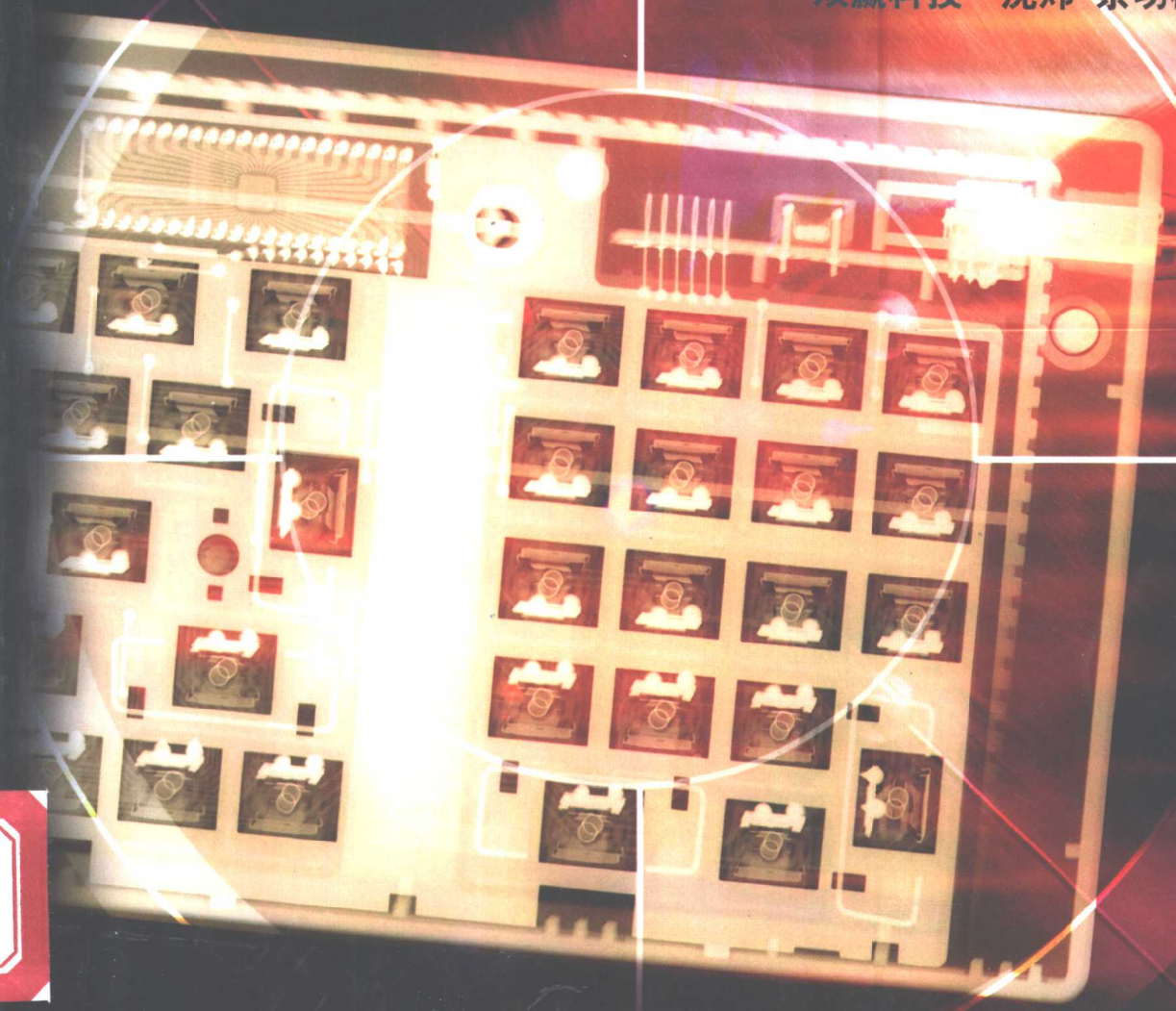
加密解密与黑客防御技术

双赢科技　沈炜　余功栓　编著



科学出版社
www.sciencep.com

加密解密与黑客防御技术

沈　炜　余功栓　编著

科学出版社

北　京

内 容 简 介

本书从加密解密、网络安全、病毒防治三个方面，以理论结合实际的方法来讲解如何保证用户电脑的安全。本书详细讲解了硬件、操作系统、办公软件、常用软件、驱动器等全方位加密解密的技术，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、网络监听、扫描器、Web 攻防、防火墙技术等当前最新的黑客攻击防范技术，最后介绍了保证个人电脑安全的一个重要部分即电脑病毒的防治技术以及常用的杀毒软件。

本书全面地介绍了电脑安全技术，本书有 100 多个具体的实用技术，都是经过作者亲自上机实践验证的。

本书适合个人电脑用户以及各种电脑爱好者阅读，也可以作为高校的教材参考书以及培训教材。

图书在版编目（CIP）数据

加密解密与黑客防御技术/沈炜，余功栓编著. —北京：科学出版社，2003

ISBN 7-03-012334-4

Ⅰ.加… Ⅱ.①沈… ②余… Ⅲ.①电子计算机—密码—加密②电子计算机—密码—解密译码③计算机网络—安全技术 Ⅳ.①TP309.7 ②TP393.08

中国版本图书馆 CIP 数据核字（2003）第 091949 号

策划编辑：李 娜/责任编辑：陈 钢

责任印制：吕春珉/封面设计：十四目图文设计

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2003 年 10 月第 一 版 开本：787×1092 1/16

2003 年 10 月第一次印刷 印张：26 1/4

印数：1—4 000 字数：432 000

定价：35.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

随着当前计算机软硬件技术的飞速发展，个人电脑越来越普及，网络的发展也日新月异。这给人们带来了很多方便的同时，也带来了一些麻烦。最为突出的就是个人电脑中的隐私会被人窃取或者自己的电脑会莫名其妙地受到别人的攻击。

正是基于这些原因，我们考虑编写本书。本书从个人电脑的内部和外部安全出发，向读者详细介绍了如何通过加密解密手段来保护个人资料安全，并详细介绍了网络中各种可能碰到的攻击以及应对措施。最后本书还介绍了如何防治病毒以及如何使用一些最常用的杀毒软件。通过这几个部分的学习，读者的电脑一定会固若金汤了。本书介绍的各种攻击技术目的是让读者了解其中的原理，这样才能知道如何防护自己的电脑免受各种外界攻击，从而做到知彼知己，百战不殆。

本书的主要内容：

第 1 章介绍了硬件的加密解密技术，包括计算机、硬盘、软盘、光盘以及 U 盘等。

第 2 章介绍了系统加密解密的技术，其中包括大部分流行的操作系统，如 Windows 9x、Windows NT、Windows XP 以及 Windows Server 2003。

第 3 章介绍了常用办公软件的加密解密技术，包括 Office 系列以及 WPS 等。

第 4 章介绍了常用应用软件的加密解密技术，包括 WinZip、WinRAR、SQL Server、PDF 等。

第 5 章介绍了文件夹/驱动器的加密解密技术，如驱动器的隐藏加密、文件夹的隐藏加密等。

第 6 章介绍了当前的各种操作系统的漏洞，以及针对各种漏洞的攻防措施。

第 7 章介绍了常用软件的攻击防范措施，如 QQ、电子邮件、WWW 聊天室以及 FTP 等破解防范技术。

第 8 章介绍了当前流行的木马技术以及攻防措施。

第 9 章介绍了电子欺骗攻击手段，如 IP 欺骗攻击、DNS 欺骗攻击、ARP 欺骗攻击和 Web 欺骗攻击等。

第 10 章介绍了 Windows 下的各种拒绝服务攻防技术，以及在 Linux 下的各种分布式拒绝服务攻防技术。

第 11 章介绍了 NetXray、Sniffer pro、Commview 等各种功能强大网络监听软件的攻防技术。

第 12 章介绍了黑客的基本武器扫描器的攻防技术，包括比较有名的有 Nmap 扫描器，Superscan 扫描器等。

第 13 章介绍了各种 Web 攻击手段以及防范措施，如 ASP、CGI、PHP、JSP、Web 服务器等漏洞分析以及攻防措施。

第 14 章介绍了目前最常用最经典的各种防火墙技术，如天网防火墙、Sygate 防火墙等技术。

第 15 章介绍了当前著名的病毒防治手段和措施。

第 16 章介绍了当前知名的杀毒软件的使用方法，如金山毒霸、诺顿、瑞星等。

参加本书编写的还有付勇、余功栓、郑晓清、汪晓平、刘海英、李平、吴亮、汪杰、吴阳、王占全、李建华等。在此一并致谢。

如果对本书有任何疑问，可以登录到 www.2wintech.net 进行咨询。

作 者

2003 年 8 月

目　录

第 1 章　硬件加密解密技术

加密和解密是矛盾的两个方面。加密是为了阻止别人获取他们不应该获得的东西，而解密正相反。这一矛盾的斗争已经有相当长的历史了，在这一历史长河中，用某种“物”的特定属性来实现加密则占有很重要的地位，一个典型的例子就是“隐写术”。“隐写术”表现在计算机上，就是基于硬件的加密，也就是说利用某些计算机硬件的特性，来达到阻止他人获得某种信息的目的。不过，“你有你的张良计，我有我的过墙梯”，各种具有针对性的解密技术也相继出笼。看来斗争还将在计算机领域长时间的存在下去。

在这一章，我们将介绍一些硬件加密和解密技术，通过了解这些技术，读者可以对硬件加密和解密有一定的了解。相信读者在了解并合理地使用这些技术之后，可以有比较好的应用效果。

1.1　CMOS 加密解密技术

目标

了解 CMOS 的作用、口令的设置和破解。

知识背景

CMOS（Complementary Metal Oxide Semiconductor），本意是指互补金属氧化物半导体存储器，是一种大规模应用于集成电路芯片制造的原料，在不引起混淆的情况下，有时候也指相应的半导体制造技术。在计算机主板上，有一块用 CMOS 制造的用电池供电的存储器，用于存放 BIOS（Basic Input/Output System，基本的输入输出系统）的配置信息，这些信息共有 256 个字节，它们直接用于设置相应的硬件设备，因而占有很重要的地位。所谓 BIOS 设置就是配置这些信息，由于 CMOS 存放了 BIOS 的设置信息，因而也常常称 BIOS 设置为 CMOS 设置。

CMOS 设置中有一个很重要的功能就是设置口令，一旦完成口令设置，在计算机完成自检、引导操作系统之前，会要求用户输入相应的口令，如果输入的口令不正确，计算机将不会引导操作系统，所以具有一定的安全性。但如果忘记了口令也会造成一定的麻烦。

实现步骤

1. 设置 CMOS 口令

设置 CMOS 口令一般在计算机完成自检后，未引导操作系统之前进行（只有很少

的计算机系统是在操作系统引导后进行 CMOS 设置的，例如一些 Compaq 计算机)。下面是设置 CMOS 的操作步骤（以目前使用得最多的 Award BIOS 为例)：

（1）启动计算机，在计算机屏幕的左下角出现“Press DEL to enter SETUP”（图 1-1）时按 DEL 键，直到出现 CMOS SETUP 主界面（图 1-2），也就是 CMOS 菜单。

图 1-1 按 DEL 进入 SETUP

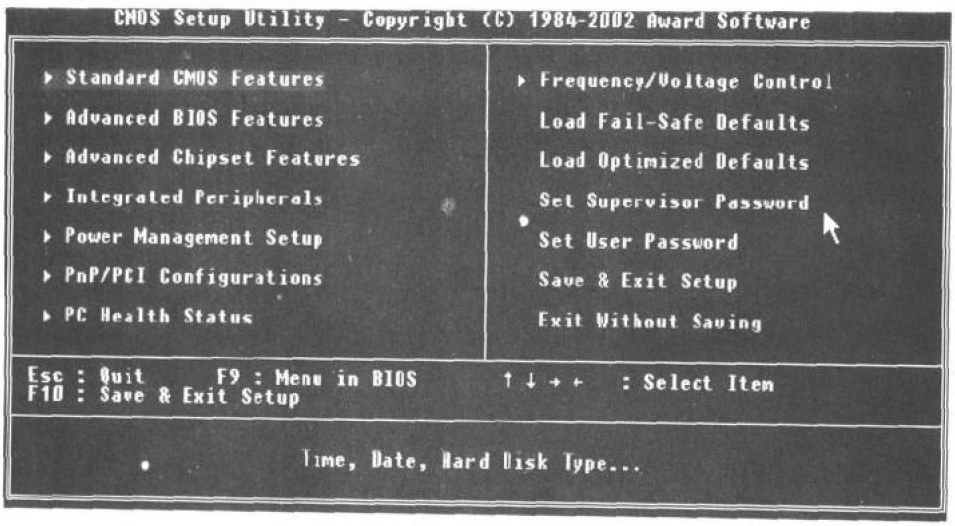


图 1-2 Award CMOS 设置主界面

（2）在右边鼠标箭头所指的地方有两项，分别是“Set Supervisor Password”（设置管理员口令）和“Set User Password”（设置用户口令)；移动光标至这两项中的任意一项，按回车键；CMOS 会提示输入口令和再次输入口令（图 1-3），此时可以输入口令，最长 8 个字符，若两次输入的口令不相同，CMOS 会提示错误，并要求重新输入。

图 1-3 口令输入

（3）口令输入完毕后，再选择 CMOS 菜单左边第二项“Advanced BIOS Features”（高级 BIOS 属性设置)，选择图 1-4 中鼠标箭头所指的“Security Option”项，将这一项的值设置为“System”，而不是图中的“Setup”。

（4）选择 CMOS 菜单右边的“Save & Exit Setup”（保存并退出设置）项，回车后，CMOS 会提示“Save & Exit Setup? (Y/N)”（是否保存并退出设置？是/否)，按 Y 键后回车，就完成了口令设置。

注意：进入 CMOS 设置可以多按几下 Del 键，但不要按住不放，否则可能会出现键盘错误的信息；有的计算机进入 CMOS 的快捷键不是 Del，例如大部分笔记本计算机就是 F2，具体看计算机的相应提示；“Security Option”中设置为

Setup 表示进入 CMOS 设置时需要验证口令，设置为 System 表示计算机启动时就需要验证口令。

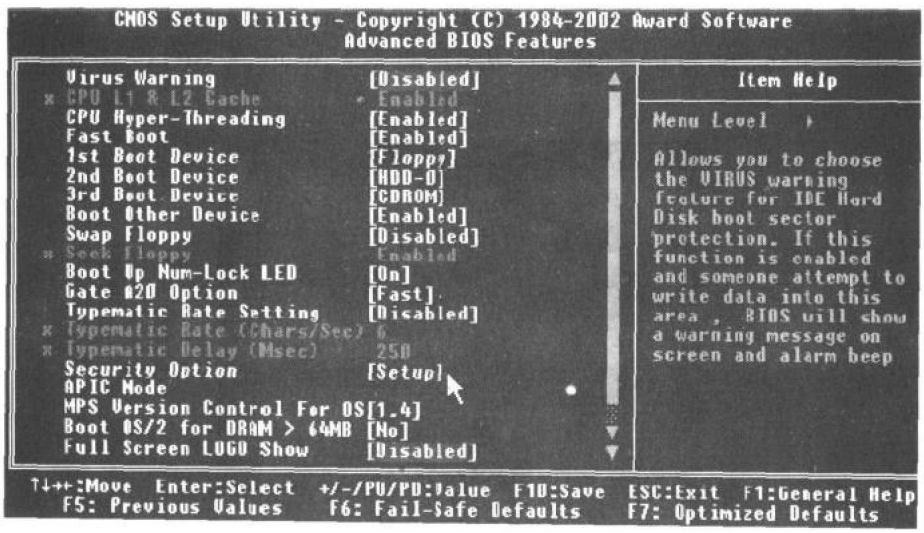


图 1-4　高级 BIOS 属性设置

2. 破解 CMOS 口令

如果不小心丢失了 CMOS 口令，但计算机还能够引导操作系统，那么重新找回 CMOS 口令或清除有这么几种方法：

（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 DOS 状态下，运行 Debug，然后输入：o 70 16 回车，o 71 16 回车，q 回车（图 1-5）。不过，这个方法在 Windows 2000/XP 的“命令提示符”下是无效的。

图 1-5　用 Debug 法改写 BIOS

（2）工具法。CMOS 并不存储用户输入的口令，而是对口令进行了一些变换后，存储了变换后的结果，一般说来，这一过程是不可逆的。但是由于在 CMOS 中，存储口令只用了 3 个字节，而口令最多可以输入 8 个字符，因此，一定有很多的口令经过变换后的结果是相同的。当然，不同的 BIOS，不同版本的 BIOS，有不同的变换。一些软件可以模拟这些变换，通过穷举来获得有相同变换结果的口令。这里介绍一款很有用的 CMOS 口令读取软件 BiosPwds（图 1-6）。它是一款德国人写的软件，使用非常方便，

只要单击主界面中的“Get passwords”按钮，就可以获得相应的口令。如图 1-6 中，BiosPwds 查到 CMOS 的口令是“AKAKAPZW”。不过，这个软件有个限制，会在 Windows2000 上运行不正常，会提示“Your PC doesn't have an Award Bios. Please look for a newer version of this program”（你的计算机用的不是 Award 的 BIOS，请寻找本软件的更新版本）。

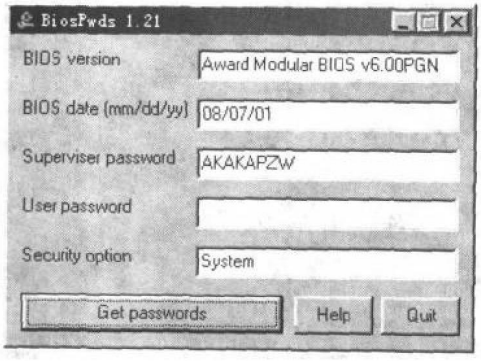


图 1-6 BiosPwds

另一款优秀的工具是 CmosPwd，它是 CMOS 口令读取工具，能够获得 AMI、Award 以及一些品牌机的 CMOS 口令，使用也很简单，只要运行一下这个程序（图 1-7），就能够获得相应的口令，不过运行前你需要知道你的 BIOS 品牌和版本信息。这个软件可以到下列网址去下载：

http://js-http.skycn.net:8080/down/cmospwd-4.3.zip。

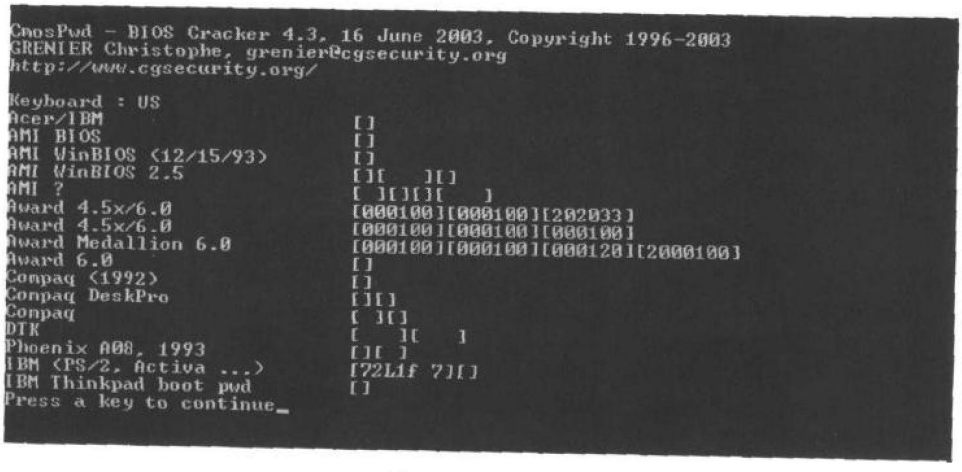


图 1-7 CmosPwd

（3）通用口令法。上面的两个方法都是在 CMOS 设置了口令后，仍能引导操作系统时可采取的办法，如果在 CMOS 中将“Security Option”项设置为“System”，那么这两个方法也将“英雄无用武之地”了。

主板 CMOS 的通用口令是一个偏方。通用密码一般是由主板厂家设置的，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

等。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。表 1.1 和表 1.2 是一些通用口令，读者可以试一下，更多信息可以访问网址：http://www.biosrepair.com/pic/pic15.htm。

表 1.1　Award BIOS

AWARD_SW	SKY_FOX	j256	j262	BIOSTAR	AWARD?SW
HLT	lkwpeter	LKWPETER	SER	CONCAT	Syxz
ALFAROME	awkward	aLLy	589721	589589	j64
	AWARD_SW	j322	?award	awkward	lkw peter
1322222	BIOS	lkwpeter	1EAAh	bios*	PASSWORD
256256	biosstar	SER	589589	biostar	setup
589721	CONCAT	SKY_FOX	admin	condo	SWITCHES_SW
alfarome	CONDO	Sxyz	aLLy	djonet	SZYX
aPAf	efmukl	t0ch20x	award	g6PJ	t0ch88
AWARD SW	h6BB	TTPTHA	award.sw	HELGA-S	ttptha
AWARD?SW	HEWITT RAND	TzqF	award_?	HLT	wodj
award_ps	j09F	ZAAADA	zbaaaca	zjaaadc	j262
AWARD_PW	j256				

表 1.2　AMI BIOS

AMI	BIOS	PASSWORD	HEWITT RAND	AMI SW	AMI_SW
LKWPETER	A.M.I	589589	AMI	aammii	AMI!SW
AMIPSWD	AMI.KEY	amipswd	ami.kez	AMISETUP	AMI~
bios310	ami?	BIOSPASS	amiami	CMOSPWD	amidecod
HEWITT RAND	KILLCMOS				

对付通用口令的办法就是升级 BIOS，因为新版本的 BIOS 大家都不了解，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。

（4）放电法。主板的 CMOS 是由一个 3V 的电池供电。一般在这颗电池的旁边，会有一个跳线（Jumper），这个跳线用来设置是否清除 CMOS 内容的。这个跳线有三根针，在一般情况下，第 1 和第 2 针短接，如果要清除 CMOS 内容，则把第 2 和第 3 针短接。这个方法是一定能够成功的，不过如果没有主板说明书，则有点难度，也有点风险。图 1-8 中箭头所指的跳线就是某款主板上清除 CMOS 的跳线。

注意：不同的主板清除 CMOS 内容的跳线位置是不相同的，虽然大多数都在电池附近，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，因为可能会造成主板烧毁。

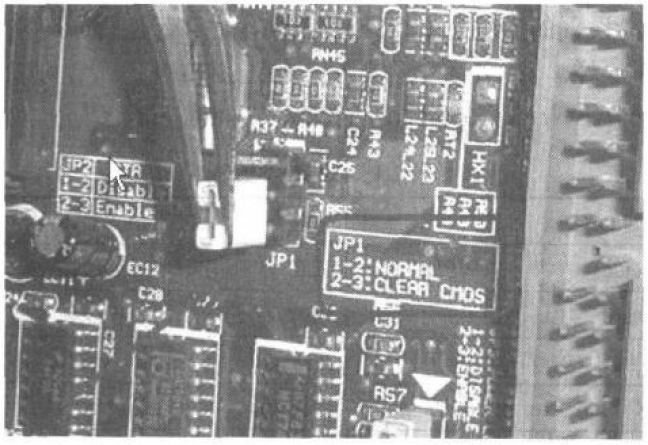


图 1-8 清除 CMOS 的跳线

你问我答

Q：我按照你说的 Debug 方法做，为什么还是不能清除我计算机上的 BIOS 口令？

A：Debug 方法的实质是改写用于存放口令变换结果的那 3 个字节或者引起 CMOS 内容校验出错，强迫 BIOS 以缺省内容改写 CMOS。但不同的 BIOS，相同的 BIOS 的不同版本，这 3 个字节的位置不一定相同，这就是本章介绍的方法在不同的计算机上可能行也可能不行的原因。在 Debug 中，输入 o 70 16 的含义是向端口 0x70（表示 16 进制的 70)发送一个字节值为 0x16，这个命令的目的是告诉计算机要改写 CMOS 中的第 0x16（即十进制的 22）个字节，输入 o 71 16 的含义是告诉 CMOS 将第 0x16 个字节的内容改写为 0x16。了解了这一点，我们就有一个一定成功的方法：写一个程序，将 CMOS 的 256 个字节全部清 0，就一定会将口令清除。方法如下：

```
C:\>debug                    //运行 Debug，要在纯 DOS 状态下
-a                           //进入汇编模式
xxxx:0100 mov cx, 0          //设置循环变量
xxxx:0103 mov dx, 70         //将 dx 设为 0x70
xxxx:0106 mov ax, cx         //要改写的第 cx 个字节
xxxx:0108 out dx, al         //向 0x70 输出要改写的字节序数
xxxx:0109 mov dx, 71         //将 dx 设为 0x71
xxxx:010C mov ax, 0          //将 ax 置为 0
xxxx:010F out dx, al         //向 0x71 输出 0，即将第 cx 个字节置为 0
xxxx:0110 add cx, 1          //cx 增加 1，这样可以将 cx 递增，从而改写全部字节
xxxx:0113 jmp 103            //从 103 开始循环执行
```

上面的程序中 xxxx 表示段地址，是计算机自动显示的，不同的计算机有不同的数值，读者不必关心。程序是一个死循环，执行后，等几秒钟，就可以热启动或 Reset 计算机，重启后，屏幕上会出现“CMOS checksum error，Default Loaded”，这时计算机就停在那里，你可以从容地按 DEL 键来进入 CMOS 设置程序。

Q：我的计算机很怪，我找不到 Clear CMOS 的跳线，而且我使用的是 Windows 2000，没办法用 Debug 法，而 BiosPwds 说我的 BIOS 不认识，那我该怎么办？

A：你可以这样试一下：打开计算机机箱，然后将硬盘的数据线和电源拔掉，然后

将一张可启动软盘插入软驱，将一张可启动光盘放入光驱，再启动计算机。一般情况下，计算机允许从多个设备（包括软驱、硬盘和光驱）启动，此时你的计算机应该可以从软盘或光盘引导，再用 Debug 法就可以了。

1.2　硬盘加密技术

目标

了解一定的硬盘知识，并知道如何使用 Diskedit 来加密解密硬盘。

知识背景

从个人计算机中出现硬盘开始到现在，硬盘的容量日益增大，但整个硬盘的结构没有什么根本性的变化。目前的硬盘采用的仍是“温彻斯特”（Winchester Hard Disk Drive）技术：就是盘片在高速旋转，而磁头则利用盘片旋转而激起的气流在盘片上飞行，这些盘片和磁头都被封装在一个相对密封的盒子中。

一个硬盘，一般都有多个盘片和磁头，这些磁头被固定在同一个主轴上，能够同时读出多个盘片上的一条磁道，而这些磁道分布在同一个圆柱面上，所以这一系列磁道也称为一个柱面。0 柱面是最重要的一个柱面，它位于盘片的最外侧，用于存放硬盘的引导记录和分区信息。这也是硬盘 0 柱面损坏后硬盘无法使用的原因。

硬盘的引导记录（Main Boot Record）和分区表（Partition Table）位于硬盘 0 柱面 0 面 1 扇区，也是整个硬盘的第 1 个扇区（图 1-9）。在图 1-9 中，划红框的 64 个字节就是分区表，记录硬盘最开始的四个分区的信息，每个分区占用 16 个字节。划红框的“55 AA”是分区启动标志，如果这两个字节内容不是“55 AA”，则该硬盘或分区无法被使用。

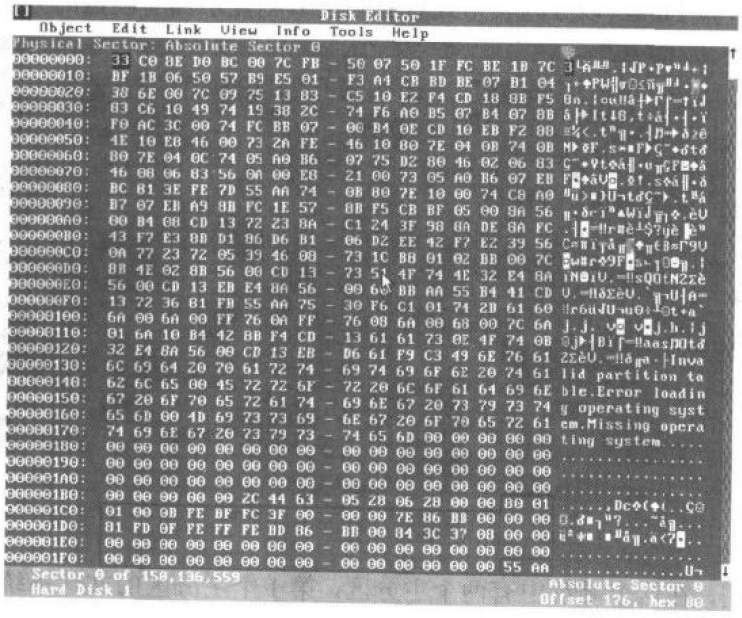


图 1-9　硬盘分区表

这个时候你一定在想：如果我适当地修改分区表，不是就可以达到阻止别人访问硬盘的目的了吗？没错，适当地修改引导记录和分区的确是能够起到加密硬盘的作用。

实现步骤

打开 Norton 的 Diskedit（需要在纯 DOS 状态下，否则可能无法改写硬盘），选择“Object”菜单中的“Disk”菜单项（可能鼠标无法使用，可以用 Alt+O 打开 Object 菜单，或用 F10 再加光标键来打开相应菜单），在出现的“Select the disk you wish to edit”（选择你想编辑的磁盘）窗口中（图 1-10），选择“Physical disks”（物理磁盘），然后选择“Hard Disk 1”（第 1 个硬盘，如果有多个硬盘，此处会有多项），然后回车确认，此时 Diskedit 会打开第 1 个硬盘的第 1 个扇区，也就是分区表所在的扇区（图 1-9）。

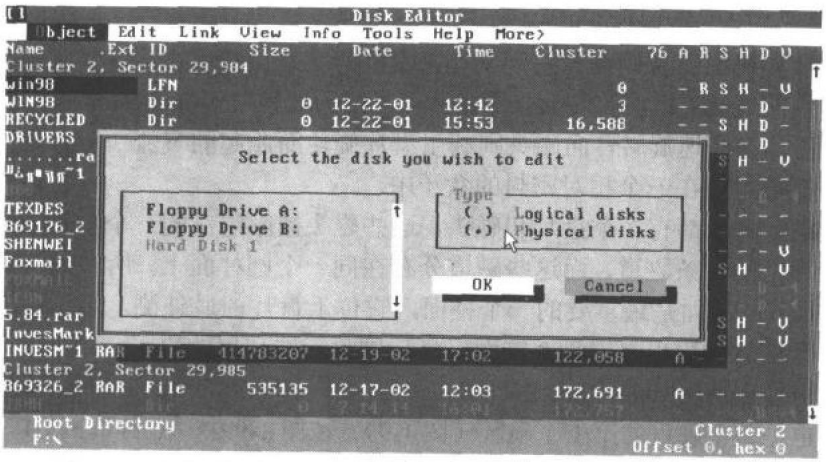


图 1-10 选择硬盘

在图 1-9 中，按 F6 键（以分区表形式查看扇区），则显示当前硬盘的分区表（图 1-11）。

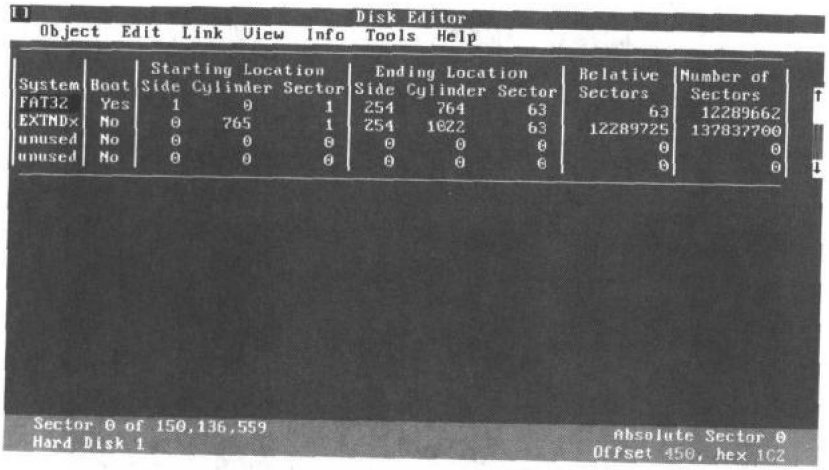


图 1-11 分区表

图 1-11 说明，在这个硬盘中有两个主分区，第 1 个主分区的文件系统是 FAT32，共有 12289662 个扇区，在这个分区前面，有 63 个保留扇区（Relative Sectors，即分区表