Windows 平台下基于 HPA 的 Ghost 技术①

陈君臣 王成良 (重庆大学 计算机科学与技术系 重庆 400044)

摘 要: 基于HPA的windows平台下系统备份与还原技术的研究与设计是军队信息化建设项目(军用终端保护系统)中的核心内容，解决了 ghost 软件 Dos 下执行的缺陷，并实现了利用 HPA 技术分区隐藏系统备份文件，使操作系统备份与还原软件技术向前迈进了一个新阶段，同时为军队信息化建设提供了可靠了保障。软件最终性能表明：基于 HPA 的 windows 平台下系统备份与还原技术完全达到了预期效果，能足够满足军队信息化建设需求，同时相比 ghost 软件，性能和用户体验得到了巨大提升。

关键词: HPA; 系统备份; 系统还原; 虚拟文件系统; Ghost

Ghost Technology Research Based on HPA Space in Windows Platform System

CHEN Jun-Chen, WANG Cheng-Liang

(Dept. of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: In this paper, the windows platform backup and restore technology Research and design based on HPA for military construction projects (military end-protection system), the core content addressed the defects of ghost software which running under Dos, and implements the use of HPA technology hidden system partition backup file, forward the operating system backup and restore software technology to a new phase, while provided a reliable guaranteed the military information construction. The final performance of the software that: system backup and restore under the windows platform and Based on HPA technology is completely achieved the expected results, provide sufficient information to meet the building needs of the armed forces, while compared to ghost software, performance and user experience has been a huge boost.

Keywords: HPA; system backup; system restore; virtual file system; Ghost

1 引言

Windows 系统的稳定性和安全性一直是人们关注的主要方面，目前操作系统备份产品使用比较多的有国外软件 ghost、Acronis TrueImage 等,国产软件有一键 GHOST 等,但它们都是依赖于 ghost 内核。

文中提到的基于 HPA 的 windows 平台下系统备份与还原技术(运用于国防信息化建设项目-军用终端保护系统)是具有知识产权并解决了 ghost 在 dos 下运行的缺陷，磁盘划分 HPA 空间存放备份文件，增强了数据的安全性，同时打破了此类国内同行软件依靠国外内核的现状。提高了军队信息化建设的水平。

2 HPA技术

HPA[3]是 Hidden protected area 或 Host protected area 的缩写，隐藏保护分区的意思。HPA 是在 ATA/ATAPI-4 里面定义的一个区域，在 BIOS 可见空间之后，BIOS 访问不到。但是可以通过直接发送 AT 命令的方式访问。在实现方面可以利用 Device—oCtrl()函数来发送 IO 控制码来驱动磁盘驱动程序来实现我们目的。

2.1 基于 HPA 技术的一键恢复系统的优势

HPA 技术可以提供用户级安全性保护，以全面保护 HPA 分区不被未授权用户访问、修改及删除.非 HPA

① 收稿时间:2010-03-17;收到修改稿时间:2010-04-13

技术的磁盘备份与还原的缺点：a、隐藏分区可被破坏、删除，造成无法成功恢复系统。b、隐藏分区必须为一个主分区，会对用户造成一些不便。

基于 HPA 技术的一键恢复系统的优势：a、HPA 技术可以提供用户级安全性保护，以全面保护 HPA 分区不被未授权用户访问、修改及删除。根据白皮书上提供的安全性对应表来看，在最高等级的安全性下，无法访问、看到、删除 HPA 分区，无法克隆。b、不必占用一个主分区，其解决了 ghost 备份后的文件在主分区。

2.3 HPA 分区内部虚拟文件系统结构

2.2 HPA 空间调整

HPA 一般在磁盘的末尾区域，但是根据不同磁盘的分区结构的不同，也可能造成尾盘空间不能划分到 HPA 空间。使用 HPA 时会对磁盘大小进行调整,常见的调整方式有以下两种：一是将可见空间划分至 HPA,二是将 HAP 空间划分至可见空间。

可见空间 è HPA：在格式化,创建 HPA ,扩展 HPA 空间时都可能发生。a.只有在空间足够，数据写完后才能卸载卷—>设置 Max 地址- - >跟新分区表信息。b.凡是使用了扩展分区的空间都要调整分区表。

HPA è 可见空间：这也叫：回收空间．有两种情况：a.尾盘有效且其后无可用空间或未分配空间，则回收至尾盘。b.尾盘无效则回收成未分配空间．

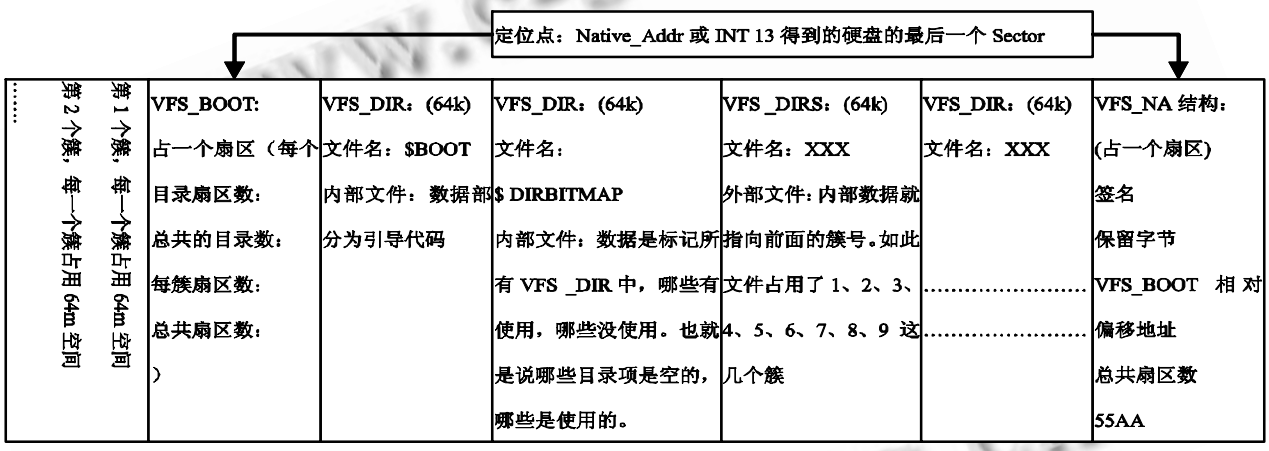

图 1　HPA 分区内部虚拟文件系统结构

图上描述的是 HPA 空间内部文件存放方式(VPF)，VFS_BOOT 相对磁盘 Native 地址的间隔为固定大小，其占用一个扇区，存放一些基本数据信息,包括 HPA 区域中总共的目录数、每簇扇区数、总共扇区数等信息。其后的一个扇区存放的为引导代码。此引导代码可以启动起 HPA 中的操作系统(在没被压缩保存的情况下)，紧接的下一个扇区是描述后面的目录使用情况的目录位图，为 1 是表示使用，为 0 表示为空(没有使用)。再后面是目录项，其中存放此目录使用了那些簇号。最后一个扇区存放的签名标识、VFS_BOOT 相对偏移地址和总共扇区数、磁盘末尾标识 55AA.VFS_BOOT 前面是簇，每个簇的大小为 64m 空间。此设计结构式 fat32 文件系统的简单化设计，完全能够满足我们必要的存储和读取操作。

3　系统备份与还原软件体系结构

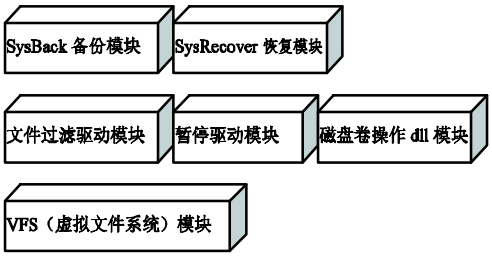

图 2　系统备份与还原软件体系结构

3.1 基本的磁盘卷操作

对磁盘的某个扇区进行读写[4]，与使用

CreateFile()函数与对串行端口的访问类似，需要用与文件存放路径相类似的方式指出要操作的硬件设备(硬盘)。这里需要以某种特定的格式来指定需要访问的磁盘逻辑分区。对于逻辑分区 X，其格式为”\\.\X:”。

HANDLE CreateFile(LPCTSTR lpFileName, DWORD dwDesiredAccess,DWORD dwShare Mode,LPSECURITY_ATTRIBUTES lpSecurityAttributes,DWORD dwCreationDisposition,DWORD dwFlagsAndAttributes,HANDLE hTemplateFile);

通过 CreateFile()打开的是整个磁盘逻辑分区，要操作的是该分区的某些扇区，还要通过 SetFile Pointer()函数以文件操作的方式把指针移到要操作的磁盘扇区开始处。SetFilePointer()函数原型为：

```
DWORD SetFilePointer(
HANDLE hFile,
LONG lDistanceToMove,
PLONG lpDistanceToMoveHigh,
DWORD dwMoveMethod);
```

参数 hFile 为 CreateFile()返回的文件(设备)句柄；lDistanceToMove 和 lpDistanceToMoveHigh 指出了要设置偏移量的低端和高端部分；dwMove Method 指出文件指针从何处开始移动，可能的选项有 FILE_START(从文件开始)、 FILE_END(从文件结尾)和 FILE_CURRENT(从文件当前位置)。在定位到要访问的扇区开始位置后就可以通过 ReadFile()或 WriteFile()函数实施相应的读写访问了，具体操作与文件读写并没有什么太大的差别。最后，在完成访问操作后以 CloseHandle()关闭文件句柄释放资源，从而完成一次完整的磁盘扇区数据访问操作。

3.2 驱动模块设计

驱动模块主要是文件过滤驱动[3]和暂停驱动[5]，主要目的是当执行备份操作系统分区的时候保证数据的完整性。文件过滤驱动主要的功能是处理我们自己定义的 IOCtrl 操作码，这些操作主要功能是对 HPA 区域中的文件操作。

3.3 VFS 模块

Vfs(virsual file system)虚拟文件系统模块，此文件系统是为了对备份数据的存储和读取做定位和查询操作。(见 3.3 图 1)。实现了基本的文件系统所有接口。基于 fat32 系统并结合了我们的实际需求简化了相关操作。

4 系统实现

4.1 实现系统备份主干流程

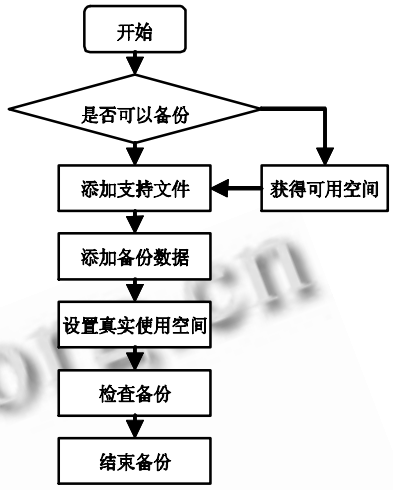

图 3 系统备份主干流程

系统开始备份前，先关闭 ShellHWDetection 服务和互斥加锁磁盘分区管理器，在备份完成或中途失败是对其进行相反操作。系统在整个备份过程中像大部分软件使用一样,不需要重新启动进入到 dos 平台。同时在备份过程中我们完全做其他系统操作和文件操作，因为我们使用图二的驱动技术。

检查是否可以备份方法：主要是检查 HPA 是否有足够空间，流程如下：a.获得需要备份的扇区数，b.获得 HPA 空闲空间扇区数，c.比较并返回，如果有足够空间则转添加支持文件，否则获得可用空间。

获得可用空间流程如下：a.整理尾盘数据文件(前移)，b.可用空间->HPA 空间(见 2.2)磁盘空间调节，c.初始化虚拟文件系统 vfs。设置好相应标识。

设置真实使用空间：a.获得备份真实使用的空间，b.重新分区，c.重写分区表中卷的名字(为了防止分区表被破坏)d.更新磁盘分区表，e.设置 MaxAdress[3](此地址为 window 系统可见的磁盘最大空间的地址)，f.更新磁盘大小(系统非可见区域为 HPA 区域)

4.2 实现系统还原主干流程

初始化操作主要是获得系统分区号，Max 地址，native 地址，初始化 Vfs(图 1 中 VFS_NA 结构)，将 HPA 区域作为一个系统卷，通过改写主引导扇区，指明磁盘的活动分区的信息为 HPA 所在分区信息，进入虚拟平台，启动 HPA 中的系统，然后把虚拟平台下的

系统分区写到原来的系统分区。同时改变主引导记录，这样再下次操作时，实现了我们还原系统的目的。同样我们不需要进入 dos 平台做任何操作，大大的简化了用户的使用。

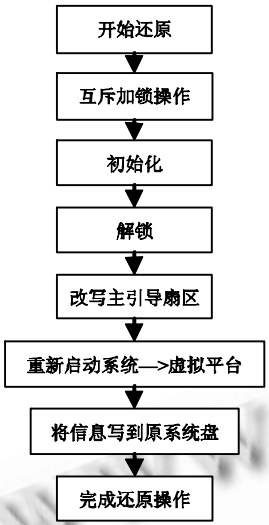

图 4　系统还原主干流程

5　结束语

目前的软件测试效果来看，第一解决了 ghost 的缺陷，既需要在 dos 系统下运行，第二系统在用户体验和稳定性上做出了很大的提升，避免了前 ghost 产品备份的系统使用异常。总体来看我们打破内核技术国外垄断现象，同时为国防信息化建设提供了安全保障。但是软件在研究和设计中只考虑了备份系统所在分区，并没有考虑系统分区之外其他分区的情况。软件设计中表现层和功能并没有完全分开，模块中出现了交叉耦合现象，影响软件后期扩展开发。在软件工程方面，由于前期开发时间的紧迫性，程序的易读性相对比较差。模块粒度比较大。随着操作系统的不但升级，内核的升级会影响到软件的部分功能模块。接下来需要继续处理的事情就是在主要功能模块下添加附加模块，完成整个系统设计。

参考文献

1 张宗伟.基于 Windows 9x / NT 内核操作系统下的磁盘备份与恢复的实现与研究[硕士学位论文].上海:东华大学, 2004.

2 James K, McGill, III, Dover. Disk operating system backup and recovery system. Patent Application Publication, 1993.

3 Maxtor Corporation. Information technology AT attachment with Packet interface-5(ATA/ATAPI-5), 2000-02-29.

4 宋群生,宋亚琼.硬盘扇区读写技术-修复硬盘与恢复文件.北京:机械工业出版社, 2004.

5 张帆,史彩成. Windows 驱动开发技术详解.北京:电子工业出版社, 2008:506—520.