常见密码破解方法

设置密码是运用最多、也是最方便有效的安全控制措施，但随着密码数量的增多，忘记密码的现象也与日俱增，在这种情况下如何解除所设置的密码，尽可能减少损失也是广大用户所关心的问题。

1、WinZip

设置：右击需要压缩的文件，并从弹出的快捷菜单中执行"Add to Zip"命令，打开"添加到文件"对话框，然后单击"密码"按钮，打开"密码设置"对话框并输入所需密码即可。加密后可使用"WinZip"查看压缩包中的文件列表，但解压或浏览某个文件时，系统就会要求用户输入密码。

解除：当用户遗忘 ZIP 压缩包的密码时，可以到 http://www.elcomsoft. com 下载一个解除 ZIP 压缩包密码的专用解除密码软件 AZPR（Advanced ZIP Password Recovery）对密码进行搜索。只需在"ZIP password encrypted file"对话框中选择需要解除密码的 ZIP 压缩包，并在"Brute Force range options"对话框中选择密码的范围（例如是否包括大小写字母，是否包括数字、空格、符号或包括所有内容等），最后单击"Start"按钮，系统就能找到密码并将其显示出来。

2、ARJ

设置：ARJ 是一个命令行实用软件，它的操作全部通过命令行来实现。其中参数"-P"是用来设置压缩包密码的，用户只需在参数后面输入相应的密码，即可达到为压缩包设置密码的目的（注意："-P"参数与密码之间没有空格）。例如将 C 盘 DOS 目录下的所有文件全部压缩到一个名为 BACKUP 压缩包中，并为它设置

"PASSWORD"的密码，只需执行"ARJ A-PPASSWORD BACKUP C：\\DOS"命令即可。

解除：当 ARJ 压缩包的密码被遗忘后，用户同样可以到 http://www.elcomsoft.com 下载一个 ARJ 压缩包密码专用解除软件 AAPR（Advanced ARJ Password Recovery），然后再利用它找出 ARJ 压缩包的密码。AAPR 的界面及操作方法与 AZRP 基本一致，在此就不作详细介绍了。

3、Word 和 Excel

设置：执行"文件"菜单的"另存为"命令，打开"另存为"对话框并单击"选项"按钮，然后根据需要在弹出的"保存"对话框的"打开权限密码"或"修改权限密码"栏中设置所需密码（注意：设置"打开权限密码"后，不知道密码的用户将无法打开文档；设置"修改权限密码"后，其他用户仍然可以打开文档进行浏览，但不能对文档进行修改），最后单击"确定"按钮即可。

解除：遗忘 Word 或 Excel 密码后，用户可借助 MOSfPass 进行解除。MOSfPass 是一个解除 Office 文档密码的专用应用程序（目前主要是针对 Word 和 Excel），用户在启动该程序后首先应单击"Settings"按钮，打开"Brute force setting"对话框，对 MOSfPass 的解除状态进行设置（在"Pass- word character set"列表框中选择密码的范围，即是否包括大小写字母、数字、空格等内容）。单击"OK"按钮返回主菜单，然后将需要解除密码的 Word 或 Excel 文档拖拽到 MOSfPass 主菜单中，MOSfPass 即会根据指定范围采用穷尽法对所有可能的密码进行测试，直到找到密码为止。

MOSfPass 的下载网址为：http://www.lostpassword.com。另外，用户也可到 http://www.elcomsoft.com 下载一个 AWPR（Advanced

Word Pass- word Recovery）或 AEPR（Advanced Excel Password Recovery）程序来解除 Word 文档或 Excel 密码，使用方法与 Advanced ZIP Password Recovery 完全一致。

4、Access

设置：执行"工具"菜单"安全"子菜单中的"加密数据库"命令，然后再输入适当的密码即可。

解除：利用 UltraEdit 等软件采用二进制格式打开加密后的 Access 数据库，然后将地址为 0042 的字节改为 0086 并存盘退出，数据库的密码即失效（建议：执行此操作前先做一个备份）。另外，用户也可到 http://www.elcom-soft.com 下载一个 AAPR（Advanc- ed Access Pass- word Recovery）程序来解除 Access 数据库密码。

5、解除应用"*"显示的密码

用户输入密码时，大部分软件不显示原始字符，而显示为"*"。这种密码又该如何解除呢？Snadboy 是一个专门用于解除用"*"显示密码的工具软件，它可将这些密码的原始字符查找出来。要使用它解除密码，只需先打开其它应用程序并显示出密码对话框（即显示"*"），然后用鼠标将 Snadboy"密码区选择器"中的"十字架"拖拽到这些应用程序的"*"密码上，Snadboy 就会把密码破解出来，并将其原始字符显示到"密码"框中。Snadboy 的下载网址为：http://www.snadboy.com。除此以外，类似的软件也有很多，例如 VIEWPASSWORD 等。

6、BIOS 密码破解

在使用电脑的时候，如果在 BIOS 中设置了密码口令而忘记了设置口令，就

不能进入 BIOS 设置程序或者进入电脑系统中，这时我们可以给 CMOS 供电电池放电的方法来解决这个问题，或者用低级语言进行编程解密码。

6.1 CMOS **放电**

（1）电的原因

为了防止其它人使用自己的电脑，会在 BIOS 设置程序中设置一个开机口令，存放在 CMOS RAM 中，可是后来改了配置情况，需要在使用新的配置前进入 BIOS SETUP 重新更改设置，却忘掉了进入口令或是病毒，可是非法侵入电脑的 CMOS RAM 中，但 CMOS RAM 的内容在机器断电的情况下仍然不会消失，所以不能很方便地将病毒清除。在碰到了以上情况时，就要对 CMOS 进行放电。

（2）放电的原理

只要电脑主板上的电池电容不消失，CMOS RAM 里面的信息即使在整台电脑断电的情况下也不会消失，为了使存储在 CMOS RAM 中的信息消失，必须使主板上的电池消失。所以在整机断电的情况下，将电脑主板上对 CMOS RAM 供电端的正极与电脑主板上的内置电池或外接电池的正极断开一定的时间，即“对主板放电”，便可使 CMOS RAM 中的内容因为得不到正常的供电，而内容丢失

（3）放电的方法

在具体进行放电操作时，可以根据不同的情况，有以下几种方法：

① 路线清除方法

在某些主板上，有一组单独的两针跳线，用来清除 CMOS RAM 是的内容。该组跳线一般标注为 CLEAR CMOS。当需要清除 CMOS RAM 中的内容时，用一个跳线帽将该组跳线短接一会儿即可。

在某些主板上，有一组单独的三针跳线，要来清除 CMOS RAM 中的内容。该

组跳线两端的两根针一般分别标注为 NORMAL 和 RESET CMOS。在正常情况下，盖子跳线中间的一根针和标注为 NORMAL 的一根针短接。如果将该组跳线中间的一根针和标注为 RESET CMOS 的一根针短接，就可以清除掉 CMOS RAM 中的内容。

清除 CMOS RAM 中的内容，请千万不要忘记将该组跳线中间的一根针和标注为 NORMAL 的一根针恢复短接；否则开机时，主板可能没有任何显示。

②跳线放电方法 2

要某些主板上 ,有一组单独的四针跳线 ,用来对 CMOS RAM 供电和清除 CMOS RAM 中的内容。该组跳线的两端的两根针一般用来外接 CMOS RAM 的供电电池（EXTERNAL BATT）; 如果 CMOS RAM 采用的主板内置电池供电，用一个跳线帽将第三根针和第四根针短接一会儿即可将 CMOS RAM 中的内容清除，短接的时间应参照主板的说明书。清除掉 CMOS RAM 中的内容后，请不要忘记将跳线器的状态恢复原状。

③跳线放电方法 3

在某些主板上 ,有一组单独的四针跳线 ,用来对 CMOS RAM 供电和清除 CMOS RAM 中的内容，该组跳线四针的电路作用与方法 2 中的相同。这些主板的 CMOS RAM 采用通过四针跳线的一、四根针外接电池的方法供电。为了避免将该跳线外接电池的极性接反，外接电池的插接连线的三号插孔就堵死了，所以主板的四针跳线的第三根针（即与 CMOS RAM 供电端连接的针）也就折断了。若要清除 CMOS RAM 中的内容则需要采取下面的办法；在主机断电后，打开主机箱，找到 CMOS RAM 外接的供电电池，将其在主板四针上的插接线拔下；然后用万用表，将开关打到直流电压 10V 档，用黑表笔接触四针跳线的第四针（即 CMOS RAM

供电的负端），红表笔接被扭断的第三针残留的根部，持续一段时间，当万用表的指示接近 0 时，即可达到放电目的。

④自然放电方法

在断电时打开主机箱，取下主板上内部供电电池；或将主板外接电池拔下，两面三刀三天后再装好，即可达到放电目的。

⑤短路电池法

如果电池是焊在主板上面上，可以用一根导线，分别触及该电池的正极和负极，以使得该电池的正极和负极连通；并持续一段时间，就可将 CMOS RAM 的内容清除。

通过以上的方法，就可以对 CMOS 进行放电处理。但主板上的 CMOS RAM 的内容丢失后，在重新启动电脑时，将会出现诸如 CMOS 电池无效，请重新设置其内容的提示，并且给出可以进入 CMOS RAM 设置的按键。这个时候只需要进入 BIOS SETUP 中 ,选择主菜单中的 LOAD BIOS DEFAULTS(装载 BIOS 缺省设置值）或 LOAD SETUP DEFAULTS（装载设置程序缺省值），然后重新启动电脑即可。

6.2 编程破解密码

编制程序清除口令密码比上面介绍的方法或许更加方便。下面将详细介绍几个相关的小程序。

CMOS 开机密码按密码框出现的不同地点分为两种(这里不是指用户密码和超级用户密码），一种是要进入 CMOS 设置时出现的密码；另一促是每次开机时出现的密码，破解方法有很多，下面将分别讲解。

（1）更改硬件配置

当丢失 CMOS 密码时，可以先改动机器的硬件后再重新启动，因为启动时如

果系统发现新的配件配置与原来的硬件配置不相同，可能会允许你直接进入CMOS 重新设置而不需要密码。改动硬件配置的方法很简单，比如拔下一根内存条或安装一块不同型号的 CPU（当然要主板支持）、更换一块硬盘等。

（2）建立自己的密码破解文件

当系统自检完毕，准备引导 Windows 时按下 F8 键，选择 Safe mode command prompt only(安全命令模式)后，在 DOS 提示符下输入 COPY CON YK.COM，回车后在编辑环境里输入：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 后，按 F6 键保存。

启动时选择安全命令模式后，输入 COPY CON YK.COM，然后在编辑环境里输入：ALT+176、ALT+17、ALT+230、P、ALT+176、ALT+20、ALT+230、P、ALT+205、空格后，按 F6 键保存，重新启动计算机即可。

保存退出后，直接运行 YK.COM 文件，屏幕上没有任何提示信息，然后重新启动计算机即可清除 CMOS 里的密码，此时，CMOS 里的其他设置也会同时被清除。

（3）DEBUG 法

在 DOS 提示下，运行 DEBUG 后输入：

```
-0 70 18
-0 71 18
-Q
```

或者

```
-0 70 21
-0 71 21
-Q
```

或者

-0 70 10

-0 71 0

-Q

退出到 DOS 提示符号，重新启动计算机即可将 CMOS 密码完全清除。

（4）万能密码

如果将 CMOS 里的安全选项为系统，当每次开机时都必须输入正确密码，否则变无法进入 Windows、DOS 系统，这样只能靠万能密码来解决问题。

●AMI 的 BIOS 万能密码为：AMI：Sysg。

●AWARD 的 BIOS 万能密码为：award；Syxz；h996；wantgirl；ebb；dirrid。

以上的万能密码在 386 、486、奔腾主板上破解 CMOS 口令几乎是百发百中，而对 PII 级或以上的主板就很困难，能破解 PII 以上新主板的万能密码很少，但可以通过一些软件进行破解。

（5）使用工具软件

破解 CMOS 密码的破译软件在网上比比皆是，其中 Biospwds 软件的破译能力较好，只需轻轻一点 Getpasswords（获得密码）按钮，CMOS 密码便完全显示，此外，还可以看到 BIOS 版本、时间等信息。该软件可在 http://www.geocities.com/ 处下载。

7、Windows 2000 管理员密码破解指南

最近，有不少朋友都向我反映说由于种种原因，他们的 Win2000 系统(或 NT、XP 系统)管理员密码丢失了，问我该如何找回密码。好朋友嘛，我总不能不帮，于是针不同的情况，分别给于相应的对策，最终帮他们找回了自己的密码。余暇

时，稍做整理促成本文，全文以实际破解操作为例，详细讲述了Windows2000(NT/XP)系统下如何找回丢失的管理员密码。希望能对众多Windows2000（NT/XP）系统管理员及广大用户有所帮助。

7.1 **终极武器** Windows Key **篇**

系统：Windows2000 Professional [Version 5.00.2195]

相关情况：系统管理员帐号 administrator 密码丢失、无其它可登陆用户帐号、SAM 文件无法读取或做其它操作、无输入法漏洞等可利用漏洞。

所需工具：Windows2000 安装光盘（或 Windows2000 启动盘）、Windows XP-2000-NT Key、空软盘一张。

操作过程及相关解答：

首先，我们需要借助 Windows XP-2000-NT Key 制作一张特殊的驱动盘。Windows XP-2000-NT Key 是美国 Passware 公司出品的一款专门针对 Windows 密码破解的工具软件，http:www.password.com 提供该软件的 DEMO 版及详细使用说明，有兴趣的朋友不防前去一看。打开该软件，可以看到最下方有一行提示：Please insert a blank floppy disk into drive A:and click NEXT when ready。这时，将准备好的软盘插入软驱，点 Next，Windows XP-2000-NT Key 会自动将此盘制作为一张特殊的驱动盘。驱动盘做好后，就可进行下步工作了。用 Windows2000 的安装盘（或启动盘，本例中使用安装盘）启动待恢复密码的计算机，当提示 Press F6 if you need install party SCSI or RAID driver...时，按 F6，等待加载过程结束后，看到提示：To specify addition al SCSI adapters,CD-ROM drivers.or special disk controllers for use with Windows 2000,including those for which you have a device support disk from mass storage device manufacturer,press S ,立刻按 S 键，

然后系统会接着提示：Please insert the disk labeled maufacturer-supplied hardwaresupport disk into driver A: * Press ENTER when ready。这时插入软盘加载上面做好的 Windows XP-2000-NT Key 驱动。稍等片刻，系统便会自动进入 Windows XP-2000-NT Key 环境。这时系统会提示：Set Administrator'Password to '12345'？(Y/N)：，键入 Y，待显示：

Password has been reset.

User name is 'Administrator'.

New password is '12345'

此时，系统管理员帐号 administrator 的密码已被改为 12345 了。取出安装光盘及软盘，重新启运系统即可用此帐号登陆。

后记：以上即是一例破除 Windows2000 系统管理员密码的全过程，也许有人会说，这并没有把密码破解呀！不错，本例中并没有做到把密码破解，但的的确确这样做完全可以拯救管理员帐号，效果是一样的。再则，这种方法可以称得上是破除 Windows2000/NT/XP 管理员密码的终极方法，100％的成功率！而且操作简单，易学易用！唯一的缺撼就是这套 Windows NT-2000-XP 软件是商业软件，并不是人人可以用得到的。

接下来，笔者将带领各位用第二种方法破解 Windows2000(NT/XP)系统管理员密码。有兴趣的朋友请接着往下看。

7.2、破解利器 LC4 篇

LC4 可以称得上是一款古董级的超级密码解破利器，在 LC4 发行之前已有数个被称为 L0phtCrack 的旧版本。这个工具可以实现从 Sam 文件中进行密码刺探破解，对于可以取得 Sam 文件的情况来说，选用它是个极不错的想法。

系统：Windows2000 Professional [Version 5.00.2195]

相关情况：系统管理员帐号 administrator 密码丢失、无其它可登陆用户帐号、无输入法漏洞等可利用漏洞，通过种种手段可取得其 SAM 文件。

所需工具：LC4、KLC4

操作过程及相关解答：

首先，我们需要做的是下载本例中所需的两款软件，软件下载后需要注册才能实现其全部功能。KLC4 的使用极为简单，按软件提示操作即可轻松取得 LC4 的注册码，这里不多缀述。接下来我们需要做的仅仅是以下的几个简单步骤：

打开 LC4，并新建一个任务。然后依次点击 IMPORT、Import from SAM file..... 打开已待破解的 SAM 文件。此时 LC4 会自动分析此文件，并显示出文件中的用户名。之后点击 Session 中的 Begin Audit，即可开始破解密码。如果密码不是很复杂的话，很短的时间内就会有结果的。

当然，LC4 是个功能强大的软件，它的一些高级功能允许用户自定破解策略，以及断点等等，但其已不在本文讨论范围之内，具体使用方法这里不多讲述，有兴趣的朋友可以自己研究。

然而，这种方法也有它的不足之处，如果密码比较复杂的话，可能会需要几天或数月甚至几年的时间，很显然，在这如此况下这种方式就不再那么有效了。