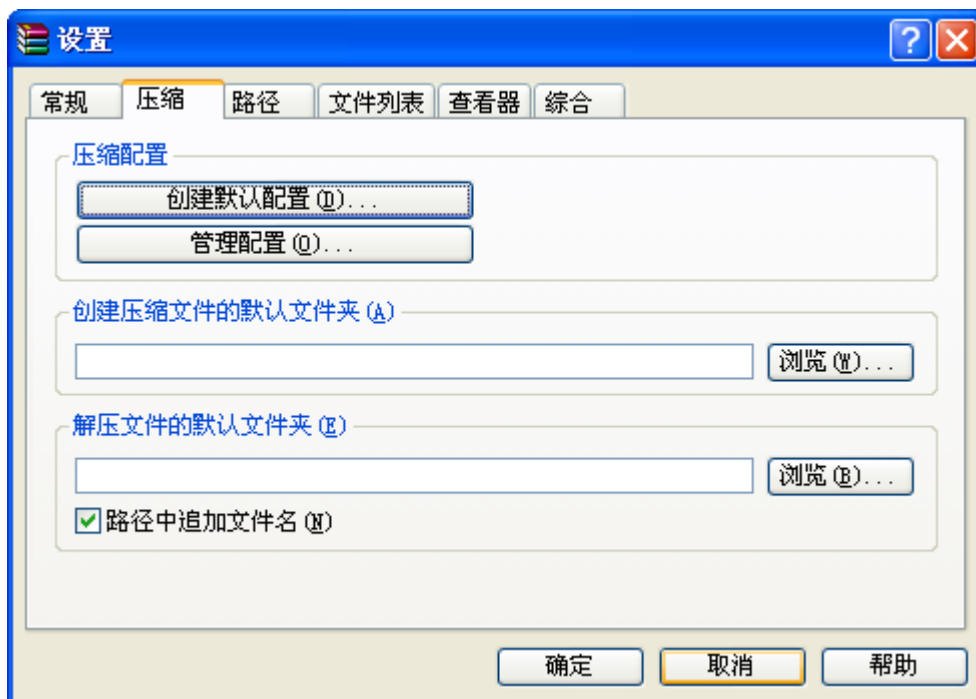


图 8 — 7 压缩窗口

然后点击上面的“创建默认配置”按钮。在随后打开的窗口中选择“高级”，如图 8 — 8 所示：

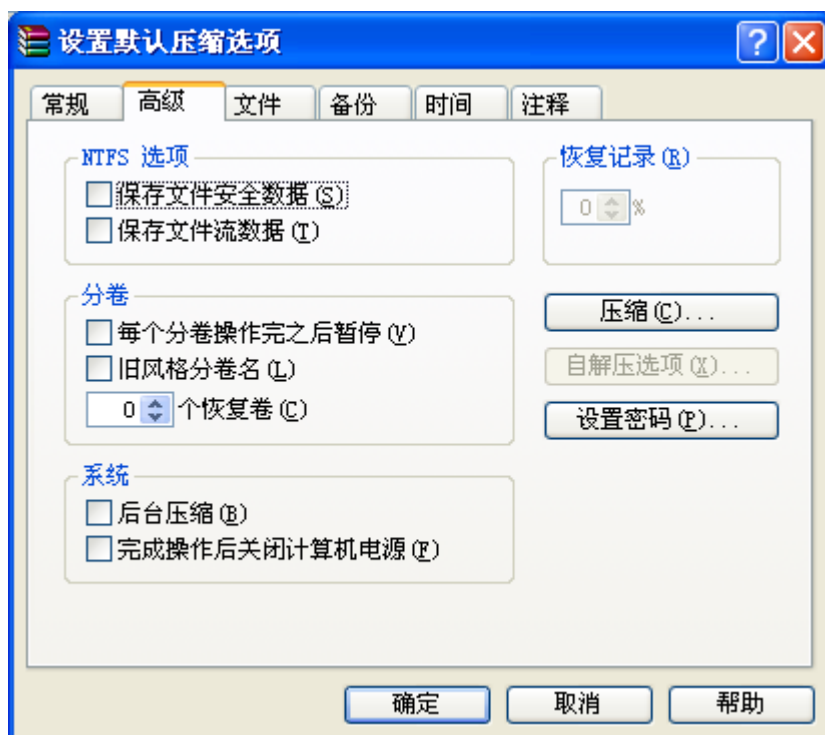


图 8 — 8 默认设置的高级选项

接着，我们点击其中的“设置密码”按钮。在“带密码压缩”窗口中，输入密码，并点击“确定”完成设置。如图 8 — 9 所示：

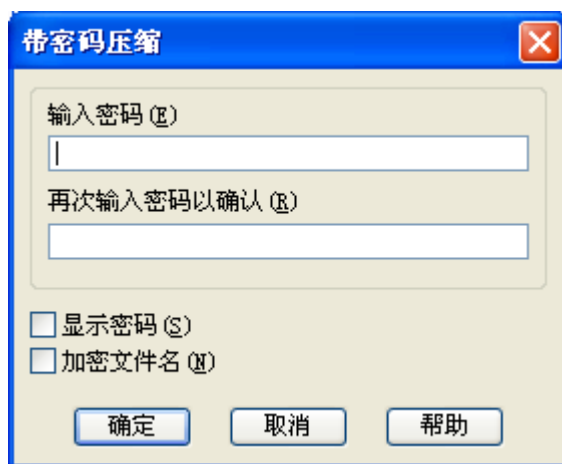


图 8 — 9 输入密码窗口

这样，每次用 WinRAR 压缩文件时，这个密码就会自动加入了，是不是方便了许多呢。

我们知道，WinZip 是互联网上久负盛名的压缩/解压缩工具软件，由于其压缩效率高、速度快、安全可靠，无论是数据资料的交流与传播，还是共享软件或者商业软件包的发行，WinZip 都是首选的压缩格式，WinZip 工具及其压缩的文件包在互联网上广为流传，已经成为事实上的工业标准。

为了保证数据的安全性，WinZip 为其压缩文件包提供了基于口令的保护措施，通过设定口令，WinZip 可以保护压缩文件包中的全部或者部分被压缩文档。

#### 一、WINZIP 的口令加密方法

WinZip 使用工业标准的 Zip 2.0 加密格式。这种格式可以防止不知道口令的用户查看压缩文件的内容。但要注意，Zip 2.0 格式的加密强度不能和 DES 或者 RSA 之类的公共密钥加密算法相提并论，不可能完全抵御一个拥有高级破译工具的解密高手的攻击。虽然 Zip 2.0 加密格式加密强度不高，WinZip 这样做的考虑一是与 Zip 2.0 标准兼容，二是基于美国政府对加密技术产品出口的严格限制。

在 WinZip 中设定口令保护的步骤是：

##### (1) 打开或者新建一个压缩文件包

点击“NEW”（新建）按钮新建一个压缩文件包，或者点击“OPEN”（打开）按钮打开一个压缩文件包。

##### (2) 设定口令

可以在菜单“OPTION”（选项）中设定“PASSWORD”（口令），也可以在添加文件对话框（ADD）中设定。

注意：必须在添加文件之前设定口令。

在 WinZip 的主窗口中，凡是带有加密口令的文件名之后都有一个加号作为标记。

在设定了口令之后，当用户试图展开、测试或者直接从压缩文件包安装时，将被自动提问口令。

若选择“Mask Password”（验证口令），则用户输入的口令将以“\*”的形式显示，并提示用户输入两次口令以进行验证。若关闭该选项，则用户输入的口令内容将以明码显示，并且只输入一次。

设定口令，添加被压缩文件，关闭压缩文件包之后，口令保护有效。当用户利用 WinZip 打开含有口令的压缩文件包时，能够在 WinZip 的主窗口中看到压缩文件包中的所有被压缩文件名等信息，并且在有加密口令的文件名之后以加号作为标记，这些文件目录信息无需口令就可以浏览，但是如果展开一个被压缩文件将会被要求输入口令。

## 二、AZPR 的功能特点

但是，口令在增强安全性的同时，也增加了遗忘口令可能带来的麻烦。于是，破解口令的工具就成为当务之急。由于目前尚未有直接从压缩文件包破译口令的方法，因此最有效的破解方法仍然是基于口令字典的破解或者强力搜索破解，实际上是试探各种口令组合的穷举搜索方式。本文所介绍的 Advanced ZIP Password Recovery 便是采用这两种方式进行口令的破解。

与其他工具相比，Advanced ZIP Password Recovery（简称 AZPR）具有以下优点：

- 具有使用方便的用户界面。
- 破解速度很快，据作者声称能够在 Pentium II 上每秒钟运算 100 万个口令。
- 能够破解仅有部分文件被口令保护的压缩文件包。
- 支持破解不同软件生成的 ZIP 压缩文件包。
- 支持排序等不同压缩模式。
- 支持自动解压缩文件包。
- 具有多项用户可定制的属性：口令长度及其范围、生成口令的字符集等等。
- 支持非英语字符集。
- 可以使用基于字典的攻击方式。
- 支持带有掩码的攻击，即用户可以指定口令中的某些已知或者猜测字符。
- 注册版本口令长度无限制。
- 无需额外的虚拟内存。
- 用户可以随时中断和从断点继续破解过程，这一点将会节约大量时间。
- 能够在后台运行，可以设定在 CPU 空闲时才进行破解运算。

## 三、AZPR 的设置与使用

AZPR 提供了一个图形化的用户界面（如图），用户可以经过几个简单的步骤进行 ZIP 压缩文件包的解密。

### 1. ZIP password-encrypted file

打开被加密的 ZIP 压缩文件包。可以利用浏览按钮或者功能键 F3 来选择将要解密的压缩文件包。

### 2. Type of attack 选择攻击方式。

**Brute-force:** 强力攻击。这是利用穷举搜索法在所有的组合方式中试探口令的攻击方式，耗时最长。强力攻击必须将指定的字母、数字、特殊符号集合中所有符号的排列组合进行穷举试探。

**Password mask:** 掩码搜索。假如已知口令的部分字符，就可以指定掩码来大大缩小排列组合的空间。例如，用户已知口令长度为 8 个字符，且开头字母为“Y”，结尾字母为“D”，则可以指定掩码为“Y?????D”，掩码中的问号表示任意字符，则 AZPR 仅仅在掩码指定的排列空间内进行搜索，将会大大加快搜索速度。

如果问号是已知口令的一部分，为避免掩码冲突，可以用“#”或者“\*”来代替问号表示未知字符，例如，用户已知口令长度为 8 个字符，且开头字母为“Y”，结尾字符为“？”，则可以指定掩码为“Y#####？”。

**Dictionary:** 字典攻击。穷举搜索的强力攻击非常消耗时间，特别是在口令长度增加的情况下，如果搜索时间过长，过高的解密成本将使解密变得不切实际。于是解密者另辟蹊径，从人的心理习惯入手，缩小试探空间，字典攻击法便诞生了。大多数人设定密码口令都有一定的规律可循，而且经常使用一些重复频率较高的英文单词，例如 god、china、hero 等等，字典攻击法就是将人们可能用作口令的英文单词或者字符组合制作成一个字典，利用试探数量远远小于穷举法的字典进行试探，实践证明也是一个非常有效的攻击手段。

### 3. Brute-force range options

设定强力攻击法的搜索范围，如果用户了解口令的组合特点，通过设定以下选择可以大大缩短搜索时间。

All capital letters: 所有大写字母。

All small letters: 所有小写字母。

All digits: 所有数字字符，0-9。

All special symbols: 所有特殊符号，例如@、%。

Space: 空格。

All printable: 所有可打印字符，即包含以上所有类型的字符集合。

User-defined: 用户自定义字符集，需同时指定 char set（字符集文件）。

### 4. Start from password

当用户知道口令的起始字符序列时，可以设定该选项。例如，当用户知道口令全部使用小写字母，长度是 5，并且以字母“k”开头，那么可以在该项填写“kaaaa”，AZPR 将从这个口令开始依次向后搜索所有的可能解答。

该选项的另一个功能是继续上次被中断的搜索。当用户暂停某个搜索过程时，当前搜索的口令将被保存在该窗口。

口令搜索的顺序是：大写字母-> 空格-> 小写字母-> 数字字符-> 特殊字符。

### 5. Password mask

设定口令掩码，仅当用户知道组成口令的某些字符时设定。

### 6. Password length

设定口令长度，这也是一个决定搜索时间的重要选项。对于长度小于等于 4 个字符的口令，在奔腾计算机上只需要几分钟即可解密，但是对于更长的口令，则要求用户有更大的耐心以及对口令知识的深入了解。

如果用户设定口令最小长度与最大长度不相等，则 AZPR 将试图从最小长度组合开始搜索，直到成功或者满足最大长度为止。

搜索过程中将会显示当前工作状态，包括当前试探的口令、平均速度、消耗时间、剩余时间、试探口令总数、已处理口令数等等。

未注册的 AZPR 仅能处理最大长度为 5 个字符的口令。当口令长度大于 12 时，解密时间将会很长，这也说明，适当增加口令长度是增强口令安全的方法之一。

### 7. Dictionary options

设定字典攻击选项。

Try to capitalize first character: 试探首字母大写的口令。

Try to capitalize all characters: 试探全部字母大写的口令。

这些选项将会试探某个字典中口令的所有大小写可能。AZPR 的字典文件 english.dic 中包含了 27000 个口令，用户也可以到如下网址寻找更新的字典或者口令文件：

<ftp://sable.ox.ac.uk/pub/wordlists/>

<ftp://ftp.cdrom.com/pub/security/coast/dict/wordlists/>

<ftp://ftp.cdrom.com/pub/security/coast/dict/dictionaries/>

### 8. Auto-save

自动存储选项的功能是定期自动保存软件当前设置与当前工作状态，这些关键参数将会定期自动保存在一个名为“~azpr.ini”，用户可以自行指定保存参数的文件名、自动保存的时间间隔等等，该选项使得用户能够继续上次中断的解密进程。

### 9. Other options

其他选项。

Priority: 优先级。设定为后台“background”，则只有当 CPU 空闲时才会进行解密运算。如果设定为高优先级“High”，将会加快运算速度。

Minimize to tray: 最小化到系统托盘区。

Log to azpr.log: 自动将各种工作状态信息记录到日志文件 azpr.log。

Progress bar update interval: 进度栏更新周期，默认值是 500 毫秒。

#### 10. Start

如果以上项目都设定完毕，可以点击“Start”（开始）按钮进行解密运算，由于 AZPR 有以上保存参数和状态的功能，用户随时可以中断或者继续运算过程。

最后，当密码找到后，用户会在结果窗口中看到密码内容、试探密码总数、破解消耗时间、平均运算速度等信息。如果没有找到密码，也会有相应的提示信息。

#### 8.3.5 QQ 密码忘记了怎么办？

首先，介绍一下我们要用到的工具软件——Keymake。Keymake 是中文界面的国产软件（如图 8-10），它是一款可以很方便的制作出自己的“注册机”或软件补丁的软件。之所以给“注册机”加上了引号，是因为严格说来，用 Keymake 来制作的“注册机”并不是真正的注册机，只能算做是软件的补丁或另类注册机（用 Keymake 制作的“注册机”在运行后，可以让注册码自己跳出来，直接显示在屏幕上）。

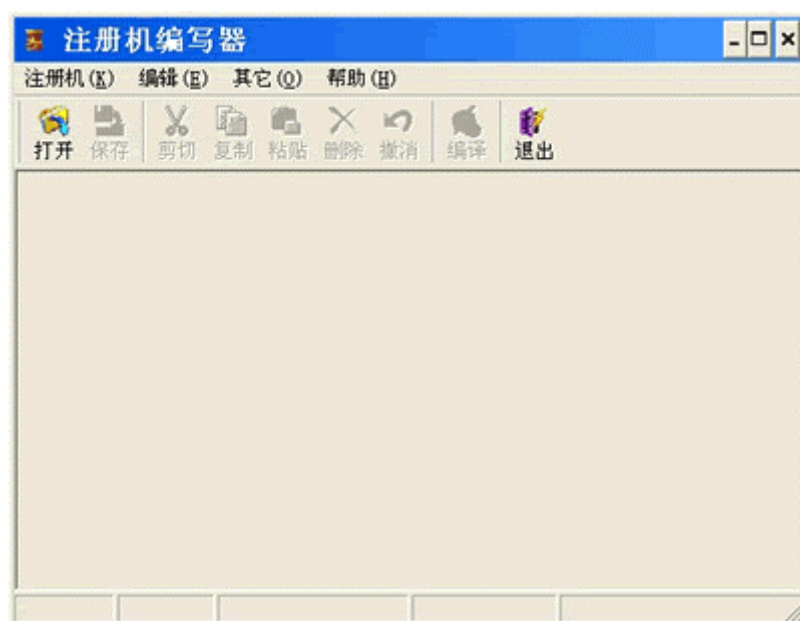


图 8-10 运行窗口

目前有许多程序的注册码算法都与硬件有关，这类程序在每一台机上安装时都会生成一个机器码，要把这个机器码 E-MAIL 给作者，待他收到机器码后，再算出注册码寄回给用户，一机一码的结果就是软件只能一机一用。本来这样无可厚非，但是有些时候，这样做给用户却造成了不少的麻烦，因为只要用户重装系统或升级更换硬件，就要重新去注册软件。对于这种程序，一般人只能在内存中找到自己机器的注册码，但这种注册码到了其它的机器上又不能用了，而自己又没有办法写出注册机来，为了解决这方面的问题，作者写了这个小软件，它可以从另一进程中取出注册码，并在屏幕中显示出来，并且不需要你去了解待注册程序的算法也不需要你会编程，是不是很方便呀？今天我们就利用它的制作补丁功能制作出 QQ 聊天补丁，突破 QQ 的本地密码验证，使得我们无需输入密码就可以进入 QQ，实现自由查看 QQ 聊天记录的目的。

首先，请你下载 16 进制文件编辑器 UltraEdit 汉化版，用它来修改 QQ 的主文件，改造出一个可以无需密码就能登陆的 QQ，安装完毕之后，单击桌面上的 UltraEdit 图标运行它，

然后点击“文件”菜单中的“打开”，找到 QQ 安装目录下的 QQ.EXE，点击“确定”打开该文件。然后点击“搜索”菜单下的“查找”，在出现的对话框的“查找什么”栏中填入：0F849900000837D1801（如图 8－1 1），这些代码中的“0F8499000000”就是判定你输入的密码是否和真正的 QQ 密码是否相等的汇编代码的机器码。

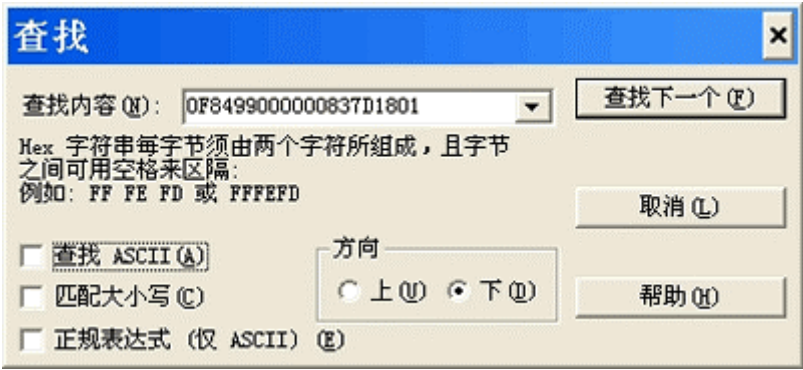


图 8－1 1 查找窗口

这些代码中的“0F8499000000”就是判定你输入的密码是否和真正的QQ密码是否相等的汇编代码的机器码。然后点击“下一个”按钮查找这些字符串（注意该窗口中的“查找 ASCII 字符”选项一定不能选上），会找到唯一的一处结果，如图所示（如图 8－1 2）。

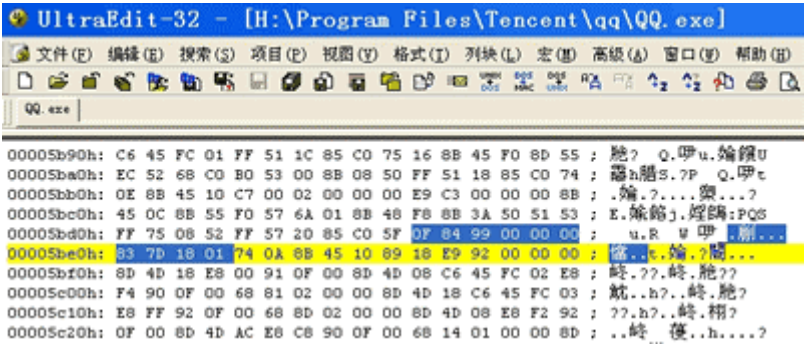


图 8－1 2 查找结果

把其中的“84”改为：85 即可（如图 8－1 3），这样修改的结果使得无论QQ密码是否相等，都使程序跳转到登陆上QQ这段代码中执行程序，这样就突破了QQ的密码验证关。

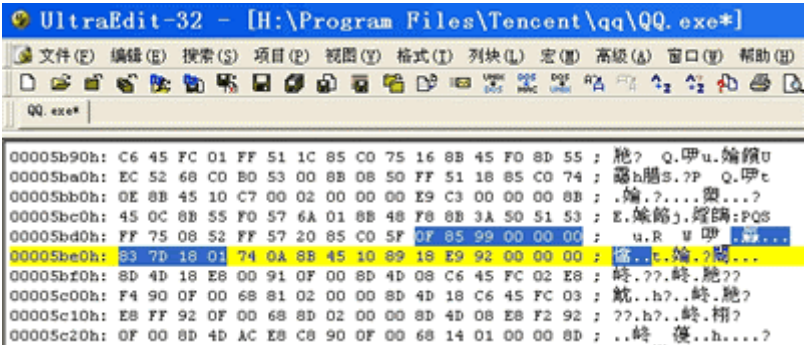


图 8－1 3 修改密码

最后点击“文件”菜单中的“另存为”，把修改后的文件保存在 QQ 安装目录下，命名为任意名字，如 QQ1.EXE，然后关闭 UltraEdit 即可。在离线状态下运行 QQ1.EXE，在登陆窗口中无需输入密码或随意输入任何字符，点击“登陆”按钮都可以直接进入 QQ 中。该技巧对 QQ2003II 正式版至 QQ2003III Build0117(含)之间各版本的 QQ 用户。对于 QQ2000C 1230 版的 QQ 用户，可以用 UltraEdit 打开 QQ.EXE 文件，然后查找如下代码：



85C05F0F8489000000，将找到的结果改为：85C05FE98A00000090；以后无需密码也能离线进入 QQ 中，无论是查看或导出聊天记录都可以。如果你使用的是 QQ2000C Build 0825 版 QQ，可以搜索：0F8564010000A1，找到后替换为：E96501000090A1，其他内容不变，然后另存为 QQ1.EXE 即可。注意，一定要另存为为一个新文件才行，不能直接保存，否则接下来无法制作出“QQ 密码破解器”。

接下来运行 Keymake 开始制作“QQ 密码破解器”。点击“其他”菜单下的“制作补丁文件”（如图 8－1 4），会出现一个制作补丁文件窗口（如图 8－1 6），在“窗口标题”中输入任意内容，比方说我输入的是：QQ 密码破解器，在“你的主页”和“你的邮件”中输入你的相关信息即可，如果没有可以不填，这些内容会在你制作的“QQ 密码破解器”中显示出来，如果你想让你的大名名扬天下的话，还是填入为好。



图 8－1 4 开始制作补丁选项

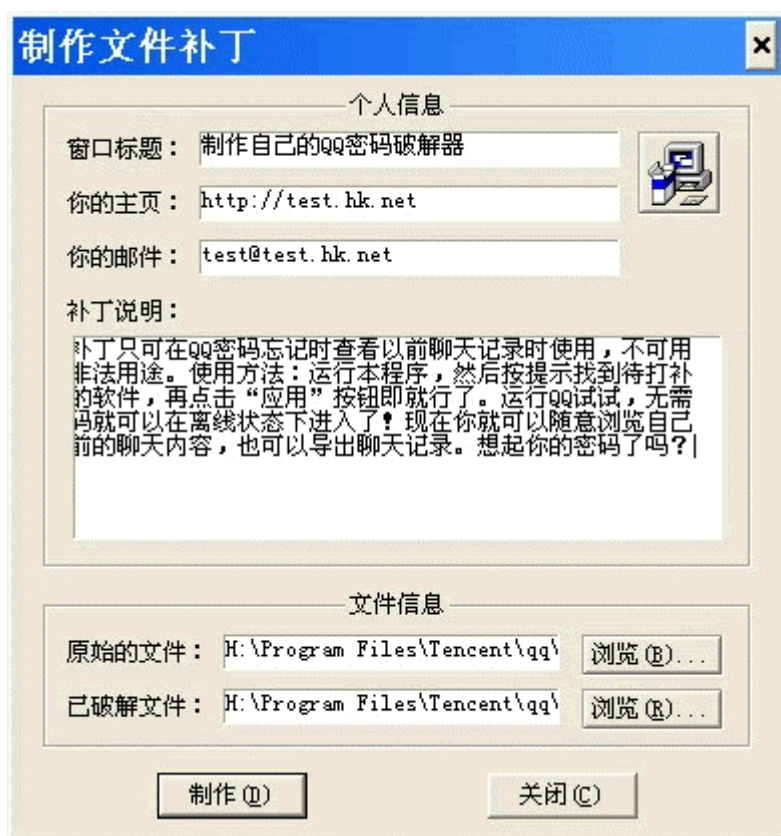


图 8—1 5 制作补丁

在“补丁说明”中输入该文件的相关说明，这些说明的内容会在你制作的“QQ 密码破解器”运行界面中出现。比方说你可以输入该软件的使用方法和注意事项等，例如：我们这里输入：本补丁只可在 QQ 密码忘记时查看以前聊天记录时使用，不可用于非法用途。使用方法：运行本程序，然后按提示找到待打补丁的软件，再点击“应用”按钮即就行了。运行 QQ 试试，无需密码就可以在离线状态下进入了。现在你就可以随意浏览自己以前的聊天内容，也可以导出聊天记录。想起你的密码了吗？接下来点击“浏览”按钮分别找到“原始的文件”（即 QQ.EXE）和“已破解文件”（QQ1.EXE），然后点击“制作”按钮，会出现一个窗口要你选择补丁文件的界面（如图 8—1 6），有“界面一（传统样式）”和“界面二（增强样式）”可供选择，我们选择“界面二（增强样式）”，然后单击“确定”按钮，选择好制作出来的补丁文件的保存路径，并将该文件命名为“QQ 密码破解器”就可以了，生成的文件是 EXE 格式，大小只有 6KB。注意，使用本方法有一个前提条件，那就是你一定要有一个修改过的 QQ 主文件，还要有一个未修改过的 QQ 主文件。另外，一般说来制作出的补丁文件，只能应用于该版本的 QQ，不能混用。

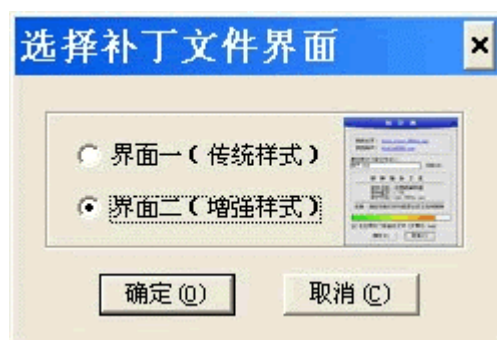




图 8—1 6 选择补丁界面

然后我们把“QQ 密码破解器”运行试试，界面中有你的大名和使用说明。点击“浏览”按钮找到待打补丁的 QQ.EXE 文件，单击“应用”按钮即可。然后再运行 QQ 试试，怎么样在登陆时无需输入密码了吧？对于任何号码都如此。

#### 8.4 光盘及软盘的加密与解密

目前保护光盘的方法有很多种，但其主要原理是利用特殊的光盘母盘上的某些特征信息是不可再现的，而且这些特征信息大多是光盘上非数据性的内容，在光盘复制时复制不到的地方。为了能使大家对保护光盘的技术有一定的了解，我们下面就对目前一些较新的保护技术进行一下介绍。

##### 1. 外壳保护技术

所谓“外壳”就是给可执行的文件加上一个外壳。用户执行的实际上是这个外壳的程序，而这个外壳程序负责把用户原来的程序在内存中解开压缩，并把控制权交还给解开后的真正的程序，由于一切工作都是在内存中运行，用户根本不知道也不需要知道其运行过程，并且对执行速度没有什么影响。如果在外壳程序中加入对软件锁或钥匙盘的验证部分，它就是我们所说的外壳保护了。其实外壳保护的作用还不止于此，在 Internet 上面有很多程序是专门为加壳而设计的，它对程序进行压缩或根本不压缩，它的主要特点在于反跟踪，保护代码和数据，保护你的程序数据的完整性。如果你不希望你的程序代码被黑客修改，如果你的程序不希望被人跟踪调试，如果你的算法程序不想被别人静态分析，这种外壳程序就是为你设计的。

##### 2. 光盘狗技术

一般的光盘保护技术需要制作特殊的母盘，进而改动母盘机，这样实施起来费用高不说，而且花费的时间也不少。针对上述的缺点，光盘狗技术不在母盘制造上动手脚，因此我们可以自由选择光盘厂来压制光盘。该保护技术能通过识别光盘上的特征来区分是原版盘还是盗版盘。该特征是在光盘压制生产时自然产生的，即由同一张母盘压出的光盘特征相同，而不同的母盘压制出的光盘即便盘上内容完全一样，盘上的特征也不一样。也就是说，这种特征是在盗版者翻制光盘过程中无法提取和复制的。光盘狗是专门保护光盘软件的优秀方案，并且通过了中国软件评测中心的保护性能和兼容性的测试。

##### 3. CSS 保护技术

CSS 的英文全称为 Content Scrambling System，中文含义为数据干扰系统。该技术的主要工作思路就是将全球光盘设置为 6 个区域，并对每个区域进行不同的技术保护，只有具备该区域解码器的光驱才能正确处理光盘中的数据。使用该技术保护时，首先需要将所有存入光盘的信息经过编码程序来处理一下，而要访问这些经过编码的数据，必须先对这些数据进行解码。

##### 4. CPPM 技术

该技术的中文含义为预录媒介内容保护技术，该技术一般用于 DVD-Audio。该技术取代了 CSS 保护技术，它通过在盘片的导入区放置密钥来对光盘进行保护，但在 sector header 中没有 title 密钥，盘片密钥由"album identifier"取代。该技术的鉴定方案与 CSS 相同，因此现有设备无须任何改动。

##### 5. DCPS 技术

该技术的中文含义为数字拷贝保护系统技术，它的主要作用是让各部件之间进行数字连接，但不允许进行数字拷贝。有了该项保护技术，以数字方式连接的设备，如 DVD 播放机和数字电视或数字录象机，就可以交换鉴证密钥建立安全的通道。DVD 播放机对已编码的音频/视频信号进行保护，然后发送给接收设备，由接收设备进行解密。这就防止那些未鉴证的已连接设备窃取信号。无须拷贝保护的内容则不进行保护。新内容（如新的盘片或广播

节目)和含有更新的密钥和列表(用来识别非认证设备)的新设备也可获得安全特性。

## 6. CPRM 技术

该技术也称为录制媒介内容保护技术,它将媒介与录制相联系。该技术的保护原理是,在每张空白的可录写光盘上有一个 64 比特盘片 ID 放置在 BCA 上。当受保护的内容被刻录到盘片上时,它可由盘片 ID 得到的 56 位密码进行保护。需要访问光盘信息时,则从 BCA 中读取盘片 ID,然后生成盘片内容解密所需要的密钥。如果盘片内容被复制到其他媒介,那么盘片 ID 将会丢失或出错,数据将无法解密。

## 7. CGMS 技术

CGMS 技术也叫内容拷贝管理技术,该技术主要是用来防止光盘的非法拷贝的。该技术主要是通过生成管理系统对数字拷贝进行控制,它是通过存储于每一光盘上的有关信息来实现的。CGMS 这一“串行”拷贝,生成管理系统既可阻止母版软件进行拷贝,也可阻止对其子版软件进行再拷贝。而就在被允许正常拷贝的情况下,制作拷贝的设备也必须遵守有关规则。数字拷贝信息可以经编码后送入视频信号,这样做的目的在于使数字录音机能很方便地予以识别。

## 8. APS 保护技术

APS 的英文全称为 Analog Protection System,中文含义为类比信号保护系统。该保护技术的主要作用是为了防止从光盘到光盘的复制。APS 保护技术主要是通过一颗 Macrovision 7 的芯片,利用特殊信号影响光盘的复制功能,使光盘的图象产生横纹、对比度不均匀等等。当然,我们在使用计算机来访问光盘时,如果想通过显示卡输出到电视机上时,那么,显示卡必须支持类比保护功能,否则,将无法得到正确的信息,我们就无法在电视上享受光盘影片的优秀画面。

下面我们再看看软磁盘反拷贝加密技术:

软磁盘反拷贝实质上就是在磁盘中制作一些特殊的标记,这种标记不能被轻易复制,可以由被加密程序识别,由此来达到软件加密的目的。软磁盘反拷贝技术在多年来的发展过程中不断成熟,涌现出多种方法,但由于拷贝工具也在发展,有些反拷贝技术已不能抵御功能强大的拷贝工具的进攻而逐渐被淘汰。但也有一些经典的加密技术,至尽仍被广泛运用。

### 1. 超级扇区法

这种方法利用专用设备在软盘上写上一些超长(往往接近一个磁道)扇区,正常情况下这种长扇区磁盘控制器无法在磁盘上写出,但可以在程序的控制下在其中读出信息。将密钥存放在正常情况下扇区间隙的位置处,这样,一般的复制程序就无法将其复制,而在被加密程序中却可以将间隙处的密钥作为超级扇区的一部分读出,判断读出信息的正确性就可以确定该盘是否是原盘,从而获得加密效果。

设超级扇区字节长度为 4096,所在磁道为 0 面 0 道。读出的信息放在 DS 段偏移 1000H 开始的区域中。

```
C:\DEBUG
```

```
-E 0:0525 ; 修改磁盘技术表
```

```
0000:0525 02.05 09.01
```

```
-A 100
```

```
1180:0100 MOV AX,0201 ; 读一个扇区
```

```
1180:0103 MOV BX,1000 ; 读出数据缓冲区指针
```

```
1180:0106 MOV CX,0 ; 0 道 0 扇
```

```
1180:0109 MOV DX,0 ; A 道 0 扇
```

```
1180:010C INT 13
```

```
1180:010E INT 3
```

1180:010F

-G=100

## 2. 异常 ID 法

扇区中的 ID 字段由柱面号 (C)、磁头号 (H)、扇区号 (R) 和扇区字节长度 (N) 四个参数组成。对于 5.25in 双面低密度软盘来讲, 这四个参数的正常取值的范围是: C (0~39), H (0,1), R (1~8 或 9), N=2。异常 ID 的扇区是不能正确读写的, 而 ID 在格式化写入时不作正确性检查, 于是就可以用这一点来人为地制造异常 ID 扇区, 阻止一般拷贝软件的复制。

有很多种方法来产生异常 ID 扇区, 如: 使扇区长度不等于 512 字节 (即使  $N \neq 2$ ); 将扇区号取大雨 9 的值; 打乱磁道上扇区的排列顺序; 使磁头的逻辑号与物理号不相符, 等等。对于打乱磁道上扇区的排列顺序的方法可以采取以下步骤来实现, 这段程序在 A 盘第 20 道 0 面进行格式话时, 把 9 个扇区的顺序完全颠倒了。

C:\DEBUG

-E 1000

2884:1000 00.14 00.00 00.09 00.02 00.14 00.00 00.08 00.02

2884:1008 00.14 00.00 00.07 00.02 00.14 00.00 00.06 00.02

2884:1010 00.14 00.00 00.05 00.02 00.14 00.00 00.04 00.02

2884:1018 00.14 00.00 00.03 00.02 00.14 00.00 00.02 00.02

2884:1020 00.14 00.00 00.01 00.02

-A 100 格式化 A 盘 0 面 20 道

2884:0100 MOV AX, 0509

2884:0103 MOV BX, 1000

2884:0106 MOV CX, 1401

2884:0109 MOV DX, 0

2884:010C INT 13

2884:010E INT 3

2884:010F

-G=100

## 3. 额外扇区法

一个扇区由标识区 (长度为 22 字节, 对 5.25in 双面低密软盘而言) 和数据区 (长度为  $512+16+2=530$  字节) 以及两个间隙 (GAP2 和 GAP3, 长度分别为 22 和 84 字节) 组成, 其实际长度为  $22+22+530+84=658$  字节, 9 个扇区在加上前置区和后置区的长度, 一个磁道的容量大约有 6224 字节, 而其中的 GAP3 和后置区的长度都是可改变的, 尤其是 GAP 的调整可以在格式化时通过修改磁盘基数表位移 07 处的值来设定, 所以完全可以通过减小 GAP3 长度来减少一个扇区所占的字节数, 从而在一个磁道内多装入一个扇区。例如取 GAP3 的长度为 10 (不能小于 5, 否则有可能出现磁盘故障) 时, 每扇区长度为  $625 - (84-10) = 584$ ,  $10 \times 584 + 32 = 5872$ , 所以一个磁道内足以装下 10 个扇区。

如此格式化出的第 10 个扇区, 常规拷贝软件无法访问, 如果把密钥放在这一额外扇区中, 就可以防止磁盘被复制。

C:\DEBUG

-E 0:526 ; 修改磁道基数表

0000:0526 09.0A 2A ; 每道扇区数改为 10~~~~~

0000:0528 FF 54.0A ; GAP3 长度改为 10

-E 10000 ; 格式化所需的扇区 ID 参数

5068:1000 00.14 00.00 00.01 00.02 00.14 00.00 00.02 00.02

```

5068:1008 00.14 00.00 00.03 00.02 00.14 00.00 00.04 00.02
5068:1010 00.14 00.00 00.05 00.02 00.14 00.00 00.06 00.02
5068:1018 00.14 00.00 00.07 00.02 00.14 00.00 00.08 00.02
5068:1020 00.14 00.00 00.09 00.02 00.14 00.00 00.0A 00.02
-A 100: ; 格式化 A 盘 0 面 20 道
5068:0100 MOV AX,050A
5068:0103 MOV BX,1000
5068:0106 MOV CX,1401
5068:0109 MOV DX,0
5068:010C INT 13
5068:010E INT 3
5068:010F
-G 100
格式化额外扇区
C:\DEBUG
-E 0:526 ; 修改磁道基数表
0000: 0526 09.0A 2A ; 每道扇区数改为 10
0000: 0528 FF 54.0A ; GAP3 长度改为 10
-A 100 ; 读 A 盘 0 面 20 道第 10 扇区
5068:0100 MOV AX,0201
5068:0103 MOV BX,1000
5068:0106 MOV CX,140A
5068:0109 MOV DX,0
5068:010C INT 13
5068:010E INT 3
5068:010F
-G=100

```

#### 4. 伪扇区法

该方法在一磁道上按扇区的标准格式顺序存放若干扇区头标志，后边不跟数据。当拷贝软件复制这一磁道时，要在其缓冲区内分配足够的内存来存放这些伪扇区的数据值，于是很快就会使缓冲区溢出，从而保护了伪扇区后面真正有用的关键数据。

#### 5. 扇区对齐法

绝大多数 PC 机及其兼容机使用的磁盘都是软分段的。所谓软分段，就是在整张磁盘上只有一个索引孔，通过磁盘的旋转以及磁头的步进来存取信息。磁盘每转一周，磁盘驱动器将自动产生一个索引脉冲信号，以次标记磁道的开始。在索引脉冲信号之后，依次为每个扇区写上扇区识别标志（ID），这些标志能标志磁道的开始。传统的磁盘复制实际上就是一个读写交错的过程，它将读到的磁盘的信息全部写到目标盘的对应磁道上，而全然不顾扇段与扇段是否对期。这里的扇段对齐是指每个磁道的磁偏角相等。因而，如果有了对齐的扇段，便可以通过一些检测手段达到加密的目的。

有了这种想法，如何制作一张扇段对齐的磁盘呢？这可以通过精确磁道位置（即按相同的磁偏角）将相应的扇段写到每个相应的磁道中，来完成扇段的对齐操作。由于传统的复制程序的“非智能性”（即全然不管扇段是否对齐），以及磁盘机的转速存在着误差，因而利用传统的自复制程序复制的磁盘必然导致扇段的磁偏角不再相等，即扇段不再对齐。可以在被加密程序中安排一段代码，用它来读一个磁道上的某个扇段，步入下一个磁道，等待确定的

时间，读它找到的下一个扇段的号码来检查扇段是否对齐，从而可以判断是否为原盘，达到加密的目的。可以通过精确控制磁盘驱动器的磁头，将相应的扇区以相对于索引孔的精确偏移写到每个对应的磁道来实现扇区对齐。

扇段对齐技术是一种十分有效的磁盘软加密方法。但是由于要精密依靠磁盘的转动速度来判断扇段对齐，而磁盘的转动速度实际上时时刻刻都不相同，因而这种加密技术实施难度大，也较难得到高可靠性。因此在实际应用中，扇区对齐技术的使用并不多见。

#### 6. 未格式化扇区法

众所周知，微机上使用的软盘必须经过格式化处理后才能存储信息，未格式化的磁盘是无法使用的。未格式化扇区的加密原理就是利用这个特点，该方法在制作原盘时对某一磁道的部分扇区不作格式化处理，这部分扇区无法存储信息，一般的拷贝软件无法拷贝，这样，在被加密程序中对某一特定的磁道进行检查，看其是否为正常磁道，即不含未格式化的扇区，若是正常磁道，则必定为复制盘。下面提供一段制作含未格式化扇区原盘的程序：

GSH\_BUF DB 27H, 00, 01, 02 ; 格式化时所需的标识字段集合

DB 27H, 00, 02, 02

DB 27H, 00, 03, 02

DB 27H, 00, 04, 02

DB 27H, 00, 05, 02

DB 27H, 00, 06, 02

DB 27H, 00, 07, 02

DB 27H, 00, 04, 02

... ..

PUSH ES

MOV AH,35H

INT 21H MOV AL,07H

ADD BX,04H

MOV ES:[BX],AL

POP ES

MOV DL,0 MOV DH,0

MOV CH,27H

MOV BX,OFFSET GSH\_BUF

MOV AH,05

INT 13H

PUSH ES MOV AH,35H

MOV AL,1EH

INT 21H

MOV AL,09H

MOV BX,04H

MOV ES:[BX],AL

POP ES

... ..

在被加密程序中可以安排一段专门程序，用来检查磁盘是否为原盘。具体做法是：检查磁盘上的 39 道上扇区数是否大于 7。若大于 7，则此盘为拷贝盘；否则为原盘。下面给出检查程序：

MOV AX, SEG MY\_BUF

```

MOV ES, AX
MOV BX, OFFSET MY_BUF
MOV AL, 01H MOV DL, 00H
MOV DH, 00H
MOV CH, 27H
MOV CL, 08H
MOV AH, 02H
INT 13H
CMP AX, 0400
JNZ ILLEGL_DISKETTE

```

应当注意，上面这段程序很容易受到攻击。首先，程序是透明的，攻击者用调试程序可将其轻易抹掉；其次，由于某些高级拷贝工具软件功能强大，能完全复制一张磁盘，从而使这段程序失去作用。因而，这段程序还有待于进一步改进，如在应用程序中增加回写操作、明文变密文等。这里就不再一一说明。

#### 7. 螺线型磁道法

磁盘上的磁道是一个个同心圆，当磁头从一个磁道移到另一个磁道进行读写时，必须由 FDC 控制磁头步进，并等待一段时间，待其稳定后，再进行正常的读写操作。通常，这一等待时间称为安顿时间。

螺线型磁道法就是在磁盘上生成一些螺线型磁道，使磁头步进和读写操作同时进行，从而彻底扰乱一般拷贝软件的复制。

螺线型磁道加密技术是将信息写入非标准格式的磁盘，使得普通的拷贝工具无法复制，因而这种方法是一种十分有效的加密方法，但要成功地读写螺线型磁道，必须掌握步进速率和转动速率之间的精确的比率，这是很难做到的，故这种方法可靠性不是很高。

#### 8. 磁道间距不规则变化法

在一般的磁道密度为 48TPI 的软盘驱动器中，磁道间距为  $529\mu\text{m}$ ，其读写磁道宽度为  $330\mu\text{m}$ ，抹去宽度为  $150\mu\text{m}$ 。磁道间距通常是相同的，一般的拷贝软件就是直接控制磁道驱动器的步进电机，使读写磁头在磁道间距相等的磁道上来回移动进行拷贝的。磁道间距不规则变化方法就是抓住拷贝软件这一漏洞。利用软件控制步进电机，使磁头在磁盘上产生不规则的磁道间距，使拷贝软件无法正常拷贝。

该方法是一种很有效的加密方法，但其制作涉及到的驱动器硬件结构，所需专门编制软件来控制步进电机的动作，因而在实际中应用不广。

#### 9. 宽磁道法

有些磁盘复制机构中配有宽磁头，这种磁头可以在多个磁道上同时写入数据，也可以在相邻的两个磁道及其间隙写入相同内容，从而产生一个相当宽的磁道。在被加密程序读磁盘的代码中，让磁盘驱动器的读写磁头在这个“宽磁道”的两个写有相同数据的磁道之间来回步进，数据流是不会中断的，但如果是复制的磁盘，读/写磁头外侧的消磁磁头的抹除作用会使这个宽磁道在物理上分开，成为两个普通磁道，两个之间的间隙中充满了噪音信号，会导致数据流中断。利用这一点即可判断所读取的磁盘是否是原盘。

#### 10. 磁道接缝软指纹技术

所谓磁道接缝，指的就是每个磁道中位于索引孔两边的前置区和后置区。前置区和各个扇区的长度不变，后置区（GAP4）的长度是随机变化的，从 200 字节到 300 字节不等，其中包含的信息也是随机的，不同磁道后置区的长度和内容不同，即使是同一软盘的同一磁道，每格式化一次，其后置区的长度和内容就变化一次。后置区的这一特性就保证了其不可复制性，其内容就像人的指纹一样具有唯一性，完全可以用来加密。

如何将不定长度的后置区取出以作为鉴别的依据,是利用磁道接缝软指纹加密技术进行加密的关键。一般来说,对于标准的磁道要读取后置区是比较困难的,除非用端口读磁道命令来实现,而端口读磁道命令又是十分烦琐的。

读取磁道接缝中的“指纹”有一种巧妙的方法,因为 GAP4 的长度不超过 300 字节,又紧跟在第 9 扇区之后,所以只需在格式化时对第 9 扇区 ID 标志中的 N 改为 3 (磁盘基数表中的 N 不变),这样格式化出的第 9 扇区实际数据长度仍为 512 字节,但在读第 9 扇区时,将磁盘基数表中的 N 改为 3,就可读出 1024 字节的内容,其中就有 GAP4 的信息。这种方法目前是比较强的一种反拷贝方法,可以防止任何拷贝工具的复制,读者可以从此为基础,结合其他方法,设计出更强的反拷贝技术。

#### 11. 扇区软指纹法

通常所讲的每扇区 512 字节指的只是扇区中数据区的长度,但除数据区之外,每个扇区还有其他区域。正常格式化的磁盘,扇区的各个扇区都是可以复制的,但经过特殊格式化的扇区,其某些域上的值就不能被一般的拷贝软件复制,通过检验这些域上数据的正确性就可以判断是否原盘。

一种制作读取这种扇区指纹的方法如下(假定在 30 道 0 面 1 扇区上制作): 制作:对 30 道 0 面进行特殊格式化,取第 1 扇区 ID 字段的 N 为 4 (其余扇区的均为 2),格式化时不修改磁盘基数表,使每个扇区的数据仍为 512 字节。读取:先修改磁盘技术表中的 N 值为 4,而后读 30 道 0 面 1 扇区,同时也就把第 2 扇区的内容全部读出。对原盘和复制盘上读出的内容加以比较就可发现其中有些内容不同,因此来判断是否原盘。

#### 12. 弱位方法

磁盘是用不同的磁化单位来记录信息的。磁盘机读取磁盘时,将磁盘上不同的介质磁场转换成磁头读/写线圈中强度不同的电流,而后由电流信号判断读取的信息是 0 还是 1,电平幅度高于某阈值电平时为 1,远低于阈值电平时为 0;磁盘机写数据到磁盘时,则是将电信号转化为磁介质记录的磁场强度,与读过程相反。

弱位方法就是在写盘时,采用特殊的技术使磁介质记录的磁场强度变小,使磁盘机在读数据时产生的读出电平恰在阈值电平附近,即比 1 信号弱,又比 0 信号强(这一位就叫弱位),再加上鉴别电路的稳定性与精确性有限,使之对读出值产生误判有时判 0,有时判 1。这样的弱位可作为软指纹来防止拷贝。一般的拷贝软件在复制带有弱位的磁盘时,读出的弱位非 0 即 1,写在复制盘上的就是 0 或 1 (而不是弱位),在被加密程序中对这些位进行是否弱位的判断就可得知该盘是否是原盘。判断方法很简单,只需对这些位多读几次,看每次读出的结果是否一致,若每次相同,则是非弱位,否则是弱位。

#### 13. 错误 CRC 法

每个扇区的标识区和数据区的后面都有两个字节的循环冗余码校验码 CRC。CRC 是 FDC 在写完最后一个数据字节时自动产生并写入的,用来校验扇区记录信息是否出错。正常情况下,FDC 产生的 CRC 都是绝对正确的,除非软盘有物理性的损坏。如果人为地在某一个扇区产生错误的 CRC,那么一般拷贝软件按通常的拷贝方法所制出的复制盘中肯定不会无法复制的。于是在被加密程序中判断某一特定的扇区是否有错误的 CRC 就可以知道该盘是否原盘。

有一个简单的方法可用来生成错误的 CRC,即当 FDC 正在写某一扇区时,人为地打断 FDC 的写入过程(如复位 FDC),这个时刻可由修改后的时钟中断程序不断检测 FDC 的主状态寄存器得到。这样就会打乱正常数据的写入,从而在该扇区得到一错误的 CRC 码。检测这一特定扇区的 CRC 是否正确的方法也很简单,用 INT 13H 的 1 号读扇区功能读该扇区,而后判断 AH 的值,若是 10H,则 CRC 错,否则 CRC 正确。

#### 14. 磁道噪音法

磁盘上的信息通常采用 FM 或 MFM 格式进行编码, 这种编码实际上就是在 0, 1 序列中按一定格式插入一定的同步脉冲, 从而形成一个新的脉冲序列, 所插入的同步脉冲对所存的信息本身来说并无什么重要意义, 只是为了读出时提取同步信息。同步脉冲改善了全 0 或全 1 脉冲的频率特性, 使读出信息时不易出错。磁道噪声法就是采用一种特殊的手段在磁盘上写入一种特殊的编码 (即噪声), 使系统在对其读写时产生同步混乱, 使读出的信息出错, 阻止拷贝软件的复制。

#### 15. FDC 移花接木法

FDC 是 CPU 与软盘驱动器之间的接口, 种类很多, 采用的记录方式和功能都不完全相同, 而且用一种 FDC 在磁盘上制作的标记, 可用另一种 FDC 读出, 但却不能被复制, 这就给加密者一个可乘之机, 可以利用两种不同的 FDC 在同一原盘上制作两个不同的标记, 这两个标记可用其中任一种读出并检测, 但却不能只用一种 FDC 来制作, 于是可防止拷贝。

#### 16. 扇区交错保密法

在一个磁道内, 不将扇区按\$0—\$F 编号存放, 而是按任意顺序存放, 这叫做扇区交错法, 采用此方法, 提高了 DOS 向磁盘存取文件时的速度。APPLE 的 DOS3.3 操作系统中, 扇区交错是由软件来完成的, 用 DOS3.3 格式化的磁盘上, 16 个扇区完全按\$0—\$F 顺序排列, 并无交错, 但在内存\$BFB8—\$BFC7 处存放着另一个转换表, 此表将磁盘上的实际扇区编号一一对应到另一组假的扇区编号来供给 DOS3.3 使用, 见下表:

真实编号 0 1 2 3 4 5 6 7 8 9 A B C D E F

对应编号 0 D B 9 7 5 3 1 E C A 8 6 4 2 F

假设修改了\$BFB8—\$BFC7 转换表后, 再用修改过的 DOS3.3 来 INIT 新盘, 可以想象, 如果在这个盘上存入程序, 用标准的 DOS3.3 将无法存取这些程序, 因为它们之间扇区转换表不相同。

“扇区交错”程序保密法可以利用上述办法来制作出能保密程序的保密磁盘。制作保密磁盘对硬件的要求是: APPLE 机的内存为 48K, 6 号槽口接上磁盘机, 磁盘机的编号为 1

制作方法如下:

(1) 制作一个不同于 DOS3.3 的扇区转换表。将 16 进制数字 0 至 F 间除去 0 剩余的 15 个数随意添入下表横线上 (尽量不与标准 DOS3.3 的转换表一致):

00 \_\_\_\_\_

假设你添入的是:

00 07 0D 04 05 09 0E 01 06 0A 02 0C 08 0F 03

在纸上记下这组数字, 然后根据 APPLE 机的显示 ASCII 码表, 把每个数字加上 C0 所得的值转化成字母, 本例应为:

@ G M K D E I N A F J B L H O C

这就是以后使用保密盘时所必须给出的通行口令。有了这个口令, 才能往保密盘上存入或取出程序。记住这个密码。

(2) 将标准 DOS3.3 引入内存, 用 CALL-151 进入监控后, 把刚才记在纸上的 16 个数输入从\$BFB8 开始的单元中。

\*BFB8: 00 07 0D 0B 04 05

09 0E 01 06 0A 02

0C 08 0F 03

\* (敲入 CTRL—C)

I NEW

]

再将一个空盘插入接在 6 号槽口的 1 号驱动器中。



]I NI T HELLO

]CALL—151

\*6000: 01 60 01 00 00 11 60 00 40 00 00 01 00 00 60 01 00 01 EF D8

\*7000: A0 00 A9 60 4C D9 03 N 7 0 0 0 G

\*404E: <4 04 D 4 05 B M

\*404E8: A2 01 20 1B FD 29 0F 9D 4C 08 E8 E0 11 D0 F3 A5 2B 4A 60

\*4007: 20 E8 08 N 4 0 4 A :4C 69 BA N 60 0 C :02 N 7 0 0 0 G

\*600C: 01 N 60 05: 09 N 7 0 0 0 G

40B9 <40B8 40 C 6 M N 600C: 02 N 7000G

\*600C: 01 N 6005: 04 N 7 0 0 0 G

\*4069: 84 FF A0 10 B9 4C 08 99 B7 88 D0 F7 A4 FF 6C FD 6C FD 08 N 60 0C: 02 N 7 0 0 0 G

至此，加密盘已制作好。

#### 8.4.1 破解加密光盘

如今市面上有很多加密光盘，这些光盘是以特殊形式刻录的。将它放入光驱后，就会出现一个软件的安装画面要你输入序列号，如果序列号正确就会出现一个文件浏览窗口，错误则跳回桌面。如果你是从资源浏览器中观看光盘文件就是一些图片之类的文件，你想找的文件却怎么也看不到。这样的事情你碰到过吧？如果你的光盘序列号丢了或者光盘上的序列号根本不对，那该怎么办呢？别急，有下面几种方法来帮我们。

第一：用 UltraEdit 等 16 进制编辑器直接找到序列号

运行 UltraEdit，用它打开光盘根目录下的 SETUP.EXE，然后点击菜单上的“搜索”→“查找”，在弹出的对话框“查找什么”栏中填入“请输入序列号”，注意要将多选框“查找 ASCII 字符”勾选上，回车，在找到的“请输入序列号”后面，接下去的数字就是序列号了。

第二：用 IsoBuster 等光盘刻录软件直接去浏览光盘上的隐藏文件

运行 IsoBuster，选择加密盘所在的光驱，点击选择栏旁边的刷新按钮，此时它就会读取光驱中的文件，这时你就会发现在左边的文件浏览框中多出一个文件夹，那里面就是你真正想要的文件。这时你就可以运行或复制这些文件了。

第三：要用到虚拟光驱软件(如 Vcdrom，虚拟光驱 2000)和 16 进制编辑器(如 UltraEdit，WinHex)

方法是：

1. 用虚拟光驱软件把加密光盘做成虚拟光碟文件，进度到 1%的时候就可以按 Ctrl+Alt+Del 组合键强行终止虚拟光驱程序的运行。

2. 用 16 进制编辑器打开只做了%1 的光碟文件(后缀名为 vcd 或 fcd 的文件)，在编辑窗口中上下查找任意看得见的目录名或文件名(由于文件不大很容易找到的)，在该位置的上下就可以看见隐含的目录名或文件名了(一般是目录名)。

3. 在 MS-DOS 窗口下用 CD 命令进入看到的那个目录，再 Dir 一下就可以看见你想要的了，此时是运行还是复制文件就随你了

第四式：在光驱所在盘符下执行：

dir filelist.exe 即可运行浏览程序(filelist.exe 为隐藏的浏览光盘的程序)。

用这种方法对付好多光盘都有效，而且不需要任何软件。

第五：利用 File Monitor 对付隐藏目录的加密光盘

File Monitor 这个软件大家可能不是很熟悉，它是纯“绿色”免费软件，可监视系统中指定文件运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它，你指定监控的文件有任何读、写、打开其它文件的操作都能被它监视下来，

并提供完整的报告信息。我们就是用它的这个功能来监视加密光盘中的文件运行情况，从而得到我们想要的东西。

下面以某新版 DDR 跳舞碟为例，来看看如何发现隐藏目录。

1. 运行 File Monitor 的主文件 FileMon，在“Options”内将“Capture Events”打上勾；
2. 运行 DDR 跳舞碟，当选择的舞曲已调入内存后即可退出 DDR；
3. 回到 FileMon，把所有的文件调用均被记录下来。现在再将“Capture Events”前面的勾去掉，免得它仍旧不断的增加记录，然后来看看记录的都是什么。以下是截取的部分内容：

```
Explorer FindOpen E:DDR99.EXE SUCCESS
Explorer FindClose E:DDR99.EXE SUCCESS
.....
.....

Ddr99 FindOpen E:BGMS.WAV NOMORE
Ddr99 FindOpen E:BGMS.WAV NOMORE
.....
.....

Ddr99 Open E:BGMTRACK_01.WAV SUCCESS
Ddr99 Seek E:BGMTRACK_01.WAV SUCCESS
```

一切显而易见了，原来新版的 DDR 跳舞碟其加密子目录为“BGM”。

8.4.2 DVD 影片（区码）的保护与破解

DVD 影片既然有加密，就一定有破解之道。因此，在这篇文章里，我将试着将我所知道的有关 DVD 影片（区码）保护和破解的方法介绍给大家。

大家应该都知道 DVD 影片不像 VCD 一样，DVD 影片对于它里面所记录的数据做了十分严密的加密，最简单的一个例子就是区码保护。下面我就简短地介绍一下现在 DVD 影片的加密技术：

现在的 DVD 加密防拷技术主要分成：数码加密”和：类比加密”两部分。

1. 数码加密（CSS）

DVD 影片的数码加密主要是由所谓的“CSS（Content Scrambling System，数据干扰系统）”加密的。所谓的 CSS，就是所有存入 DVD 影片内容的数据都要经过编码程序，而要播放这些影片数据必须先经过解码才能播放。传统的 VCD，它是把影音数据放成光盘的 MPEGAV 这个目录下，直接用 VCD 播放工具打开文件，就可以播放了。而现在的 DVD 却不行，因为 DVD 影片数据现在被 CSS 保护，所以你在 DVD 影片里看的影像必须经过“解码授权”，也就是用合法的解码程序才能播放，不管在家电产品的 DVD 影碟机，还是在电脑上用的 DVD-ROM 和 PowerDVD 之类的播放软件播放影片，都必须经过解码才能正常播放。现在 DVD 影片分成了 6 个区，分别是：

| 区码  | 区域范围                      |
|-----|---------------------------|
| 1 区 | 加拿大、美国                    |
| 2 区 | 日本、欧洲、中东、埃及、南非            |
| 3 区 | 东南亚、东亚                    |
| 4 区 | 澳洲、新西兰、南太平洋群岛、中美洲、墨西哥、南美洲 |
| 5 区 | 非洲、印度、中亚、蒙古、前苏联、北朝鲜       |
| 6 区 | 中国                        |

所以你去美国买来的“原版”DVD，带回中国，却不能播放，因为在 CSS 里面，你的

“解码授权”只被限定在你可以看第 6 区（中国）的 DVD 影片，而美国的第 1 区的 DVD 影片，你没有授权，不能看，给我们造成了很大的不方便，而我们这篇文章的重点，就是告诉如何突破区码的禁锢。

## 2. 类比加密（APS）

DVD 影片的另一个加密保护的重点就是防止你用录像机拷贝。即然数码图像经过 CSS 编码，无法复制，那我们录像机对拷总行了吧？很不幸，这一点也被封锁了，在 DVD 影片内，有一个所谓“APS（Analog Protection System，类比信号保护系统）”，它主要是通过一颗 Macrovision 7 的芯片，利用特殊信号影响录像机的录像功能。如果你用的是电脑播放 DVD 影片，而你想把它接到电视上欣赏，假如你的显卡没有 APS Macrovision 认证的话，你就无法在电视上享受 DVD 影片的优秀画面。对于不想换显卡（或者想用录像带备份）的人来说，我将会介绍一款硬件来帮你突破 APS 的限制。

下面我们就来看看如何破解区码：

前面提过，CSS 规定，必须同时软、硬件都经过“授权认证”才可以成功的解码播放 DVD 影片内容，也就是说你在电脑里面的 DVD-ROM 的 DVD 播放软件都必须同时通过区码的授权，所以破解区码的方法要分成软、硬件两条路线来进行。

在软件方面，因为区码是一定要设定的，不然播放软件不知道如何来解码，我们可以在网上找到专门更改软件区码的软件。

在硬件方面，我们选一台无区码限制的 DVD 既可。

### 1. DVD 的区码和破解

DVD-ROM 的问世其实和 DVD 影片一点关系都没有。所在在早期的 DVD-ROM 内根本没有什么区码的保护限制，也就是早期厂的 DVD-ROM 可以读取所有 6 个区域的 DVD 影片。不过在 1999 年，所有出厂的 DVD-ROM 都加上了区码的设置，也就是说最迟 2000 年来开始，所有出厂的 DVD-ROM 都必须经过 CSS 的区码认证，也就是要加上“区码设定”限制，而每一台 DVD-ROM 最多可以改 5 次区码，在第 5 次后，这台 DVD-ROM 就只能用最后一次设置的区码了。所以我们要使用 2000 年之前出产的 DVD-ROM。

另外，需要提醒的是，有些机子后面还有一个“RPC Jump”的设定，这个“RPC Jump”大家千万记得不要去动它，不然你本来一台没有区码限制的机器，在拔掉后瞬间，就成了区码永远被锁了，而且再也无法恢复。下面我就着重讲一下这两种 DVD 的破解方法：

### 2. 如何更新机器固件破解区码保护

在“DVD UTILS NETWORK”网站内提供了无区码保护的固件，有条件上网的朋友可以在那里选上你的 DVD 的品牌，下载对应型号的固件后，更新你自己的 DVD-ROM，这样你的 DVD-ROM 就成了没有区码限制了。之前我也提到过，原来 DVD-ROM 就没有什么区码的保护，它们全都属于 RPC-1 的机型，也就是所有的 6 个区的 DVD 影片都可以读取，不过后来由于新的规定，所有新出厂的 DVD 都必须在固件中加入区码限制，所以这些机型才成了 RPC-2 的机型。因此我们只要自己将机器的硬件还原成 RPC-1，就可以回到以前没有区码的环境下了。

### 3. 利用 flash 工具破解区码保护

对于最近新出的 DVD-ROM 来说，由于都必须符合 CSS 的规定，因此它们全部都是 RPC-2 的机型。这些 DVD-ROM 设计之初就是须要区码保护的，所以你也找不到什么硬件更新的方法来破解它。不过网上针对某些型号的 DVD-ROM（Pioneer 的机器及它的 OEM 机器）写了一个叫做“Region Eraser”的 flash 工具，它可以让你将 DVD-ROM 硬件内有关区码的设置清除，而且还把有关的更改次数也一起清掉，这样可以使我们无限制的改变机器的区码。算是间接的破解区码保护限制了。

选择“Pioneer 10X DVD-Rom drivers:Make them “nearly” region free!” 的链接进入。

进去后你可以看到有关“Region Eraser”的说明，和它可以工作的 DVD 型号。在这里我要说明一下，首先，使用“Region Eraser”有一定的危险性，所以你必须清楚你自己在做什么；其次，如果你的 DVD-ROM 属于那些可以通过修改固件来破解区码的型号，请不要使用“Region Eraser”来破解。最后，“Region Eraser”会把机器内的区码设置清除，所以在清除后，你要自己重新设置区码，这个网站上也同时提供了区码设置工具，如果你买的 DVD-ROM 里没有附送的话，你可以去[这里](#)下载。

#### 4. 如何更新软件区码的设置

前面说了一大堆有关 DVD-ROM 区码的破解方法，不过这只算成功了一半，因为 DVD 播放软件也做有区码保护，同样也只能更改区码 5 次，而且没有所谓的无区码限制播放软件，它们一定要设置区码才能工作。网上有一套叫做“DVD GENIE”的免费工具，它的做有点类似于刚刚提到过的“Region Eraser”，它可以让你无限次数的更改播放软件里面的区码设置，这个工具支持很多常用的 DVD 播放软件，如 PowerDVD、SoftDVD、Xing、WinDVD……等等，在“DVD Genie”里你可以更改播放软件的区码，它还提供了“Reset”功能，能够让你将区码已更改次数重设为 0，这样你就可以无限制的改变区码，不用再担心只能更改 5 次。