户的信息保存在lsass服务中，和网络服务器文件夹一起，用户可以通过上述两种配置拥有一个访问网络的用户名和密码。Windows Vista的储巢列表在图11-11中显示。

储巢文件	挂载名称	使用
SYSTEM	HKLM TEM	OS配置信息，供内核使用
HARDWARE	HKLM DWARE	记录探测到的设备的内存储巢
BCD	HKLM BCD*	启动配置数据库
SAM	HKLM	本地用账户信息
SECURITY	HKLM URITY	lass的账号和其他信息
DEFAULT	HKEY_USERS .DEFAULT	新用户的默认储巢
NTUSER.DAT	HKEY_USERS <user id>	用户相关的储巢，保存在home目录
SOFTWARE	HKLM TWARE	COM注册的应用类
COMPONENTS	HKLM NENTS	SYS组件的清单和依赖

图11-11 Windows Vista中的注册表储巢。HKLM是HKEY_LOCAL_MACHINE的缩写

在引入注册表之前，Windows的配置信息保存在大量的.ini文件里，分散在硬盘的各个地方。注册表则把这些文件集中存储，使得这些文件可以在系统启动的过程中引用。这对Windows热插拔功能是很重要的。但是，随着Windows的发展，注册表已经变得无序。有些关于配置的信息的协议定义得很差，而且很多应用程序采取了特殊的方法。许多用户、应用程序以及所有驱动程序在运行时具有私有权限，而且经常直接更改注册表的系统参数——有时候会妨碍其他程序导致系统不稳定。

注册表是位于数据库和文件系统之间的一个交叉点，但是和每一个都不像。有整本描写注册表的书(Born，1998;Hipson，2000;Ivens 1998)。有很多公司开发了特殊的软件去管理复杂的注册表。

regedit能够以图形窗口的方式来浏览注册表，这个工具允许你查看其中的文件夹（称作键）和数据项（称作值）。微软的新PowerShell脚本语言对于遍历注册表的键和值是非常有用的，它把这些键和值以类似目录的方式来看待。Procmon是一个比较有趣的工具，可以从微软工具网站：www.microsoft. com/technet/sysinternals中找到它。

Procmon监视系统中所有对注册表的访问。有时，一些程序可能会重复访问同一个键达数万次之多。

正如名字所显示的那样，注册表编辑器允许用户对注册表进行编辑，但是一旦你这么做就必须非常小心。它很容易造成系统无法引导或损坏应用软件的安装，因此没有一些专业技巧就不要去修改它。微软承诺会在以后发布时清理注册表，但现在它仍是庞杂的一堆——比UNIX保留的配置信息复杂得多。

微软Windows Vista已经引入了一个基于事务管理的内核，用来支持对跨越文件系统和注册表操作的事务进行协调。微软计划在未来使用该功能以避免由于软件非完全正确安装而在系统目录和注册表储巢中留下当时局部状态信息所造成的元数据讹用问题。

Win32程序员通过函数调用可以很方便地访问注册表，包括创建、删除键、查询键值等。如图11-12所示。

当系统关闭时，大部分的注册表信息被存储在硬盘储巢中。因为极其严格的完整性要求使得需要纠正系统功能，自动实现备份，将元数据冲写入硬盘以防止在发生系统崩溃时所造成的损坏。注册表损坏需要重新安装系统上的所有软件。

Win32 API 函数	描述
RegCreateKeyEx	创建一个新的注册表键
RegDeleteKey	删除一个注册表键
RegOpenKeyEx	打开一个键并获得句柄
RegEnumKeyEx	列举某个键的下级副键
RegQueryValueEx	查询键内的数据值

图11-12 一些使用注册表的Win32 API 调用

11.3 系统结构

前面的章节从用户态下程序员写代码的角度研究了Windows Vista系统。现在我们将观察系统是如何组织的，不同的部件承担什么工作以及它们彼此间或者和用户程序间是如何配合的。这是实现底层用户态代码的程序开发人员所能看见的操作系统部分，类似于子系统和本地服务，以及提供给设备驱动程序开发者的系统视图。