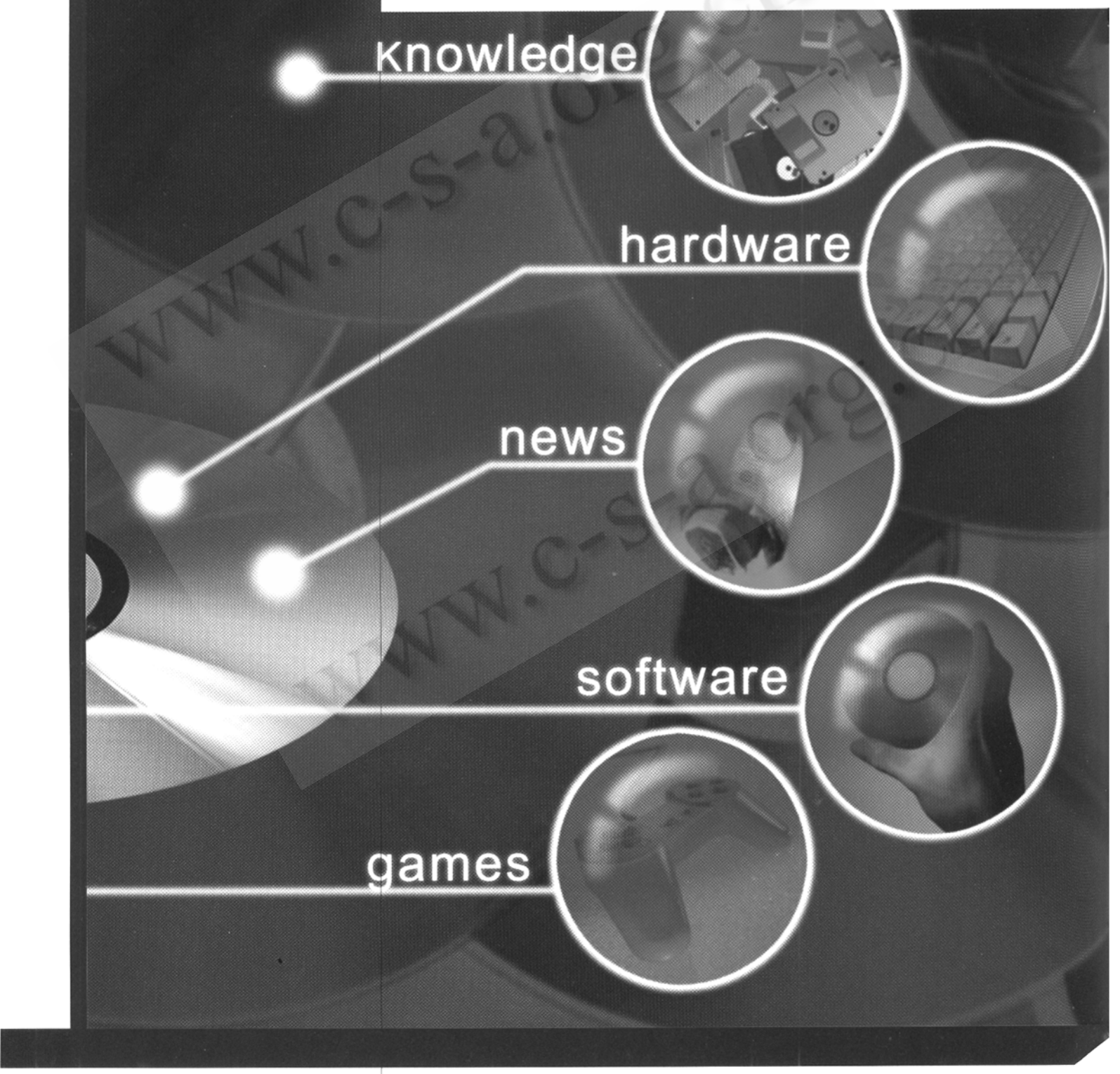
RegMon 使用方法及其扩展应用

丁 健 （中科院南京地理与湖泊研究所、中科院研究生院、解放军理工大学工程兵工程学院）
杜 青 （南京工程学院计算机科学系 210009）
陈永红 （南京军区军事医学研究所 210000）
张万军 （蚌埠 总装工程兵驻蚌埠地区军代室 233000）

摘要 本文介绍了注册表监视程序RegMon的使用方法和其在解除试用软件使用日期或次数限制方面的应用。

关键词：注册表 监视



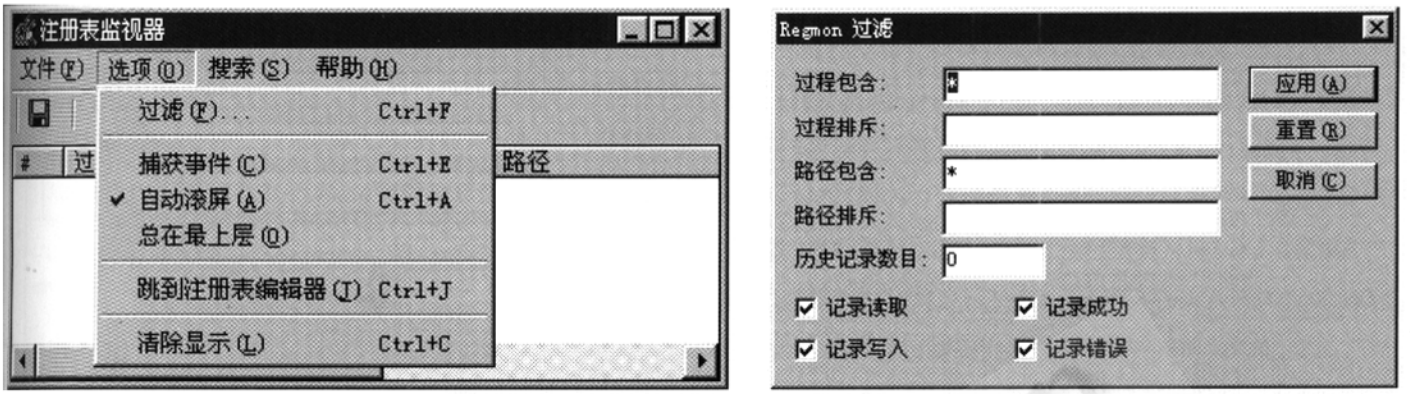


图 1 RegMon运行界面及"过滤"功能设置

1 对试用版软件借助注册表进行用户试用限制控制方法的分析

网络技术的飞速发展和网络的普及促使一种全新的软件销售方式的产生：在网络上建立公司主页，开辟专门的软件试用版下载区，任何上网者经过一定的注册步骤后均可以免费下载软件的试用版本，让用户先试用一段日期或次数，然后决定是否购买。这种网上传播方式无疑是一种快速、低价的发放方式，有利于提高软件企业的竞争力。但是，这种方式也带来如何有效控制用户有限使用的问题，即限制用户使用的日期或次数。在对一些软件试用版本试用控制机制的研究中，我们发现不少软件利用注册表进行加密，具体方法可简单描述如下：在注册表一定位置的子键中建立用户已使用次数或日期的档案，并根据该子键判断是否到期以终止或继续用户的试用。这种控制方法嵌在程序内部极具隐蔽性，软件卸载时Windows的Uni nstall Shield无法删除程序自己加入的子键，用户即使重新安装软件也无法改变控制条件到期的状态，改回日期等已不再奏效，因而可以有效地控制用户的试用。

不过，注册表监视程序的出现，使得用户较容易就能找到控制信息所在子键。注册表监视程序能随时监测到系统及应用程序过程对注册表的读、写、更改等操作，可以设定对指定过程跟踪，可以将指定过程对注册表的读写位置及内容列示出来，原本嵌在过程内部对注册表的读写操作将毫无隐蔽性，用户对监视结果稍加分析，即能找到延长软件试用日期或次数的办法。

RegMon是众多注册表监视软件中较为典型的一个，本文对其使用方法作说明，着重介绍其在解除软件试用限制中的应用。

2 RegMon介绍

RegMon，全称Registry Monitor，实用、小巧，可执行文件只有70kB左右。RegMon监视注册表数据库，它将与注册表数据库相关的一切操作(如读取、修改等)全部记录下来供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理。RegMon的功能都可通过选单命令实现，其选单栏共有"文件、选项、搜索、帮助"四项(见图1左图)。核心功能体现在"选项"选单的调用，此选单中包含一个"过滤"选项卡及捕获事件、自动滚屏、跳至注册表和清除显示等项(见图1右图)。在"过滤"选项卡我们可设置过滤选项，指定监视(忽略监视)的程序名称、指定要监视(忽略监视)的注册表分支，让RegMon有选择性地记录下部分注册表操作而舍弃另一部分。并可要求RegMon记录对注册表操作成功的信息或记录对注册表操作失败的信息。为了方便起见，用户一般不必打开读取监视，只需对写操作重点注意。灵活使用"过滤"选项卡提供的各种过滤功能来缩小监视范围是绝对必要的，这将有助于避开大量无用的记录，迅速找到感兴趣的信息。

3 RegMon在解除软件试用限制中的应用

我们分别以解除"金山毒霸2001试用版"(杀毒软件)30天试用日期限制和"TalkToMe"(英文朗读软件)20次试用次数限制为例，说明具体的操作过程和识别方法。

3.1 解除"金山毒霸2001试用版"一个月试用日期限制

金山毒霸2001试用版从安装日起一个月内试用，无任何提示和功能限制，一个月后提示试用版已过期。监视时，先在RegMon的过滤对话框内进行如图2所示设置，注意只输入文件名，不能带EXE扩展名。点"应用"按钮后，双击"KAV9X.EXE"文件，启动金山毒霸2001试用版，可以观察到RegMon界面的监视结果列表内不停地有信息加入。

关键的工作是对监视结果列表内信息的分析，往往是在成百上千条信息中只有几条真正与软件开发时设置的注册表加密子键有关。通过注册表进行用户试用控制的软件在启动过程中对注册表加密子键必然有打开(打

开存放控制条件的子键)、读取(读取子键内现有日期或次数)、更新(以现有日期或目前累加次数更新子键)、关闭(关闭存放控制条件的子键)四步操作，其对应的RegMon“请求”是OpenKey、QueryValue、SetValue、CloseKey，对上述四种操作连续出现的信息应加以重点分析，在信息条上双击进入注册表内对应键。

在对金山毒霸2001试用版的监视结果中，如图3所示的信息条具备OpenKey、QueryValue、SetValue、CloseKey四种操作连续出现的特征，事实上信息条所指注册表子键正是加密子键(见图4)。软件将用户最初安装日期存放在“drf”子键中，运行时的当前日期存放在“drl”子键中，如“drl”与“drf”值差值大于30，即表明试用日期已满，提示结束试用。如想延长试用日期，最简单的方法是删除加密子键，软件在启动时会误认为是最新安装。

3.2 解除“TalkToMe”20次试用次数限制

“TalkToMe”在试用20次后，启动时提示试用次数到期，用户须注册或购买。我们用RegMon对TalkToMe运行过程进行跟踪。首先，在“过程包含”编辑框内输入TalkToMe的主程序文件名“TalkToMe”，确认后，RegMon运行，进入监视状态。接着启动TalkToMe，RegMon对TalkToMe运行过程注册表操作监视的部分结果如图3所示，这一部分显示RegMon的判断过程。每次RegMon运行前期先从注册表一定位置处读出上次存放的已使用次数，如未到限制次数即继续运行，并将已使用次数加1后存入指定位置；如到限制次数即结束运行，并提示购买。从图5中的监视内容中，我们注意到[HKEY-CURRENT-USER\Software\VB and VBA Program S ettings\101\0]键下串值“Windata”的值随使用次数不停增加，我们不难断定[HKEY-

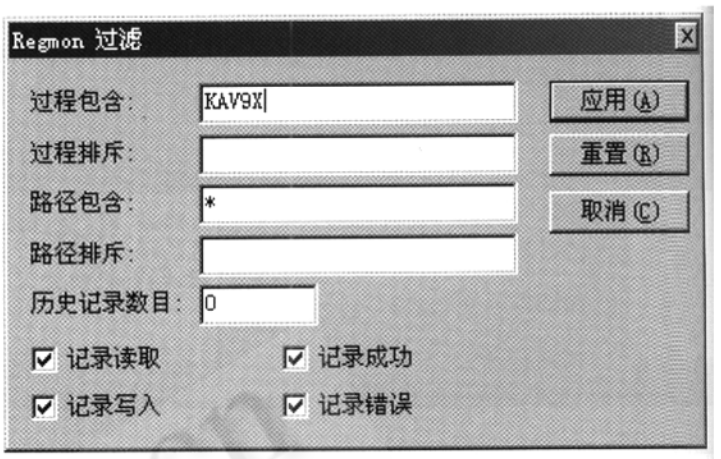


图 2 过滤对话框设置

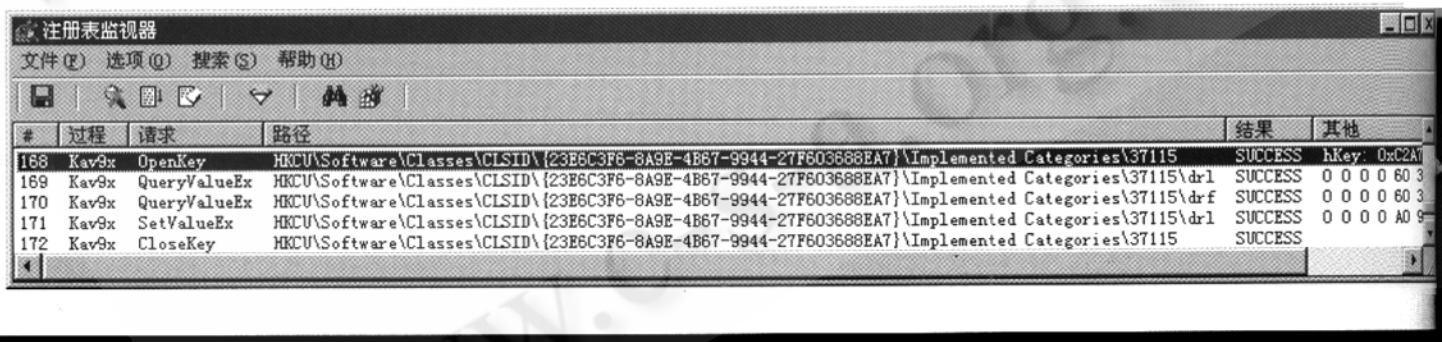


图 3

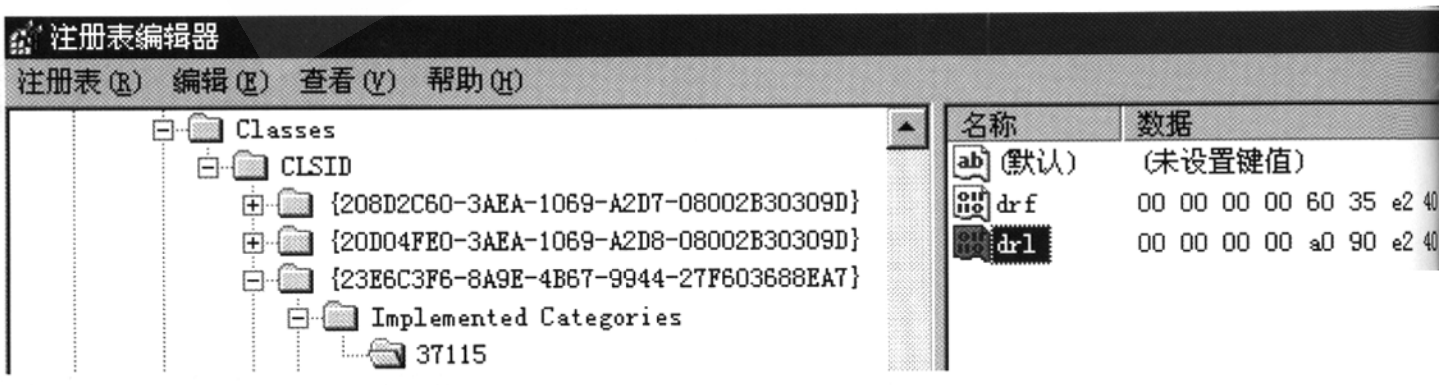


图 4 加密子键

请求	路径	结果	其他
CreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	hKey: 0xC5388288
CreateKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	hKey: 0xC53882B4
SetValueEx	HKLM\Software\Description\Microsoft\Rpc\UuidPersistentDat...	SUCCESS	0x414
SetValueEx	HKLM\Software\Description\Microsoft\Rpc\UuidPersistentDat...	SUCCESS	C0 2B 65 AB C4 6E
CreateKey	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settings	SUCCESS	hKey: 0xC56575B8
SetValueEx	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settin...	SUCCESS	"686"
CreateKey	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settings	SUCCESS	hKey: 0xC56575B8
SetValueEx	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settin...	SUCCESS	"686"
CreateKey	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settings	SUCCESS	hKey: 0xC56575B8
SetValueEx	HKCU\Software\VB and VBA Program Settings\TalkToMe\Settin...	SUCCESS	"492"
CreateKey	HKCU\Software\VB and VBA Program Settings\101\0	SUCCESS	hKey: 0xC551835C
SetValueEx	HKCU\Software\VB and VBA Program Settings\101\0\Windata	SUCCESS	"3"

图 5 RegMon 对 TalkToMe 监视的部分结果

CURRENT-USER \ Software \ VB and VBA Program Settings \ 101 \ 0]键下串值"Windata"存放着已使用次数，因此，每当提示到期注册时改回"Windata"键值为 0，"TalkToMe"即可继续使用。

4 RegMon 使用注意点

RegMon 对所监视过程的文件名称有特殊要求，文件名必须以英文字母开头，可包含汉字字符，总的字符长度不能大于 8 (一个汉字长度为 2)。所以，如果过程的名称不符和上面的规定，用户可自行修改名称，使其符合上述规定，以便顺利进行跟踪、监视。

参考文献

1 http://srana.cjb.net，Mystery Behind Windows Registry。