
附多媒体教学光盘
易学易用系列
新手
学保护电脑隐私·防病毒·防黑客
神龙工作室 编著
技高一筹——监控与反监控
防范电脑病毒、小心木马及防范黑客
蛛丝马迹——三招两式查看谁动过我的电脑
保护文件隐私、个人上网隐私、电子邮件隐私和QQ聊天隐私
人民邮电出版社
POSTS & TELECOM PRESS

易学易用系列

新手

学保护电脑隐私·防病毒·防黑客

● 神龙工作室 编著

人民邮电出版社

图书在版编目（CIP）数据

新手学保护电脑隐私·防病毒·防黑客 / 神龙工作室编著. —北京：人民邮电出版社，2005.7
（易学易用系列）

ISBN 7-115-13520-7

Ⅰ. 新… Ⅱ. 神… Ⅲ. 电子计算机－安全技术－基本知识 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2005）第 064259 号

内 容 提 要

本书是指导初学者学习保护电脑隐私、防病毒、防黑客的入门书籍。书中详细地介绍了初学者必须掌握的基本知识、操作方法和使用步骤，并对初学者经常会遇到的问题进行了专家级的指导，以避免初学者在起步的过程中走弯路。全书共分 12 章，分别介绍操作系统隐私保护、文件隐私保护、保护个人上网绝对隐私、保护电子邮件隐私、保护 QQ 聊天隐私、保护局域网中的共享资源、防范电脑病毒、小心木马、防范黑客、网络安全屏障——防火墙、技高一筹——监控与反监控、三招两式查看谁动过我的电脑等内容。

本书充分地考虑了初学者的实际需要，对保护电脑隐私、防病毒、防黑客“一点都不懂”的读者，通过学习本书能够轻松地掌握保护电脑隐私、防病毒、防黑客的方法。同时，本书还附带有 1 张多媒体教学光盘。

本书适合初学保护电脑隐私、防病毒、防黑客的读者阅读，也可以作为保护电脑隐私、防病毒、防黑客短训班的培训教材。

易学易用系列

新手学保护电脑隐私·防病毒·防黑客

◆ 编　　著　神龙工作室
责任编辑　魏雪萍

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：16.5　　彩插：1
字数：395 千字　　2005 年 7 月第 1 版
印数：1－8 000 册　　2005 年 7 月北京第 1 次印刷

ISBN 7-115-13520-7/TP·4717

定价：29.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前言

保护电脑隐私、防病毒、防黑客很神秘吗?

不神秘!

学习保护电脑隐私、防病毒、防黑客难吗?

不难!

阅读本书能够保护电脑隐私、防病毒、防黑客吗?

能!

为什么要阅读本书

随着电脑的普及和互联网的高速发展，网络已不再是虚无缥缈的世界。你是否会对别人肆意地操控你的电脑而愤愤不平？你是否想知道他们在你的电脑上干了些什么？你是否正在为如何保护电脑里的个人隐私或商业机密而发愁？你是否为处在风头浪尖的网络环境中的系统而担忧……在本书中你都能找到所需要的答案。

阅读本书能学到什么

- 操作系统隐私保护、文件隐私保护、保护局域网中的共享资源
- 保护个人上网绝对隐私、保护电子邮件隐私、保护 QQ 聊天隐私
- 防范电脑病毒、小心木马、防范黑客
- 网络安全屏障——防火墙、技高一筹——监控与反监控
- 三招两式查看谁动过我的电脑
- 端口及对应服务一览表、常见木马程序与连接端口、Windows 中的常见进程解释

授之以鱼，不如授之以渔，本书在传授知识的同时，还侧重培养读者自学的能力。同时，**本书还附带有 1 张多媒体教学光盘，其中包括多个精彩实例操作步骤的多媒体演示**。

本书由神龙工作室编著，参与资料收集和整理工作的有姜永水、孙莉婧、宋真真、张晓、宫明文、宫涛、谭翠君、王亚男、李京龙、崔红霞、陈西杰、张东晓、张梦如、孙丽丽、邢宁霞、孙立新、朱乐平等。

由于时间仓促，书中难免有疏漏和不妥之处，恳请广大读者不吝批评指正。

E-mail 地址：zhiyin101@tom.com。

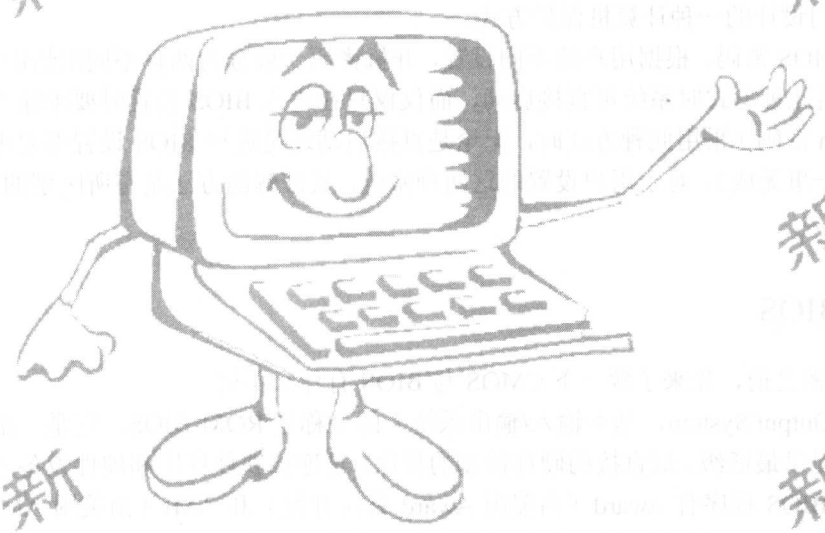
编者

2005 年 6 月

目录

第 1 章　操作系统隐私保护

在大多数黑客入侵的案例中，都是先对目标系统进行相关的探测和分析，在确定系统存在相应的缺陷、漏洞后再实施入侵操作，力求获取相应操作权利的口令或密码，从而顺利地控制整个电脑系统。从黑客入侵的案例中可以看出：系统密码的安全是非常重要的，针对系统密码的特殊性必须采用相应的应对策略。



本章首先简单地介绍一些密码的知识，然后讲解如何进行系统的设置从而有效地防止外人非法地进入到本地计算机中。

1.1 认识密码学

加密（Encryption）是使信息不可解读的过程，其目的是保护信息（尤其是在传输或储存期间）以避免未授权者查看或使用。加密依据的是一种算法并且至少应该有一种密钥，这样即使知道了算法而没有密钥也无法解读信息。

密码学（Cryptography）一词源于古希腊的 Crypto 和 Graphein，意思是密写。它是以认识密码变换的本质、研究密码保密与破译的基本规律为对象的学科。经典密码学主要包括两个既对立又统一的分支：密码编码学和密码分析学。研究密码变化的规律并用之于编制密码以保护秘密信息的科学称为密码编码学。研究密码变化的规律并用之于破译密码以获取信息情报的科学称为密码分析学，也称为密码破译学。前者是实现对信息保密的，后者是实现对信息反保密的。密码编码学和密码分析学相辅相成，共处于密码学的统一体中。

现代密码学除了包括密码编码学和密码破译学两个主要的学科之外，还包括近几年才形成的新分支——密码密钥学，它是以密码的核心部分——密钥作为研究对象的学科。密钥管理是一种规程，它包括密钥的产生、分配、存储、保护和销毁等环节，在保密系统中至关重要。

上述 3 个分支学科构成了密码学的主要学科体系。

1.2 CMOS 密码的设置和清除

说起计算机加密，不论是从“菜鸟”的角度还是从计算机应用高手的角度来说，CMOS 的加密都应该是最先被谈到的。因为每一台计算机要想使用的话都需要开机，所以 CMOS 的加密就是针对开机而专门设计的一种计算机保护方式。

开机密码也就是 CMOS 密码。根据用户的不同设置，开机密码一般分为两种不同的情况：一种是 Setup 密码（采用此种方式时系统可直接启动，而仅仅只在进入 BIOS 设置时要求输入密码），另一种是 System 密码（采用此种方式时，无论是直接启动还是进行 BIOS 设置都要求输入密码，没有密码将一事无成）。对于用户设置的这两种密码，其破解的方法是有所区别的，下面分别介绍。

1.2.1 CMOS 与 BIOS

在介绍 CMOS 的加密之前，先来了解一下 CMOS 与 BIOS 有什么不同。

BIOS（Basic Input/Output System，基本输入/输出系统）的全称是 ROM-BIOS，它是一组被固化在计算机中用以提供最低级、最直接的硬件控制的程序，是连接软件程序和硬件设备之间的枢纽。目前常见的 BIOS 程序有 Award（由美国 Award 公司开发）和 AMI（由美国 AMI 公司开发），其中以 Award BIOS 最为流行。考虑到用户在组装或使用计算机时可能需要对部分硬件的参数以及运行的方式进行调整，所以厂家在 BIOS 芯片中专门设置了一片 SRAM（静态存储器），并配备电池来保存这些可能经常需要更改的数据。由于 SRAM 是采用传统的 CMOS 半导体技术生产，所以人们也习惯地将其称为“CMOS”，而将 BIOS 设置称为“CMOS 设置”。事实上在 BIOS 设置主菜单上显示的就是“CMOS Setup”（CMOS 设置）。

可以说：为了使 BIOS 在各种特定的环境中能正常工作，用户对 BIOS 中的一些参数可以根据需求手动地进行调整和设置，调整的结果就存放在 CMOS 中，CMOS 的设置程序存放在 BIOS 芯片中。从某种意义上说，CMOS 就像运行在 BIOS 上的软件。

1.2.2　设置开机密码

CMOS 密码的设置根据用户的不同设置，一般分为两种不同类型的密码：一种是 Supervisor 密码（超级用户密码），另一种是 User 密码（普通用户密码）。它们之间的区别是：使用“超级用户密码”的用户不但可以正常地启动计算机、运行各类软件，而且还可以进入 BIOS 设置菜单对部分项目进行修改，包括直接修改或撤销由不同用户设置的“用户密码”；而使用“普通用户密码”的用户虽然可以正常地启动计算机、运行各类软件，也能够进入 BIOS 设置菜单进行浏览，但不能更改其中的设置。

所谓的 CMOS 加密，实际上就是在计算机对硬件完成自检后，强制中断对其他硬件设备的检测，而加入一个口令确认窗口，如果口令输入错误那么硬件的检测将被停止。若是连续 3 次都没有输入正确的口令，系统将被彻底锁死，此时惟一的解决办法就是重新启动计算机并再一次输入正确的口令。可见对于一般的用户而言，采用 CMOS 加密能够在启动计算机的时候就增加一道防护措施。

对“超级用户密码”和“普通用户密码”可以同时设置，并可设置成不同的密码，也可以只设置其中的一种。下面以 Award BIOS 为例讲解具体的设置步骤。

❶ 开机启动计算机，当 BIOS 检测完 CPU 和内存后在屏幕的下方显示“Press DEL to enter SETUP,ESC to Memory test”时按下【Del】键。

❷ 当屏幕显示 BIOS 设置主菜单后选择【Advanced BIOS Features】菜单项，然后按下【Enter】键进入【Advanced BIOS Features】设置菜单。

❸ 在【Advanced BIOS Features】设置菜单中选择【Security Option】菜单项，然后根据需要使用【PageUp】和【PageDown】键设置计算机使用密码的情况。如果设置为【System】，则计算机在启动和进入 BIOS 设置菜单时都需要输入密码；如果设置为【Setup】，则只需要在进入 BIOS 设置菜单时才需要输入密码。

❹ 按下【Esc】键返回主菜单，用光标移动“光条”选择【Set Supervisor Password】或【Set User Password】后按下【Enter】键。当弹出一个密码录入框（其中提示“Enter Password”）时在其中输入 3～8 位密码，此时输入的字符会以“*”代替。输入完成后按下【Enter】键会再次提示用户将刚才已输入的密码重新输入一遍以进行确认，再一次输入密码后提示框就会消失。

❺ 选择主菜单中的【Save＆Exit Setup】或者直接按【F10】键，当屏幕上出现“Save to CMOS and EXIT(Y/N)？N”提示后按【Y】键退出 BIOS 设置菜单，随后输入的密码就会生效。

❖ 不同厂家的 CMOS 设置可能不一样，用户应留意查看开机提示或主板说明书。

1.2.3　破解 CMOS 密码

用户通过设置 CMOS 密码的确可以达到保护自己计算机的目的，但是如果用户忘记了已

设置的 CMOS 密码，那么就会面对无法进入系统或无法进入 BIOS 设置程序的境地，这时该怎么办呢？本小节介绍几种常用的破解 CMOS 密码的方法：DEBUG 法、COPY 法、CMOS 放电法、跳线短接法以及改变硬件配置法。

1. DEBUG 法

对 CMOS 数据的访问是通过两个 I/O 端口来实现的。端口 70H 是一个字节的地址端口，用来设置 CMOS 中数据的地址；端口 71H 用来读写 70H 端口所设地址中的数据内容。可以用 DOS 的调试工具 DEBUG.COM 来清除 CMOS 密码，也就是用 DEBUG 向端口发送数据的 O 命令来向 70H 和 71H 端口发送特定的数据。

在 DOS 命令行中输入“Debug”，然后输入表 1-1 中 6 组数据中的一组后重启电脑，这样再进入 BIOS 时就不用输入密码了。

表 1-1　　Debug 命令的参数值

第 1 组数据	第 2 组数据	第 3 组数据	第 4 组数据	第 5 组数据	第 6 组数据
o 70 2F o 71 00 Q	o 70 2E o 71 00 Q	o 70 23 o 71 34 Q	o 70 16 o 71 16 Q	o 70 10 o 71 01 Q	o 70 10 o 71 FF Q

另外需要注意：每个组数值中的第一个字符均为英文字母“o”，70 和 71 是两个端口地址；后面为向这两个端口中写入的值，是英文和数字的组合，其中的“0”是阿拉伯数字零，用户要区分清楚，不要混淆。

2. COPY 法

在 DOS 状态下输入以下命令。

```
C:\>COPY CON CMOS.com（然后进入编辑状态）
```

用户可以用一只手按住【Alt】键，用另一只手在小键盘上敲击下列数字串，然后同时抬起双手，如此反复：179，55，136，216，230，112，176，32，230，113，254，195，128，251，64，117，241，195。

上面的操作完成后，按住【Ctrl】＋【Z】组合键即可得到程序（注意：上面的数字一定要全部录入，不能漏掉一个，否则编译出来的程序可能出错而导致产生其他的问题）。另外可以用 Type CMOS.com 查看内容，以后只要运行程序 CMOS.com 即可解开 CMOS 密码。然后重新启动，按【Del】键直接进入即可重新设置 CMOS。

需要注意的是：此方法只适用于那些不能进入BIOS设置的程序，但是能进入系统（System）密码设置的情况。对于那些连系统都无法进入的情况此方法显然不行，而需要通过别的方法进行清除。

3. CMOS 放电法

对于那些连系统都无法进入的情况，用户可以通过 CMOS 放电法来解决问题。

打开机箱，找到主板上的电池，将其与主板的连接断开（就是将电池取下），此时 CMOS 将因断电而失去存储于内部的一切信息。等过一段时间再将电池接通，合上机箱开机。由于 CMOS 此时已是“一片空白”，因此它不会要求用户输入密码。此时进入 BIOS 设置程序，然后选择主菜单中的【LOAD BIOS DEFAULT】（装入 BIOS 默认值）或者【LOAD SETUP

DEFAULT】（装入设置程序默认值）菜单项即可。前者可以最安全的方式启动计算机，后者则能使计算机发挥出较高的性能。

4. 跳线短接法

如果电池被焊死在主板上了，不能使用 CMOS 放电法，则可使用“跳线短接法”对 CMOS 放电（建议一般用户使用此法）。具体的操作步骤如下。

在电池的附近有一个跳线开关（可参考主板说明书），一般情况下，在跳线旁边有 RESET CMOS、CLEAN CMOS、CMOS CLOSE 或者 CMOS RAM RESET 等字样。跳线开关一般为 4 脚，有的在 1、2 两脚上有一个跳线器，此时将其拔下接到 2、4 脚上即可放电；有的所有的脚上都没有跳线器，此时将 2 脚短接即可放电。

另外应该注意：几乎所有的主板都有清除 CMOS 的跳线和相关的设置，但因生产厂商不同而各有所异。例如有的主板的 CMOS 清除设备并不是常见的跳线，而是很小的焊接锡点，需要用镊子小心地将其短路来清除 CMOS 密码。

5. 改变硬件配置法

使用放电法需要重新设置 CMOS 中的所有参数，很不方便。最后介绍一种简便易行的方法。关闭计算机，打开机箱，找到并拔下硬盘上连接的通讯接口线，然后接通电源启动就能绕过 CMOS 的口令进行设置了。这是因为当系统的硬件配置变化时，系统不需要输入口令就能够自动地进入 Setup 程序。当然也可以变动其他的硬件进行设置，如拔掉声卡等。

1.3 Windows 密码详解

设置密码是保护电脑数据的重要措施，它好比是电脑的“防盗锁”，用户只有使用所拥有的对应的“钥匙”才能够进入电脑，从而得到自己想要得到的数据。

1.3.1 用户和密码概述

保护计算机的安全是非常重要的。不仅要保护计算机本身的数据，还要保护网络上的数据。优秀的安全系统可以对试图访问计算机资源的人员进行身份识别，以防止特定的资源被未经许可的用户非法访问，并且能提供一种简单而高效的方法来设置和维护计算机的安全。Windows 系统为用户提供了一定级别的密码安全系统。

系统密码简单地说就是用户登录到操作系统时所用到密码，它为计算机提供了一种安全保护，可以使计算机免受非法用户侵入，从而达到保障计算机和机密数据安全的目的。

Windows 系统中【控制面板】里的“用户账户”允许将用户添加到计算机并将其添加到组中。在 Windows 2000 中，权限和用户权利通常授予组。通过将用户添加到组就可以将指派给该组的所有权限和用户权利授予这个用户。

例如，用户组里的成员可以执行完成其工作所需的大部分任务，如登录到计算机、创建文件和文件夹、运行程序以及保存文件的更改等，但却不能进行系统的设置和添加用户等操作，

而只有 Administrators 组的成员才可以将用户添加到组、更改用户的密码或者修改大多数的系统设置。

“用户账户”允许创建或更改本地用户账户（本地用户账户是指此计算机创建的账户）的密码，这对于创建新用户账户或者出现了用户忘记密码的情况时非常有用。如果用户的计算机是网络的一部分，则可将网络用户账户添加到计算机上的组中，并且组中的用户可以使用他们的网络密码登录，但不能更改网络用户的密码。

1.3.2 密码设置注意事项

密码可能是计算机安全方案中最薄弱的环节。由于密码破解水平的不断提高，用来破解密码的计算机的功能愈来愈强大，曾经需要几个星期才能破解的密码现在几个小时就可以破解了，所以设置具有强保密性的密码就显得非常重要。

密码破解软件往往使用下面 3 种方法中的某一种方法：巧妙猜测、词典对照和自动试验字符的每一种可能的组合。只要有足够的时间，使用自动试验字符的每一种可能的组合方法可以破解任何密码，但是要破解一个保密性很强的密码则需要几个月甚至更长的时间。

Windows 2000/XP 的密码最长可以达 127 个字符。如果是在 Windows 98 运行的网络上使用 Windows 2000 系统，那么使用的密码不要长于 14 个字符，这是因为 Windows 98 支持的最长密码长度为 14 个字符。

为了使密码具有比较强的保密性以免被破解，在设置密码的时候应该注意以下事项。

① 密码的设置至少应该在 8 位以上，当然越长越保险。

② 密码应包含表 1-2 所示 3 组字符中的每一组类型。

③ 建议每隔一段时间（如一个月）更改一次密码，不要怕麻烦而存在侥幸的心理。

④ 密码不要太常见也不要使用常见的英文单词作为密码，如用 password 作为密码就是不可取的。不要使用用户名、登录名以及单位名作为密码，也不要用自己或家人的名字作为密码。不要使用和自己有关的可以轻易获得的信息作为密码，如出生日期、电话号码、身份证号码等。

⑤ 应限制尝试登录的次数。建议用户允许有限次地（如 3 次）输入密码，如果在规定的次数内登录都失败了则禁止访问。

表 1-2　　密码字符类型

组数	说明	范例
第一组	字母（大写字母和小写字母）	A、B、C，…a、b、c，…
第二组	数字	0、1、2、3、4、5、6、7、8、9
第三组	符号（没有定义为字母或数字的其他所有字符）	` ～ ！@#$%^*()_+-={}|[]\:"<>?,/

1.3.3 Windows 98 系统密码

1. 设置 Windows 98 系统密码

❶ 在系统桌面上选择【开始】➢【设置】➢【控制面板】菜单项。打开【控制面板】窗

口，如图 1-1 所示。

❷ 双击【用户】图标打开【允许多用户设置】对话框，如图 1-2 所示。

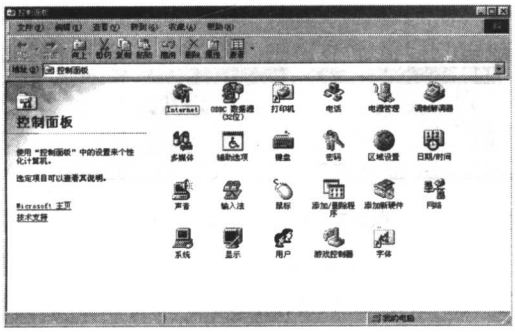


图 1-1　【控制面板】窗口

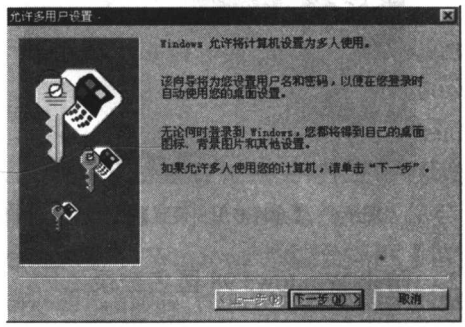


图 1-2　【允许多用户设置】对话框

❸ 单击 下一步(N) > 按钮进入【添加用户】对话框，如图 1-3 所示，在【用户名】文本框中输入自己设定的用户名。单击 下一步(N) > 按钮进入【输入新密码】对话框，在【密码】文本框中输入密码，然后在【确认密码】文本框中输入同样的密码，如图 1-4 所示。

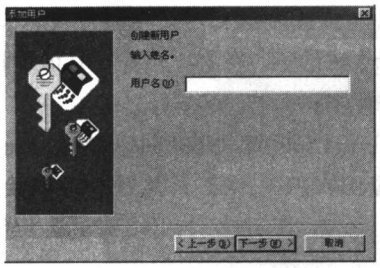


图 1-3　【添加用户】对话框

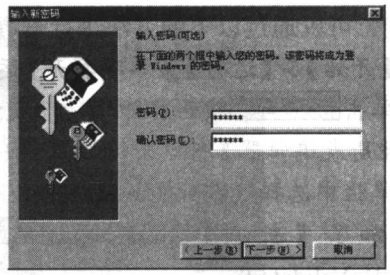


图 1-4　【输入新密码】对话框

❹ 单击 下一步(N) > 按钮进入【个性化项目设置】对话框，如图 1-5 所示。在该对话框中可以对计算机进行一些个性化的设置。设置完成后将改变原始的面貌，而以刚刚设置的效果显示出来。

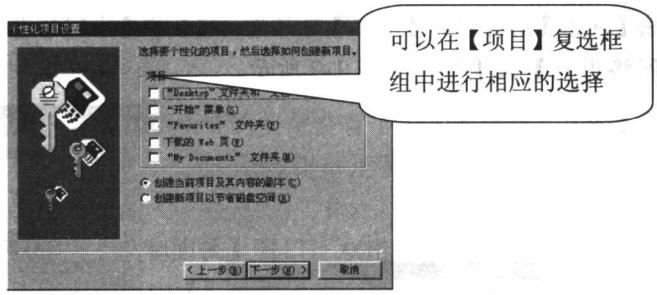


图 1-5　【个性化项目设置】对话框

❺ 设置完成后单击 下一步(N) > 按钮进入【允许多用户设置】对话框，如图 1-6 所示。单击 完成(F) 按钮弹出【正在创建个人设置】对话框，等几秒钟创建完成后会出现如图 1-7 所示的【用户设置】对话框。然后根据提示信息单击 是(Y) 按钮重新启动计算机，这样再一次进入 Windows 98 时就可以通过设定的用户名和密码进入系统了。