CMPE 283:Virtualization

Assignment 2: Instrumentation via hypercall

Name: Deep Khajanchi (013764686)

Github repo: <https://github.com/deepkhajanchi/linux>

Problem Statement:

(1)For CPUID leaf node %eax=0x4FFFFFFF:

◦ Return the total number of exits (all types) in %eax

(2) For CPUID leaf node %eax=0x4FFFFFFD:

◦ Return the number of exits for the exit number provided (on input) in %ecx

▪ This value should be returned in %eax

Steps to follow:

1. With the configuration od Assignment 1, follow the step in the sequence.
2. In the hypervisor code, open the folder linux-master/arch/x86/kvm.
3. Edit the file cpuid.c and add the the logic function for saving total exit counts to EAX and total time time spent cycles in EBX and ECX respectively.
4. GO to the folder linux-master/arch/x86/kvm/vmx.
5. Edit the file vmx.c and add the logic .
6. Save your changes and go back to the root folder.
7. Now build the source code using below command. Make sure you are using super user mode.

Sudo make

1. Reboot the system after successful build.
2. Switch on the guest VM and install the package CPUID in it.
3. Run the belox command to check all the number of exits occurred by passing 0x04FFFFFFF instruction.

Cupid -l 0x04FFFFFFF

1. To check the the number of exits for the exit number provided (on input) in %ecx.

Cupid -l 0x04FFFFFFD.

1. Now reboot the guest VMand run the command in step 10.
2. Count the total number of exits occur in a full system boot.
3. Exit counter before reboot
4. Exit counter after reboot

Comment on the frequency of exits – does the number of exits increase at a stable rate? Or are there

more exits performed during certain VM operations? Approximately how many exits does a full VM

boot entail?

The no. of exits increases every time but not on a stable rate. The number of exits depends on the different operations, like io or ept violation the exits are more in comparison with the other operations. A full VM boot entails approximately exits for the source tree.

OF the exit types defined in the SDM, which are the most frequent? Leas?

CPUID is the most frequent.