Windows 2000 注册表彻底剖析

章轩工作室　编著

清 华 大 学 出 版 社

需要全本请访问 www.ertongbook.com

（京）新登字 158 号

内 容 简 介

本书详细介绍了 Windows 2000 注册表的结构和功能，并深入介绍了 Windows 2000 系统内置的 Regedit 和 Regedt 32 两种注册表编辑软件。其中包括如何修改、删除、新建注册表项，还针对各类型的数据项的特点，进行了仔细的分析与说明。

注册表所涉及的范围遍及整个 Windows 系统。本书从【开始】菜单开始，介绍了利用注册表对【系统】、【屏幕保护程序】、【控制面板】、【打印机】、活动桌面、TCP/IP、DHCP、WINS 等的设置。除说明了必要的注册表项路径、值项名称、注册表项功能、数据类型外，还特地介绍了与其相对应的组策略编辑器(Group Policy Editor，GPE)路径，使读者可以通过运行 Gpedit.msc 命令打开组策略编辑器，然后根据书中所介绍的 GPE 路径，快速方便地修改注册表。另外，本书还介绍了一个比较流行的注册表编辑软件——Tweaki…for Power Users。

本书内容涵盖面较广，语言浅显易懂，是所有渴望深入研究 Windows 的读者不可多得的一本好书。

本书繁体字版名为《Windows 2000 Registry 彻底剖析》，由文魁资讯股份有限公司出版，版权属章轩工作室所有。本书简体中文版由文魁资讯股份有限公司授权清华大学出版社独家出版。未经本书原版出版者和本书出版者书面许可，任何单位和个人均不得以任何形式或任何手段复制或传播本书的部分或全部内容。

北京市版权局著作权合同登记号：图字　　号

版权所有，翻印必究。
本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

书　　名：Windows 2000 注册表彻底剖析
作　　者：章轩工作室　编著
责任编辑：张秋香
出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
　　http://www.tup.tsinghua.edu.cn
印 刷 者：
发 行 者：新华书店总店北京发行
开　　本：787×960　1/16　印张：16　字数：420 千字
版　　次：2001 年 9 月第 1 版　2001 年 9 月第 1 次印刷
书　　号：
印　　数：0001~
定　　价：00.00 元

序　言

虽然 Linux 操作系统开放源码，但仍很难与 Windows 抗衡。微软一直不想让用户了解太多关于注册表数据库的知识。我想原因有两点，第一，危险性高；第二，注册表所涉及范围太广，很难介绍全面。但作者认为：不想问题发生的最好方法，就是先去认识它、了解它，而不是视而不见。

读者可以在计算机书店中找到许多关于 Widnows 2000 注册表数据库的书，但本书与其他书最大的不同点，就是提供完整的 GPE 路径。也就是说，用户既可以在 Regedit 中凭着自己对注册表的了解进行操作，也可以使用界面更友好的组策略编辑器来操作，避开了冗长的注册表项路径，相信读者会更有信心去学习注册表数据库。

另外，本书中也为读者介绍了一个比较流行的注册表编辑软件 Tweaki...for Power Users。它的功能比较强大，下载量也相当大。

但是有一点您不能不记住。修改注册表数据库的确具有相当的危险性，其结果更是难以预料，所以希望读者们务必小心行事。但只要按照书中的说明进行操作是绝对安全的，因为作者亲自测试过书中所介绍的每一项。

本书各章内容大致如下：

第 1 章对注册表进行简单介绍，并介绍了配置设置文件及注册表的结构。

第 2 章分别介绍了 Windows 系统内置的两种注册表编辑软件，及其相关操作。

第 3 章介绍了备份应用程序及修改注册表前如何备份注册表数据库。

第 4、5、6 章介绍了如何用注册表修改【开始】、【系统】、【屏幕保护程序】、【控制面板】、【活动桌面】、【磁盘配额】等。

第 7、8 章介绍了用注册表修改 Internet Explorer 和网络设置，如 TCP/IP、DHCP、WINS 等。

第 9 章详细介绍了最近比较流行的注册表编辑软件 Tweaki...for Power Users.

本书适合所有渴望深入研究 Windows 的读者阅读。

目　录

第 1 章　注册表简介 1

1.1　配置设置文件 2
1.2　从 INI 到注册表 3
1.3　注册表结构 3
1.3.1　5 大注册表项 4
1.3.2　子键和值项 7
1.4　Hive 12

第 2 章　注册表编辑器 15

2.1　打开注册表编辑器 16
2.2　Regedit 与 Regedt32 的比较 17
2.3　Regedit 26
2.3.1　界面 26
2.3.2　新建注册表项或值项 26
2.3.3　修改值项名称 29
2.3.4　修改数值 30
2.3.5　删除值项 33
2.3.6　查找 34
2.3.7　数据的导出与导入 35
2.3.8　复制注册表项名称 37
2.4　Regedt32 38
2.4.1　界面 38
2.4.2　新建注册表项或值项 40
2.4.3　修改值项名称和数据 41
2.4.4　删除项目 44
2.4.5　查找注册表项 44
2.4.6　数据的导出与导入 45
2.4.7　安全功能 45

第 3 章　准备工作 47

3.1　备份应用程序 50
3.1.1　备份什么 50
3.1.2　备份与还原的权限 50
3.1.3　打开备份应用程序 51
3.1.4　备份向导 52
3.1.5　备份类型 58
3.1.6　还原向导 59
3.1.7　远程备份 65
3.2　远程备份注册表数据库 66
3.2.1　远程备份 Windows 9X/Me 66
3.2.2　远程备份 Windows NT/2000 .. 71
3.3　注册表数据库的限制 71
3.3.1　虚拟内存大小 71
3.3.2　注册表大小 72

第 4 章　开始、系统和屏幕保护程序 71

4.1　开始菜单 74
4.1.1　新增展开功能 74
4.1.2　限制开始菜单与任务栏的某些操作 75
4.1.3　限制修改开始菜单和任务栏 .. 76
4.1.4　屏蔽菜单中的程序 77
4.1.5　屏蔽关机命令 78
4.1.6　屏蔽搜索功能 79
4.1.7　屏蔽文档菜单 80

4.1.8 不记录文件 80
4.1.9 清除文档记录 81
4.1.10 文件最大记录 81
4.1.11 屏蔽文档菜单 82
4.1.12 屏蔽 Windows Update 命令 .. 83
4.1.13 屏蔽收藏命令 84
4.1.14 屏蔽注销按钮 85
4.1.15 屏蔽注销命令 86
4.1.16 显示注销命令 87
4.1.17 屏蔽用户文件夹 88
4.1.18 屏蔽共享程序组 89
4.1.19 屏蔽运行命令 90
4.1.20 屏蔽网络和拨号连接 91
4.1.21 屏蔽任务栏的快捷菜单 91
4.1.22 屏蔽帮助命令 92
4.1.23 屏蔽我的文档 93
4.1.24 屏蔽个性化菜单(1)..... 93
4.1.25 屏蔽个性化菜单(2)..... 94
4.2 系统 95
4.2.1 删除文件夹选项命令 95
4.2.2 限制修改文件关联 96
4.2.3 在资源管理器中禁用鼠标右键 97
4.2.4 停止使用磁盘 97
4.2.5 屏蔽特定磁盘驱动器 98
4.2.6 删除映射网络驱动器 99
4.2.7 屏蔽文件菜单 99
4.2.8 屏蔽邻近的计算机 100
4.2.9 限制修改我的文档的路径 ... 101
4.2.10 屏蔽我的电脑的管理命令 . 102
4.2.11 删除搜索按钮 103
4.3 屏幕保护程序 104
4.3.1 登录前的密码 104
4.3.2 启用屏幕保护程序密码 105
4.3.3 启用屏幕保护程序 106
4.3.4 指定屏幕保护程序 107
4.3.5 等待时间 109
4.3.6 隐藏屏幕保护程序选项卡 110
第 5 章 控制面板、打印机和添加/删除程 111
5.1 控制面板 114
5.1.1 屏蔽控制面板 114
5.1.2 显示部分控制面板程序（1） 115
5.1.3 显示部分控制面板程序（2） 116
5.1.4 屏蔽部分控制面板程序（1） 119
5.1.5 屏蔽部分控制面板程序（2） 120
5.1.6 屏蔽控制面板 121
5.1.7 屏蔽硬件选项卡 123
5.1.8 屏蔽控制面板中的显示程序 124
5.1.9 屏蔽外观选项卡 124
5.1.10 屏蔽背景选项卡 125
5.1.11 屏蔽屏幕保护程序选项卡 .. 126
5.1.12 屏蔽设置选项卡 127
5.1.13 禁止更改墙纸 129
5.1.14 只允许使用位图墙纸..... 129
5.2 打印机 130
5.2.1 禁止添加打印机 131
5.2.2 禁止删除打印机 132
5.3 添加/删除程序 133
5.3.1 限制添加/删除程序 134
5.3.2 屏蔽更改或删除程序页..... 135
5.3.3 屏蔽添加程序页 136

需要全本请访问 www.ertongbook.com

5.3.4 屏蔽添加/删除 Windows 组件页 137
5.3.5 屏蔽光盘或软盘按钮 138
5.3.6 屏蔽从 Microsoft 添加程序 .. 140
5.3.7 禁用支持信息 141
5.3.8 屏蔽从网络上添加程序 142

第 6 章 桌面、活动桌面、登录和磁盘配额 141

6.1 桌面 144
6.1.1 限制调整任务栏 144
6.1.2 限制在工具栏上拖放快捷方式 145
6.1.3 隐藏桌面上的所有图标 146
6.1.4 隐藏桌面上的网上邻居图标 146
6.1.5 隐藏桌面上的我的文档图标 147
6.1.6 隐藏桌面上的 Internet Explorer 图标 147
6.1.7 结束时不保存设置 148
6.1.8 不将文件记录到网上邻居窗口中 148
6.2 活动桌面 149
6.2.1 启用活动桌面 150
6.2.2 禁用活动桌面 151
6.2.3 禁止更改 152
6.2.4 启用传统外壳 153
6.2.5 禁用所有项目 153
6.2.6 禁止添加项目 154
6.2.7 禁止删除项目 155
6.2.8 添加/删除项目 156
6.2.9 活动桌面墙纸 157
6.2.10 禁止关闭 157
6.3 登录 158
6.3.1 配置文件的种类 160
6.3.2 自动登录 161
6.3.3 提示找不到域控制器（1） .. 161
6.3.4 提示找不到域控制器（2） .. 162
6.3.5 提示找不到域控制器（3） .. 162
6.3.6 漫游失败便自动注销 163
6.3.7 注销时删除漫游配置文件 163
6.3.8 启用检测慢速网络连接 164
6.3.9 等候远程用户配置文件 165
6.3.10 设置对话框等候时间（1） 165
6.3.11 设置对话框等候时间（2） 166
6.3.12 慢速网络时提示用户 166
6.3.13 等候用户响应时间 167
6.3.14 最多重试次数 167
6.4 磁盘配额 168
6.4.1 启用磁盘配额 169
6.4.2 启用磁盘配额限制 170
6.4.3 默认配额限制及警告水平 171
6.4.4 超出配额限制时将事件记录到日志中 172
6.4.5 超出警告水平时将事件记录到日志中 174
6.4.6 应用到可移动媒体 175

第 7 章 Internet Explorer 175

7.1 Internet 选项 178
7.1.1 禁用更改主页设置 178
7.1.2 禁用更改 Internet 临时文件设置 178
7.1.3 禁用更改历史记录设置 179
7.1.4 禁用更改颜色设置 180
7.1.5 禁用更改链接颜色设置 181
7.1.6 禁用更改语言设置 182
7.1.7 禁用更改辅助功能设置 182
7.1.8 禁止用户添加/删除网站 183

7.1.9 限制修改安全性级别 184
7.1.10 限制更改分级设置 185
7.1.11 禁用更改证书设置 185
7.1.12 停止使用保存密码 187
7.1.13 禁用更改配置文件 188
7.1.14 禁用 Internet 连接向导 189
7.1.15 禁用更改连接设置 190
7.1.16 限制修改代理服务器设置 . 191
7.1.17 限制修改关联程序（1） ... 191
7.1.18 限制修改关联程序（2） ... 192
7.1.19 限制修改检查默认浏览器 . 193
7.1.20 限制修改高级选项卡 194
7.1.21 限制还原为默认值 194
7.2 快速设置 Internet 属性对话框 195
7.2.1 屏蔽常规选项卡 195
7.2.2 屏蔽安全选项卡 196
7.2.3 屏蔽内容选项卡 197
7.2.4 屏蔽连接选项卡 197
7.2.5 屏蔽程序选项卡 198
7.2.6 屏蔽高级选项卡 198
7.3 IE 菜单..... 199
7.3.1 屏蔽收藏菜单 200
7.3.2 屏蔽上下文菜单 200
7.3.3 禁用新建菜单项 201
7.3.4 屏蔽打开命令 202
7.3.5 限制【另存为】命令 202
7.3.6 限制另存为 Web 页命令..... 203
7.3.7 停止关闭窗口 204
7.3.8 限制全屏幕显示 204
7.3.9 限制查看源文件 205
7.3.10 限制 Internet 选项命令 206
7.3.11 屏蔽使用每日提示 207
7.3.12 屏蔽 Netscape 用户命令..... 207
7.3.13 屏蔽教程命令 208
7.3.14 屏蔽发送反馈意见命令..... 209
7.3.15 屏蔽在新窗口打开命令..... 210
7.3.16 限制目标另存为命令..... 210
7.3.17 禁用 F3 搜索命令 211
7.4 脱机 Web 网页 211
7.4.1 禁用添加频道 212
7.4.2 禁用删除频道 212
7.4.3 禁用所有已计划的脱机页.... 213
7.4.4 禁用添加脱机页计划..... 214
7.4.5 限制删除脱机页计划..... 214
7.4.6 禁用脱机页记数 215
7.4.7 完全禁用频道用户界面..... 215
7.4.8 预定限制 216

第 8 章 网络设置..... 215

8.1 TCP/IP..... 218
8.1.1 设置传送 ARP 的次数..... 218
8.1.2 储存标准 Internet 数据库路径 218
8.1.3 设置 TTL 时间 219
8.1.4 取得 DHCP 协议..... 219
8.1.5 是否传送包到所有网络..... 220
8.1.6 定义转发缓冲区的大小..... 220
8.1.7 回应不是单播 ARP..... 220
8.1.8 使用名称解释 221
8.2 RAS..... 221
8.2.1 增加 RAS 的网络流量..... 221
8.2.2 限制看到整个网络 222
8.2.3 回电等待时间 222
8.2.4 连接重试次数 223
8.2.5 记录 NetBIOS 流量..... 223
8.2.6 对 RAS 进行检查..... 224
8.2.7 是否以拨号方式连接到 Windows 域..... 224

8.2.8 使用 RAS 的 L2TP 功能 225
8.2.9 不缓存登录密码 225
8.2.10 加强对本地网络的使用权限 225
8.2.11 记录连接端口 226
8.2.12 等待确认时间 226
8.2.13 使用 RAS 数据广播 227
8.2.14 最大广播值（1） 227
8.2.15 最大广播值（2） 228
8.2.16 自动断线 228
8.2.17 控制 RAS 的等级 228
8.2.18 指定 RAS NetBIOS 网关等待时间 229
8.2.19 关闭 NetBIOS 的 RAS 拨入 229
8.2.20 RAS NetBIOS 广播方式 230
8.2.21 修改 RAS WINS 服务器名称 230
8.3 DNS 231
8.3.1 指定 TTL 时间 231
8.3.2 是否覆盖现存的资源记录 231
8.3.3 删除无效记录 232
8.3.4 搜索 DNS 数据库间隔 232
8.3.5 DNS 服务记录程度 233
8.3.6 传递名称查询 233
8.3.7 等待 DNS 服务器回应 234
8.3.8 没有响应时 DNS 服务器的工作 234
8.3.9 筛选记录方式 235
8.4 DHCP 235
8.4.1 记录与检查 DHCP 236
8.4.2 DHCP 数据库名称 236
8.4.3 DHCP 数据库路径 236
8.4.4 数据库类型 237
8.4.5 DHCP 数据库备份路径 237
8.4.6 指定 DHCP 数据库备份频率 238
8.4.7 删除数据库中过期记录 238
8.5 WINS 238
8.5.1 启用 BrustHandling 239
8.5.2 WINS 数据库路径 240
8.5.3 自动备份数据库 240
8.5.4 启动在暂停状态 241
8.5.5 WINS 服务的记录等级 241
8.5.6 是否记录改变到记录文件中 241
8.5.7 指定记录文件路径 242
8.5.8 控制 WINS 服务的线程数目 242
8.5.9 设置 WINS 代理 243

第 9 章 Tweaki...for Power Users 243

9.1 Tweaki...for Power Users 246
9.2 程序安装 246
9.3 运行程序 249
9.4 限制的功能 250
9.5 撤销 252
9.6 Security 253
9.6.1 Interface 选项卡 253
9.6.2 System 选项卡 257
9.6.3 Internet Explorer 261
9.7 Win Tweaks 267
9.7.1 Interface 267
9.7.2 System 选项卡 273
9.7.3 Internet Explorer 选项卡 280
9.8 NT4/Windows 2000 284
9.8.1 General 选项卡 284
9.8.2 Performance 选项卡 289

9.8.3 Network 选项卡 291
9.8.4 Server 选项卡 292
9.8.5 Debug 选项卡 294
9.8.6 Windows 2000 Specific 296
9.9 Microsoft Office 299
9.9.1 Access 300
9.9.2 Excel 303
9.9.3 Office 309
9.9.4 PowerPoint 313
9.9.5 Word 316
9.10 Registry 320
9.11 Options 322
9.11.1 Password Protection 323
9.11.2 User Preferences 324
9.11.3 Remote Connections 326
9.11.4 Check for Upgrade 与 About/Register 327

第 1 章　注册表简介



- 配置设置文件
- 从 INI 到注册表
- 注册表结构
- Hive

从 Windows 3.1 便开始使用注册表(Registry)来记录计算机中的一切，其中不但包含用户的个人信息，还有很多用户对系统或应用程序所作的设置。但是要注意，注册表是供应用程序(当然也包括操作系统)所使用的，绝对不是给用户使用的。关于这一点，从系统内置的注册表编辑器的界面便可以知道。

作者认为必须在这里强调一下，在您按照本书所介绍的内容进行操作之前，请务必先把注册表备份起来。当然，作者也亲自测试过本书所介绍的注册表项目，只要正确地按照书中所介绍的步骤进行操作是绝对安全的。除非您任意地修改或者不小心操作失误(至于如何进行备份，将在后面的章节进行详细的介绍)。另外，请千万不要随意导入电子邮件中所附带的注册表项目，百分之九十九是没有好处的。

1.1 配置设置文件

虽然，注册表与它的前身之间不论是在记录数据的方式还是结构上都存在着极大的差异。但是在深入了解注册表之前，我们必须对它的前身有所了解。

注册表的前身是配置设置文件(Initialize，也有人称它为初始文件)，而它的文件格式为.INI，也就是我们俗称的“INI 文件”。以前 INI 文件主要是应用在 16 位应用程序中，虽然 WindowsNT 系列操作系统都是 32 位，不过为了支持这些较旧的应用程序，Windows 2000 中还是包含了不少的.INI 文件。

INI 文件可以分为两大类：一种是系统使用的 INI 文件，例如我们所熟知的 SYSTEM.INI、WIN.INI、PROGRAM.INI、WINFILE.INI、PROTOCOL.INI 等。简单地说，各个 INI 文件在系统中分别负责不同的功能，目的就是让系统知道计算机中安装了哪些硬件和软件以及用户对操作系统、软件及硬件的设置。WIN.INI 中记录了应用程序对系统的设置，所以只要安装新的应用程序，便会有新的信息写入其中。换句话说，它会一直有新数据写入，所以它就会变得越来越大；SYSTEM.INI 则记录着一些有关硬件的信息，在该文件的[boot]区段中指定了操作系统在启动时必须加载的硬件驱动程序(VXD)，并且用[device=]来指定文件所在的路径。而 PROGRAM.INI 和 WINFILE.INI 则用来记录窗口文件总的初始化设置；PROTOCOL.INI 用来记录 Windows 网络的初始化设置。

需要全本请访问 www.ertongbook.com

另一种 INI 文件是个人的 INI 文件，通常这些 INI 文件都是在安装应用程序时所创建的。%SystemRoot%中有很多.INI 文件，例如 WINAMP.INI、Ulead32.INI、SYSTEM.INI 等。其中所记录的数据则各不相同，常见的有窗口的位置、程序的安装路径、背景颜色、用户信息以及最新使用过的文件记录等，如图 1.1 所示。



图 1.1　用记事本显示配置设置文件的内容

1.2　从 INI 到注册表

自从微软公司推出第 1 个比较完善的图形化操作系统——Windows 95 开始，注册表才算是真正诞生了。注册表是一个中央化的数据库，它将原来分散在多个 INI 文件中的信息，统一集中到一个数据库中，而且按照一个标准化的方式来记录。“统一”与“集中”的优点，使追踪系统或应用程序的问题更加方便，而只有“标准化”后才可以使整个环境进入一种稳定的状态。也就是说，程序员可以专心地改良他们的产品，而无需在意如何告诉系统有关软件的设置；用户也不必担心为每套软件而去学习不同的维护技巧。

1.3　注册表结构

在整个注册表数据库中共有 5 大注册表项，如图 1.2 所示。他们在整个系统中分别发挥着不同的作用，而且都相当重要。也只有当它们正常工作时，我们才可以正常地使用整个 Windows 2000 系统。



图 1.2 Windows 2000 中的注册表结构

1.3.1 5 大注册表项

- HKEY_CLASSES_ROOT

  HKEY_CLASSES_ROOT(**以下简称** HKCR)，**是由** HKEY_LOCAL_MACHINE \ SOFTWARE \ CLASSES **子键对应而来的。**

  单击上述两组注册表项及子键前方的“ + **”号以展开其树形结构，便可以发现两组注册表项的子键都是一一对应的，如图** 1.3 **所示。**



图 1.3 两组注册表项的子键是一一对应的

HKCR 的子键又分两大类：一类是用来标识注册表扩展名(Filename-extension)的子键，另一类是类别定义(Class-definition)子键。与以往所有 Windows 系统不同的是，如果某一值项同时出现在上述的两个注册表项路径中，Windows 2000 会为 HKEY_LOCAL_MACHINE \ SOFTWARE \ CLASSES 中的值项赋予较高的优先权，而优先使用。

扩展名子键的特点是子键的名称格式都是小数点加上 3 个字符的扩展名，如.txt、.jpg 等。当然也可以是 1、2 或 4 个字符，如.z、.ra、.html 等，但一般都用 3 个字符。它的主要功能是记录系统所能接受的扩展名类型。通常在我们安装新的应用程序时，安装程序便会在这个子键中创建一些新的子键，目的就是要告诉系统一种新的文件格式。如图 1.4 所示为 .txt 子键的记录，可以看到默认文件类型为 txtfile。

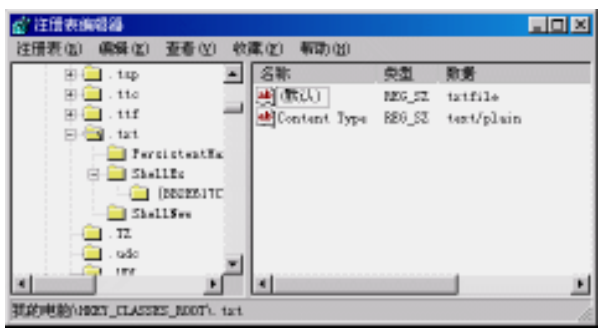


图 1.4　子键的记录

HKCR 子键的类别定义中记录着上述扩展名所需要打开(关联)的应用程序。我们再以.tXt 文件为例，在类别定义子键中定义了与其关联的应用程序，这里定义为 NOTEPAD.EXE，如图 1.5 所示。

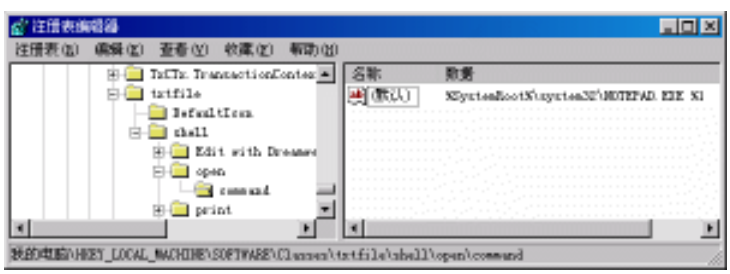


图 1.5　指定与文件类别定义有关的应用程序

- HKEY_CURRENT_USER

  HKEY_CURRENT_USER(以下简称 HKCU) 注册表项中共包含 9 个子键，这 9 个子键都是从 HKEY_USERS \ .DEFAULT 或 HKEY_USERS \ UserName 中对应而来的。

  HKCU 是当前登录系统的用户的各种设置，如果您的计算机只设置了一个用户的话，HKCU 会对应 HKEY_USers(以下简称 HKU)中的.DEFAULT 子键。

  但是，如果计算机中设置了多个用户的话，每个用户的设置项会在 HKU 中使用用户的安全标识符(Security ID，SID)来添加子键，并记录所有设置项。这时 HKCU 在启动 Windows 2000 时便会对应到当前登录的用户的子安全标识符中。而 SID 是由 Windows 2000 安全子系统(Security Subsystem)所创建的，SID 会在安全规则对象建立的同时指定给用户、计算机或组等，如图 1.6 所示。

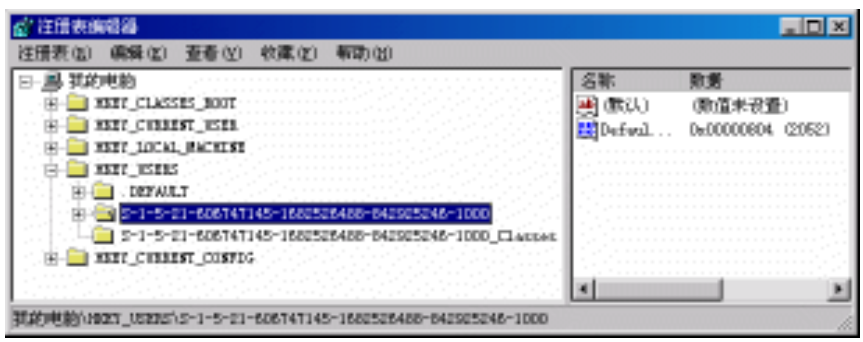


图 1.6 HKU 以用户的 SID 来区分

- HKEY_LOCAL_MACHINE

  HKLM \ Hardware 中的值项是由 Ntdetect.com 在开机的时候所获取的硬件信息。HKLM Hardware \ Description \ System 中便是有关于 BIOS、CPU、总线、内存地址等信息。其中的 HKLM \ Software \ Microsoft \ Windows 子键，在本书中将会经常提到，因为其中有 Win32 子系统的程序与工具程序的设置，如图 1.7 所示。

- HKEY_USERS

  HKU 中则放置着默认用户和各个已登录的用户信息。默认用户信息会对应到本注

册表项中的.DEFAULT 子键中，而其他的用户信息则是对应到以各自的安全标识符为名称的子键中。

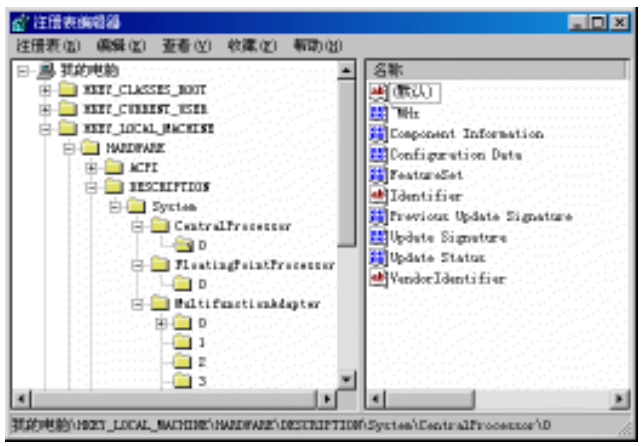


图 1.7　该子键中记录着 CPU 的信息

- HKEY_CURRENT_CONFIG

  对于一般的台式计算机来说，HKEY_CURRENT_CONFIG(以下简称 HKCC)的子键是从 HKLM \ System \ CurrentControlSet \ Hardware 子键对应而来的。而在 HKCC 中的数据其实也是 HKLM \ Software 和 HKLM \ System 中数据的子集。

不过，综合以上的说明后，您可以发现其实这 5 个注册表项实际上只有两组注册表项——HKLM 和 HKU，另外 3 个注册表项都是从它们对应而来的。

但要注意，在 Windows 2000 中已经没有了 HKEY_DYN_DATA 注册表项，我们可以在 Windows 9X / Me 系统中找到这个注册表项，而在 Windows NT 中只有使用 Regedit 时才可以看到该注册表项。

1.3.2　子键和值项

子键(Subkey)，就是紧接在上述 5 大注册表项下的部分。如果以注册表编辑器来看，单击注册表项前方的“ + ”号后所能看到的注册表项都称为子键。而子键当中可以包含其他子键，最下层的子键所包含的就是值项(data item)。

值项是注册表中的基本单位。它由 3 部分定义而成，分别是名称、类型和数据，如图 1.8 所示。在值项的【名称】列中会显示选取的值项名称，而在值项的【数据】列中则会显示设置的值，通常我们要修改的就是这个值。需要注意的是，在同一个子键中不可能有重复的键名。值项名称通常用一个组合式的名字来体现其功能，例如 LogEventLevel 项目的功能是记录事件的详细程度。

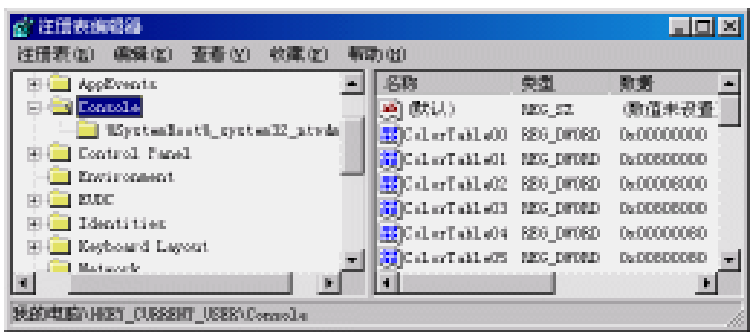


图 1.8　值项的 3 个组成部分

不同类型的值项，其值记录的方式也有不同的方式。接下来便要为大家说明各种不同的类型：

- REG_DWORD

  REG_DWORD 是由两个各含 16 位的字符所组成的，也就是说一个 REG_DWORD 的值项共用 32 位。这种数据类型遍布于整个注册表中，大部分项目都是使用这种数据类型。如果我们在这种类型的值项上双击鼠标左键的话，便会出现如图 1.9 所示的【编辑双字节值】对话框。

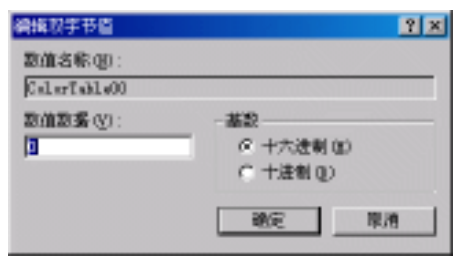


图 1.9　Regedit 的【编辑双字节值】对话框

需要全本请访问 www.ertongbook.com