思科认证辅导:常见硬盘加密解密的几种方法解析思科认证
 一、修改硬盘分区表信息 硬盘分区表信息对硬盘的启动至关重要，如果找不到有效的分区表，将不能从硬盘启动或即使从软盘启动也找不到硬盘。通常，第一个分区表项的第0子节为80H，表示C盘为活动DOS分区，硬盘能否自举就依*它。若将该字节改为00H，则不能从硬盘启动，但从软盘启动后，硬盘仍然可以访问。分区表的第4字节是分区类型标志，第一分区的此处通常为06H，表示C盘为活动DOS分区，若对第一分区的此处进行修改可对硬盘起到一定加密作用。 具体表现在： 1.若将该字节改为0，则表示该分区未使用，当然不能再从C盘启动了。从软盘启动后，原来的C盘不见了，你看到的C盘是原来的D盘，D盘是原来的E盘，依此类推。 2.若将此处字节改为05H，则不但不能从硬盘启动，即使从软盘启动，硬盘的每个逻辑盘都不可访问，这样等于整个硬盘被加密了。另外，硬盘主引导记录的有效标志是该扇区的最后两字节为55AAH。若将这两字节变为0，也可以实现对整个硬盘加锁而不能被访问。硬盘分区表在物理0柱面0磁头1扇区，可以用Norton for Win95中的Diskedit直接将该扇区调出并修改后存盘。或者在Debug下用INT 13H的02H子功能将0柱面0磁头1扇区读到内存，在相应位置进行修改，再用INT 13H的03H子功能写入0柱面0磁头1扇区就可以了。 上面的加密处理，对一般用户来讲已足够了。但对有经验的用户，即使硬盘不可访问，也可以用INT 13H的02H子功能将0柱面0磁头1扇区读出，

根据经验将相应位置数据进行修改，可以实现对硬盘解锁，因为这些位置的数据通常是固定的或有限的几种情形。另外一种保险但显得笨拙的方法是将硬盘的分区表项备份起来，然后将其全部变为0，这样别人由于不知道分区信息，就无法对硬盘解锁和访问硬盘了。 二、对硬盘启动加口令 我们知道，在CMOS中可以设置系统口令，使非法用户无法启动计算机，当然也就无法使用硬盘了。但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。要对硬盘启动加口令，可以首先将硬盘0柱面0磁头1扇区的主引导记录和分区信息都储存在硬盘并不使用的隐含扇区，比如0柱面0磁头3扇区。然后用Debug重写一个不超过512字节的程序(实际上100多字节足矣)装载到硬盘0柱面0磁头1扇区。该程序的功能是执行它时首先需要输入口令，若口令不对则进入死循环.若口令正确则读取硬盘上存有主引导记录和分区信息的隐含扇区(0柱面0磁头3扇区)，并转去执行主引导记录。 由于硬盘启动时首先是BIOS调用自举程序INT 19H将主硬盘的0柱面0磁头1扇区的主引导记录读入内存0000：7C00H处执行，而我们已经偷梁换柱，将0柱面0磁头1扇区变为我们自己设计的程序。这样从硬盘启动时，首先执行的不是主引导程序，而是我们设计的程序。在执行我们设计的程序时，口令若不对则无法继续执行，也就无法启动了。即使从软盘启动，由于0柱面0磁头1扇区不再有分区信息，硬盘也不能被访问了。当然还可以将我们设计的程序像病毒一样，将其中一部分驻留在高端内存，监视INT 13H的使用，防止0柱面0磁头1扇区被改写。 三、对硬盘实现用户加密管理 UNIX操作系统可以实现多用户管理，在DOS系统下，将硬盘

管理系统进行改进，也可实现类似功能的多用户管理。该管理系统可以满足这样一些要求： 1.将硬盘分为公用分区C和若干专用分区D。其中“ 超级用户 ”来管理C区，可以对C区进行读写和更新系统.“ 特别用户 ”(如机房内部人员)通过口令使用自己的分区，以保护自己的文件和数据.“ 一般用户 ”(如到机房上机的普通人员)任意使用划定的公用分区。后两种用户都不能对C盘进行写操作，这样如果把操作系统和大量应用软件装在C盘，就能防止在公共机房中其他人有意或无意地对系统和软件的破坏，保证了系统的安全性和稳定性。 2.在系统启动时，需要使用软盘钥匙盘才能启动系统，否则硬盘被锁住，不能被使用。 此方法的实现可通过利用硬盘分区表中各逻辑盘的分区链表结构，采用汇编编程来实现。 四、对某个逻辑盘实现写保护 我们知道，软盘上有写保护缺口，在对软盘进行写操作前，BIOS要检查软盘状态，如果写保护缺口被封住，则不能进行写操作。而写保护功能对硬盘而言，在硬件上无法进行，但可通过软件来实现。在DOS系统下，磁盘的写操作包括几种情况：①在COMMAND.COM支持下的写操作，如MD、RD、COPY等.②在DOS功能调用中的一些子功能如功能号为10H、13H、3EH、5BH等可以对硬盘进行写操作.③通过INT 26H将逻辑扇区转换为绝对扇区进行写.④通过INT 13H的子功能号03H、05H等对磁盘进行写操作。 但每一种写操作最后都要调用INT 13H的子功能去实现。因此，如果对INT 13H进行拦截，可以实现禁止对硬盘特定逻辑盘的写操作。由于磁盘上文件的写操作是通过INT 13H的03H子功能进行写，调用此子功能时，寄存器CL表示起始扇区号(实际上只用到低6位).CH表示磁道号，在硬盘即为柱

面号，该柱面号用10位表示，其最高两位放在CL的最高两位。对硬盘进行分区时可以将硬盘分为多个逻辑驱动器，而每个逻辑驱动器都是从某一个完整的柱面开始。如笔者的硬盘为 2.5GB，分为C、D、E、F、G五个盘。其中C盘起始柱面号为00H，D盘起始柱面号为66H，E盘起始柱面号为E5H，F盘起始柱面号为 164H，G盘起始柱面号为26BH。如果对INT 13H进行拦截，当AH=03H，并且由CL高两位和CH共同表示的柱面号大于E4H并小于164H，就什么也不做就返回，这样就可以实现对E盘禁止写。 