ECE4095 Trustable Computing Systems Lab
February 1, 2013

Memory Remenance

The goal of this lab is to capture the memory from a system after the system has been turned off. The lab uses a technique described in the paper “Lest We Remember: Cold Boot Attacks on Encryption Keys” by Halderman et al in the 20048 USENIX Security Symposium. The mode of attack is to create a USB boot disk that will be used to boot a computer after it has been turned off. The USB boot disk will contain code that copies all of memory to the disk. Once the memory has been copied it can be analyzed later to retrieve any sensitive data.

1. Build the USB boot disk

Download the source code from https://citp.princeton.edu/memory-content/src/bios_memimage-1.2.tar.gz to a Linux machine.

On the Linux machine, do the following

```
% tar xvfz bios_memimage-1.2.tar.gz
% cd bios_memimage/stand
% make
% cd ../usbdump
% make
% cd ../usb
```

Edit the Makefile, and change the CFLAGS line to the following:

```
CFLAGS= -ffreestanding -Os -Wall -I../include -march=i386 -fno-stack-protector
```

Then, do

```
% make
```

This will make the scraper.bin file which is the boot code for the USB stick. The following code will copy the boot code to the USB stick. Note that the /dev/sdbX will have to be changed to whatever device the USB stick is mounted as.

```
% dd if=scraper.bin of=/dev/sdbX
```

2. Dump the memory

On the target machine, insert the USB stick. The USB stick will not mount properly because it does not have a file system. That’s OK.

Open up a text file.   Create a repeating pattern of text – e.g.

U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™U™

The advantage of this pattern is that the ASCII code for `U` is 0x55 and the ASCII code for ™ is 0xAA meaning all bits are tested.

Repeat the pattern so that the file is about 4M in size.

While the text file is still open, pull the plug on the machine. Wait up to 30 seconds, and plug the machine back in and power it back up. Time exactly how long the power is off. Before, the machine can boot into Windows, press the key to activate the BIOS boot menu. On the Dell machines, its usually F12.

Find the boot selection screen, and select USB. This should boot into the scraper code on the USB stick. The scraper code will start running and dump the memory onto the USB stick. It can take up to 20 minutes per gigabyte of memory.

3. Retrieve the memory

Back on the Linux machine, do the following:

```
% cd ../usbdump
% usbdump /dev/sdbX > /tmp/memdump
```

You will need to write a small program that opens the memdump file and searches for the pattern that you wrote to the textfile. If the memory hasn't decayed, you should be able to find it. If the memory has partially decayed, only part of the pattern may be visible. Your program should calculate how many bits have been flipped (if any) in the total 4M pattern.

4. Lab Assignment

What to hand in:

1. Turn in the code that finds the pattern in the memdump file
2. Show the results of your decay calculation – i.e. number of bits flipped and how long the power was off.