Assignment 3

RUNNING MULTIPLE VIRTUAL MACHINES AND PROFILING PERFORMANCE

As part of this assignment we will be splicing a physical machine's capabilities (CPU, main memory, hard disk and networking) to create multiple virtual machines. One (or more) of the virtual machines that are created will be part of a private cloud that would be used to run distributed programs. For this assignment you will be working with Xen. Version 8.0.4 of Ubuntu will be installed on Domain0.

Step 1: Installing Xen

Follow the instructions at http://www.howtoforge.com/ubuntu-8.04-server-install-xen-from-ubuntu-repositories for installing Xen on Ubuntu 8.0.4. You need to use the kernel provided at http://www.il.is.s.u-tokyo.ac.jp/~hiranotaka/; the kernel to be used is linux-image-2.6.24-16-xen_2.6.24-16.30zng1_i386.deb.

After the Xen-enabled kernel has been installed you need to go to /boot/grub/menu.lst and change the timeout and default kernel that should be loaded. Make sure that the normal kernel (without Xen) is loaded by default. This is to ensure that the Network Security students have access to the machine without Xen at all times.

IP Addresses for Domain0 and DomainU installations

When setting up Domain0 and each of the DomainU you need to assign them IP addresses. The NetSec lab has its own subnet, and the machines have private IPs (i.e. 192.168.*.*).

The IP address for a machine/Domain0 should be 192.168.0.2x, where x is the number of the machine (cs457-x).

A DomainU should use 192.168.1xy, where x is same as the machine number, and y can be anything. However, you should ping the IP that you are trying to use just to be doubly sure that IP is not being used.

The Gateway and DNS configurations that you will need are listed below:

```
gateway:192.168.0.1
netmask:255.255.255.0
DNS:129.82.45.181
```

Step 2: Setting up DomainU

The distributions that have been confirmed to work are Ubuntu 8 (hardy heron), Debian 4 (etch) and Debian 5 (lenny). The requirements for this assignment are that:

a. There are at least two different OSes

b. There are a total of four DomainUs that are up and running.

c. Each OS should be allocated 128MB memory, 4GB HDD, and 256MB swap space. Domain0 gets to use the entire disk.

Extra credit: There is a 10% extra credit if you can get Fedora11 or CentOS5 to work as DomainU
Grading points

1. Minimum requirements: Xen kernel should be running

Executing the command `uname -a` should display a kernel with 'xen' in its name.

2. Check for DomainU and its memory allocation

When you boot the machine with Xen-enabled kernel, you should be able to configure the DomainUs to be running at startup. The command `xm list` will be used to verify the list of domains that are running and the size of the allocated memory for each of these domains.

2.(a) Check disk allocation

We will look at the locations where the disk images for DomainUs are stored to verify that the OSes have allocated disk sizes as specified in the assignment. This assignment requires that you store the disk images in the following locations:

/home/xen/domainName/disk.img  
/home/xen/domainName/swap.img

2.(b) Logon to DomainU

We need to be able to access specific domains. The command `xm console domainName` will be used to verify that the logon process succeeds. Note that in some cases (debian) you would need to use ssh.

2.(c) Check if you can run tasks on DomainUs

You will have to run your cryptographic attacks on all the domains concurrently. A check will be made to see that the applications are running concurrently on the different domains. `xm top` will be used to see how resources are being utilized.

Part II

Launching a brute force Cryptographic attack

As part of this assignment you will be launching a cryptographic attack to retrieve a secret key. Each of you will be given a plain-text, encrypted-text and a cryptographic key search space. You will use this information to launch the attack and retrieve the key.

Solution: The solution to the assignment is submitting the complete AES cryptographic key.

You will run your program under the following situations for the machine assigned to your group:

1. Running only the native kernel
2. With Xen, but no DomainU
3. With Xen and 4 DomainUs concurrently
Your report should reason about the differences you see in performance.

Also, estimate the number of machines that you will need to launch an unassisted cryptographic attack; for the purposes of your calculation assume that your machine will have 1024 cores, with 4 execution pipelines per core.