Windows原理与应用

5.注册表

计算机学院

《Windows原理与应用》课程组

内容提要

- 什么是注册表
- 注册表的编辑
- 注册表的结构
- …

5.1概述

- 注册表是 Windows 的一个内部数据库，是一个巨大的树状分层的数据库。
- 它容纳了应用程序和计算机系统的全部配置信息、系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据。
- 注册表中存放着各种参数，直接控制着Windows的启动、硬件驱动程序的装载以及一些Windows应用程序的运行，从而在整个Windows系统中起着核心作用。
- 注册表在Windows 中起到中介的作用，负责系统同软件、硬件、用户之间的沟通

5.2注册表的编辑

- 两个注册表编辑器
  - REGEDT32起源于Windows NT早期版本，
  - 而REGEDIT起源于Windows9x产品系列
  - 两个工具各有特色

5.2注册表的编辑-两个注册表编辑器的比较

REGEDIT	REGEDT32
使用较新的Windows95/98用户界面	使用较早的Windows3.1用户界面
可搜索：键名、值名、值内容	只能搜索键名
可以搜索并编辑远程注册表	可以搜索并编辑远程注册表
在一个窗口中显示整个注册表	对每一根键(root key)显示各自的窗口
与Windows9x的注册表编辑器很相似	与WindowsNT的注册表编辑器很相似
可以导入、导出文本文件	可以导出但不能导人文本文件
不能导入或导出二进制文件	可以导入并导出二进制文件
不提供‘’只读“模式	提供“只读”模式，但不作为缺省形式
不提供安全特性	支持完整的Windows 2000访问控制和审计
存放在C:\WINNT文件夹里	存放在C:\Windows\System32文件夹里
只完全支持Windows95/98注册表数据类型(字符串、二进制、DWORD))	支持全部Windows 2000注册表数据类型(字符串、二进制、DWORD、多字符串、可 扩展字符串、资源描述符)

REGEDIT概述

- 优点
- 不足
  - 安全
  - 特殊数据类型

REGEDIT的图形模式

注册表编辑器REGEDT32

- REGEDT32的窗口结构

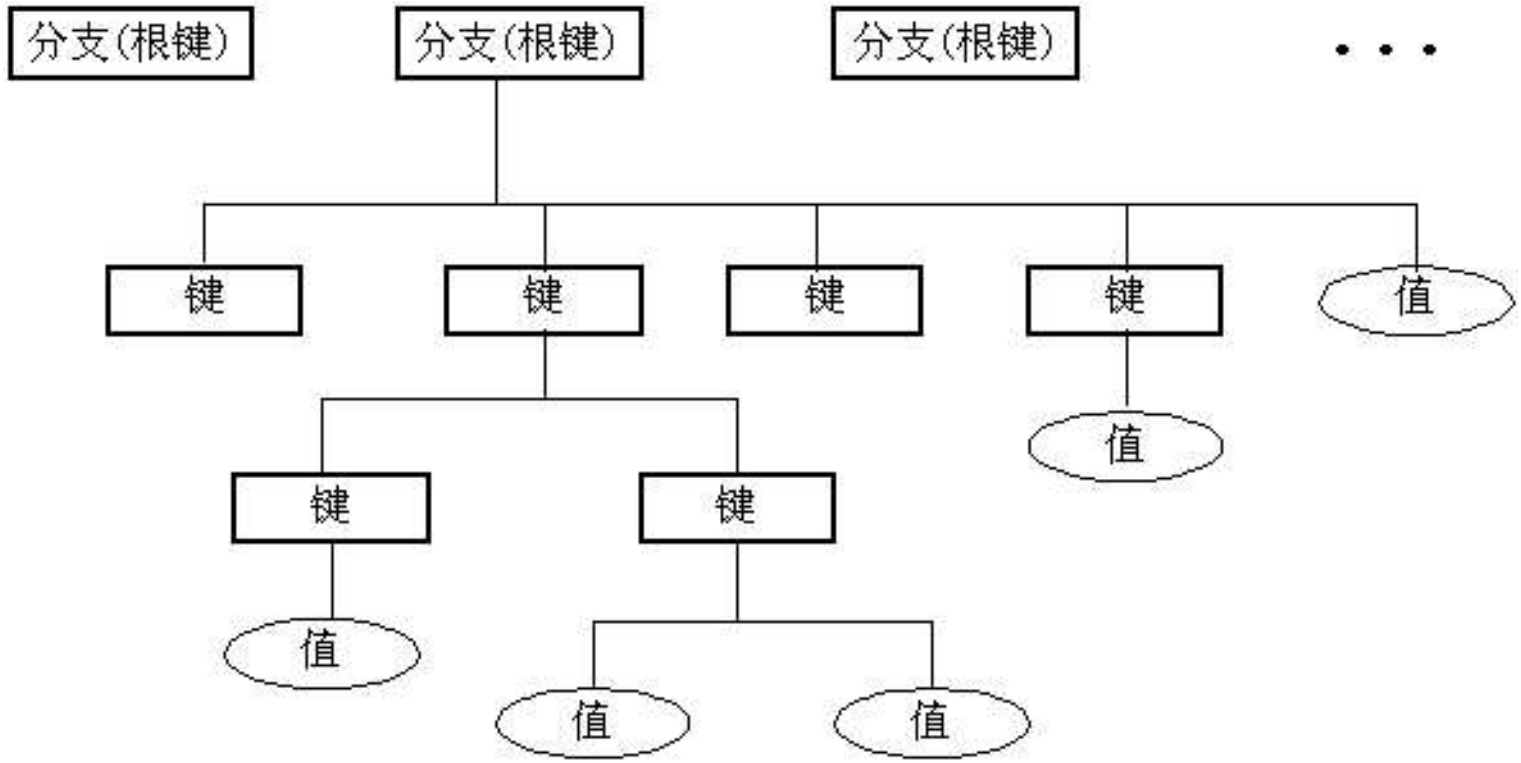
REGEDT32与REGEDIT窗口的主要差别

- 不再是一个单一的窗口，而是五个根键各有一个窗口
- 可以将五个独立窗口中的任意一个最大化，最小化，或重新调整大小，但不能单独关闭其中之一
- 没有“Favorites”菜单
- 在REGEDT32中见不到状态栏
- REGEDT32不支持右击

- REGEDT32用符号显示值类型
  - REG_SZ　　表示“字符串(string)”。
  - REG_BINARY　　表示“二进制(binary)”。
  - REG_DWORD　　表示“DWORD”。
  - REG_MULTI_SZ　表示“多字符串(multi-string)”。
  - REG_EXPAND_SZ　　表示“可扩展字符串(expandable string)”，包含一个可扩展变量的字符串。

5.3注册表的逻辑结构和内容

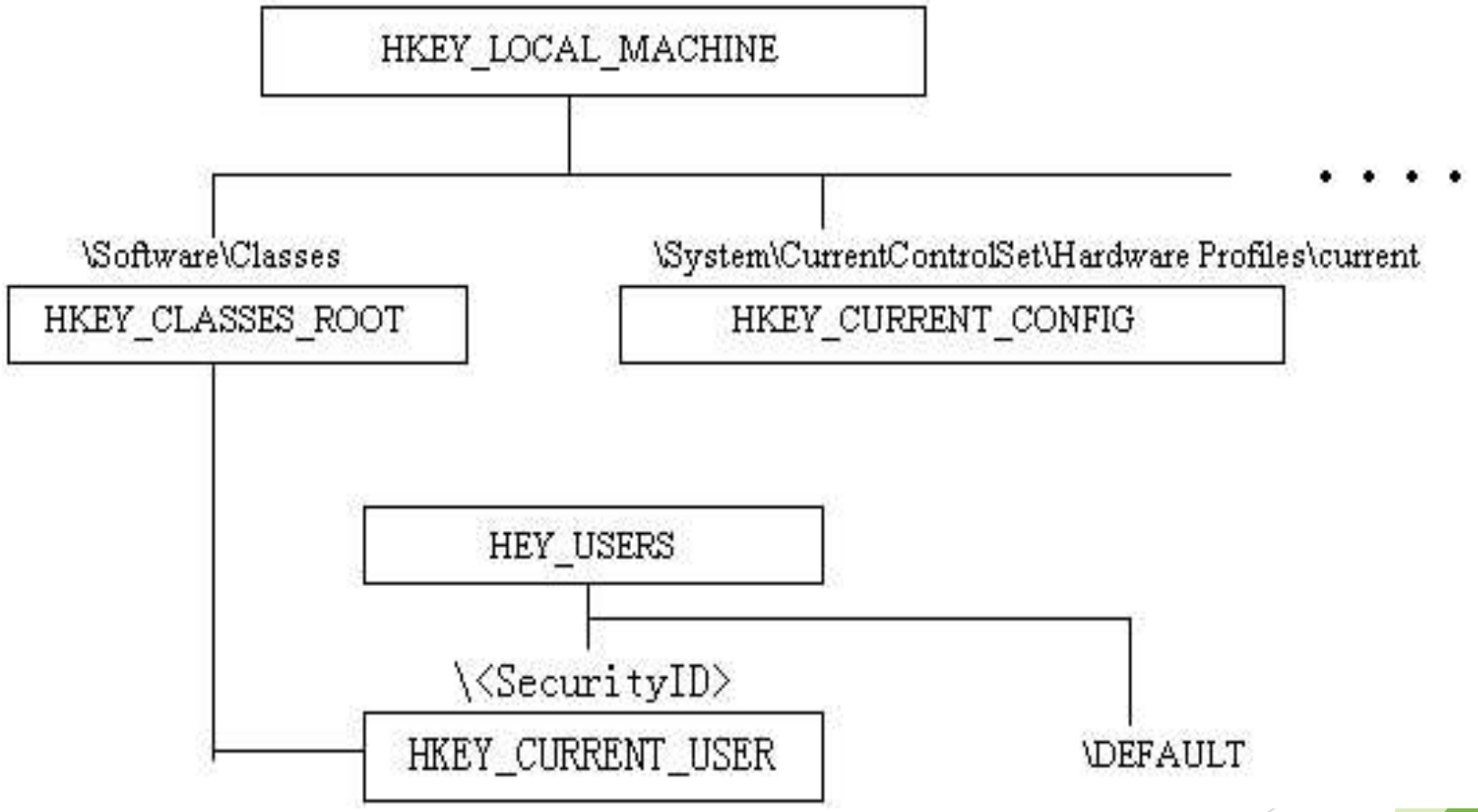
- 注册表的基本组织结构



注册表分支

分支名称	指向	缩写
HKEY_LOCAL_MACHINE		HKLM
HKEY_CURRENT_CONFIG	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current	HKCC
HKEY_CLASSES_ROOT	HKLM\SOFTWARE\Classes＋HKCU\SOFTWARE\Classes	HKCR
HKEY_USER		HKU
HKEY_CURRENT_USER	HKU\<Security ID>	HKCU

注册表分支结构的详细关系图



注册表中的值

- Windows 2000注册表使用三种类型的值：字符串、二进制及DWORD(双字)
- 在注册表编辑器里，值类型是使用前缀REG的“匈牙利语式”符号，例如REG_BINARY

注册表中的值

- 字符串REG_SZ
  - 扩展字符串 REG_EXPAND_SZ，允许用户创建含有一个系统变量的字符串
  - 多重字符串，REG_MULTI_SZ，是字符串类型的另一个变体，是注册表把几个字符串集合成为一个值
- 二进制 REG_BINARY
- DWORD值 REG_DWORD ，是一种特殊的二进制值，即四个字节的二进制值

HKEY_LOCAL_MACHINE

- HKEY_LOCAL_MACHINE(HKLM)
  - 子目录树中的设置内容是关于本地计算机系统的信息，包括硬件和操作系统数据，如总线类型、系统内存、设备驱动程序和启动控制数据。这些信息只与本地的用户有关，而与其他用户无关。
  - 包含五个子项。注意不能使用注册表编辑器修改HKEY_LOCAL_MACHINE子目录树中的SAM子项和SECURITY子项，这些子项对应的是“计算机管理器”等系统功能。

HKEY_LOCAL_MACHINE

- HKEY_LOCAL_MACHINE\HARDWARE
  - 保存了Windows 2000 系统中的所有硬件信息，系统和应用程序都是通过该项的设置与具体的硬件进行沟通。
- HEKY_LOCAL_MACHINE\SOFTWARE
  - 包含系统中软件的设置信息。由于用户安装的软件不同，该项中的设置信息也会不同。
- HEKY_LOCAL_MACHINE\SYSTEM
  - 包含系统启动需要的详细信息，包含设备的驱动程序及其配置信息、控制数据、系统分区及其他驱动器的设置信息，以及系统不能启动时，如何恢复正确配置信息。

HKEY_CURRENT_CONFIG

- HKEY_CURRENT_CONFIG子目录树是用来控制系统硬件配置信息的，它包含系统不同的硬件配置信息之间的差异。如果在系统中设置了多个不同的正确的配置文件，则系统在启动时会让用户选择要使用的配置文件。HKEY_CURRENT_CONFIG控制项代表的就是用户或用户选择的硬件配置文件，但是它只列出用户选择的配置文件与其它配置文件不同的地方。

HKEY_CLASSES_ROOT

- 为了加强对系统数据类型的管理，Windows 在注册表中组织了HKEY_CLASSES_ROOT子目录树，它包含了对数据文件类型的定义；每一种在系统中注册过的文件类型，都会在此建立一个子项。在每一个子项中定义的数据文档的扩展名、扩展名的说明性文字、在文件列表窗口中显示的图标以及与数据文档关联的应用程序和应用程序对数据文档的操作方式。如果用户要动手注册新的数据文档，可以在HKEY_CLASSES_ROOT中创建相应的子项。

HKEY_USERS

- HKEY_USERS子目录树是用来控制用户配置文件的，它包含所有用户的配置文件的内容。每个用户都会在HKEY_USERS项中有一个子项，该子项的内容和HKEY_CURRENT_USER项的内容相似，具体功能也相同，只是使用子项的用户不同。

HKEY_CURRENT_USER

- HKEY_CURRENT_USER子目录树是Windows 注册表最重要的部分之一，它包含Windows 系统、系统的集成部分以及应用软件的配置信息，主要是针对系统的声音、时间、控制面板的功能（如桌面、鼠标、配色方案、屏幕保护程序）、键盘等建立的配置信息以及安装软件时由安装程序建立的项和值

HKEY_CURRENT_USER常用项

- HKEY_CURRENT_USER\AppEvents
- HKEY_CURRENT_USER\Console
- HKEY_CURRENT_USER\Control Panel
- HKEY_CURRENT_USER\Environment
- HKEY_CURRENT_USER\Printers
- HKEY_CURRENT_USER\Keyboard Layout
- HKEY_CURRENT_USER\software

5.4注册表的备份与恢复

- 备份方法
  - 通过REGEDIT菜单工具进行备份。
  - 通过reg.exe工具备份。export
  - 利用磁盘管理工具备份。
- 恢复方法
  - 通过REGEDIT菜单工具进行恢复。
  - 通过reg.exe工具恢复。import
  - 利用磁盘管理工具恢复。

5.5 注册表文件组成

- 文件组成
  - 大多数注册表文件都存放在%SystemRoot%\System32\Config文件夹。
  - *.LOG文件，日志文件，保存运行时更新信息。
  - Default文件，登录网络前所用缺省用户配置文件。
  - Sam (Security Account Manager,安全帐目管理器)
  - Security文件，含有与安全有关的内容。
  - Software文件，安装软件内容。
  - System文件，包含的主要是硬件配置的信息。
  - Documents and Settings\UserName\NTUSER.DAT

上机练习作业

- 使用windows API实现对注册表的操作
  - 创建键与子健
  - 删除键
  - 修改键值
  - 读取键值