Research on the Method of "Add to Lock" and "Relief Target" Registry Editor

加锁与解除锁定 Windows 2000/XP 注册表编辑器的方法研究

摘要：注册表是 Windows 系统的核心数据库，在系统的启动、运行与操作过程中起着重要的 作用。用户往往通过注册表编辑器（Regedit.exe）与 32 位注册表编辑器(Regedt32.exe) 来修改注册表，同时考虑到计算机安全与应用，有必要锁定与解除锁定注册表编辑器。本文 分析了注册表编辑器加锁与解除锁定的原理，提出了几种解决方法。

关键词：注册表　键　注册表编辑器　Windows API

孟万化　（浙江 绍兴文理学院　312000）

1 引言

在Windows2000操作系统中，注册表是一个系统数据库，它容纳了应用程序和计算机系统的 全部配置信息、Windows2000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，对系统的启动、运行与操作过 程中起着重要的作用。用户通过修改Windows2000/XP注册表，可以提高系统性能，增强系统 效果，清除病毒，对Windows2000/XP系统进行安全控制，解决应用软件的使用问题，排除系统故障等等。另一方面，一些恶意的程序，悄悄地修改系统的注册表信息；把您使用的计算机的系统信息乱改一通，然后锁住注册表编辑器，让您不能直接执行注册表编辑器程序来修 改设置。因此，用户需要对注册表编辑器进行加锁和解除锁定的操作。

用户要实施对注册表编辑器加锁与解除锁定，关键是注册表信息HKEY_CURRENT_USER \ Softw are \ Microsoft \ Windows \ CurrentVersion \ Policies \ System中的DisableRegistryTool s这一项值。如果这一项值为0（0代表关闭），或是把System这个注册表信息删除，注册表编辑器就可运行了。相反，只要把这一项的值设置为1，或者创建相应项，并把值设为1，注 册表编辑器就加锁了。

2 加锁与解除锁定注册表编辑器的几种实施方法

2.1 用户自编应用程序

应用程序对注册表进行管理、维护或访问的过程，实际上就是建立、修改、删除、读取注册表的键及键值项的过程。VB、VC++、VFP等面向对象的程序设计语言调用Windows API注册表 函数，可以充分地满足Windows应用程序对注册表的不同访问需求。

现以VB为例，调用三个Windows API函数来创建和修改注册表中的关于锁定与解除锁定注册 表编辑器的键及其值项。这三个函数是：RegCreateKeyEx（创建或打开一个键，并可取得句 柄）、RegSetValueEx（设置一个键的指定键值项的键值类型和键值）、RegCloseKey（释放 已获取的键的句柄）。程序代码如下：

```
Dim phkResult As Long
Dim lcreate As Long
Dim lResult As Long
Dim sa As SECURITY_ATTRIBUTES
Const REG_DWORD = 4
Const REG_OPTION_NON_VOLATILE =
0
Const HKEY_CURRENT_USER =
&H80000001
Const KEY_ALL_ACCESS.= &H3F
Private Sub Command1_Click()
Dim kk As Long
Call RegCreateKeyEx
(HKEY_CURRENT_USER, "Software \ Microsoft
\ Windows \ CurrentVe rsion \ Policies
\ System", 0&, "",
REG_OPTION_NON_VOLATILE,
KEY_ALL_ACCESS, sa, phkResult, lcrea te)
If Check1.Value = 1 Then
kk = &H1
Else
kk = &H0
End If
Call RegSetValueEx(phkResult,
"DisableRegistryTools", 0&, REG_DWORD, kk,
4)
Call RegCloseKey(phkResult)
Command1.Enabled = False
End Sub
Private Sub Command2_Click()
End
```

```
End Sub
```

在工程中建立一个标准模块，代码如下：

```
Type SECURITY_ATTRIBUTES
    nLength As Long
    lpSecurityDescriptor As Long
    bInheritHandle As Long
End Type
Public Declare Function RegCreateKeyEx Lib "advapi32.dll" Alias "RegCreateKeyExA " (ByVal hKey As Long, ByVal lpSubKey As String, ByVal Reserved As Long, ByVal lpClass As String, ByVal dwOptions As Long, ByVal samDesired As Long, lpSecurityA ttributes As SECURITY_ATTRIBUTES, phkResult As Long, lpdwDisposition As Long) As Long
Public Declare Function RegSetValueEx Lib "advapi32.dll" Alias "RegSetValueExA" (ByVal hKey As Long, ByVal lpValueName As String, ByVal Reserved As Long, ByVal dwType As Long, lpData As Any, ByVal cbData As Long) As Long
Public Declare Function RegCloseKey Lib "advapi32.dll" (ByVal hKey As Long) As L
ong
```

用户编制的应用程序，经编译后运行程序进行相应的选择操作，并经确认就达到加锁或解除 锁定注册表编辑器的目的。程序运行后界面如图1所示。

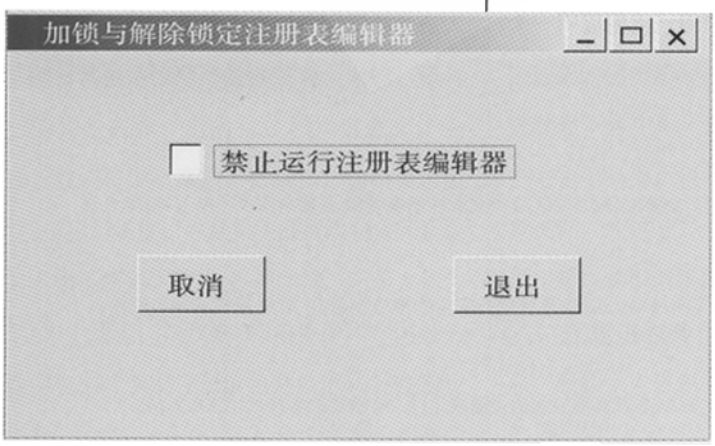

图1

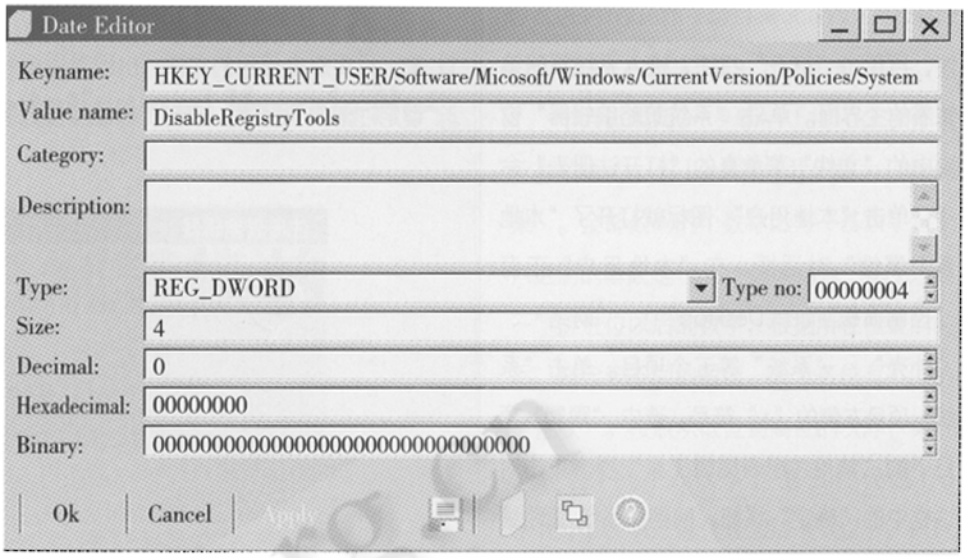

图2

2.2 利用系统管理实用工具

尽管到目前为止，Windows 2000/XP系统自带的注册表编辑器是管理Windows2000注册表最常 用的工具，但是它并不是唯一的工具。其它工具包括：Resplendent Registrar编辑工具、 与Windows 2000/XP Resource Kit一起提供的命令行工具、系统策略编辑器、以及注册表 编辑器创建的REG脚本文件，等等。同样可以用来加锁和解除锁定Windows2000/XP的注册表 编辑器。现以Resplendent Registrar编辑工具和系统策略编辑器为例。

2.2.1 Resplendent Registrar编辑工具

Resplendent Registrar编辑工具（Version 3.01，简称为RR301）是新一代的注册表编辑器 ，它使用类资源管理器的界面。进入RR301后，呈现在用户面前是一个主窗口，有标题栏、菜单栏、地址栏、键种类栏、工具栏、树格窗口与内容格窗口组成，地址栏内的地址可以具 有记录功能。

用户要加锁和解除锁定Windows自带的注册表编辑器，只要在树格窗口中逐级展开到HKEY_CU RRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System，双击 System进入该键值的属性对话框，如果没有DisableRegistryTools这一项，创建这一项，并 设置其类型为REG_DWORD，值为1（即为加锁），单击“OK”按钮。否则，只要值设置为1， 单击“OK”按钮。相应地，只要值修改为0，单击“OK”按钮，就完成注册表编辑器被锁的 解除。如图2：

2.2.2 系统策略编辑器

如果用户对注册表还不很熟悉，则可以借助系统策略编辑器等工具来自动修改注册表。系统 策略编辑器对个人、用户组或者所有用户设置各种策略，当这些策略被设定后，系统就会自动修改注册表中相应的内容，并且当用户一旦登录系统，系统就会自动修改注册表中的信息 。系统策略编辑器（Poledit）一般需要另外安装，在Windows2000/XP光盘的 \ tools \ resk it \ netadmin \ poledit子目录中可以找到Poledit.exe。将它复制到Windows2000/XP系统 目录下，与ADMIN.ADM文件在一起就可使用系统策略编辑器了。

在Windows的“运行”对话框中执行Poledit.exe，则提示用户打开一个模板文件，

选择C:\Windows目录中的ADMIN.ADM文件，再单击“打开”扭钮，进入系统策略编辑器的主界面。单击“系统策略编辑器”窗口中的“文件”菜单直的“打开注册表”命令，单击“本地用户”图标就打开了“本地用户属性”对话框。在“本地用户”下有“控制面板”、“Desktop”、“网络”、“外壳”、“系统”等五个项目。单击“系统”项目左侧的“+”符号，选中“限制”项目下的“禁用注册表编辑工具”项。单击对话框中的“确定”按钮，回到“系统策略编辑器”窗口，然后单击“文件”菜单下的“保存”命令，所选的限制设置就生效。反之，只要取消“限制”项下的“禁用注册表编辑工具”所选项，进行相同的“保存”操作后，就可以使用Windows系统自带的注册表编辑工具了。

2.3 制作REG文件

2.3.1 制作解除文件Unlock.reg

新建一个文本文件，扩展名为REG，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

这个文本文件的内容中，也可把最后一行"DisableRegistryTools"=dword:00000000去掉，原因是上一行要求“Regedit”直接把“System”的注册表信息项删除，而“DisableRegistryTools”是在“System”之下。

2.3.2 制作加锁文件lock.reg

新建一个文本文件，扩展名也为REG，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000001
```

假定将自己制作的两个文本文件unlock.reg与lock.reg保存在E:\MWH下，要进行相应的设置，只要双击相应的文件，出现对话框后，单击“是”或“确定”按钮即可。例如，要解除锁定注册表编辑器，双击E:\MWH下的unlock.reg文件，出现如下图3对话框：

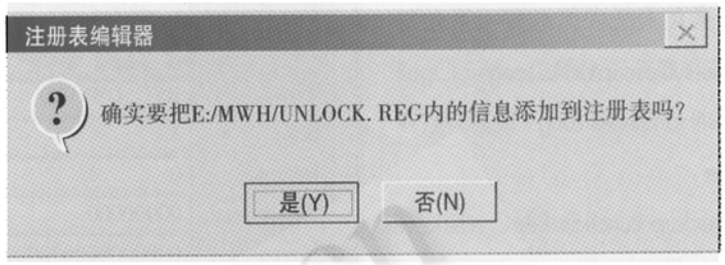

图3

单击“是”按钮或按回车键，出现如图4对话框后，单击“确定”按钮或按回车键。

图4

3 小结

让计算机更好地、安全地运行，是每一个用户都在思考的问题。注册表编辑器是管理Window s 2000/XP注册表最常用的工具。本文分析了注册表编辑器加锁与解除锁住的原理，提出了几种解决锁定与解除锁定注册表编辑器的方法。另外，还可以分别在注册表编辑器可以使用时备份注册表，在需要时修改相应键与键值项导入注册表、利用WEB页面以及在线加锁与解除锁定注册表编辑器等方法。这些对于维护计算机系统的安全性、可靠性与提高系统性能是很有用的。

参考文献

1 曹国均、王健编著，WINDOWS 2000中文版注册表使用开发与实例[M]，清华大学出版社，2000。

2 孟万化，注册表对Windows 2000系统运行安全的神奇作用[J]，计算机应用与软件，20 02,(6)。

3 胡文军、秦恒，利用WEB页面捍卫您的注册表[J]，电脑知识与技术，2002,(4)。