硬盘数据保护策略分析

黄 红 曾纪粤 黄 超 （华中理工大汉口分校自控系）

摘要：本文介绍了公用计算机房的硬盘数据的网络、软件及硬件的维护策略，以及它们的工作原理和优缺点。

关键词：硬盘 系统 BOOT ROM 远程启动 硬盘分区表 区域保护硬盘锁硬盘保护卡 Windows NT

一、运用 WINDOWS NT 网络远程恢复系统

目前新建成的计算机房大多采用WINDOWS NT 网络管理，工作站均使用 WINDOWS 95/98 操作系统，各工作站通过集线器、交换机等设备与服务器相联，我们完全可以通过网络来恢复系统受到破坏的工作站。

1. 用 BOOT ROM 技术远程启动工作站

利用BOOT ROM登陆网络的工作站，其网卡上必须安装以RPL（Remote Initial Program Load ）方式运行，且支持WINDOWS NT 的BOOT ROM 。以我们机房为例，采用的网卡可加装一块2029 BOOT ROM 芯片。首先在WINDOWS NT SEVER 上安装并启动“远程启动服务”，然后安装利用BOOT ROM 启动的工作站所需的MS-DOS 操作系统和WINDOWS 95/98操作系统，以后工作站上的WINDOWS 95/98操作系统的安装，就可以利用此SBS（Server-Based Setup）服务器内的WINDOWS 95/98文件。如果要将工作站设置成用BOOT ROM启动，则在工作站上执行RPLENABL.EXE 程序。工作站登录以后，C盘是一个虚拟的磁盘，它映射到远程服务器中的一个目录，而不是真正的C盘，并且工作站的硬盘映像文件也保存在里面。而工作站上硬盘分区的磁盘代号被改为由D开始。远程启动工作站启动时，使用的是NetBEUI通信协议，也可添加TCP/IP、DLC、与IPX协议。一旦某工作站系统受到破坏，则开机后直接按DEL 键进入 CMOS 设置，改 BIOS 中的 LAN BOOT FIRST 为ENABLE，就可直接登录到 WINDOWS NT SEVER，然后在服务器端运行Norton Ghost Server，在工作站运行Norton Ghost，通过广播方式将工作站的硬盘映像同时恢复到每台工作站的硬盘中，从而达到恢复工作站操作系统的目的。

2 用 WINDOWS NT SEVER 制作 DOS CLIENT 启动盘登录到 WINDOWS NT SEVER

通过NT4.0安装光盘，可以制作DOS CLIENT启动盘。启动盘制作成功后，就可以通过它启动工作站到DOS方式，并登录到WINDOWS NT SEVER，将存放有工作站的硬盘映像文件的目录映射成网络驱动器。然后可利用Norton Ghost 来恢复工作站的操作系统（方法同本地恢复）。

以上两种方法都必须在WINDOWS SEVER的某个分区内安装由WINDOWS 95/98工作站所需的系统软件和应用软件所构成的映象压缩文件，然后通过GHOST程序恢复被破坏的工作站。其优点是：若机房内每台计算机均成功登录到WINDOWS NT SEVER ，则可采用广播方式来恢复工作站，这样对大批量的工作站恢复，时间短，效率高。其缺点是：过分依赖网络，一旦网络出问题，则只有开机箱进行硬盘对拷，工作量相当大。再者，对每一个使用者来说，他的读写权利不受任何限制，系统被破坏的概率大大增加，GHOST的次数也大大增加。

二、用软件保护硬盘数据安全

1 用被软件隐藏的硬盘分区来恢复系统

这种方法首先对每个WINDOWS 98 工作站的硬盘用FDISK进行分区，一般分为二个区，C区装有系统文件和一些常用的软件，D区装有C区的映象压缩文件。再用软件备份硬盘分区表，并隐藏D区，使上机人员看不到D区；一旦C区受到破坏，即可用软盘启动，利用软件恢复硬盘分区表，解锁D区，再用GHOST程序，选择

PARTION to PARTION，恢复C区内容。隐藏D区的C语言程序主要部分如下：

```
/*read CYLINDER 0,SECTOR 1,HEAD 0,DRIVE 80H to buffer*/
if (biosdisk(0x02,0x80,0x0,0x0,0x01,0x01,buffer)==0)
{
    printf("\nSucceed to Read Disk D information!");
}
else
{
    printf("\nFail to Read Disk D information!");
}
/*clear D partion information*/
for (i=0x1CE;i<0x1DE;i++)
{
    buffer [i] =0;
}
/*write buffer to CYLINDER 0,SECTOR 1,HEAD 0,DRIVE 80H*/
if (biosdisk(0x03,0x80,0x0,0x0,0x01,0x01,buffer)==0)
{
    printf("\nSucceed to Lock Disk D information!");
}
else
{
    printf("\nFail to Lock Disk D information!");
}
```

这种方法的优点是：不依赖于网络即可恢复系统，快捷方便。其缺点与“网络远程恢复”方案类似，因为C区不受任何保护，则管理员做GHOST的次数一定不少，如果使用者使用FDISK命令，那么它所带来的麻烦就更大了（C语言的源程序ProtectD.zip可到http://pophard.top263.net/下载）。

2 区域保护硬盘锁

硬盘的逻辑驱动器是由MASTER BOOT的分区表来决定，一个硬盘可以分成C、D等多个逻辑驱动器。如果要做到只对第一逻辑驱动器的保护就必须算出第二逻辑驱动器开始的柱面，然后改写驱动器的中断程序，使用它只拦截第一逻辑驱动器的写操作。其检查操作如下：

```
CHECK:
CMP DL，80H      ；若不为C盘
JNE     CONTI    ；则继续
PUSH    CX       ；保留CX及DX值
XCHG    CH，CL   ；
AND     CH，11000000B；取得CH最高两个BIT
MOV     CL，6    ；
SHR     DH，CL   ；使DH向右移位6BIT
CMP     DX，WORD PTR CYL ；判断是否超过
POP     DX       ；
POP     CX       ；超过表示为D盘，不写保护
```

使用区域写保护有以下三个文件：HDLOCK.EXE，SETPASS.EXE，HDREMOVE..EXE。这种方法的优点是：经济、可靠、方便，只要安装了区域写保护程序，对DELETE、FORMAT，甚至破坏力最强的FDISK都可有效制止。其缺点是：安装硬盘锁时不能使用其他硬盘保护软件和防毒程序。

3 用“美萍电脑卫士”保护系统和硬盘

“美萍电脑卫士”是可在网上下载的共享软件，其保护原理是：通过修改WINDOWS操作系统的注册表、MSDOS.SYS文件和底层的VxD(Virtual Device Driver)来限制用户部分操作权限，好像在WINDOWS外加了一层“外壳”，从而达到不允许用户任意添加和删除操作系统和各种软件的目的。使用美萍电脑卫士的优点是：获取容易，价格低廉，所有要用的程序都以快捷方式出现在桌面上，既一目了然又方便快捷；其缺点是：在纯DOS环境下，“美萍电脑卫士”的保护性就荡然无存，而且在WINDOWS环境中的性能也不太稳定。

三、采用硬盘保护卡保护

硬盘保护卡是将保护程序固化在ROM BIOS上，不易修改，是一个良好的维护策略。计算机启动时会对640K以上的接口卡内存区做扫描，当发现在该段内存的某地址中存有AA55H两个十六进制值时，则将以CALL FAR形式跳到下一位置执行。硬盘保护卡把负责拦截INT 13H驱动器中断的程序固化在EPROM中，然后将EPROM地址解码于A000H至F000H间未用到的区域，

扫描程序在扫描640K以上内存时，一旦发现AA55H值，则跳到EPROM中程序开始的地址位置，并执行拦截INT 13H驱动器中断的程序。保护卡大多可以利用跳线JUMPER的方法更换EPROM的地址，此后所有的对硬盘的写入或格式化的操作都被拦截，从而达到其保护的目的。

以将硬盘分为C、D两个区为例，用保护卡保护装有系统的C区，而将D区则作为资料盘开放。它的优点是既能防写入、DELETE、FORMAT、FDISK，还能防止某些病毒的感染。缺点是临时需要装入软件较麻烦，若系统被某些病毒感染时，只能采用硬盘对拷的方式来恢复系统，而且存在某些硬盘保护卡和某些板卡不兼容的问题。

综上所述，各种硬盘数据保护方法各有优缺点，我们必须扬长避短，综合运用。比如可以将硬盘分为三个区，采用硬盘保护保护系统盘C盘，D盘作资料盘，E盘上放C盘的压缩映象文件，采用硬盘隐藏技术隐藏E盘。建立WINDOWS NT 网络的远程和本地登陆系统。这样常规情况下，C 盘不会受到破坏；万一被破坏即可采用解锁E盘恢复系统的方法，也可采用网络远程恢复系统的方法。■

参考文献

1 戴有炜、陆年德、王明华等。《WINDOWS NT4.0 SEVER 中文版 专业指南》清华大学出版社 1997年7月

2 高云庆 《硬盘保护技术手册》人民邮电出版社 1996年3月