CMPE283 - Assignment 2
Sangwon Song

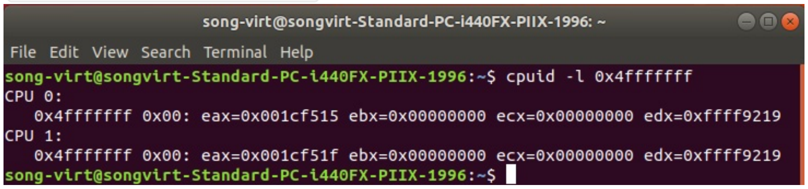
Q1. For each member in your team, provide 1 paragraph detailing what parts of the lab that member implemented / researched. (You may skip this question if you are doing the lab by yourself).

This part is skipped. I did the assginment by myself

Q2. Describe in detail the steps you used to complete the assignment. Consider your reader to be someone skilled in software development but otherwise unfamiliar with the assignment. Good answers to this question will be recipes that someone can follow to reproduce your development steps.

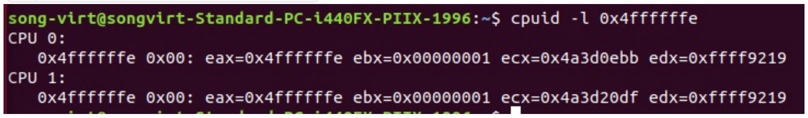
Note: I may decide to follow these instructions for random assignments, so you should make sure they are accurate.

- Pre-condition: We need to use the Assignment 1 environment. I have the information about Assignment 1 in my linux github repository.
- Check the version of the linux kenel by `uname -r` command. It should be the same as Assignment 1.
  - In my case, it was `5.4.0-rc+1`.
- Modify the code in `cpuid.c` and `vmx.c` in the linux repository.
  - Detailed modification is described in the git diff file in my github.
- Remake the module by following commands
  - `make modules && make moduels_install && make install`
- Reboot by `reboot` command
- Run virt-manager
- In the guest VM, install cpuid package by the command:
  - `sudo apt install cpuid`
- Run cpuid command with leaf in the guest VM
  - `cpuid -l 0x4fffffff`
  - `cpuid -l 0x4ffffffe`
- Check the outputs in the guest VM
  - `cpuid -l 0x4fffffff` output


song-virt@songvirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x001cf515 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x001cf51f ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$
```

    - **Note:** 0x4FFFFFFF leaf contains total number of exits in %eax.
  - `cpuid -l 0x4ffffffe` output



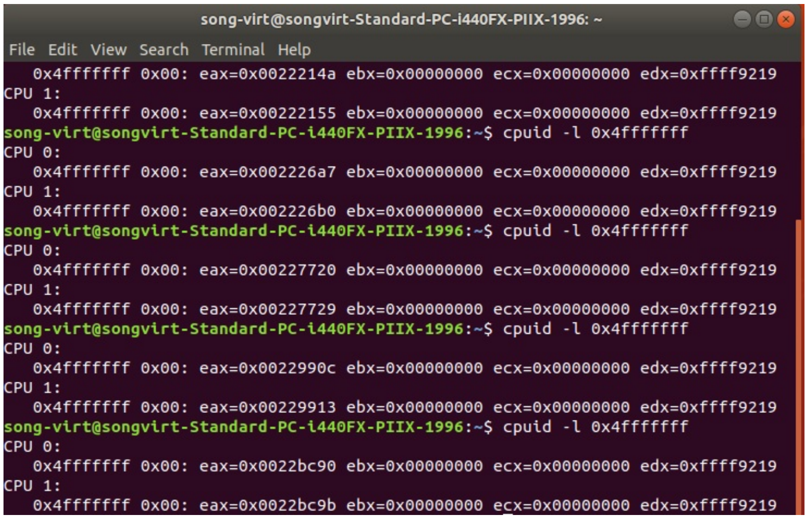
```
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4ffffffe
CPU 0:
   0x4ffffffe 0x00: eax=0x4ffffffe ebx=0x00000001 ecx=0x4a3d0ebb edx=0xffff9219
CPU 1:
   0x4ffffffe 0x00: eax=0x4ffffffe ebx=0x00000001 ecx=0x4a3d20df edx=0xffff9219
```

    - **Note:** 0x4FFFFFFE leaf contains the high 32 bits of the total time spent processing all exits in %ebx and the low 32 bits in %ecx. I manually incremented the eixt cycles to check both ebx and ecx have correct values. In addition, ebx contains some numerical values when ecs overflows.

For **Q3 & Q4**, since the requirements are about `CPUID 0x4FFFFFFD and 0x4FFFFFFC` as modified in class, I will answer those questions more correctly by Assignment 3 deadline. For assignment 2, I only implemented for 0x4FFFFFFF and 0x4FFFFFFE leaves.

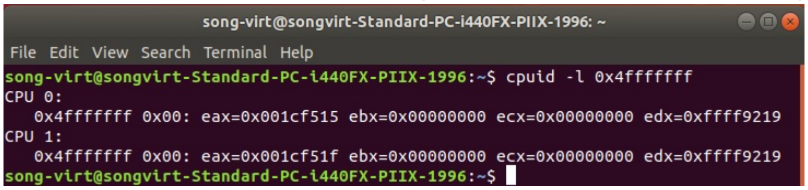
Q3. Comment on the frequency of exits - does the number of exits increase at a stable rate? Or are there more exits performed during certain VM operations? Approximately how many exits does a full VM boot entail?

When I look at the eax values in the guest VM with `0x4fffffff` leaf, the number of exits increases, but not in a stable rate as in figures below. Some VM operations generates more VM exits, such as turning on and off the guest VM generates more exits than other operations.


song-virt@songvirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
   0x4fffffff 0x00: eax=0x0022214a ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x00222155 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x002226a7 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x002226b0 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x00227720 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x00227729 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x0022990c ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x00229913 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x0022bc90 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x0022bc9b ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
```

As soon as I booted the guest VM, I had approximately 1900000 exits. It was more than I expected because I turned on and off the guest VM few times for testing the module.


song-virt@songvirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4fffffff
CPU 0:
   0x4fffffff 0x00: eax=0x001cf515 ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
CPU 1:
   0x4fffffff 0x00: eax=0x001cf51f ebx=0x00000000 ecx=0x00000000 edx=0xffff9219
song-virt@songvirt-Standard-PC-i440FX-PIIX-1996:~$
```

Q4. Of the exit types defined in the SDM, which are the most frequent? Least?
Since I implemented for `0x4FFFFFFF` and `0x4FFFFFFE` for the assignment 2, I will answer this question when I implement for `0x4FFFFFFC` and `0x4FFFFFFD` leaves.