Fadia道德黑客丛书

Windows黑客攻防

电子科技大学出版社

Fadia道德黑客丛书：

良性入侵——道德黑客非官方指导

网络安全——一个黑客的视点

公司安全——道德黑客攻防指导

手机黑客攻防

E-mail黑客攻防

[redacted]

Google黑客攻防

入侵警报

加密/解密

Linux使用诀窍与技巧

计算机使用剖析

操作系统黑客攻防

小天才：Ankit Fadia之路

海外大学访问权限破解

兴韦-法迪亚网络与信息安全中心（中国）
www.e-hacker.info

2007

ISBN 978-7-81114-655-4

9 787811 146554 >

定价：15.00元

Windows 黑客攻防

法迪亚 著
孟庆华 译

电子科技大学出版社

图书在版编目（CIP）数据

Windows 黑客攻防/（印）法迪亚著；孟庆华译. —成都：电子科技大学出版社，2007.10

ISBN 978-7-81114-655-4

Ⅰ.W… Ⅱ.①法…②孟 … Ⅲ.操作系统（软件），Windows—安全技术 Ⅳ.TP316.7

中国版本图书馆 CIP 数据核字（2007）第 154026 号

Windows 黑客攻防

法迪亚 著

孟庆华 译

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：郭　庆

责任编辑：郭　庆　杜亚提　徐守铭

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都市海翔印务有限公司

成品尺寸：185mm×260mm　　印张 4.875　　字数 138 千字

版　　次：2007 年 10 月第一版

印　　次：2007 年 10 月第一次印刷

书　　号：ISBN 978-7-81114-655-4

定　　价：15.00 元

前　言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到国家、企业、个人乃至人类社会的生存和发展。而对计算机与互联网构成最严重威胁的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

本书是“法迪亚道德黑客丛书”中，针对 Windows 系统安全环境定制的专著。本书以 Windows 系统的核心配置结构——注册表为主线，探讨了 Windows 系统各个基本层面的安全参数设置，包括密码安全保护、定制 Windows 的安全环境等。本书简明扼要，内容专注，是安全兴趣爱好者和专业人士不可或缺的参考书。

本书主要由孟庆华博士主持翻译、统稿、审校，齐金鹏博士、陆星家博士参与了全书翻译。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

有关全套“法迪亚道德黑客丛书”的出版情况，敬请登陆http://www.e-hacker.info.

译　　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 9 月

目　录

第一章 密码安全

1.1 引言

密码是全世界范围内所使用的最为古老的系统确认机制之一。系统提示用户输入正确用户名和密码，用户名和密码既是隐私又是相互关联的。每个黑客期望能够破译密码提示以破解密码，从而对系统进行恶意攻击来破坏或窃取机密数据。即使 Windows 系统数据也是通过密码机制进行保护的。

启动 Windows 系统时，一个密码提示窗口就会立刻弹出。不幸的是，一些系统可以简单地点击取消按钮就能轻松地绕过密码保护机制。即使 Windows 处于运行状态，用户也可以在具体文件、文件夹或驱动上实施密码保护。换句话说，密码已经成为全世界范围内使用最为普遍的保护机制。

不幸的是，很多人仍然把一套随意和无用的字符作为密码使用。因此，黑客通过一些软件工具就可以很容易地破解密码保护机制。尤其是，目前很多密码依然采用空白字符或与用户名相同。一旦黑客破解了受害者的密码，随后就可能实施各种不同的恶意攻击。因此，Windows 系统用户采取一些防范措施，以提高系统整体安全性就变得非常重要。在本节内容中，我们主要讨论一些与密码验证相关的要诀和技巧，这对每个 Windows 用户都是至关重要的。

警告 虽然本节内容中所涉及的例子都已在各种平台上经过测试，但为了避免意外发生，建议备份所有的系统文件。

1.2 登录提示中保护用户隐私

（适用于所有 Windows 版本）

技术级别：低　　安全级别：高

通常情况下，登录 Windows 系统时都有可能保留最后登录用户的相关信息（这些信息存放于高速缓冲存储器）。通过以下的注册表技巧就可以防止暴露这些信息：

1．打开 regedit.exe 文件

从“开始”处，点击“运行”，在运行对话框里敲入“regedit”，如图 1-1 所示。

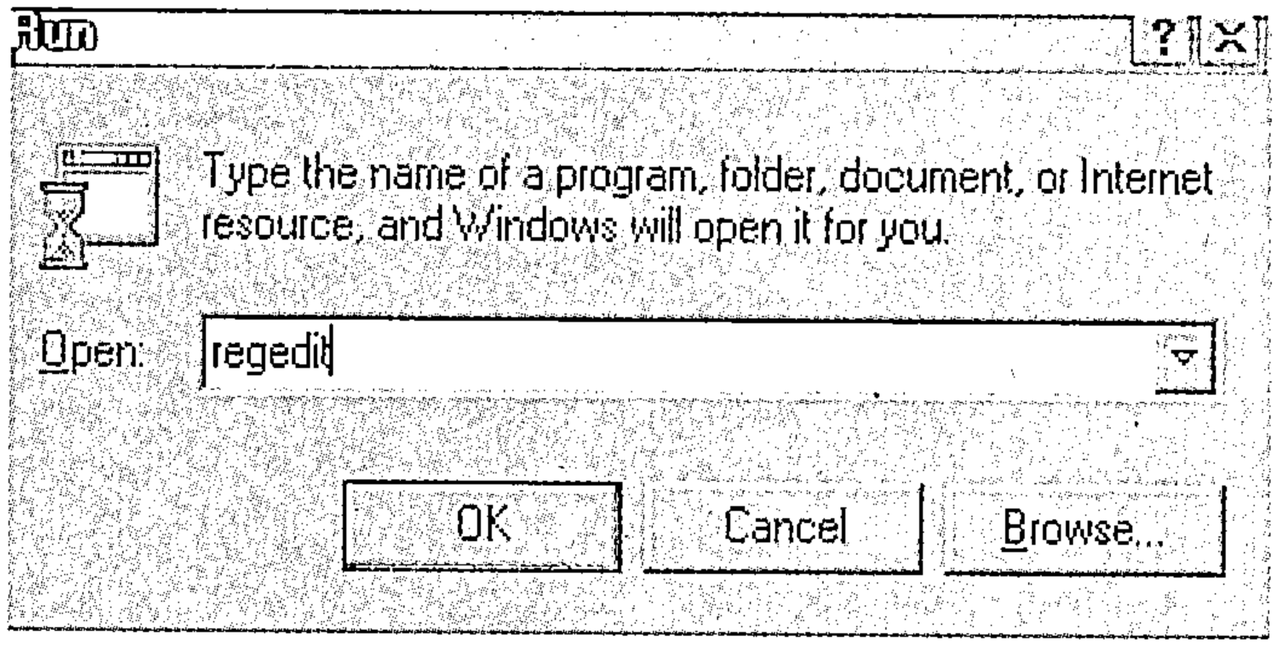

图 1-1　打开注册表命令

2．寻找或创建以下的注册键

对应于 Windows 2000 或 XP 系统：

HKEY_LOCAL_MACHINCE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

对应于 Windows 95, 98 或 Windows ME 系统：

HKEY_LOCAL_MACHINE\Network\Logon

对应于 Windows NT 系统：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．创建一个名为 DontDisplayLastUserName 新双字键值（在上述注册键内）

设置该双字键值为 1 即可启用该限制，设置为 0 即可对其进行禁用，如图 1-2 所示。

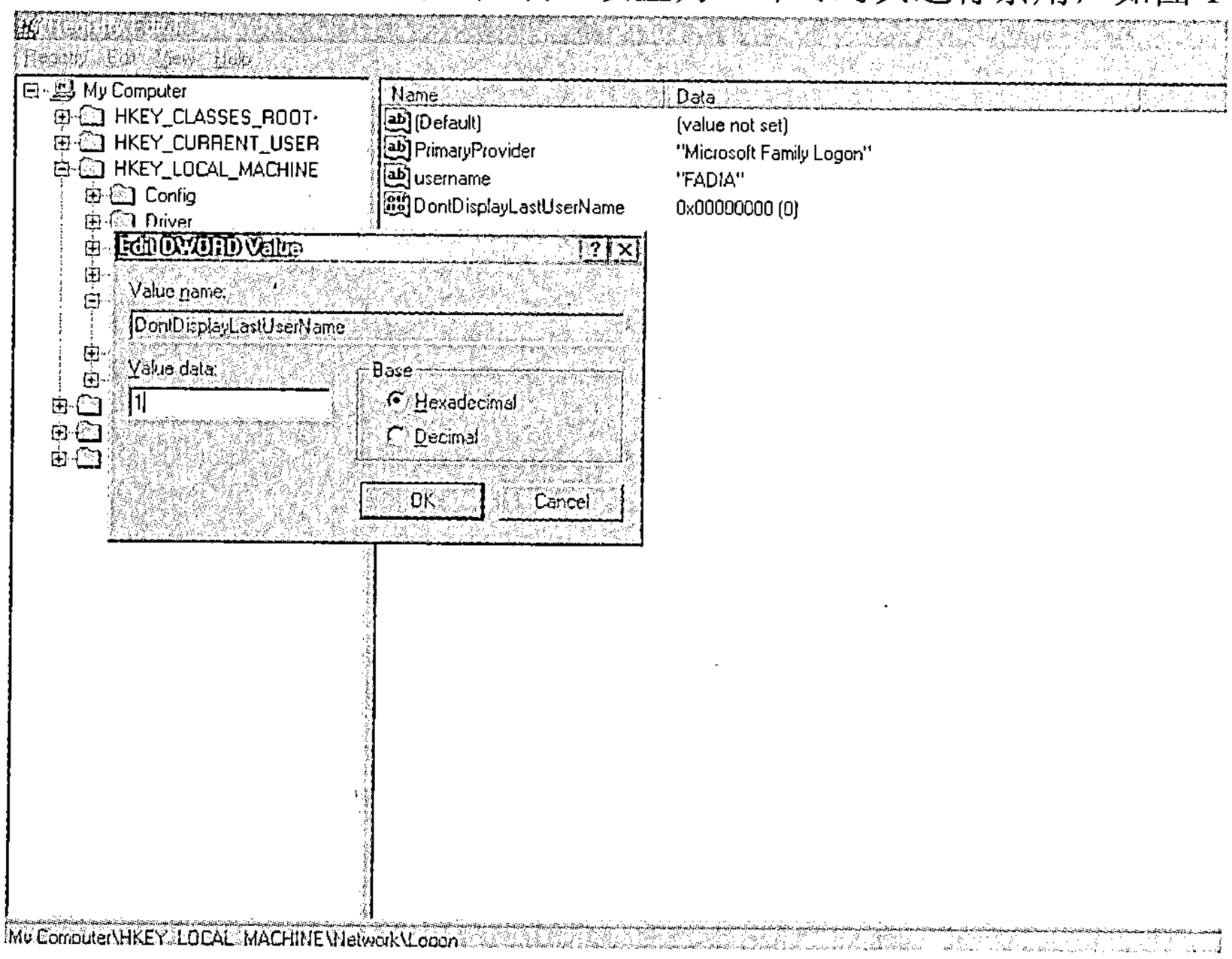

图 1-2　隐藏登录信息

1．退出 Windows 注册表，为了使改变生效，需重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[注册键项取决于windows 的不同版本]
"DontDisplayLastUserName"="1"
```

1.3 增强密码安全设置

（适用于所有 Windows 版本）

技术级别：低　　安全级别：高

由于用户所设置的密码缺乏安全性，从而导致了世界范围内的系统存在安全漏洞。因此，很多管理员更倾向于采用较小长度又能有效提高系统安全性的密码。以下是具体的实现过程：

1．打开 regedit.exe 文件。

2．寻找或创建以下注册表键项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network [只适用于特殊用户]

或者 *HKEY_CURRENT_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network* [适用于所有用户]

3．在上述注册键项中创建一个名为 AlphanumPwds 的新双字键值，设置该双字键值为 1 即可启用该限制，设置为 0 对其进行禁用。默认情况下，Windows 可以接受任意形式的密码。一旦该设置生效，Windows 将只接受字母与数字形式的密码，如图 1-3 所示。

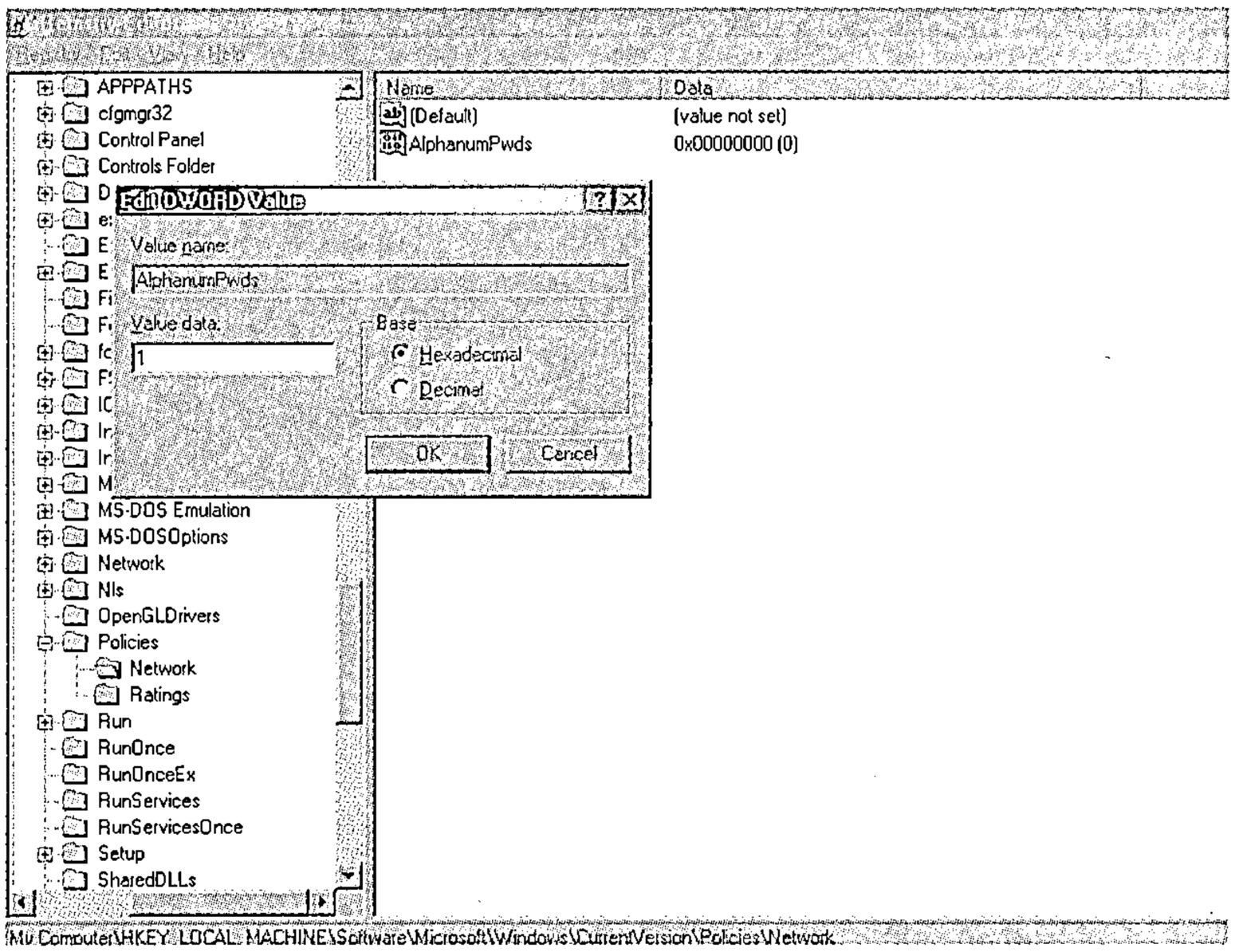

图 1-3　增强密码性安全设置

4．退出 Windows 注册表，为使设置更改生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

"MinPwdLen"="在这里输入长度值"

1.4 配置最小长度的 Windows 登录密码

适用于 Windows 所有版本

技术级别：低　　安全级别：高

另一项安全措施就是系统管理员经常为所有用户设定最小长度的密码，以提高系统安全性。可以通过以下的注册编辑技巧实现该功能：

1．打开 regedit.exe 文件。

2．寻找或创建以下注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network

3．创建一个名为 *MinPwdLen* 双字键值（在以上的注册键内），将其数值设定在密码所要求的最小长度范围内，如图 1-4 所示。

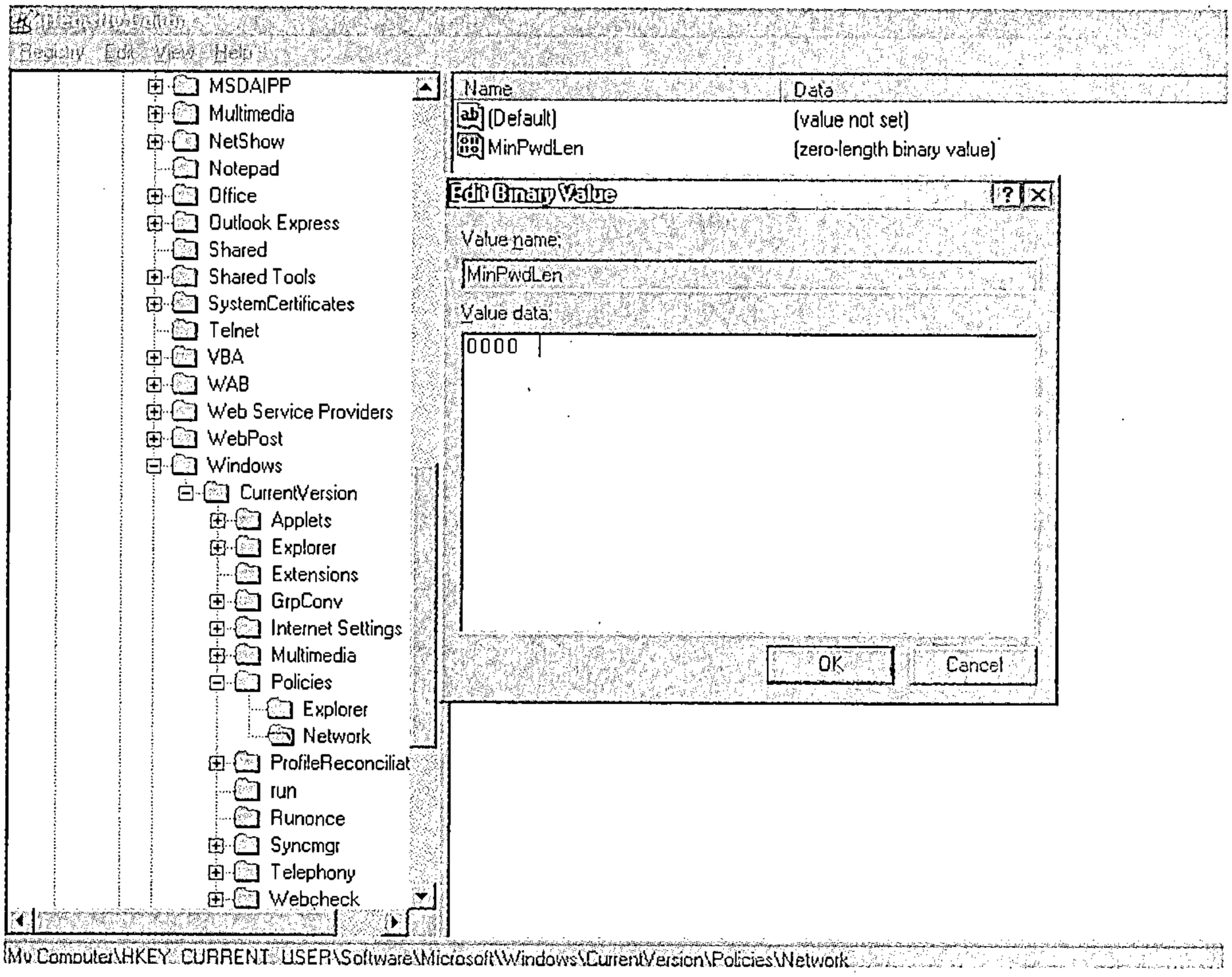

图 1-4　设置最小长度密码

4．退出 Windows 注册表，为了使改变生效，需重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
"MinPwdLen"=“在此输入长度值”

1.5 选择安全性高的密码

（适用于所有 Windows 版本）

技术级别：低　　安全级别：高

为获得该问题的更多相关信息，请参考本书中的安全列表部分。

1.6 防止 Windows 登录密码被盗

（适用于所有 Windows 版本）

技术级别：低　　安全级别：高

事实上，大多数 Windows 系统会面临另一个安全风险，就是用户密码的副本经常存放于本地系统，大大增加了系统受到恶意攻击的风险。然而，系统管理员简单地通过以下步骤就能轻松防止密码被盗：

1．打开 regedit.exe 文件。

2．寻找或创建以下注册键项：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network

3．在上述注册键中新建一个名为 DisablePwdCaching 的 DWORD 值，设置该双字键值为 1 即可启用该限制，设置为 0 对其进行禁用，如图 1-5 所示。

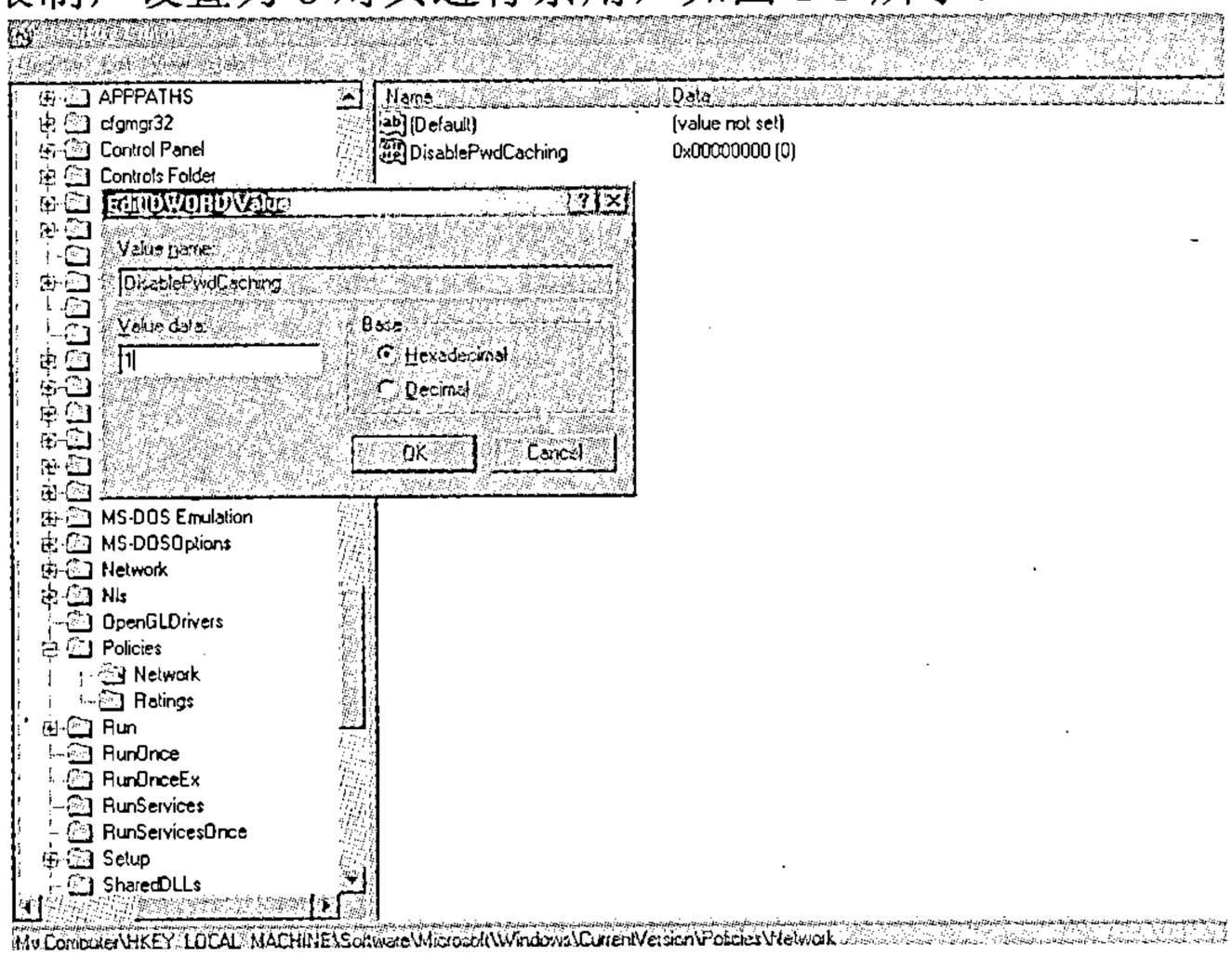

图 1-5　防止 Windows 登录密码被盗

4．退出 Windows 注册表，为了使改变生效，需重新启动 Windows 系统。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network
"DisablePwdCaching"=" 1"
```

1.7 防止 IE 浏览器缓存密码信息

（适用于所有 Windows 版本）

技术级别：低　　安全级别：高

用户每次在受到密码保护的网页中输入密码时，IE 浏览器就会询问用户是否保存密码信息。这样更增加了系统受到恶意攻击、非法入侵等破坏活动的威胁。然而，系统管理员通过以下步骤就可以防止密码被 IE 浏览器缓存：

1．打开 regedit.exe 文件。

2．寻找或新建以下注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

3．在上述注册键中新建名为 DisablePasswordCaching 双字键值，设置该双字键值为 1 即可启用该限制，设置为 0 即可实现对其进行禁用，如图 1-6 所示。

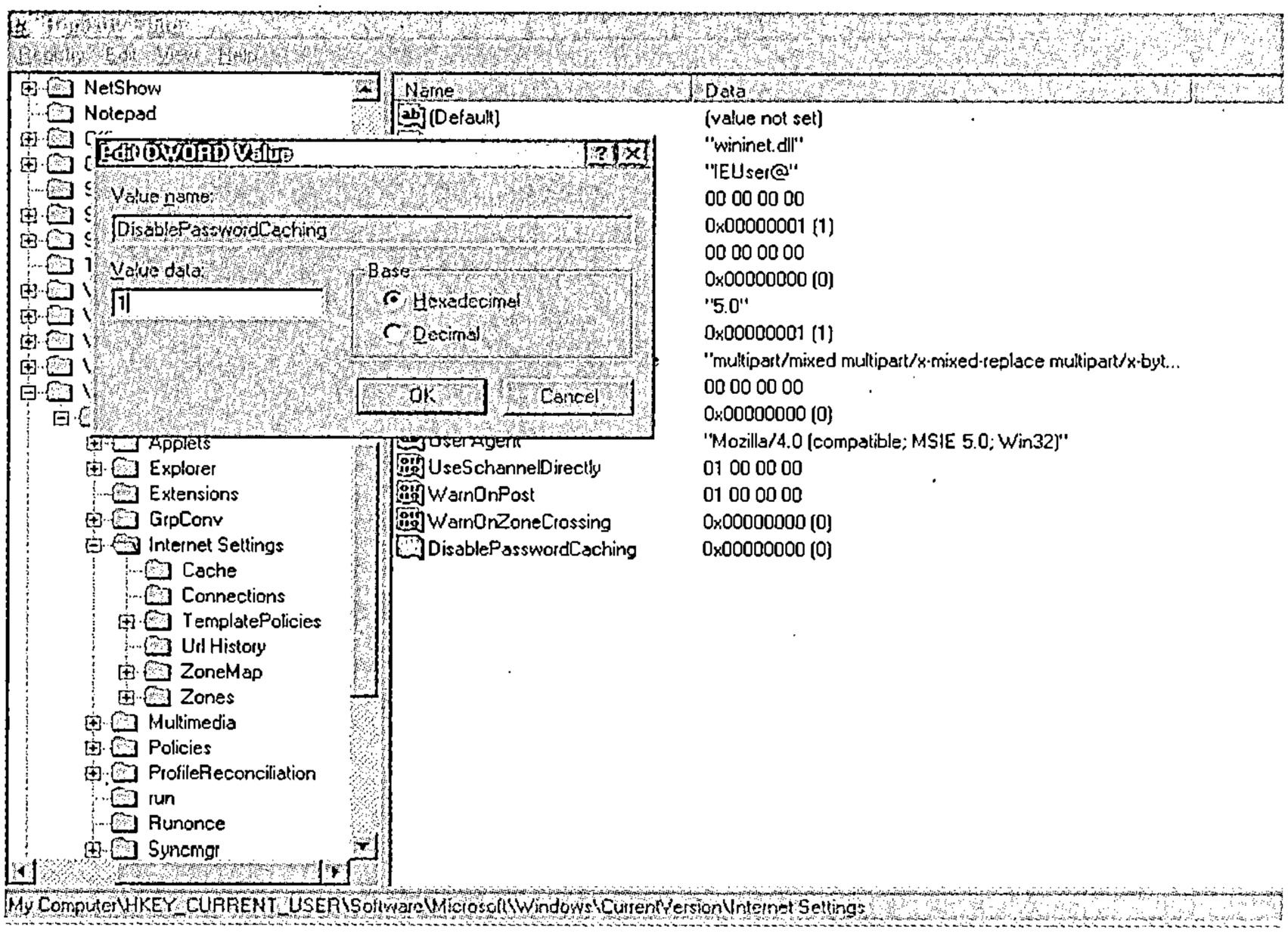

图 1-6　防止 IE 浏览器缓存密码信息

4．退出 Windows 注册表，重新启动 Windows，使设置更改生效。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"DisablePasswordCaching"=" 1"

1.8 定制密码对话框标题

（适用于 Windows 2000，XP 和 NT 系统）

技术级别：中等　　安全级别：中等

以前述事例为基础，我们可以在密码提示的对话框中定制欢迎消息。通过以下步骤就可实现该功能：

1．打开 regedit.exe 文件。

2．寻找或新建以下的注册键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．在该注册键中新建一个名为 *LogonPrompt* 字符串键值，将其设定为你想在登录提示对话框中显示的消息文本，如图 1-7 所示。

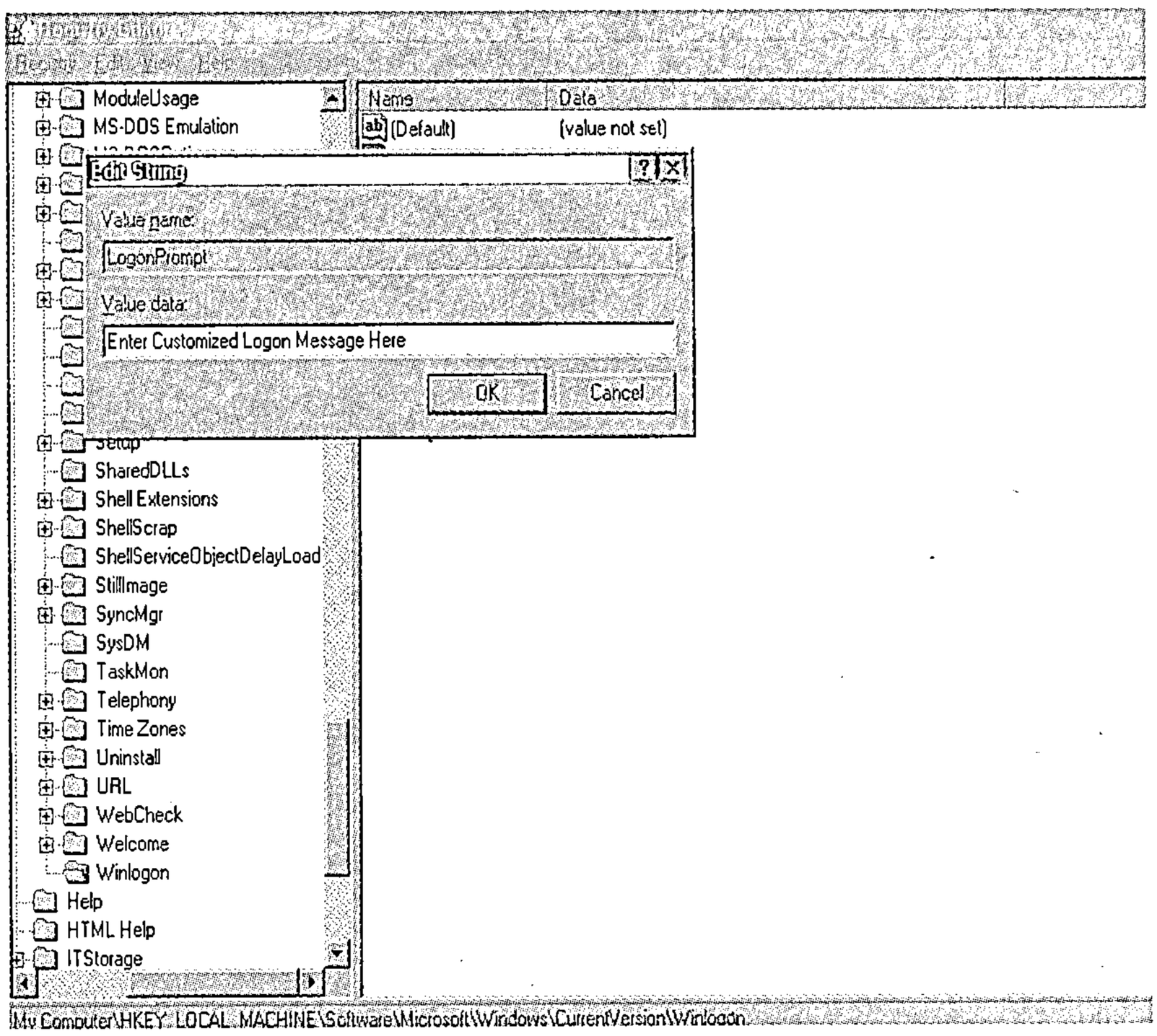

图 1-7　定制欢迎信息

4．退出 Windows 注册表，为了使设置生效，需重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]
"LogonPrompt"="输入消息文本"

1.9 定制密码提示标题

(适用于 Windows 2000，NT 和 XP 系统)
技术级别：中等　　安全级别：中等

通过以下步骤就可以对 Windows 密码对话框标题进行更改:

1．打开 regedit.exe 文件。

2．寻找或新建以下的注册键项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．新建一个名为 *Welcome* 的字符串键值，将其数值改变为显示在登录提示中所定制的文本，如图 1-8 所示。

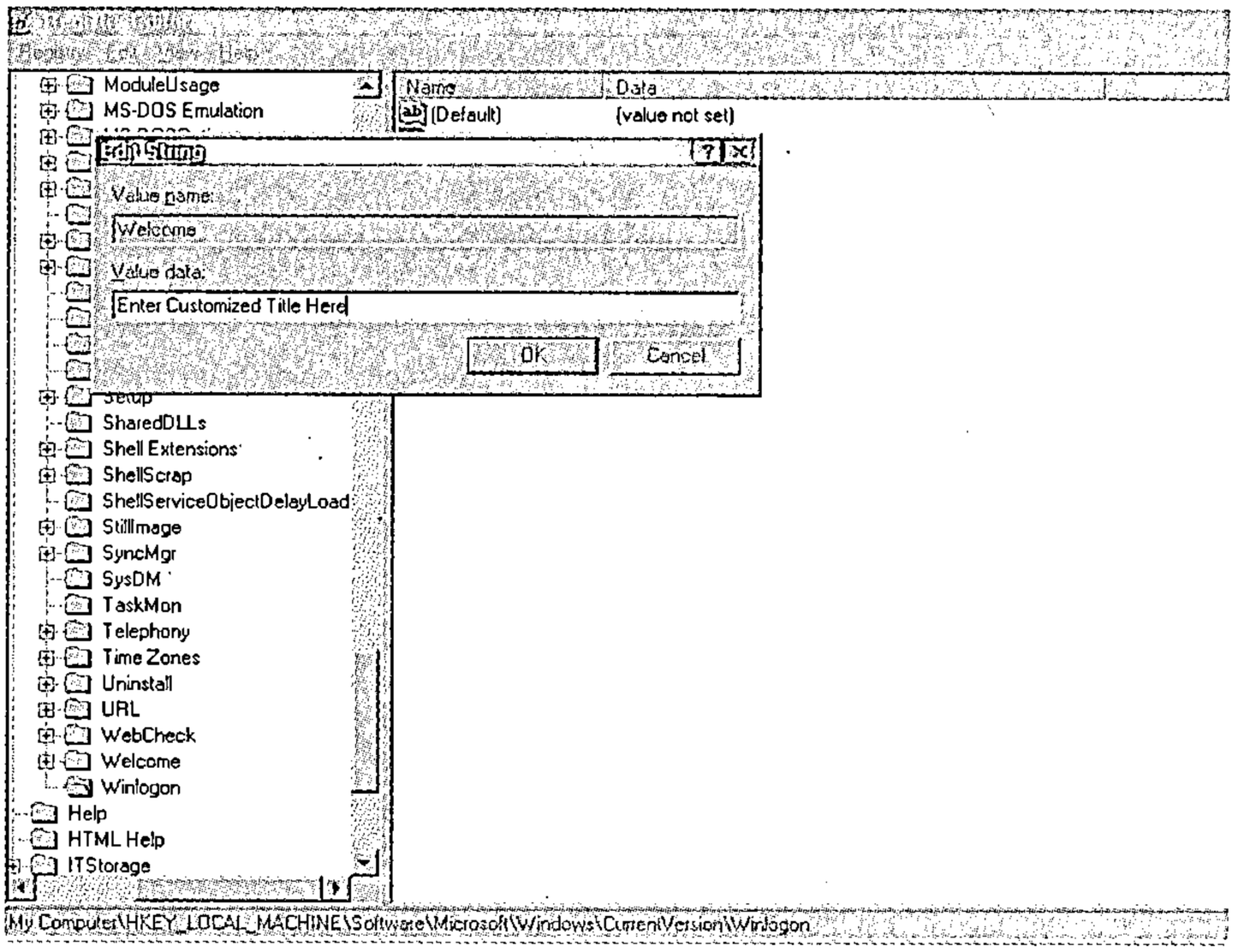

图 1-8　定制密码提示标题

4．退出 Windows 注册表，为使改变生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
"Welcome"="标题定制信息"

1.10 准许从密码提示中关机

（适用于 Windows 2000，XP 和 NT 系统）

技术级别：低　　安全级别：中等

执行以下步骤，就可以允许用户在密码提示对话框中关闭系统:

1．打开 regedit.exe 文件。

2．寻找或新建以下注册键：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

3．新建一个名为 ShutDownWithoutLogon 的双字键值，设置其键值为 1 即可启用该限制，设置为 0 即可禁止该选项，如图 1-9 所示。

4．退出 Windows 注册表，为使更改生效，需重新启动 Windows 系统。下次启动时，一个关闭按钮将在密码输入对话框中显示。

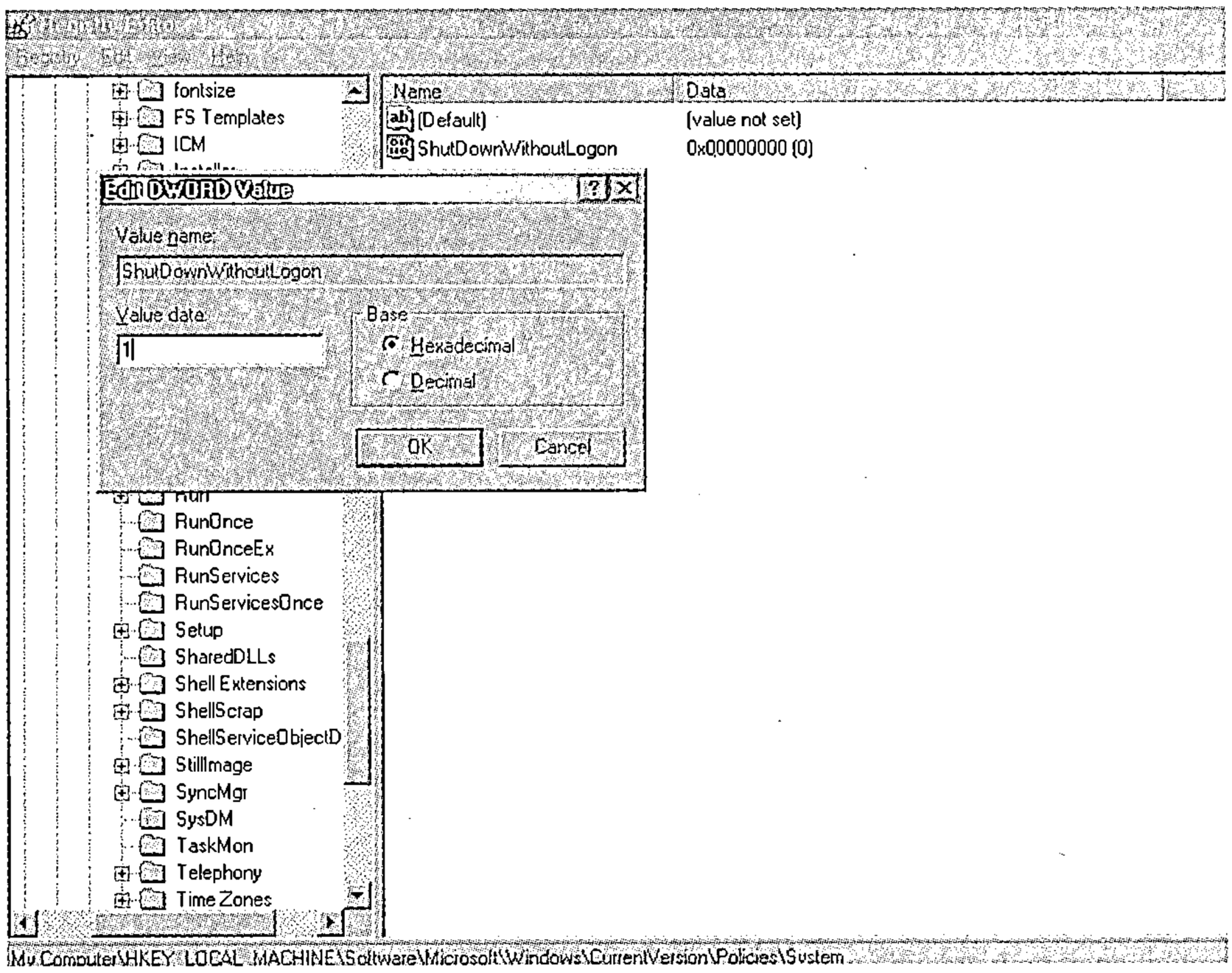

图 1-9　设置从密码提示中关机

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
    "ShutDownWithoutLogon"="1"
```

1.11　Windows 启动屏幕中显示定制消息

（适用于所有 Windows 版本）

技术级别：高　　安全级别：高

每次 Windows 启动之前，可以在对话框里展示定制的消息，比如，法律通知、隐私权政策、警告、友好欢迎等信息。换句话说，在用户使用计算机之前，能够使用户接收此类信息。通过下面步骤即可在每次 Windows 启动时在屏幕上显示定制的信息：

1．打开 regedit.exe 文件。

2．寻找或新建以下注册键：

对于 Windows 95，Windows 98 和 Windows ME 用户：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon

对于 Windows 2000，Windows XP 和 Windows NT 用户：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．新建一个名为 LegalNoticeCaption 的字符串键项，该项用于设定对话框的标题文本信息。右击该键项即可对该标题文本进行编辑。

4．新建另外一个名为 *LegalNoticeText* 的字符串键项，该项主要用于对显示在消息对话框中的主体消息进行编辑，如图 1-10 所示。

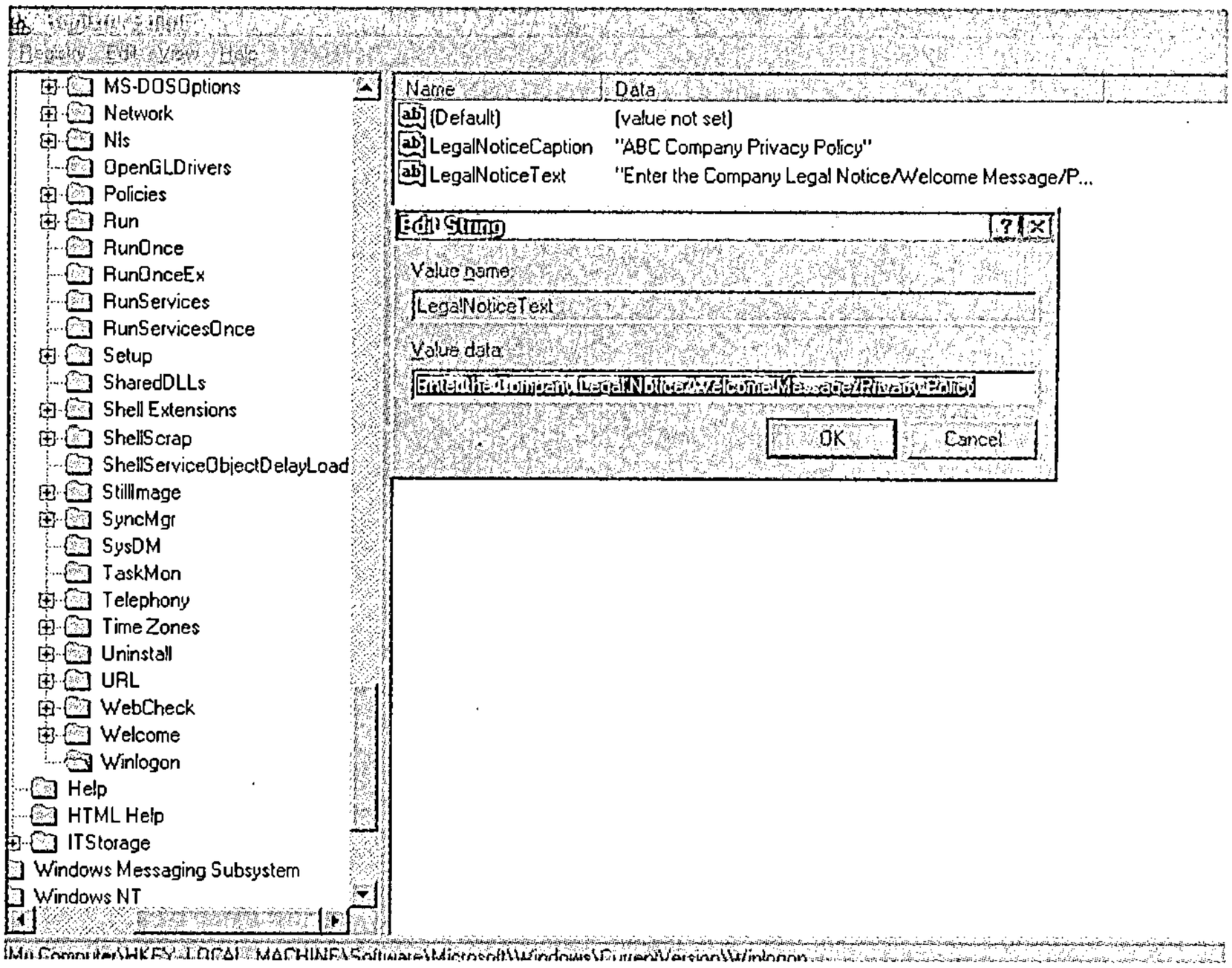

图 1-10　启动屏幕中的信息提示

5．退出 Windows 注册表，为使设置更改生效，需重新启动 Windows 系统。下次进入 Windows 时，就会看到所设置的内容。也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Winlogon]
LegalNoticeCaption"="输入标题信息"
LegalNoticeText"="输入正文信息"
```

1.12 按 Ctrl+Alt+Delete 键登录

（适用于 Windows 2000，和 XP 系统）

技术级别：低　　安全级别：高

在 Windows 系统开始身份认证过程之前，用户按 CTRL+ALT+DEL 键就可迫使系统正常登录。该功能可通过以下步骤实现：

1．打开 regedit.exe 文件。

2．寻找或新建以下注册键项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．新建一个名为 DisableCAD 的双字键值，设置该双字键值为 1 即可启用改限制，设置为 0 对其进行禁止。如图 1-11 所示。

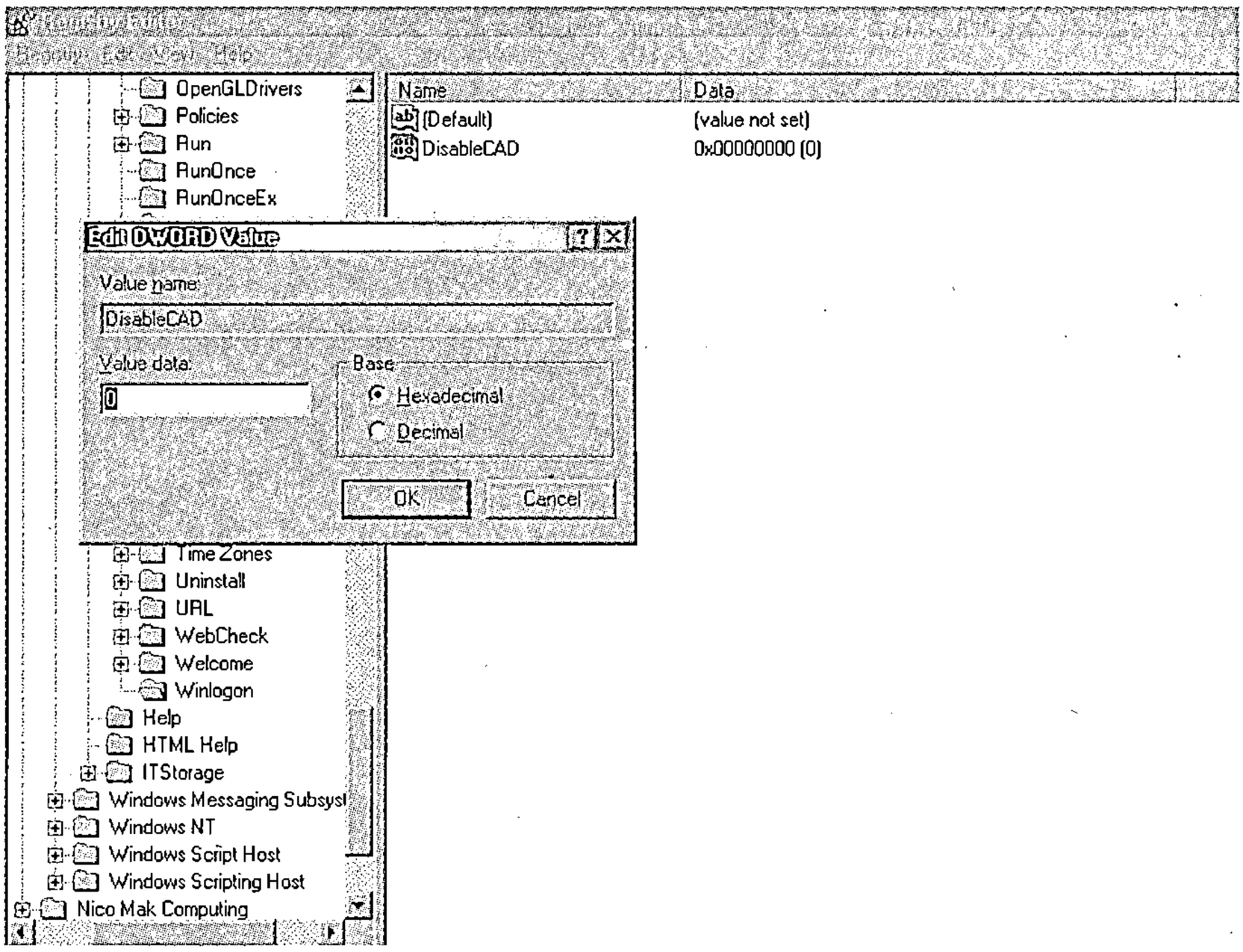

图 1-11　强制启动身份认证

4．退出 Windows 注册表，要使更改生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]
"DisableCAD"="0"
```

1.13 绕过 Windows 屏幕保护密码（一）

（适用于所有 Windows 版本）

技术级别：高　　安全级别：高

多数 Windows 用户喜欢设置屏幕保护程序，其初衷可能是由于屏幕保护比较好看！同时，用户也可以对屏幕保护进行密码设置。换句话说，如果屏保有密码保护，一旦启动了屏保，就需要正确的密码才能使它停止。假设忘记了自己的 Windows 屏幕保护程序密码，或由于种种原因想要重新设置朋友的屏幕保护程序密码，该如何实现呢?

以下几个步骤即可避开 Windows 屏幕保护密码保护：

1．打开 regedit.exe 文件。

2．寻找以下注册键：

HKEY_CURRENT_USER\Control Panel\Desktop

3．清空 *ScreenSave_Data* 键值即可取消屏幕保护密码。如图 1-12 所示。

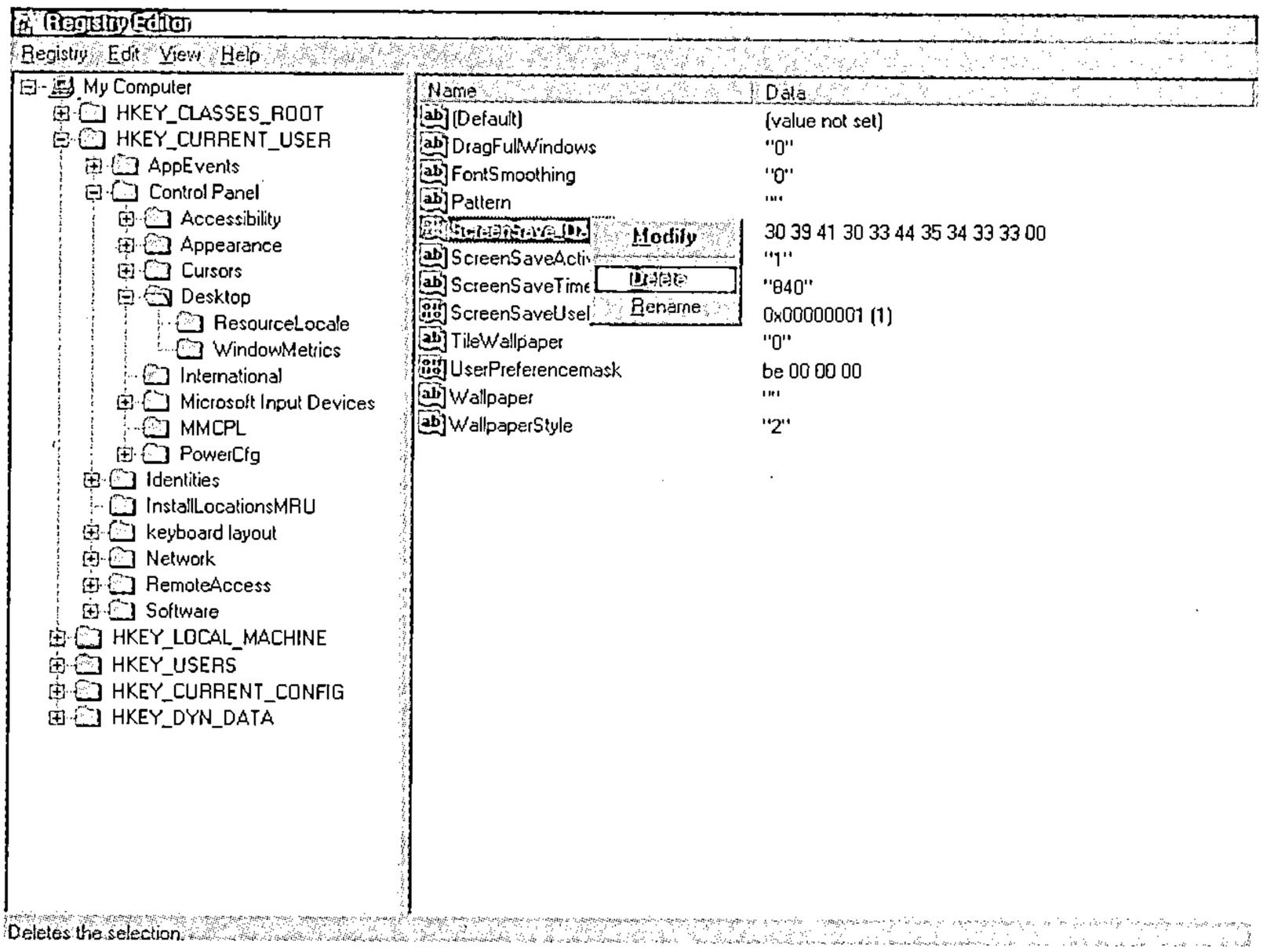

图 1-12　取消屏保密码

4．退出 Windows 注册表，为了让改变生效，需重新启动 Windows 系统。下次在运行屏保程序的计算机时，不管在密码提示框中输入什么密码，用户都可以正常登录系统。

1.14　绕过 Windows 屏幕保护密码（二）

（适用于所有 Windows 版本）

技术级别：高　　安全级别：高

通过另外一种方法也可以取消 Windows 屏幕保护密码，主要操作步骤如下：

1．在系统目录中找到屏幕保护文件。例如，3dpipe~1.scr。

2．在 MS DOS 编辑器中打开上述屏幕保护文件：

c:\>cd winnt

c:\winnt>cd system32

c:\winnt\system32>edit /70 3dpipe~1.scr

3．找到以下的字符串:

VerifyScreenSavePwd

该关键字指示操作系统弹出屏幕保护密码对话框。在没有该关键字的情况下，系统将不允许用户进行任何操作。

1．可以对上述字符串的任意一个字符进行修改，比如，将其修改为VarifyScreenSavePwd。

2．保存文件并退出 MS DOS 编辑器。当下次进入系统并激活屏幕保护程序时，由于修改了 VerifyScreenSavePwd 关键字，因此不会显示输入密码的提示对话框。

1.15 禁用 Windows 屏幕保护

（适用所有 Windows 版本）

技术级别：高　　安全级别：高

通过执行以下操行，就可以完全禁用 Windows 屏幕保护程序:

1．打开 regedit.exe 文件。

2．寻找以下注册键:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\ControlPanel\Desktop

3．在上述注册键中新建一个名为 ScreenSaveActive 的双字键值，将其双字键值设置为 1 即可启用该限制，设置为 0 即可实现对其进行禁用，如图 1-13 所示。

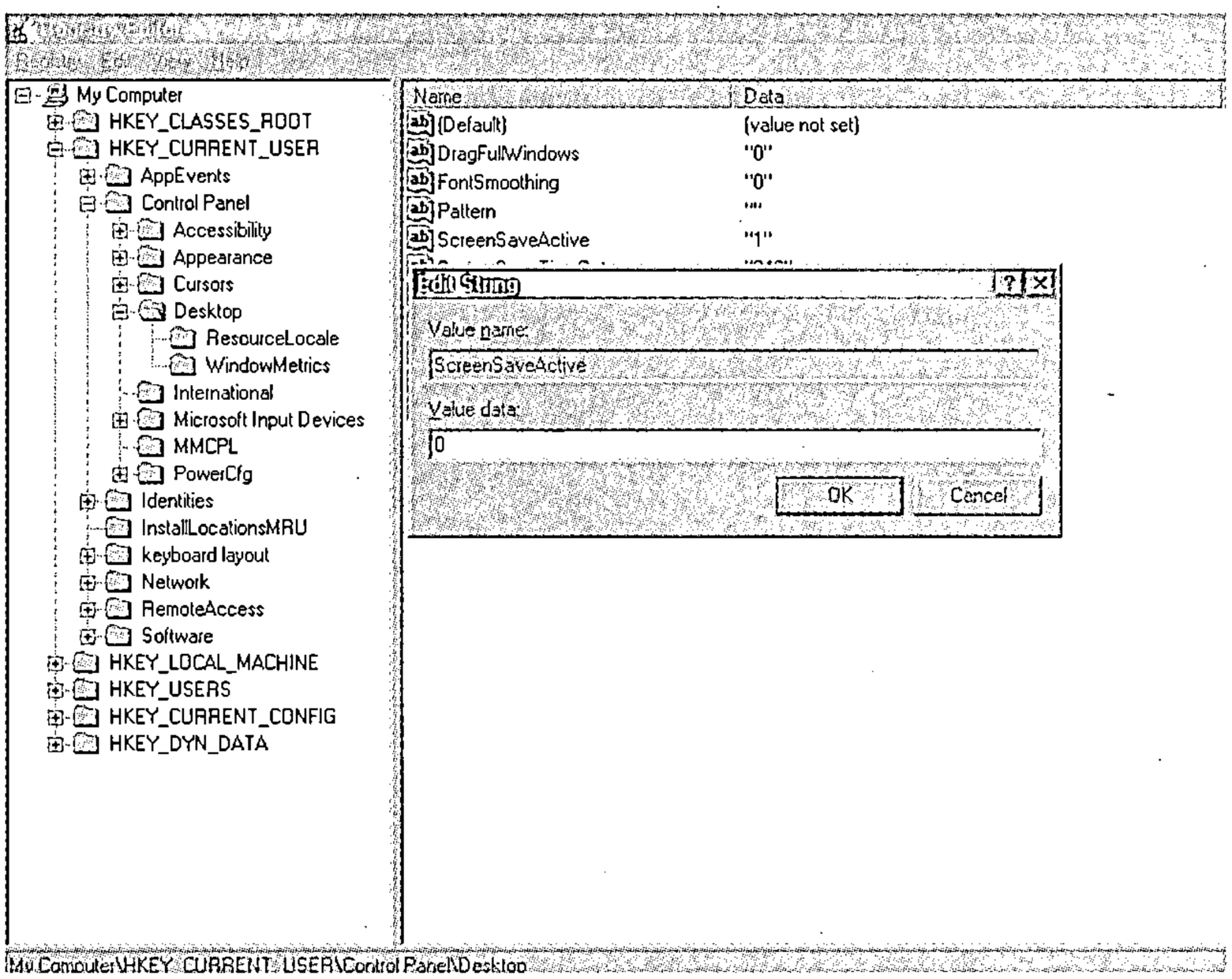

图 1-13　禁用 Windows 屏保程序

4．退出 Windows 注册表，为了使更改生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop]
"ScreenSaveActive"="0"
```

1.16 屏保密码提示中强制重新登录

（适用于 Windows 2000，Windows NT 和 Windows XP 系统）

技术级别：低　　安全级别：高

在 Windows 屏保密码程序运行时，只有正确输入屏保密码才能正常登录系统。也就是说，如果用户输入的密码不能通过系统验证，系统将保持锁定状态。为能有效地防止恶意攻击等非法入侵行为威胁，较好的方法就是强迫 Windows 对用户登录信息进行验证，以增强系统的安全性。该功能可通过以下步骤实现：

1．打开 regedit.exe 文件。

2．寻找以下注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．在该键项中新建一个名为 *ForceUnlockLogon* 的双字键值，将该双字键值设为 1 即可启用该限制，设置为 0 对其进行禁用，如图 1-14 所示。

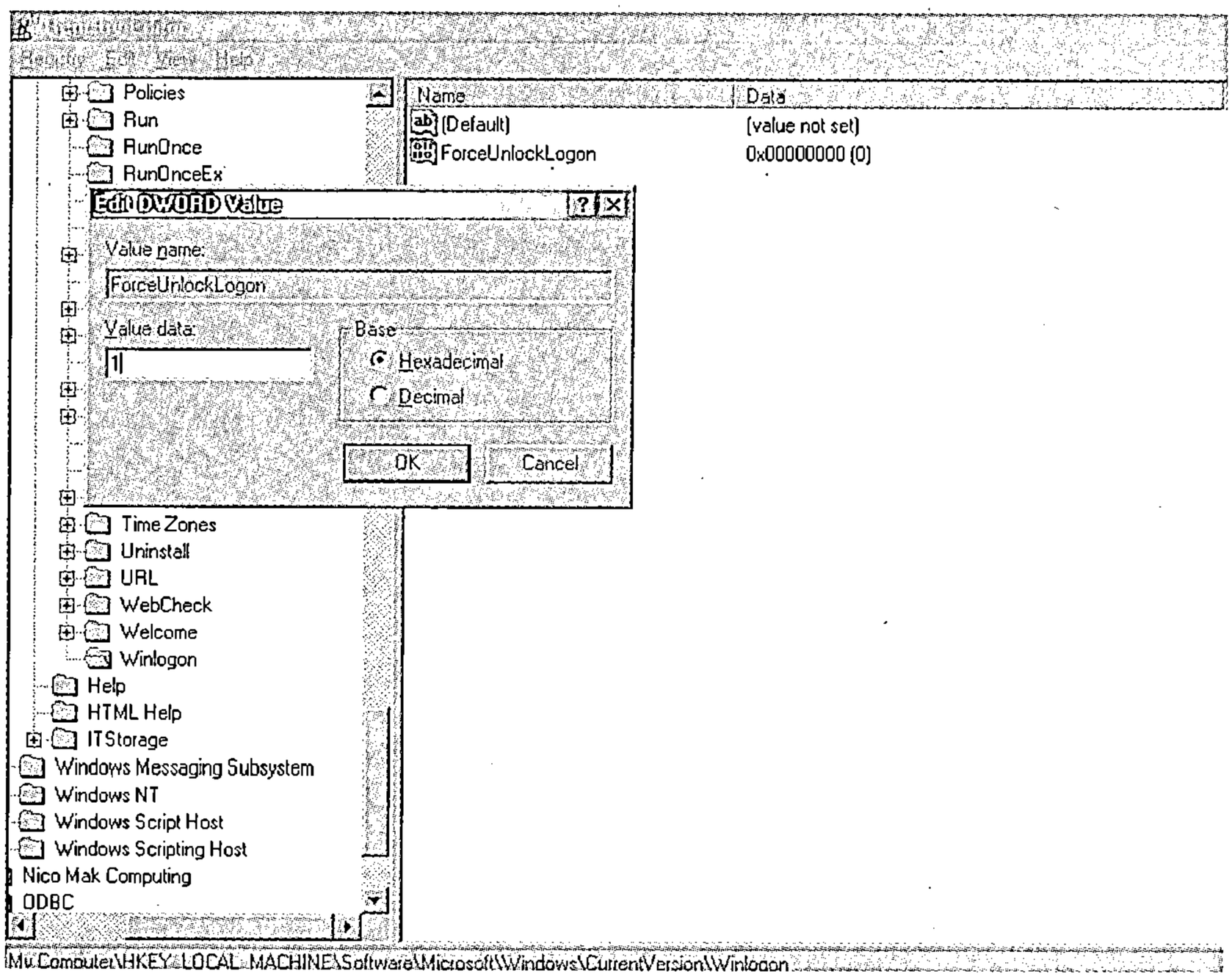

图 1-14　屏保密码提示中强制重新登录

4．退出 Windows 注册表，为使设置更改生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Network\Logon]
"ForceUnlockLogon"="1"
```

1.17 登录时禁用密码提示

（适用于所有 Windows 9x 系统）

技术级别：中等　　安全级别：低

在每次启动 Windows 系统时，系统都要求用户在密码提示对话框中输入正确的用户名和密码。有时这项限制可能会引起用户反感，并希望 Windows 在每次启动时都不出现该提示。可以通过以下步骤在登录系统时阻止该对话框出现：

1．登录密码信息被存储在 Windows 系统中后缀名为.pwl 的密码文件里。需要在系统里寻找所有的.pwl 文件并将其删除。如图 1-15 所示。

2．在下次登录 Windows 系统时，不需要在该对话框中输入任何值。这样密码提示将不会再次出现。

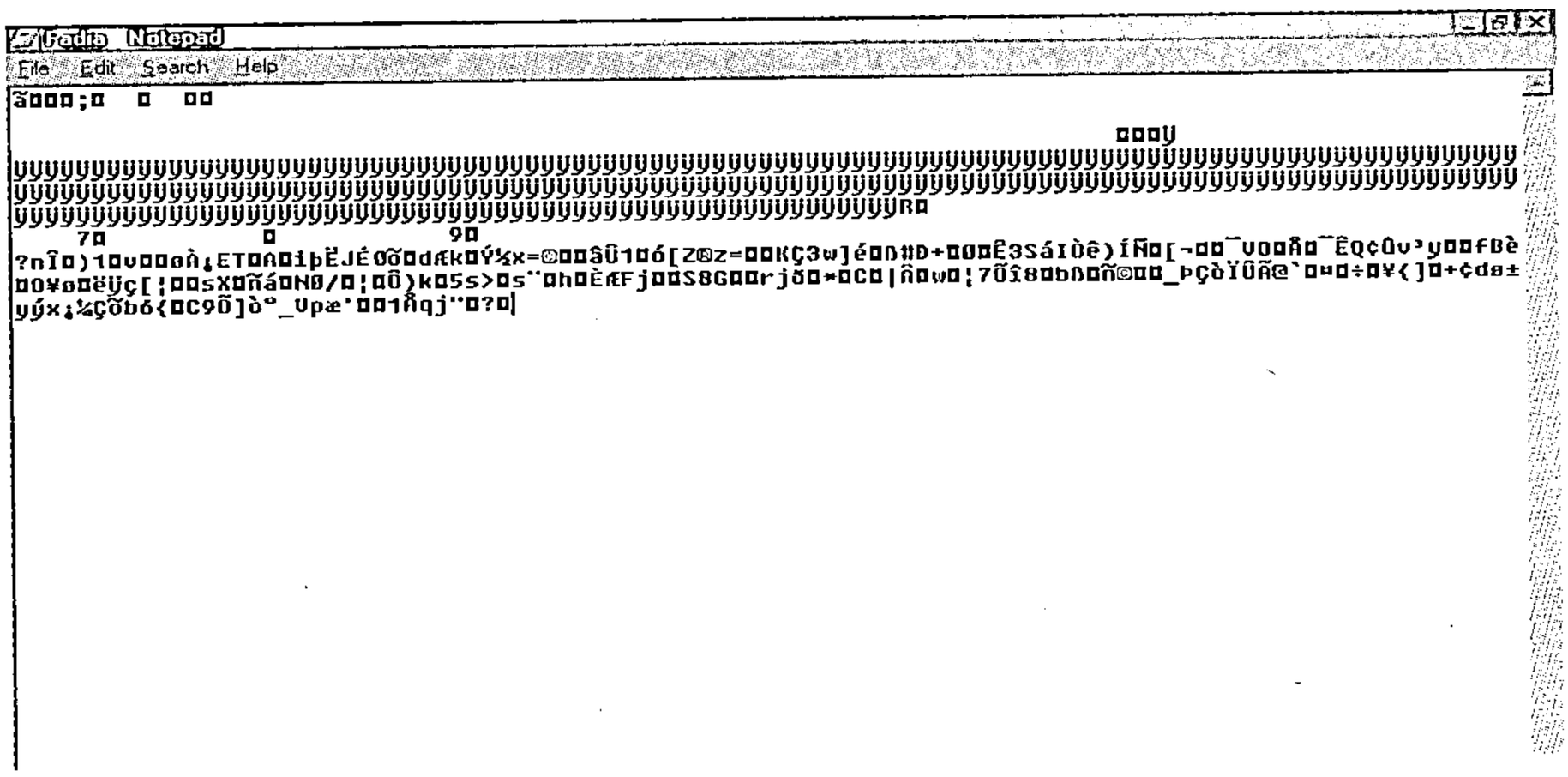

图 1-15　.PWL 密码文件

1.18 禁止密码提示中的取消键

（适用于 Windows 95，98 和 Me 系统）

技术级别：低　　安全级别：高

几乎所有的 Windows 系统都允许多用户使用同一个系统，并根据用户名和密码进行身分验证。不幸的是，在 Windows 的较低版本中，用户简单地点击取消按钮就能轻易地绕过

密码验证过程。因此，许多系统管理员利用以下方法强制进行用户身份验证：

1．打开 regedit.exe 文件。

2．寻找以下注册键：

HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run

3．新建一个名为 NoLogon 的字符串键项，将其值设置为：

RUNDLL32 shell32,SHExitWindowsEx0

4．退出 Windows 注册表，为使设置更改生效，需重新启动 Windows 系统。下次登录系统时，点击密码提示中的取消按钮将不能绕过用户登录的身份认证过程，也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
 [HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\ Run]
"NoLogon"="RUNDLL32 shell32,SHExit WindowsEx 0"
```

1.19 禁止密码更改选项

（适用于 Windows 2000，Me，XP 和 NT 系统）

技术级别：低　　安全级别：高

通过以下步骤即可在安全设置页中将密码更改选项失效：

1．打开 regedit.exe 文件

2．寻找以下注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

3．新建一个名为 DisableChangePassword 的双字字符串键值，将其值设置为 0 即可启用该限制，设置为 1 即可禁止该限制。

4．类似地，也可以创建一个名为 *DisableLockWorkstation* 的双字键值，用于防止用户无意或有意地锁定电脑。

5．退出 Windows 注册表，为使设置更改生效，需重新启动 Windows 系统。

也可以通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableChangePassword"="1"
"DisableLockWorkstation"="1"
```

1.20 解除所有 Windows 密码

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

如今，多数用户不但在 Windows 登录过程中使用密码保护，而且也开始使用内置的密码保护机制保护各种各样的应用文件。不幸的是，这些密码保护机制的安全性很差。借助于互联网上的小工具就可以轻松地破解所设定的各种密码。表 1-1 列出了一些常用的 Windows 应用以及破解这些密码保护的相应工具，图 1-16 为 Office 文件破解工具，图 1-17 为即时消息口令破解工具，图 1-18 为压缩文件破解工具，图 1-19 为 Web 密码破解工具。

表 1-1 常用 Windows 密码破解工具

Windows 应用	密码破解工具
压缩文件	Advanced ZIP Password Recovery
所有即时信使	Advanced Instant Messenger Password Recovery
Windows 登录密码	L0phtcrack
Outlook Express, Eudora Pro 等邮件客户端	Advanced Mailbox Password Recovery
Adobe Acrobat PDF 文件	Advanced PDF Password Recovery
Microsoft Office 密码	Office Key
所有 Windows 密码	Advanced Windows Password Recovery
Internet Explorer 密码	Internet Explorer Password Recovery
文件生成器密码	File Maker Key
Web 密码	WebBrute

冒着被指责的危险向大家推荐《script kiddies》这本书，该书附带的 CD 光盘中包含了一些黑客所使用的最普遍和最流行的密码破解工具。

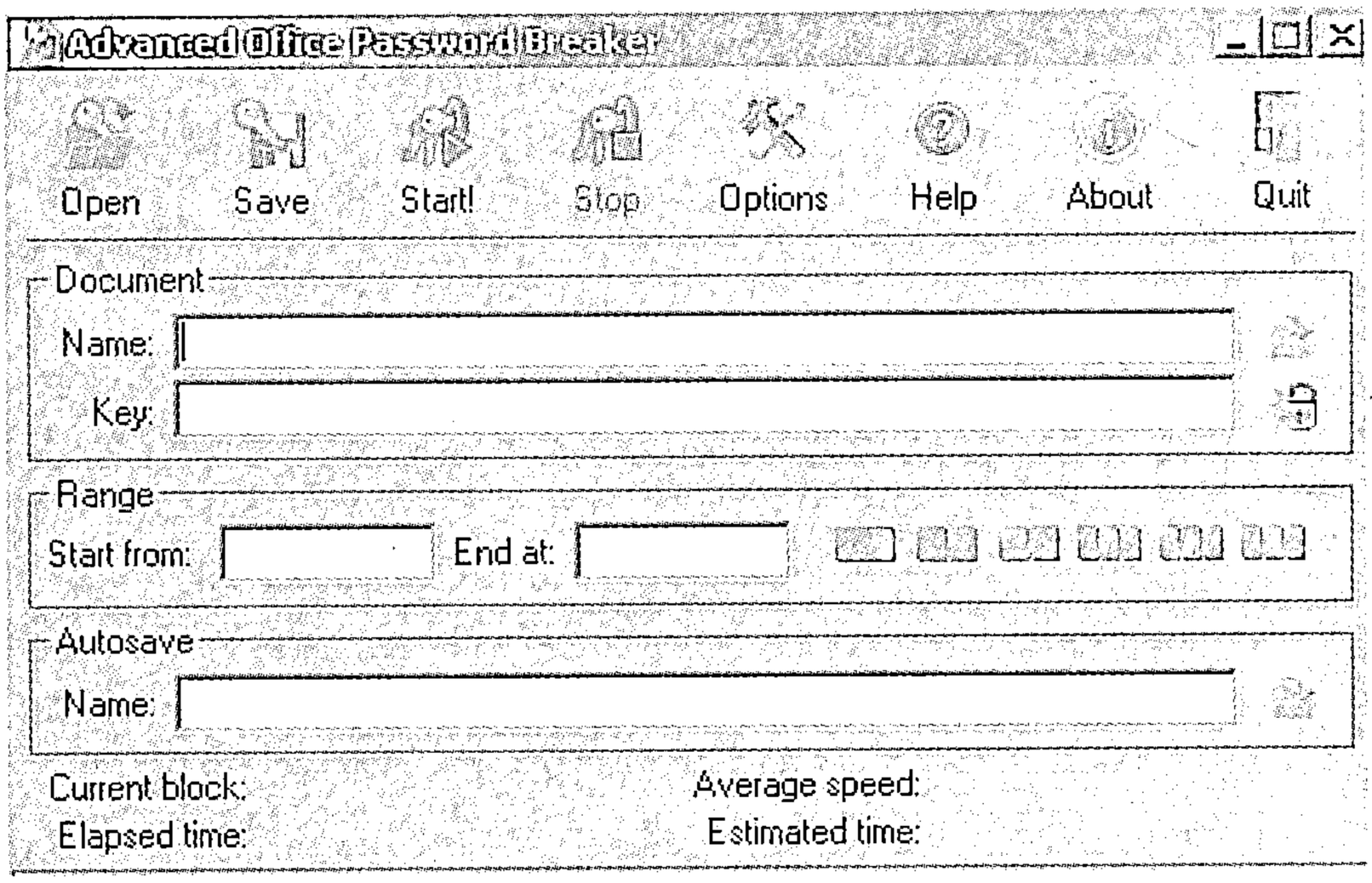

图 1-16 Office 文件破解

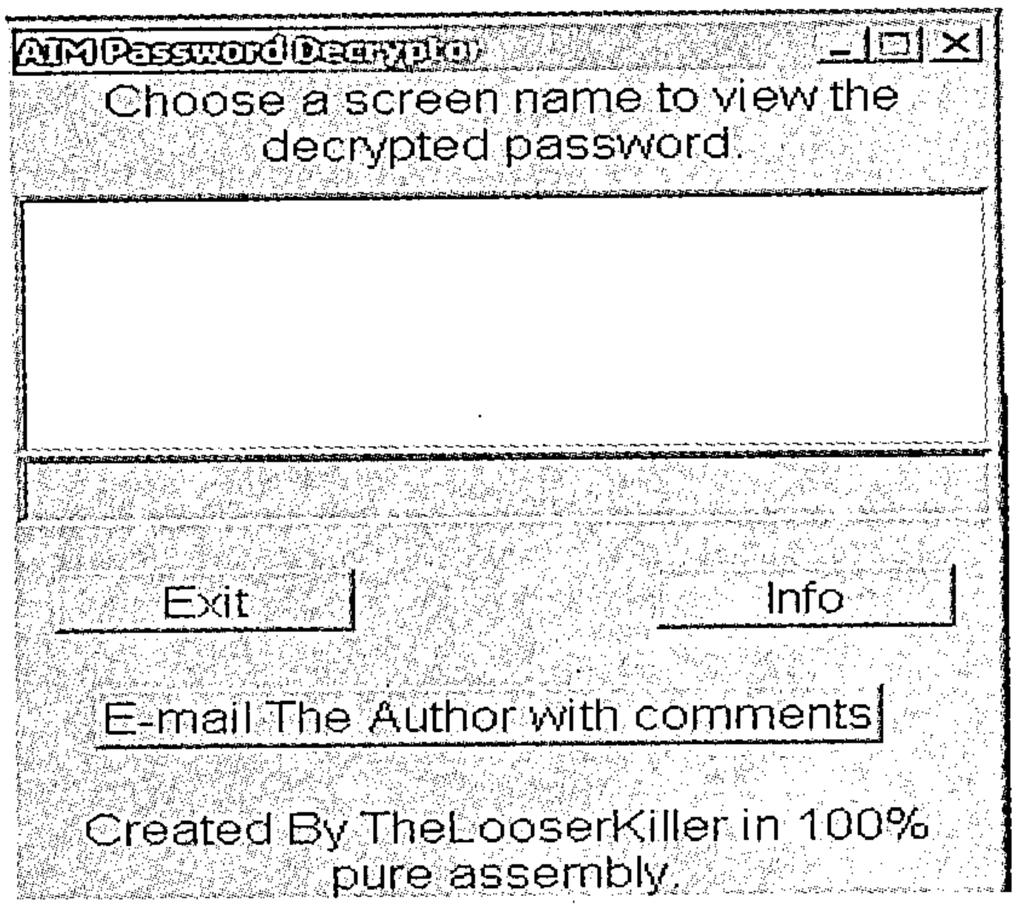

图 1-17　即时消息口令破解

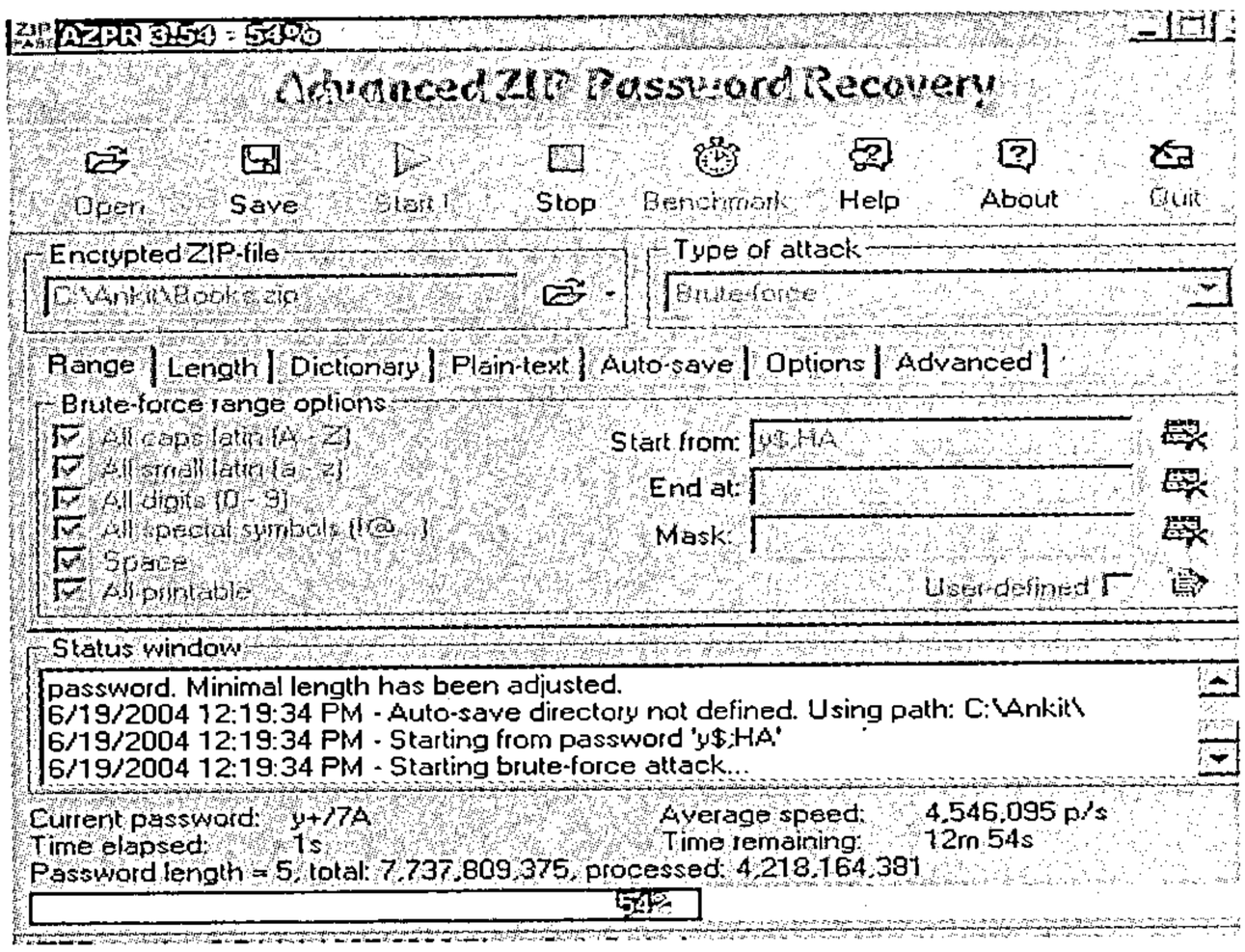

图 1-18　压缩文件口令破解

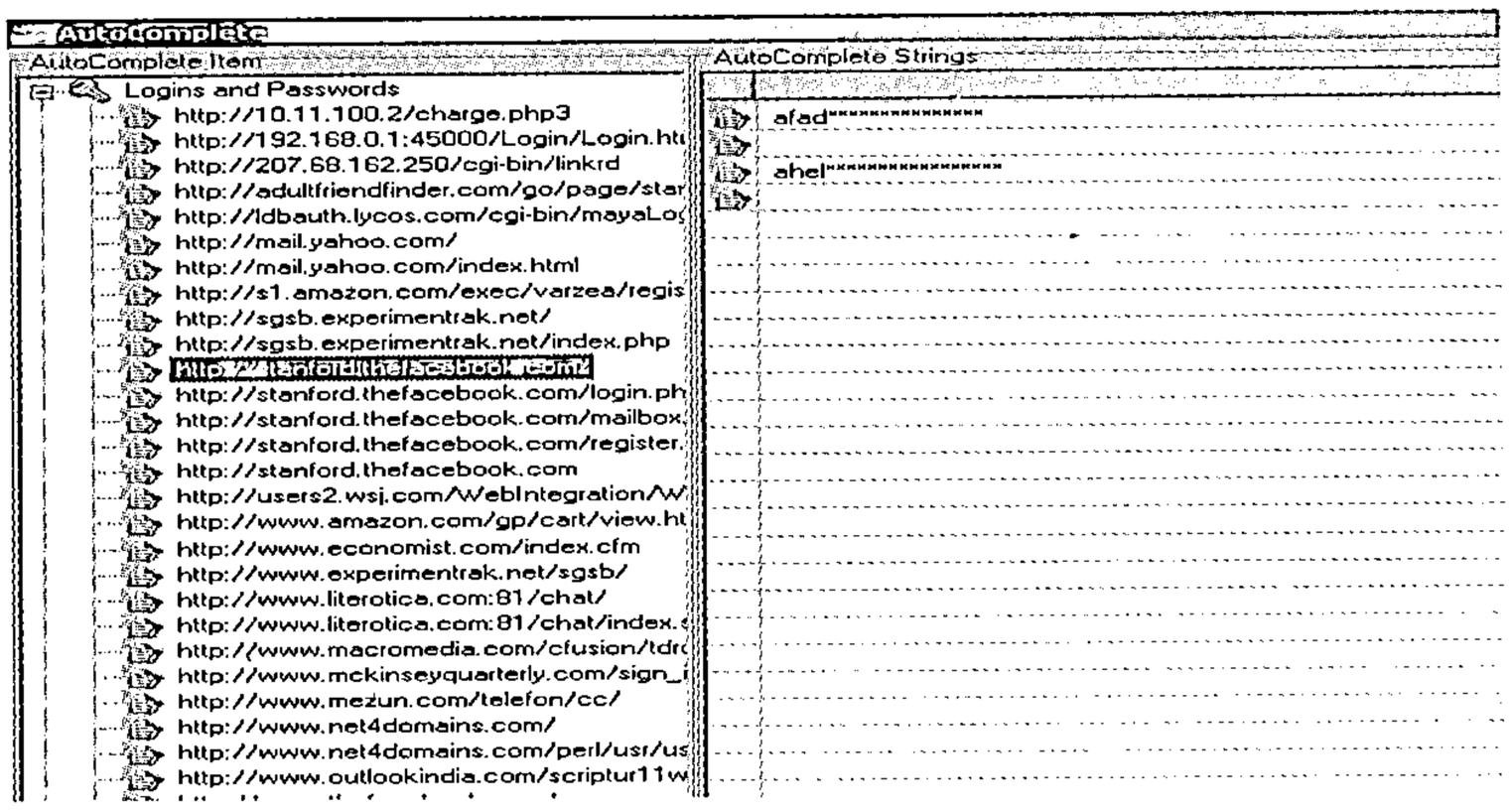

图 1-19　Web 口令破解

第二章　定制 Windows 安全环境

2.1 引言

全世界范围内数以百万计的计算机系统中运行着 Windows 操作系统。然而，有时候人们就会觉得 Windows 系统的外观非常呆板、平庸并且令人厌烦。世界范围内所有的 Windows 系统通常都运行着类似的窗口，屏幕左下角有一个开始按钮，右下角有一个时钟，用户点击屏幕某个区域时都会弹出相同内容的菜单等等。因此，屏幕底部的工具条保持了 Windows 操作系统非常普通的外观特性。此外，微软更倾向于让 Windows 系统给人以高深莫测的印象，使大家误认为不可能对 Windows 的传统外观进行更改。

实际上，许多人已经开始使用第三方应用程序，对 Windows 操作系统的外观进行更改。然而，人们使用这些第三方应用软件或许不能按照自己的意愿随意更改与美化操作系统外观。本节我们将学习各种有趣的技巧、诡计和诀窍，用于定制 Windows 外观、功能等特性，以符合您的个人需要和喜好。

警告：尽管本节中用到的所有例子已经在各种平台上得到测试，但还是强烈建议备份所有的系统文件，以避免发生任何意外损失。

2.2 定制开始菜单和关机屏幕

（适用于 Windows9x 的所有版本）

技术级别：高　　安全级别：低

有时您会认为 Windows 默认的欢迎和关机屏幕很平凡，甚者会感觉厌烦。事实上，我们可以简单地通过下面步骤修改这两个屏幕画面，使得 Windows 的外观更加生动有趣。

1．首先备份 Logos.sys 文件（关机屏幕图像文件通常保存在 c:\windows 目录下）以及 Logo.sys 文件（开机屏幕图像文件通常保存在 c:\根目录下）。

2．将 Logos.sys 和 Logo.sys 扩展名更改为.bmp。

3．现在，就可以通过图像编辑器，将个人偏好添加到这些图像文件中。

4．最后，将这些修改后的文件更改为原始的文件名并替代原有的文件。

5．在下一次启动 Windows 系统时，开机和关机屏幕将会被定制的图像文件所替代，如图 2-1 所示。

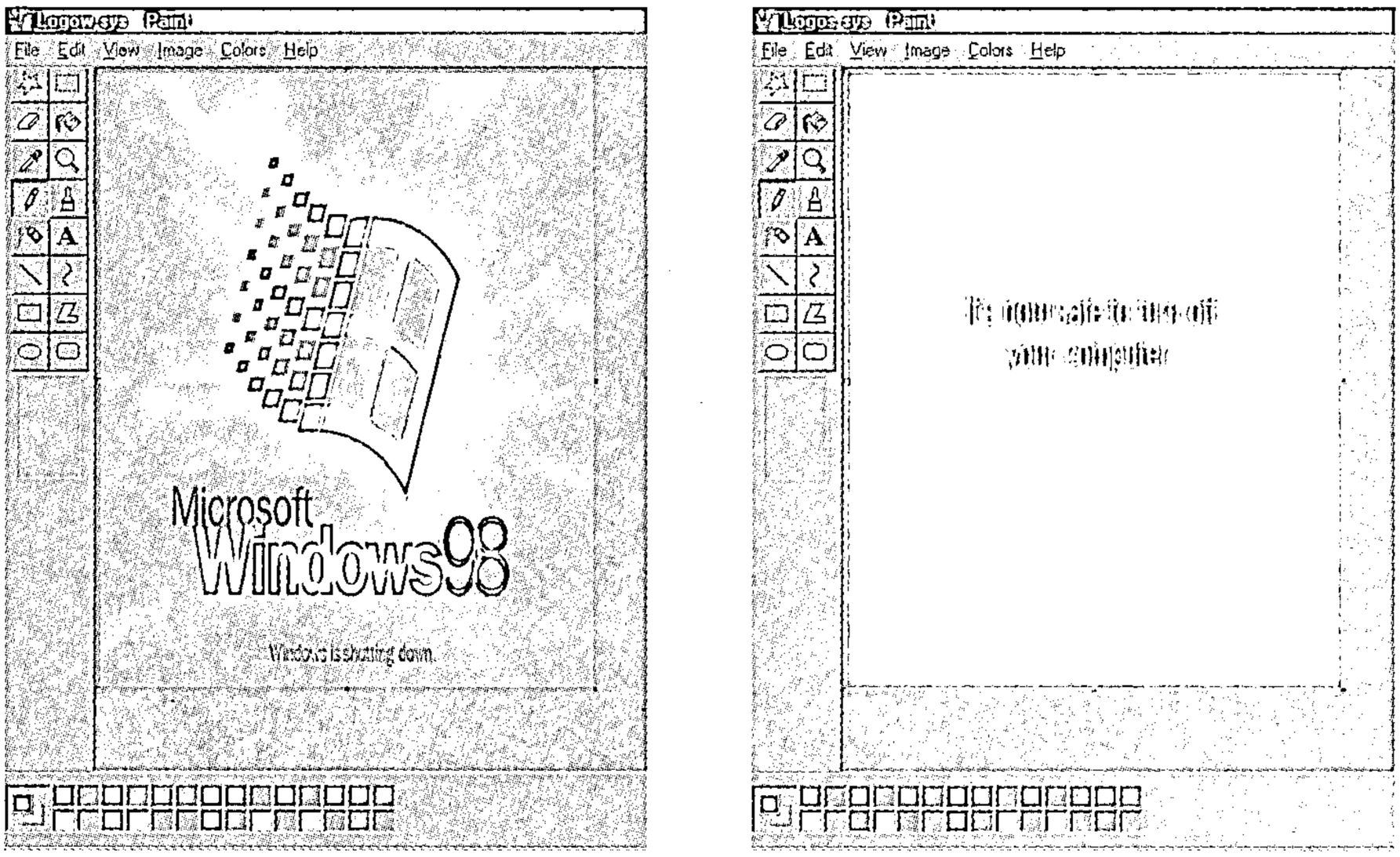

图 2-1　定制开机屏幕

2.3　禁用 Windows 热键

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：中等

通过下面的步骤，就可以防止用户使用 Windows 的快捷键，比如 Alt + Tab 等。

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

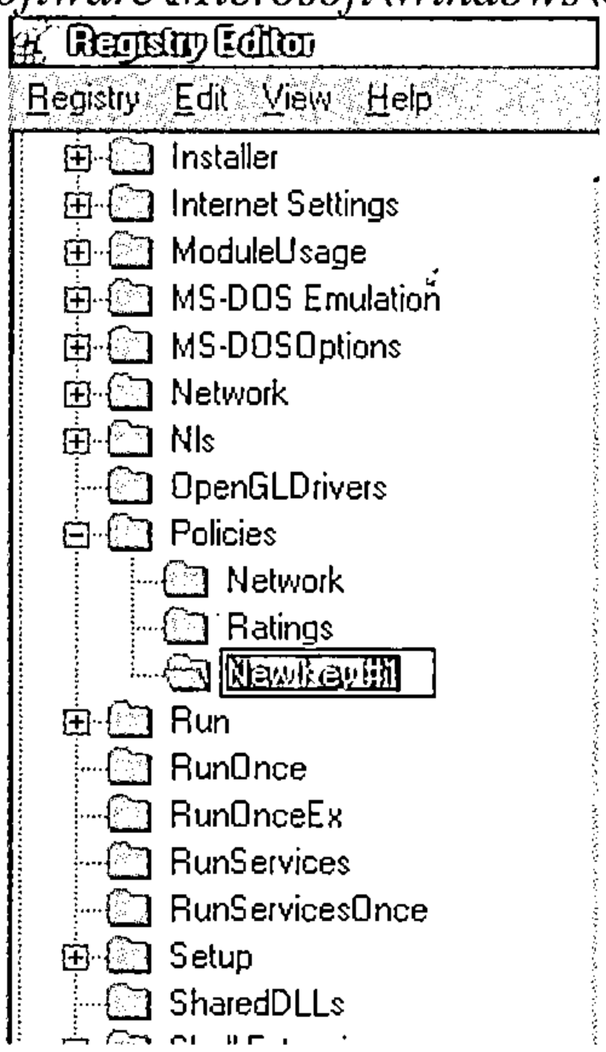

图 2-2　建立新键

3．在以上的注册键中建立一个新的双字键值，将其命名为 *NoWinKeys*，并将其初值设为 1 以禁用 Windows 热键，设置为 0 就可以激活这些热键，如图 2-2，2-3 所示。

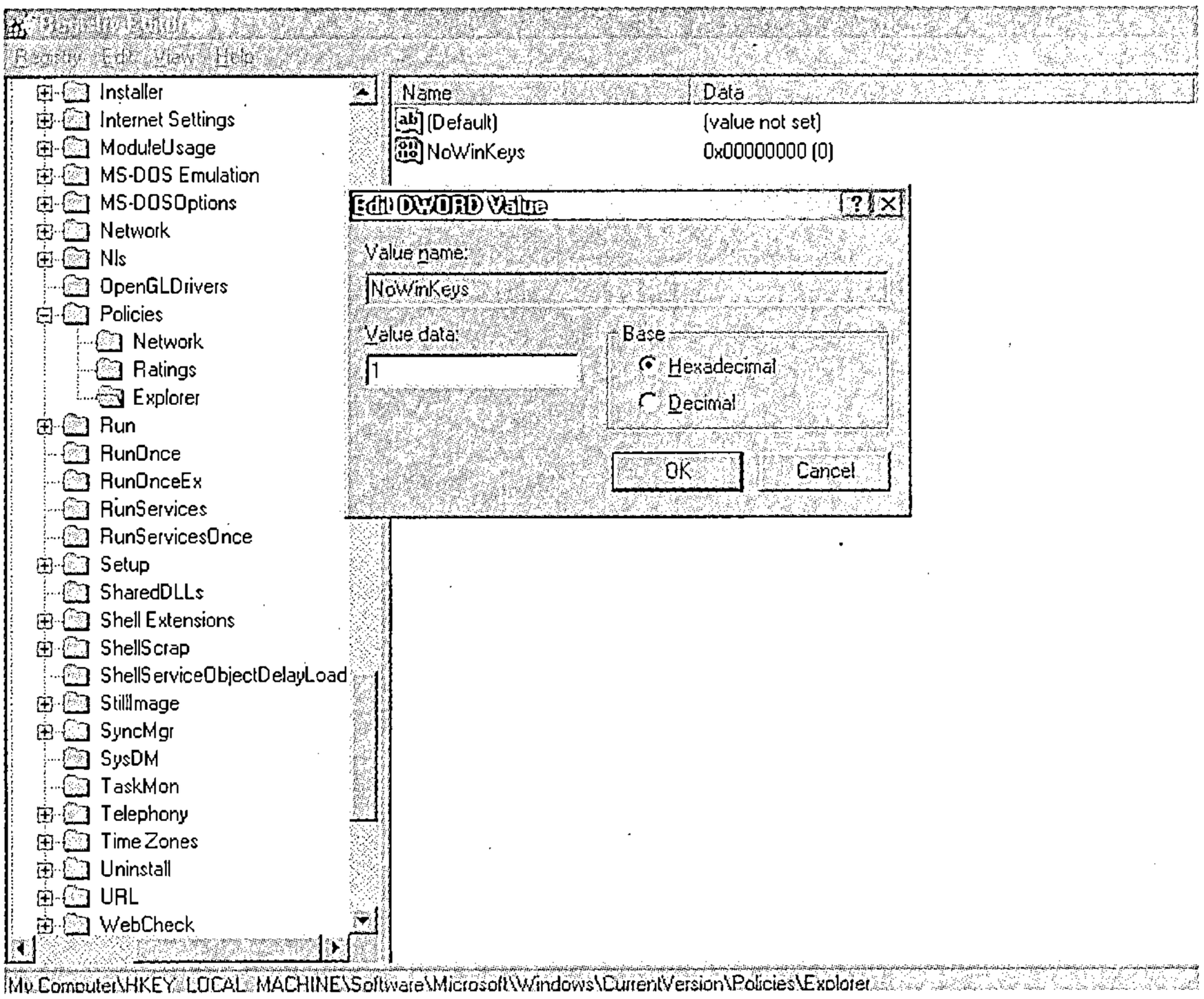

图 2-3　禁止 Windows 热键

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoWinKeys"="1"
```

2.4　禁用桌面右键

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

通常情况下，每次右击桌面时屏幕上都会弹出一个包含诸如粘贴、复制、属性以及其它项目的菜单，如图 2-4 所示。

可以通过以下步骤禁止用户对其进行操作。

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

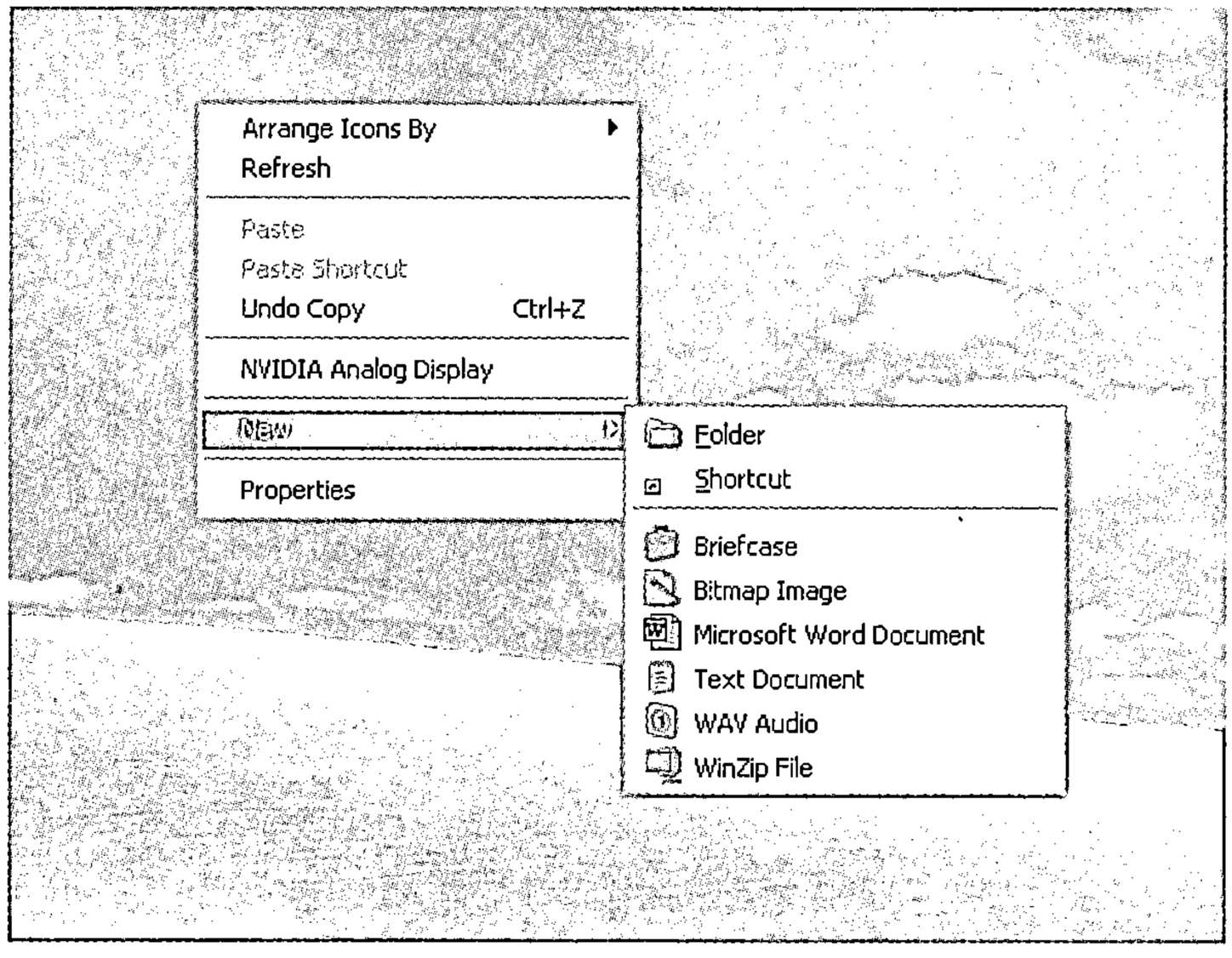

图 2-4　桌面单击右键出现快捷菜单

3．在以上的注册键中建立一个新的双字键值，将其命名为 *NoViewContentMenu*，并将其初值设为 1 以禁用 Windows 热键，设置为 0 就可以激活这些热键，如图 2-5 所示。

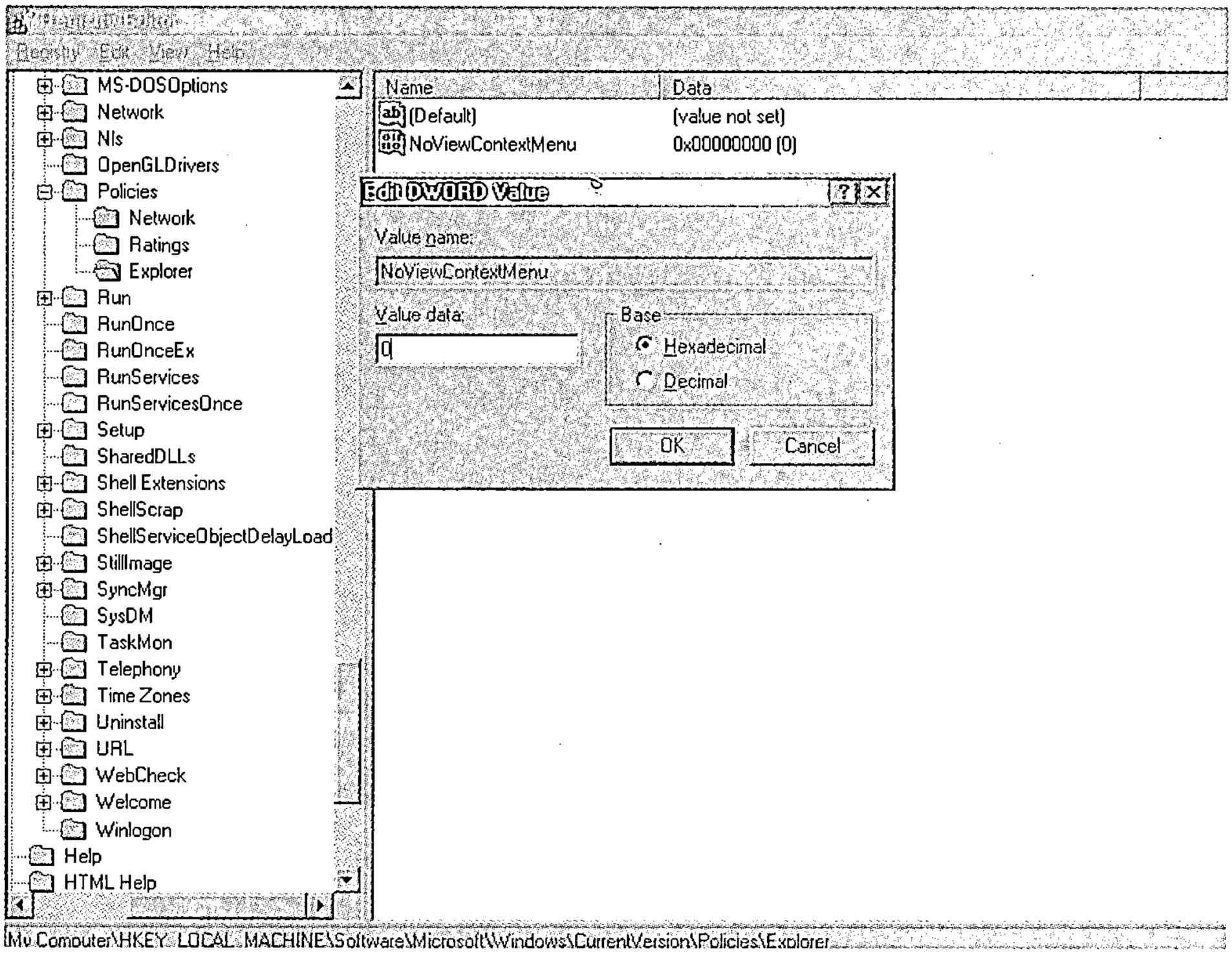

图 2-5　禁用桌面右键快捷菜单

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoViewContextMenu"="0"
```

2.5 禁用开始菜单右键

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

通常情况下，每次右击开始菜单时屏幕上都会弹出一个包含诸如打开、浏览、搜索以及其他项目的菜单，如图 2-6 所示。

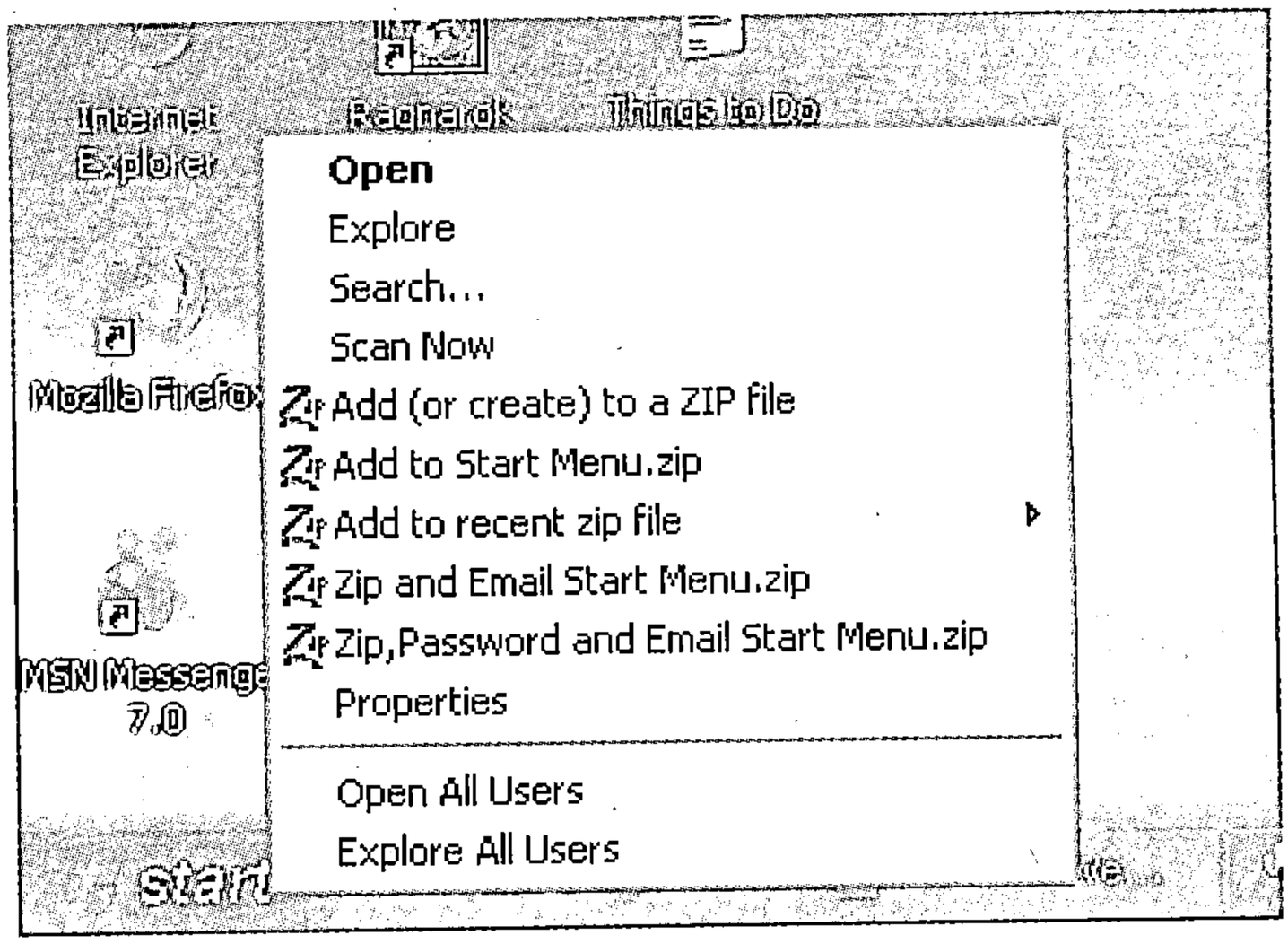

图 2-6　开始菜单右键图例

实际上，可以通过以下技巧禁用这些菜单项：

1．打开 regedit.exe 文件。

2．搜索以下注册键：

HKEY_CLASSES_ROOT\Directory\shell

将其从 shell 重新命名为 shell.old。

3．搜索以下注册键：

HKEY_CLASSES_ROOT\Folder\shell

将其从 shell 重新命名为 shell.old。

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。如图 2-7 所示。

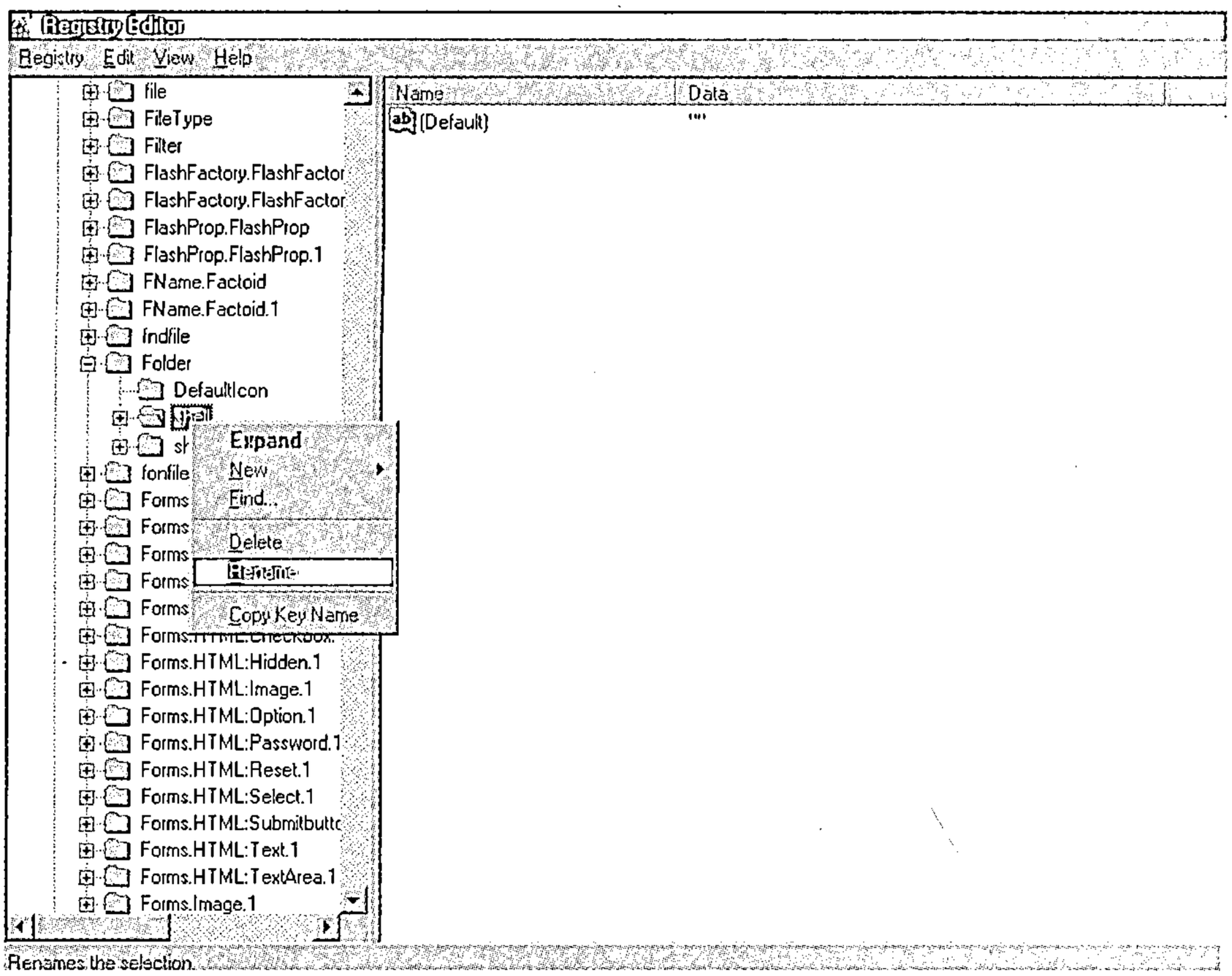

图 2-7　禁用开始菜单右键

2.6　定制开始菜单右键菜单

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：低

上述例子中我们学习了如何禁止用户右击开始菜单。实际上，可以定制该右击菜单的内容，并添加新的项目或者链接到一个应用程序，如图 2-8 所示。可通过下面方法实现该功能：

1．打开 regedit.exe 文件。

2．搜索以下注册键：

HKEY_CLASSES_ROOT\Directory\Shell

3．在以上的注册键中建立一个新的子键，该子键中包含了预添加到右击菜单中的应用程序的名字。该名字也就是在开始按钮右击菜单项中所显示的文本内容。比如，如果您想添加 *Notepad* 到该菜单中，就需要将新的子键命名为 *Notepad*。

4．接下来，在该键中建立另外一个子键，将其命名为 Command。该新建的字符将在右侧面板中自动显示。

4．更改注册表右侧面板中新建的字符串值，并将该值指向预添加到菜单项中应用程序的完整路径名。比如，在上例中我们想将记事本添加到菜单项中，就需要将该字符串的数值指向该记事本应用程序文件的路径。

5．退出 Windows 注册表。重新启动 Windows 系统，方可使更改生效。在下次右击开

始按钮时，一个新的记事本项将出现在该菜单中。

图 2-8　定制开始菜单右键菜单

同时，我们通过删除以下的注册键中特定的子键也可以从该右击菜单中删去相应的菜单项目。

HKEY_CLASSES_ROOT\Directory\Shell

2.7　禁用开始按钮和 Windows 菜单栏

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

通过以下步骤就能很容易地完全禁用开始按钮和 Windows 菜单栏：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_CLASSES_ROOT\CLSID\{5b4dae26-b807-11d0-9815-00c04fd91972}

3．将以上的键重新命名为：

*HKEY_CLASSES_ROOT\CLSID\{*5b4dae26-b807-11d0-9815-00c04fd91972}*

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。此时，开始按钮和标准菜单栏将全部消失，如图 2-9 所示。

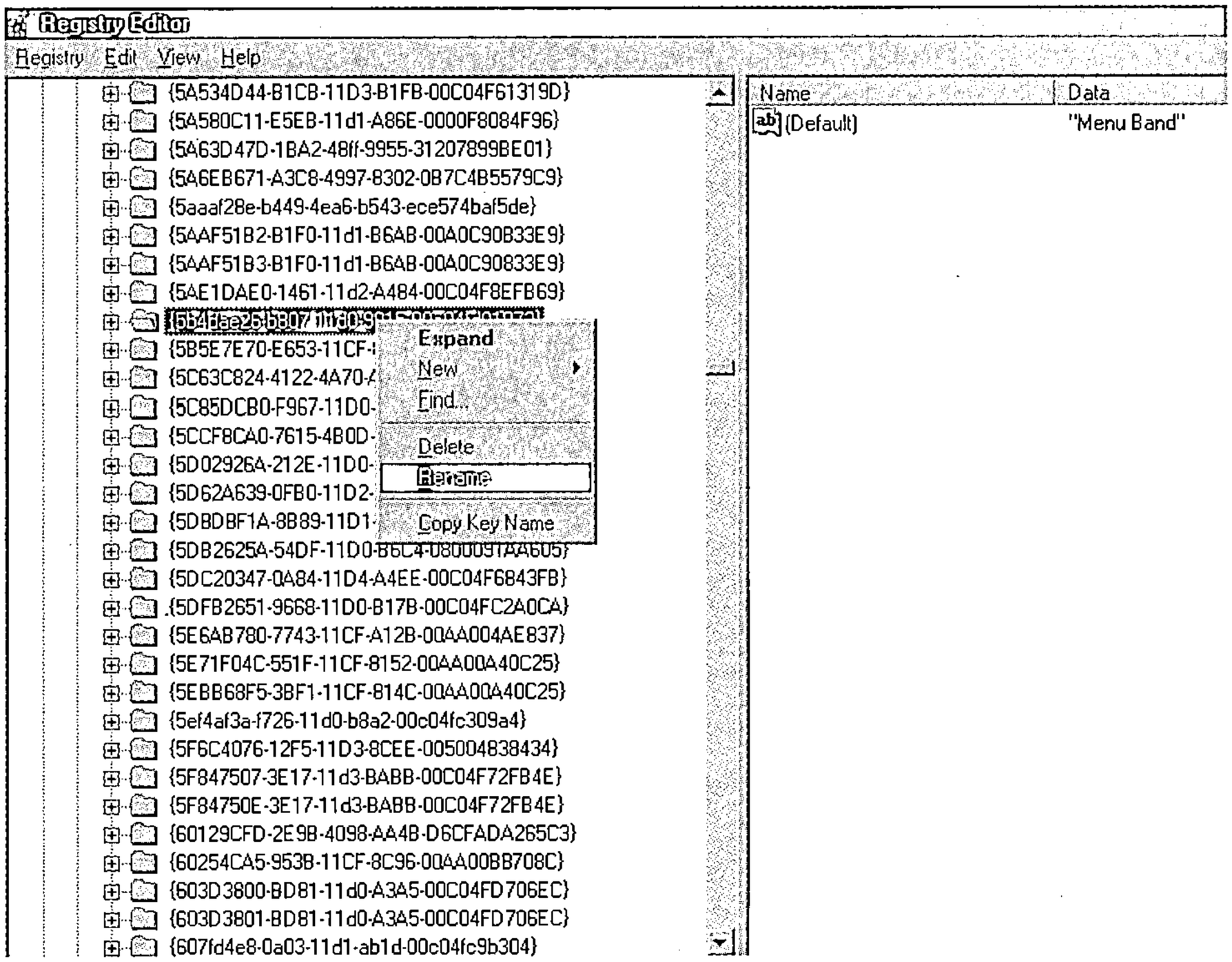

图 2-9　禁用开始按钮和 Windows 菜单栏

2.8　锁定工具栏

（适用于 Windows 所有版本）

技术级别：低　　安全级别：中等

一般情况下，Windows 用户可以简单地通过视图>工具栏选项定制、禁用或启动各种工具栏。然而，对于系统管理员就可以锁定工具栏，并禁止用户对工具栏的各种选项进行操作。以上功能可通过以下步骤实现：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．在以上的注册键中建立一个新的双字键值，将其命名为 *NoBandCustomize*，并将其初值设为 1 以禁用 Windows 热键，设置为 0 就可以激活这些热键，如图 2-10 所示。

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoBandCustomize"="1"
```

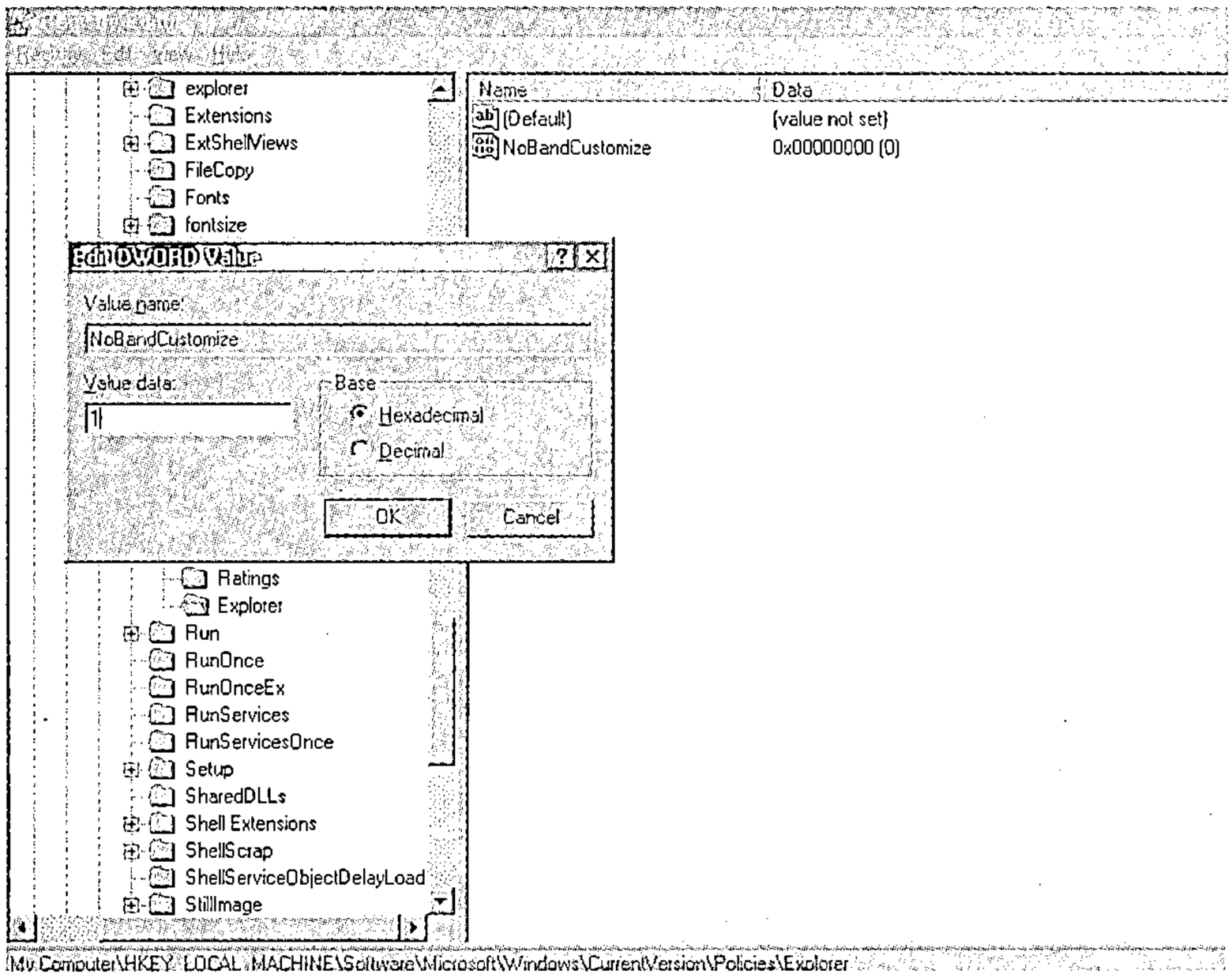

图 2-10　锁定工具栏

2.9　禁止新建菜单项目

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

通常，在每次右击桌面或一个文件夹时，都会出现一个“新建”菜单项目，允许用户新建一个对象、快捷键等。实际上，可以通过以下的 Windows 注册表技巧禁用该菜单项目：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_CLASSES_ROOT\CLSID\{D969A300-E7FF-11d0-A93B-00A0C90F2719}

将以上的键重新命名为：

*HKEY_CLASSES_ROOT\CLSID\{*D969A300-E7FF-11d0-A93B-00A0C90F2719}*，如图 2-11 所示。

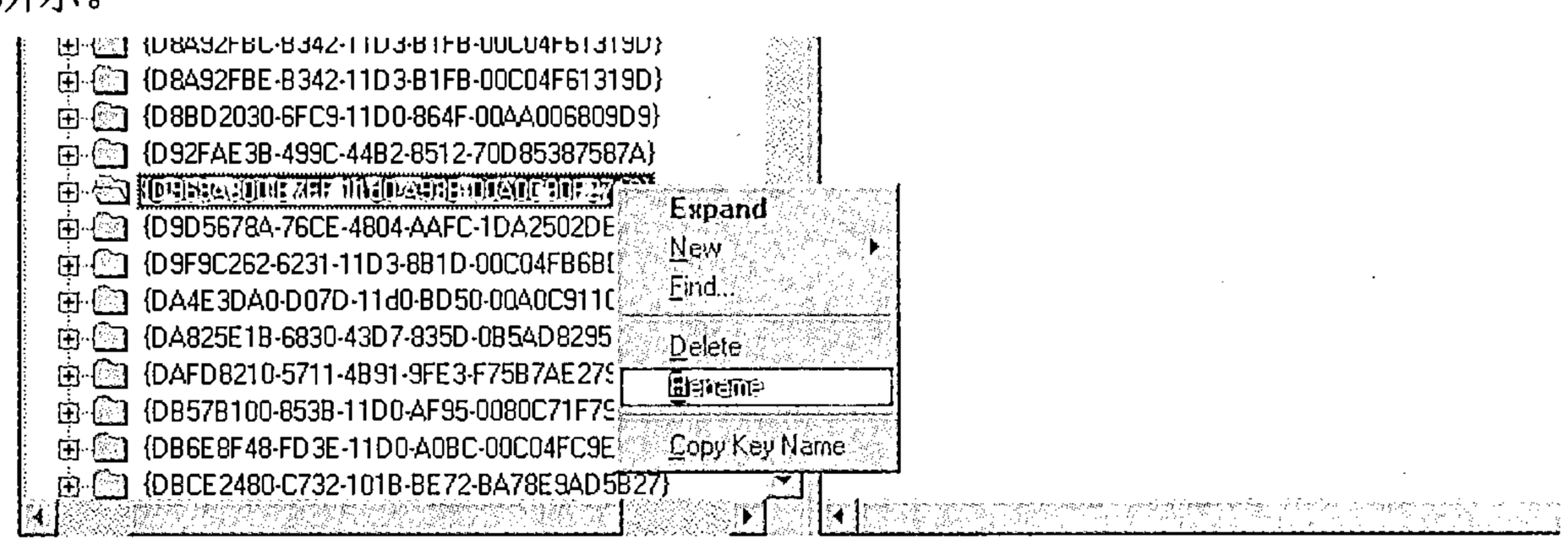

图 2-11　重命名以禁止新建菜单项目

4. 退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

2.10 禁止用户关机

（适用于 Windows 所有版本）

技术级别：高　　安全级别：高

作为系统管理员，可以禁止用户使用开始菜单的关机项目。该隐藏特性适用于所有 Windows 版本，系统管理员可以通过该属性的禁用，限制用户对机场候机厅、办公室、图书馆以及其他公共场所计算机的误用。对于那些爱开玩笑的人也可通过该技巧对他的朋友们施展一下小伎俩。通过下面步骤就可以实现对关机选项的禁用：

1. 在 Windows 根目录下打开 *regedit.exe* 文件。

2. 找到或者创建以下的注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3. 在右侧面板中找到现有的名为 *NoClose* 的一个双字键值，或通过点击编辑>新建>双字值对其进行重新创建。

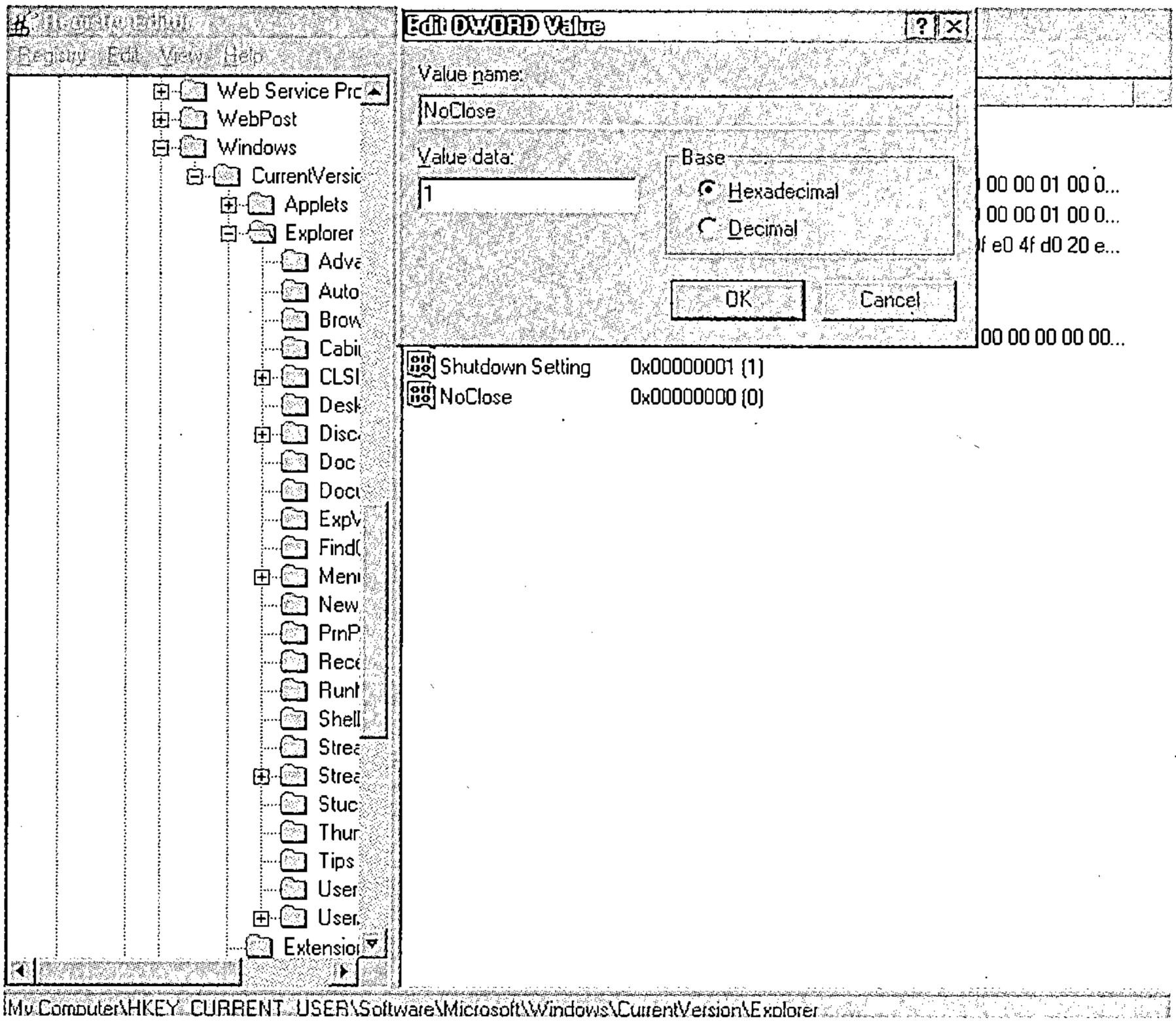

图 2-11　禁止用户关机

4. 将其键值设定为 1 就可禁用该关机选项，设置为 0 就可对其重新启用，如图 2-11 所示。

5．退出 Windows 注册表。重新启动 Windows 系统，使更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoClose"="1"
```

2.11 禁止用户注销

（Windows 2000/ME/XP）

技术级别：高　　安全级别：高

以上述例子进一步说明如何通过以下步骤禁止用户使用注销选项：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．在右侧面板中创建一个名为 *StartMenuLogoff* 的双字键值（通过右击并选择新建>Dword 值）并将其值设为 0 启用注销选项，设置为 1 禁止该选项，如图 2-12 所示。

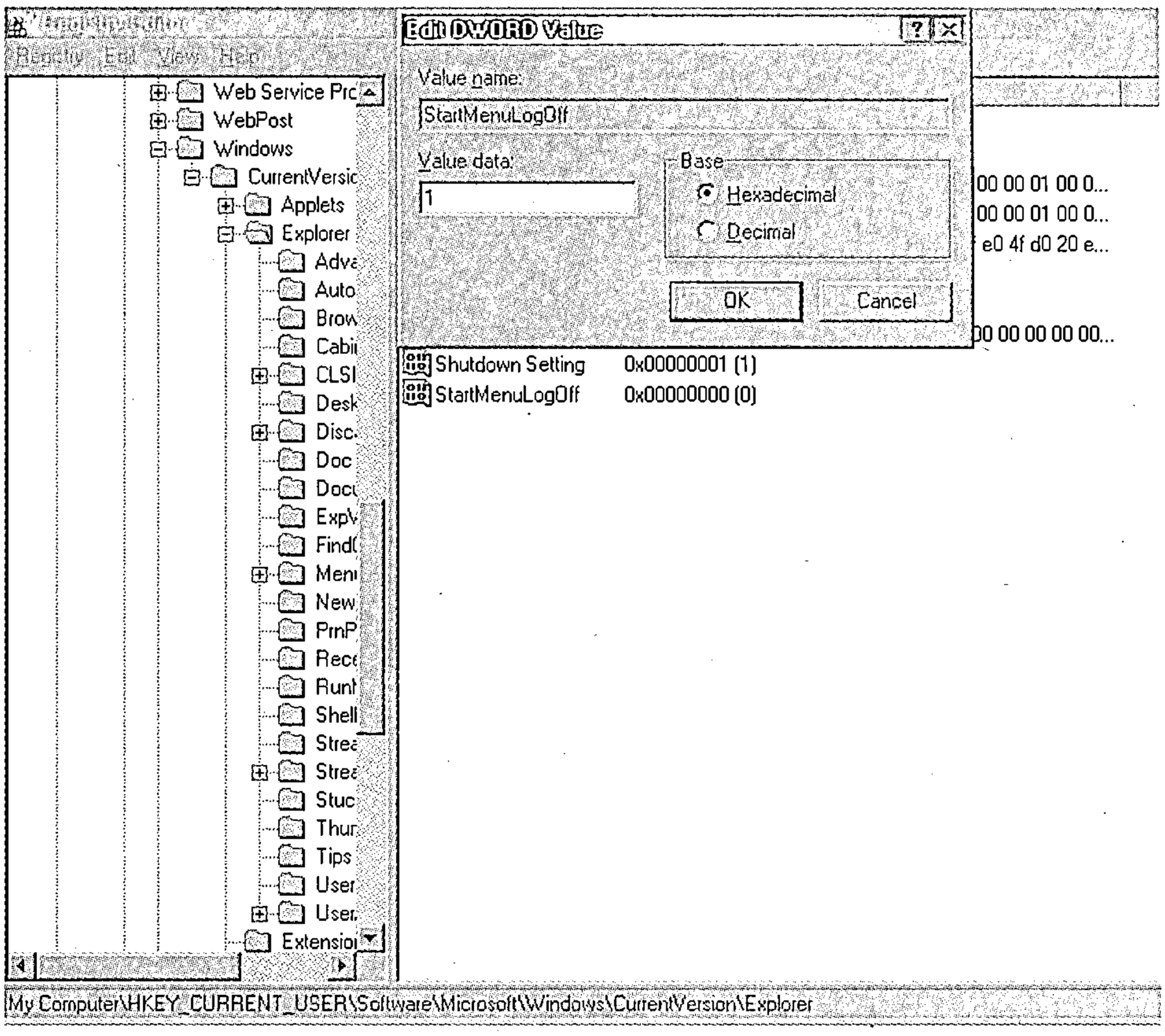

图 2-12　禁止用户注销

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

" StartMenuLogoff "="1"

2.12 开始菜单中强制注销

（适用版本 Windows 2000 and XP）

技术级别：高　　安全级别：低

可通过以下步骤将注销按钮强制性地放置于开始菜单中：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．创建一个名为 *ForceStartMenuLogoff* 双字键并将其值设定为 1，将注销按钮强制放置于开始菜单中，如图 2-13 所示。

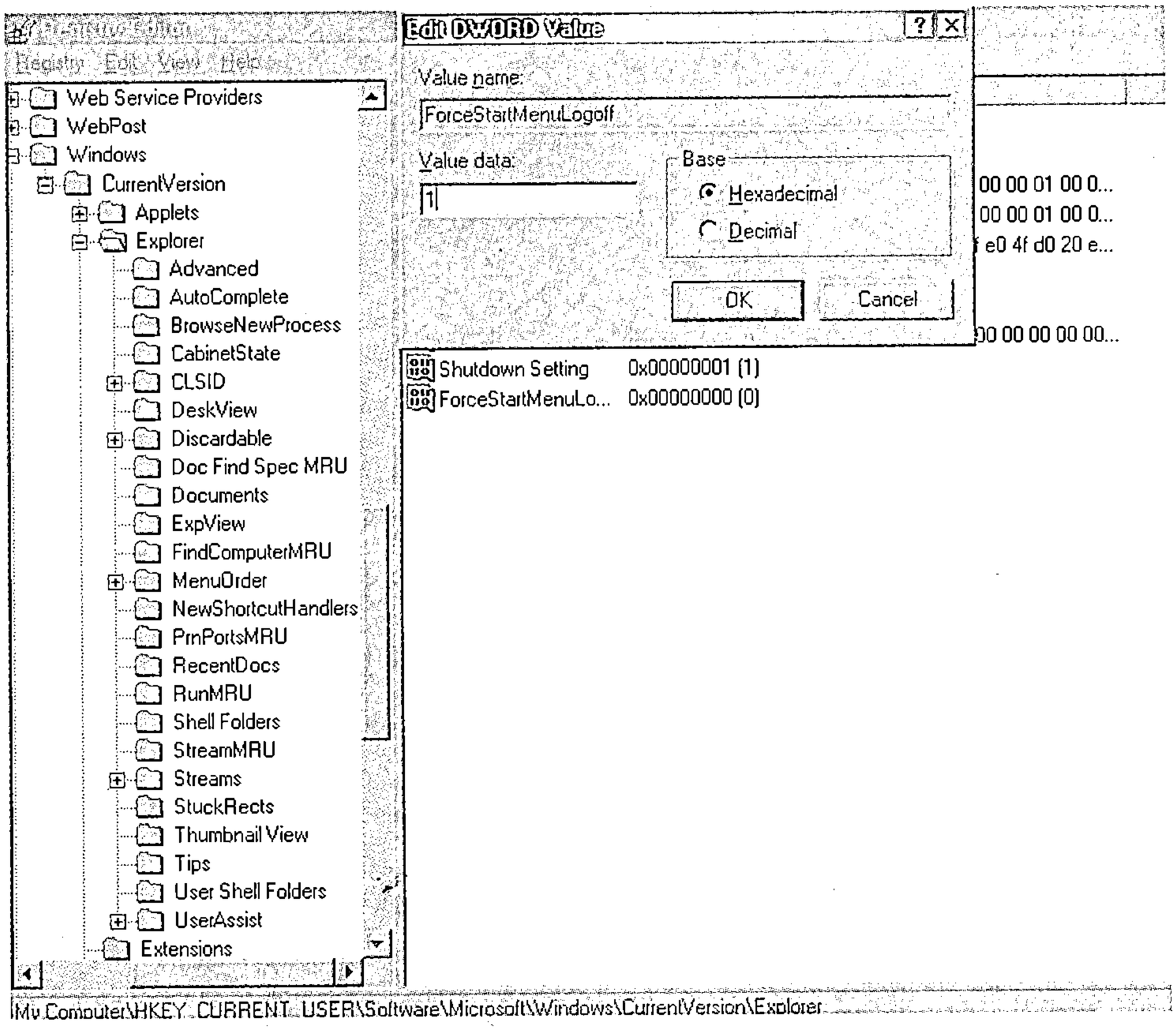

图 2-13　禁止用户注销

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"ForceStartMenuLogoff "="1"

2.13 允许快速重启

（适用于 Windows 2000 and XP）

技术级别：低　　安全级别：低

通过设置快速重启选项可以允许用户在没有完全关闭系统情况下启动 Windows。快速重启选项可借助于以下的技巧加以实现：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．创建一个名为 *EnableQuickReboot* 的新字符串键，并将其值设定为 1 启用该选项，设定为 0 即可禁用，如图 2-14 所示。

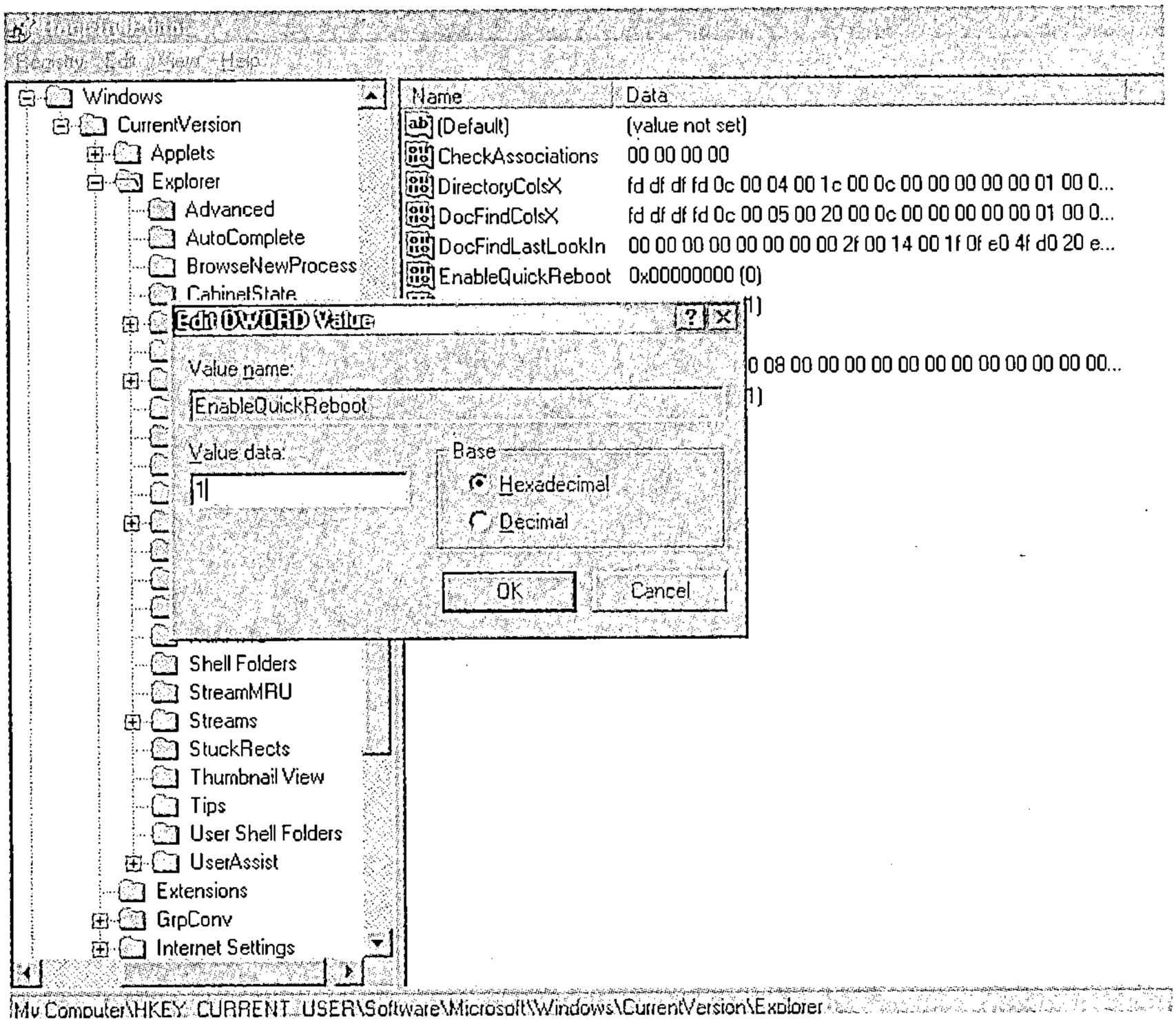

图 2-14　允许快速重启

4．退出 Windows 注册表，并重新启动 Windows，使得对设置的更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]
"EnableQuickReboot "="1"
```

2.14 禁止用户使用 Windows 更新选项

（适用于 Windows 所有版本）

技术级别：高　　安全级别：中等

默认情况下，每个 Windows 系统都有一个 Windows 更新选项（可在开始菜单中找到），如图 2-15 所示，允许用户从微软官方网站上下载更新或补丁程序以确保操作系统安全。然而，近几年世界各地的一些病毒感染案例证实了病毒有可能修改默认的 Windows 更新站点地址，并指向恶意攻击的 web 站点。这些恶意修改随后将下载一些病毒的更新版本！

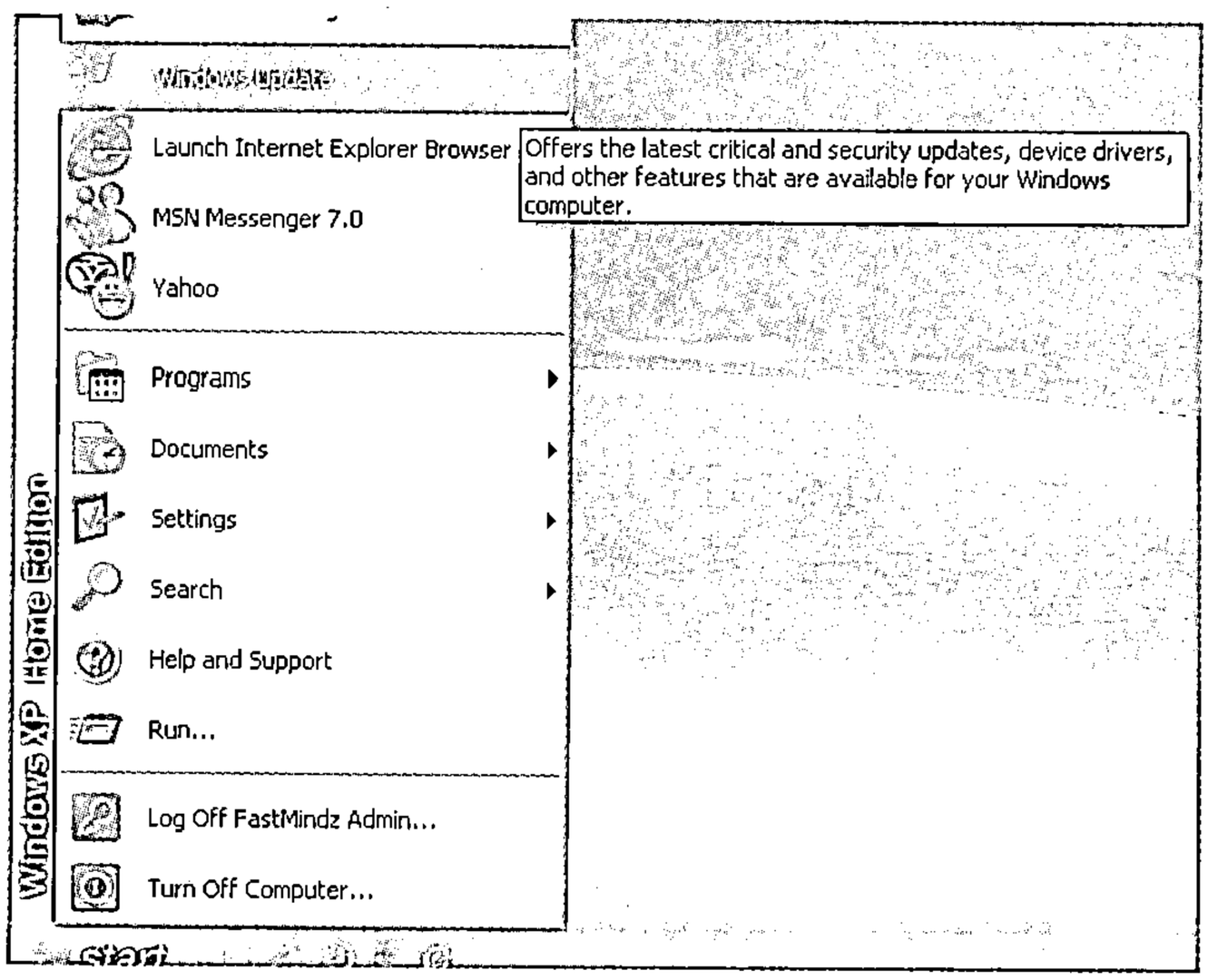

图 2-15　Windows 自动更新选项

因此，一些系统管理员已经开始禁止用户使用 Windows 更新选项。该功能可以非常容易地通过下面步骤实现：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate

3．在上述注册键中创建一个名为 *DisableWindowsUpdateAccess* 的双字键值，并将其设定为 1，如图 2-16 所示。

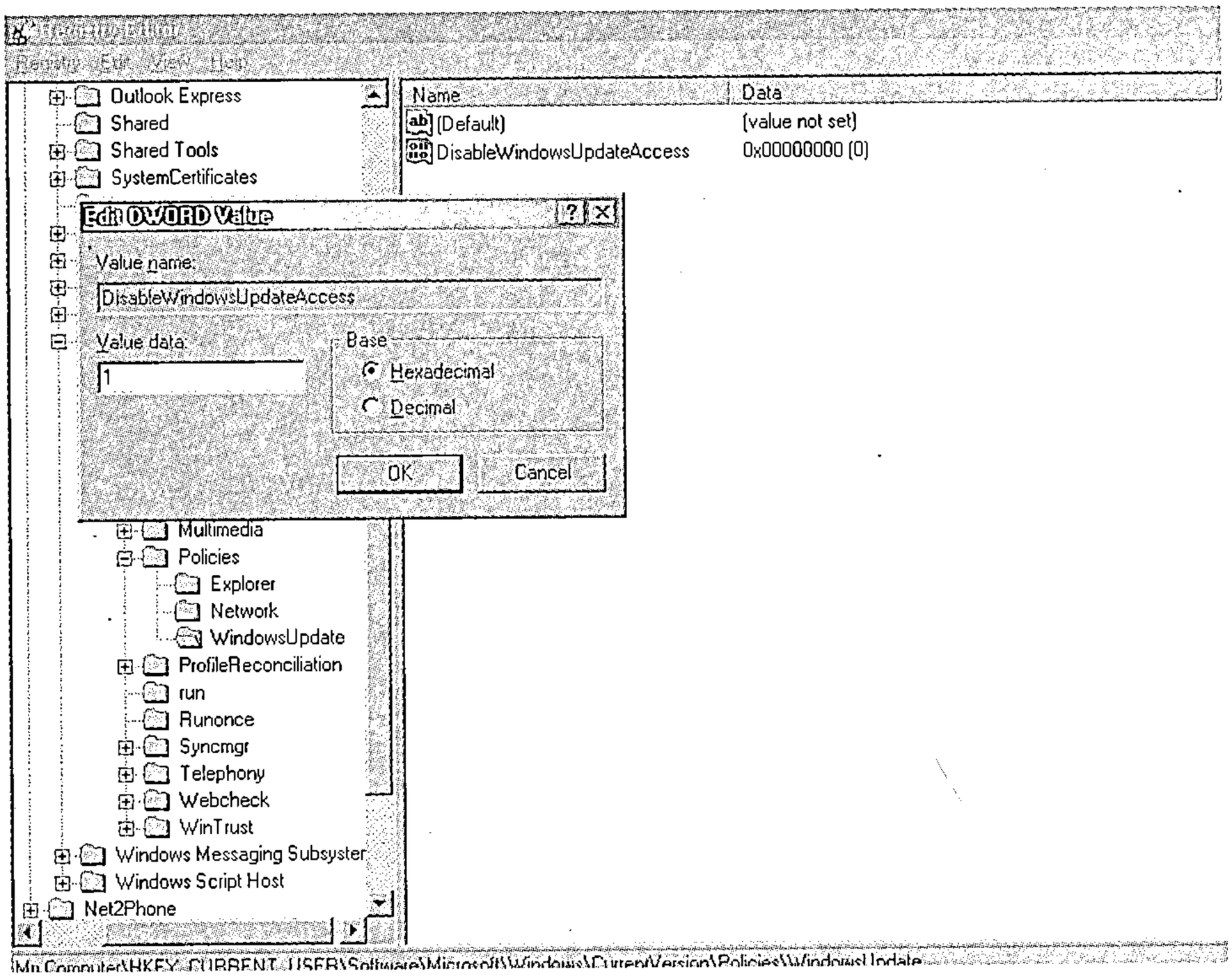

图 2-16　禁止用户使用 Windows 更新选项

4．退出 Windows 注册表。重新启动 Windows 系统，使更改生效。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate]

"DisableWindowsUpdateAccess"="1"

2.15　禁止特定应用程序运行

（适用于 Windows 2000 and XP）

技术级别：高　　安全级别：高

多数情况下，系统管理员有效地控制程序至关重要，需要确定哪些应用程序文件可以执行，哪些不能执行。下面介绍一个 Windows 注册表技巧，有助于系统管理员禁止特定应用程序文件的执行。需要通过下面的步骤对该限制加以实现：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．在上述的注册键中创建一个名为 RestrictRun （或 *DisallowRun*）的键值，并将其值

设定为 1 即可禁止应用程序的运行，设置为 0 即可启动应用程序运行，如图 2-17 所示。

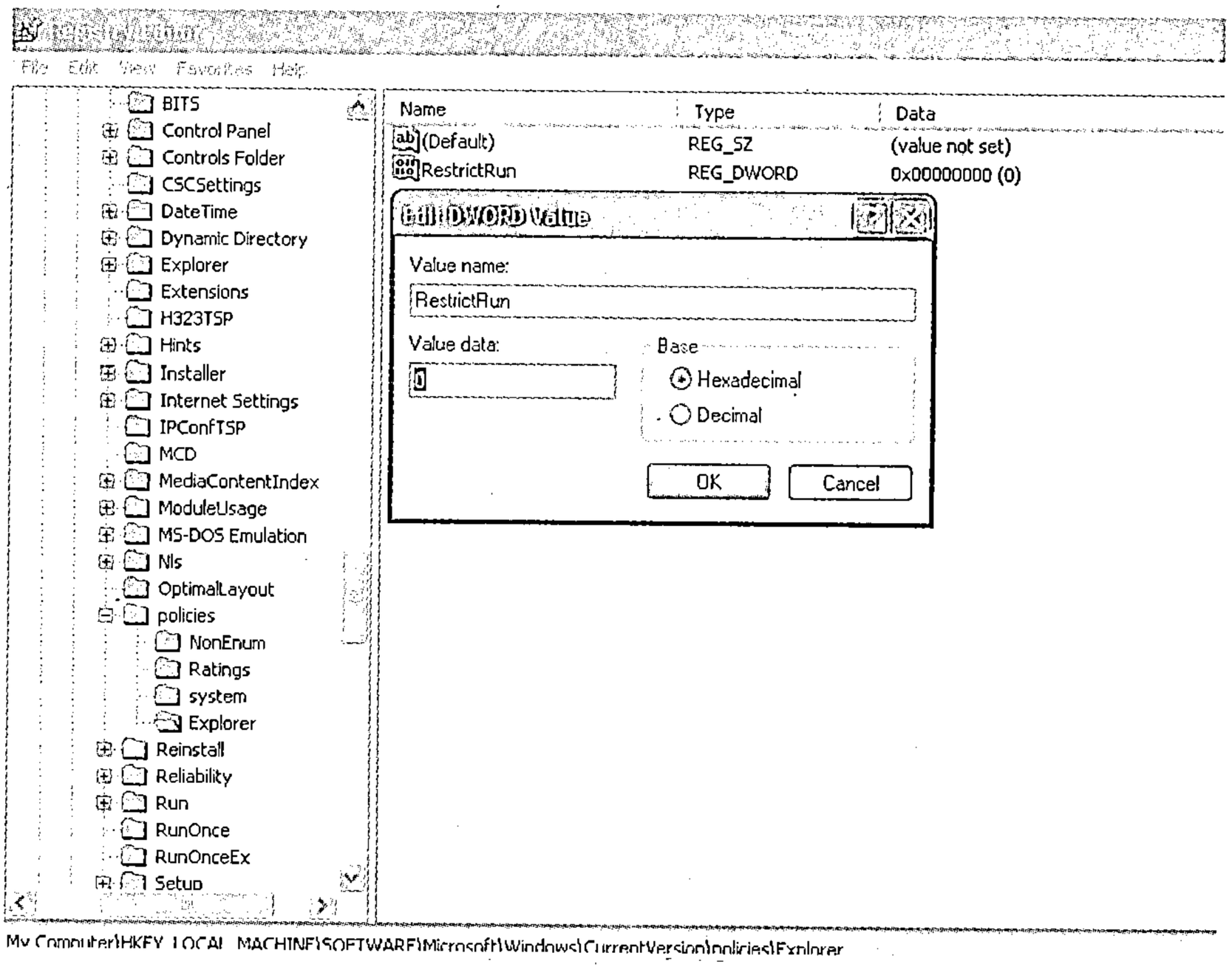

图 2-17　禁止特定应用程序运行

4．找到以下的注册键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion　\Policies\Explorer\RestrictRun

或者

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion　\Policies\Explorer\DisallowRun

5．对于每个欲被禁止的应用程序，需要创建一个新的字符串键，并从数字 1 开始以连续的序号命名。将每个欲被禁止的文件名赋值给每个新的字符串键。比如，想禁止画笔的运行，您就需要设定其字符串键值为：“mspaint.exe”。

6．退出 Windows 注册表。重新启动 Windows 系统，使更改生效。

2.16　禁止用户定制

（适用于除 Windows NT 之外的所有版本）

技术级别：中等　　安全级别：中等

许多企业或公司，为了维持公司制度，禁止用户根据个人喜好定制其配置文件就显得非常重要。可通过以下步骤禁止用户使用用户配置特性：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_LOCAL_MACHINE\Network\Logon

3．创建一个新的名为 *UserProfiles* 的双字键值，设定其值为 1 即可启动用户配置，设定为 0 即可禁止它们，如图 2-18 所示。

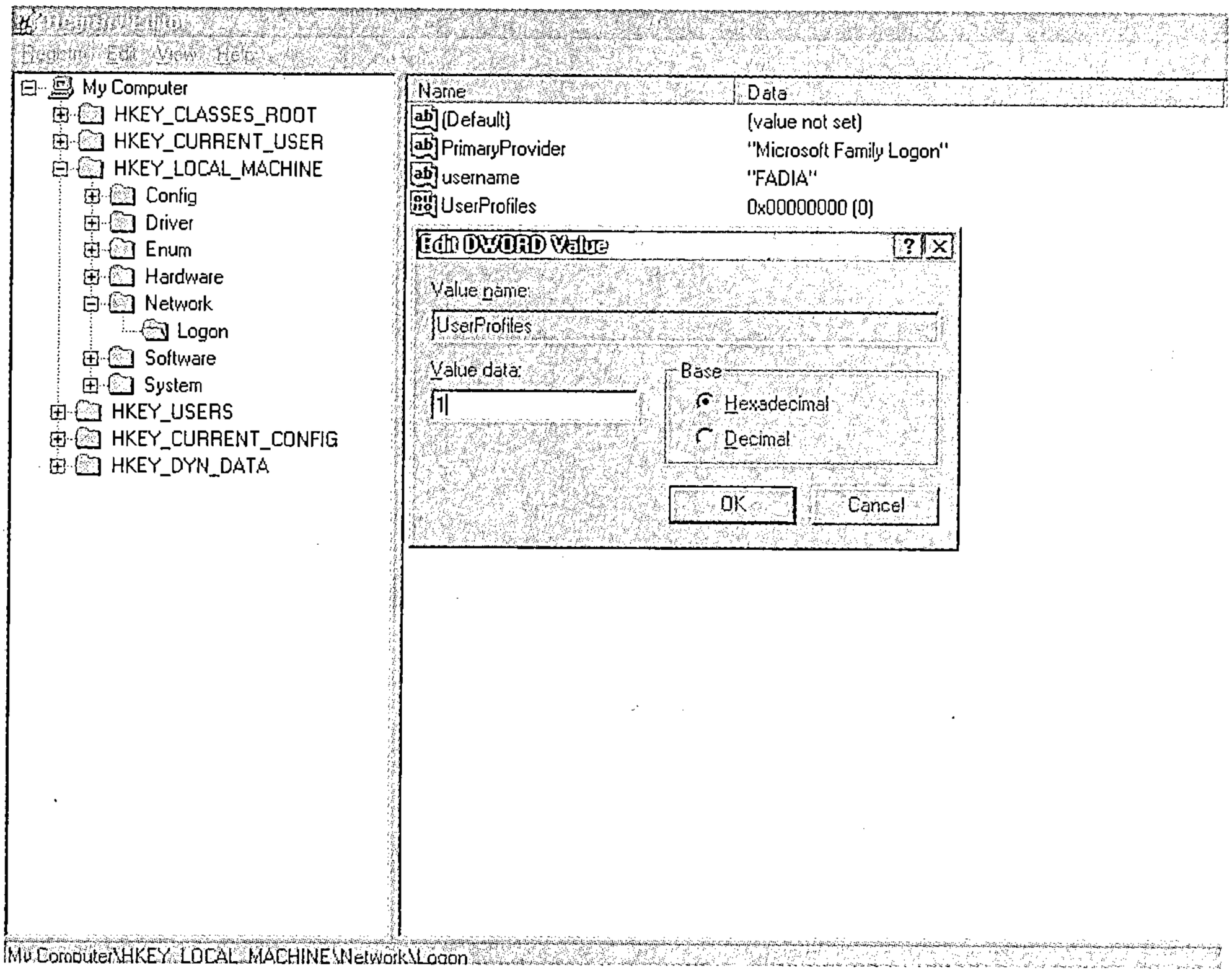

图 2-18　禁止用户定制环境

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Network\Logon]
"UserProfiles"="0"
```

2.17　快速退出 Windows

（适用于 Windows 9x and 2000）

技术级别：高　　安全级别：低

可创建一个快捷方式，使用户通过单击该快捷图标就可以立即且快速地退出 Windows。可通过下面步骤实现（如图 2-19 所示）：

1．桌面上右击选择新建>快捷方式创建一个快捷键。

2．在对话窗口空白处键入以下文本：

C:\windows\rundll.exe user.exe,exitwindowsexec

3．点击确定。该快捷方式允许用户立即退出 Windows，同时不会出现任何的提示或警告信息。

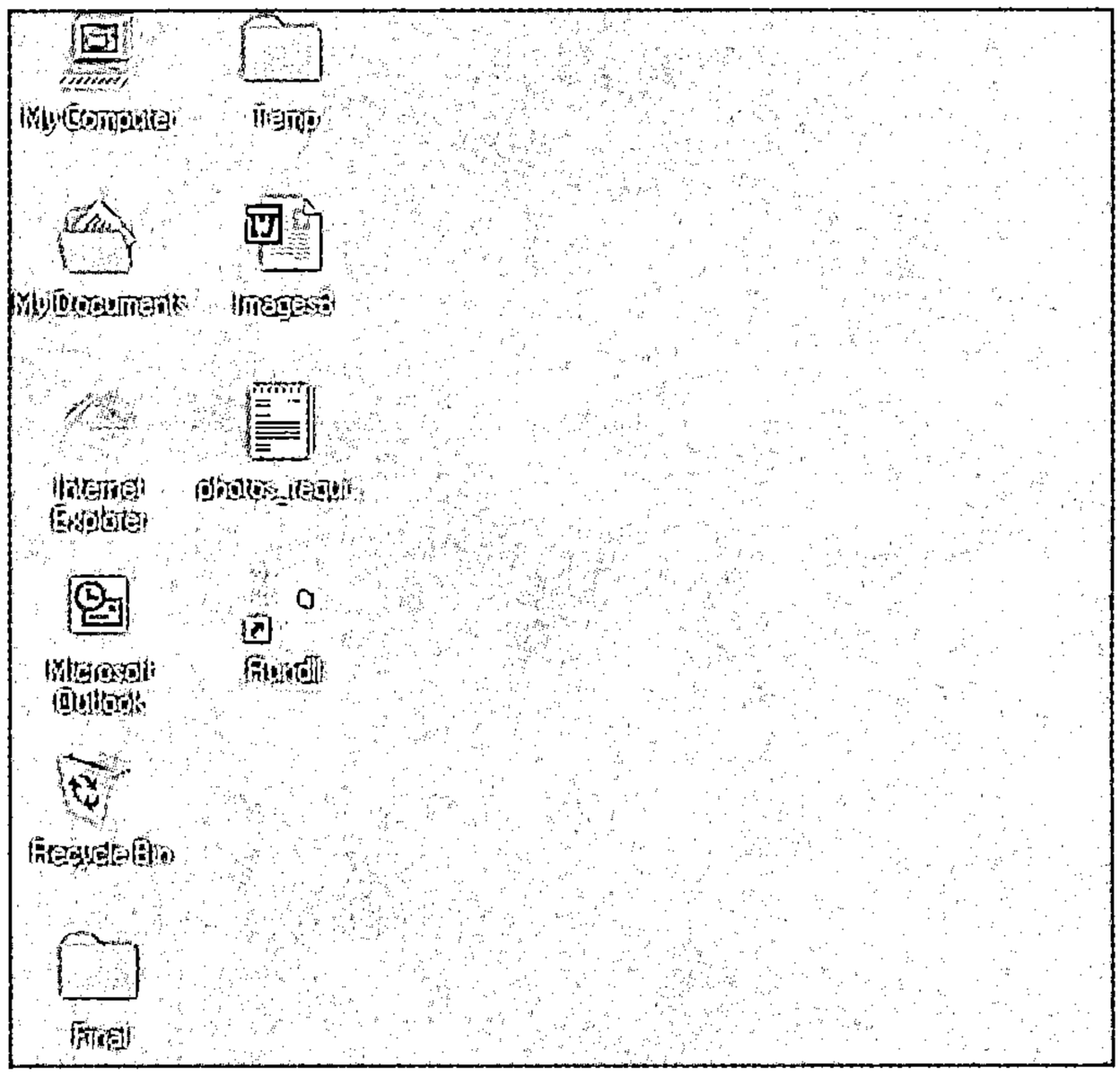

图 2-19　快速退出 Windows

4．类似地，也可以创建一个快速退出并重新启动的快捷方式。在此情形下，需要键入下列文本代替上述的文本输入：

C:\windows\rundll.exe user.exe,exitwindows

2.18　定制文件夹图标

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：低

Windows 系统预先设定的所有文件夹都是令人厌烦的黄色图标。不过，通过下列步骤就可方便地更改这些文件夹的外观：

1．创建一个包含如下内容的文本文件，将其命名为 *desktop.ini* 并保存在需要更改外观的文件夹中，如图 2-20 所示：

[.ShellClassInfo]
ICONFILE=Path of the icon

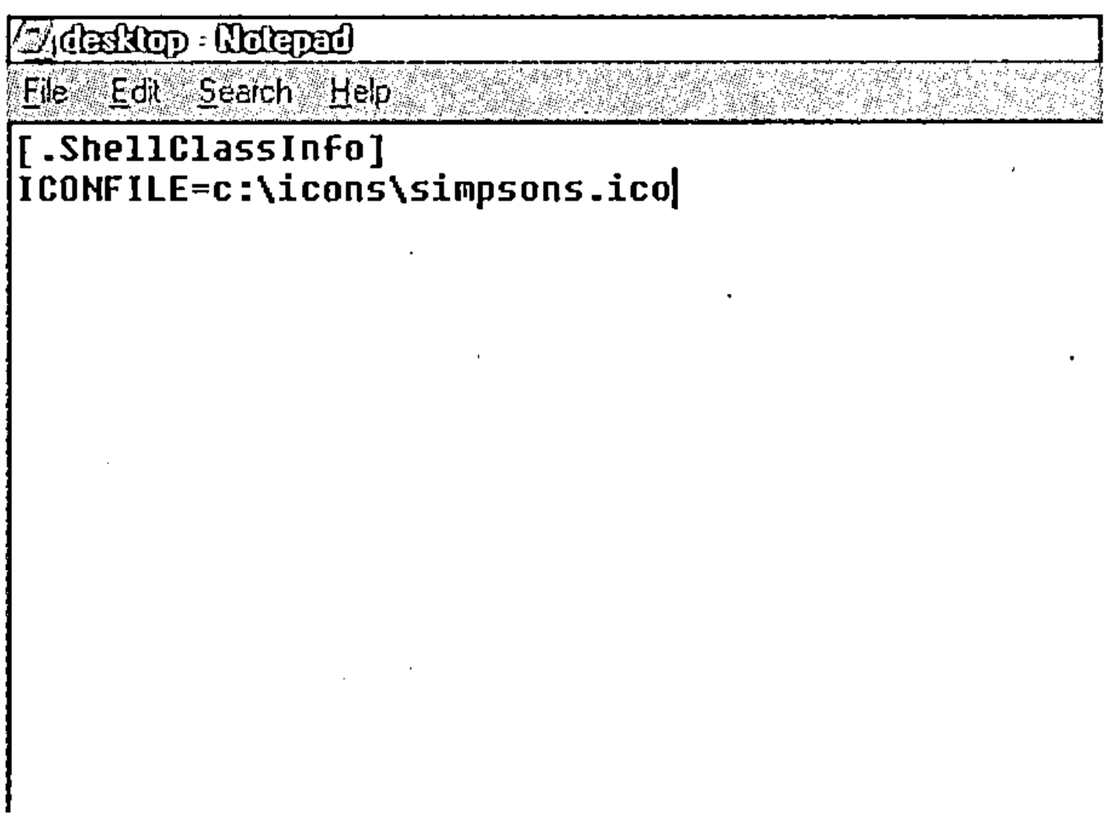

图 2-20 定制文件夹图标

2. 类似地，可以创建包含如下文本的一个文件，将其命名为 *autorun.inf* 并保存在需要更改图标的驱动器根目录下，实现对一个驱动器的图标的更改：

[Autorun]
ICON=Path of the icon

3. 强烈建议将该文件的属性更改为只读和隐藏，以防止不必要的意外损坏。

2.19 禁止访问特定驱动器

（适用于 Windows 2000 and XP）

技术级别：中等　　安全级别：高

多数情况下，禁止用户访问特定的驱动器是一项非常有效的安全措施。它不但是一项非常好的隐私保护工具，也可用于知识产权的有效保护。通过下面步骤就可以实现对特定驱动器的访问禁止（如图 2-21 所示）：

1. 打开 regedit.exe 文件。

2. 找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
（用户特定的限制）
或者
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
（系统范围内的限制）

创建一个名为 *NoViewOnDrive* 的双字键值，并用如下数值之一赋值给需要隐藏的驱动器：

A: 1, B: 2, C: 4, D: 8, E: 16, F: 32, G: 64, H: 128, I: 256, J: 512, K: 1024, L: 2048, M: 4096, N: 8192, O: 16384, P: 32768, Q: 65536, R: 131072, S: 262144, T: 524288, U: 1048576, V:

2097152, W: 4194304, X: 8388608, Y: 16777216, Z: 33554432, ALL: 67108863

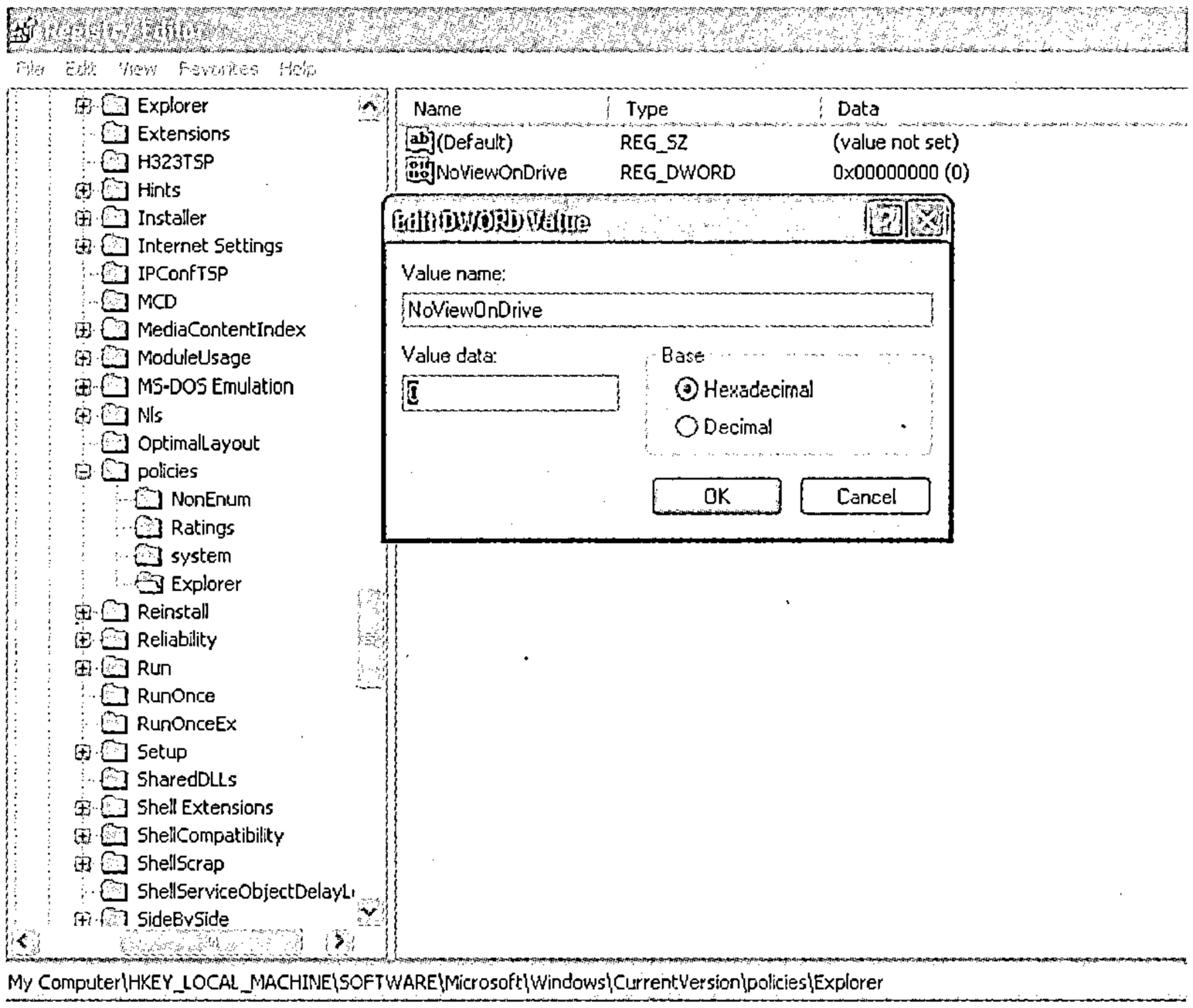

图 2-21　禁止用户访问特定驱动器

3．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[Choose Registry Key From Key]
"NoViewOnDrive"="Drive number"
```

2.20　锁定 Windows 注册表

（适用于 Windows 所有版本）

技术级别：低　　安全级别：高

对系统管理员而言，限制 Windows 注册表的编辑是非常有效的系统安全措施。可通过下面有关注册表的简单技巧实现上述功能：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3．创建一个新的名为 *Disablehegistry Tools* 的双字键值，设定其值为 1 即可启动用户配置，设定为 0 即可禁止锁定，如图 2-22 所示。

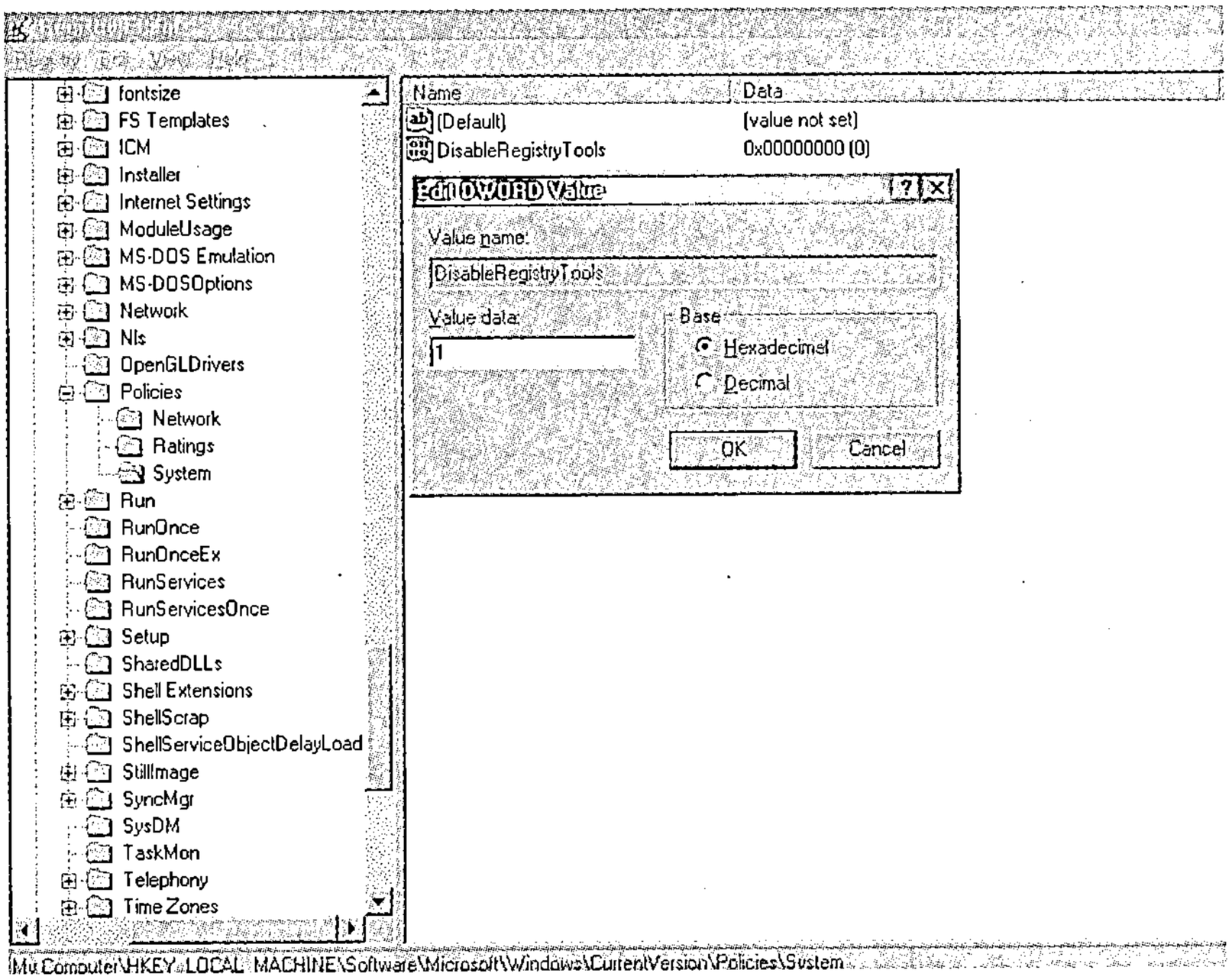

图 2-22 锁定 Windows 注册表

4. 退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"="1"
```

2.21 删除桌面特定文件夹

（适用于 Windows 所有版本）

技术级别：高　　安全级别：中等

在 Windows 桌面上有许多专门的系统文件夹，比如回收站、打印机、网上邻居、IE 浏览器等，这些文件夹都拒绝被删除。遗憾的是，如果在该类文件夹上右击并试图删除时，其右击菜单中不会出现删除菜单项（也没有重命名、剪切、复制或粘贴等项）。然而，这些并不意味着不能删除这些专门的系统文件夹。实际上，我们通过下列步骤就能删除这些系统文件夹：

1. 打开 regedit.exe 文件。

2. 找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespae

3. 每个系统文件夹都对应一个 16 比特位的 CLSID 键值（或者称其为类 ID）。CLSID

值用相应的键值在注册表中标识特定的对象。最常用的系统文件夹及其对应的 CLSID 值如下所示：

收件箱 :{00020D76-0000-0000-C000-000000000046}
我的电脑 :{20D04FE0-3AEA-1069-A2D8-08002B30309D}
网上邻居:{208D2C60-3AEA-1069-A2D7-O8002B30309D}
打印机 :{2227A280-3AEA-1069-A2DE-O8002B30309D}
回收站 :{645FF040-5081-101B-9F08-00AA002F954E}
控制面板:{21EC2020-3AEA-1069-A2DD-08002B30309D}
我的公文包:{85BBD920-42AO-1069-A2E4-08002B30309D}
Microsoft Network:{00028B00-0000-0000-C000-000000000046}
历史： {FF393560-C2A7-11CF-BFF4-444553540000}
桌面： {00021400-0000-0000-C000-0000000000046}
Winzip :{E0D79300-84BE-11CE-9641-444553540000}
拨号网络:{992CFFA0-F557-101A-88EC-00DD01CCC48}
字体： {BD84B380-8CA2-1069-AB1D-08000948534}

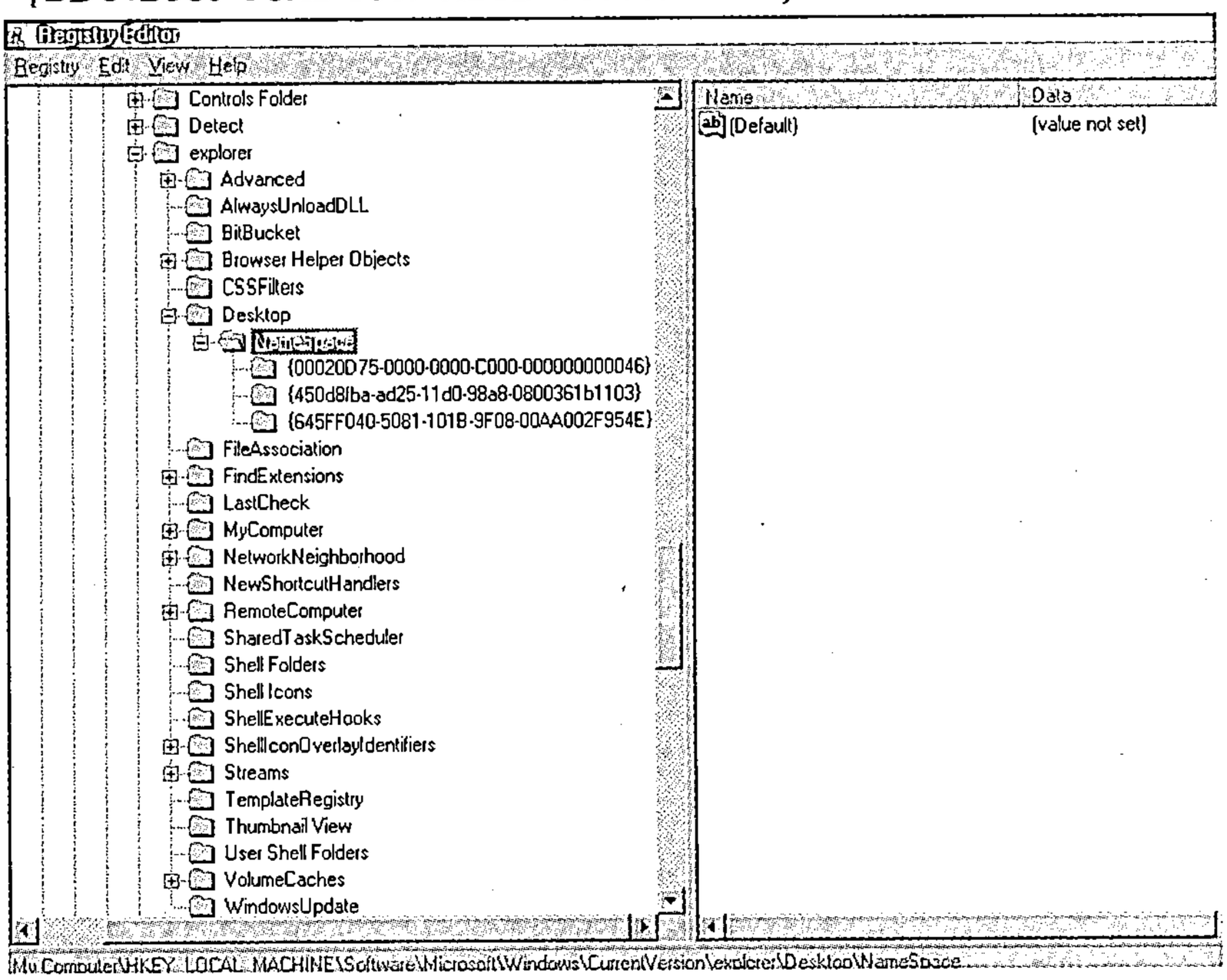

图 2-23 删除桌面特定文件夹

4．每个系统文件夹都可简单地通过清除其对应的 16 比特位 CLSID 数值将其删去。

例如，如果想从桌面上删去我的电脑图标，仅需要删除以下的注册键项目：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespace\{20D04FE0-3AEA-1069-A2D8-08002B30309D}

类似地，如果想从桌面上删去回收站图标，仅需要删除以下的注册键项目，如图 2-23

所示：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\Namespace\{645FF040-5081-101B-9F08-00AA002F954E}

5．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

2.22 禁止更改特定文件夹位置

（适用于 Windows 2000 and XP）

技术级别：低　　安全级别：高

进一步探讨上例，我们可以通过注册表技巧禁止用户更改这些特定文件夹的位置。实现方法如下所示：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．在上述的注册键项目中创建特定的双字子键，通过将其赋值为 1 启用该限制，赋值为 0 即可禁用该限制，特定双字值如表 2-1 所示，修改如图 2-24 所示。

表 2-1　子键与文件夹位置对应表

双 字 值	限 制 内 容
DisableMyPicturesDirChange	禁止更改 My Pictures 文件夹位置
DisableMyMusicDirChange	禁止更改 My Music 文件夹位置
DisableFavoritesDirChange	禁止更改 My Favorites 文件夹位置
DisablePersonalDirChange	禁止更改 My Documents 文件夹位置

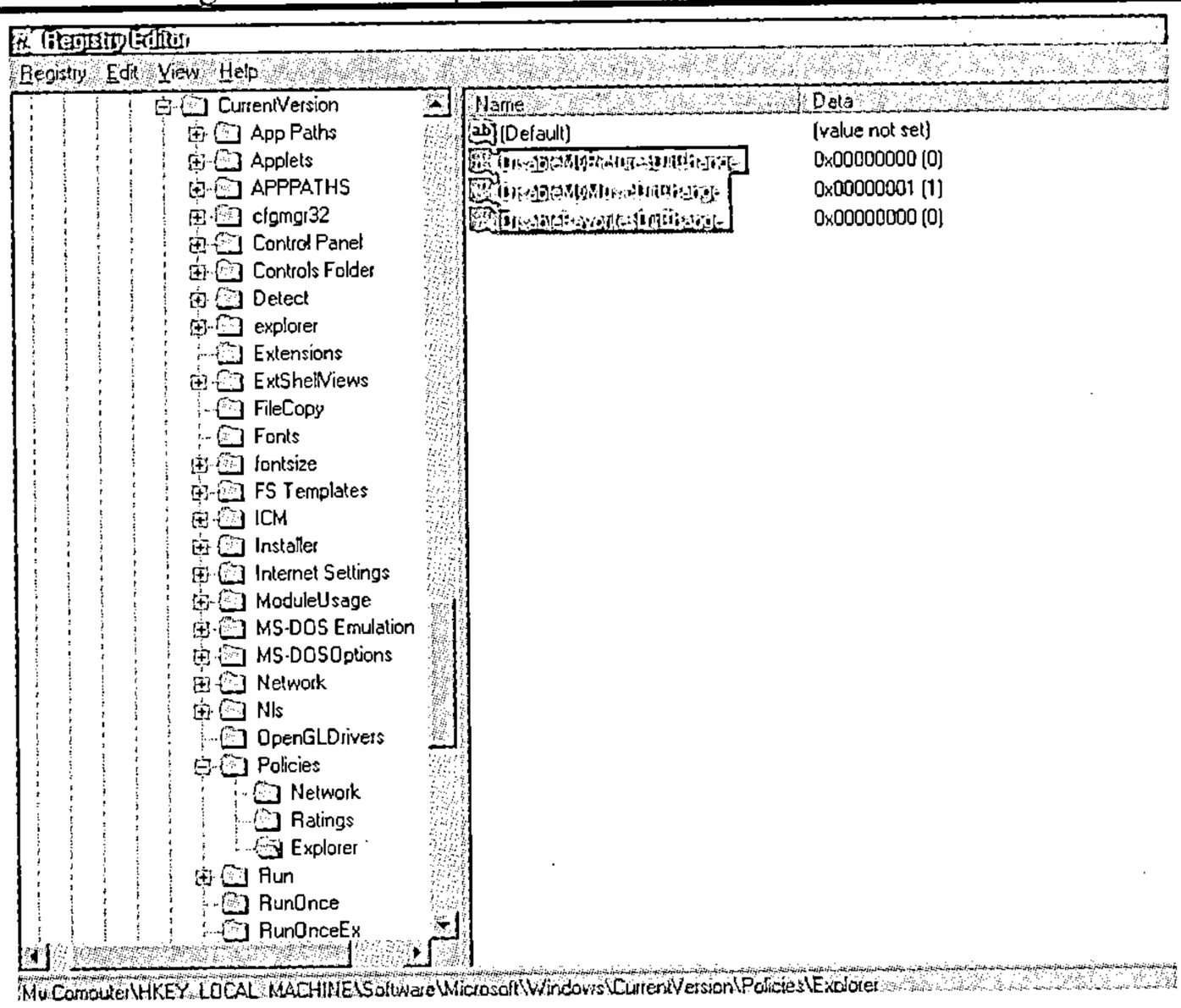

图 2-24　禁止更改特定文件夹位置

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"DWORD Entry"="1 or 0”
```

2.23 锁定软盘驱动器

（适用于 Windows 2000 and XP）

技术级别：高　　安全级别：高

默认情况下，本地和远端的授权用户都可以访问软盘驱动器。因此，系统会存在着非常严重的安全隐患。系统管理员可通过以下方法禁用软盘驱动器，以防止恶意入侵：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．创建一个名为 *AllocateFloppies* 的字符串注册键并赋值为 1，以确保软盘驱动器仅对本地登录的用户可用。如果将其值设定为 0，所有对软盘驱动器的限制就将被取消，如图 2-25 所示。

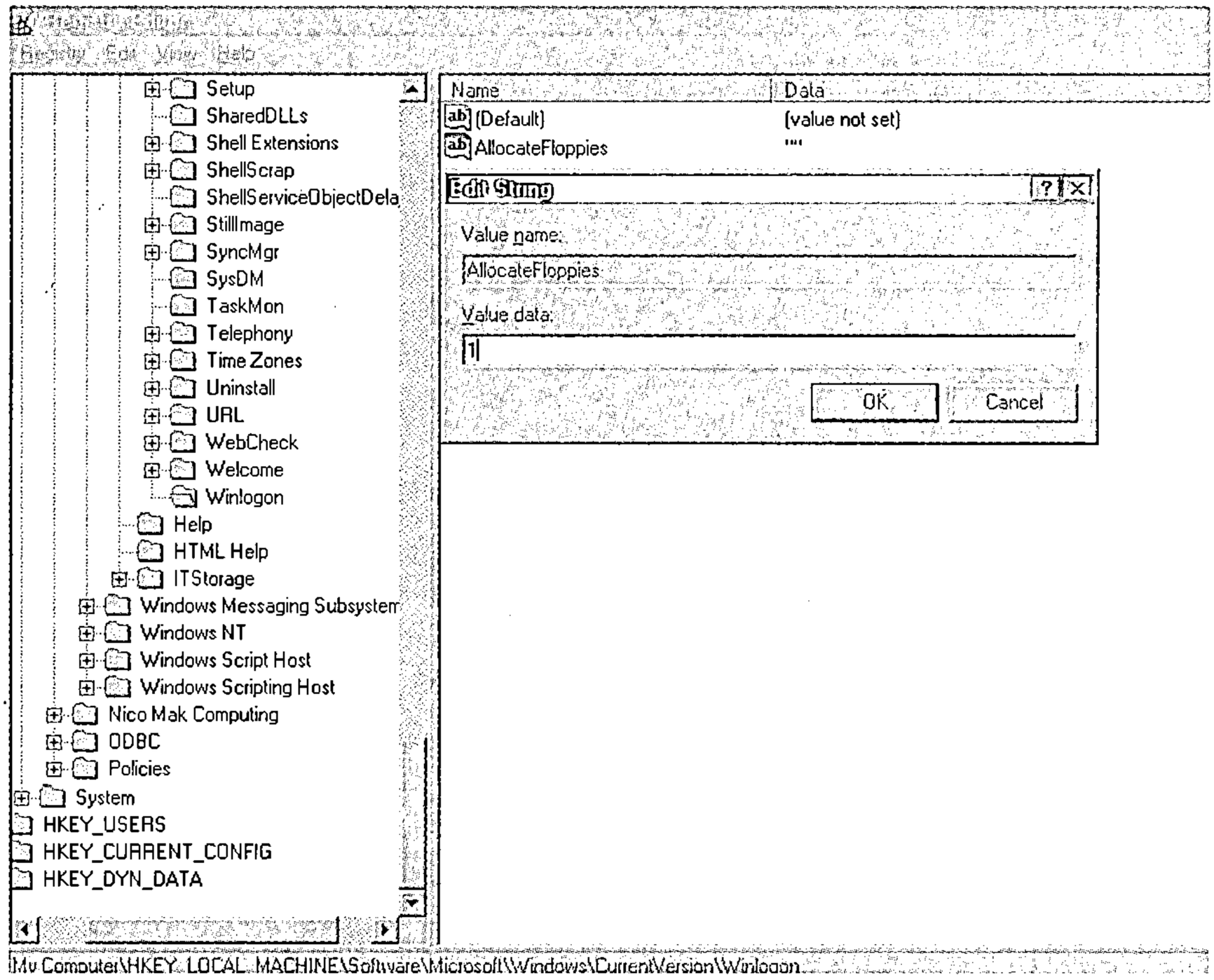

图 2-25　锁定软盘驱动器

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]
"AllocateFloppies"="1"
```

2.24 锁定 CD-ROM 驱动器

（适用于 Windows 2000 and XP）

技术级别：高　　安全级别：高

以上例进一步说明，可以通过下面操作禁止对 CD-ROM 驱动器的访问：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

3．创建一个名为 *AllocateCDRoms* 的字符串注册键并赋值为 1，以确保 CD-ROM 驱动器仅对本地登录的用户可用。如果将其值设定为 0，所有对软盘驱动器的限制就将被取消，如图 2-26 所示。

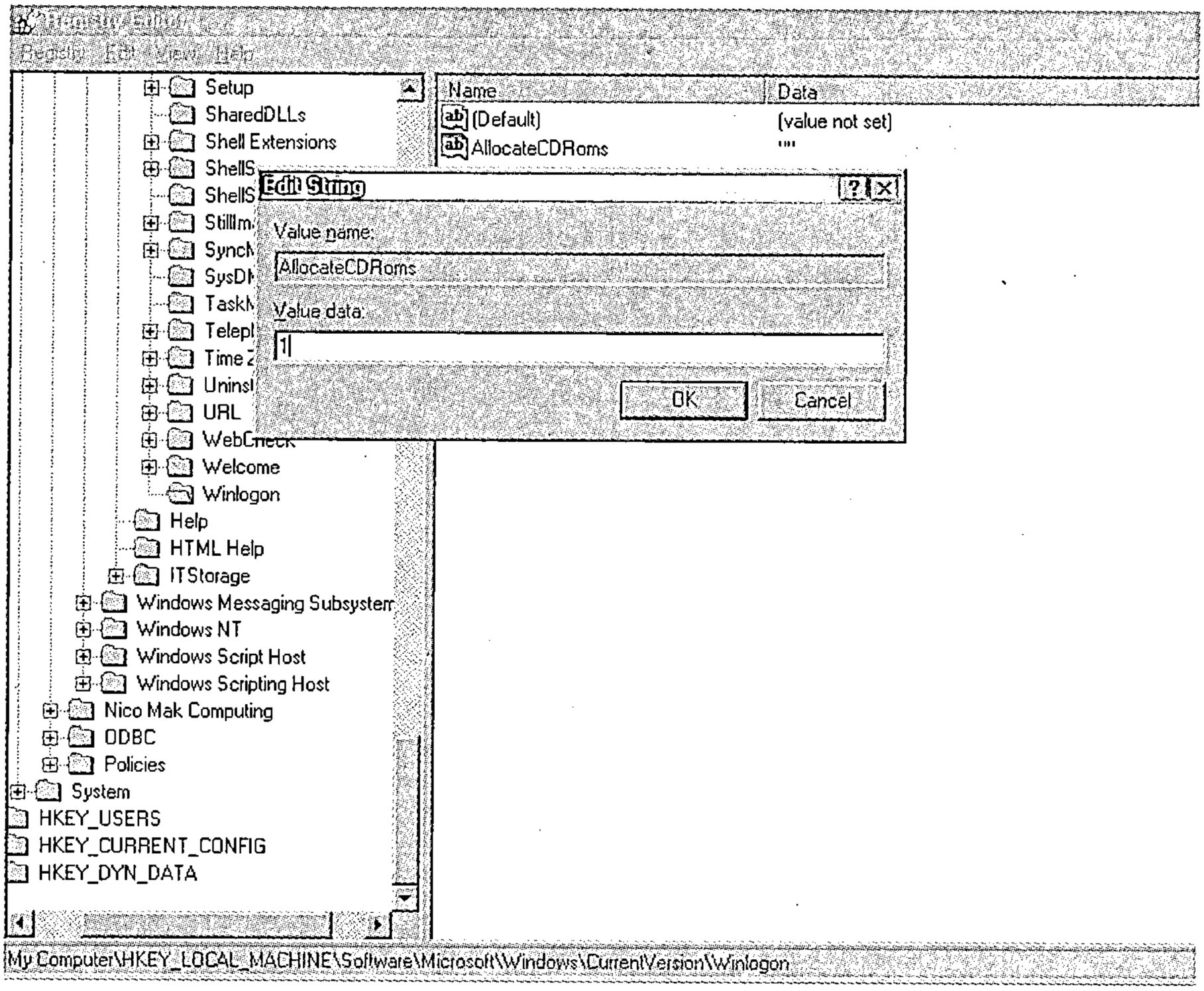

图 2-26　锁定 CD-ROM 驱动器

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]
"AllocateCDRoms"="1"
```

2.25 向文件夹中添加菜单项目

（适用于 Windows 所有版本）

技术级别：高　　安全级别：低

进一步讨论上述例子，我们可以向这些专门的系统文件夹的右击菜单中添加菜单项目。比如，向所有的系统文件夹右击菜单中增加诸如重命名、删除、剪切、复制、粘贴等项目。通过以下方法就可以实现上述功能：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_CLASSES_ROOT\CLSID\{CLSID Number Here}\ShellFolder

比如，如果向我的电脑文件夹中添加新菜单项目，就需要打开如下的注册键：

HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder

3．Windows 注册表的右侧面板中名为 *Attributes* 的双字键包含着特定的键值，该键值对应各个系统文件夹的右击菜单中新添加的菜单项目。该 *Attributes* 双字键项能用于向系统文件夹中添加如表 2-2 所列的新菜单项目。

表 2-2　菜单与键值对应表

被添加的菜单项目	*Attributes* 所对应的键值
重命名	50 01 00 20
删除	60 01 00 20
重命名&删除	70 01 00 20
复制	41 01 00 20
剪切	42 01 00 20
复制&剪切	43 01 00 20
粘贴	44 01 00 20
复制&粘贴	45 01 00 20
剪切	46 01 00 20
剪切、复制	47 01 00 20
默认设置	40 01 00 20

举例说明，为了向“回收站”的右击菜单中添加删除项，就需要将 *Attributes* 键值相应地更改为 60 01 00 20。

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_CLASSES_ROOT\CLSID\{Enter CLSID Value Here}\Shell-Folder]
"Attributes"=hex:此处键入相应的数值
```

2.26 向 Windows 系统各个环节添加限制

（其结果会因版本的不同而有所不同）

技术级别：高　　安全级别：高

Windows 操作系统用尽各种方法使得用户难以隐藏或显示各种选项、特性或外观。然而，我们仍然可以通过多种方法对 Windows 系统各个方面进行更改。Windows 注册表包含了所有对操作系统进行修改、禁用或启用的键项目。也就是说，系统管理员可以通过使用注册表对系统用户的所有方面加以限制。尽管对用户活动的各种限制主要通过本地注册表技术加以实现，但系统管理员有时也可通过主服务器对系统用户的各种活动加以限制。

可通过如下步骤，以最简洁的方法对用户活动加以限制：

1．打开 regedit.exe 文件。

2．找到以下的注册键：

HKEY_CURRENT_USER/Software/Microsoft/CurrentVersion/Policies/Explorer

3．可以在该键值中添加一些非常有趣的限制，我们将在以后章节详细叙述。在右侧面板中新建如下的双字键项目，以向用户添加各种限制：

NoDeletePrinter

该双字键值用于对已安装打印机的删除操作进行控制。数值 1 意味着已安装的打印机不能被删除，而数值 2 允许删除已有的打印机。

NoAddPrinter

该双字数值对用户添加新的打印机加以限制，除此之外，与上述的限制特性类似。

NoRun

该双字键值用于禁止/隐藏或者启动开始菜单中的 RUN 选项。数值 1 将隐藏 RUN 选项，数值 0 将其设定为显示，如图 2-27 所示。

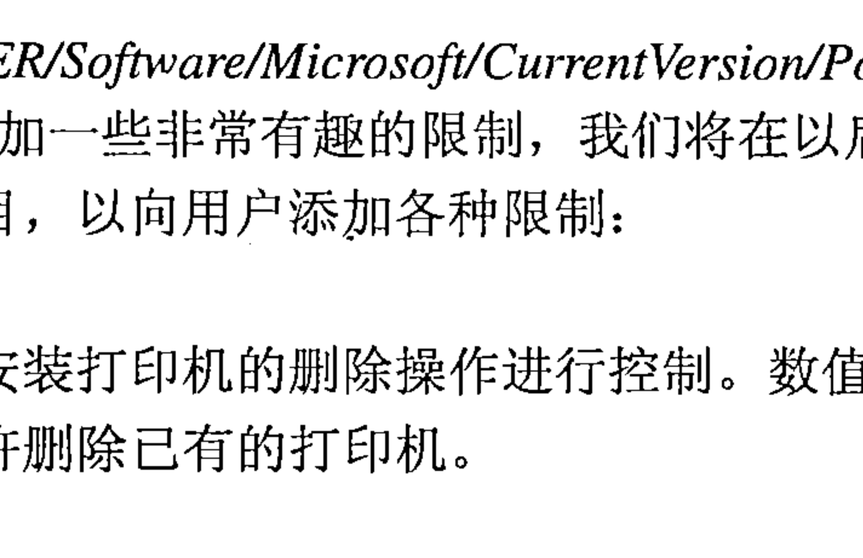

图 2-27　禁止/隐藏开始菜单中的 RUN 选项

以下诸多选项的修改，如图 2-28 所示。

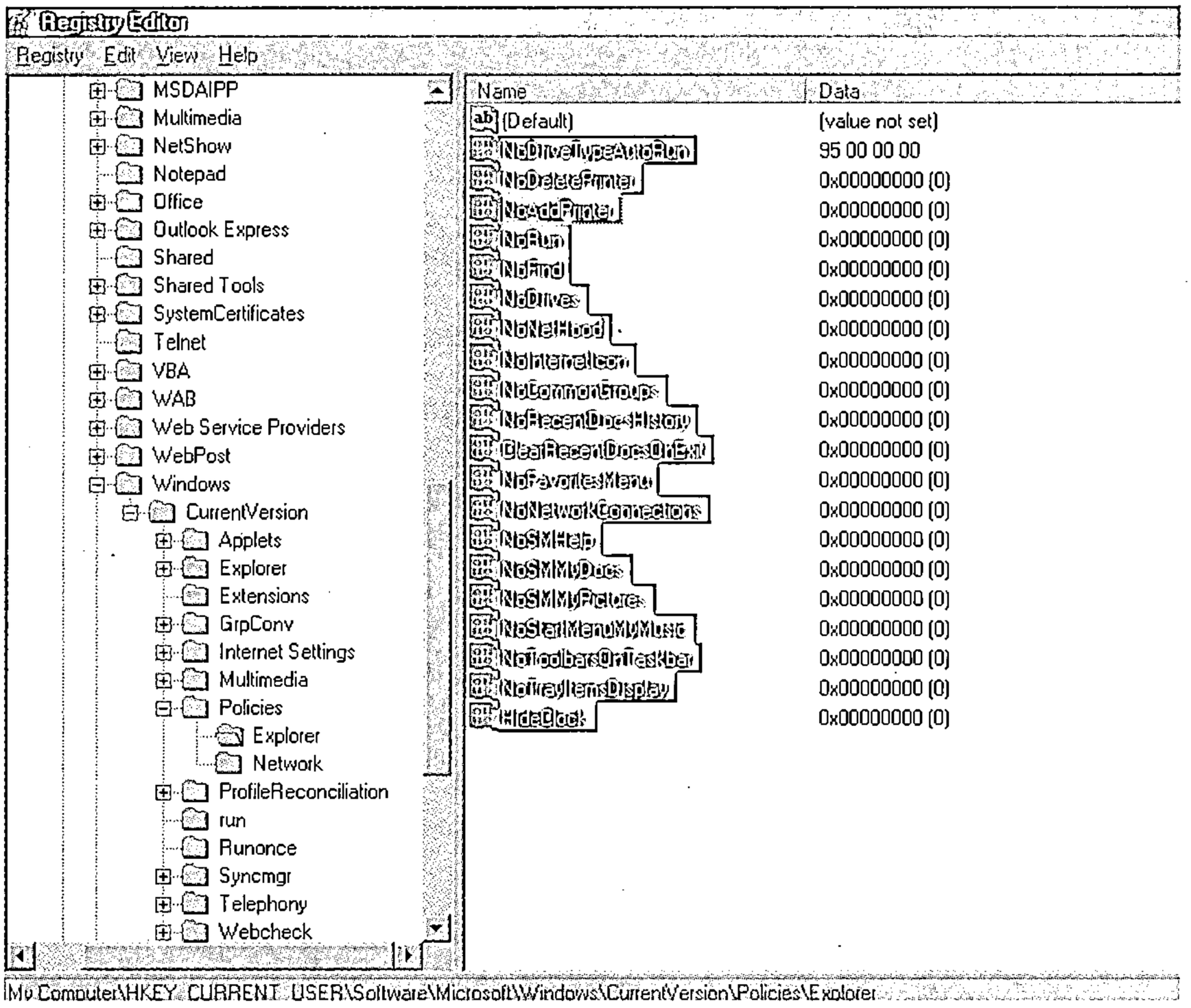

图 2-28　向 Windows 系统中添加多项限制

NoFind

该双字键值用于禁止/隐藏或者启用开始菜单中的查找选项。数值 1 将隐藏查找选项，数值 0 将其设定为显示。

NoDrives

该双字用于隐藏“我的电脑”中的所有驱动器。数值 1 将隐藏驱动器，数值 0 将其设定为显示。可利用 Windows 注册表中的这些隐藏特性向你的好朋友开个小玩笑哦！ 然而，系统管理员也可利用 *NoDrives* 对特定用户的访问权限加以限制。

NoNetHood

该双字键值可用于隐藏桌面上的“网上邻居”图标。数值 1 将隐藏该图标，数值 0 将其设定为显示。

NoInternetIcon

该双字键值可用于从桌面中隐藏 IE 浏览器图标。数值 1 将隐藏该图标，数值 0 将其设定为显示。

NoCommonGroups

该双字键值用于隐藏开始菜单（开始→程序）中的通用组文件夹。数值 1 将隐藏通用组文件夹，数值 0 将其设定为显示。

NoRecentDocsHistory

每次打开一个 Windows 系统文本或文件时，系统都会将其添加到开始菜单中的最近文档列表中。该列表包含了计算机系统访问本地文件的历史记录，类似于浏览器的历史记录列表。该双字 *NoRecentDocsHistory* 键值可用于禁止将文档添加到该列表中。数值 1 将从开始菜单中移除该列表，数值 0 将其设定为显示。

ClearRecentDocsOnExit

进一步讨论上述的技巧，可以在每次系统退出时自动地清除最近文档。将双字的 *ClearRecentDocsOnExit* 键值设定为 1 启动该选项，设定为 0 将禁止该选项。

NoFavoritesMen

该双字键值用于禁止/隐藏或者启动开始菜单中 FAVORITES 选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoNetworkConnections

该双字键值用于禁止/隐藏或者启动通过开始菜单（开始→设置）正常访问到的网络和拨号连接选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoSMHelp

该双字键值用于禁止/隐藏或者启动通过开始菜单正常访问到的帮助选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoSMMyDocs

该双字键值用于禁止/隐藏或者启动通过开始菜单（开始→文档）正常访问到的“我的文档”选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoSMMYPictures

该双字键值用于禁止/隐藏或者启动通过开始菜单（开始→文档）正常访问到的“图片收藏”选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoStartMenuMyMusic

该双字键值用于禁止/隐藏或者启动通过开始菜单（开始→文档）正常访问到的我的音乐选项。数值 1 将从开始菜单中隐藏该选项，数值 0 将其设定为显示。

NoToolbarsOnTaskbar

Windows 操作系统的新版本允许用户创建工具栏，内嵌到任务栏中以方便快速访问。比如，快速启动、地址、链接等。将 *NoToolbarsOnTaskbar* 双字键设定为 1 即可隐藏所有的工具栏，设定为 0 则将重新启用它们。

NoTrayItemsDisplay

通常，许多应用程序图标显示在屏幕右下角并靠近系统时钟。通过一些简单注册表技巧，就可以禁止这些图标的显示。将该双字 *NoTrayItemsDisplay* 的键值设定为 1 即可隐藏这些图标，而设置为 0 则将显示它们。

HideClock

该双字键值可用于禁止/隐藏或启动正常显示在屏幕右下角的系统时钟。数值 1 将隐藏该时钟，数值 0 将其设定为显示，如图 2-29 所示。

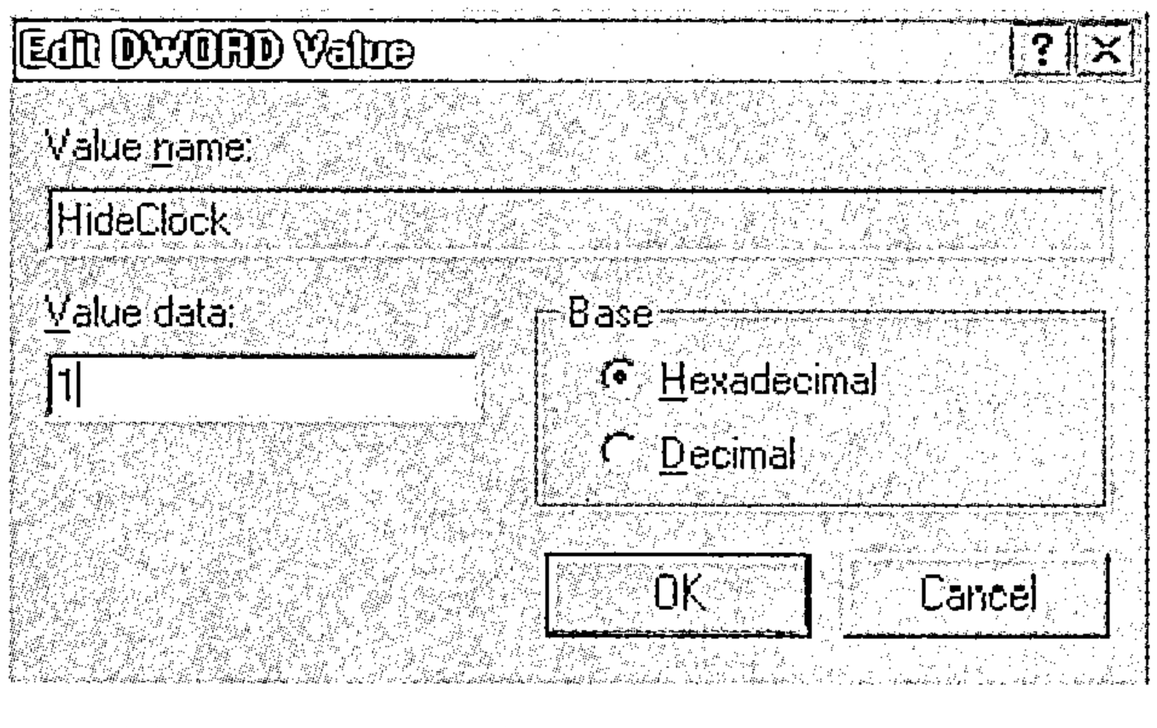

图 2-29　禁止或隐藏屏幕右下角的系统时钟

以下诸多选项修改，如图 2-30 所示。

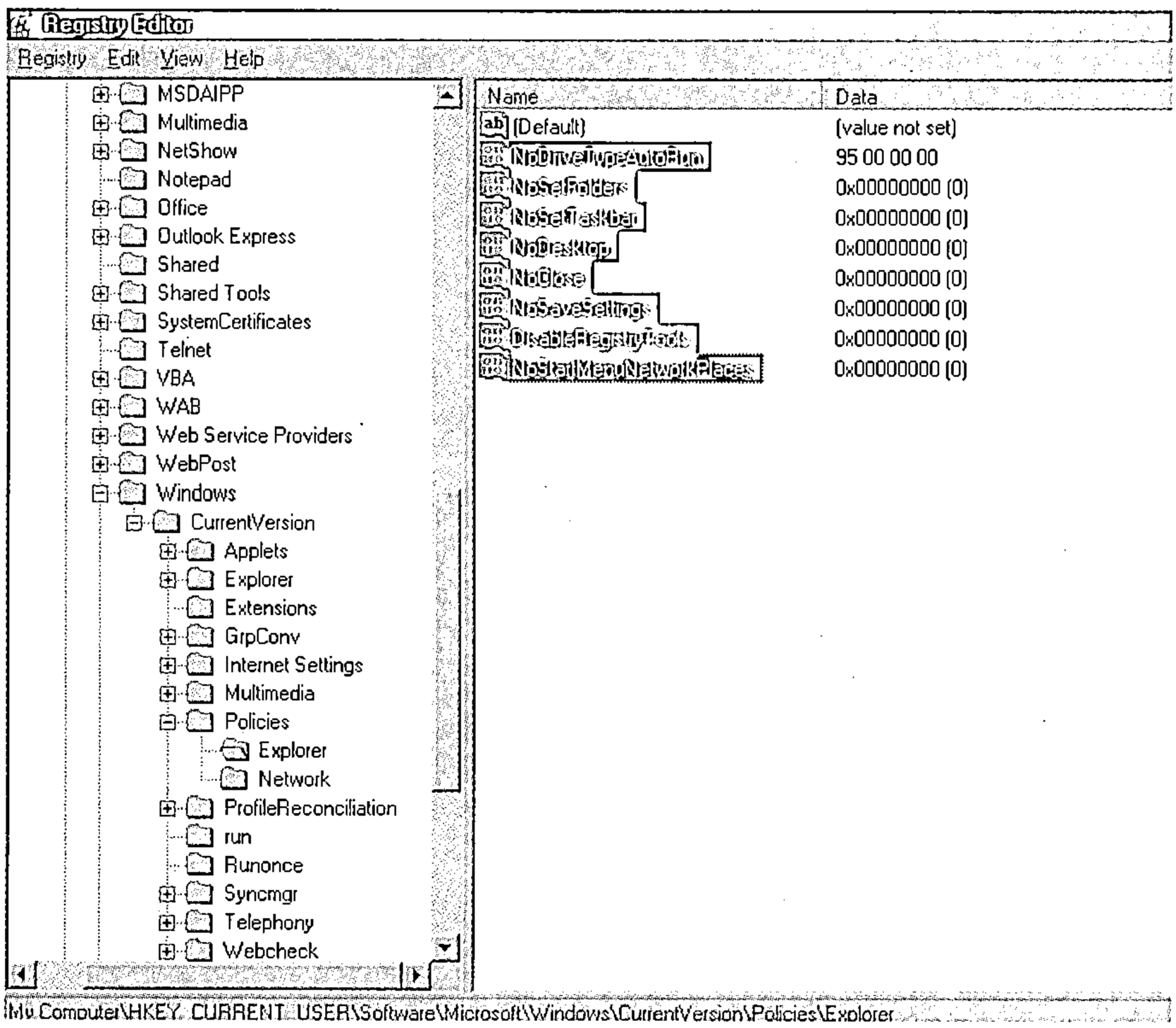

图 2-30　Windows 系统中关闭多项选项

NoSetFolders

该双字键值用于从开始菜单中移除整个设置文件夹（包括所有的诸如控制面板、打印机、任务栏等子文件夹）。数值 1 将隐藏该文件夹，数值 0 将其设定为显示。

NoSetTaskbar

从开始菜单中删除设置选项中的任务栏对应的系统文件夹。该选项限制从控制面板的菜单中删除任务栏和开始菜单项目，并可以限制从开始菜单中删除 Properties 菜单项。

NoDesktop

该双字键值用于完全隐藏系统桌面（包括所有文件、文件夹、系统文件夹等）。数值 1 将隐藏桌面以及桌面上的所有内容，数值 0 即可将其设定为显示。

NoClose

禁止关机并阻止用户正常关闭 Windows。

NoSaveSettings

该双字键值用于禁止用户更改桌面设置。数值 1 将保护桌面设置，数值 0 将允许用户更改桌面设置。

DisableRegistryTools

禁用注册表编辑工具。如果禁用该选项，Windows 注册表 (regedit.exe)也将不能正常工作。

NoStartMenuNetworkPlaces (仅适用于 Windows XP)

该双字键值用于从开始菜单中移除“我的网络连接”文件夹。数值 1 将隐藏该文件夹，数值 0 将其设定为显示。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"DWORD Entry"="VALUE"
```

4．在同一键项下，比如，*HKEY_CURRENT_USER/Software/Microsoft/Current Version/Policies*，可以新建一个名为 *System* 的子键，如图 2-31 所示。在该键中可以创建如表 2-3 所示的双字键值，并能获得许多非常有趣的特性，修改界面见图 2-32。

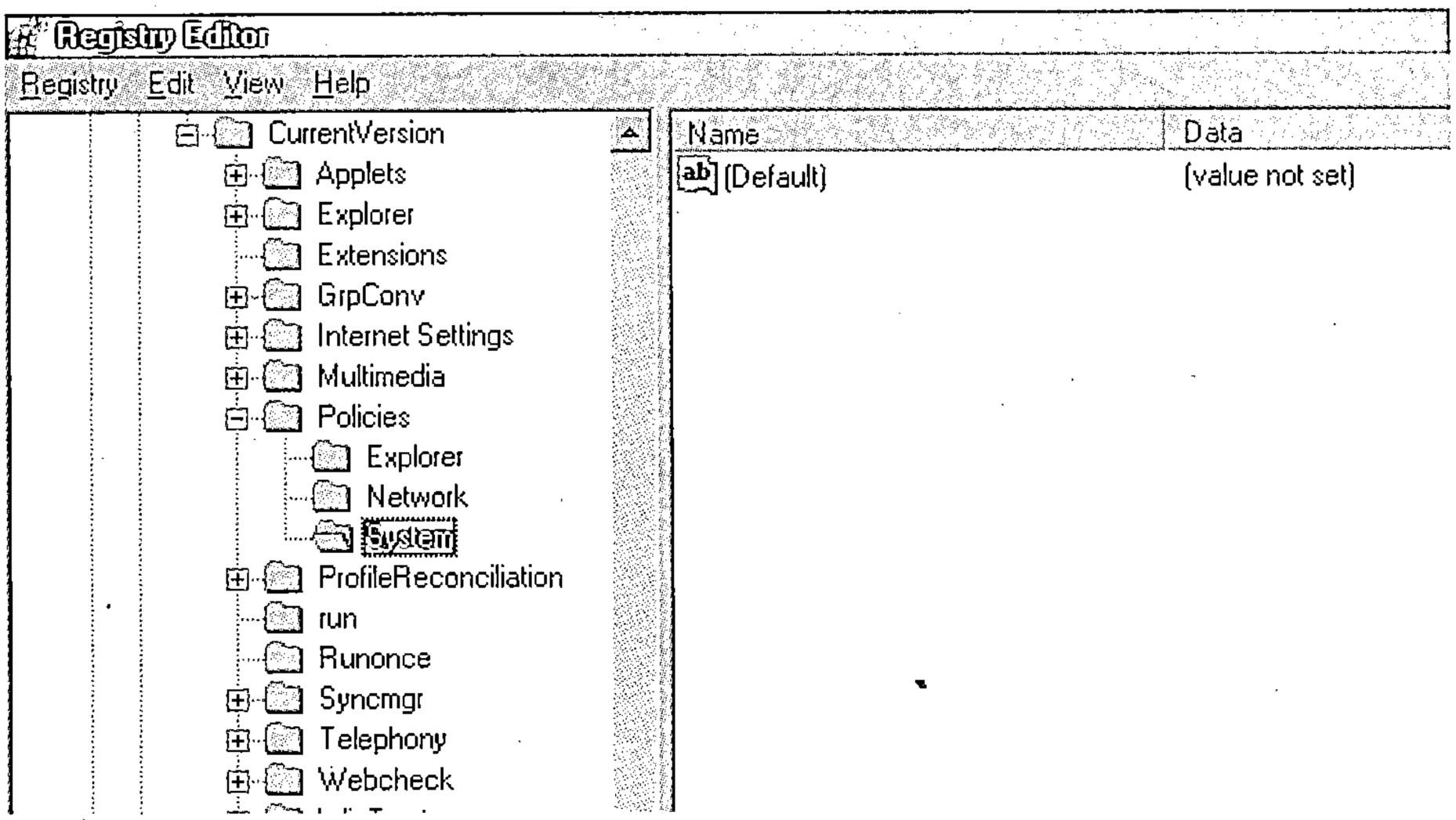

图 2-31　增加 System 子键

表 2-3　定制多项 System 选项

双字值	功　　能
NoDispCPL	隐藏控制面板
NoDispBackgroundPage	隐藏背景页
NoDispScrsavPae	隐藏屏保页
NoDispAppearancePage	隐藏外观页
NoDispSettingsPage	隐藏设置页
NoSecCPL	隐藏控制面板中的安全页
NoPwdPage	隐藏密码页
NoAdminPage	隐藏远程管理页
NoProfilePage	隐藏用户配置页
NoDevMgrPage	隐藏驱动器管理页
NoConfigPage	隐藏硬件配置页
NoFileSysPage	隐藏文件系统按钮
NoVirtMemPage	隐藏虚拟内存按钮

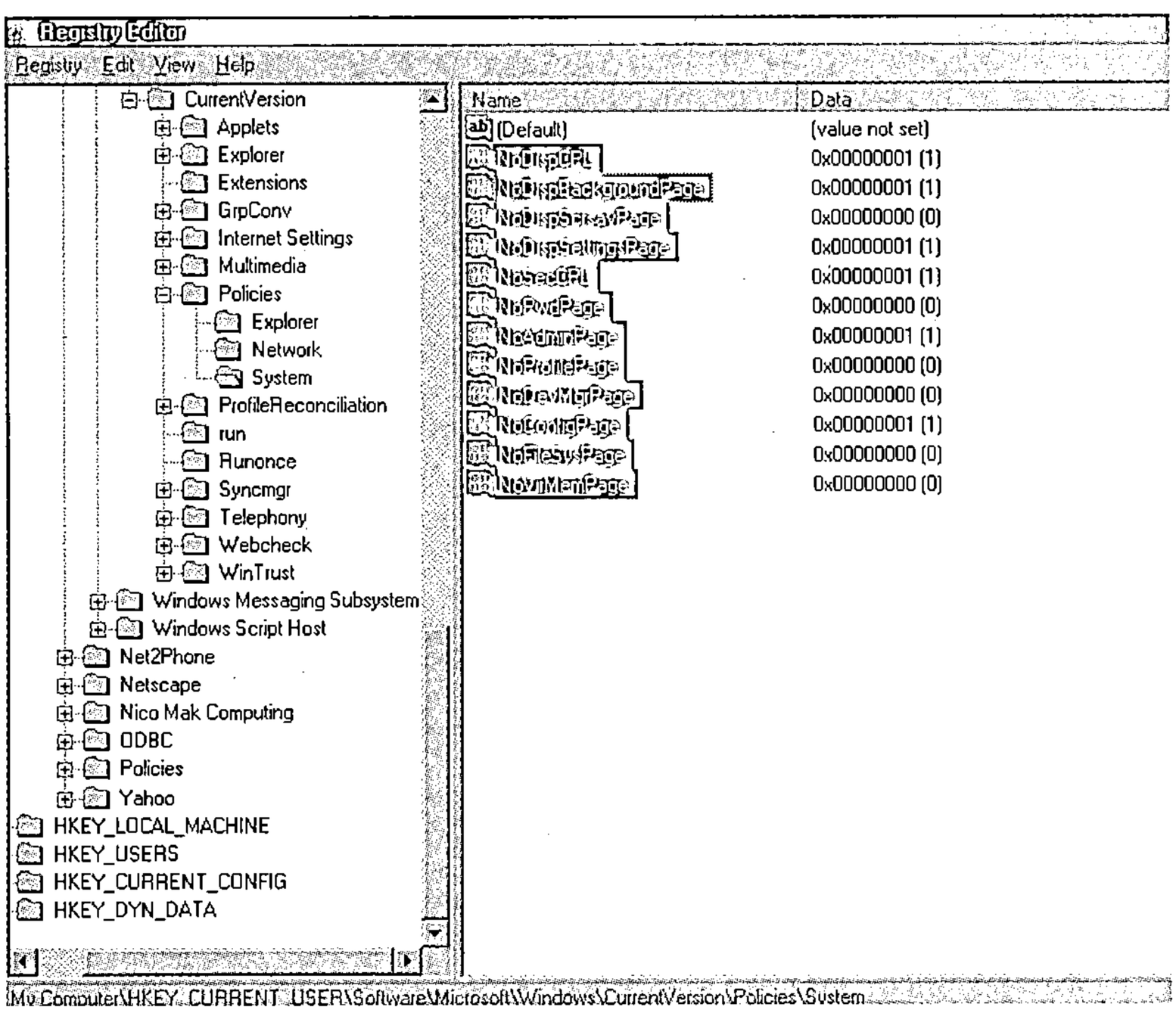

图 2-32　定制 System 多项选项

特别提醒的是，对于以上的双字键值，数值 1 即可启用该特性，而数值 0 将禁用该特性。也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_CURRENT_USER/Software/Microsoft/Current Version/Policies /System]
"DWORD Entry"="VALUE"
```

5．以相同的键项目为例，在 *KEY_CURRENT_USER/Software/Microsoft/Current Version/olicies* 下可以新建另外一个名为 *Network* 的子键，如图 2-33 所示。该子键可用于创建许多不同的双字键值，如表 2-4 所示，修改界面见图 2-34。

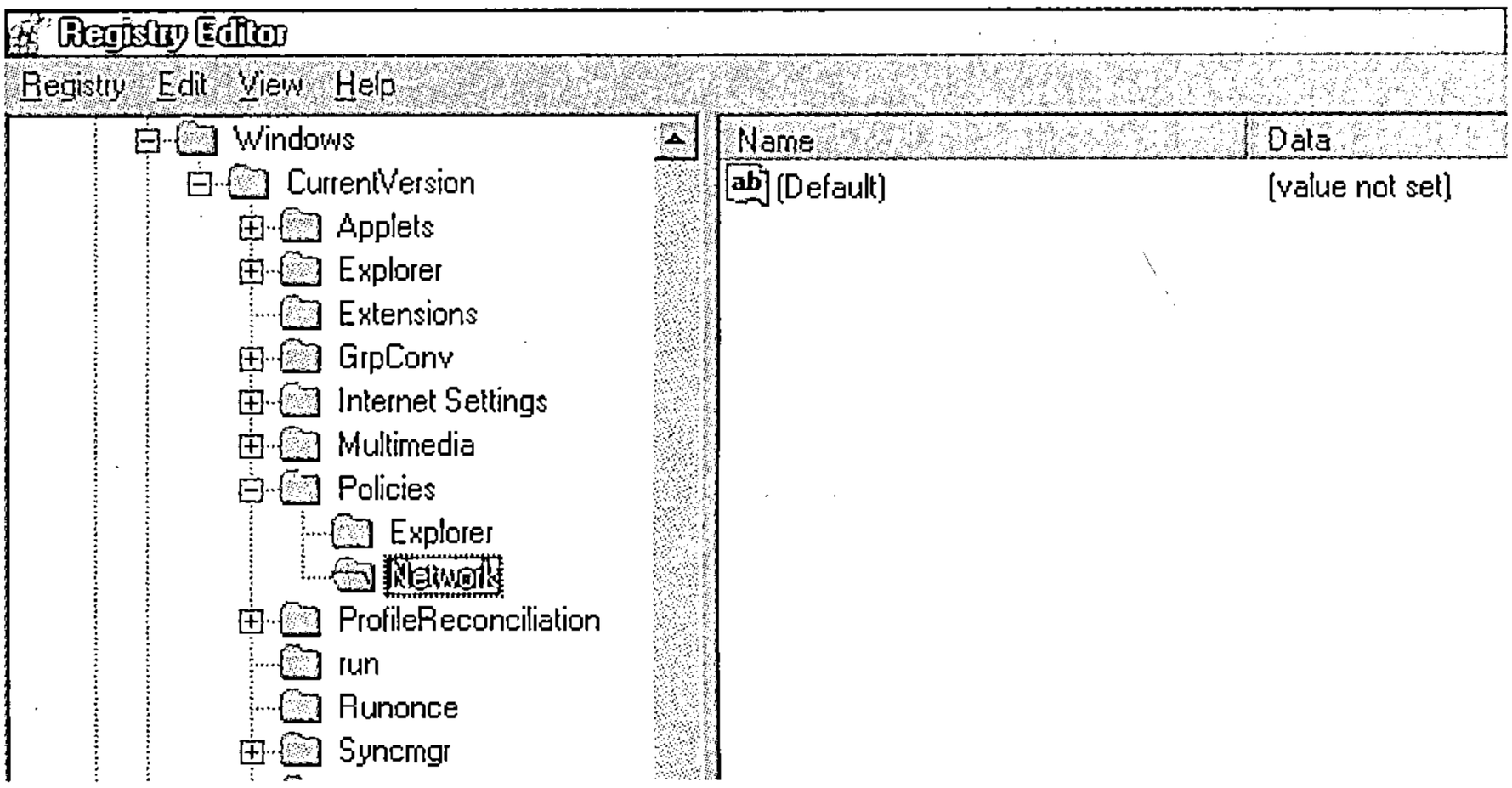

图 2-33　建立 Network 子键

表 2-4　字串与多项隐藏对照表

双字值	功　　能
NoNetSetupSecurityPage	隐藏网络安全页
NoNetSetup	隐藏控制面板中的网络选项
NoNetSetupIDPage	隐藏标识页
NoNetSetupSecurityPage	隐藏访问控制页
NoFileSharingControl	隐藏文件共享控制页
NoPrintSharing	隐藏打印机共享控制页

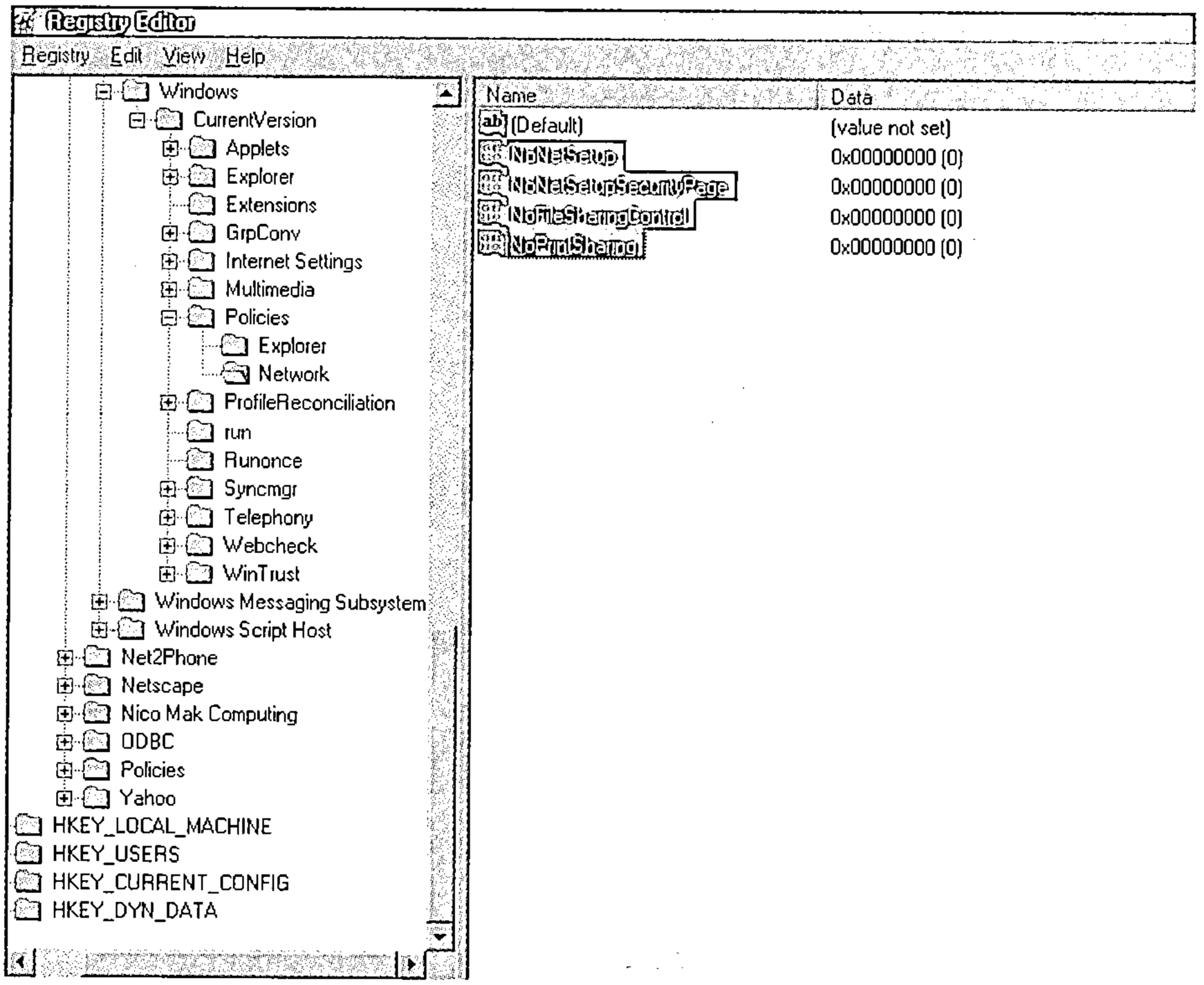

图 2-34　定制 Network 选项

特别提醒的是，对于以上的双字键值，数值 1 即可启用该特性，而数值 0 将禁用该特性。也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_CURRENT_USER/Software/Microsoft/Current Version/Policies /System]
"DWORD Entry"="VALUE"
```

2.27　通过 Explorer.exe 编辑 Windows

（其结果会因版本的不同而有所不同）

技术级别：高　　安全级别：高

每次同时按下 Ctrl+Alt+Del 组合键时，屏幕将出现结束程序的窗口。运行在当前内存中的应用程序文件所包含的进程中，总有一个被称为 *explorer.exe* 的文件。该文件控制着几乎所有的 Windows 操作系统的外观和功能。因此，可以说该文件中包括了用于定制 Windows 的键项目，以完全符合个人兴趣和偏好。可通过下面步骤编辑 *explorer.exe* 文件：

1．特别要注意的是，*explorer.exe* 文件不能在 Windows 操作系统工作的时候进行编辑。因此，首先需要如下操作——开始编辑 explorer.exe 文件之前，需要点击开始→关机→重新启动，在命令行模式重新启动计算机。

2．一旦以命令行模式启动计算机，要确保系统当前所在的目录为 *explorer.exe* 文件所

在的 Windows 根目录。

C:\>cd windows

3．在 MSDOS 编辑器中以/70 参数形式打开 *explorer.exe* 文件，也就是编辑器窗口以每行 70 列的格式打开该文件。

C:\windows>edit /70 explorer.exe

4．*explorer.exe* 文件将在蓝色屏幕上打开，其中包含了许多不可辨识的字符，以及一些可识别的字符。多数情况下，我们在编辑 *explorer.exe* 文件时更关注于那些可识别的字符。在屏幕上显示的每个字符都会在屏幕底部的状态栏上显示出相应的数值及其所在的行数，如图 2-35 所示。

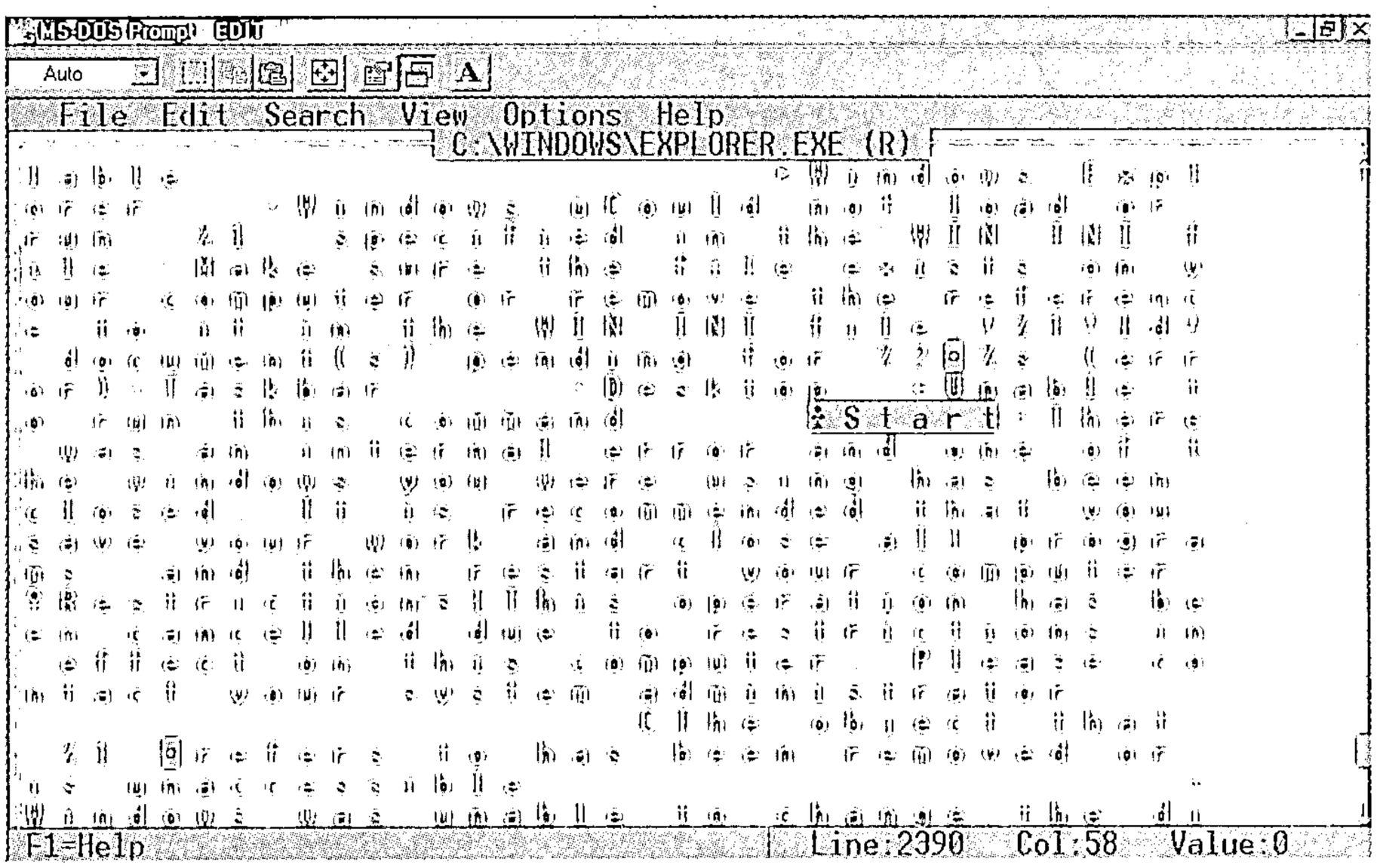

图 2-35　编辑 explorer.exe 文件

5．通过编辑 *explorer.exe* 文件中可识别区域的文本，就可以对 Windows 操作系统的外观等各种不同特性进行编辑。尽管编辑该文件不是很难，但仍然需要特别注意以下几点：

- ✓ 一定要确保 *explorer.exe* 文件中的字符总数在编辑前后的一致性，以避免系统崩溃。因此，编辑该文件过程中一定要小心，以防止意外的删除、修改或者添加。
- ✓ *explorer.exe* 文件包含了许多空格。然而，值得注意的是，文件中的这些空格不同于点击空格键所产生的空格。*explorer.exe* 文件中的空格所对应的数值为 0，而由空格键产生的空格所对应的数值为 32。
- ✓ *explorer.exe* 文件中的每个&表示其下一个字符在 Windows 操作系统中是非常关键的，通常被用来作为执行特定功能的键盘快捷方式。

- ✓ 一般情况下，右击 Windows 桌面的任务栏，随后将出现一个弹出菜单，包含了诸如属性、总在顶端、自动隐藏等各种菜单选项。可以通过 *explorer.exe* 文件中的第 1 300～1 400 行内容对该菜单选项进行修改。
- ✓ 当右击屏幕右下角的时钟图标时也会出现一个弹出菜单，为编辑该菜单选项内容，我们需要定位到 *explorer.exe* 文件中的第 2 300 行。
- ✓ 而为了编辑开始按钮中的开始菜单选项也需要更改从第 2 300 行开始的内容。

2.28 定制控制面板的外观

（其结果会因版本的不同而有所不同）

技术级别：高　　安全级别：高

控制面板可比作操作系统的控制中心，几乎所有的设置和属性都可以在控制面板中得到更改。可从开始菜单通过点击开始→设置→控制面板的方式访问它。控制面板中包含了比如声音和媒体、添加/删除硬件、日期/时间等许多不同的设置页。实际上，它几乎包含了 Windows 涉及的所有外观设置页，如图 2-36 所示。

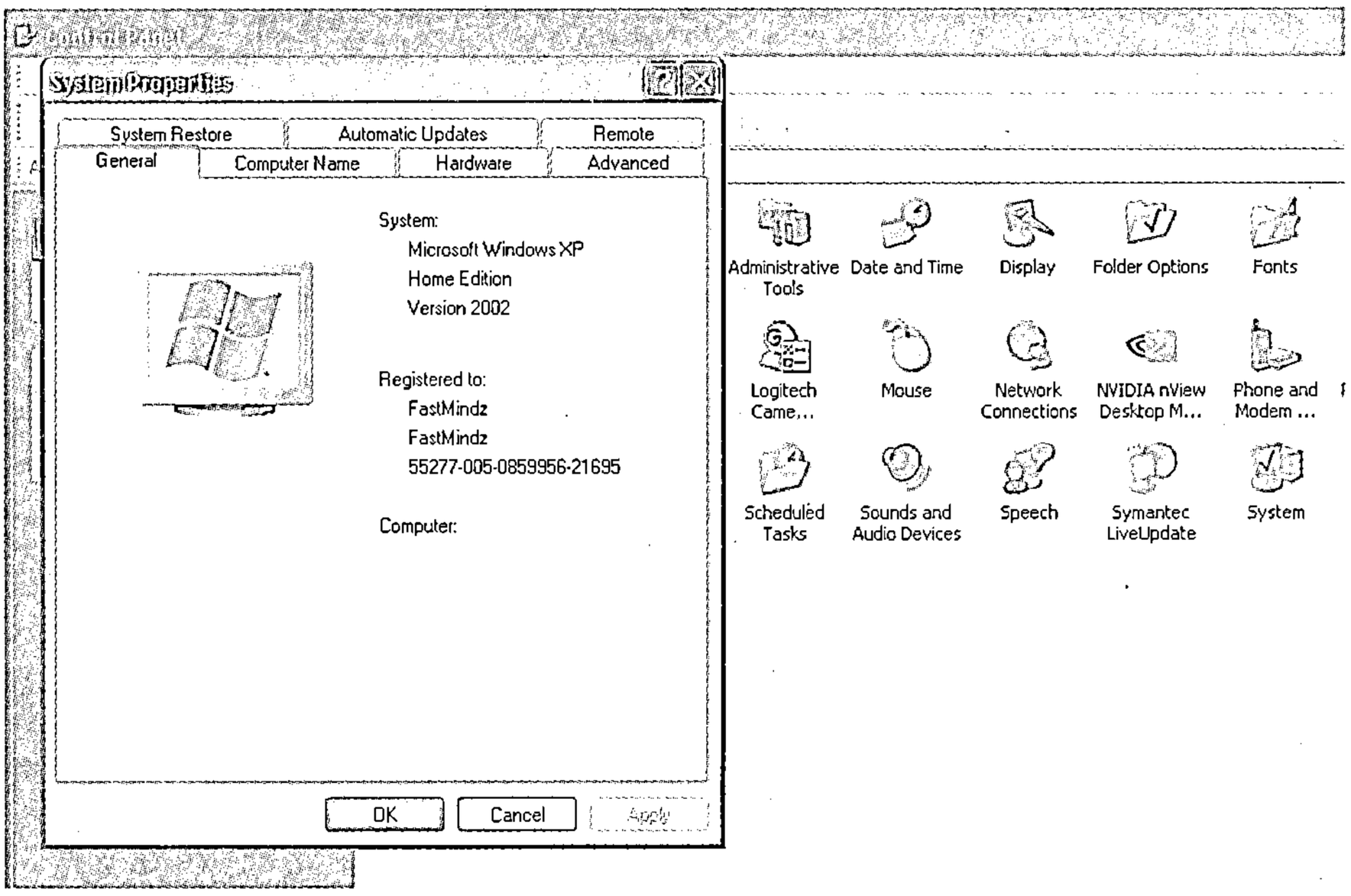

图 2-36　控制面板显示“系统”属性

控制面板中的每个设置页显示的实际上是存储于系统文件夹中的一个专门的.cpl 文件中的信息。也就是说，每个设置页的外观实际上是由它所对应的.cpl 文件进行控制的。比如，多媒体属性设置页体现的就是存储在系统文件夹中的 mmsys.cpl 文件中的内容。这些.cpl 文件包括了更改所有内容、外观等属性的键项，可通过以下步骤进行更改：

1．反复尝试或通过参照表 2-5 找到控制面板（需要进行定制的）设置页面及其所对应的.cpl 文件。

表 2-5 控制各项与文件对照表

控制面板页	.cpl 文件	控制面板页	.cpl 文件
添加/删除程序	Appwiz.cpl	调制解调器设置	Modem.cpl
显示属性	Desk.cpl	网络设置	Netcpl.cpl
区域设置	Intl.cpl	端口设置	Ports.cpl
传真设置	Fax.cpl	密码设置	Password.cpl
硬件向导设置	Hdwwiz.cpl	电源配置	Powercfg.cpl
Internet 选项	Inetcpl.cpl	系统属性	Sysdm.cpl
红外端口设置	Irprops.cpl	拨号设置	Telephon.cpl
世界/区域设置	Intl.cpl	扫描仪和照相机	Sticpl.cpl
鼠标选项	Main.cpl	日期/时间设置	Timedate.cpl
游戏控制器	Joy.cpl	访问设置	Access.cpl
多媒体属性	Mmsys.cpl	桌面主题	Themes.cpl

2．需要用 ATTrib 命令打开需要更改属性的.cpl 文件，才可以对该文件进行更改。

3．按照如下方式在 MSDOS 编辑器中打开.cpl 文件，如图 2-37 所示。

```
c:\>cd winnt
c:\winnt>cd system32
c:\winnt\system32>edit /70 abc.cpl
```

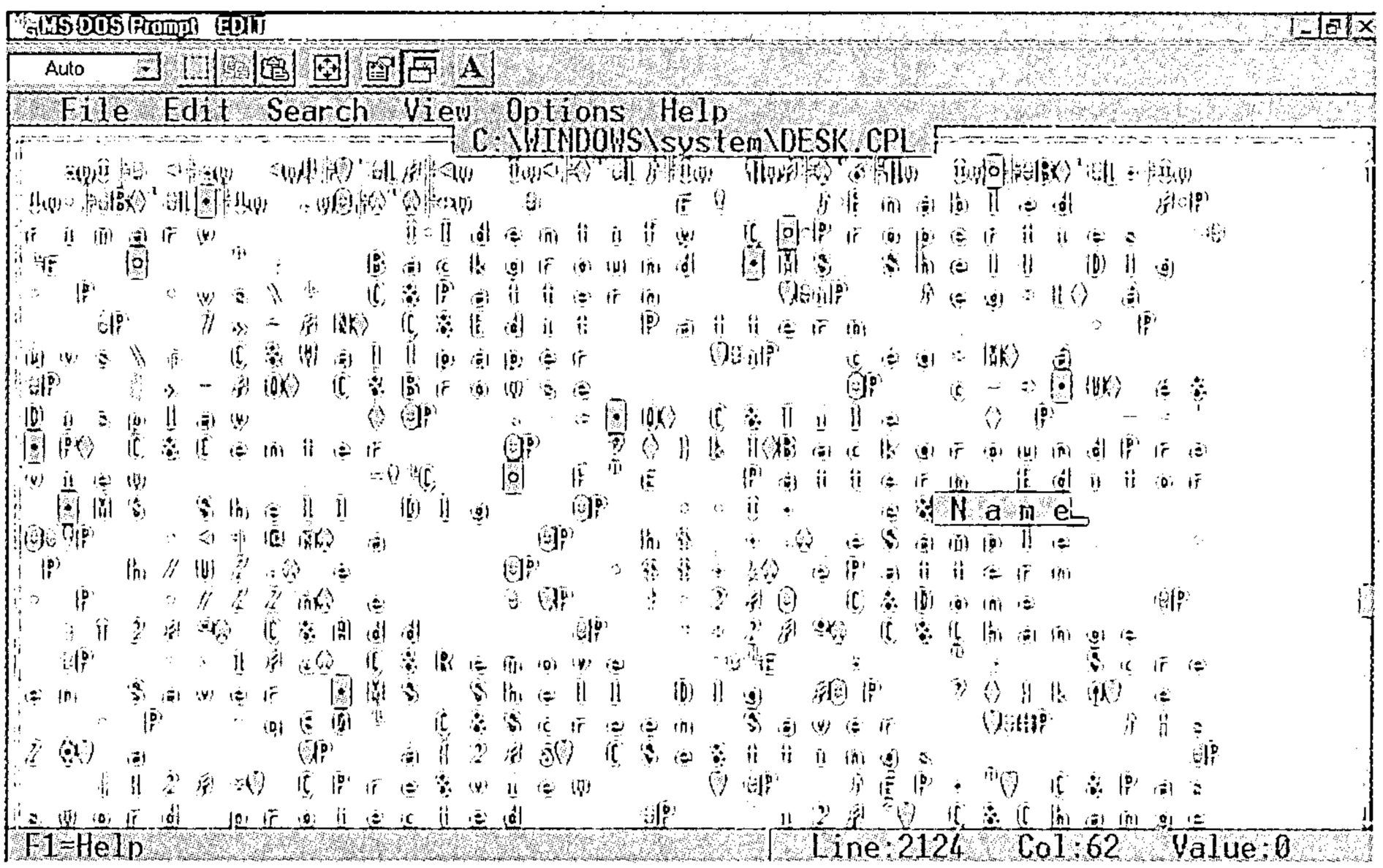

图 2-37 修改.cpl 文件

4．此时，你就可以对控制面板中相应的设置页的内容、外观等属性进行所有的更改。

5．更改完毕后，保存该.cpl 文件并退出 MSDOS 编辑器。下次打开控制面板中的特定设置页面时，你就会察觉到相应的变化。

2.29 隐藏控制面板设置页

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：高

可以在控制面板中隐藏特定的设置页面。有些时候，一个系统特性不但对系统安全非常关键，同时也极大程度地限制了用户操作空间。可通过如下步骤实现对 Windows 特性的隐藏功能：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_CURRENT_USER\Control Panel\don't load

3．对于控制面板中每个需要隐藏的设置页，都需要新建一个字符项，并以该设置页所对应的 .cpl 文件名来命名。请参照上述事例中所提及的所有文件名列表。

4．设置该字符项的数值为 No 即可隐藏控制面板中的设置页，设置为 Yes 即可将其显示，见图 2-38。

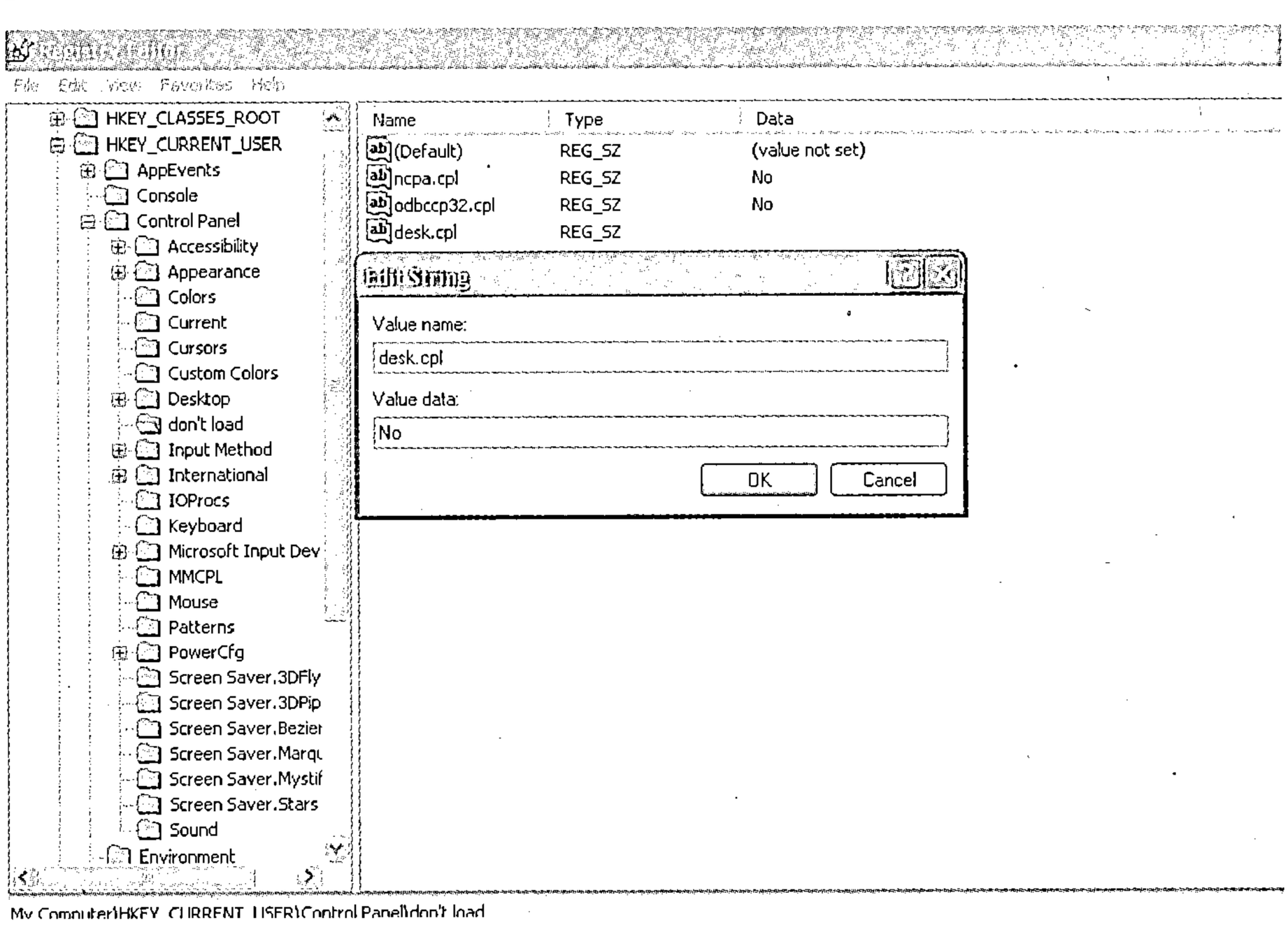

图 2-38　隐藏控制面板中的设置页

5．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

REGEDIT4

HKEY_CURRENT_USER\Control Panel\don't load

"Complete .cpl filename"="No or Yes"

2.30 定制添加/删除程序页（控制面板）

（适用于 Windows 2000 and XP）

技术级别：高　　安全级别：高

正如其名，用户通过添加/删除程序设置页即可在 Windows 操作系统中添加或者删除应用程序。该设置页可在控制面板中找到。通过注册表技巧，系统管理员可以完全定制该添加/删除程序设置页中的各种设置。

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall

3．在上述的 Windows 注册键项中可以创建如表 2-6 所示的双字键值。

表 2-6　字符与功能选项对照表

双字键值	功　　能
NoAddRemovePrograms	禁止添加/删除程序
NoAddPage	禁止添加页面
NoRemovePage	禁止删除页面
NoAddFromCDorFloppy	禁止从 CD/软驱中添加
NoAddFromInternet	禁止从 Internet 中添加
NoAddFromNetwork	禁止从网络中添加
NoServices	禁止其他的服务项
NoWindowsSetupPage	禁用 Windows 向导
NoSupportInfo	隐藏支持信息

尤其要注意的是，在上述的每种情况下，设置该双字键值为 1 即可启用该限制，设置为 0 即可对其进行禁用，见图 2-39。

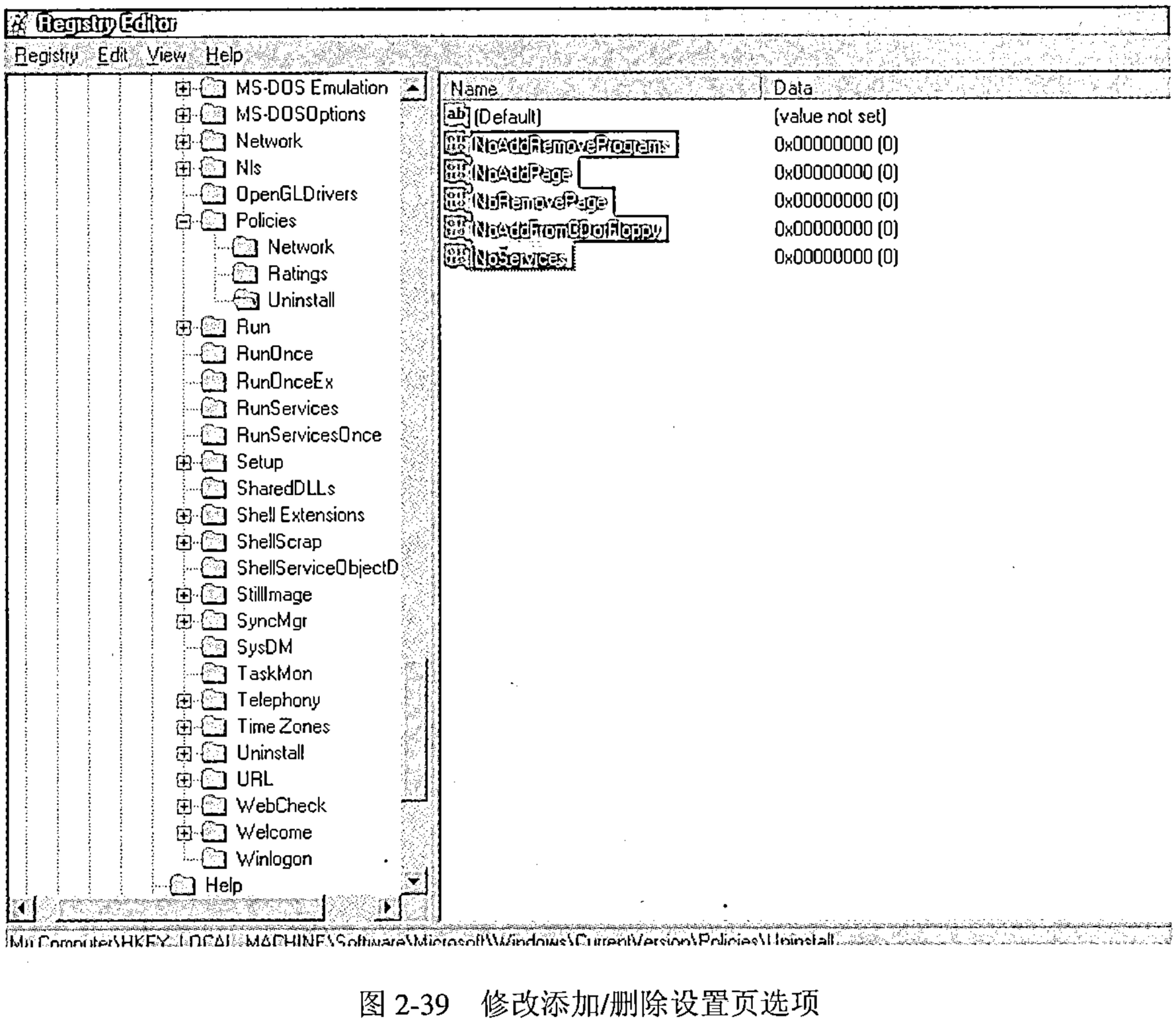

图 2-39　修改添加/删除设置页选项

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall]
"DWORD Value"="Data Value 0 or 1"
```

2.31　禁止程序自动启动

（适用于 Windows 所有版本）

技术级别：低　　安全级别：高

多数恶意程序，比如病毒、木马等都会在 Windows 启动时自动加载到内存。可很容易地通过一个简单的注册表项对程序的自动运行进行配置。因此，一个非常好的解决办法就是系统管理员通过 Windows 注册表禁止应用程序的自动启动。该注册表技巧如下所示：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

3．在上述的注册表项中，可以新建一些双字键项，所对应的功能如表 2-7 所示。

表 2-7　字符串与功能选项对照表

双子键项	功　　能
DisableLocalMachineRun	操作系统整个运行期间禁止所有应用程序的自动启动
DisableLocalMachineRunOnce	系统下一个会话期间禁止所有应用程序的自动启动
DisableCurrentUserRun	对特定用户的整个运行期间禁止所有应用程序的自动启动
DisableCurrentUserRunOnce	对特定用户的下一个运行期间禁止所有应用程序的自动启动

值得注意的是，在上述的每种情况下，设置该双字键值为 1 即可在每次加载 Windows 时禁止应用程序自动运行，为 0 即可允许其自动运行，如图 2-40 所示。

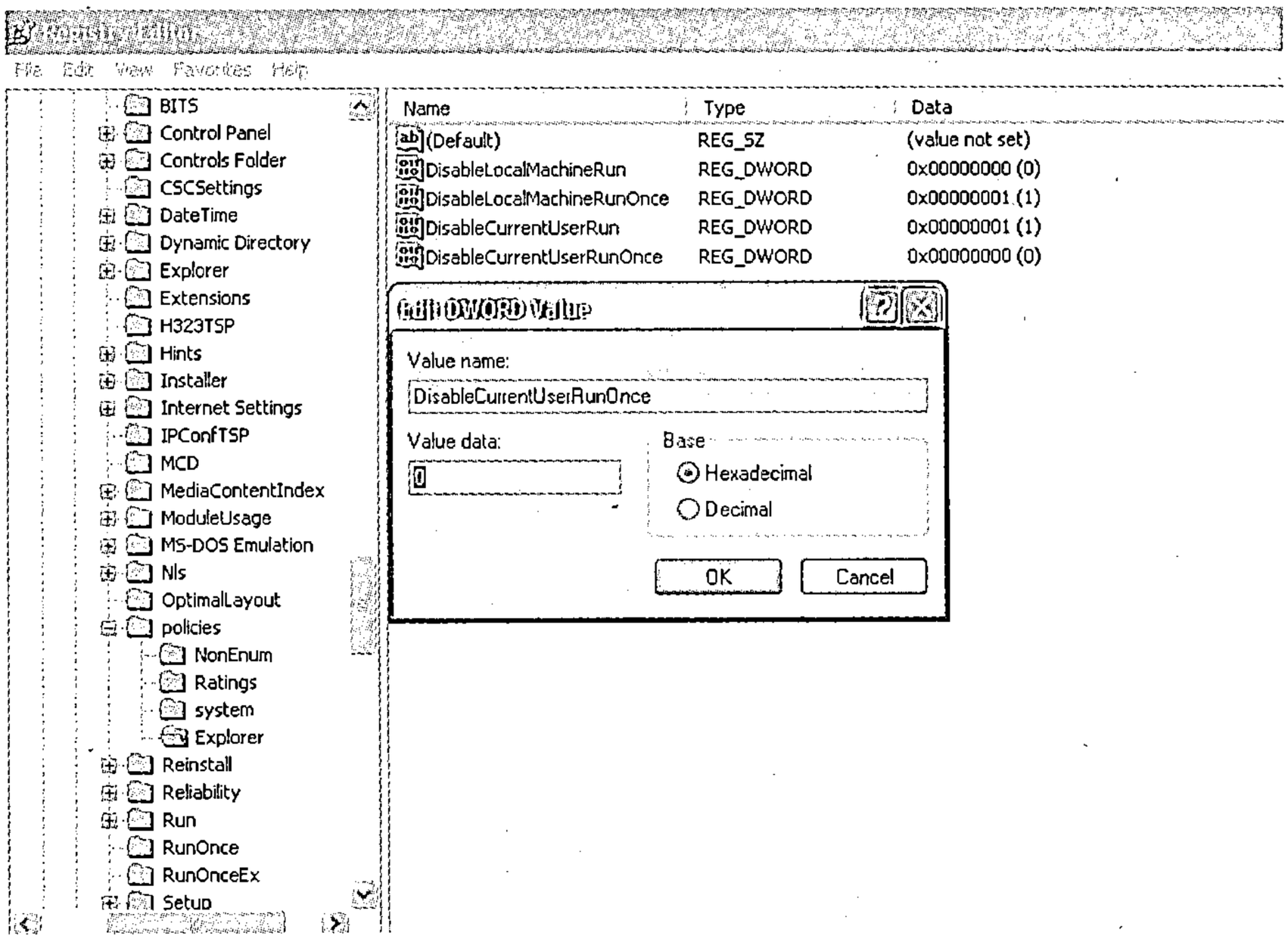

图 2-40　禁止程序自动启动

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"DWORD Entry"="Value"
```

2.32　禁止特定应用程序的自动运行

（适用于 Windows 所有版本）

技术级别：低　　安全级别：高

以上例为基础进一步讨论，实际上，我们可以在每次 Windows 启动时有选择性地阻止特定的应用程序自动加载到内存。可通过下面步骤实现：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\User init]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows]

3．在上述的注册表键项中，找到你想阻止其自动加载的应用程序所对应的键，并从 Windows 注册表中将其删除即可，如图 2-41 所示。

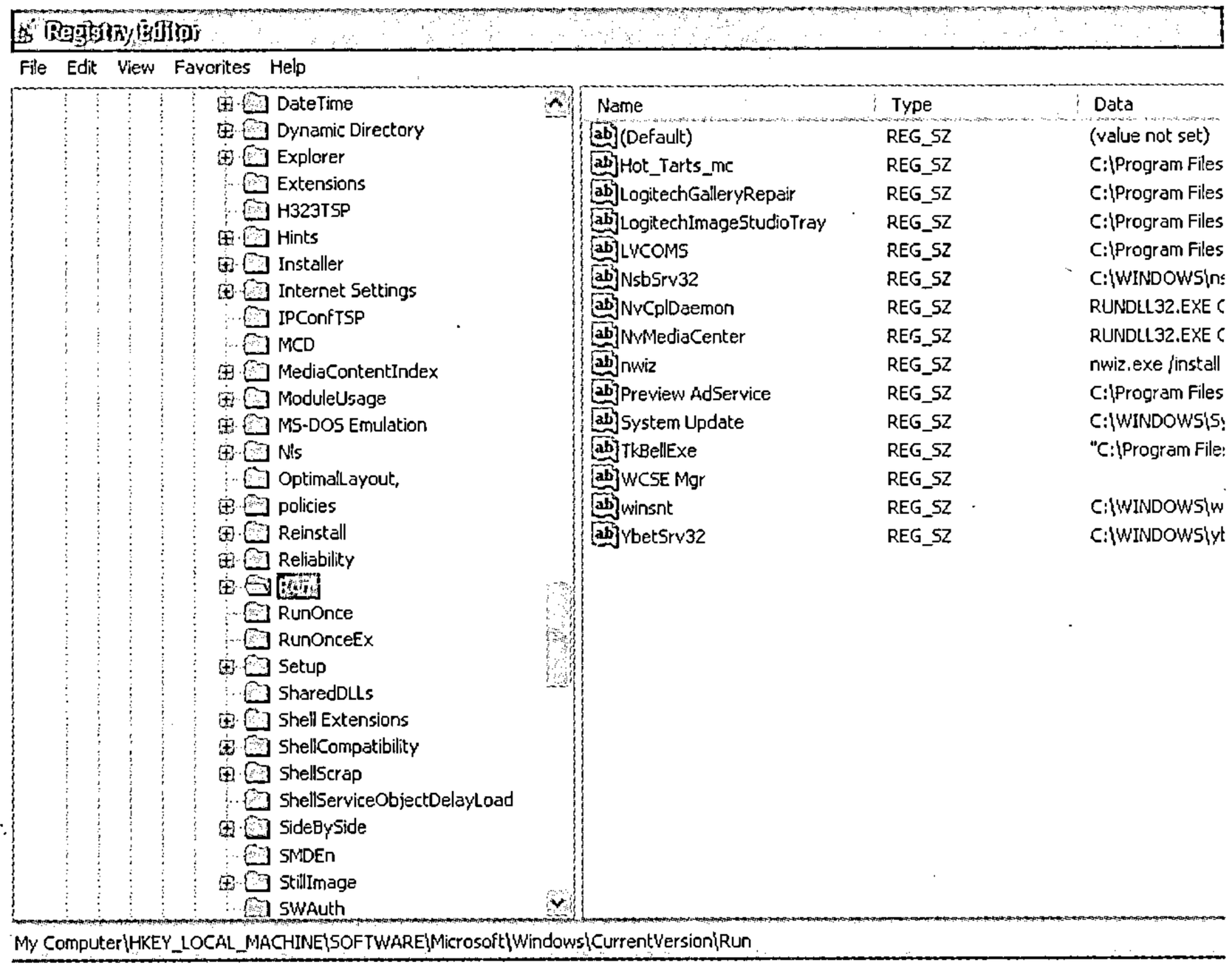

图 2-41　禁止特定应用程序的自动运行

4．需要留意的位置还有启动文件夹（C:\WINDOWS\开始菜单\程序\启动）以及 Win.ini

文件。

5．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

2.33 定制 MSN 信使的警告信息

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：中等

每次打开一个新的 MSN 信使会话时，就会出现一个如下的警告信息：

请不要在即时消息会话透露您的信用卡信息。

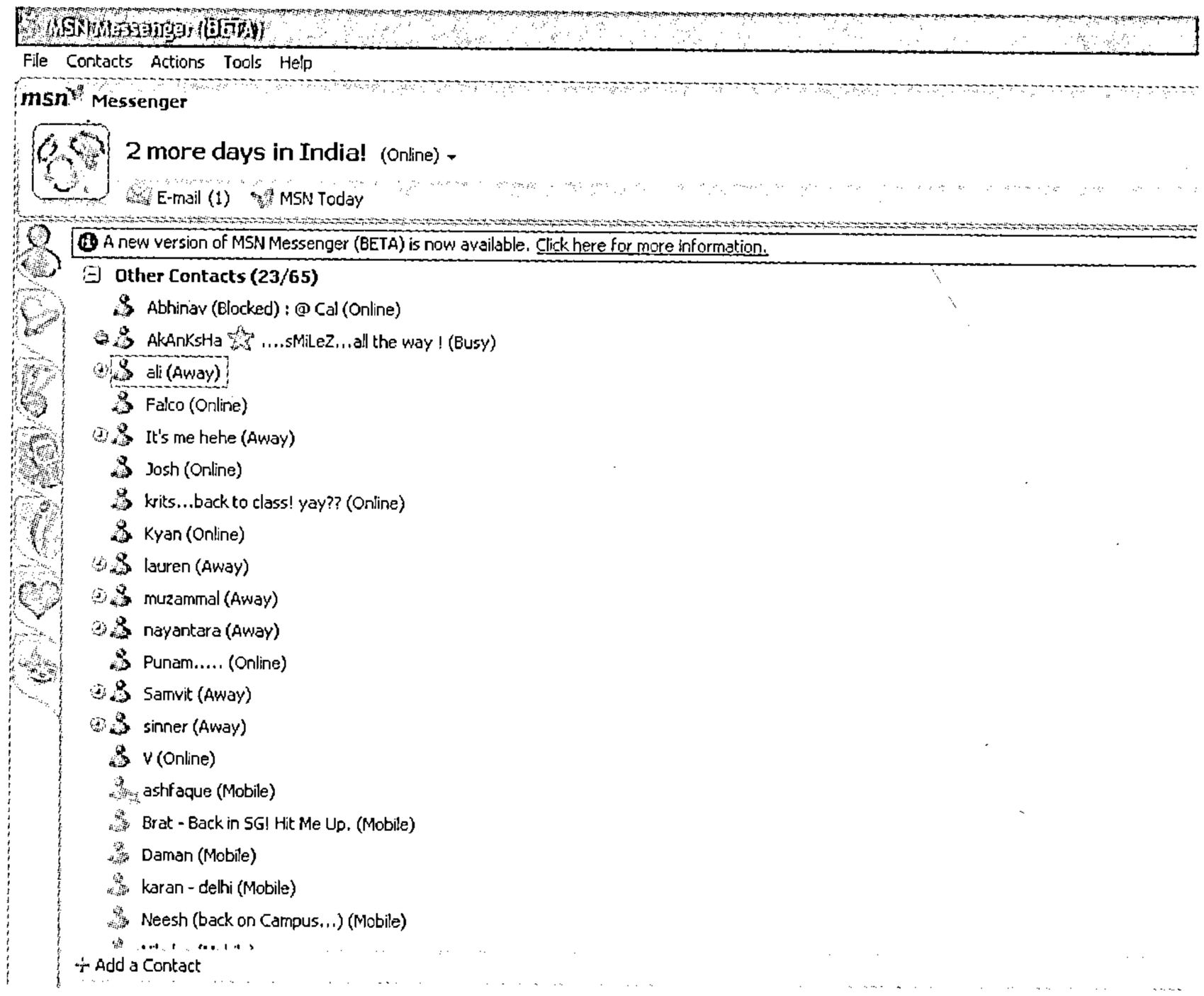

图 2-42　MSN 主界面

我们可以借助于 Windows 注册表技巧，通过以下步骤即可实现用自己定制的信息代替该警告消息：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies

3．在上述的注册键项中新建一个名为 *IMWarning* 的键值，并将其值设定为你所定制的欢迎信息。该信息就会在每次启动一个新的 MSN 信使会话时显示，如图 2-43 所示。

4．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能：

REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies]

" IMWarning"="Enter Customized Welcome Message"

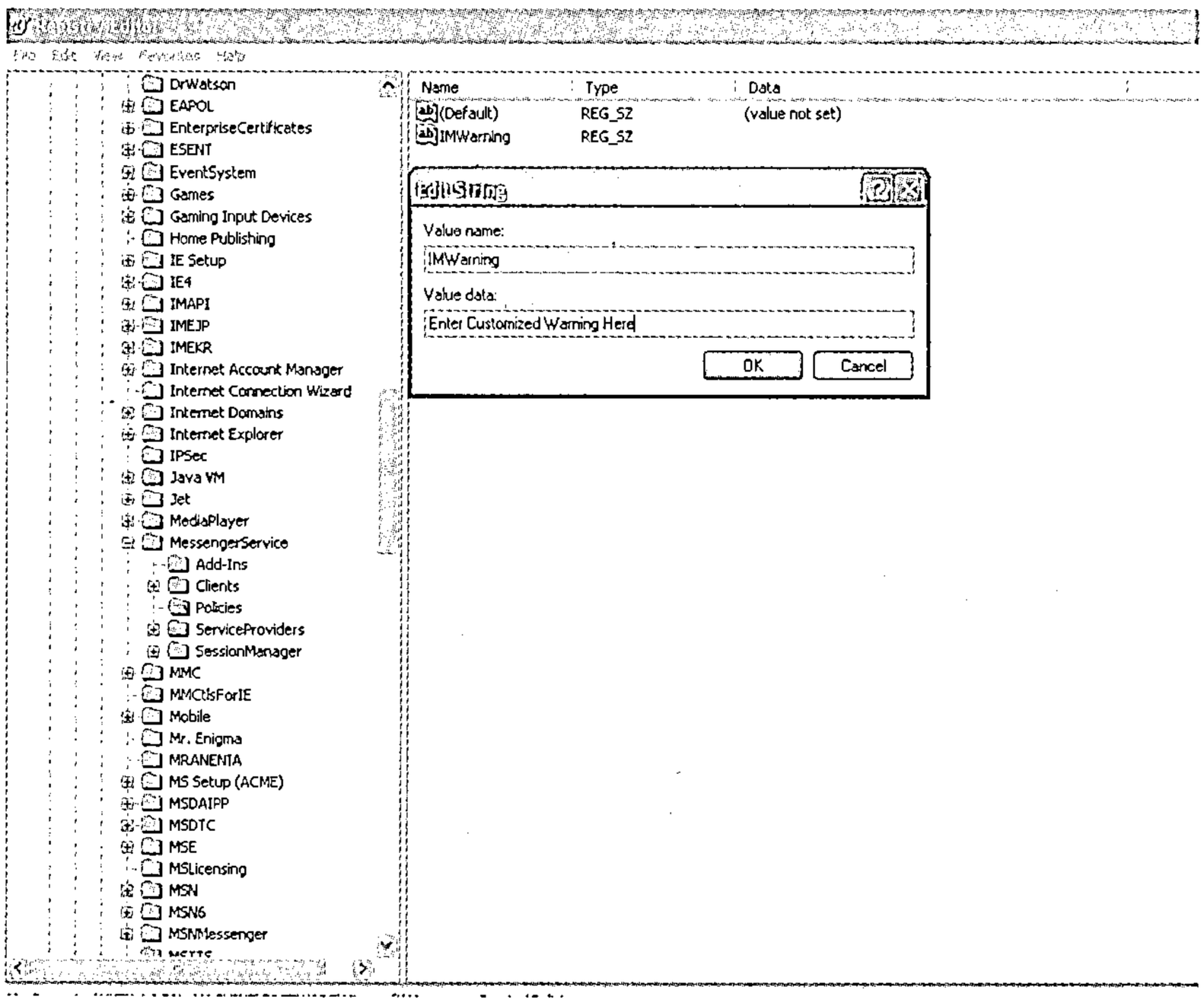

图 2-43　修改 MSN 信使的警告信息

2.34　定制 MSN 信使背景图像

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：低

MSN 信使的较新版本允许用户根据自己的偏好定制背景图像。大家曾经对 MSN 信使的这项新功能感到怀疑过吗？实际上，我们可通过下面步骤实现相同的功能：

1．定位到 MSN 信使的安装目录。

2．将 *lvback.gif* 图像文件用新定制的背景图片替换掉。

3．为使更改生效，需要重新启动 Windows。

2.35　限制 MSN 信使

（适用于 Windows 所有版本）

技术级别：中等　　安全级别：高

容易看得出诸如 MSN Messenger 等即时信使软件不但存在着安全隐患，同时也非常容易遭受非法入侵攻击。因此，一些系统管理员倾向于对用户的 MSN 信使活动进行检查。通过使用 Windows 注册表就可以使用一些小巧而又行之有效的方法，对 MSN 信使进行安全限制：

1. 打开 regedit.exe 文件。
2. 找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger\Client

3. 在上述的注册表项中，可以新建一些双字键项，所对应的键值及其功能如表 2-8 所示。

表 2-8 字符串与限制选项对照表

双字名称	限制内容
DisableFileTransfer	禁止文件传输
DisablePC2PCAudio	禁止语音聊天
DisablePC2Phone	禁止拨通电话
DisableVideo	禁止视频聊天
PreventAutoUpdate	禁止 MSN 自动更新
PreventBackgroundDownload	禁止背景下载
PreventConsumerVersion	禁止用户版本

4. 在上述例子中，可将该双字键值设定为 1 启用特定的限制，设置为 0 即可对其进行禁用，如图 2-44 所示。

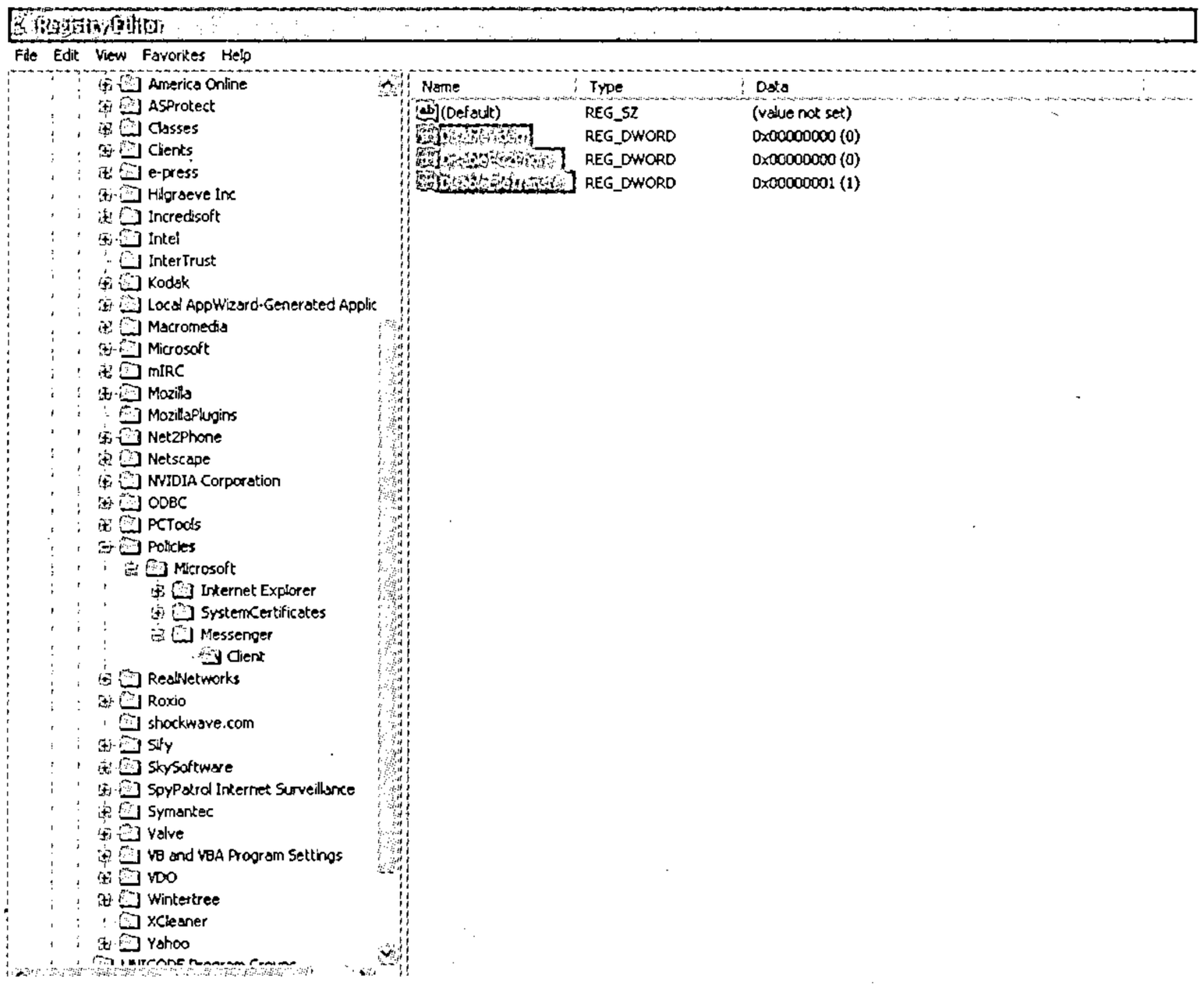

图 2-44 限制 MSN 信使

5．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger\Client]
"DWORD Name"="Value"
```

2.36 禁用 MSN 信使

（适用于 Windows 所有版本且适用于 MSN 信使 4X 及以上版本）

技术级别：中等　　安全级别：高

特定情况下，最好的办法就是借助于以下的注册表技巧禁用 MSN 信使服务：

1．打开 regedit.exe 文件。

2．找到或者创建以下的注册键：

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger\Client

3．新建名为 *PreventRun* 和 *PreventAutoRun* 的双字键项，分别用于阻止 MSN 信使自动启动以及将其完全禁用。

4．将上述的双字键值设定为 1 即可启用这些限制，设定为 0 即可禁用这些选项，如图 2-45 所示。

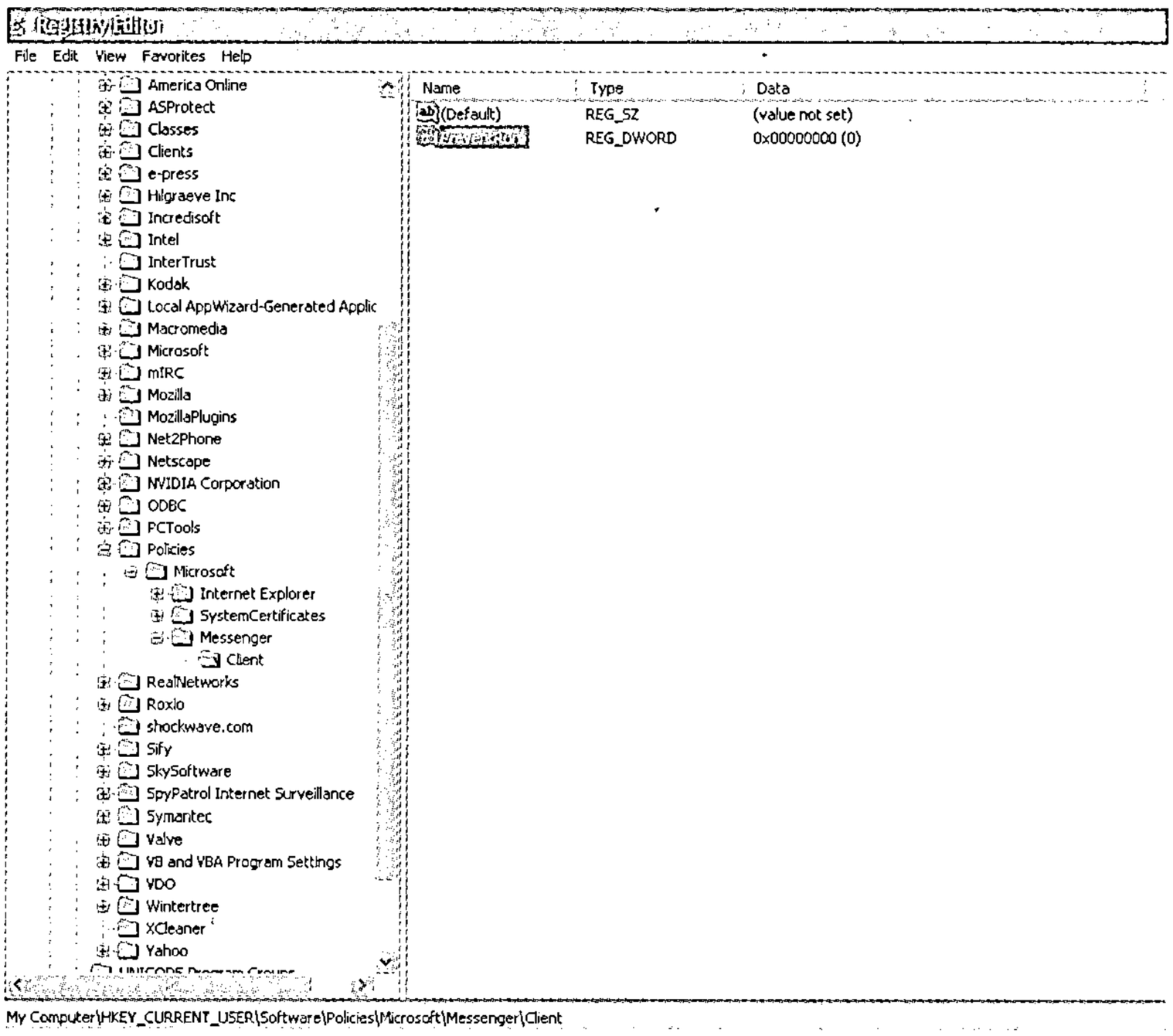

图 2-45　禁止用 MSN 信使

5．退出 Windows 注册表。为使更改生效，需要重新启动 Windows。根据你对 MSN 信使所做的限制，可以使用或者禁止使用该信使软件！

也可通过创建并执行包含以下代码的一个.reg 文件实现上述功能。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger\Client]
"DWORD Name"="Value"
```

2.37 模拟一个桌面地震

（适用于 Windows 所有版本）

技术级别：高　　安全级别：低

Windows 操作系统为用户提供了一些特有的功能，利用这些功能可以向受信任的朋友开个小玩笑。其中最为流行的技巧或者是错觉，就是被很多人所喜欢的桌面地震技巧，如图 2-46 所示。该技巧可借助于如下所示的 JavaScript 脚本实现：

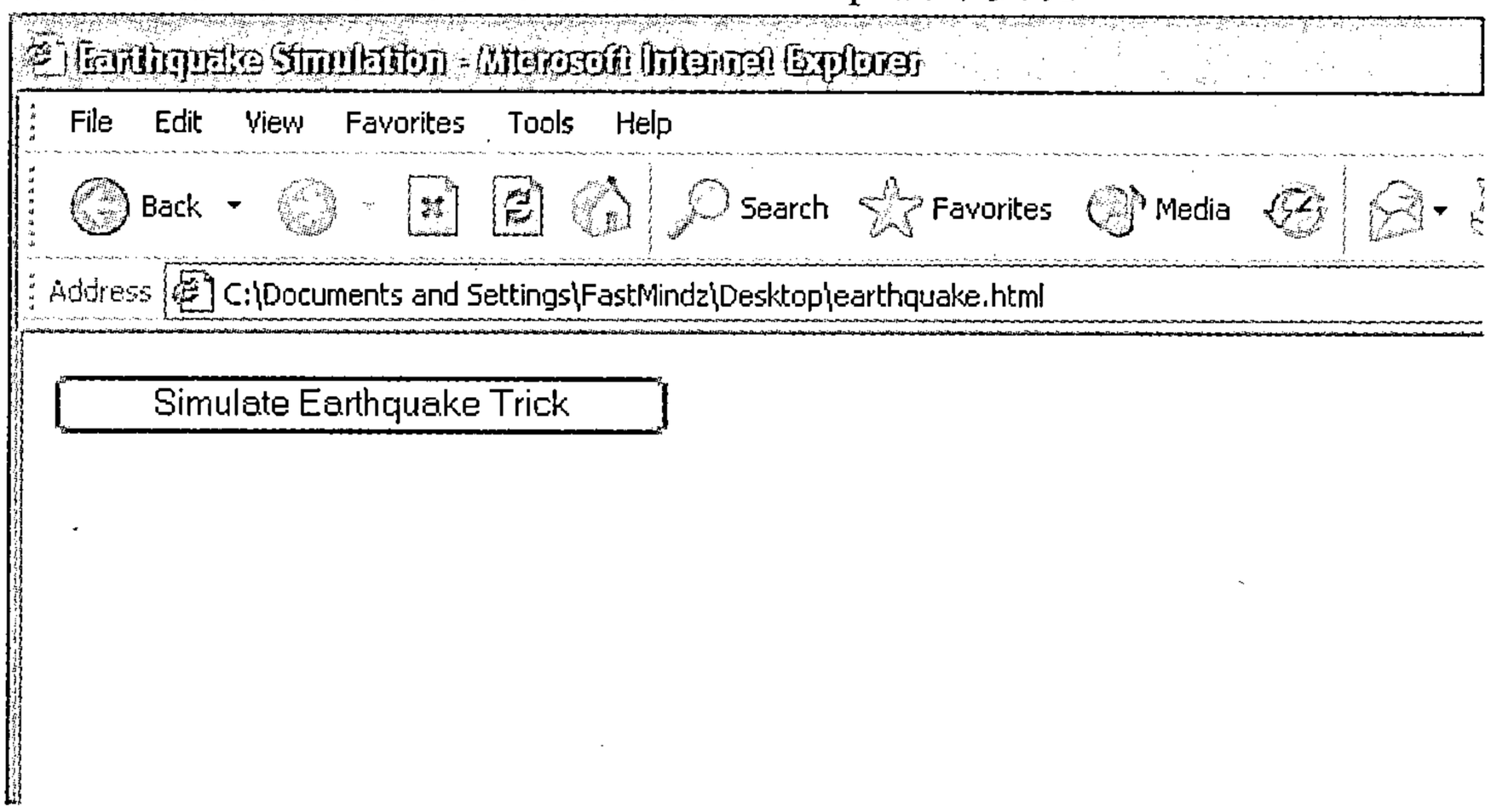

图 2-46　模拟桌面地震

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3c.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Earthquake Simulation</title>

<script language="javaScript" type="text/javascript">
<!--
function Quake(time)
```

```
{
  if (self.moveBy)
 {
    for (var side = 25; side > 0; side=side-1)
     {
       for (var tmp = time; tmp > 0; tmp=tmp-1)
        {
    self.moveBy(0,side);
    self.moveBy(side,0);
    self.moveBy(0,-side);
    self.moveBy(-side,0);
         }
    }
  }
}
//-->
</script>
</head>
<body>

    <form><input type="button" value="Simulate Earthquake Trick"
onclick="Quake(20);"/></form>
    </body>
    </html>
```

第三章 安全列表

3.1 强有力的密码保护

✓ 你所选的密码最好不要出现在字典里（以防止基于字典的攻击）。

✓ 密码不应该为空或者与用户名相同。

✓ 密码应该是字母、数字和特殊字符的组合。最好尝试使用大小写混用的组合。

✓ 密码最好不要用你的名字后面紧随自己的生日的组合。比如，不应该用 ankit2405 作为密码。

✓ 密码不应该是重复的。

✓ 必须定期更换密码。

✓ 密码不应该写在便条或者纸条上，更不能粘贴在你显示屏或者 CPU 背面。

✓ 不能在多种场合或多个系统中使用同一个密码。

✓ 密码不应是随机产生的，这样自己很容易忘记密码。

3.2 确保计算机安全的基本措施

✓ 至少一周运行一次 Windows 更新，下载补丁程序修补系统，以防止系统威胁、漏洞和恶意攻击。

✓ 使用强有力的密码保护（参见上述内容）。

✓ 安装较好的防病毒软件，并至少一周更新一次病毒库，以防范最新的病毒和木马。

✓ 在系统中安装防火墙（比如 Zonealarm、BlackIce，或者防病毒软件自带的防火墙）。这将会使你对任何恶意攻击、恶意数据或探寻保持警惕。

✓ 尽量使用代理服务器访问互联网。

3.3 防范木马攻击

一旦发现受到了木马攻击，就要尽可能地采取以下的防范措施：

✓ 如果在受害计算机上所保存的极其机密的数据或知识产权受到潜在攻击的威胁，较好的办法就是立即将受害计算机从互联网上断开。该举措将会尽可能缩小受到潜在危害的范围。

✓ 通常情况下，好的防病毒工具能够探测并删除木马程序。因此好的办法就是及时更新病毒库文件，以有力地防范最新的病毒和木马。