

Analyzing heavily protected P2P voice over IP software

G rard Wagener

October 18, 2007



Introduction

- ▶ Such software does not like dis-assemblers.
- ▶ And it does not like debuggers like soft-ice.
- ▶ Messages are encrypted, . . .
- ▶ Such software gathers hardware information ¹ i.e. bios scan and does not like virtual machines . . .
- ▶ Many such obscure rumors exists . . .
- ▶ We want to:
 - ▶ Check these statements.
 - ▶ Understand such clients.
 - ▶ We are presenting how internals of such software can be revealed.
- ▶ One example of p2p clients for voip is **Skype**.

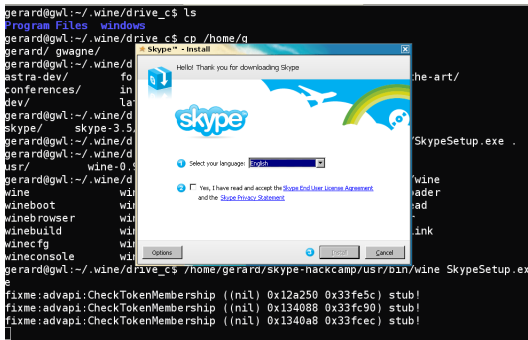
¹<http://www.pagetable.com/?p=27>

Analysis concept

- ▶ Analysis problems:
 - ▶ Soft-ice, gdb, objdump does not work.
 - ▶ Use **wine** to start the software.
 - ▶ If it works patch wine to discover internals ...
- ▶ Solution
 - ▶ Download voice over IP software.
 - ▶ Download wine source from <http://www.wine-hq.com>

Installation problems

- ▶ Software crashes during installation.
- ▶ Configure wine as Windows 98² → still crash.
- ▶ Solution: Use wine 0.9.22 (old version)



Ok it boots :-)



Analyzing debug messages of wine

- ▶ Looking at the executed function calls:
 - ▶ export WINEDEBUG=trace+relay
 - ▶ wine Skype.exe 2&>1 | tee relay.trace
- ▶ Examine network information
 - ▶ export WINEDEBUG=trace + winsock
 - ▶ wine Skyp.exe 2&>1 | tee winsock.trace
- ▶ Some observations:
 - ▶ Skype created 142 sockets!

Output

```
0009:Call kernel32.CreateFileW(0056abb8 L"\\.\  
NTICE",0,0,0,3,0,0) ret=0056ac17  
trace:winsock:WS_bind socket 0248, ptr 0x21e030 {  
family 2, address 127.0.0.1
```

Analyzing Skype with the tool fiw

Advantage

- ▶ Block execution.
- ▶ Inspect memory, disassemble, read or write ...

Example (Check if functions returns are checked)

```
gerard@gwl:~/dev/fiw$ ./startfiw.sh
fiw>start Skype.exe
Program started
RtlInitUnicodeString(bfefc738, 7ee9a0aa) pid: 17371 tid: 0009 ret:
: 7ee55458

fiw>
fiw>break name CreateFileW
Break point set
fiw>cont
fiw>CreateFileW(0056abfc, NUL", 00000000, 00000000, 00000000, 000
00003, 00000000) pid: 17371 tid: 0009 ret: 0056ac77

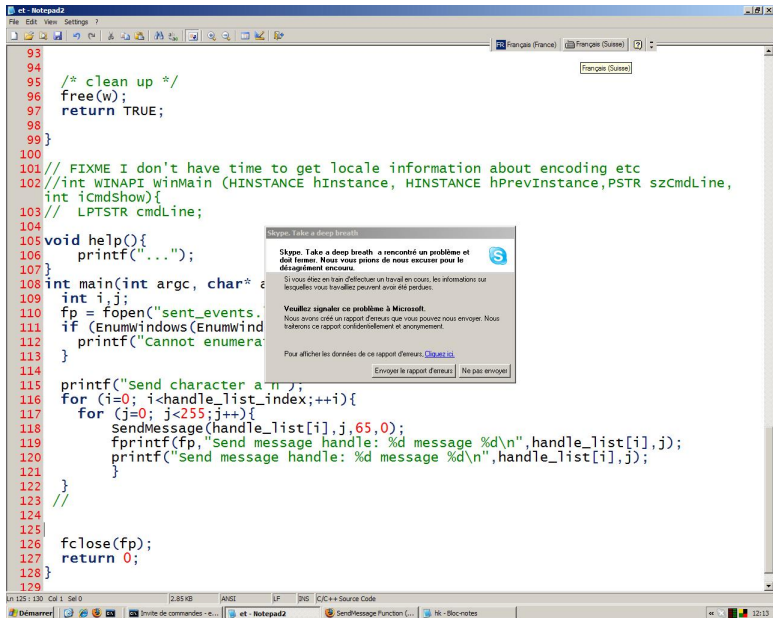
fiw>cont
fiw>CreateFileW(0056abb8, \\.\Ntice", 00000000, 00000000, 0000
0000, 00000003, 00000000) pid: 17371 tid: 0009 ret: 0056ac17

fiw>dasm 0056ac17 64
*** Disassemble address 56ac17 size 64
0056AC17 85C0          test eax,eax
0056AC19 760F          jna 0x56ac2a
0056AC1B 83F8FF       cmp eax,byte -0x1
0056AC1E 730A          jnc 0x56ac2a
0056AC20 B301          mov bl,0x1
```

Injecting data into the p2p software

- ▶ Via network.
- ▶ Via files, temp files, config files, ...
- ▶ Via windows events! (i.e. Skype API)

Having fun with Windows events ...



```
93
94
95 /* clean up */
96 free(w);
97 return TRUE;
98
99 }
100
101 // FIXME I don't have time to get locale information about encoding etc
102 //int WINAPI WinMain (HINSTANCE hInstance, HINSTANCE hPrevInstance, PSTR szCmdLine,
103 // LPTSTR cmdLine;
104
105 void help(){
106     printf("...");
107 }
108 int main(int argc, char* a
109     int i,j;
110     fp = fopen("sent_events.
111     if (EnumWindows(EnumWind
112         printf("Cannot enumera
113     }
114
115     printf("Send character a\n");
116     for (i=0; i<handle_list_index;++i){
117         for (j=0; j<255;j++){
118             SendMessage(handle_list[i],j,65,0);
119             printf(fp,"Send message handle: %d message %d\n",handle_list[i],j);
120             printf("Send message handle: %d message %d\n",handle_list[i],j);
121         }
122     }
123 //
124
125
126 fclose(fp);
127 return 0;
128 }
129
```

Skype. Take a deep breath

Skype. Take a deep breath a rencontré un problème et doit fermer. Nous vous prions de nous excuser pour le désagrément rencontré.

Si vous êtes en train d'effectuer un travail en cours, les informations sur lesquelles vous travaillez peuvent avoir été perdues.

Veillez signaler ce problème à Microsoft.
Nous avons créé un rapport d'erreurs que vous pouvez nous envoyer. Nous traiterons ce rapport confidentiellement et anonymement.

Pour afficher les données de ce rapport d'erreurs, [cliquez ici](#).

Envoyer le rapport d'erreurs | Ne pas envoyer

In 125 x 130 Col 1 Sel 0 2.85 KB ANSI LF JMS C/C++ Source Code

Démarrer | InVite de commandes - e... | et - Notepad2 | Send/Message Fonction (... | nk - Bloc-notes | 12:13

Having fun with Windows events ...

- ▶ How it works! (w32)
 - ▶ Enumerate all windows on Desktop EnumWindows.
 - ▶ Map them with processes GetWindowThreadProcessId.
 - ▶ Opens the processes OpenProcess.
 - ▶ Get the process **name** GetModuleBaseName.
 - ▶ **If** our client is found examine handles.
 - ▶ Get windows class info & name.

Ready to start **fuzzing** the handles.

Having fun with Windows events ...

Discovering the handles of the application that should be analyzed.

```
C:\WINDOWS\system32\cmd.exe
C:\>net>sp.exe
C:\>net>sp.exe
skype handle: 2491056 class name: tSkMainForm.UnicodeClass
Non window handle 2491056
skype handle: 1246070 class name: TActions.UnicodeClass
Non window handle 1246070
skype handle: 4653674 class name: TApplication
Non window handle 4653674
skype handle: 2949976 class name: ComboBox
classinfo: class name X\-
WNDPROC: 7e38c98e
skype handle: 1442664 class name: TPUtilWindow
Non window handle 1442664
skype handle: 1966940 class name: TPUtilWindow
Non window handle 1966940
skype handle: 2753342 class name: TPUtilWindow
Non window handle 2753342
skype handle: 1901356 class name: TPUtilWindow
Non window handle 1901356
skype handle: 1442634 class name: TPUtilWindow
Non window handle 1442634
skype handle: 1442594 class name: TPUtilWindow
Non window handle 1442594
skype handle: 1377150 class name: TPUtilWindow
Non window handle 1377150
skype handle: 1311666 class name: TPUtilWindow
Non window handle 1311666
skype handle: 2163538 class name: TPUtilWindow
Non window handle 2163538
skype handle: 1573830 class name: TChatManager.UnicodeClass
Non window handle 1573830
skype handle: 1377118 class name: TTrayIconManager.UnicodeClass
Non window handle 1377118
skype handle: 1246066 class name: TPUtilWindow
Non window handle 1246066
skype handle: 2294644 class name: TPUtilWindow
Non window handle 2294644
skype handle: 1246024 class name: TPUtilWindow
Non window handle 1246024
skype handle: 1311538 class name: TPUtilWindow
Non window handle 1311538
skype handle: 1573732 class name: TPUtilWindow
Non window handle 1573732
skype handle: 983906 class name: TPUtilWindow
```

Having fun with Windows events ...

Sending the events ...

```
C:\WINDOWS\system32\cmd.exe - et.exe
skype handle: 66468 class name: TPUtilWindow
Non window handle 66468
skype handle: 132000 class name: TPUtilWindow
Non window handle 132000
skype handle: 66462 class name: TPUtilWindow
Non window handle 66462
skype handle: 66458 class name: SkypeWindowClass2
Non window handle 66458
skype handle: 66456 class name: TPUtilWindow
Non window handle 66456
skype handle: 66454 class name: TSkyLibEx.UnicodeClass
Non window handle 66454
skype handle: 66452 class name: TPUtilWindow
Non window handle 66452
skype handle: 66450 class name: TPUtilWindow
Non window handle 66450
skype handle: 66448 class name: OleDdeWndClass
Non window handle 66448
skype handle: 66446 class name: TPUtilWindow
Non window handle 66446
skype handle: 131974 class name: TPUtilWindow
Non window handle 131974
skype handle: 66510 class name: MSCTFIME UI
Non window handle 66510
skype handle: 131976 class name: IME
classinfo: class name IME
WNDPROC: 7e3bc6f6

C:\et>notepad et.c

C:\et>c:\notepad2\notepad2 et.c

C:\et>gcc -o et.exe et.c -lpsapi

C:\et>et.exe
Send message handle: 66480 message 20
Send message handle: 66480 message 21
Send message handle: 66480 message 22
Send message handle: 66480 message 23
Send message handle: 66480 message 24
Send message handle: 66480 message 25
Send message handle: 66480 message 26
Send message handle: 66480 message 27
Send message handle: 66480 message 28
Send message handle: 66480 message 29
```