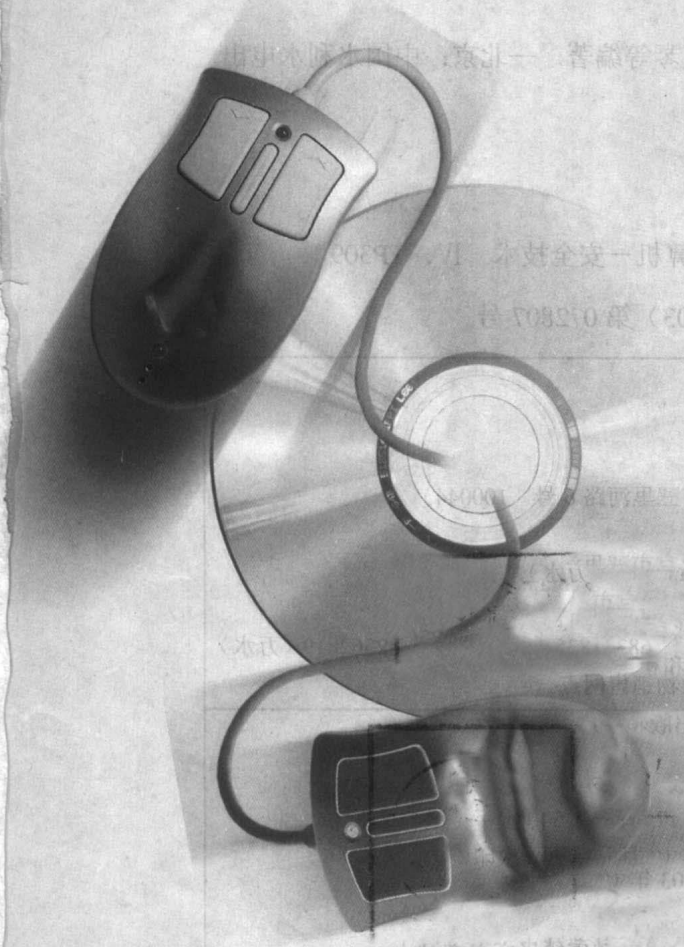
中国电脑教育报
CCID CHINA COMPUTER EDUCATION 系列图书

电脑隐私保护及防黑技术精解

中国水利水电出版社
www.waterpub.com.cn

CCID 中国电脑教育报 CHINA COMPUTER EDUCATION 系列图书

电脑隐私保护及防黑技术精解



作　者：周正琴　杨宏权　冀帅领
责任编辑：吴立群

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书主要介绍了在使用电脑的过程中如何保护个人隐私，让您在使用电脑时多一份放心。与此同时，还向您讲解黑客入侵、攻击、破坏系统与获取信息的各种方式，您不必会写程序也不需要了解专业的网络知识，即可轻易按照书中的说明与操作完成“黑客”任务。当然，您还可以根据本书介绍的方法措施防御黑客的入侵与破坏。

图书在版编目（CIP）数据

电脑隐私保护及防黑技术精解/周正琴等编著. —北京：中国水利水电出版社，2003

（中国电脑教育报系列图书）

ISBN 7-5084-1662-7

Ⅰ. 电… Ⅱ. 周… Ⅲ. 电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2003）第 072807 号

书　　名	**电脑隐私保护及防黑技术精解**
作　　者	周正琴　杨宏权　冀帅领
策划编辑	莫亚柏
出版、发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@public3.bta.net.cn（万水） sale@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京峥峥印刷厂印刷
规　　格	787×1092 毫米　16 开本　17 印张　540 千字
版　　次	2003 年 10 月第一版　2003 年 10 月北京第一次印刷
印　　数	00001—10000 册
定　　价	19.00 元

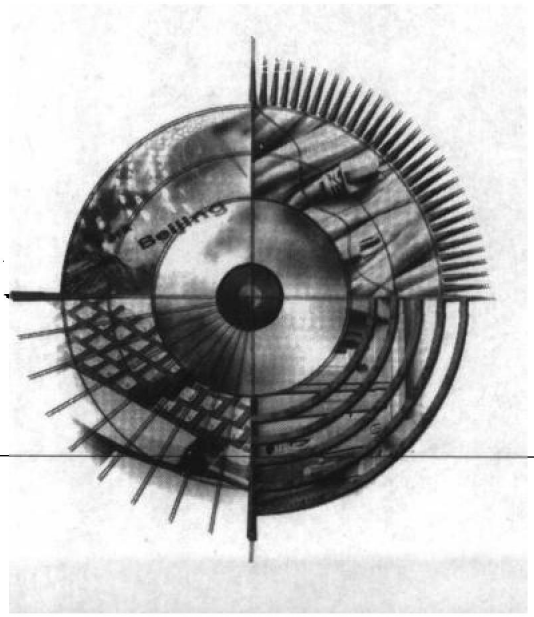
目　录

第三部分　黑客帝国 81

第一部分

隐私保护

- 操作系统隐私保护
- 文件的加密和隐藏
- 电子邮件隐私保密
- 网吧隐私保密
- 去除广告保护隐私



第 1 章　操作系统隐私保护

1.1 设置 CMOS 密码

开门先开锁，如果没有开门的钥匙，想行“窃”也不那么容易哟。所以我们为了保护计算机的安全，第一步需要做的就是为电脑设置开机密码。

1.1.1 设置开机密码

开机密码可以通过设置 CMOS 密码来实现。CMOS 是电脑主板上的一块可读写的 RAM 芯片，主要用来保存当前系统的硬件配置。而且 CMOS RAM 芯片由系统通过一块后备电池供电，无论是不是开机，CMOS 的信息都不会丢失。每当开机时，首先要运行检测的就是 CMOS 中的信息了，所以我们先要设置 CMOS 密码，因为它是第一道“大门”哟。

下面我们以 AWARD BIOS 主板为例，将设置 CMOS 的具体操作介绍如下：

步骤 1 启动计算机，在出现计算机系统自检画面时连续按【Del】键(注意：是不停地按动，而不是按住不放)，直到出现 CMOS Setup 主界面即可(如图 1.1.1 所示)。在这一步需要注意的是，并不是所有的电脑都是按 Del 键进入 CMOS Setup 主界面的，如康柏电脑就是按 F2 功能键进入，所以在实际操作时，一定要仔细查看主板说明或是开机后屏幕下面的文字说明。

图 1.1.1

步骤 2 用键盘上的光标键选择【Supervisor Password】选项，然后按回车键，出现【Enter Password】文本框后(如图 1.1.2 所示)，输入密码。如果是第一次进行此项设定，输入口令不要超过 8 个字符，屏幕不会显示输入的口令，输入好后按回车键。

步骤 3 出现【**Confirm Password**】文本框，再次输入同一密码(注意：该项原意是对刚才输入的密码进行校验，如果两次输入的密码不一致，则会要求用户重新输入)。

步骤 4 再通过移动光标键，选择 CMOS Setup 主界面中的【User Password】项后按回车键，操作同步骤二、三，密码需输入两次才能生效。

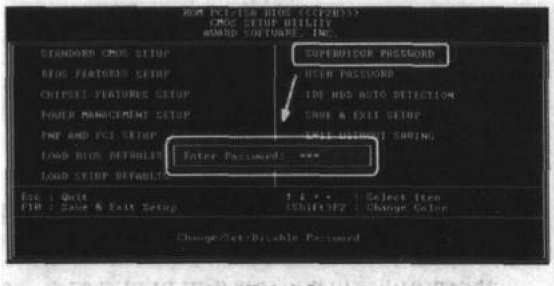


图 1.1.2

【说明】

上面我们设置了两个密码，即“Supervisor Password”与“User Password”，它们又称为超级用户密码与普通用户密码，这样我们就对计算机设置了开机密码。它们的根本区别在于对于 CMOS 的修改权。普通用户密码是用于开机，超级用户密码不但可以开机进入系统，还能进入 CMOS 修改选项。笔者建议两个均取同一密码，以便记忆。

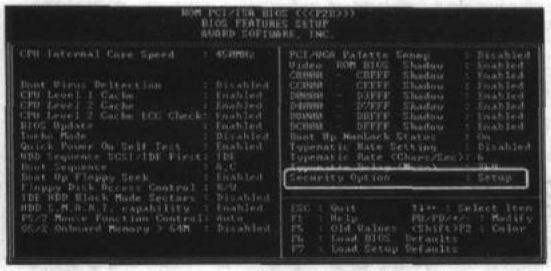


图 1.1.3

步骤 5 在 CMOS Setup 主界面中，再通过移动光标键选择【BIOS Features Setup】选项按回车键，用光标键选择【Security Opion】项后用键盘上的 Page Up/Page Down 键把选项改为 System（如图 1.1.3 所示）。设定为 System 的目的在于让计算机在任何时候都要检测密码，包括启动机器。然后按【Esc】键退回主界面。

【说明】

其实【Security Option】选项有两个参数，即 Setup 与 System。这是 CMOS 密码的两种状态。如果选择 Setup，在开机的时候是不会出现密码输入提示的，只有在进入 CMOS 设置时才要求输入密码，密码设置的目的在于禁止未授权用户设置 BIOS，保证 CMOS 设置的安全。如果选择 System，那么每次开机启动时都会要求输入密码（只要输入超级用户密码或是普通用户密码其中的一个即可），如果密码不对，就无法使用计算机，此密码的设置目的在于禁止外来者使用计算机。根据上面的分析不难发现，设置了 System 密码，安全性更高一些。

步骤 6 选择【Save&Exit Setup】选项回车（或按【F10】功能键），出现提示后按【Y】键再按回车键，以上设置的密码即可生效。

1.1.2 更改与消除 CMOS 密码

步骤 1 进入 CMOS Setup 主界面后，利用移动光标键选择【Set User PassWord】或【Set Supervisor Password】，这时弹出【Enter Password】文本框，重新输入更改的密码，然后直接按回车键，在检证对话框，两次输入后，按回车键。

步骤 2 选择【Save&Exit Setup】选项按回车键（或按【F10】功能键），出现提示后按 Y 键再回车键，以上密码更改即可生效。

如果想消除密码，只要在两次输入密码的对话框中，不输入任何密码即可。

1.1.3 如何破解 CMOS 密码

CMOS 密码并不是万能的，破解它的方法也是招招在手。

1.Debug 法

如果在 CMOS 设置中设置的密码检测不是“System”，而是“Setup”（进入系统之前总是要密码），那么就可以进入系统，然后利用 DEBUG（DOS 自带的一个程序，Windows 根目录下面有的）向端口 70h 和 71h 发送一个数据，可以清除口令设置。

破解步骤如下：

步骤 1 启动系统，在 Starting Windows 9x……的画面时，立即按下【F8】键，然后选择进入纯 DOS 状态；

步骤 2 然后在根目录下面输入以下内容：

```
C:\>DEBUG
—O 70 10
—O 71 01
—Q
```

步骤 3 重新启动计算机，这时发现 CMOS 校验错，需要重新设置，这时候用户可以不用输入密码就可以进入系统了。

其实我们也可以将上述操作用 DEBUG 写成一个程序放在一个文件（如 DELCMOS.COM）中，以后运行 DELCMOS.COM 就能清除口令设置了。具体操作如下：

```
C:\>DEBUG
```

```
—A 100
XXXX:0100 MOV DX,70
XXXX:0103 MOV AL,10
XXXX:0105 OUT DX,AL
XXXX:0106 MOV DX,71
XXXX:0109 MOV AL,01
XXXX:010B OUT DX,AL
XXXX:010C
—R CX
CX 0000
: 0C
—N DELCMOS.COM
—W
Writing 000C bytes
—Q
```

如果他在CMOS中设置的是“System”,这样你就无法进入系统了,不过在他使用电脑时,只要他一离开电脑,哪怕只有两分钟,我想你就足够了。进入【开始】|【程序】|【MS-DOS方式】,然后输入上面命令的内容即可清除了。

2.“万能”密码法

现在主板上用的BIOS大多数是Award、AMI等厂商的,而他们一般留有通用密码。

(1) AMI BIOS“万能”密码一般为:

可以试一试这几个:AMI,BIOS,PASSWORD,HEWITT RAND,AMI? SW,AMI_SW,LKWPETER,A.M.I。

(2) AWARD BIOS“万能”密码为:

可以试一试这几个:AWARD_SW,j262,HLT,SER,SKY_FOX,BIOSTAR,ALFAROME,lkwpeter,j256,AWARD? SW,LKWPPETER,Syxz,aLLy,589589,589721,awkard(注意大小写)。

其实,“万能”密码就是BIOS程序上留的Back Door,通常厂商用来方便自己的工程人员使用,所以“万能”密码无论你设什么密码,都能进入BIOS重新设定。不过这些密码对于以前的486主板可说是攻无不克、战无不胜,对于现在的主板可能不太实用了,因为人人都知道了,“密码”也就不复存在了。不过我们还是可以找出它们的“万能”密码的,那就请BiosPwds帮忙吧。大家可以先去华军软件园将其下载,下载地址为http://www.newhua.com/BiosPwds.htm。下载后,解压得到一个EXE可执行文件BiosPwds.exe,然后运行它,进入BiosPwds的主界面,这时只需按下主界面上的【Get Passwords】按钮,等候约2~3秒即会将BIOS各项信息显示于BiosPwds的界面上,包括:BIOS版本、BIOS日期、使用密码等(如图1.1.4所示),这时你看到的在【Supervisor password】后面的文字框显示的内容为“AJAXHXZW”,这说明该主板超级用户的通用密码就是AJAXHXZW,用它试试吧,一定让你轻松搞定。

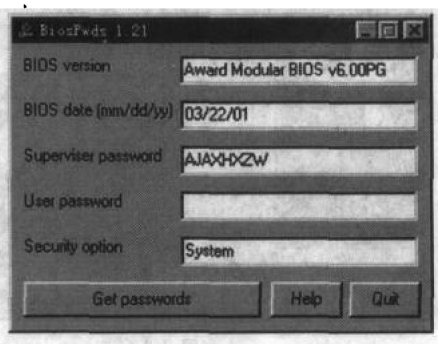


图 1.1.4

3.CMOS放电法

其实以上解破方法都是进入电脑系统后,才可能破解的。如果无法进入系统,即设置为“System”,那我们应该怎么办呢?

(1)拆下电池法:打开机箱,找到主板上的电池,将其与主板的连接断开(就是取下电池),此时CMOS将因断电而失去内部储存的一切信息。再将电池接通,合上机箱开机,由于CMOS已是一片空白,它将不再要求你输入密码,此时进入BIOS设置程序,选择主菜单中的【Load Setup Default】(装入设置程序缺省值)即可。

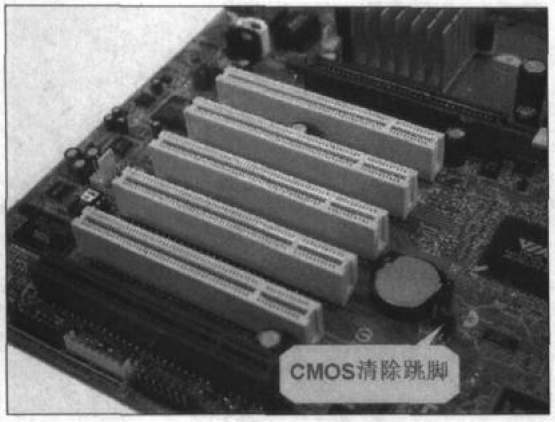


图 1.1.5

(2)跳线短接法:目前大多数主板都带有 CMOS 清除跳脚(JBATI)。一般情况下它的位置就处于主板电池的旁边(如图 1.1.5 所示),跳线开关一般为三脚。默认状态,是将跳线器放在 1、2 两脚上,这时可以储存 CMOS 中的信息,如果我们要清除 CMOS 中的信息(当然是密码了),只要将电脑电源断开,然后将 1、2 两脚上的跳接器取下,安插在 2、3 两脚上即可进入放电了,然后再将跳线器插回到 1、2 两脚上即可。

【说明】

请勿在电脑开机时(即未断开电源)进行跳线,这样会造成主板的烧毁。

1.2 设置 Windows 登录口令

如果 CMOS 密码被攻破了,那加固你的第二把"锁"吧——设置操作系统登录口令。

1.2.1 设置 Windows 98 登录口令

1.添加用户名

步骤 1 在桌面,单击【开始】|【设置】|【控制面板】,打开【控制面板】窗口。

步骤 2 双击其中的【用户】图标,打开【允许多用户设置】对话框。

步骤 3 单击【下一步】按钮,出现【添加用户】对话框在【用户名】后面的文本框中输入用户名(如图 1.1.6 所示)。

步骤 4 单击【下一步】按钮,进入【个性化项目设置】对话框,可以进行一些个性化的设置如图(1.1.7 所示)。

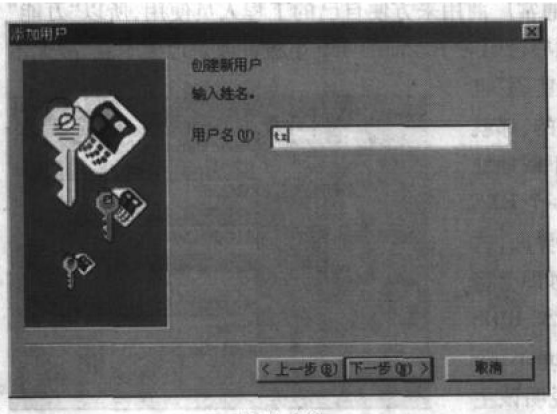


图 1.1.6

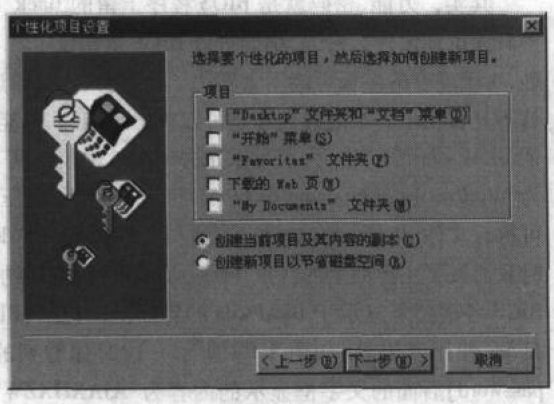


图 1.1.7

步骤 5 设置完成后,单击【下一步】按钮,即可以完成用户名的添加。

2.设置密码

用户名已经设置好了,不过这时的用户名并不安全,因为还没有密码保护,下面为用户名设置相应的密码。

步骤 1 双击【控制面板】中的【用户】图标,弹出【用户设置】对话框(如图 1.1.8 所示)。

步骤 2 选择【用户列表】中的用户名,即刚刚设置的"tz",下面的【设置密码】由灰色变为黑色,表示可以使用了,单击【设置密码】按钮。

步骤 3 弹出【更改 Windows 密码】对话框,在对话框中有三个文本框,即:旧密码、新密码、确认新密码。由于没有设

置过密码,在旧密码的文本框中不必输入字符,只要在【新密码】与【确认新密码】这两个文本框中输入相应的密码即可,输入结束后,单击【确定】按钮(如图 1.1.9 所示)。

重新启动 Windows 98,系统会要求输入用户名和密码才能进入。

图 1.1.8

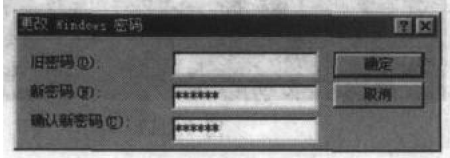


图 1.1.9

1.2.2 防止匿名登录

经过上面的设置,现在如果要进入"tz"这个用户的个性设置状态,没有密码是不行的,可是如果只是要使用这台电脑,没有这个密码也没关系。只要在出现登录窗口时,按【Esc】键或是单击窗口中的【取消】按钮,即可匿名登录了。那么如果防止匿名用户登录呢?请参照以下步骤:

步骤 1 选择【开始】|【运行】,在输入文本框中输入"Regedit",打开注册表编辑器。

步骤 2 找到"HKEY_LOCAL_MACHINE\Network\Logon"主键(如果没有,就创建一个)。

步骤 3 在右窗口中新建一个 DWORD 值,命名为 MustBeValidated,键值为 1。

步骤 4 退出注册表编辑器,重新启动计算机,如果不输入相应用户名的密码,只是单击【取消】按钮或是只按【ESC】键,不可以进入。

【说明】

如果真的把用户名和密码给忘了,自己都进不去了,可以进入电脑的安全模式,将【MustBeValidated】的值由刚才"1"改为"0",即可恢复【取消】按钮的功能。

1.2.3 破解 Windows 98 登录口令

遗忘 Windows 的启动密码虽然不会影响系统的启动,但它会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。一般情况下,破解 Windows 98 登录口令方法有二:

方法一:删除 Windows 安装目录下的 *.PWL 密码文件(或者把 *.pwl 改名)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。

方法二:选择打开【开始】|【运行】,在输入文本框中输入 "regedit", 打开注册表编辑器, 打开注册表数据库 "HKEY_LOCAL_MAHINE\Network\Logon" 分支下的 "UserProfiles",将其值修改为"0"(如图 1.1.10 所示),然后重新启动 Windows 也可达到同样的目的。

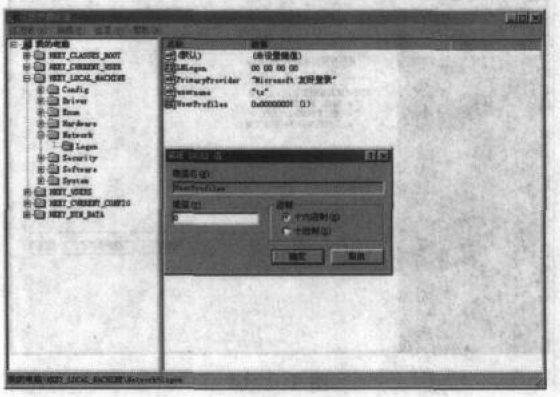


图 1.1.10

1.2.4 设置 Windows XP 新账户

由于 Windows 98 登录密码的脆弱性, 微软在 Windows 2000 与 Windows XP 中对 Windows 自身的加密功能大大加强了。由于这两个操作系统的新账户的添加方法差不多,下面以 Windows XP 为例,讲一讲在 Windows XP 操作系统下如何创建一个新账户:

步骤 1 单击【开始】|【控制面板】,在【控制面板】窗口中单击【用户账户】图标,打开【用户账户】对话框(如图 1.1.11 所示)。

步骤 2 单击【创建一个新账户】,进入【创建新账户】向导,提示输入账户名,例如输入用户名"byyhq"(如图 1.1.12 所示)。

图 1.1.11

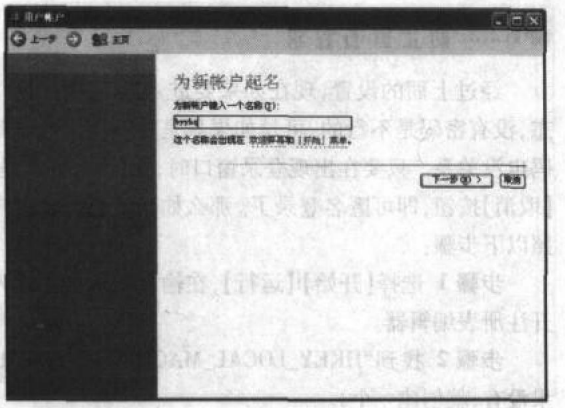


图 1.1.12

步骤 3 单击【下一步】按钮,按照提示选择自己的账户类型为"计算机管理员"或者是"受限用户"(如图 1.1.13 所示)。在用户权限方面,计算机管理员有权限安装程序和设备、统一更改系统、浏览并打开所有非私人文件、创建并删除用户账户、更改自己的账户名、账户类型和账户图标、创建、删除或更改自己的密码;受限用户只能更改自己的账户图标、创建、更改和删除自己的密码。

步骤 4 单击【创建账户】按钮,向导自动完成账户创建工作,返回【用户账户】窗口中,可以看到账户中多了一个名称为"byyhq"的用户账户。

新创建的账户是没有密码的,如要添加密码,可以这样进行操作:

单击新建立的账户名"byyhq"或账户图标,在打开的"byyhq"账户管理对话框中单击【创建密码】,进入【用户账户】窗口设置密码(如图 1.1.14 所示),输入密码并确认后,系统就会给用户"byyhq"创建密码。

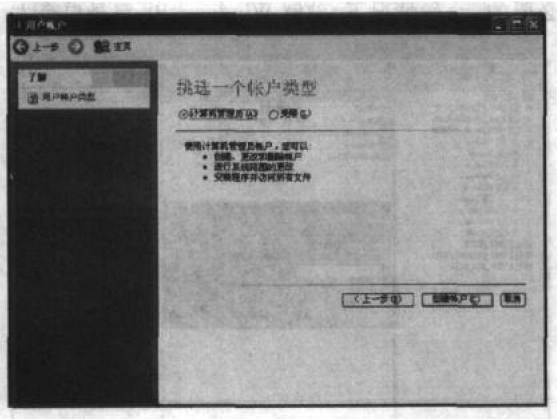


图 1.1.13

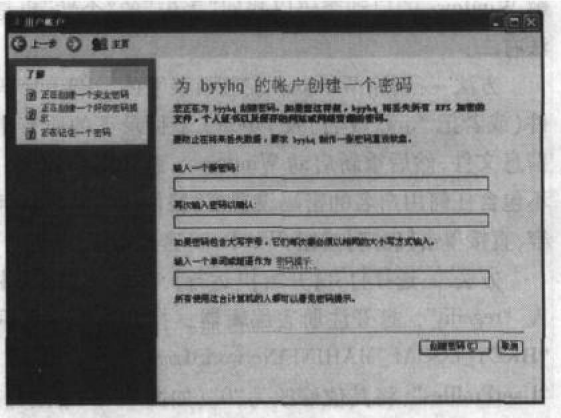


图 1.1.14

1.2.5 破解 Windows 2000 的登录密码

我们知道 Windows 2000 的登录密码,要比起过去的 Windows 操作系统的登录密码安全得多,一般情况下是无法破解的,如果你不一小心将密码给忘了,那你只有接受悲惨的事实——重新安装了。不过,世上无难事,下面我们就利用 Windows 2000 中的输入法的一个小小漏洞,就可以破解 Windows 2000 登录密码了。

步骤 1 Windows 2000 启动之后,按照屏幕提示按下【ALT】+【CTRL】+【DEL】组合键进行登录,在登录界面将

光标移至用户名输入框，按键盘上的【Ctrl】+【Shift】组合键进行输入法的切换，屏幕上出现输入法状态条，在出现的【全拼】输入法中将鼠标移至输入法状态条单击鼠标右键，出现的选单中选择【帮助】，然后继续选择【输入法入门】，在窗口顶部会出现几个按钮，奥妙就在【选项按钮】上。

步骤 2 如果系统未安装 Windows 2000 ServicePack1 或 IE 5.5，那么现在就可以在【操作指南】窗口上边的标题栏单击右键，选择【跳至 URL】，此时会弹出 Windows 2000 的系统安装路径并要求输入路径，输入"C:\WinNT\system32"(假设 Windows 2000 安装在 C: \WinNT 下)，单击【确定】按钮，我们就成功地绕过了身份验证进入系统的 system32 目录。

步骤 3 在 system32 目录下找到"net.exe"，用鼠标右键单击并选择【创建快捷方式】，右键单击该快捷方式，在【属性】|【快捷方式】|【目标】里输入"C:\winnt\system32\net.exe user backup ABC/ADD"，然后单击【确定】按钮。

【说明】

这一步骤的目的在于用 Net.exe 创建一个 backup 用户，密码为大写的"ABC"，双击该快捷方式完成用户的添加。

步骤 4 现在把 backup 用户添加到 Administrators (管理员组中)，同样把 Net.exe 的快捷方式目标修改为"C:\winnt\system32\net.exe LOCALGROUP Administrators backup/ADD"，双击执行。

步骤 5 最后我们用 backup 用户登录，并修改你原先用户的密码，最后当然不要忘了删除 backup 用户。

1.2.6 如何在 Windows XP 中创建修复密码的启动盘

Windows XP 的安全性能提高了不少，你可以通过对自己的账户设置密码来保护自己的隐私，但是如果您自己忘记了这个密码那该怎么办呢？大家不要紧张，我们可以创建一个修复密码启动盘，这样在忘记密码的时候便可以通过这张软盘来启动电脑了。具体操作步骤如下：

步骤 1 在【控制面板】|【用户账户】选项，在弹出的窗口中选择自己的账户便会进入自己账户的控制界面，单击左上方的【阻止一个已忘记的密码】选项打开【忘记密码向导】。

步骤 2 将一张格式化过的空白磁盘插入到软驱中，然后跟随【忘记密码向导】单击【下一步】按钮，会让你输入这个账户现在的密码(如图 1.1.15 所示)，输入后稍稍等待几秒钟便可以创建完成密码启动盘。

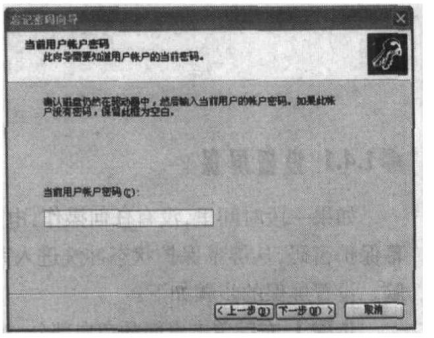


图 1.1.15

【说明】

这个启动盘一定要放好，如果让别人得到这张软盘便也可以轻而易举地用您的账户进行登录了。

1.3 设置电源管理密码

1.3.1 设置电源管理密码

Windows 的电源管理功能也可以设置密码，设置此功能后，系统在从节能状态返回时就会要求输入密码，从而在一定程度上实现保护系统的目的。电源管理一般情况在【控制面板】里面，但由于操作系统不同，这个功能有着不同的名称，例如 Windows 98 里面称为"电源管理"，Windows Me、Windows 2000 和 Windows XP 均称为"电源选项"。下面我们就以 Windows 98 为例，看一看如何设置电源管理密码：

步骤 1 在桌面，单击【开始】按钮，选择【设置】|【控制面板】，打开【控制面板】窗口。

步骤 2 双击其中的【电源管理】图标，打开【电源管理属性】对话框(如图 1.1.16 所示)。