

CMPE 283: Virtualization Technologies

Assignment 2: Modifying Instruction Behaviour in KVM

Bhavya Tetali (014535144), Supriya Meduri (015262767)

Contribution of Team Members

Bhavya Tetali:

1. Built the kernel.
2. Researched about atomic variables and cpuid instruction.
3. Understood where to place the measurement code in vmx.c.
4. Modified the code in **vmx_handle_exit** function in vmx.c and defined global variables.
5. Created a test file and compiled it.
6. Updated documentation.

Supriya Meduri:

1. Firstly, I rewatched the lecture 5 video.
2. Built the kernel.
3. Tried to understand the assignment requirements of leaf function.
4. Created a CPUID leaf function in **kvm_emulate_cpuid** when %eax=0x4FFFFFFF function in cpuid.c.
5. Created documentation.

Environment Setup:

1. Forked and Cloned the Linux Repository

```
$git clone https://github.com/torvalds/linux.git
```

2. Enter sudo mode

```
$ sudo bash
```

3. Install all the build essentials required to compile

```
$ apt-get install build-essential kernel-package fakeroot  
libncurses5-dev libssl-dev ccache bison flex libelf-dev
```

4. Set up the config file

```
$ make menuconfig
```

5. Select kernel-based virtual machine(kvm) support option on the screen prompt

6. Increased the number of processors in the outer VM to eight.

7. Compile and build the kernel

```
$ make -j8 && make modules -j8 && make install -j8 && make  
modules_install -j8
```

8. Reboot the system , to get the new kernel

```
$ reboot
```

9. Check the current version of newly built kernel

```
$ uname -a
```

Modification of kernel code:

1. Add the assignment functionality of building a leaf function.
2. In vmx.c, created two global variables : no_of_exits and cpu_cycles.
3. Additionally, in **vmx_handle_exit** function calculated the no of exits using inc function and total time spent processing all exits using rdtsc function.
4. In cpuid.c, created a new cpuid leaf in **kvm_emulate_cpuid** function which reads the no_of_exits into % eax and moves high 32 bits of cpu_cycles into %ebx and low 32 bits of cpu_cycles into %ecx when % eax =0xFFFFFFFF.
5. Else, **kvm_emulate_cpuid** function executes the default code.
6. Compile the code

```
$ sudo make -j modules M=arch/kvm/x86
```

7. Executed the below commands to load and unload kvm kernel modules and kvm intel modules.

```
$ sudo rmmod arch/x86/kvm/kvm-intel.ko
$ sudo rmmod arch/x86/kvm/kvm.ko
$ sudo insmod arch/x86/kvm/kvm.ko
$ sudo insmod arch/x86/kvm/kvm-intel.ko
```

Nested VM Setup:

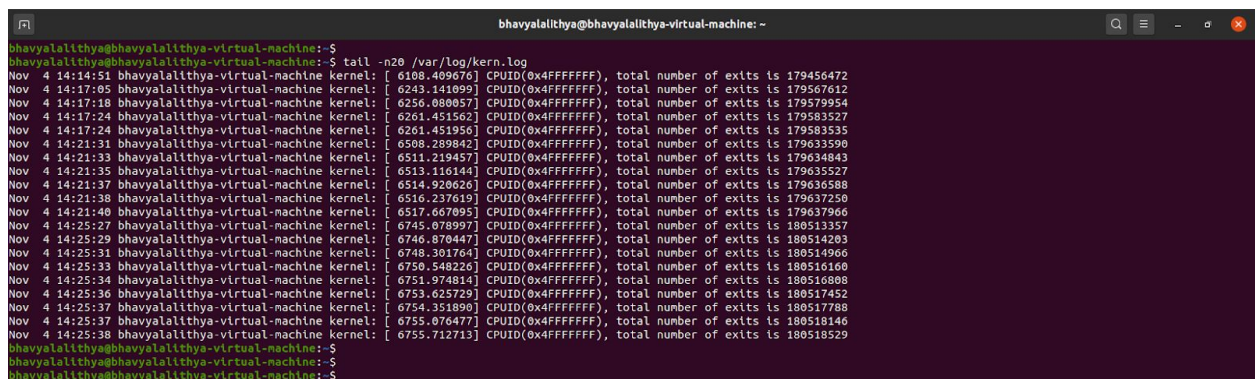
1. Install virt-manager

```
$ sudo apt-get install virt-manager
$ sudo apt-get install libvirt-bin libvirt-doc
$ sudo apt-get install qemu-system
$ sudo virt-manager
```

2. Download Ubuntu iso image
3. Finish the installation process following all the setup prompts(enable nested VM to prevent further warnings) and configure the inner VM.
4. Build the test code inside the inner VM to test the changes made in the Outer VM kernel and compile it.

Screenshots:

Kernel log in outer VM

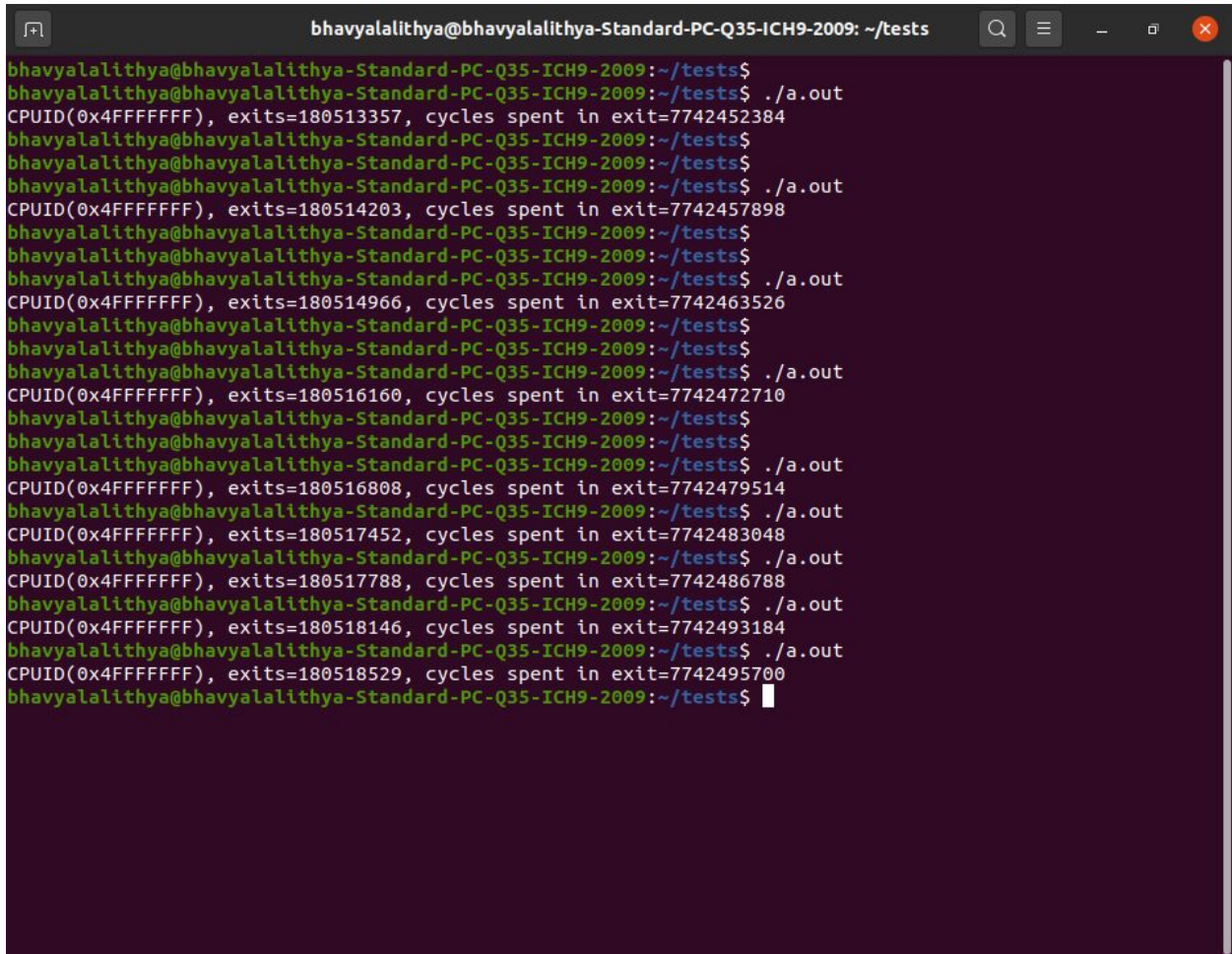


```
bhavyalalithya@bhavyalalithya-virtual-machine: ~
bhavyalalithya@bhavyalalithya-virtual-machine:~$ tail -n20 /var/log/kern.log
Nov  4 14:14:51 bhavyalalithya-virtual-machine kernel: [ 6108.409676] CPUID(0x4FFFFFFF), total number of exits is 179456472
Nov  4 14:17:05 bhavyalalithya-virtual-machine kernel: [ 6243.141099] CPUID(0x4FFFFFFF), total number of exits is 179567612
Nov  4 14:17:18 bhavyalalithya-virtual-machine kernel: [ 6256.080057] CPUID(0x4FFFFFFF), total number of exits is 179579954
Nov  4 14:17:24 bhavyalalithya-virtual-machine kernel: [ 6261.451562] CPUID(0x4FFFFFFF), total number of exits is 179583527
Nov  4 14:17:24 bhavyalalithya-virtual-machine kernel: [ 6261.451956] CPUID(0x4FFFFFFF), total number of exits is 179583535
Nov  4 14:21:31 bhavyalalithya-virtual-machine kernel: [ 6500.289042] CPUID(0x4FFFFFFF), total number of exits is 179633500
Nov  4 14:21:33 bhavyalalithya-virtual-machine kernel: [ 6511.219457] CPUID(0x4FFFFFFF), total number of exits is 179634843
Nov  4 14:21:35 bhavyalalithya-virtual-machine kernel: [ 6513.116144] CPUID(0x4FFFFFFF), total number of exits is 179635527
Nov  4 14:21:37 bhavyalalithya-virtual-machine kernel: [ 6514.920626] CPUID(0x4FFFFFFF), total number of exits is 179636588
Nov  4 14:21:38 bhavyalalithya-virtual-machine kernel: [ 6516.237619] CPUID(0x4FFFFFFF), total number of exits is 179637250
Nov  4 14:21:40 bhavyalalithya-virtual-machine kernel: [ 6517.667095] CPUID(0x4FFFFFFF), total number of exits is 179637966
Nov  4 14:25:27 bhavyalalithya-virtual-machine kernel: [ 6745.078997] CPUID(0x4FFFFFFF), total number of exits is 180513357
Nov  4 14:25:29 bhavyalalithya-virtual-machine kernel: [ 6746.876447] CPUID(0x4FFFFFFF), total number of exits is 180514203
Nov  4 14:25:31 bhavyalalithya-virtual-machine kernel: [ 6748.301764] CPUID(0x4FFFFFFF), total number of exits is 180514966
Nov  4 14:25:33 bhavyalalithya-virtual-machine kernel: [ 6750.548226] CPUID(0x4FFFFFFF), total number of exits is 180516160
Nov  4 14:25:34 bhavyalalithya-virtual-machine kernel: [ 6751.974814] CPUID(0x4FFFFFFF), total number of exits is 180516808
Nov  4 14:25:36 bhavyalalithya-virtual-machine kernel: [ 6753.625729] CPUID(0x4FFFFFFF), total number of exits is 180517452
Nov  4 14:25:37 bhavyalalithya-virtual-machine kernel: [ 6754.351890] CPUID(0x4FFFFFFF), total number of exits is 180517788
Nov  4 14:25:37 bhavyalalithya-virtual-machine kernel: [ 6755.076477] CPUID(0x4FFFFFFF), total number of exits is 180518146
Nov  4 14:25:38 bhavyalalithya-virtual-machine kernel: [ 6755.712713] CPUID(0x4FFFFFFF), total number of exits is 180518529
bhavyalalithya@bhavyalalithya-virtual-machine:~$
bhavyalalithya@bhavyalalithya-virtual-machine:~$
bhavyalalithya@bhavyalalithya-virtual-machine:~$
```

Before boot

```
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ gcc test_cpuid.c
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179633590, cycles spent in exit=7705549436
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179634843, cycles spent in exit=7705553288
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179635527, cycles spent in exit=7705556696
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179636588, cycles spent in exit=7705561288
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179637250, cycles spent in exit=7705565376
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=179637966, cycles spent in exit=7705568660
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
```

After boot

A terminal window titled 'bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests' showing the execution of a program named 'a.out'. The program outputs CPUID(0x4FFFFFFF), exits=..., cycles spent in exit=... for each run. The exit counts are: 180513357, 180514203, 180514966, 180516160, 180516808, 180517452, 180517788, 180518146, 180518529. The cycles spent are: 7742452384, 7742457898, 7742463526, 7742472710, 7742479514, 7742483048, 7742486788, 7742493184, 7742495700.

```
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180513357, cycles spent in exit=7742452384
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180514203, cycles spent in exit=7742457898
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180514966, cycles spent in exit=7742463526
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180516160, cycles spent in exit=7742472710
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180516808, cycles spent in exit=7742479514
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180517452, cycles spent in exit=7742483048
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180517788, cycles spent in exit=7742486788
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180518146, cycles spent in exit=7742493184
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$ ./a.out
CPUID(0x4FFFFFFF), exits=180518529, cycles spent in exit=7742495700
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009: ~/tests$
```

Observations:

Does the number of exits increase at a stable rate? Or are there more exits performed during certain VM operations?

From the last five command outputs (shown in the 'after boot' screenshot), we can see that the difference between exit counters is not stable (i.e., sometimes the difference is ~600 & sometimes it is ~400).

How many exits does a full VM boot entail?

From the above screenshots, we can observe that VM boot entails ~870,000 exits.