
Subject: Re: Function Hooking

Posted by [Neijwiert](#) on Sun, 28 Dec 2014 17:58:22 GMT

[View Forum Message](#) <> [Reply to Message](#)

iRANian wrote on Sun, 28 December 2014 07:05What you can also do is place a JMP at the very start of the original function to your own hook. Then when you want to call the original function you re-create the first 5 bytes you overwrote in assembly then just jmp 5 bytes into the original function.

function:

```
push ebp ; byte 1
push edi ; byte 2
push esi ; byte 3
push ebx ; byte 4
push ecx ; byte 5
push edx ; byte 6
```

Then after jumping hooking:

function:

```
jmp <hookfunc> ; byte 1-5
push edx ; byte 6
```

```
void HookFunc()
```

```
{
    blabla
}
```

```
void __declspec(naked)Call original func()
```

```
{
    __asm
    {
        push ebp ; byte 1
        push edi ; byte 2
        push esi ; byte 3
        push ebx ; byte 4
        push ecx ; byte 5
        jmp to byte 6; where 'push edx' is located
    }
}
```

That was exactly what I was trying to achieve in my first attempt. Yet it somehow didn't jump to the new function, If you toggle the spoilers in the first post you can see how I tried it.
