大众网络报
POPUNET WEEK

密码终极攻防战II

黑客首选

得到他（她）的「秘密」 犹如囊中取物

PASSWORD ATTACK&KEEP AWAY

送

Word Excel OE……密码恢复工具 磁盘加密器 密码查看器
震荡波 冲击波 MSN射手 QQ……病毒专杀工具 金山毒霸 诺顿2004 瑞星2004下载版 木马克星最新版

Windows Linux系统密码轻松破解
传奇2 传奇3 天堂II……热门游戏密码装备手到擒来
QQ2004 MSN6.2 ICQ……密码任意窥探
论坛 在线电影 收费网站账号密码全线突破
BIOS的密码查看 清除 修改 随心所欲
OE FlashFXP 还原精灵……数十种软件密码简单解密
Word RAR WPS……文件密码100%成功破解

山东电子音像出版社出版

密码终极攻防战II

新增五倍全新内容　囊括所有破解　加密攻防精华

毋须系统学习　也能成为破解高手

超过350种解密详尽操作实例

得到他（她）的「秘密」　犹如囊中取物

山东电子音像出版社出版

内容简介

QQ密码被盗、游戏账号丢失、系统密码、邮箱密码神秘失踪……令人愤恨的事件频繁出现。为了让网民能保卫自己的密码，了解黑客攻击、破译手法就成了当务之急。本书续《密码终极攻防战》累计畅销10万册之后，再次新增五倍全新内容，囊括最新账号密码攻防精华。

本书采用技巧大搜捕式的风格，从Windows系统密码破解；《传奇2》、《传奇3》、《天堂II》等热门游戏密码装备手到擒来；QQ2004、MSN6.2 、ICQ……密码任意窥探到论坛在线电影收费网站账号密码全线突破；BIOS的密码查看、清除、修改，随心所欲；OE、FlashFXP、还原精灵等数十种软件密码、文件密码100%成功破解……超过350种账号密码攻防实例，为普通电脑用户定做的密码安全图书，最浅显易懂的实例讲解，只要会操作电脑，就能成为解密高手。

注：切勿利用本书介绍的知识进行恶意攻击，违者将受到法律制裁。

光盘运行环境

CPU主频	PII 500以上
分辨率	800×600像素
内存	32M以上
显存	8M
光驱	8倍速以上
操作系统	Windows 9X/2000/XP

密码终极攻防战II

策　　划：大众网络报社

制　　作：山东翔宇软件开发中心

责任编辑：刁　戈

特邀编辑：杨　波　孙淑培

出版发行：山东电子音像出版社

装帧设计：聂　培　匡小波

定　　价：19.8元（本手册随盘赠送）

目录

密码终极攻防战II

第一章 系统密码完全破解

第二章 文件密码设置与恢复

目录

密码终极攻防战II

第三章 常见工具软件密码破解

此为试读，需要完整PDF请访问：www.ertongbook.com

第四章 网络游戏盗号与反盗号

目录

第五章 聊天工具密码破解与防范

目录

密码终极攻防战II

第一章
系统密码完全破解

此为试读,需要完整PDF请访问: www.ertongbook.com

第一章 系统密码完全破解

防止他人自由登录你的电脑就必须设置系统密码，但是，不同系统，密码安全性不同，不要以为设置了系统密码，就可以高枕无忧了。特别是对于喜欢玩游戏的朋友选择的Win98系统，尤其要小心，因为它的密码安全性最差，而选择安全性比较高的WinXP系统，也不能掉以轻心……

1.1 Win98密码

对于Win98系列的操作系统来讲（也包括WinMe），它的密码安全较差，很容易破解。与其说是用于“系统安全”，还不如说成是用来“做秀”，这一点从下面Win98密码轻松被破解就可以看出来。

1.1.1 Win98登录密码设置与破除

1. 创建Win98的系统登录密码

在安装完Win98系列产品之后，第一次进入操作系统时都会有一个对话框，要求你输入密码，并且提示你如果不输入密码直接进入，那么下次这个对话框将不再出现。这时，你可以输入你的密码，用作登录Windows。如是这时你没有输入密码，而以后你又想使用这个功能，那么只能从控制面板里进行更改了，具体步骤如下：

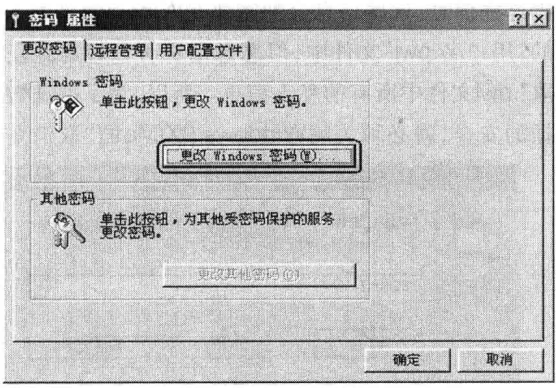

图1-1

步骤1 打开“控制面板”→“密码”（如图1-1）；

步骤2 单击“更改Windows密码”根据提示输入密码，然后再输入新密码并进行确认，这样下次你登录Windows时系统就会要求你输入密码了。

2. 解除Win98 密码

一般Windows用户的登录密码都记录在*.pwl的密码文件里，因此，只要能破解*.pwl文件，就可以破解登录密码，加密后的Win98密码清单即pwl文件可以在系统的根目录下找到（通常是C:\Windows）。这些文件按该系统上每个用户的初始定制文件命名。因此在驱动器A的软盘上执行如下命令可以获得大部分pwl文件：

copy c:\Windows*.pwl a:\

提示:PWL文件实际上只是一个用于访问以下网络资源的一个高速缓存的密码清单：

(1) 由共享级安全机制保护的资源；

(2)编写用到密码高速缓存API的应用程序，例如DUN(Dial_up NetWorking)；

(3) 没有加入任何NT域的WinNT计算机；

(4)不是Primary Network logon的WinNT的登录密码。

3. 破解PWL文件

破解PWL密码文件最快捷的方法是直接删出

所有Windows下的＊.pwl文件。一般来说＊.pwl放在Windows所在的目录中。因此破解文件方法非常简单，具体步骤如下：

步骤1 重新启动计算机，在进入Windows之间，按F8键通过“command prompt only”项进入DOS状态。

步骤2 在DOS下进入Windows目录，一般为C:\Windows。

步骤3 在命令符下，敲入命令Dir＊.pwl，这样在屏幕上将查出所有用户的pwl文件(如图1-2)。

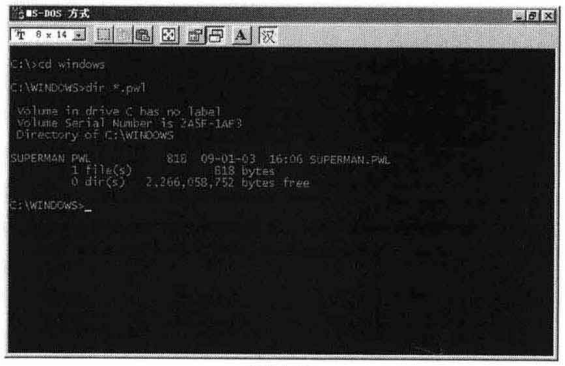

图1-2

步骤4 使用Del ＊.pwl删除所有的PWL文件。也可以DelX ＊.del删出单个PWL文件。

提示：X.pwl指某个PWL文件。在删出PWL文件之前，最好备份一下以防万一出错好即时恢复。

步骤5 重新启动计算机，进入Windows的登录窗口，选择某个用户名，随便输入密码，就可以进入Windows。

提示：注意哦，这里的用户名就是前面用Dir在DOS下查找到的文件名。虽然破解了密码，但我们

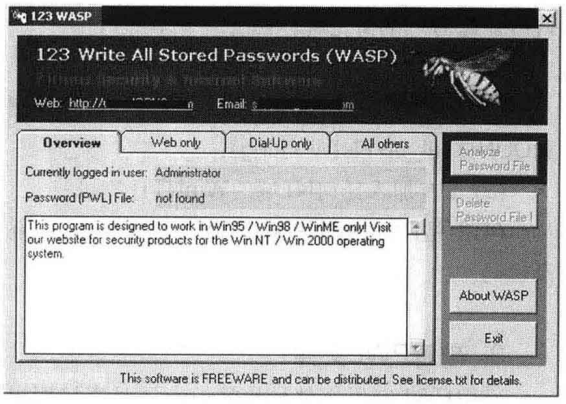

图1-3

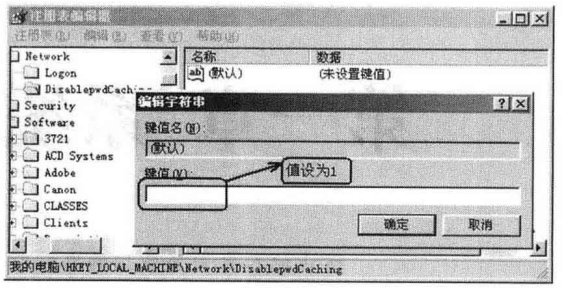

图1-4

没得到＊.pwl密码呀？怎么办呢？其实很简单，我们把＊.pwl文件Copy到软盘，拿这张盘到其他系统上安装并运行如图1-3所示的“PWL密码察看器”即可。

4. 保护措施

既然PWL文件这么容易被击破，那么我们有什么办法能防范这种攻击呢？针对PWL密码高速缓存文件的特点，Win9X的系统策略编辑器(System Policy Editor)可以用来禁止密码高速缓存，具体方法是把以下的DWORD类型注册表键创建/设置成1(如图1-4)：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVesionj\Policies\Network\DisablepwdCaching=1。

1.1.2 防止Win98匿名登录

登录Windows 9X/Me系统时，直接按下“取消”按钮，就可以在不输入密码的情况下登录了。为了保护用户的某些私人信息(上网账号，电子邮件等等)，当不登录为用户时，使用电脑的人将不能获得这些信息。这些信息会加密放在Windows目录下的“用户名.pwl”文件中，但恶意用户可以轻易地获取*.pwl文件中所有的私人信息。所以，为了保证数据的安全，就必须关闭Windows 9X/Me的“取消登

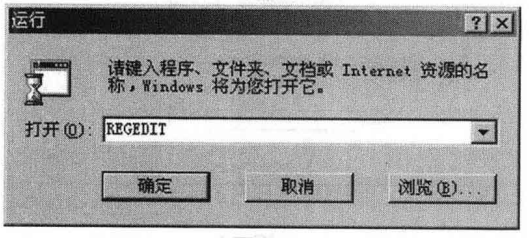

图1-5

录”功能。方法如下：

1. 执行“开始/运行”命令，在弹出的对话框中输入“REGEDIT”，按下“确定”按钮（如图1-5），打开注册表编辑器。

2. 选择注册表编辑器的HKEY_LOCAL _MACHINE\Network\Logon主键，执行“编辑/新建

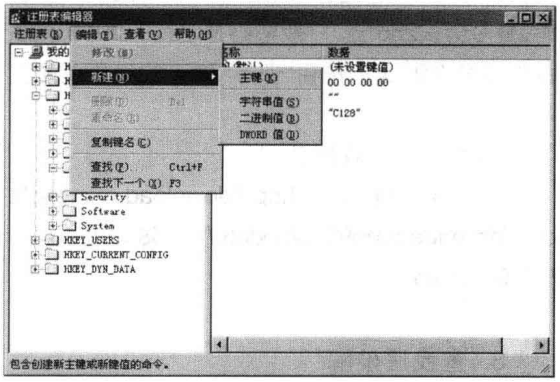

图1-6

/DWROD值”命令（如图1-6），在出现的文本框中输入“MustBeValidated”，按下“确定”按钮。双击该新建DWROD值，在弹出的“编辑DWROD值”对话框的“键值”栏中，输入“1”，点击“确定”按钮，关闭注册表编辑器（如图1-7）。

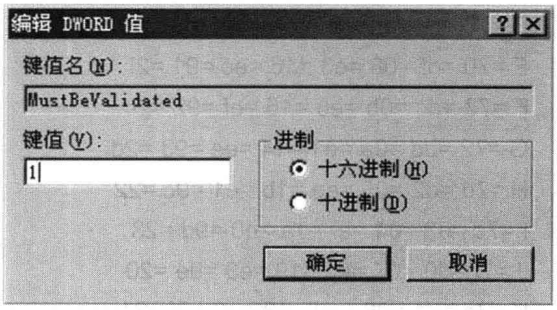

图1-7

3. 执行“开始/设置/控制面板”命令，在弹出的“控制面板”对话框中，双击“网络”图标，打开“网络”对话框。在“配置”标签的“主网络登录”下拉菜单中，选择“Microsoft网络用户”，按下“确定”按钮（如图1-8）。

4. 重启电脑后，按“取消”按钮（如图1-9），就无法登录到系统了（如图1-10）。

1.1.3 Win98共享目录密码的破解

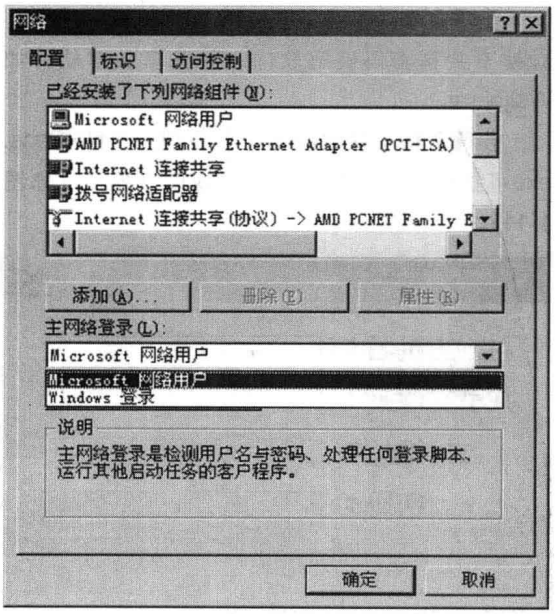

图1-8

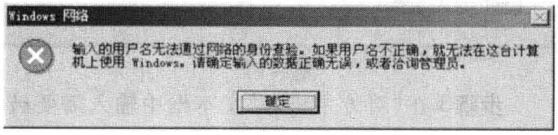

图1-9

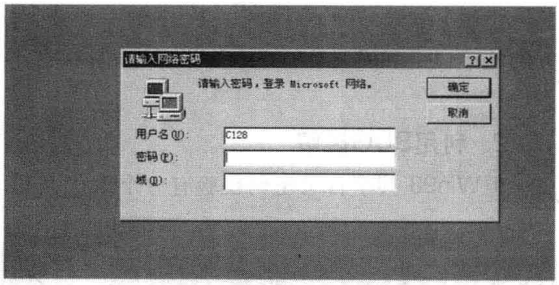

图1-10

在Win98系统中，有时我们为了能够实现某些资源的共用，往往设置一个共享目录，用户通过“网上邻居”可以实现对资源的访问。虽然共享给共享设置了密码，但由于Win98密码的脆弱性，用户很容易就能破解。由于Win9x的共享有漏洞，所以密码的安全性就岌岌可危，只要稍懂点密码知识的人都可以轻松取得你的密码。不信，我们就来看看下面几种获得密码的方法。

1.软件破解

步骤1 通过搜索引擎www.google.com从网上看搜索共享密码破解软件，如共享破解软件如Wsljpj.rar。

步骤2 将文件解压缩，会得到一个NetPass.exe可执行文件。运行它，出现以下界面（如图1-11）。

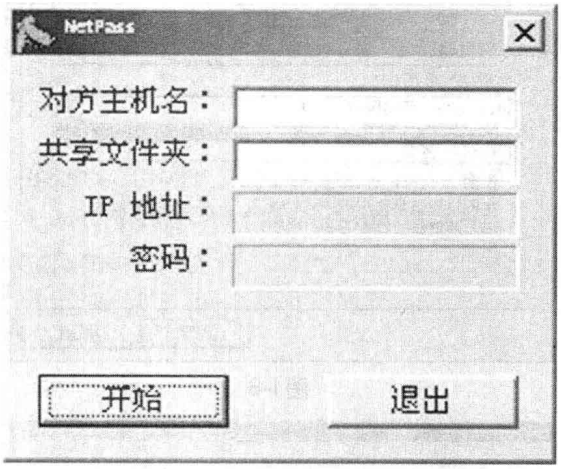

图1-11

步骤3 在“对方主机名”文本框中输入需要破解共享口令的主机名，在“共享文件夹中”输入需要破解共享口令的文件夹。

步骤4 单击“开始”，刷的一下，不到一秒钟，对方的共享口令和IP地址便显示出来了（如图1-12）。

2. 利用BUG破解

但Win98 共享目录密码校验有一个Bug，可以让其只校验密码第一个字节。你只要从网上下载Vredir.vxd，然后将Vredir.vxd文件复制到Windows\System目录并覆盖原文件，重新启动电脑。现在在进入有密码共享目录弹出提示输入密码窗口时不用再敲密码，只要按住回车键不放，直到进入此目录。如果弹出“密码不对”提示对话框，只要按住回车键不放，选择“确定”，然后测试下一个密码，最多尝试256次。一般密码是字线0×20到0×80，也就是最多96次。按住“回车”键不放很快就能进入。

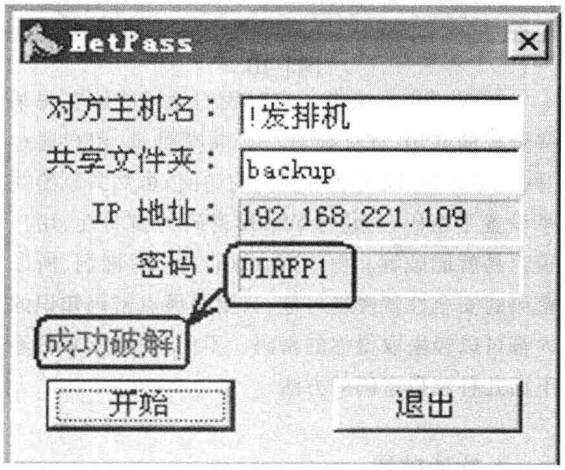

图1-12

解决方法：下载补丁

下载地址：http://download.microsoft.com/download/win98se/update/11958/w98/en-us/273991usa5.exe

3. 查找法破解

利用破解密码之前要大家先了解一下下边这些对应值表，也就是Win98 共享密码对照表。密码对照表：

A =74 =db =0c =e7=12 =e8 =95 =2b
B =77 =d8 =0f =e4 =11 =eb =96 =28
C =76 =d9 =0e =e5 =10 =ea =97 =29
D =71 =de =09 =e2 =17 =ed =90 =2e
E =70 =df =08 =e3 =16 =ec =91 =2f
F =73 =dc =0b =e0 =15 =ef =92 =2c
G =72 =dd =0a =e1 =14 =ee =93 =2d
H =7d =d2 =05 =ee =1b =e1 =9c =22
I =7c =d3 =04 =ef =1a =e0 =9d =23
J =7f =d0 =07 =ec =19 =e3 =9e =20
K =7e =d1 =06 =ed =18 =e2 =9f =21
L =79 =d6 =01 =ea =1f =e5 =98 =26
M =78 =d7 =00 =eb =1e =e4 =99 =27
N =7b =d4 =03 =e8 =1d =e7 =9a =24
O =7a =d5 =02 =e9 =1c =e6 =9b =25
P =65 =ca =1d =f6 =03 =f9 =84 =3a
Q =64 =cb =1c =f7 =02 =f8 =85 =3b
R =67 =c8 =1f =f4 =01 =fb =86 =38
S =66 =c9 =1e =f5 =00 =fa =87 =39
T =61 =ce =19 =f2 =07 =fd =80 =3e

U =60 =cf =18 =f3 =06 =fc =81 =3f
V =63 =cc =1b =f0 =05 =ff =82 =3c
W =62 =cd =1a =f1 =04 =fe =83 =3d
X =6d =c2 =15 =fe =0b =f1 =8c =32
Y =6c =c3 =14 =ff =0a =f0 =8d =33
Z =6f =c0 =17 =fc =09 =f3 =8e =30
space =15 =ba =6d =86 =73 =89 =f4 =4a
1 =04 =ab =7c =97 =62 =98 =e5 =5b
2 =07 =a8 =7f =94 =61 =9b =e6 =58
3 =06 =a9 =7e =95 =60 =9a =e7 =59
4 =01 =ae =79 =92 =67 =9d =e0 =5e
5 =00 =af =78 =93 =66 =9c =e1 =5f
6 =03 =ac =7b =90 =65 =9f =e2 =5c
7 =02 =ad =7a =91 =64 =9e =e3 =5d
8 =0d =a2 =75 =9e =6b =91 =ec =52
9 =0c =a3 =74 =9f =6a =90 =ed =53
0 =05 =aa =7d =96 =63 =99 =e4 =5a
~ =4b =e4 =33 =d8 =2d =d7 =aa =14
` =55 =fa =2d =c6 =33 =c9 =b4 =0a
! =14 =bb =6c =87 =72 =88 =f5 =4b
@ =75 =da =0d =e6 =13 =e9 =94 =2a
# =16 =b9 =6e =85 =70 =8a =f7 =49
$ =11 =be =69 =82 =77 =8d =f0 =4e
% =10 =bf =68 =83 =76 =8c =f1 =4f
^ =6b =c4 =13 =f8 =0d =f7 =8a =34
& =13 =bc =6b =80 =75 =8f =f2 =4c
* =1f =b0 =67 =8c =79 =83 =fe =40
(=1d =b2 =65 =8e =7b =81 =fc =42
) =1c =b3 =64 =8f =7a =80 =fd =43
- =18 =b7 =60 =8b =7e =84 =f9 =47
_ =6a =c5 =12 =f9 =0c =f6 =8b =35
+ =1e =b1 =66 =8d =78 =82 =ff =41
= =08 =a7 =70 =9b =6e =94 =e9 =57
[=6e =c1 =16 =fd =08 =f2 =8f =31
] =68 =c7 =10 =fb =0e =f4 =89 =37
{ =4e =e1 =36 =dd =28 =d2 =af =11
} =48 =e7 =30 =db =2e =d4 =a9 =17
; =0e =a1 =76 =9d =68 =92 =ef =51
: =0f =a0 =77 =9c =69 =93 =ee =50
' =12 =bd =6a =81 =74 =8e =f3 =4d
" =17 =b8 =6f =84 =71 =8b =f6 =48
, =19 =b6 =61 =8a =7f =85 =f8 =46
< =09 =a6 =71 =9a =6f =95 =e8 =56
. =1b =b4 =63 =88 =7d =87 =fa =44
> =0b =a4 =73 =98 =6d =97 =ea =54
? =0a =a5 =72 =99 =6c =96 =eb =55
/ =1a =b5 =62 =89 =7c =86 =fb =45
\ =69 =c6 =11 =fa =0f =f5 =88 =36
| =49 =e6 =31 =da =2f =d5 =a8 =16

然后展开注册表到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan下，看看其下键值中的参数Parm1enc，根据本地机器的共享数而定，假设有一个Tmep文件夹设置了共享的话，在LanMan键下应该也有一个相应Temp主键，我们要看的是MP3主键中的Parm1enc键的键值，将该键的键值进行拆解。例如:假设你看到parmienc的键值为“74 d8 0e”将其拆解成“74 d8 0e”然后到上面的密码表中查对就可以共享密码为ABC。

提示: 前提是你必须在此机器上操作，或者你远程可以获得本机的注册表备份文件也是可以的。当然，如果你在本地机器要对密码操作的话，直接更改就可以了，没有这么麻烦，这里只是提供一个另类的得到密码的方法而已。

1.1.4 Win98屏保密码的破解

如果一不小心忘了屏幕保护程序的密码，怎么办？直接关机吗？那可太野蛮了，而且，万一你的工作没有保存，岂不是前功尽弃！现在，你只要采用下面几个巧妙的方法，你的难题就迎刃而解了！

方法一 重新启动

在遗忘密码屏幕保护密之后只需使用“复位”键强行启动电脑，然后右击桌面空白处并从弹出的快捷菜单中执行“属性”命令，打开“显示属性”设置框并单击“屏幕保护”选项卡，最后取消“密码保护”选项即可(取消该选项时无需确认密码)。

方法二 简单去除法

注册表中HKEY_CURRENT_USER\Control Panel\Desktop找到ScreenSaveUsePassword，如果有密码，它的值为1，改为0就没密码了。（其实相关于屏保的那个密码保护选项框是否选中）。

方法三 从原理入手

一般屏保的密码为8位，再多设也无意义，所以我们可以从原理入手破译密码。

注册表中HKEY_CURRENT_USER\Control Panel\desktop找到ScreenSaveUsePassword，鼠标双击它后出现“编辑二进制”窗口，在下面的键值中看最右边的字符，如图1-13所示密码为两行，具体看密码设为多少而有所不同。

假设注册表的密码为“12345”那里会是如图

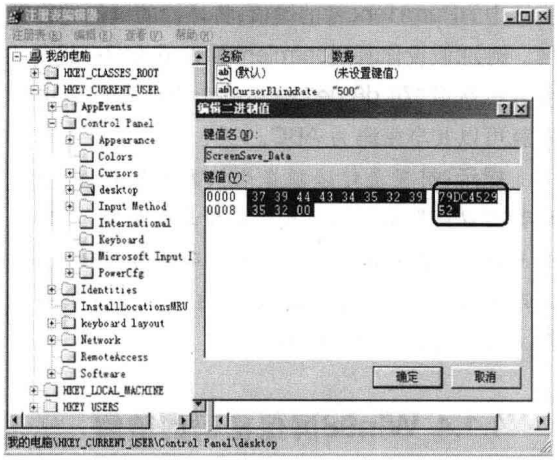

图1-13

1-13所示为：79，DC，45，29，52分别与78，DE，46，2D，57，59，91，2B进行异或（XOR），79 XOR 78→1，DC XOR DE →2，45 XOR 46 →3，29 XOR 2D→4，52 XOR 57→5，就可得到密码了，从密钥可知，密码最长只有8位。

方法四 硬件冲突法

如果用户的电脑在局域网内就可能利用另外一台机器作为解码机，将解码的IP地址改为用户的IP地址，利用硬件冲突的优先级高原理跳过屏幕保护。

步骤1 在解码机上找到“开始”→“设置”→“控制面板”，进入“控制面板”后，双击“网络”图标，进入“网络”对话框。

步骤2 选择“配置”选项卡，然后双击“TCP/IP”，进入“TCP/IP属性”→“IP地址”选项卡，将解码机的IP地址改为你的IP地址，完成后单击“确定”按钮。

步骤3 系统会提示你新的设置要重新启动计算机才能生效，确认并重新启动计算机。这样，当弹出“IP地址产生硬件冲突”的提示框时，只要在你的机器上点击“确定”，就直接进入操作系统的桌面了！

提示：整个解密的过程中，确保设有屏幕保护的计算机上还没有出现密码对话框，要求用户输入屏幕保护程序的密码，否则即使我们通过设置，造成了局域网中的硬件冲突，单击“硬件冲突”对话框中的确定按钮后，系统还会继续要求我们输入屏幕保护程序的密码。

此为试读，需要完整PDF请访问：www.ertongbook.com