操作系统安全简论(续上期)
——Windows NT操作系统安全(三)

卿斯汉 (中科院信息安全技术工程研究中心 100080)

3 注册表

Windows NT将它所有的配置信息存储在一个称为注册表(Registry)的数据库中。注册表中包含了用户、应用程序、硬件、网络协议和操作系统的信息,并且替代了来自Windows 3.X中的INI文件。它使用了一个比Windows 3.X更具有扩展性和灵活的结构,其中提供了安全性配置和多用户支持。

注册表包含了许多文件,如Config.sys、Autoexec.bat、System.ini、Win.ini、Protocol.ini、Lanman.ini、Control.ini以及其他INI文件。

注册表是一个具有容错功能的数据库,一般情况下是不会崩溃的。注册表的数据结构由以下5个子树组成:

(1) HKEY-LOCAL-MACHINE:包含了最重要的信息,其中包括硬件信息,例如处理器类型、总线类型、视频,以及磁盘I/O硬件。它还包括操作系统的软件信息,例如设备驱动程序、服务、安全性,以及安装的软件。

(2) HKEY-CLASSES-ROOT:这个Registry类似于包含在Windows 3.X中功能有限的Registry,它包含文件关联的信息,将文件扩展名与一个应用匹配,相当于一个OLE类的存储器。这个子树指向存储在HKEY-LOCAL-MACHINE\SOFTWARE\Classes子项中的信息。

(3) HKEY-CURRENT-USERS:包含正在登录上网用户的信息。包括用户所属的工作组、环境变量、桌面设置、网络连接、打印机和应用程序等。

(4) HKEY-USERS:包含所有登录入网用户的信息,包括从本地访问系统的用户。远程登录的用户信息存储在注册表的远程机器中。

(5) HKEY-CURRENT-CONFIG:包含当前硬件的配置信息,由当前硬件的预置文件指定。事实上,它指向包含下述内容的子项:

HKEY-LOCAL-MACHINE\SYSTEM\Current ControlSet\Hardware Profiles\Current

每个子树都包含叫做键值的条目,每个键又有许多子键。注册表子树中的数据是由一套叫做hive的文件得来的。每个hive包含了两个文件:数据和日志文件。每个hive代表了位于注册表最顶层部分的一组键、子键和值。

Windows NT的注册表分为两种主要文件:

(1) User.dat:注册表通过这个文件存放各个用户特定的一些设置,例如用户的桌面设置和用户引导菜单的内容等。

(2) System.dat:注册表通过这个文件存放Windows NT的一般硬件与软件的设置。

注册表中设有若干保护层,保护这些文件中的数据。所有注册表文件均以加密的二进制格式存储。如果没有相应的工具和用户授权,就无法读取这些文件。使用纯文本编辑器是无法进入注册表的,也就是说,通过类似于Editor的编辑器是不能够直接编辑User.dat和System.dat文件的。

注册表文件标有只读或隐藏的系统文件之类的标记,防止被他人无意中删除或发现。此外,即使拥有管理员特权也无法删除注册表文件。用户可以通过注册表编辑器(Registry Editor)查看和编辑注册表,通过它可以修改系统底层的配置。

4 文件系统

Windows NT采用了标准的方式对文件系统进行管理,因而能够较好地支持多文件系统。为了对每一个文件系统都提供支持,Windows NT为每一个文件系统提供驱动,通过

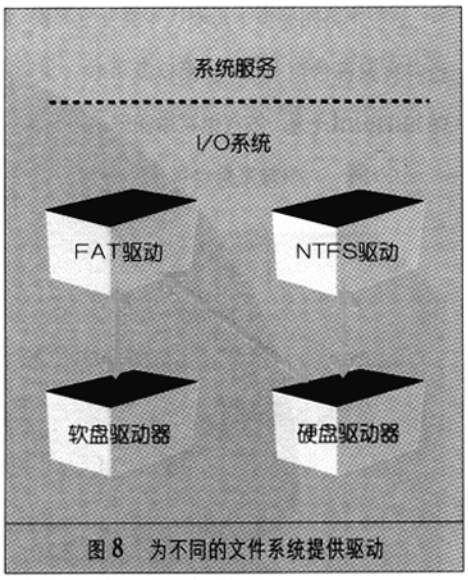

图8 为不同的文件系统提供驱动

Operating System security conspectus (III)

将低级别的驱动动态地装入系统后访问文件系统，使得对一个新的文件系统进行管理的工作，变得与在系统中再引入一个新的驱动器一样简单，如图8所示。

Windows NT支持5种文件系统FAT、HPFS、NTFS、NPFS、MSFS。前3种是传统的磁盘文件系统，后两种是用于进程间通信或是用于本地、远程进程的文件系统。

4.1 FAT (File Allocation Table)

FAT文件系统是比尔·盖茨于1976年设计的，后来应用于MS-DOS操作系统中。该文件系统比较简单，所占容量与开销很少，在小分区硬盘上运行良好。事实上，由于它的成熟和简单，几乎每一种现代个人计算机操作系统都支持它，例如：Windows 95、Windows NT、OS/2、Macintosh和UNIX。这种可移植性使FAT文件系统能方便地用于数据传送，但这也伴随着较大的不安全性。

然而，FAT文件系统的缺点比其优点要多得多：

(1) 易受损伤：缺少错误恢复技术。每当FAT文件系统损坏时计算机就要瘫痪或者不正常关机。

(2) 单用户：FAT文件系统不保存文件的权限信息。因此，除隐藏、只读之类的很少几个公共属性外，无法实施任何安全保护措施。

(3) 非最佳更新策略：FAT文件系统在磁盘的第一个扇区保存其目录信息。当文件改变时，FAT表必须随之更新，这样磁盘驱动器就要不断地在磁盘表面寻找。当拷贝多个小文件时，这种开销就变得可观了。

(4) 非最佳防止碎片措施：在需要时，FAT文件系统只是简单地以第一个可用扇区为基础来分配空间，这会增加碎片，因而增加了添加与删除文件的访问时间。

(5) 文件名长度受限：FAT文件名限制在不能超过8个字符和3个字符的扩展名。这往往不能提供有意义的文件名。

(6) 大小有限：在MS-DOS、Windows 95和Windows 98下，FAT卷限长为2GB。为了支持长文件名，在Windows 95中出现了VFAT文件系统，VFAT和FAT文件系统是兼容的。在Windows 95第二版中，出现了FAT32文件系统，这种文件系统可以支持更大的硬盘分区，并且较FAT分区而言，降低了磁盘空间的浪费程度。FAT32仅能在Windows 95第二版和Windows 98中使用，Windows NT尚不支持这种文件系统。

4.2 HPFS (High Performance File System)

HPFS是微软为OS/2 1.2设计的，支持局域网管理的文件服务器。相对于FAT文件系统，HPFS主要考虑提高可靠性和性能。它主要是通过缩短目录和数据的物理距离，以及通过数据缓冲来提高性能的。描述文件位置的表间隔地放在整个数据区。当新的数据被加入时，它们一般被写入一块足够大的空闲区域，因而减少了磁盘的碎片和磁盘的查找时间。此外，不管磁盘分区大小，HPFS总维持512字节的分配块。为了提高性能，HPFS需要在内存维护大量的数据，但是系统因而对崩溃比较敏感。当系统崩溃后，所有崩溃时的磁盘分区被标为"脏"的，在这些分区重用之前必须用磁盘检查程序对其修复。当然，随着分区的变大，这一恢复过程就越来越长。因为磁盘缓冲需要额外的内存，HPFS一般不用在小的系统中，如4-8MB的RAM系统。

相对于FAT文件系统，HPFS文件系统的另一个优点是支持长文件名，可以包含多个点和小写字母。文件名可扩展至254双字节字符。

4.3 NTFS (NT File System)

Windows NT引进了一种新的文件系统，也是微软重点推荐的文件系统，即NTFS文件系统。在NTFS中，簇是基本的分配单位，由连续的扇区组成。NTFS文件系统称为卷，它实际上是磁盘的一个逻辑分区。NTFS所支持的卷可以处于单独的硬盘分区上，也可以跨多个硬盘存在。NTFS文件系统根据卷的大小决定簇的大小，从1簇等于1扇面到128个扇面不等，当前NTFS最大可以支持232个簇的文件，因而最大可能的文件大小为248字节。

NTFS的每个卷由4个区域组成。每个卷上的前几个扇区形成了分区的引导扇区，其中包含

操作系统安全简论
——Windows NT操作系统安全(三)

Operating System security conspectus

了引导信息和代码，以及卷布局和文件系统结构的整体信息。其后是主文件表(MFT)，其中包含了该卷中所有文件和目录的信息，以及卷中可用的空间信息。从本质上讲，MFT是NTFS卷内容的清单。MFT以关系数据块表的形式组织，其中每一条记录描述了卷中的一个文件或目录，也包含MFT本身，因为NTFS将MFT看成一个文件。如果描述的文件足够小的话，则整个文件包含在MFT中，否则MFT行只包含该文件的部分信息，而其他信息包含在卷上的簇中。在MFT行中，保存着指向这些簇的指针。MFT的行包含的信息主要有：

(1) 标准的文件属性信息：包括读写属性、时间戳等。

(2) 文件名称：文件或目录的名称(长度可达255个字符)。

(3) 安全性描述符：指定文件的所有者和访问信息。

(4) 数据：即文件内容。

MFT之后一般保留1MB的空间，用来保存系统文件。其内容如下：

(1) MFT2：MFT前3行记录的镜像，用来提供MFT的冗余信息。

(2) 日志文件：用来提供NTFS可恢复性的事务步骤清单。

(3) 簇的分配位图：用来表示簇的分配情况。

(4) 属性定义表：定义卷所支持的属性类型，并表明这些属性是否可用于索引，以及是否可 在系统恢复操作中还原。

NTFS卷的最后一个区域是文件系统正常的文件区。

作为微软重点推荐的文件系统，它的关键特性如下：

(1) 可恢复性：NTFS文件系统可在系统崩溃和磁盘失效的情况下恢复。在失效情况发生时，NTFS可重新构建磁盘的NTFS文件系统，并返回到一致的状态。NTFS通过事物处理模型达到这一目的。在事物处理模型中，每个重要的文件系统修改均被看成是一次原子操作，要么失败，要么完全成功，没有中间状态。另外，NTFS保留有文件系统关键数据的冗余存储，从而，不会因为磁盘扇区失效丢失用来描述文件系统结构的数据。

(2) 安全性：NTFS使用Windows NT的对象模型实施安全性，在Windows NT支持的所有文件系统中，NTFS是唯一一个支持本地安全性的文件系统。

(3) 大磁盘和大文件：NTFS可以支持2^{64}字节大小的硬盘和2^{48}字节文件。

(4) 多数据流：文件的内容可看成是字节流，在NTFS中，单个文件可定义多个数据流。

(5) 方便的一般性索引：NTFS为每个文件定义了一组属性，文件的描述信息在文件管理系统中被组织为一个关系数据库，因此，文件可以按照任意属性索引。

4.4 NPFS (Named Pipe File System)

命名管道为进程间的高级通信提供支持。命名管道只是内存中的一部分，它提供完全双向的通道。因此，数据可以从管道的一端写入，从另一端读出，反之亦然。命名管道是用文件系统驱动实现的。

命名管道的安全依赖于存储在管道服务器端的存储控制表。当命名管道应用之前，服务器端必须连接好。因此，命名管道提供面向连接的信息传送。

4.5 MSFS (Mailslot File System)

同NPFS类似，MSFS文件系统也是通过模拟文件系统实现的，例如，数据不由磁盘写回。Mailslots提供无连接、单向的信息传送，用于数据广播。Mailslots安全的实现与命名管道类似。

未完待续