

DR DOS 安全系统的破解

余其华 (浙江省天台县统计局)

摘要: 本文简述了 DR DOS6.0 安全系统的三种方法,即开机口令、文件和目录口令、临时口令,及这三种口令的解除方法。

DR DOS 6.0 具有许多新特点,它先进的磁盘管理、内存管理和微机安全系统,是到目前为止所有 DOS 系统所没有的,这为它赢得了许多用户。

DR DOS 的安全系统提供三个功能:

(1)开机口令。分主口令和用户口令二个,开机时系统提示输入口令;要求验证用户的使用权。此时,只要输入其中一个口令,即可进入系统,正常使用机器。当用户需要更改口令或废除时,则要求输入主口令,主口令只由系统管理员掌握。当机器设定开机口令后,不知口令者,不能从硬盘启动,用软盘启动不能进入硬盘,有效地保护了硬盘中的信息。

开机口令在安装 DR DOS 时设定,或用 SETUP.EXE 设定或更改,设定开机口令后,系统自动在根目录下 CONFIG.SYS 文件中加上一行
INSTALL= C: / DRDOS / LOGIN. EXE C:
\DRDOS, (假设 DRDOS 系统文件装在 C:
\DRDOS 目录),因此,启动时不能用 Ctrl+Break 中断而绕过口令检查。

(2)文件和目录中的口令。一台数人共用的机器,为了保护自己的数据不被他人窥看和修改,系统提供了文件和目录的口令验证功能。对于文件,可以对它的读、

写、删除进行不同级别的保护;对于目录,不知口令者不能进入。

此项功能用 PASSWORD.EXE 文件实现,格式为:

PASSWORD 文件名 / 开关: 口令

(3)临时口令。当使用者临时离开机器,不想关机,而又不愿被他人使用机器,可使用此功能,要重新使用机器时,打入正确的口令即可。

在 DOS 提示符下,打入 LOCK 后跟口令即可设置此项功能,格式如下:

LOCK 口令

笔者通过对这三种设定口令的分析,破解了以上三种保护方式。

三种保护方式中,最重要的是开机口令。如果没有开机口令,则临时口令也失去作用,只要重新启动即可。

用其它 DOS 版本在软盘启动,这时不能转到 C 盘工作,也就是不承认逻辑盘 C,但此时我们仍可用其它方法读写物理盘的绝对扇区。运行 Norton 软件中的 NU(4.5 版)或 DE(5.0 版),用绝对扇区方式读出硬盘的主引导扇区(0 面 0 柱第 1 扇区),在分区表方式下,发现系统类型都改成“?”,如下表所示:

Side 0, Cylinder 0, Sector 1

Partition Table format

Partition Table Editor

System	Boot	Starting location			Ending location			Relative Sectors	Number of Sectors
		Side	Cylinder	Sector	Side	Cylinder	Sector		
?	Yes	1	0	1	4	770	17	17	65518
?	No	0	771	1	4	975	17	65535	17425
?	No	0	0	0	0	0	0	0	0
?	No	0	0	0	0	0	0	0	0

(下转第 45 页)

(上接第 46 页)

这时,可将各个分区的系统类型改变为 DOS—16、DOS—12、BIGDOS 或 EXTEND 中的一个(根据各分区实际占有扇区数而定),将修改的数据存盘后,重新用硬盘启动,此时不再提示输入口令,启动成功后,可用编辑工具将 CONFIG.SYS 中的 INSTALL= C:\DRDOS\LOGIN.EXE C: / DRDOS 这一句删除,开机口令的解除即告完成。

文件和目录中的口令解除有二种方法:

(1)用 MS DOS 3.30 以上版本从软盘启动,此时硬盘中的文件及子目录口令即失效,对加了口令的文件,可用 COPY 命令复制一个副本,删除原文件,再将副本改为原文件名,因为经复制的文件不再保留口令。对于加了口令的子目录,可在该子目录的上级目录建立一个新的子目录,将加口令子目录下的文件全部拷贝或移动到

新子目录下,删除原子目录,将新子目录名用任何一种工具改为原目录名。这时,用 DRDOS 重新从硬盘启动后,就不再有口令了。

(2)加了口令的文件或目录,实际上只是更改了文件的目录项,每个文件的目录项有 32 字节,前 11 字节是文件名和扩展名,第 12 字节是文件属性,第 13-22 字节一般为 DOS 保留未用。未加口令时,一般文件的属性字节是 20H,子目录是 10H,加口令后,其属性字节 1 位置 1,即将文件或子目录的属性改为隐含,故分别变为 22 和 12。同时将目录项的第 15、16 字节改为口令值,第 21、22 字节改为口令种类,解除口令的过程相反,将目录项的属性字节改为非隐含,即 22 改为 20,12 改为 10,将目录项的第 15、16 字节改为 0(表示口令字空)或者将 21、22 字节改为 0(无口令)即可,这一过程用 NU 或 PCTOOLS 均可实现。