实现计算机机房的科学管理

□陈家松　　徐济仁

摘要：高校学生机房的管理是公认的难题，上机制度甚至严厉的处罚措施都不足以杜绝误操作者或敢于"以身试法"者对系统安全的危害和破坏。唯有采取有效的措施，才能确保机器、系统安然无恙。

关键词：系统安全 虚拟盘 超级保镖2000

中图分类号：G47

高校学生机房的管理是公认的难题。上机制度甚至严厉的处罚措施都不足以杜绝误操作者或敢于"以身试法"者对系统安全的危害或破坏。唯有采取有效的技术措施，才能确保机器、系统安然无恙。下面是笔者的一些经验。

对策一：无盘工作站＋虚拟盘--不花钱，多办事

此策适用于至今仍采用MS－DOS平台工作的学生机房。这类机房一般采用Novell无盘工作站形式进行管理，即将所有机器的软驱、硬盘都去掉，一来可以大大降低系统造价；二来可以防止学生用软盘传播病毒；三来防止机房中的软件被人擅自拷贝。只要网络权限设置得当，这种方案在系统安全性方面应该说是无懈可击，但其弊病也很明显。因为没有软驱，学生无法学习软盘的使用。其次由于没有软驱，只好在网络上给学生开设工作目录。而面对众多学生，如果每人开一个目录，势必使网络不堪重负。如果公用一些目录，那么学生编写的程序、文档等可能被其他人随意删改。还有一个问题，就是有些软件如Pctools、KV300＋等必须有物理盘才能使用。所以笔者认为Novell工作站不配置软驱实在是弊大于利。

那么，对有软驱的工作站，如何解决系统防病毒和软件资源不流失问题呢？实践证明，可以通过在工作站上生成虚拟盘的方法得到完善解决。具体方法是在制作工作站远程引导盘时，保证其config.sys文件中有以下内容：

```
device=himem.sys

device=emm386.exeautoram

dos=high，umb

files=70

buffers=20

devicehigh=ram

ive.sys1500/e
```

其中前三行是为了优化内存，files=70和buffers=20是为了满足等级考试对系统设置的要求，而最后一句的作用就是在工作站上生成一个与1.44MB软盘容量相当的虚拟C盘。然后用dosgen命令生成无盘工作站远程引导文件net＄dos.sys，存放在服务器的sys:login目录下。同时使用户注册正本内容只有以下两句：

```
map

ivec:
```

这样，学生开机后，通常情况都是通过网络远程引导启动，注册入网后则自动转到虚拟?quot;C盘"。一般学生上机练习时产生的文件只存放在这个虚拟盘中，在重新启动后自动消失，免除了管理员经常清理垃圾文件之劳。

如果有必要长久保存文件（如未完成的程序等），可由学生用软盘拷贝带走。由于学生用户在网络服务器上没有可用空间（只要在建立学生用户时不为之建立用户工作目录，并在用户帐户中将其在服务器磁盘上的最大可用空间设为0），加上网络权限限制，即使学生带来的软盘本身有病毒，也只传染虚拟的"C盘"，而这个虚拟盘在重新

启动时会自动销毁一切所存数据，包括在它上面的一切病毒程序，所以完全不必担心学生盘上的病毒危害系统的安全。

为了防止学生通过软盘拷贝网络上保密的程序，可在有关程序所在的目录下执行以下命令：

flag＊.＊rox

该命令将所在目录下所有可执行文件设置为"仅执行"（X）属性和"只读"（Ro）属性。设置为仅执行属性后的.exe和.com文件只能执行，无法拷贝到其他位置，但可以被移动到其他位置，加上Ro属性后就无法移动了。当然，这些目录的A权和M权不能授予学生用户，否则其中的网络高手可以解除这些属性限制。

对策二：超级保镖＋FAT32－－少花钱，办实事

此策适用于采用Windows9X平台工作的学生机房。这类机房中的各台机器均配有硬盘（也有人采用无盘联网形式，但站点一多运行起来就慢如蜗牛，几乎失去实用价值）。于是一个令人头痛的问题就出来了--学生可以随意删改本地硬盘上的各种文件和系统设置。

为了解决这个问题，不少学校机房或采用加插硬盘保护卡的方法来防止和消除学生对系统的修改，或采用硬盘克隆技术来尽快恢复被毁坏的系统。但实践表明二者均有明显不足之处。加插保护卡首先要增加机器成本，其次会降低系统运行速度（至少部份产品如此），更使人感到不便的是要占用一个扩展槽。现在不少电脑扩展槽数量不足，装上网卡、声卡等后可能就没有多余的槽可用，也容易引起中断冲突等软故障。采用克隆技术则纯粹是"亡羊补牢"之举。实际上，克隆技术更适用于成批购买新机时系统的快速安装，用于学校机房的技豕芾恚　翟谥皇且恢治弈沃　嗟牟咕榷　选?br> "超级保镖2000"软件的推出为机房管理带来了新的曙光。用户可以将硬盘分成系统区（一般为C盘）和用户区，让超级保镖只保护系统区。属于超级保镖保护范围内的文件系统不管遭到多么严重的删改，只要在启动时按下F10键并输入正确密码，就可以完全恢复到超级保镖初装时的原始状态。对于超级保镖安装后修改过的或新建的文件，可通过其"高级设置"及时加以补充保护。

我们在使用中发现超级保镖实际上是将系统原始状态通过各个硬盘的T!A和T!B目录进行保存，这也许就是超级保镖所谓"整体写保护"的秘密所在。由于采用特殊技术，这两个重要目录在Windows下（包括MS－DOS方式或启动时进入命令状态）是完全不可访问和查看的，但是如果机器启动时学生按下F8并选择PreviousversionofMS－DOS，或用DOS软盘启动，就可以访问这两个目录，并对其文件进行删改，以此攻破超级保镖建立的系统防线。

了解了这一秘密，就可以采取措施来堵塞这一漏洞。我们采取的方法很简单--把欲保护的硬盘分区设置为FAT32（FAT32分区是MS－DOS无法访问的）。设置为FAT32分区后，还可以加快硬盘读写速度，增大硬盘存储空间。

对策三：NetWare5＋ZENworks－－花大钱，办大事

此策既适用于Windows9X平台环境，也适用于WindowsNT平台环境。

ZENworks是Novell公司为解决Windows平台用户桌面管理而推出的所谓"零管理"软件。ZEN works以NDS目录服务为核心，将Windows系统配置（注册表、系统策略等）作为NDS的对象库进行统一管理调配，而将Windows9X/NT工作站固化成一个只执行相关应用程序的所谓"瘦客户端"，从网络上实现对桌面系统的彻底管理。

当用户进行NDS网络登录认证后，NDS自动将Windows配置对象库的参数复制到Windows工作站上并立即生效，桌面配置被改写，应用程序自动到达用户机上，形成统一桌面设置（统一壁纸、统一屏幕保护、统一鼠标等），并能实现应用程序的自动分配和自动复原。如果用户端软件环境被破坏或关键文件丢失无法启动，只要用户登录网络，丢失的文件会自动从网络上复制到用户机上，从而保证用户机的正常运行，而这一自动修复过程完全不需要管理员介入。而且用户不管从哪台机上登录网络，其桌面设置保持不变。

这套系统还有一个很出色的功能，特别适用于学校机房，即必要时可针对不同用户登录情况分发相应的应用软件，使学生机由多任务的Windows进程变成单任务教学环境。如规定第一节上Word，第二节上Access，第三节上网页制作，管理员可在不同时段分配相应的应用程序Word、Access和Front Page，这样在规定时间内学生只能使用指定的应用程序，从而防止学生上机时"不务正业"或进行恶意破坏。

（作者单位：解放军电子工程学院合肥230037）