八、 演示版保护技术

演示版保护技术

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 序列号保护方式
- 警告窗口
- 时间限制
- 菜单功能限制
- KeyFile保护
- 网络验证
- 光盘检测
- 只运行一个实例

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

序列号（又称注册码）

- 从网上下载的共享软件（Shareware）
- 时间或功能上的限制
- 用户把自己的信息（例如用户名、电子邮件地址、机器特征码等）告诉软件公司
- 软件公司根据用户的信息，利用预先编写的一个用于计算注册码的程序（称为注册机，KeyGen ）算出一个序列号，并以电子邮件等形式将其发给用户
- 用户得到序列号后，在软件中输入注册信息和序列号。当注册信息验证通过后，软件就会取消各种限制，成为完全正式版本
- 软件每次启动时，会从磁盘文件或系统注册表中读取注册信息并对其进行检查
- 如果注册信息正确，则以完全正式版的模式运行，否则将作为有功能限制或时间限制的版本来运行
- 当软件推出新版本后，注册用户还可以向软件作者提供自己的注册信息，以获得版本升级服务

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **序列号保护的本质就是验证用户名和序列号之间的映射关系，越复杂的映射关系越难破解，根据映射关系的不同，程序检测序列号有以下方式：**
  - 序列号 = F (用户名)
  - 用户名 = F (序列号)
  - F1 (用户名) = F2 (序列号)
  - 特殊值 = F (用户名, 序列号)

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

序列号 = F (用户名)

如果把这个过程看作加密解密并进行密文对比的过程，那么用户名就是明文，而序列号则是密文，F函数就是加密算法了。这种保护方法虽然简单，但极为不安全，因为在程序运行的某一时刻，内存中一定会出现正确的序列号，也就是加密函数结束后。只要找到正确的时间点，甚至完全不用关心算法就可以完成验证

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

用户名 = F (序列号)

这里是把序列号作为明文，用户名作为密文了，这种方式通常需要F函数是一种对称加密算法的解密函数，而官方生成序列号时则使用加密函数对用户名进行加密得到的，这样就不会出现内存中有正确序列号的情况。这种保护方式的关键就是解密算法了，一旦得到解密算法就有机会逆向出加密算法，这样也就完成了验证

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

用户名 = F (序列号)

因为F^{-1}的实现代码是包含在软件中的，所以可以通过F^{-1}找出其逆变换，即函数F，从而得到正确的注册码或者写出注册机

给定一个用户名，利用穷举法找到一个满足式的序列号。这只适用于穷举难度不大的函数

给定一个序列号，利用变换得出一个用户名，从而得到一个正确的用户名/序列号对

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

F1 (用户名) = F2 (序列号)

这种方式是上一种的扩展，它相当于多套了几层加密而已

序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

特殊值 = F (用户名, 序列号)

这种保护方式的数学原理就比较复杂了，但保护效果相比前几种有了很大提升。不过在设计上有难度，并且可能出现用户名与序列号映射不唯一的情况

攻击序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **定位判断序列号的代码段**
- **通过跟踪输入注册码之后的判断找到注册码**
  - 通常用户会在一个编辑框中输入注册码，软件需要调用一些标准的API将用户输入的注册码字符串复制到自己的缓冲区中。常用的API包括GetWindowTextA（W）、GetDlgItemTextA(W)、GetDlgItemInt等
  - 程序完成对注册码的判断流程后，一般会显示一个对话框，告诉用户注册码是否正确。MessageBoxA(W)、MessageBoxExA(W)、ShowWindow、MessageBoxIndirectA(W)、CreateDialogParamA(W)、CreateDialog IndirectParamA(W)、DialogBoxParamA(W)、DialogBoxIndirectParamA(W)等 API 经常用于显示对话框

攻击序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

跟踪程序启动时对注册码的判断过程

- 根据序列号存放位置的不同，可以使用不同的API断点
- 如果序列号存放在注册表中，可以使用RegQueryValueExA(W)函数；
- 如果序列号存放在INI文件中，可以使用GetPrivateProfileStringA(W)、GetPrivateProfileIntA(W), GetProfileIntA(W)、GetProfileStringA(W)等函数
- 如果序列号存放在一般的文件中，可以使用CreateFileA(W)_lopen0等函数

攻击序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

利用消息断点

- 许多序列号保护软件都有一个按钮，当按下和释放鼠标时，将发送WM_LBUTTONDOWN(0201h) 和WM_LBUTTONUP (0202h)消息。因此，用这个消息下断点很容易就能找到按钮的事件代码

利用提示信息

- 目前大多数软件在设计时采用了人机对话的方式。所谓人机对话，即软件在执行一段程序之后会显示一串提示信息，以反映该段程序运行后的状态。例如，在TraceMe实例中输入假序列号，会显示“序列号错误，再来一次”
- 可以用OllyDbg、IDA等反汇编工具查找相应的字符串，定位到相关代码处

攻击序列号保护方式

字符串比较形式

- 寄存器直接比较

```
mov  eax [  ]     ;eax 或 ebx 中存放的是直接比较的两个数，一般是十六进制数
mov  ebx [  ]     ;同上
cmp  eax,ebx      ;直接比较两个寄存器
jz(jnz)  xxxx
```

- 函数比较a

```
mov  eax [  ]     ;比较数字直接放在 eax 中，一般是十六进制数，也可能是地址
mov  ebx [  ]     ;同上
call xxxxxxxx     ;用于比较功能的函数，可以是 API 函数，也可以是程序作者自己编写的比较函数
test eax eax
jz(jnz)
```

```
    cmp xxx,xxx
    jz Lable
    xor eax, eax      ;将 eax 清零
Lable: pop edi
    pop esi
    pop ebp
    ret               ;函数返回
```

攻击序列号保护方式

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

❖ 字符串比较形式

- 函数比较b

```
push xxxx          ;参数 1，可以是地址，也可以是寄存器
push xxxx          ;参数 2
call xxxxxxxx      ;用于比较功能的函数，可以是 API 函数，也可以是程序作者自己编写的比较函数
test eax eax
jz(jnz)
```

- 串比较

```
lea edi [  ]       ;edi 指向字符串 a
lea esi [  ]       ;esi 指向字符串 b
repz cmpsd         ;比较字符串 a 和 b
jz(jnz)
```

攻击序列号保护方式

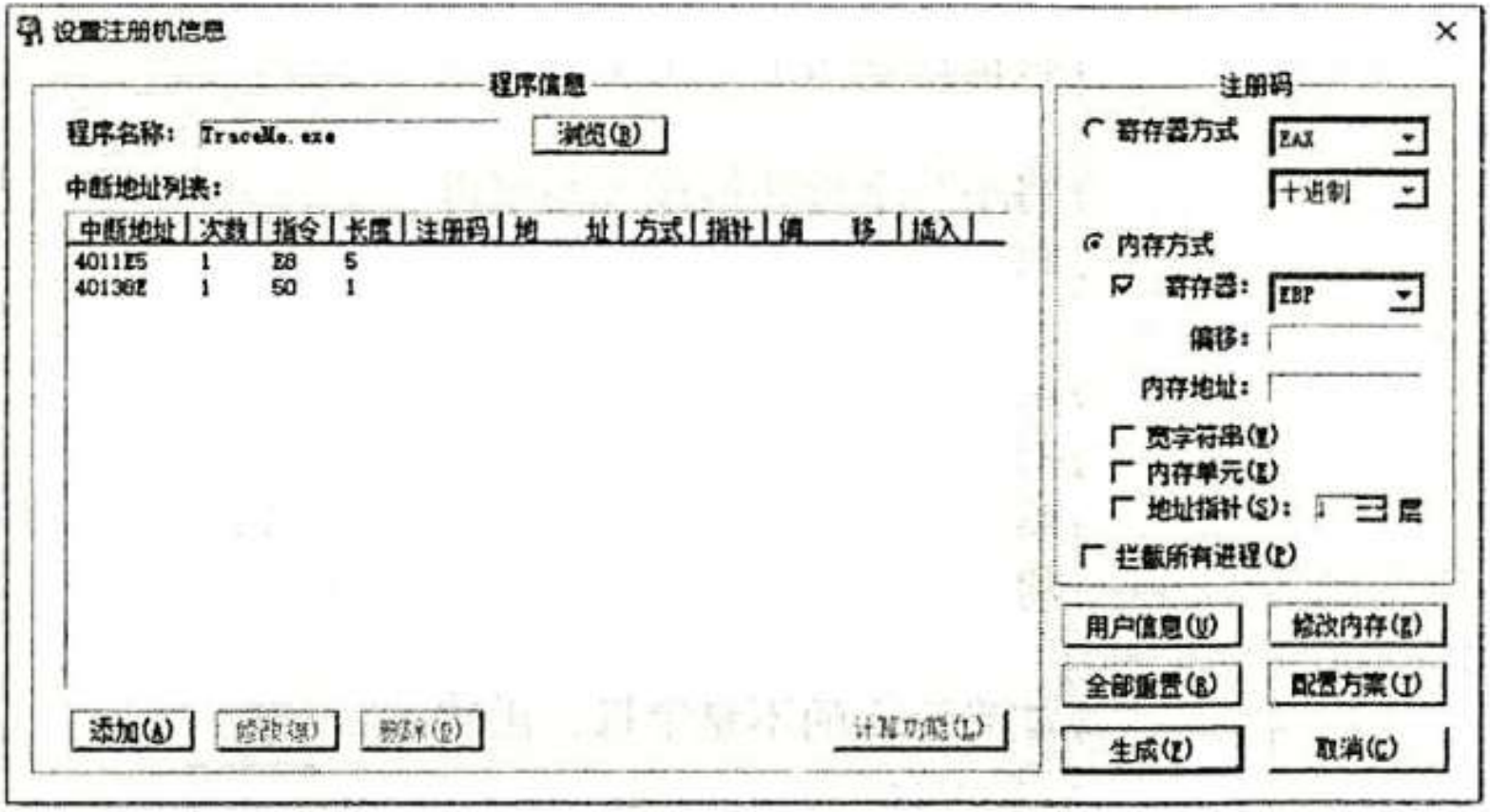
哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

❖制作注册机（明码比较）

```
004011E3   52           push    edx
004011E4   50           push    eax
004011E5   E8 56010000  call    00401340    ;进入子程序（设置第 1 次中断的地址）
{
     ......
     0040138D   55              push    ebp   ;第 2 次中断的地址（用 d ebp 命令查看真序列号）
     0040138E   50              push    eax
     0040138F   FF15 04404000   call    [<&KERNEL32.lstrcmpA>]
}
```

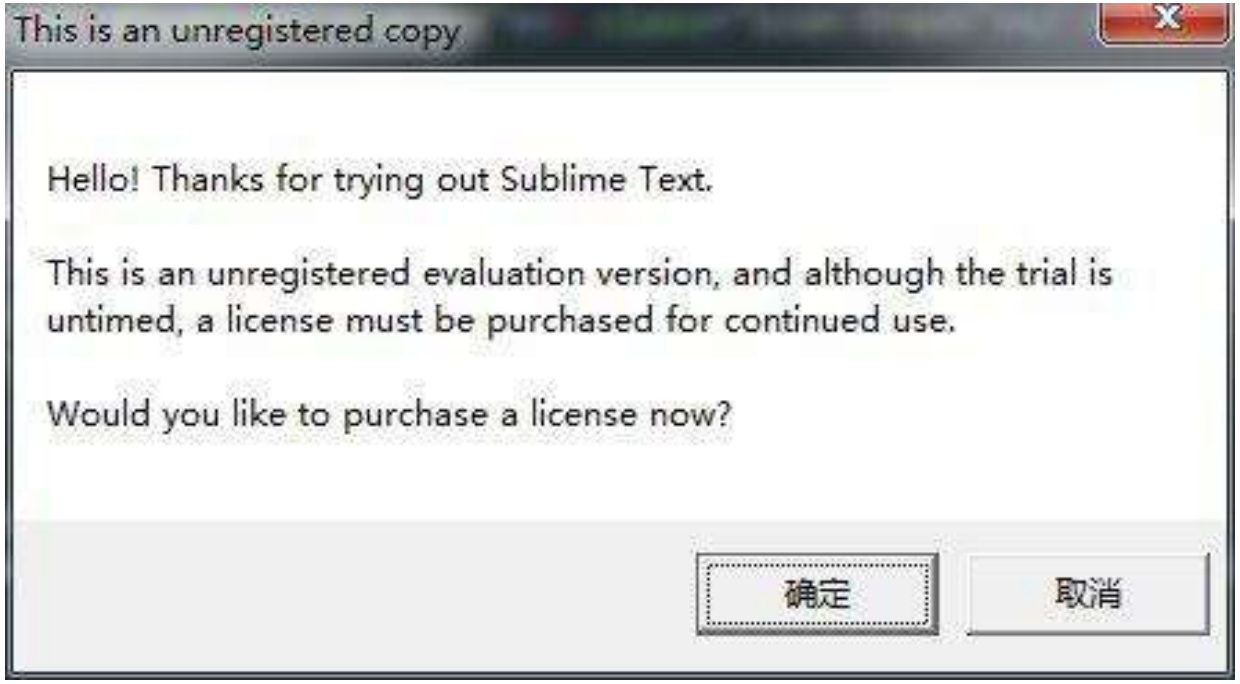
攻击序列号保护方式

- 制作注册机（明码比较）



警告窗口(Nag)


Sublime Text


This is an unregistered copy
Hello! Thanks for trying out Sublime Text.
This is an unregistered evaluation version, and although the trial is untimed, a license must be purchased for continued use.
Would you like to purchase a license now?
确定
取消

警告窗口(Nag)

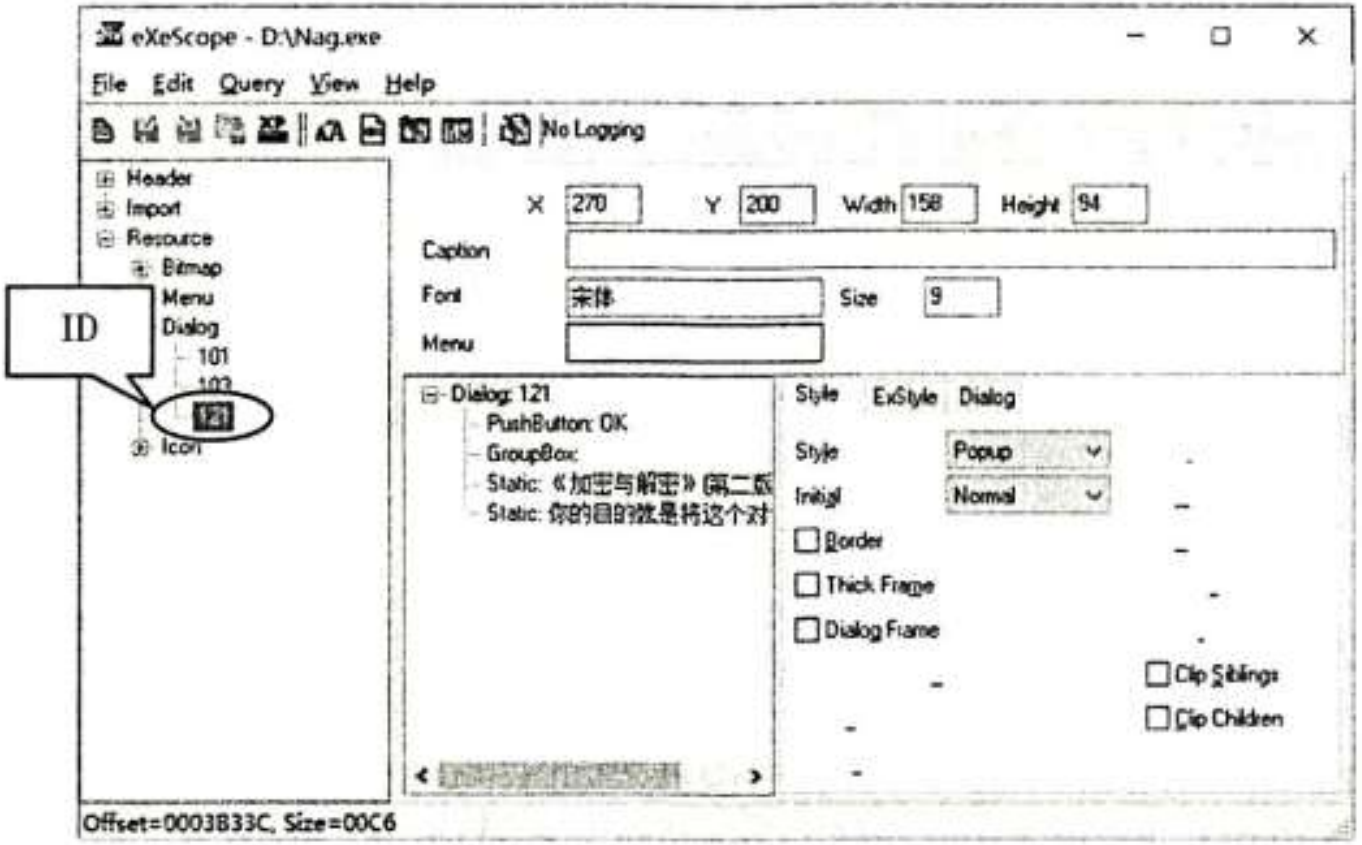
哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **修改程序的资源**
  - 透明化
  - 不可见
- **静态分析**
  - MessageBoxA(w)，MessageBoxExA(w)，DialogBoxParamA(w)，ShowWindow，CreateWindowExA(w)
- **动态分析**

警告窗口(Nag)

哈爾濱工業大學 HARBIN INSTITUTE OF TECHNOLOGY

- 修改程序的资源



警告窗口(Nag)


```
:0040104D    mov eax, dword ptr [esp+04]
:00401051    push 00000000                    ;初始化值
:00401053    push 004010C4                    ;对话框处理函数指针，指向一段子程序
:00401058    push 00000000                    ;父窗口句柄
:0040105A    push 00000079                    ;对话框 ID 为 DialogID_0079
:0040105C    push eax                         ;应用程序实例句柄，即 Nag.exe 的基地址
:0040105D    mov dword ptr [0040119C], eax
* Reference To: USER32.DialogBoxParamA, Ord:0093h
:00401062    Call dword ptr [00401010]        ;显示 Nag 对话框
:00401068    xor eax, eax
:0040106A    ret 0010
```

```
int DialogBoxParam(
    HINSTANCE hInstance,                      //应用程序实例句柄
    LPCTSTR lpTemplateName,                   //对话框 ID
    HWND hWndParent,                          //父窗口句柄
    DLGPROC lpDialogFunc,                     //对话框处理函数指针
    LPARAM dwInitParam                        //初始化值
);
```

警告窗口(Nag)

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
004010C4   mov    eax, dword ptr [esp+8]
004010C8   sub    eax, 110                  ;Switch (cases 110..111)
004010CD   je     short 00401103
004010CF   dec    eax
004010D0   jnz    short 004010FF
004010D2   mov    eax, dword ptr [esp+C]  ;Case 111 of switch 004010C8
004010D6   dec    eax
004010D7   jnz    short 004010FF
004010D9   push   0
004010DB   push   dword ptr [esp+8]
004010DF   call   [<&USER32.EndDialog>]   ;关闭对话框
004010E5   push   0                       ;初始化值
004010E7   push   00401109                ;主对话框处理函数指针
004010EC   push   0                       ;父窗口句柄
004010EE   push   65                      ;主对话框 ID 为 DialogID_0065
004010F0   push   0
004010F2   call   [<&KERNEL32.GetModuleHandleA>]
004010F8   push   eax
004010F9   call  [<&USER32.DialogBoxParamA>]
```

警告窗口(Nag)

- 跳过警告窗口代码。将"00401051 push 00000000"改成 “00401051 jmp 4010E5” 。修改时， 在OllyDbg里输入正确的代码。
- 将两个DialogBoxParam函数的参数对调。DialogBoxParam函数有两个参数很重要，一个是主 对话框处理函数指针，另一个是对话框IDO这种方法的思路是将主窗口的这两个参数放到 警告窗口的DialogBoxParam函数上。修改代码如下。

警告窗口(Nag)

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
:00401051     push 00000000
:00401053     push 00401109                    ;将此处指向主窗口的子处理程序
:00401058     push 00000000
:0040105A     push 00000065                    ;指向主对话框的 ID DialogID_0065
:0040105C     push eax
:0040105D     mov dword ptr [0040119C], eax
* Reference To: USER32.DialogBoxParamA, Ord:0093h
:00401062     Call dword ptr [00401010]        ;该函数会调用主对话框窗口
:00401068     xor eax, eax
:0040106A     ret 0010                         ;主对话框关闭后将从这里退出
```

时间限制

- 计时器，限制每次运行时长，比如运行10分钟或者20分钟
- 时间限制，比如30天

时间限制 – 计时器

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
UINT_PTR SetTimer(
HWND hWnd, // 窗口句柄
UINT_PTR nIDEvent, // 定时器ID，多个定时器时，
                   //可以通过该ID判断是哪个定时器
UINT nElapse, // 时间间隔,单位为毫秒
TIMERPROC lpTimerFunc // 回调函数
);
```

时间限制 – 计时器

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
MMRESULT timeSetEvent（ UINT uDelay,
   UINT uResolution,
   LPTIMECALLBACK lpTimeProc,
   WORD dwUser,
   UINT fuEvent ）
```

uDelay：以毫秒指定事件的周期。
Uresolution：以毫秒指定延时的精度，数值越小定时器事件分辨率越高。缺省值为1ms。
LpTimeProc：指向一个回调函数。
DwUser：存放用户提供的回调数据。
FuEvent：指定定时器事件类型

时间限制 – 计时器

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **GetTickCount( )函数**
  - 返回从操作系统启动到当前所经过的毫秒数，常常用来判断某个方法执行的时间，其函数原型是DWORD GetTickCount(void)，返回值以32位的双字类型DWORD存储，因此可以存储的最大值是(2^32-1) ms约为49.71天
- **timeGetTime( )函数**
  - 函数以毫秒计的系统时间。该时间为从系统开启算起所经过的时间。

时间限制 – 时间限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **设计方案一**
  - 记录安装时间或者第一次运行时间
  - 每次运行时获取时间与之前的比较
- **设计方案二**
  - 记录安装时间
  - 记录最近一次运行时间

时间限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
004010C2    mov     esi, dword ptr [esp+8]
004010C6    push    0                           ;/Timerproc = NULL
004010C8    push    3E8                         ;|Timeout = 1000. ms
004010CD    push    1                           ;|TimerID = 1
004010CF    push    esi                         ;|hWnd
004010D0    call     [<&USER32.SetTimer>]       ;\SetTimer
004010D6    mov     eax, dword ptr [403004]
```

```
00401175    cmp     eax, 113                    ;Case 113 (WM_TIMER)
0040117A    jnz     short 00401148
0040117C    mov     eax, dword ptr [403008]     ;[403008]处存放的是 i（定义了全局变量）
00401181    cmp     eax, 13                     ;超过 20 秒（“13”是十六进制数）
00401184    jg      short 00401137              ;超时就跳走退出，直接 NOP
00401186    inc     eax                         ;i++
00401187    lea     ecx, dword ptr [esp+C]
0040118B    push    eax
0040118C    push    00403000
00401191    push    ecx
00401192    mov     dword ptr [403008], eax     ;将 i 放进[403008]
```

菜单功能限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- **试用版和正式版是两个完全不同的版本**
  - 试用版中没有被禁止功能的代码
  - 正式版需要购买下载
- **试用版和正式版是同一文件**
  - 禁止用户使用某些功能
  - 被禁止的功能代码就在程序之中
- **显然，第一种方式要好**

菜单功能限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
BOOL EnableMenuItem(
      HMENU hMenu, // handle to menu
      UINT uIDEnableItem, // menu item to enable, disable, or gray
      UINT wEnable // menu item flags
    );
```

hMenu，菜单句柄
uIDEnableItem，欲允许或禁止的一个菜单条目的标识符
wEnable，控制标志，包括
MF_DISABLED (2h)使菜单项无效，以便它不能被选择，但不变灰
MF_ENABLED (0h)使菜单项有效，以便它能够被选择，并可从变灰的状态中恢复出来
MF_GRAYED (1h)使菜单项无效，以便它不能被选择并同时变灰

菜单功能限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
BOOL EnableWindow（HWND hWnd,
BOOL bEnable）；
```

hWnd:被允许/禁止的窗口句柄

bEnable:定义窗口是被允许，还是被禁止

若该参数为TRUE，则窗口被允许
若该参数为FALSE，则窗口被禁止

菜单功能限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
:004011E3  6A01                 push 00000001                ;控制标志
:004011E5 68459C0000            push 00009C45                ;标识符（Menu 的 ID=40005）
:004011EA 50                    push eax                     ;菜单句柄
:004011EB FF1524204000          Call USER32.EnableMenuItem
```

KeyFile保护

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- KeyFile是一种利用文件来注册软件的保护方式。其内容是一些加密或未加密的数据，其中可能有用户名、注册码等信息，文件格式则由软件作者自己定义
- 在实现这种保护的时候，建议采用稍大一些的文件作为KeyFile（一般在几KB左右），其中可以加入一些垃圾信息以干扰解密者
- 对注册文件的合法性检查可以分成几部分，分散在软件的不同模块中进行判断
- 注册文件内的数据处理也要尽可能采用复杂的运算，而不要使用简单的异或运算
- 可以让注册文件中的部分数据和软件中的关键代码或数据发生关系，使软件无法被暴力破解

KeyFile保护

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- KeyFile是一个文件
- 与Windows文件操作有关的API函数都可作为动态跟踪破解的断点

API函数	用于注册文件时的主要作用
FindFirstFileA	确定注册文件是否存在
CreateFileAx_lopen	确定文件是否存在；打开文件以获得其句柄
GetFileSize、GetFileSizeEx	获得注册文件的大小
GetFileAttributesExA、GetFileAttributesA	获得注册文件的属性
SetFilePointer、SetFilePointerEx	移动文件指针
ReadFile	读取文件内容

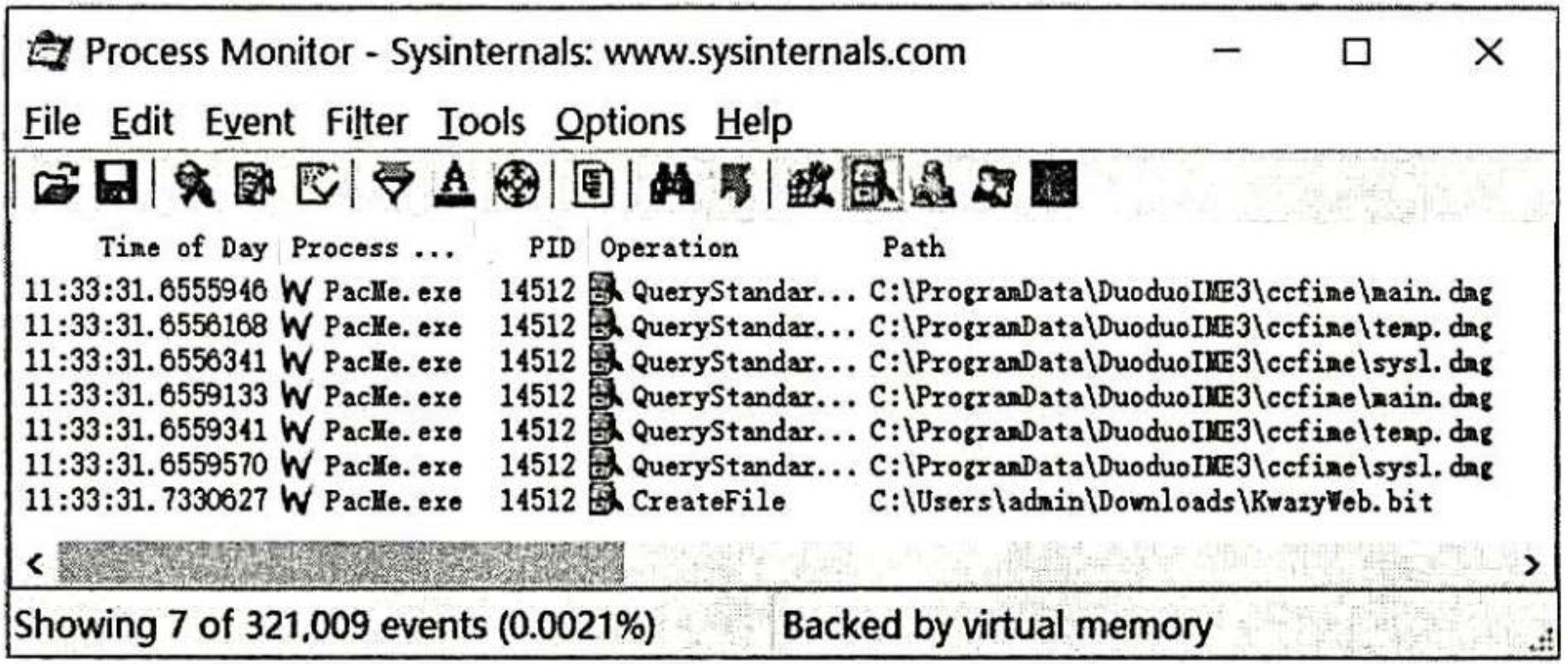
KeyFile保护

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

拆解KeyFile保护

- 用工具监视软件(如Process Monitor)对文件的操作，以找到KeyFile的文件名
- 伪造一个KeyFile文件。用十六进制工具编辑和修改KeyFile
- 在调试器里用CreateFileA函数设断，查看其打开的文件名指针，并记下返回的句柄
- 用ReadFile函数设断，分析传递给ReadFile函数的文件句柄和缓冲区地址。文件句柄一般和第三步返回的相同（若不同，则说明读取的不是该KeyFile。在这里也可以使用条件断点）。缓冲区地址是非常重要的，因为读取的重要数据就放在这里。对缓冲区中存放的字节设内存断点，监视读取的KeyFile的内容

KeyFile保护


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process ... PID Operation Path
11:33:31.6555946 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\main.dmg
11:33:31.6556168 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\temp.dmg
11:33:31.6556341 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\sysl.dmg
11:33:31.6559133 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\main.dmg
11:33:31.6559341 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\temp.dmg
11:33:31.6559570 PacMe.exe 14512 QueryStandar... C:\ProgramData\DuoduoIME3\ccfime\sysl.dmg
11:33:31.7330627 PacMe.exe 14512 CreateFile C:\Users\admin\Downloads\KwazyWeb.bit
Showing 7 of 321,009 events (0.0021%)
Backed by virtual memory

KeyFile保护

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

```
004016D8    push    edx                             ;|FileName => "KwazyWeb.bit"
004016D9    call    <jmp.&KERNEL32.CreateFileA>     ;\CreateFileA
004016DE    cmp     eax, -1
004016E1    je      short 00401747
```

```
****************
C*......*...****
.*.****...*....*
.*..**********.*
..*....*...*...*
*.****.*.*...***
*.*....*.*******
..*.***..*.....*
.*..***.**.***.*
...****....*X..*
****************
```

↓ ↓ ↓ →	↓ ↓ ↓ ←	↓ ↓ → →	↑ → ↑ ↑	→ → → ↑	↑ ← ← ←	↑ ← ↑ ↑	→ → → →	→ ↓ → →
2 2 2 1	2 2 2 3	2 2 1 1	0 1 0 0	1 1 1 0	0 3 3 3	0 3 0 0	1 1 1 1	1 2 1 1
↑ → → ↓	→ → → ↓	↓ ← ← ↓	← ← ↑ ←	← ↓ ↓ ↓	← ↓ ↓ →	→ → ↑ ↑	→ → → →	↓ ↓ ← ←
0 1 1 2	1 1 1 2	2 3 3 2	3 3 0 3	3 2 2 2	3 2 2 1	1 1 0 0	1 1 1 1	2 2 3 3

在此以用户名“pediy”推出 KeyFile。“pediy”的十六进制数是“70 65 64 69 79”。KeyFile 由 3 部分组成，如图 5.10 所示。计算步骤如下。

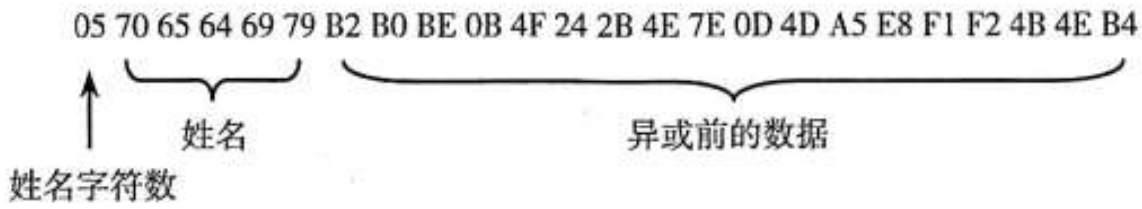


图 5.10　PacMe 的 KeyFile 内容

① 计算“pediy”字符的和，70h+65h+64h+69h+79h=21Bh，取低 8 位 1Bh。

② 用 1Bh 依次与“A9 AB A5 10 54 3F 30 55 65 16 56 BE F3 EA E9 50 55 AF”进行异或运算，结果是“B2 B0 BE 0B 4F 24 2B 4E 7E 0D 4D A5 E8 F1 F2 4B 4E B4”。

网络验证

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 网络验证是目前很流行的一种保护技术
- 优点是可以将一些关键数据放到服务器上，软件必须从服务器中取得这些数据才能正确运行
- 拆解网络验证的思路是拦截服务器返回的数据包，分析程序是如何处理数据包的

网络验证

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 常用的数据传送函数有send()和recv()两个Socket函数
- 微软的扩展函数WSASend()和WSARecv()

```
int send(
    SOCKET s,                   //套接字描述符
    const char FAR *buf,        //缓冲区
    int len,                    //实际要发送数据的字节数
    int flags                   //附加标志，一般为 0
);
```

```
int recv(
    SOCKET s,                   //套接字描述符
    char FAR *buf,              //缓冲区
    int len,                    //缓冲区 buf 的长度
    int flags                   //附加标志，一般为 0
);
```

网络验证

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 如果网络验证的数据包内容固定，可以将数据包抓取，写一个本地服务端模来拟服务器

- 如果验证的数据包内容不固定，则必须分析其结构，找出相应的算法

```
00401625    push   0                                ;/Flags = 0
00401627    mov    eax, dword ptr [ebp-23C]          ;|
0040162D    push   eax                               ;|DataSize
0040162E    lea    ecx, dword ptr [ebp-354]          ;|
00401634    push   ecx                               ;|Data
00401635    mov    edx, dword ptr [ebp-200]          ;|
0040163B    push   edx                               ;|Socket
0040163C    call   <jmp.&WS2_32.send>>               ;\send
```

nameLength	keyLength	ran_K	name	key

```
00401655    push   0                                ;/Flags=0
00401657    push   1F4                              ;|BufSize=1F4(500.)
0040165C    lea    eax, dword ptr [ebp-1F4]         ;|
00401662    push   eax                              ;|Buffer
00401663    mov    ecx, dword ptr [ebp-200]         ;|
00401669    push   ecx                              ;|Socket
0040166A    call   <jmp.&WS2_32.recv>               ;\recv
```

网络验证

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 解除网络验证
  - 编写一个服务端，模拟服务器来接收和发送数据
  - 如果软件是用域名登录服务器的，可以修改hosts文件，使域名指向本地（127.0.0.1 ）
  - 如果软件是直接用IP地址连接服务器的，可以用ineladdr或connect等设断，将IP地址修改为本地IP地址，或者使用代理软件将IP地址指向本地
  - 除了编写服务端，也可直接修改客户端程序，将封包中的数据整合进去

```
0040163C     call    0040FAA8        ;此处原是 send，现在跳转到 0040FAA8h 这个空白地址处
{
     0040FAA8     push    eax                          ;保存 eax
     0040FAA9     mov     al,byte ptr [ebp-254]        ;将随机数 ran_K 读到 al 中
     0040FAAF     mov     byte ptr [41AE76], al        ;将 ran_K 写到[41AE76]处
     0040FAB4     pop     eax                          ;恢复 eax
     0040FAB5     retn    10                           ;原 send()函数有 4 个参数入栈，现恢复
}
```

```
00401655     jmp     short 004016BE                   ;跳过 recv()函数并解密代码
00401657     push    1F4                              ;|BufSize = 1F4 (500.)
0040165C     lea     eax, dword ptr [ebp-1F4]         ;|
00401662     push    eax                              ;|Buffer
00401663     mov     ecx, dword ptr [ebp-200]         ;|
00401669     push    ecx                              ;|Socket
0040166A     call    <jmp.&WS2_32.#16>                ;\recv
0040166F     mov     dword ptr [ebp-28C], eax
00401675     mov     dword ptr [ebp-238], 0
0040167F     jmp     short 00401690
00401681     /mov     edx, dword ptr [ebp-238         ;以下代码用来解密
00401687     |add     edx, 1
0040168A     |mov     dword ptr [ebp-238], edx
00401690      mov     eax, dword ptr [ebp-238]
00401696     |cmp     eax, dword ptr [ebp-28C]
0040169C     |jge     short 004016BE
0040169E     |mov     ecx, dword ptr [ebp-238]
```

光盘检测

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

- 一些采用光盘形式发行的应用软件和游戏，在使用时需要检查光盘是否插在光驱中

- 如果没有则拒绝运行。这是为了防止用户将软件或游戏的一份正版拷贝安装在多台机器上且同时使用，其思路与DOS时代的钥匙盘保护类似，虽然能在一定程度上防止非法拷贝，但也给正版用户带来了一些麻烦，一旦光盘被划伤，用户就无法使用软件了

光盘检测

- 最简单也最常见的光盘检测就是程序在启动时判断光驱中的光盘里是否存在特定的文件
- 如果不存在，则认为用户没有使用正版光盘，拒绝运行。在程序运行过程中，一般不再检查光盘是否在光驱中
- 在Windows下的具体实现一般是：
  - 先用GetLogicalDriveStrings()或GetLogicalDrives()函数得到系统中安装的所有驱动器的列表
  - 然后用GetDriveType()函数检查每个驱动器
  - 如果是光驱，则用 CreateFile()或FindFirstFile()函数检查特定的文件是否存在，甚至可能进一步检查文件的属性、大小、内容等

光盘检测

- 解密者只要利用上述函数设置断点，找到程序启动时检查光驱的地方，然后修改判断指令，就可以跳过光盘检测
- 增强类型就是把程序运行时需要的关键数据放在光盘中。这样，即使解密者能够强行跳过程序启动时的检查，但由于没有使用正版光盘，也就没有程序运行时所需要的关键数据，程序自然会崩溃，从而在一定程度上起到了防破解的作用
- 简单地利用刻录和复制工具将光盘复制多份，也可以采用虚拟光驱程序来模拟正版光盘
- 常用的虚拟光驱程序有Virtual CD、Virtual Drive、Daemon Tools等

只运行1个实例

- 查找窗口法
  - 用FindWindowA、GetWindowText函数查找具有相同窗口类名和标题的窗口

```
HWND FindWindowA(W)(
    LPCTSTR lpClassName,        //指向窗口类名
    LPCTSTR lpWindowName        //指向窗口文本
  );
```

```
TCHAR AppName[ ] = TEXT ("只运行1个实例") ;
hWnd=FindWindow(NULL, AppName);
if (hWnd ==0) 初始化程序
else 退出程序
```

只运行1个实例

- 使用互斥对象
  - 一般用CreateMutexA函数实现，它的作用是创建有名或者无名的互斥对象

```
HANDLE CreateMutexA(W) (
    LPSECURITY_ATTRIBUTES lpMutexAttributes,  //安全属性
    BOOL bInitialOwner,                       //指定互斥对象的初始身份
    LPCTSTR lpName                            //指向互斥对象名
      );
```

```
TCHAR AppName[] = TEXT ("只运行1个实例") ;
Mutex =CreateMutex(NULL,FALSE,AppName)
if GetLastError<>ERROR_ALREADY_EXISTS
   初始化                                     //如果不存在另一个实例
else
   ReleaseMutex(Mutex);
```

只运行1个实例

- 使用共享区块
  - 创建一个共享区块（**Section**)。该区块拥有读取、写入和共享保护属性，可以让多个实例共享同一内存块。将一个变量作为计数器放到该区块中，该应用程序的所有实例可以共享该变量，从而通过该变量得知有没有正在运行的实例

```
0040100C    push    0
0040100E    push    004020F4
00401013    call    <&USER32.FindWindowA>
00401018    or      eax, eax
0040101A    je      short 0040101D              ;判断点
```

常用断点设置技巧

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

类　别	函　数	类　别	函　数
字符串	hmemcpy（仅 Windows 9x）	注册表	RegCreateKeyA(W)
	GetDlgItemTextA(W)		RegDeleteKeyA(W)
	GetDlgItemInt		RegQueryValueA(W)
	GetWindowTextA(W)		RegCloseKey
	GetWindowWord		RegOpenKeyA(W)
文件访问	ReadFile	光驱相关	GetFileAttributesA(W)
	WriteFile		GetFileSize
	CreateFileA(W)		GetDriveType
	SetFilePointer		ReadFile
	GetSystemDirectory		CreateFileA(W)
INI 文件	GetPrivateProfileString	对话框	MessageBeep
	GetPrivateProfileInt		MessageBoxA(W)
	WritePrivateProfileString		MessageBoxExA(W)
	WritePrivateProfileInt		DialogBoxParamA(W)
时间相关	GetLocalTime		CreateWindowExA(W)
	GetFileTime		ShowWindow
	GetSystemTime		UpdateWindow