PA#1: Getting Started with the Windows Research Kernel (WRK) and VirtualBox

Monday August 31, 2009 – V2 out 9/7 (minor corrections in red)
Due Thurs Sept 10 11am
Worth 5% of your grade in cs4414
You must do this assignment by yourself

Expected duration: 3 hours

The purpose of this hands-on lab is to gain experience using, compiling, and modifying the Windows Research Kernel (WRK). The basic idea is that you will:

- Install VirtualBox, an x86 virtualization platform that runs on Windows, Linux, Macintosh, etc.
- Create a *virtual machine* running Windows Server 2003
- Modify the WRK source code, recompile your kernel, install your new kernel, and confirm that your changes are executed.

You have options regarding how to perform this lab:

	Host (physical) machine is Windows 7, Windows Vista, or Windows XP	*Host (physical) machine is Linux or MacOS*
Edit and compile WRK source using Visual Studio on the Host (physical) machine	This is the **recommended** option, as Visual Studio is an excellent IDE. Install Visual Studio as necessary (it is free for students)	Not possible. Consider using the CS machines in Olsson 001 (and Visual Studio) and an external flash-based drive. This is a **good** option.
Edit and compile WRK source using a text editor (such as Emacs or VI) on the Host (physical) machine	Only use this option if you don't want to install Visual Studio or you do not have enough disk space for Visual Studio.	Not possible to compile.
Edit and compile WRK source using Visual Studio on the Guest (virtual) machine	Good option if you do not have enough space on the hard drive of the Host (physical) machine.	This is the **recommended** option.
Edit and compile WRK source using a text editor (such as Emacs or VI) on the Guest (virtual) machine	Possible, although the Vistual Studio IDE makes things easier (e.g., Intellisense)	Can be done entirely *inside* the virtual machine. This is a **good** option.

Irrespective of the options above, the virtual machine hard drive can be stored on the hard drive of the Host (physical) machine or on a flash-based drive (such as SD card or USB drive). If there is not enough available disk space on the Host (physical) machine, then an 8GB drive should be purchased. Even if there is enough available disk space on the Host (physical) machine, an external drive can be considered if portability is necessary/desired. Note, however, that if a flash-based drive is used, be careful to always "safely remove" the device, and furthermore (of course) be careful to not lose the device (if you lose this device, you can always follow these instructions to re-create your virtual machine).

It is expected that the physical machine you are using has at least 2G RAM (512 MB will be used by the virtual machine) and that there is at least 8GB disk available (4GB or 7GB will be used by the virtual machine; note that this can be from the hard drive of the computer or from a SD card or USB drive). *If you use an SD card or USB drive, make sure to always "safely remove" it from the physical machine!*

We will use DreamSpark (http://www.dreamspark.com), which is Microsoft's portal for students to obtain free copies of select Microsoft products, to obtain Visual Studio 2008 Professional Edition and Windows Server 2003 (to run on the virtual machine). You will get the source code for WRK from the class collab site (you **MUST** read and abide by the WRK license agreement – most notably that you are not allowed to make this source code available to ANYONE).

Throughout the lab, there are **fourteen** questions. It is probably easiest to use Microsoft Word to write your answers to the questions, generate a PDF from it, and then submit the PDF via Collab.

Exercise #1: Creating the WRK Virtual Machine in VirtualBox

1. The virtual machine technology we will be using is VirtualBox (http://www.virtualbox.org/) Download and install it from a web page off of the link above (it is free). (This lab assumes VirtualBox v3.0.4, although any version later than this should also work). At this point, we do not need to run VirtualBox. *If you want to use the machines in Olsson 001, you must use one of the machines in the backrow (e.g., LABPC49). VirtualBox is installed on only these machines. Also note that these machines dual-boot Linux and Windows. If Linux is booted, select the "reboot" option on the lower left of the screen and then Windows will be booted by default.*
2. Obtain the 2 ISOs for Windows Server 2003 DreamSpark (www.dreamspark.com) via Internet Explorer. It is not necessary burn CDs of these ISOs – just leave them in your file system on the physical machine (or on your flash-based drive). It is not necessary at this time to obtain a license key for this (via the "Get Key" option). *Note: these instructions assume you will not use this license key, because you are allowed to install and run for 30 days without using the license key. It is assumed that 30 days is sufficient to perform additional labs/experiments.*
3. Start VirtualBox (Start → All Programs → Sun xVM VirtualBox → VirtualBox). (You can hit the "cancel" if prompted with the VirtualBox Registration Form). Click on the "New" icon in the upper left, which will start the "New Virtual Machine Wizard" (hit "Next" to begin): *Note: if you do this in 001, every time to login, you will need to construct a new virtual machine using the existing hard drive. This is not really a problem as It doesn't take much time.*
   a. Name: "WRK", Operating System: "Microsoft Windows", Version: "Windows 2003"
   b. Memory: 512 MB
   c. The defaults on the "Virtual Hard Disk" screen are fine
      i. "Dynamically expanding storage" is fine
      ii. The default location will put the virtual hard drive into your "home" directory. If you want it on a flash-based external drive, override the default here (e.g., "G:\WRK.vdi"). Change the size to be 4GB (if you plan on installing Visual Studio *inside* the virtual machine, make this 7GB instead of 4GB). *Note that in 001 (maybe elsewhere), this interface is not great – you might need to manually confirm where the flash-based drive is mounted and type this in the dialogue by hand.*
      iii. Select "Finish"
   d. Select "Finish"
4. Start the virtual machine you just created and install the Windows Server 2003 operating system:
   a. Select the "WRK" virtual machine and hit "Start"
   b. Read the notification regarding "Auto capture keyboard". This will be only relevant for a short period of time while we're installing the OS, but you'll need to remember this (if you think you can remember that hitting the right "Ctrl" key will give you control of the mouse again, then hit the "Do not show this message again"). Hit "OK".

c. Go through the “First Run Wizard”:
   i. Change the “Media Source” to be an “Image File”, and hit the icon to navigate to the ISO:
      1. On the “Actions” pane, select “Add”
      2. Find the *first* Win Server 2003 ISO
   ii. Select the ISO you just added
   iii. Hit “Finish”

d. Go through the Windows installation questions:
   i. On the “Welcome to setup” screen, hit “Enter”
   ii. Read and agree to the licensing terms (hit F8)
   iii. Hit “Enter” to select the unpartitioned space
   iv. “Format the partition using the NTFS file system (quick)”
   v. << *windows will being copying files from the ISO to the virtual disk, and then reboot itself and continue the installation* >>
   vi. On the “regional and language options”, hit “Next”
   vii. Type in your name (organization is not necessary)
   viii. On the “Your product key” window, hit “Next” (“Do you want to enter your product key now?” no.)
   ~~ix. On the “licensing mode” window, hit “Next”.~~
   x. Hit “next” on the “Licensing Modes” window (without changing anything)
   xi. **Change the name of the machine to be your 5 or 6 character UVA ID.** It is okay if you choose a trivial admin password that you can remember (of course, if this were a real machine, you would need to use a secure password)
   xii. The date/time should be correct (it gets it from the BIOS of the physical machine), but change the time zone to “Eastern Time”
   xiii. “Typical settings” for networking should be fine
   xiv. The default for “Workgroup or computer domain” is fine
   xv. << *at this point, Windows will need approximately 30 minutes to install, depending on the characteristics of your physical machine (also: ignore any “press any key to boot from CD” directives)* >>

5. When Windows Server 2003 completes installation (you’ll see a window that says “Press ctrl-alt-delete to begin”):
   a. On the virtual machine, do “machine → insert ctrl-alt-del” and type in your administrator password (you might have to hit the right-ctrl key to regain control of the mouse)
   b. We now have to complete the installation of Windows Server 2003:
      i. On the virtual machine, do “Devices → Mount CD/DVD-ROM → CD/DVD-ROM image” (Add the second CD, and “select” that). This will make the second ISO (in your file system) appear to be as d: in the virtual machine
      ii. Hit “OK” in the window in the virtual machine
      iii. On the “welcome to the Windows Server 2003 R2 Setup Wizard”, hit “Next” and select the default choices on the remaining windows
   c. On the “Windows Server Post-Setup Security Updates”, do *not* install updates, and hit “Finish” instead
   d. On the “manage your server” window, scroll down and select the “do not display this page at logon” option, and then kill this window by hitting the “x” in the upper right of the window (NOT the “x” of the virtual machine)

6. Finally, install the “virtual machine additions” (which will make the integration between the physical machine and the virtual machine nicer) by doing the following:
   a. Devices → unmount CD / DVD-ROM

   b. Devices → install guest additions (and then accept the default options on the rest of the windows – including selecting "continue anyway" when Windows warns you that certain device drivers might not be safe. Hitting "finish" will reboot the virtual machine)
7. When the virtual machine reboots, read the window describing "mouse pointer integration", select "do not show this message again", and then hit "OK". You now have a better mouse experience, and you can also resize the virtual machine as necessary.
8. Login to the virtual machine and shutdown the virtual machine via the Windows mechanism (Start → Shut down and give it the reason of "Operating System: Reconfiguration")
9. After shutting down the virtual machine, in the VirtualBox console for the new virtual machine, click on the "CD/DVD-ROM", and then "unmount" the guest additions

Questions for this exercise:

Q-1. How big is the physical file that contains your virtual disk?

Exercise #2: Exploring the Windows Research Kernel (WRK) source

This lab assumes that you will use Visual Studio 2008 on the physical machine, so this next section describes actions that you should do on the physical machine. If you're going to run Visual Studio or a text editor such as Emacs on the virtual machine (for Visual Studio, you'll need much more physical disk space available), then boot your virtual machine and login as administrator, confirm that you have networking available by opening up Internet Explorer and going to a site, and then perform these actions within the virtual machine.

10. If you do not already have Visual Studio 2008 installed, download and install Visual Studio from DreamSpark. (otherwise skip this step)
    a. Note: MagicDisc (http://www.magiciso.com/tutorials/miso-magicdisc-overview.htm) is a great option if you want to avoid bring CDs/DVDs
    b. Note: Visual Studio 2005 should work, although it has not been tested with this lab
    c. Note: download the Visual Studio ISO onto the physical machine instead of the virtual machine. When installing onto the virtual machine, use the "Mount" option of VirtualBox.
11. Download the Windows Research Kernel v1.2 from the class collab site ("WRK-v1.2-CS4414-UVA" in "Resources") and put into C:\ or the top-level in your flash-based drive. (*Note that this probably WON'T work if you try to put it into your "My Documents" folder.*) **MAKE SURE YOU READ AND UNDERSTAND THE LICENSE (available from the collab site as well)!** Extract the file (make sure to let this operation complete – this can take a few minutes on a flash-based drive). Move the "WRK-v1.2" folder directly into C:\ or the top-level in your flash-based drive. (you can remove the now-empty folder)
12. Next, install Cygwin from http://www.cygwin.com . Click on the "Install Cygwin now" icon. For this lab, it is sufficient to install the default configuration. *In Olsson 001, cygwin is already installed and available as an icon on the desktop.*
13. If you are using Emacs, then install that now. A good option is XEmacs from http://www.xemacs.org/Download/win32/ . *In Olsson 001, Emacs is available as an icon on the desktop.*
14. We'll want to share this WRK folder on the physical machine with the virtual machine:
    a. On the VirtualBox console, select "WRK", and then on the details pane to the right, scroll down until you see the "Shared Folders" (it's off the screen at the bottom). Left click on this.
    b. Click the "Add" icon toward the upper right.
    c. In the "Add Share" dialogue, expand the "folder path" option and select "Other…" Navigate to this WRK-v1.2 folder and hit the "OK" button. The "Folder name" should fill in automatically. Do NOT select the "Read-only" option. Hit the "OK" button (and then the "OK" button again).

Questions for this exercise:

Q-2. Get a BASH shell from Cygwin by clicking the desktop icon (If that's not present, then start Cygwin via "Start → All Programs"). To allow you to cut-and-paste into this window, rightclick on the top of the Cygwin window and select "Properties", and in the "Edit Options" part select "QuickEdit Mode" (and "Modify the shortcut that started this window"). Now go to the main directory of the Windows Research Kernel source code by doing a `cd /cygdrive/c/WRK-v1.2/` Note: if you're using a flash-based drive, replace the "c" drive with the name of the flas-based-drive). How many files or directories are there? (Run the command `find | wc -l`).

Q-3. How many C files are there? (Run the command `find . -name *.c | wc -l`)

Q-4. How many lines of source code are there in the kernel? First, execute `cd base/ntos/ke` and then run the command `cat *.[ch] | grep -c "."` Note that if you're curious you can see the number of lines on per-file basis by typing `grep -c "." *.[ch]`

Q-5. How much disk space does the distribution take? `(du -s /cygdrive/c/WRK-v1.2)` What are the units of this measurement? `(man du)` Give the number of megabytes this distribution takes.

Exercise #3: Compiling the Windows Research Kernel (WRK)

Note: if you're using Visual Studio *inside* the Virtual Machine, you should use Visual Studio to edit the files but you should use the Command Prompt instructions, below, to compile and link your new kernel.

1. Open up the Visual Studio Project by opening up the WRK-v1.2 folder and double-clicking on the Visual Studio Solution. (This will take a few moments the first time, as it needs to update IntelliSense) *If you're prompted for "default environment settings", C++ is fine.*
2. Remove all of the object files by Build → Clean Solution (you may need to make sure that the Output is shown by View → Output)
3. Toward the top of Visual Studio, change the "amd64" to "x86" and execute Build → Clean Solution again
4. Build the kernel by Build → Build Solution (**NOTE: don't do this before looking at question ~~#Q-5~~ #Q-6, below!)**

If you are not using Visual Studio, do the following in a Windows Command Prompt (Start → All Programs → Accessories → Command Prompt)

a. Type: `set arch=x86`
b. Set the path by typing: `path c:\WRK-v1.2\tools\x86;%path%`
c. Download "msvcr71.dll" from: http://www.dll-files.com/dllindex/dll-files.shtml?msvcr71 and put this into c:\WRK-v1.2\tools\x86
d. Change the directory: `cd c:\WRK-v1.2\base\ntos`
e. Remove all of the object files by typing: `nmake x86= clean`
f. Build the kernel by typing: `nmake x86=` (**NOTE: don't do this before looking at question #Q-6, below!)**

Questions for this exercise:

Q-6. How long did it take to compile your kernel the first time? Run the same command a second time (not the "clean" part), how long does it take? (It is sufficient in this case to "eye-ball" it – 'seconds' resolution is fine).

Exercise #4: Monitor the invocation of “QuerySystemInformation”

In this portion of the lab you will modify the WRK kernel to print out some debugging information to keep track of the number of times “QuerySystemInformation” is invoked (sometimes a developer may wish the kernel is “instrumented” this way for performance purposes – for example, I f we find that this function is invoked A LOT, then this function is a reasonable candidate for performance optimization, right?) In this part, we’ll modify the kernel, recompile it, install it as a boot option, boot the modified kernel, and see the output on the debugging window.

1. If using Visual Studio:
    a. In the Visual Studio Solution Explorer, navigate to base\ntos\ex\sysinfo.c and double-click on it to open it for editing
    b. Go to line 1721 by hitting ctrl-g and entering 1721. Insert the following line here:

    ```
    static int NumTimesCalled = 0;
    ```

    c. Shortly after this (immediately before the line “Status = STATUS_SUCCESS”), add the following line (if you cut-and-paste this line, make sure to fix both quotation marks)

    ```
    DbgPrint( “WRK  %d: Execute NTQuerySystemInformation!!\n”,++NumTimesCalled );
    ```

    d. Save the file via ctrl-s and recompile the kernel via Build → Build Solution
2. If you’re using Emacs:
    a. Start XEmacs (via Start → All Programs → XEmacs → XEmacs-21.4.21) and edit `C:/WRK-v1.2/base/ntos/ex/sysinfo.c` by hitting ctrl-x ctrl-f and specifying the file’s pathname. (To make it easier to look at the source code, in XEmacs, Options → Syntax Highlighting → In This Buffer).
    b. Get to line 1721 by hitting Ctrl-u 1 7 2 0 *down-arrow*. Insert the following line here:

    ```
    static int NumTimesCalled = 0;
    ```

    c. Shortly after this (immediately before the line “Status = STATUS_SUCCESS”), add the following line: (if you cut-and-paste this line, make sure to fix both quotation marks)

    ```
    DbgPrint( “WRK  %d: Execute NTQuerySystemInformation!!\n”,++NumTimesCalled );
    ```

    d. Save the file via ctrl-x ctrl-s and recompile the kernel as above (Exercise #3 – but skip the “`nmake x86=  clean`” step)
3. Boot the WRK virtual machine and log in as Administrator.
4. Our previous step made the “shared folder” *potentially* available to the virtual machine. Now we have to have Windows “mount” the shared folder:
    a. In the virtual machine, open “my computer” and select Tools → Map Network Drive
    b. Click “Browse”, expand the “VirtualBox Shared Folders”, and select \\VBOXSVR\WRK-v1.2
    c. Hit “Ok” and then “Finish” (this will now appear as Z:)
5. On the virtual machine, copy from the shared folder Z:\base\ntos\BUILD\EXE\wrkx86.exe to C:\WINDOWS\system32\
6. We now configure the Virtual Machine to make booting your new kernel an option:

a. On the virtual machine, copy from the shared folder z:\WS03SP1HALS\x86\halacpim\halacpim.dll to c:\WINDOWS\system32

b. On the virtual machine, use notepad to add a *single line* to the end of c:\Boot.ini file, enabling the selection of your new kernel (Note: manually type in "C:\Boot.ini", as it is hidden via the GUI, and that if you cut-and-paste this line, make sure to fix the quotation marks and to make this one long line instead of 3 lines).

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=”WRK OS”
/kernel=wrkx86.exe /hal=halacpim.dll /noexecute=optout
/fastdetect/DEBUG
```

7. After saving the new Boot.ini on the Virtual Machine, reboot the Virtual Machine via Start → Shutdown → Restart (give the reason as "Operating System: Reconfiguration"). Immediately after it reboots, select your new boot option ("WRK OS")
8. Once the new machine reboots, *inside the virtual machine,* download and unzip "DebugView for Windows" from here: http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx (save it on the desktop)
9. Start Dbgview, Capture → Capture Kernel
10. If everything is working, you should start seeing something like:

```
WRK 82: Execute NTQuerySystemInformation!!!
WRK 83: Execute NTQuerySystemInformation!!!
WRK 84: Execute NTQuerySystemInformation!!!
```

If you're not seeing this, then go back through the instructions to see if you've missed something. *Note that if your new kernel does not boot, then you can most likely reboot into a "safe" kernel, such as the kernel from the previous steps that has debugging turned on.*

Questions for this exercise:

Q-7. In the virtual machine, select the "DebugView" screen, hit Alt-PrintScreen. Now start up Microsoft Word and "paste" the image to show that you successfully completed this part.

Q-8. Once you've completed that, and closed your Virtual Machine and debugging window, how big is the physical file that contains your virtual disk now? Why is this? (I.e., why is it the same, or why has it changed?)

A few last questions:

Q-9. How much time did it take you to finish this lab?

Q-10. Did you use your own machine, a machine in 001 or some other machine?

Q-11. Did you use a flash-based drive?

Q-12. Did you use Visual Studio, Emacs, or some other editor (please specify)?

Q-13. What was the most difficult (trickiest?) part of this lab? How would you improve this lab?

Q-14. Do you feel you understand what's going on or did you feel that you were just following a script/recipe and did not understand?

That's it! You have successfully modified the Windows Research Kernel and observed your change in action. By following this basic procedure, you are now able to explore all kinds of kernel modifications and subsequently test the effect of such changes.