Software Protection - an assembly programmer's view

B92901051 何熙明
B92901016 翁秉義

There are many types of software protection:

Shareware:

* Registration number
  - A special reg. number for a name

* Keyfile
  - With a keyfile, shareware version will become full version

* Time limit
  - Ex: unregistered version won't run after 30 days

* Nag screen
  - Popup an annoying window frequently

Commercial software:

* Serial number
  - Ask when install

* Game CD protection
  - Ex: SecuROM, SafeDisc, StarForce..

* Online check
  - Ex: Game server CD-key check

* Time or feature limited trial versions
  - Ex: Vbox, SalesAgent..

* License files (usually used by *very expensive* softwares)
  - Ex: FlexLm

* Dongles (usually used by *very expensive* softwares)
  - Ex: AutoCAD, 3D Studio Max..

- In this project we focus on "registration number" protection.

General scheme:

```
Name = GetDlgItemText(NameEditBox);
InputRegNumber = GetDlgItemText(RegNumber);

RegNumber = f(Name);

if (RegNumber = InputRegNumber)
      // Registration success!
else
      // Registration failed..
```

Registration number protection is not safe. In fact, for many cases it's really weak.

How to crack it?

* Patch
    - directly patch the instructions in .exe file

        Ex:

```
...
...

mov     esi, offset RegNumber
mov     edi, offset InputRegNumber
mov     ecx, length
repz    cmpsb
jz      Reg_success
call    Reg_failed
ret

Reg_success:

...
...
```

    - We can modify "**jz**" to "**jmp**"!

* Don't patch
    - Dump RegNumber in debugger (and write it down :Q)
    - Don't work when RegNumber is encrypted

* Write KeyGen
    - RegNumber = f(Name);
    - Try to figure out function f and use it in a small program
    - We can simply type any name and get registration number!

We'll show how to defeat:

* UEStudio '05 v5.00b+1 (http://www.ultraedit.com/)
* PowerMap3D (PaPaGO!) v7.5 (http://www.papago.com.tw/)

Goal: Write working KeyGens for them.

Steps:

- Use OllyDbg to load .exe
- Trace
- Copy disassembled code
- Fix references. In this project, we use FASM (http://flatassembler.net/)

Conclusion:

** About assembly language:*

Software protection is very closely linked to assembly language.

If you want to protect your software, you *MUST* know assembly language.

Programmers with little or no assembly language knowledge *CANNOT* protect their work.

- We have seen one that the programmer writes the time limit straightly into the Windows registry file. How weak!

** About software protection:*

In general, there's no lock which is not unlockable.

There *MUST* be a key, which can *ABSOLUTELY* be found.

However, if finding out the key takes a very long time, it is equivalent to safety.

In this project, we discovered that using only registration number is *NOT* safe.

More protecting methods must be used to ensure safety.