New reverse engineering technique using API hooking and sysenter hooking, and capturing of cash card access

NetAgent Co., Ltd.
http://www.netagent.co.jp

Kenji Aiko

What is API (function) hook?

- A technique in which you temporarily alter jmp command or call command when an application program calls a function (instruction code) in an external library (.dll or .so files,) to divert the process to an alternative function.

- There are libraries for API hook for Linux (UNIX) and Windows each.

The method of function intercepts

- An intercept that change the head address of functions (Detours).
- An intercept that change the IAT (Import Address Table) which is on the process.
- An intercept that replace DLL.
- Native API intercepts by SSDT alteration.

There are some other methods …

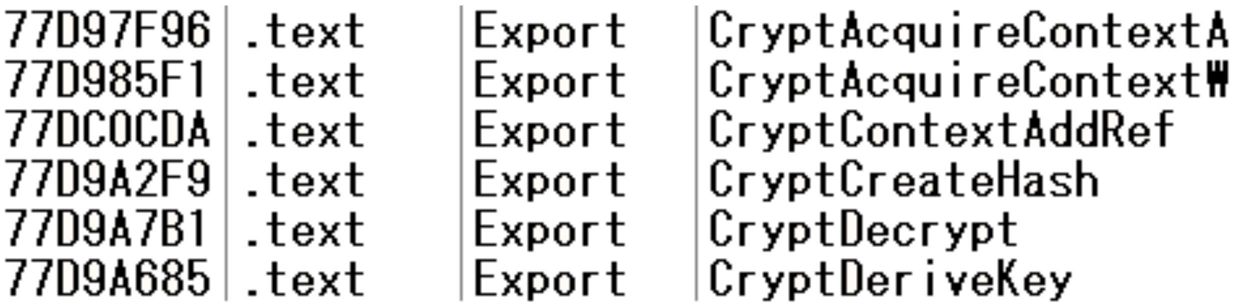
Windows CryptoAPI（1/2）

- Decoding API provided by ADVAPI32.dll.
- Available in Windows 2000 and later.
- You can use many crypt algorithm without professional knowledge.
- Related libraries like Hash, Signature, Confirmation as well.
- SSL communications in Windows environment often uses CryptoAPI internally.

Windows Crypt APIs（2/2）

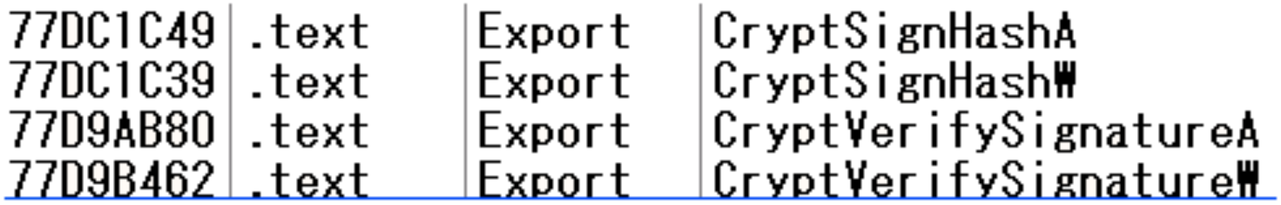
- Cryptographic train is exported with function names Crypt***.

Crypt functions exported by ADVAPI32.dll



```
77D97F96 .text    Export  CryptAcquireContextA
77D985F1 .text    Export  CryptAcquireContextW
77DC0CDA .text    Export  CryptContextAddRef
77D9A2F9 .text    Export  CryptCreateHash
77D9A7B1 .text    Export  CryptDecrypt
77D9A685 .text    Export  CryptDeriveKey
```

…………………



```
77DC1C49 .text    Export  CryptSignHashA
77DC1C39 .text    Export  CryptSignHashW
77D9AB80 .text    Export  CryptVerifySignatureA
77D9B462 .text    Export  CryptVerifySignatureW
```

A demonstration（1/4）

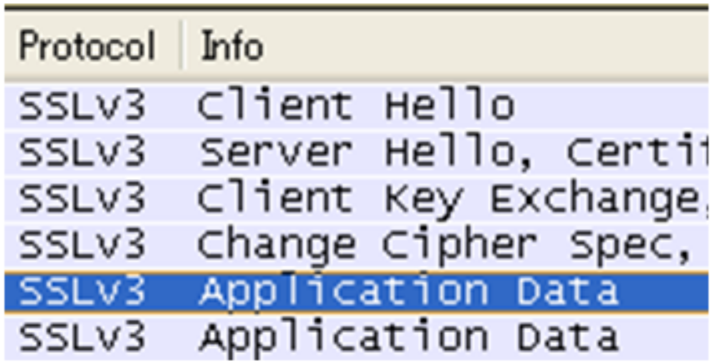
- As the data in SSL communication go through CryptoAPI, you can capture them by intercepting cryptographic functions in the process.

Demo 1

Capturing InternetExplorer’s SSL communication

Encrypted Data via SSL

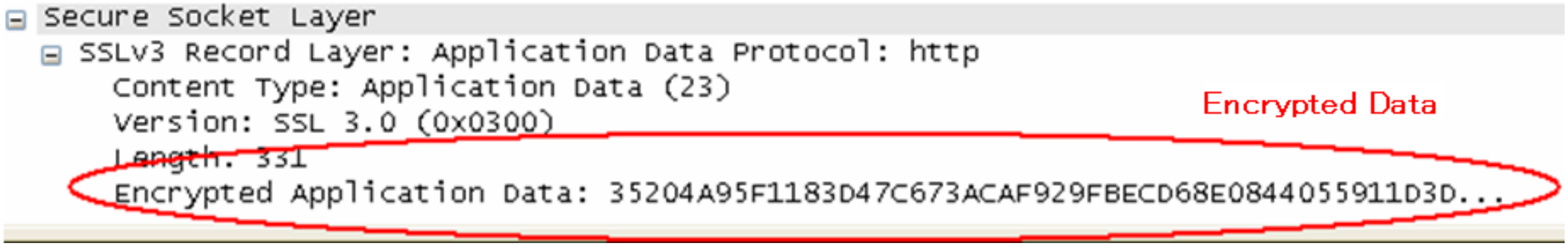
Wireshark can capture SSL (https) communications running on IE as illustrated below: Confirm that data has been encrypted by SSL.



Protocol	Info
SSLv3	Client Hello
SSLv3	Server Hello, Certi
SSLv3	Client Key Exchange,
SSLv3	Change Cipher Spec,
SSLv3	Application Data
SSLv3	Application Data

detail

We can watch encrypted data

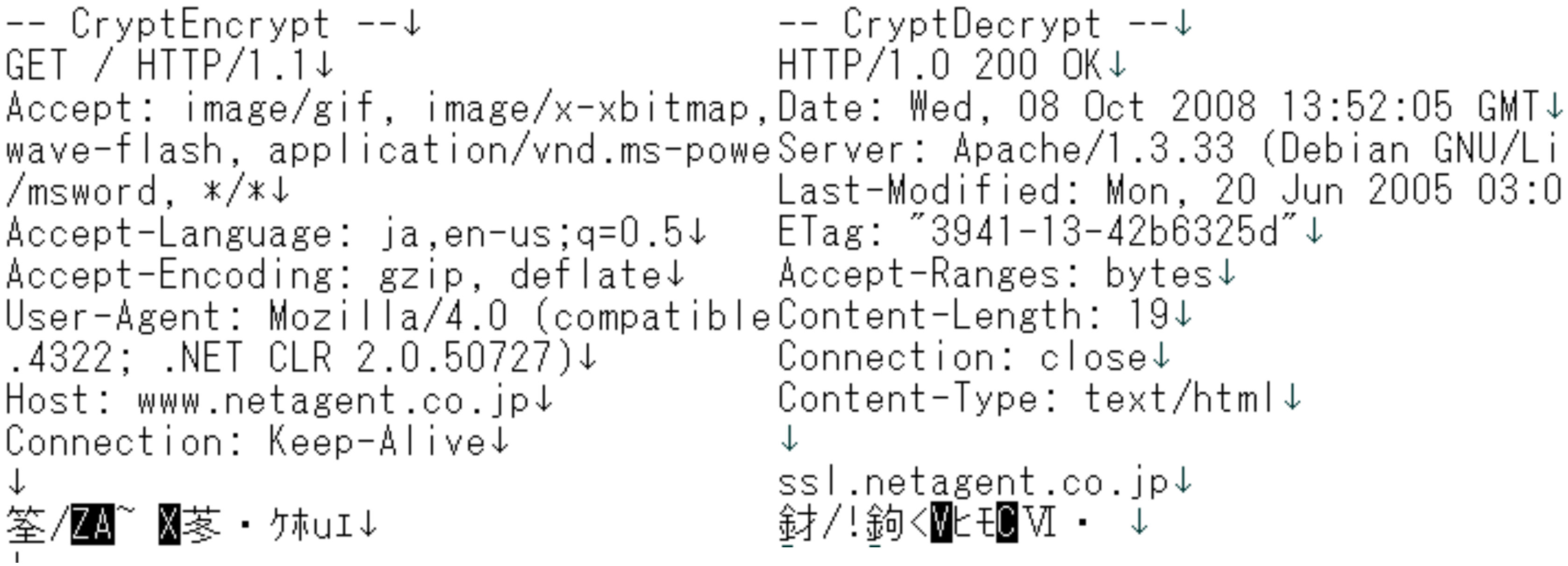


```
⊟ Secure Socket Layer
  ⊟ SSLv3 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: SSL 3.0 (0x0300)
      Length: 331
      Encrypted Application Data: 35204A95F1183D47C673ACAF929FBECD68E0844055911D3D...
```

Encrypted Data

Data gone through CryptoAPI

- Data gone through Crypt Encrypt/Decrypt can be seen in plain text.



■send data

```
-- CryptEncrypt --↓
GET / HTTP/1.1↓
Accept: image/gif, image/x-xbitmap,
wave-flash, application/vnd.ms-powe
/msword, */*↓
Accept-Language: ja,en-us;q=0.5↓
Accept-Encoding: gzip, deflate↓
User-Agent: Mozilla/4.0 (compatible
.4322; .NET CLR 2.0.50727)↓
Host: www.netagent.co.jp↓
Connection: Keep-Alive↓
↓
筌/ZA~ X蓼・ｹﾎuI↓
```

■recv data

```
-- CryptDecrypt --↓
HTTP/1.0 200 OK↓
Date: Wed, 08 Oct 2008 13:52:05 GMT↓
Server: Apache/1.3.33 (Debian GNU/Li
Last-Modified: Mon, 20 Jun 2005 03:0
ETag: "3941-13-42b6325d"↓
Accept-Ranges: bytes↓
Content-Length: 19↓
Connection: close↓
Content-Type: text/html↓
↓
ssl.netagent.co.jp↓
鈫/!鉤<VﾋﾓCⅥ・  ↓
```

Security in SSL communications

- An encrypted, simply tapping the traffic will not show the contents.

- While eavesdropping with MITM (Man In The Middle) is possible, reliability and security of the communication is guaranteed by using legitimate security certificate.

Multiple purposes of API hooking

- By intercepting at the very moment of decoding in an application program, the contents of SSL traffic are visible.
- Even the contents of traffic can be altered.
- The contents can be altered no matter whether the security certificate is valid or not.

API hooking is easy

- We can intercept some functions,
  - by using LD_PRELOAD on Linux (UNIX).
  - by installing Detours library which is released from Microsoft Research Team on Windows.

Detours libraries

http://research.microsoft.com/sn/detours/

LD_PRELOAD

- Available on Linux (UNIX).
- Only have to register corresponding .so file in LD_PRELOAD environmental variable.

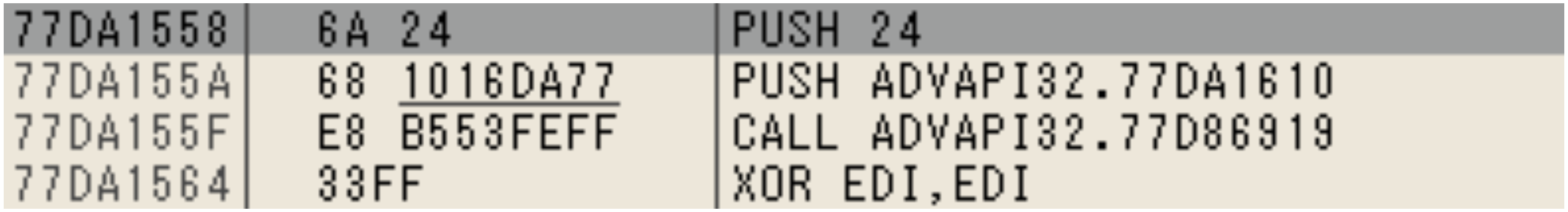
```
-----  terminal
% gcc –shared –fPIC –o intercept.so intercept.c –ldl
% LD_PRELOAD=./intercept.so target_prog
-----
```

Detours library（1/3）

- This is function intercept library which is released by Microsoft Research Team.
- This can intercept by changing the first few bytes of target function.
- It’s simple and easy to use.

Detours library（2/3）

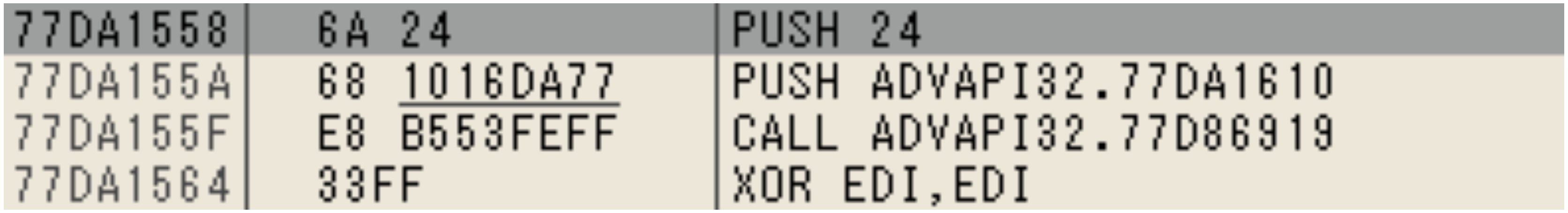
- I indicate head few byte of CryptEncrypt function blow.



```
77DA1558   6A 24         PUSH 24
77DA155A   68 1016DA77   PUSH ADVAPI32.77DA1610
77DA155F   E8 B553FEFF   CALL ADVAPI32.77D86919
77DA1564   33FF          XOR EDI,EDI
```

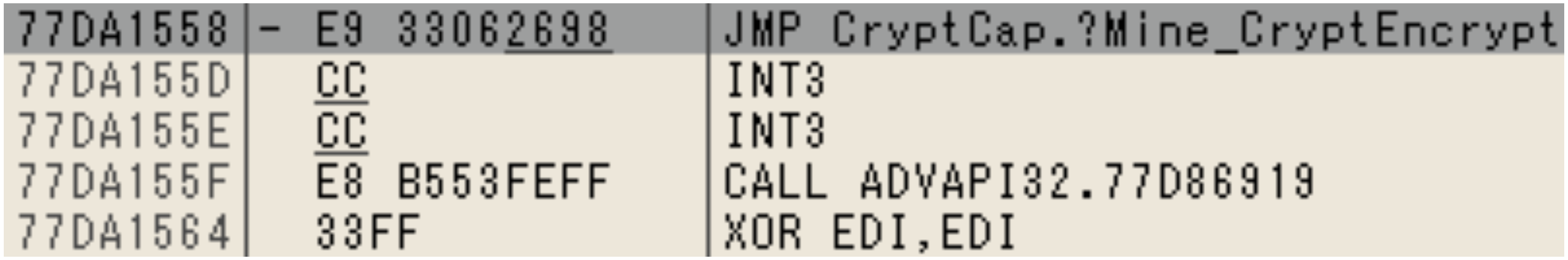
- This is a trivial assembler code, but if we intercept function by using Detours, assembler code will be changed as seen in the picture next page.

Detours library（3/3）



```
77DA1558    6A 24           PUSH 24
77DA155A    68 1016DA77     PUSH ADVAPI32.77DA1610
77DA155F    E8 B553FEFF     CALL ADVAPI32.77D86919
77DA1564    33FF            XOR EDI,EDI
```

The head few bytes of function will be changed by detours.dll.



```
77DA1558  - E9 33062698     JMP CryptCap.?Mine_CryptEncrypt
77DA155D    CC              INT3
77DA155E    CC              INT3
77DA155F    E8 B553FEFF     CALL ADVAPI32.77D86919
77DA1564    33FF            XOR EDI,EDI
```

- The first 5 bytes of CryptEncrypt function was changed to “jmp” by detours.dll.

Iintercept by changing IAT

- The way of jumping another function by changing IAT in process.

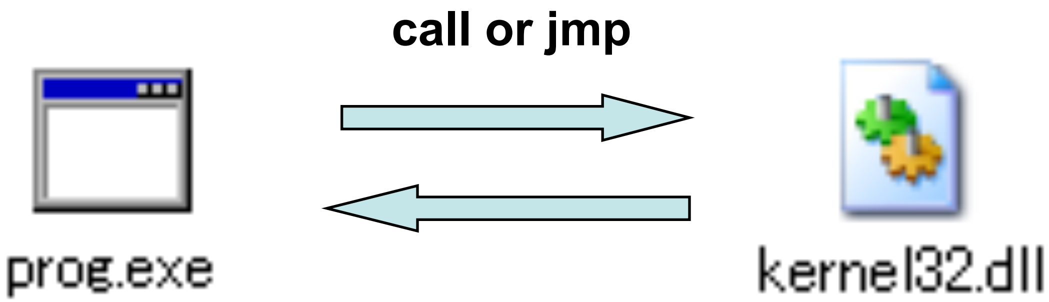
You can see more detail in

“Advanced Windows” by Jeffrey Richter.

DLL replacing（1/2）

- We can intercept a function by making fake DLL based on legitimate DLL with identical export function.

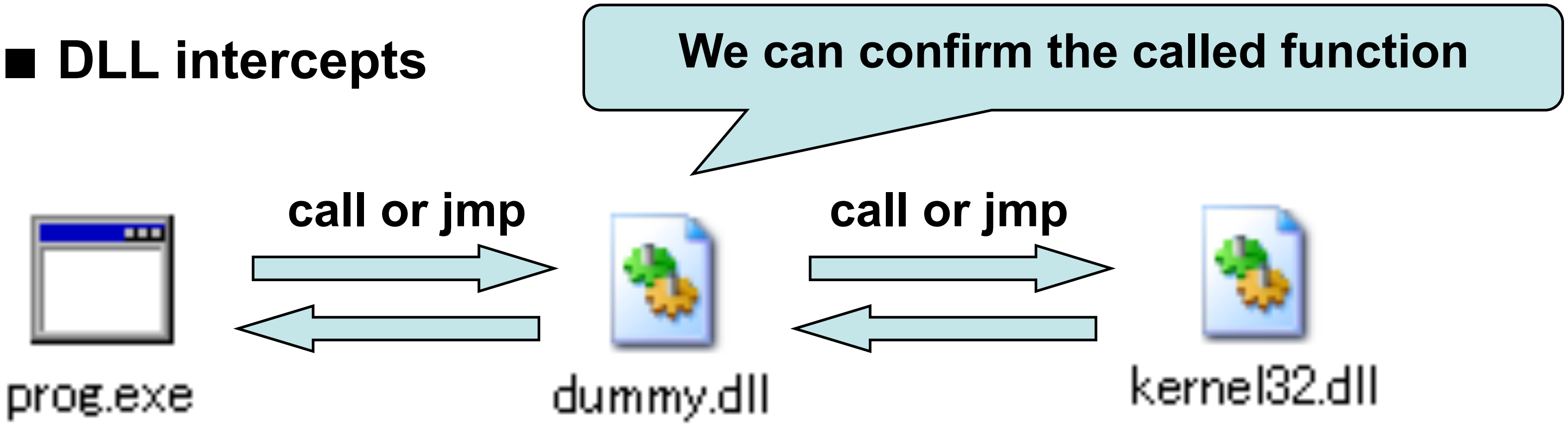
■ **normal**



DLL replacing（2/2）

- We can intercept a function by making fake DLL between prog.exe and kernel32.dll.

■ DLL intercepts



We can confirm the called function

call or jmp

call or jmp

prog.exe

dummy.dll

kernel32.dll

SystemServices hooking（1/2）

- System service (synonymous with system call on Linux) intercept by altering SSDT (System Service Descriptor Table).

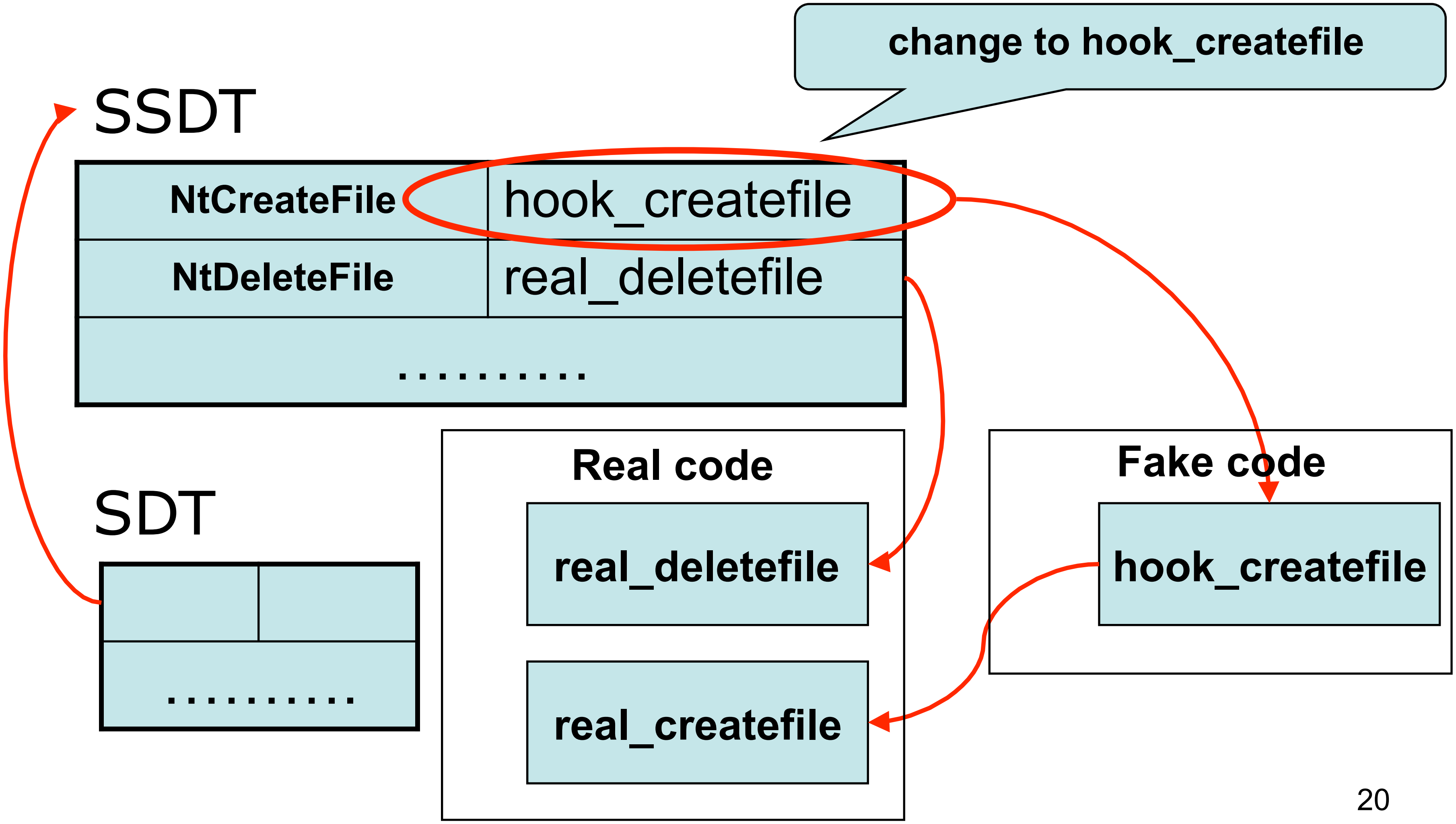
- Processing takes place in the kernel land.

Details found at

Hooking Windows NT System Services

http://www.windowsitlibrary.com/Content/356/06/2.html

SystemServices hooking（2/2）



change to hook_createfile

SSDT

NtCreateFile	hook_createfile
NtDeleteFile	real_deletefile
……….	

SDT

……….

Real code

real_deletefile

real_createfile

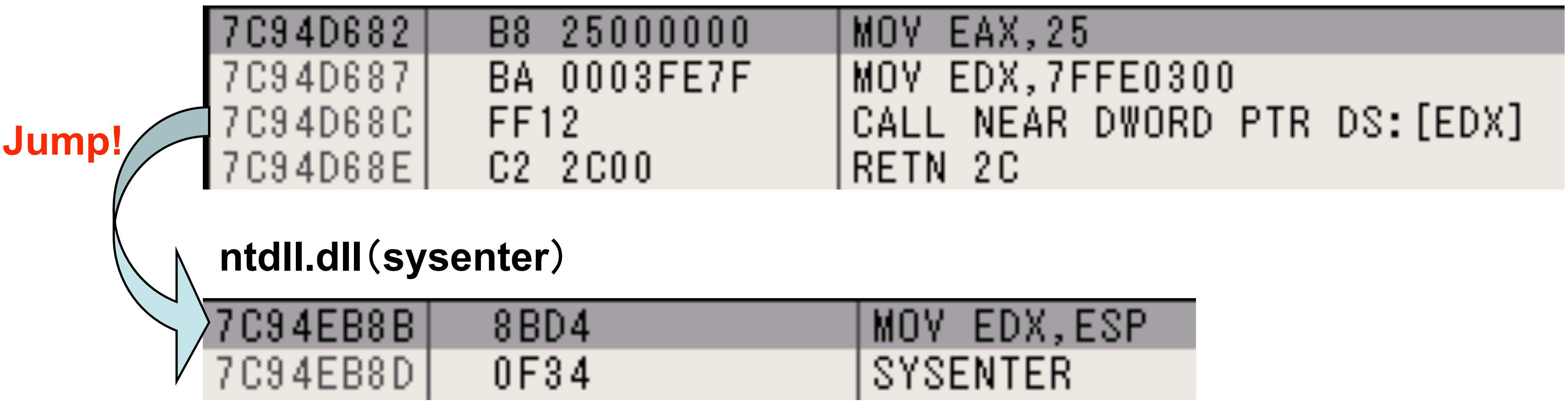
Fake code

hook_createfile

sysenter hooking（1/4）

- In WindowsXP/2003 (x86) environment, processes are handed over to the kernel by sysenter command.
- sysenter is called in ntdll.dll.
- sysenter will jump to the value assigned in MSR.

sysenter hooking（2/4）



ntdll.dll（ZwCreateFile）

```
7C94D682   B8 25000000   MOV EAX,25
7C94D687   BA 0003FE7F   MOV EDX,7FFE0300
7C94D68C   FF12          CALL NEAR DWORD PTR DS:[EDX]
7C94D68E   C2 2C00       RETN 2C
```

Jump!

ntdll.dll（sysenter）

```
7C94EB8B   8BD4          MOV EDX,ESP
7C94EB8D   0F34          SYSENTER
```

The value in eax registor shows system call number.

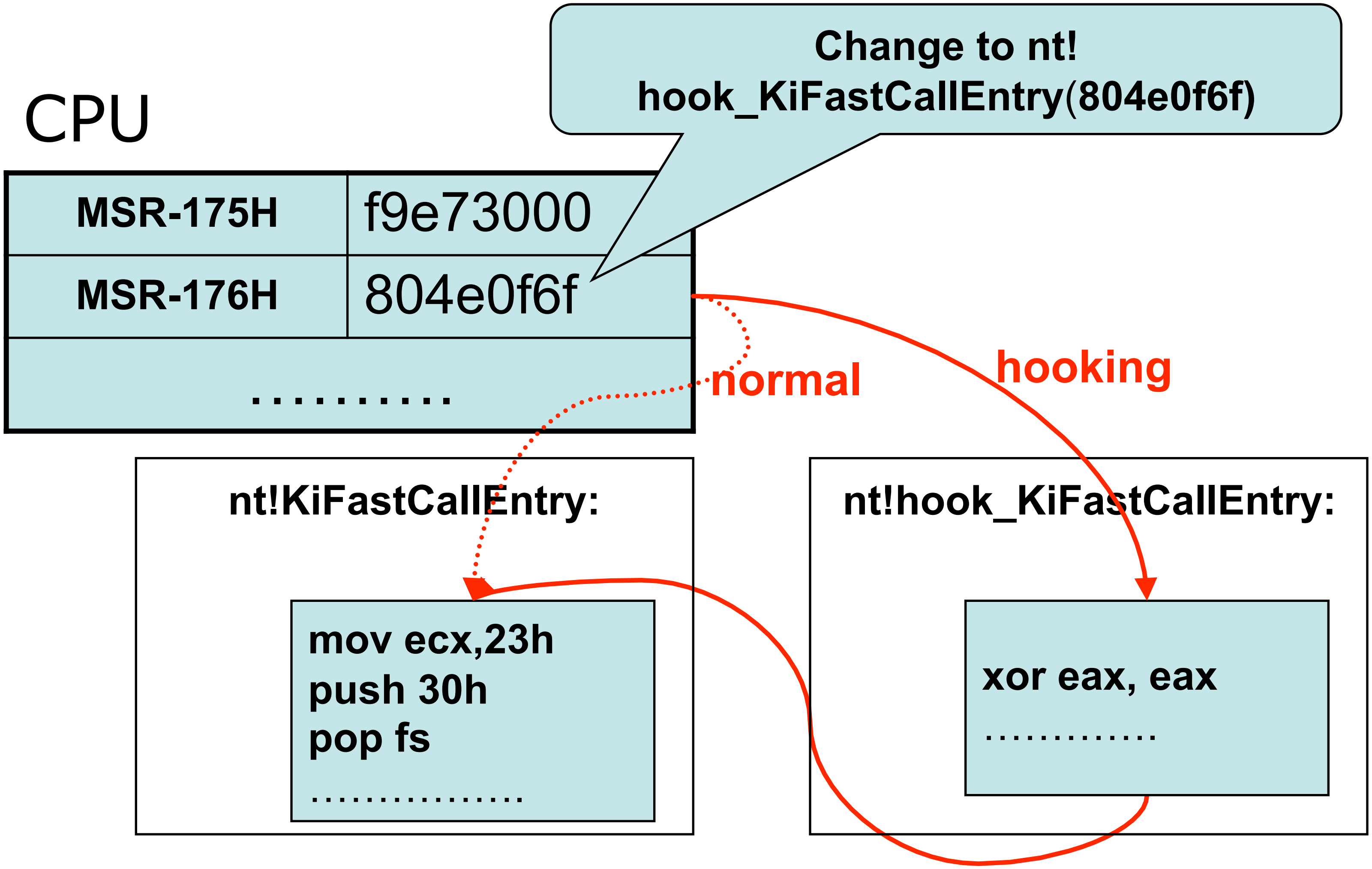
sysenter hooking（3/4）

■sysenter executed

1. Load the value of (MSR-174H) into CS
2. Load the value of (MSR-176H) into EIP
3. Load the value of (MSR-174H) + 8 into SS
4. Load the value of (MSR-175H) into ESP

Therefore, sysenter hooking can be achieved by altering (MSR-176H) corresponding to the CPU.

sysenter hooking（4/4）



CPU

MSR-175H	f9e73000
MSR-176H	804e0f6f
……….	

Change to nt!
hook_KiFastCallEntry(804e0f6f)

nt!KiFastCallEntry:

```
mov ecx,23h
push 30h
pop fs
……………..
```

nt!hook_KiFastCallEntry:

```
xor eax, eax
……………
```

A Demonstration（2/4）

- Eavesdropping with MITM by using API hooking.

Demo 2

Capturing the traffic of P2P programs

E-money Edy

- Prepaid e-money (technically identical to suica).

- Can be charged by bank transfer.

- Balance can be confirmed in real-time, also can be recharged, using a devoted software.

FeliCa Port（PaSoRi）

- A device to read the data in IC cards directly into PC’s developed by SONY.

- External ones connected through USB also available in stores.

- There are libraries for FeliCa Port available under BSD license.

EdyViewer.exe

- A software to read and maintain the data stored in Edy.
- Can be charged from registered bank account.
- Operable on Windows.
- Official software for FeliCa Port.

felicalib libraries

- Library to access IC cards using an USB-type device (PaSoRi). Licensed under BSD.

  http://felicalib.tmurakam.org/

- Can be used to access e-money’s like Suica、Edy、nanaco.

- Inofficial libraries for FeliCa Port.

A Demonstration（3/4）

- IC card reading tool can be built with felicalib.

Demo 3

Get the information from the IC card

Security of IC cards（1/2）

- Have readable blocks and unreadable blocks.
- Have encrypted blocks as well in IC card.
- Can not be written with felicalib.
- Can not be accessed to encrypted blocks with felicalib.

Security of IC cards（2/2）

- With the official tool EdyViewer.exe reading from encrypted blocks, writing , all possible.

- Uses SSL (https) to communicate with the admission server.

A demonstration（4/4）

- Examine the SSL communication while charging to an IC card.

Demo 4

Capturing the SSL traffic of the official tool

Perspectives（1/2）

- With API hook, communication between the user land and the kernel land can be captured.

- How can we capture the communication between EdyViewer.exe and a FeliCa Port driver?

Perspectives（2/2）

- With sysenter hook, system call can be observed.

- How can we estimate the function call history using the system call history at hand?

Thank you!

Any questions?