“十五”重点计算机普及出版物规划项目·电脑技能辅导丛书

电脑狂人笔记系列

看住你的电脑

——电脑隐私保护与防黑完全攻略

成晓静 毕靖 编著

天哪！每个人都在很牛地用电脑，但是我还不太会用，怎么办？

为了配合国家普及计算机操作以及Internet网络应用的大规划，我们特邀权威电脑专家担任企划，并从清华大学、北京大学、中科院组织了大批技术专家，特为迫切需要掌握基本电脑操作和各种应用技能的读者开发了本套《电脑狂人笔记系列》丛书。

本丛书以轻松、愉快、高效的学习方式，引导读者逐步掌握电脑应用中各种必备的知识，帮助读者成为真正的电脑应用高手！

中国电力出版社
www.infopower.com.cn

“十五”重点计算机普及出版物规划项目 · 电脑技能辅导丛书

看住你的电脑

——电脑隐私保护与防黑完全攻略

成晓静　毕靖　编著

中国电力出版社
www.infopower.com.cn

图书在版编目（CIP）数据

看住你的电脑——电脑隐私保护与防黑完全攻略 / 成晓静，毕靖编著. —北京：中国电力出版社，2004
（电脑狂人笔记系列）
ISBN 7-5083-2507-9

Ⅰ.看... Ⅱ.①成...②毕... Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2004）第 089510 号

策　　划： 裴红义
责任编辑： 于先军
责任校对： 崔燕菊
责任印制： 邹树群

丛 书 名： 电脑狂人笔记系列
书　　名： 看住你的电脑——电脑隐私保护与防黑完全攻略
编　　著： 成晓静　毕靖
出版发行： 中国电力出版社
地址：北京市三里河路 6 号　邮政编码：100044
电话：（010）88515918　传真：（010）88518169
印　　刷： 北京丰源印刷厂
开本尺寸： 170 × 230　　**印　张：** 15.25
版　　次： 2004 年 10 月北京第 1 版
印　　次： 2004 年 10 月第 1 次印刷
印　　数： 1~8000
书　　号： ISBN 7-5083-2507-9
定　　价： 19.80 元

在现实世界中，个人的隐私权是非常重要的。随着当前计算机软硬件技术的飞速发展，个人电脑和网络已经成了人们生活、工作中不能或缺的重要工具，这给人们带来方便的同时也带来了一些额外的烦恼，主要表现为个人电脑中的隐私会被他人窃取或者上网时自己的电脑会莫名其妙地受到攻击。在办公室，你可能需要与多人合用一台计算机，你的计算机以及其中的重要文件、数据有可能遭到他人有意无意的窥视或者破坏，隐私权遭到严重侵害；在你上网冲浪时，QQ 密码被盗、游戏账号被盗、遭遇恶意网站都是经常碰到的烦心事，病毒导致系统瘫痪、被人种下木马也威胁着我们的网络安全，QQ 炸弹、聊天室炸弹、邮箱炸弹更是让人防不胜防。

“在互联网上，没有人知道你是一条狗。”这句话曾经闻名全球，让人们相信在互联网上没有人知道你的真实身份。事实真的是这样的吗？网络世界是一个无法匿名、没有隐私的世界。每一个网民都以自己最真实的面目在网络世界中活动，并且都有被人窥探和记录的可能。

如何保护自己的系统和文件，如何针对网络上形形色色的攻击手段进行有效防御？这正是本书的两大重点，本书从这两方面首先详细讲解了硬件、操作系统、文件/文件夹和常用软件的加密/解密技术、电子邮件隐私保护、聊天安全宝典；同时为了知己知彼，百战不殆，本书还详细介绍了各种网络安全技术，如系统漏洞、常用网络软件、木马、欺骗攻击、拒绝服务等当前最新的黑客攻击防范技术，其目的是让读者了解其中的原理，这样才能有效防护自己的电脑免受外界的攻击。为了方便读者，在本书最后列出了国内外著名的黑客网站网址。

本书定位在初、中级读者，凡具有一点电脑基础知识的读者均能够顺利阅读。在内容上侧重实用性和可操作性，语言通俗易懂，全面介绍了电脑安全技术。书中的所有操作步骤，都经过上机验证通过，并配以大量的 Step by Step 的图解操作步骤，即使读者对相关的技术内幕不是很了解，也能按照书中的步骤顺利完成系统和文件的加密/解密以及防黑反黑工作，成功保护个人隐私。

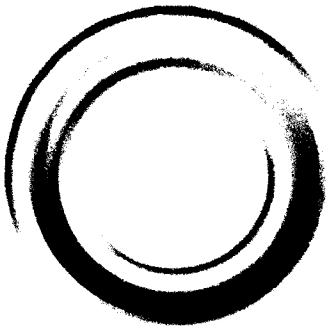
本书中使用的软件，读者可以到 http://www.skycn.com/等网址下载，或在www.google.com上搜索该软件的名称，然后进行下载。

本书由毕靖、成晓静主持编写，参加本书编写和制作的人员还有吴维、李昌隆、何磊、陈轩、唐妮、曹国峰、鲍超、田砚宇、蔡念、杨祖虎、戎恺、施润和、黄涛、王超、赵会霞、何博和史登峰等。由于计算机技术的迅速发展，加上编者的水平有限，时间仓促，本书中错误之处在所难免，读者对本书内容有疑问或意见请发E-mail至bijing@bicea.edu.cn。

目录

第 2 篇　没人知道我是一条狗

第 3 篇　红与黑的较量

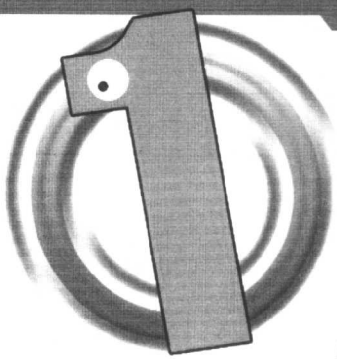


第1篇

绝对隐私

本篇内容包括：

- 第 1 章　硬件隐私保护
- 第 2 章　操作系统隐私保护
- 第 3 章　文件 / 文件夹隐私保护



硬件隐私保护

一提到计算机的安全，绝大多数人的脑海中都会跳出类似于“病毒”、“黑客”这样的字眼。是的，这些安全问题的确重要，而且也是所有 IT 媒体都不遗余力介绍的东西，这些都将在本书后半部分涉及。但有一种计算机的安全却较少被提及，这就是我们将要在本章以及后面几章介绍的计算机终端的安全。

有一点需要说明的是，确保终端的安全并不是不让别人碰它，而是要对每一个人进行区别对待，只有合法用户才被允许（即认证）使用该终端，然后再根据用户的情况分配不同的应用权限（即授权）。为了避免将你的电脑锁到保险柜里，本章将从以下几个方面首先介绍如何进行硬件隐私保护以达到数据安全保护的目的。

本章内容包括：

- CMOS 密码的设置与破解
- 硬盘加密与隐藏
- USB 硬盘加密/解密
- 光盘加密技术

1.1 CMOS 密码的设置与破解

爱机岂能无安全措施？怎么办，设个密码不就解决了？为了保护计算机的安全，设置 CMOS 密码是我们的第一道防线。

1.1.1 设置 CMOS 密码

CMOS 是电脑主板上的一块可读写的 RAM 芯片，主要用来记录计算机的日期、时间、硬盘参数、软驱情况及其他的高级参数。平常人们说的 BIOS 设置或 CMOS 设置指的就是这方面的内容。CMOS 能把这些信息保存下来，即使关机它们也不会丢失，所以以后不必对它重新设置，除非想改变电脑的配置或意外情况导致 CMOS 内容丢失。CMOS 中为用户提供了两种密码设置，即 Set Supervisor Password（管理员密码设置）和 Set User Password（普通用户密码设置）。具体设定步骤如下：

Step1　启动计算机，在出现计算机系统自检画面时连续按 Delete 键，直到出现 CMOS Setup 主界面，如图 1.1 所示的蓝屏。

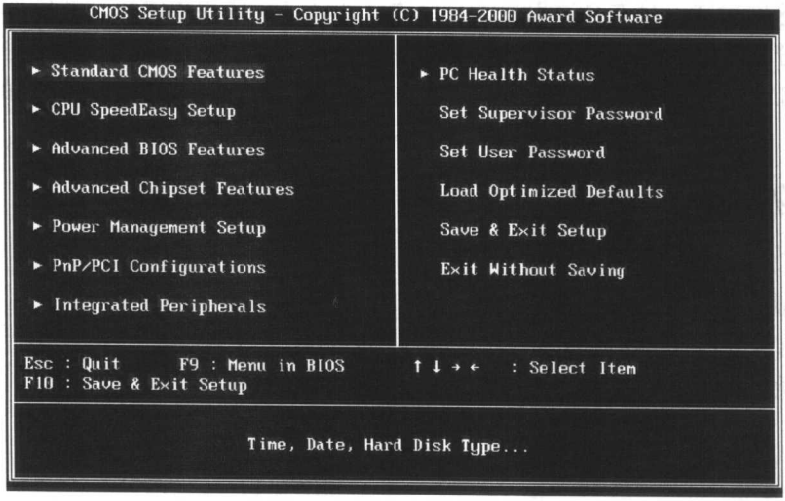


图 1.1　CMOS Setup 主窗口

进入 CMOS 设置可以多按几下 Delete 键，但不要按住不放，否则可能会出现键盘错误的信息。有些电脑进入 CMOS 的快捷键不是 Delete，而是按 Ctrl+Alt+Esc 组合键，有些是按 F2 键，具体要看屏幕上的提示。

Step2　利用键盘上的方向键将光标移到右边的 Set Supervisor Password 选项，然后按 Enter 键，出现 Set Supervisor Password 对话框后（如图 1.2 所示），输入密码。输入的密码不能超过 8 个字符，屏幕不会显示输入的密码，输入完成后按 Enter 键。

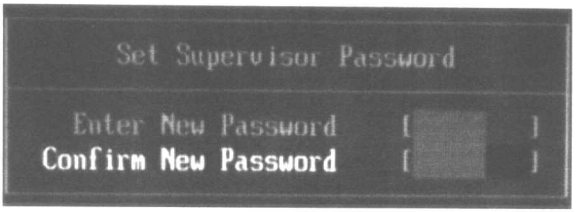


图 1.2　设置管理员密码

普通用户密码与其设置一样，就不再多说了，如果需要删除先前设定的密码，只需选择此密码然后按 Enter 键即可（不要输入任何字符），这样将删除先前所设的密码。管理员与普通用户的密码的区别在于进入 CMOS 时，输入管理员的密码可以对 CMOS 所有选项进行修改，而普通用户只能更改普通用户密码，而不能修改 CMOS 中的其他参数。

Step3　这时出现 Confirm Password（校验密码）对话框对用户刚才输入的密码进行校验，再次输入同一密码，然后按 Enter 键就可以了。如果两次输入的密码不一致，则会要求用户重新输入，这有点像我们在银行开户时账户密码的设置。

Step4　在 CMOS Setup 窗口中，再通过移动方向键选择 BIOS Features Setup（BIOS 功能设置）选项然后按 Enter 键，在出现的新窗口中用方向键选择 Security Option（安全选项）后用键盘上的 Page Up/Page Down 键把选项改为 SyStem。设定 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。

CMOS 密码分两种，一种是 Setup 密码；另一种是 System 密码，即 Security Option 选项的两个参数：Setup 和 System。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 Setup 窗口时才要求输入密码，该密码的设置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（输入管理员密码或普通用户密码中的任一个即可），如果密码不对，就无法使用计算机，此密码的设置在于禁止外来者使用计算机。显然，给你的爱机设置 System 密码，安全性更高一些。

Step5　我们所做的修改工作都要保存才能生效，要不然就会前功尽弃。选择 Save & Exit Setup（保存并退出设置）选项按 Enter 键（或者按 F10 键），出现提示后按字母 Y 键再按 Enter 键，以上设置的密码即可生效。

1.1.2　更改与消除 CMOS 密码

Step1　进入 CMOS Setup 主界面后，上下左右移动方向键选择 Set User Password 或 Set Supervisor Password，这时弹出 Enter Password（输入密码）对话框，重新输入新密码，接着直接按 Enter 键，在 Confirm Password（校验密码）对话框中两次输入更改后的密码，然后再次按 Enter 键。

Step2　利用方向键选择 Save & Exit Setup（保存并退出设置）选项后按 Enter 键（或者按 F10 键），出现提示后按字母 Y 键再按 Enter 键，以上所进行的密码更改即可生效。

如果想取消密码，只要在两次输入密码的对话框中，不输入任何密码就可以了。

1.1.3　破解 CMOS 密码

从 CMOS 密码的设置知道，设置 System 密码安全性更高，其破解也更复杂，设置 Setup 密码的安全性相对较低，破解也相对简单。下面就列出常用的 CMOS 密码破解方法。

1．DEBUG 法

DOS、Windows 95/98/2000 都提供了一个工具 Debug.exe。这是一个调试工具，可以对内存、端口等设备进行读写，也可以用来编写和调试汇编程序。由于 CMOS 设置就是通过对相应的端口进行读写来完成的，所以在操作系统中对这些端口进行改写也能够改写相应的设置，从而达到清除口令的目的。在开机过程中按住 F8 键，进入纯 DOS 环境下，运行 Debug，然后输入如图 1.3 所示的代码，并按 Enter 键即可破解 MOS 密码。但是这个方法在 Windows 2000/XP 的命令提示符下是无效的。

图 1.3　用 Debug 法改写 BIOS

2．万能密码法

有些 BIOS 可以使用万能密码，万能密码就是 BIOS 程序上面的 Back Door（后门），通常由主板厂家自己设置，以便于主板厂家向用户提供技术支持时不需要知道用户设定的密码，就可以打开电脑进行维护。不过，不同厂商设置的 BIOS 通用密码都不一样，而且同一厂家生产的不同版本的 BIOS 密码可能也不一样，所以有时候此法并不能奏效。但如果 BIOS 支持，此法很有效。

（1）AMI BIOS 万能密码。

你可以试一试下面的几个单词：AMI、BIOS、PASSWORD、HEWITT RAND、AMI? SW、AMI_SW、LKWPETER、A.M.I。

（2）AWARD BIOS 万能密码。

你可以试一试下面的几个单词：AWARD_SW、j262、HLT、SER、SKY_FOX、BIOSTAR、ALFAROME、lkwpeter、j256、AWARD?SW、LKWPPETER、Syxz、aLLy、589589、589721、awkard（注意大小写）。

对付万能密码的方法就是升级 BIOS，因为大家都不了解新版本的 BIOS，而且原有的通用口令可能也不复存在，这对提高计算机的安全性和稳定性都是有利的。

3．CMOS 放电法

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 BIOS DEFAULT（载入 BIOS 默认值）或 LOAD SETUP DEFAULT（载入设置程序默认值）即可，前者以最安全的方式启动计算机，后者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，也就是说不能进行上面的操作，那又该怎么办？不要紧，我们还可以使用“跳线短接法”的方法对 CMOS 放电（建议一般用户使用此法），具体操作如下。

在电池附近有一个跳线开关（可参考主板说明书），一般情况下，在跳线旁边注有 RESET CMOS、CLEAN CMOS、CMOS CLOSE 或 CMOS RAM RESET 等字样，跳线开关一般为 4 个引脚，其中标注为 External BATT 的引脚 1 用来连接外接电池的正极；与其相邻的引脚 2 与主板上内置电池的电池相通；引脚 3 为 CMOS RAM 供电端的正极；引脚 4 为 CMOS RAM 供电端的负极。有的主板在 1、2 引脚上有一个跳

接器，此时将其拔下接到3、4引脚上即可放电；有的主板所有引脚上都没有跳接器，此时将2引脚与充电电容短接即可放电，跳线操作如图1.4所示。

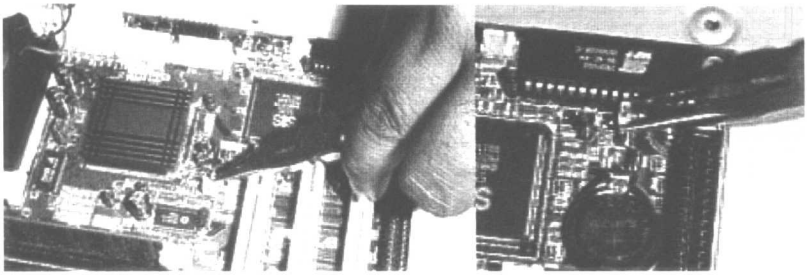


图1.4　跳线操作

此法关键之处在于找到相应的跳线（如果没有主板说明书，则难度就更大了），几乎所有的主板都有清除CMOS的跳线和相关设置，但因厂商不同而各有所异，虽然大部分都在电池附近，但也有例外。除非确定无疑，否则尽量不要试着短接主板上的跳线，这很容易造成主板烧毁。而有的主板的CMOS清除设备并不是我们常见的跳线，而是很小的焊接锡点，一般都要用镊子，小心地将其短路，就可成功清除CMOS密码！

1.2　硬盘加密与隐藏

在CMOS中设置系统密码，使非法用户无法启动计算机，是我们给爱机设置的第一道防线，可是这并未真正锁住硬盘，因为只要将硬盘挂在别的计算机上，硬盘上的数据和软件仍可使用。而硬盘是我们存放数据最常用的存储介质，里面存放着操作系统、软件、文档、游戏、音乐、电影等数字化信息，对它的保护和加密也就显得格外重要。下面就介绍一些硬盘加密、保护的技术，将你的第一道防线打造得更加牢固。

1.2.1　利用硬盘还原卡

在提供多人集体上机的公共场所如学校机房、网吧等，经常会碰到有些人故意捣乱，在公用计算机上安装一些有害软件甚至病毒，甚至一些包含色情、暴力、反动等内容的文件。这样一来，不但后来的人无法使用受害的机器，还会造成不良影响。正是在这样的情况下，国内出现了硬盘还原卡（又称硬盘保护卡）这一硬件保

护硬盘的设置，只要将还原卡插入计算机，并且指定需要维护的磁盘区域，这样任由他人进行删除、格式化、安装、卸载等操作，只要重新启动计算机，一切都会恢复如初。

1．安装与设置

目前市面上的硬盘还原卡品种越来越多，功能也越来越强大，常见的有小哨兵、全能、远志、金盾、神盾、时光、中孚和美嘉等。可以根据需要选择一种价位不高又能满足要求的还原卡。图 1.5 所示为美嘉硬盘还原卡。

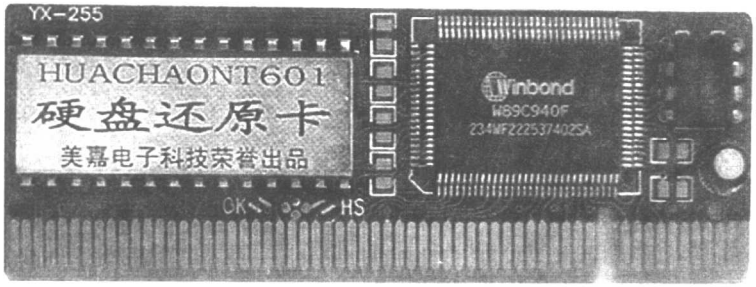


图 1.5　硬盘还原卡

安装步骤如下：

Step1　首先要确定系统是否达到说明书中的最低要求，如某种还原卡的最低要求为：386 及以上 CPU、VGA 彩显、硬盘、软驱，一个空的 PCI 插槽（或者是 ISA 插槽），如果需要网络维护功能还应该有网卡。

Step2　检查并更改 CMOS 参数设置。将 CMOS 中的 Virus Warning（病毒警告）选项设为 Disabled。注意绝大多数还原卡仅支持第一物理硬盘，对于加挂的硬盘不起作用。

Step3　检查一下计算机病毒，确保在安装还原卡之前系统无病毒。关闭杀毒软件的实时病毒监控功能，并卸载基于 Windows 的系统防护、恢复软件，以免引起软硬件冲突。

Step4　最后关闭计算机，打开机箱，将还原卡插到一个空的 PCI 插槽（如果是 ISA 接口的卡则插到 ISA 插槽内）内，确认插牢后盖好机箱。

还原卡提供两种工作模式：保护模式和开放模式。同时，提供三种特权操作：系统设置、更新数据和还原数据。可以根据需要对还原卡加以设置。

2．破解还原卡

既然可以安装还原卡来保护硬盘，就一定可以找到办法来破解它。但要提醒大家的是，我们研究破解它的方法只是为了了解快速恢复数据硬盘数据的原理，而不是搞破坏！