CMPE283- Assignment 1

Student ID: 015293460 Name: Parvathi Pai
Student ID:015304393 Name: Shreya Ghotankar

1. For each member in your team, provide 1 paragraph detailing what parts of the lab that member implemented / researched.
   - **Parvathi Pai**:
     - Cloned the Kernel code from GitHub repository.
     - Identified the information from SDM.
     - Updated the code in cmpe283-1.c for the MSRs 0x482, 0x48B, 0x483, 0x484
     - Generated the desired output and took snapshots of it.
     - Created the initial documentation.

   - **Shreya Ghotankar**:
     - Cloned the Kernel code from GitHub repository.
     - Compiled the Kernel code
     - Re-built and tested the modified cmpe283-1.c code.
     - Added snapshots of output after testing.
     - Updated the documentation.

2. Steps followed –

   1) Install VMware Fusion (Mac OS) /Workstation (Windows) and Ubuntu
   2) Create a VM machine that will run on Ubuntu.
   3) Install git: *sudo apt-get install git*
   4) Install make: *sudo apt-get install make*
   5) Install gcc: *sudo apt-get install gcc*
   6) Clone the Kernel code from GitHub: *git clone https://github.com/torvalds/linux.git*

   Kernel Code Compilation :
   - sudo apt-get install build-essential kernel-package fakeroot libncurses5-dev libssl-dev ccache bison flex libelf-dev
   - uname -a
   - cp -v /boot/config-5.4.0-52-generic ./.config
   - make oldconfig
   - make -j
   - sudo make modules
   - sudo make modules_install

- sudo make install
- reboot
- uname -a

```
sghotankar@ubuntu:~$ uname -a
Linux ubuntu 5.9.0+ #1 SMP Fri Oct 23 11:03:42 PDT 2020 x86_64 x86_64 x86_64 GNU
/Linux
```

7) cmpe283-1.c code changes:
   - Downloaded the Makefile and cmpe283-1.c file from the SJSU canvas
   - Build the file using *make*

```
ava@ubuntu:~/Documents/assignment$ make
ake -C /lib/modules/5.4.0-51-generic/build M=/home/pava/Documents/assi
ules
ake[1]: Entering directory '/usr/src/linux-headers-5.4.0-51-generic'
 CC [M]  /home/pava/Documents/assignment/cmpe283-1.o
 Building modules, stage 2.
 MODPOST 1 modules
ARNING: modpost: missing MODULE_LICENSE() in /home/pava/Documents/assi
e283-1.o
ee include/linux/module.h for more information
 CC [M]  /home/pava/Documents/assignment/cmpe283-1.mod.o
 LD [M]  /home/pava/Documents/assignment/cmpe283-1.ko
ake[1]: Leaving directory '/usr/src/linux-headers-5.4.0-51-generic'
```

   - After building the file check if there is kernel object file is created.

```
pava@ubuntu:~/Documents/assignment$ ls -latr .
total 116
drwxr-xr-x 5 pava pava  4096 Oct 17 12:22 ..
-rw-rw-r-- 1 pava pava  2404 Oct 22 07:48 cmpe283-1.c
-rw-rw-r-- 1 pava pava   161 Oct 22 07:48 Makefile
-rw-rw-r-- 1 pava pava  4024 Oct 22 07:50 cmpe283-1.o
-rw-rw-r-- 1 pava pava 30967 Oct 22 07:50 .cmpe283-1.o.cmd
-rw-rw-r-- 1 pava pava    45 Oct 22 07:50 modules.order
-rw-rw-r-- 1 pava pava   162 Oct 22 07:50 .cmpe283-1.mod.cmd
-rw-rw-r-- 1 pava pava    45 Oct 22 07:50 cmpe283-1.mod
-rw-rw-r-- 1 pava pava     0 Oct 22 07:50 Module.symvers
-rw-rw-r-- 1 pava pava   560 Oct 22 07:50 cmpe283-1.mod.c
-rw-rw-r-- 1 pava pava  2808 Oct 22 07:50 cmpe283-1.mod.o
-rw-rw-r-- 1 pava pava 31180 Oct 22 07:50 .cmpe283-1.mod.o.cmd
-rw-rw-r-- 1 pava pava   290 Oct 22 07:50 .cmpe283-1.ko.cmd
-rw-rw-r-- 1 pava pava  5808 Oct 22 07:50 cmpe283-1.ko
drwxrwxr-x 2 pava pava  4096 Oct 22 07:50 .
```

   - After *sudo insmod ./cmpe283-1.ko* and *dmesg* the configuration of kernel is –

Output of pinbased controls

```
[ 2000.241138] Pinbased Controls MSR: 0x3f00000016
[ 2000.241139]   External Interrupt Exiting: Can set=Yes, Can clear=Yes
[ 2000.241140]   NMI Exiting: Can set=Yes, Can clear=Yes
[ 2000.241140]   Virtual NMIs: Can set=Yes, Can clear=Yes
[ 2000.241141]   Activate VMX Preemption Timer: Can set=No, Can clear=Yes
[ 2000.241141]   Process Posted Interrupts: Can set=No, Can clear=Yes
```

- Then in the cmpe283-1.c file added the configuration of the various controls and build the file.

- To rebuild the file use commands –
    - sudo rmmod cmpe283-1
    - sudo insmod ./cmpe283-1.ko,
    - dmesg

Output:

1) Output of Procbased controls

```
[ 6145.761223] Procbased Controls MSR: 0xfff9fffe0401e172
[ 6145.761223]   Interrupt-window exiting: Can set=Yes, Can clear=Yes
[ 6145.761224]   Use TSC offsetting: Can set=Yes, Can clear=Yes
[ 6145.761224]   HLT exiting: Can set=Yes, Can clear=Yes
[ 6145.761225]   INVLPG exiting: Can set=Yes, Can clear=Yes
[ 6145.761225]   MWAIT exiting: Can set=Yes, Can clear=Yes
[ 6145.761225]   RDPMC exiting: Can set=Yes, Can clear=Yes
[ 6145.761226]   RDTSC exiting: Can set=Yes, Can clear=Yes
[ 6145.761226]   CR3-load exiting: Can set=Yes, Can clear=No
[ 6145.761227]   CR3-store exiting: Can set=Yes, Can clear=No
[ 6145.761227]   CR8-load exiting: Can set=Yes, Can clear=Yes
[ 6145.761250]   CR8-store exiting: Can set=Yes, Can clear=Yes
[ 6145.761251]   Use TPR shadow: Can set=Yes, Can clear=Yes
[ 6145.761251]   NMI-window exiting: Can set=Yes, Can clear=Yes
[ 6145.761251]   MOV-DR exiting: Can set=Yes, Can clear=Yes
[ 6145.761252]   Unconditional I/O: Can set=Yes, Can clear=Yes
[ 6145.761252]   Use I/O bitmaps: Can set=Yes, Can clear=Yes
[ 6145.761253]   Monitor trap flag: Can set=Yes, Can clear=Yes
[ 6145.761253]   Use MSR Bitmaps: Can set=Yes, Can clear=Yes
[ 6145.761253]   MONITOR exiting: Can set=Yes, Can clear=Yes
[ 6145.761254]   PAUSE exiting: Can set=Yes, Can clear=Yes
[ 6145.761254]   Activate secondary controls: Can set=Yes, Can clear=Yes
```

After testing:

```
[ 7854.270069] Procbased Controls MSR: 0xfff9fffe0401e172
[ 7854.270070]   Interrupt-window exiting: Can set=Yes, Can clear=Yes
[ 7854.270071]   Use TSC offsetting: Can set=Yes, Can clear=Yes
[ 7854.270072]   HLT exiting: Can set=Yes, Can clear=Yes
[ 7854.270073]   INVLPG exiting: Can set=Yes, Can clear=Yes
[ 7854.270074]   MWAIT exiting: Can set=Yes, Can clear=Yes
[ 7854.270075]   RDPMC exiting: Can set=Yes, Can clear=Yes
[ 7854.270076]   RDTSC exiting: Can set=Yes, Can clear=Yes
[ 7854.270077]   CR3-load exiting: Can set=Yes, Can clear=No
[ 7854.270078]   CR3-store exiting: Can set=Yes, Can clear=No
[ 7854.270079]   CR8-load exiting: Can set=Yes, Can clear=Yes
[ 7854.270080]   CR8-store exiting: Can set=Yes, Can clear=Yes
[ 7854.270081]   Use TPR shadow: Can set=Yes, Can clear=Yes
[ 7854.270082]   NMI-window exiting: Can set=Yes, Can clear=Yes
[ 7854.270083]   MOV-DR exiting: Can set=Yes, Can clear=Yes
[ 7854.270084]   Unconditional I/O: Can set=Yes, Can clear=Yes
[ 7854.270085]   Use I/O bitmaps: Can set=Yes, Can clear=Yes
[ 7854.270086]   Monitor trap flag: Can set=Yes, Can clear=Yes
[ 7854.270087]   Use MSR Bitmaps: Can set=Yes, Can clear=Yes
[ 7854.270088]   MONITOR exiting: Can set=Yes, Can clear=Yes
[ 7854.270089]   PAUSE exiting: Can set=Yes, Can clear=Yes
[ 7854.270090]   Activate secondary controls: Can set=Yes, Can clear=Yes
```

2) Secondary Procbased controls

```
[ 6145.761256] Secondary Procbased Controls MSR: 0x553cfe00000000
[ 6145.761256]   Virtualize APIC accesses: Can set=No, Can clear=Yes
[ 6145.761257]   Enable EPT: Can set=Yes, Can clear=Yes
[ 6145.761257]   Descriptor-table exiting: Can set=Yes, Can clear=Yes
[ 6145.761257]   Enable RDTSCP: Can set=Yes, Can clear=Yes
[ 6145.761258]   Virtualize x2APIC mode: Can set=Yes, Can clear=Yes
[ 6145.761258]   Enable VPID: Can set=Yes, Can clear=Yes
[ 6145.761259]   WBINVD exiting: Can set=Yes, Can clear=Yes
[ 6145.761259]   Unrestricted guest: Can set=Yes, Can clear=Yes
[ 6145.761260]   APIC-register virtualization: Can set=No, Can clear=Yes
[ 6145.761260]   Virtual-interrupt delivery: Can set=No, Can clear=Yes
[ 6145.761261]   PAUSE-loop exiting: Can set=Yes, Can clear=Yes
[ 6145.761261]   RDRAND exiting: Can set=Yes, Can clear=Yes
[ 6145.761261]   Enable INVPCID: Can set=Yes, Can clear=Yes
[ 6145.761262]   Enable VM functions: Can set=Yes, Can clear=Yes
[ 6145.761262]   VMCS shadowing: Can set=No, Can clear=Yes
[ 6145.761263]   Enable ENCLS exiting: Can set=No, Can clear=Yes
[ 6145.761263]   RDSEED exiting: Can set=Yes, Can clear=Yes
[ 6145.761263]   Enable PML: Can set=No, Can clear=Yes
[ 6145.761264]   EPT-violation: Can set=Yes, Can clear=Yes
[ 6145.761264]   Conceal VMX nonroot operation from Intel PT: Can set=No, Can clear=Yes
[ 6145.761265]   Enable XSAVES/XRSTORS: Can set=Yes, Can clear=Yes
[ 6145.761265]   Mode-based execute control for EPT: Can set=Yes, Can clear=Yes
[ 6145.761266]   Sub-page Write Permissions for EPT: Can set=No, Can clear=Yes
[ 6145.761266]   Intel PT Uses Guest Physical Addresses: Can set=No, Can clear=Yes
[ 6145.761267]   Use TSC scaling: Can set=No, Can clear=Yes
[ 6145.761267]   Enable user wait and pause: Can set=No, Can clear=Yes
[ 6145.761268]   Interrupt-window exiting: Can set=Yes, Can clear=Yes
```

After testing:

```
[ 7854.270092] Secondary Procbased Controls MSR: 0x553cfe00000000
[ 7854.270093]   Virtualize APIC accesses: Can set=No, Can clear=Yes
[ 7854.270094]   Enable EPT: Can set=Yes, Can clear=Yes
[ 7854.270095]   Descriptor-table exiting: Can set=Yes, Can clear=Yes
[ 7854.270096]   Enable RDTSCP: Can set=Yes, Can clear=Yes
[ 7854.270097]   Virtualize x2APIC mode: Can set=Yes, Can clear=Yes
[ 7854.270098]   Enable VPID: Can set=Yes, Can clear=Yes
[ 7854.270099]   WBINVD exiting: Can set=Yes, Can clear=Yes
[ 7854.270100]   Unrestricted guest: Can set=Yes, Can clear=Yes
[ 7854.270101]   APIC-register virtualization: Can set=No, Can clear=Yes
[ 7854.270102]   Virtual-interrupt delivery: Can set=No, Can clear=Yes
[ 7854.270103]   PAUSE-loop exiting: Can set=Yes, Can clear=Yes
[ 7854.270104]   RDRAND exiting: Can set=Yes, Can clear=Yes
[ 7854.270105]   Enable INVPCID: Can set=Yes, Can clear=Yes
[ 7854.270106]   Enable VM functions: Can set=Yes, Can clear=Yes
[ 7854.270107]   VMCS shadowing: Can set=No, Can clear=Yes
[ 7854.270108]   Enable ENCLS exiting: Can set=No, Can clear=Yes
[ 7854.270109]   RDSEED exiting: Can set=Yes, Can clear=Yes
[ 7854.270110]   Enable PML: Can set=No, Can clear=Yes
[ 7854.270111]   EPT-violation: Can set=Yes, Can clear=Yes
[ 7854.270112]   Conceal VMX nonroot operation from Intel PT: Can set=No, Can clear=Yes
[ 7854.270113]   Enable XSAVES/XRSTORS: Can set=Yes, Can clear=Yes
[ 7854.270114]   Mode-based execute control for EPT: Can set=Yes, Can clear=Yes
[ 7854.270115]   Sub-page Write Permissions for EPT: Can set=No, Can clear=Yes
[ 7854.270116]   Intel PT Uses Guest Physical Addresses: Can set=No, Can clear=Yes
[ 7854.270117]   Use TSC scaling: Can set=No, Can clear=Yes
[ 7854.270119]   Enable user wait and pause: Can set=No, Can clear=Yes
[ 7854.270120]   Enable ENCLV exiting: Can set=No, Can clear=Yes
```

3) VM Exit controls

```
[ 6145.761268] Exit Controls MSR: 0x3fffff00036dff
[ 6145.761269]   Save debug controls: Can set=Yes, Can clear=No
[ 6145.761269]   Host addressspace size: Can set=Yes, Can clear=Yes
[ 6145.761270]   Load IA32_PERF_GLOB AL_CTRL: Can set=Yes, Can clear=Yes
[ 6145.761270]   Acknowledge interrupt on exit: Can set=Yes, Can clear=Yes
[ 6145.761271]   Save IA32_PAT: Can set=Yes, Can clear=Yes
[ 6145.761271]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[ 6145.761272]   Save IA32_EEFR: Can set=Yes, Can clear=Yes
[ 6145.761272]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[ 6145.761272]   Save VMXpreemption timer value: Can set=No, Can clear=Yes
[ 6145.761273]   Clear IA32_BNDCFGS: Can set=No, Can clear=Yes
[ 6145.761273]   Conceal VM exits from Intel PT: Can set=No, Can clear=Yes
[ 6145.761274]   Clear IA32_RTIT_CTL: Can set=No, Can clear=Yes
[ 6145.761274]   Load CET state: Can set=No, Can clear=Yes
[ 6145.761275]   Load PKRS: Can set=No, Can clear=Yes
```

After testing:

```
[ 7854.270121] Exit Controls MSR: 0x3fffff00036dff
[ 7854.270122]   Save debug controls: Can set=Yes, Can clear=No
[ 7854.270123]   Host addressspace size: Can set=Yes, Can clear=Yes
[ 7854.270124]   Load IA32_PERF_GLOB AL_CTRL: Can set=Yes, Can clear=Yes
[ 7854.270125]   Acknowledge interrupt on exit: Can set=Yes, Can clear=Yes
[ 7854.270126]   Save IA32_PAT: Can set=Yes, Can clear=Yes
[ 7854.270128]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[ 7854.270128]   Save IA32_EFER: Can set=Yes, Can clear=Yes
[ 7854.270129]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[ 7854.270130]   Save VMXpreemption timer value: Can set=No, Can clear=Yes
[ 7854.270131]   Clear IA32_BNDCFGS: Can set=No, Can clear=Yes
[ 7854.270132]   Conceal VM exits from Intel PT: Can set=No, Can clear=Yes
[ 7854.270133]   Clear IA32_RTIT_CTL: Can set=No, Can clear=Yes
[ 7854.270135]   Load CET state: Can set=No, Can clear=Yes
[ 7854.270136]   Load PKRS: Can set=No, Can clear=Yes
```

4) VM Entry controls

```
[ 6145.761275] Entry Controls MSR: 0xf3ff000011ff
[ 6145.761276]   Load debug controls: Can set=Yes, Can clear=No
[ 6145.761276]   IA-32e mode guest: Can set=Yes, Can clear=Yes
[ 6145.761277]   Entry to SMM: Can set=No, Can clear=Yes
[ 6145.761277]   Deactivate dual-monitor treatment: Can set=No, Can clear=Yes
[ 6145.761278]   Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[ 6145.761278]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[ 6145.761278]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[ 6145.761279]   Load IA32_BNDCFGS: Can set=No, Can clear=Yes
[ 6145.761279]   Conceal VM entries from Intel PT: Can set=No, Can clear=Yes
[ 6145.761280]   Load IA32_RTIT_CTL: Can set=No, Can clear=Yes
[ 6145.761280]   Load CET state: Can set=No, Can clear=Yes
[ 6145.761281]   Load PKRS: Can set=No, Can clear=Yes
```

After testing:

```
[ 7854.270137] Entry Controls MSR: 0xf3ff000011ff
[ 7854.270138]   Load debug controls: Can set=Yes, Can clear=No
[ 7854.270139]   IA-32e mode guest: Can set=Yes, Can clear=Yes
[ 7854.270140]   Entry to SMM: Can set=No, Can clear=Yes
[ 7854.270141]   Deactivate dual-monitor treatment: Can set=No, Can clear=Yes
[ 7854.270142]   Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[ 7854.270143]   Load IA32_PAT: Can set=Yes, Can clear=Yes
[ 7854.270144]   Load IA32_EFER: Can set=Yes, Can clear=Yes
[ 7854.270145]   Load IA32_BNDCFGS: Can set=No, Can clear=Yes
[ 7854.270146]   Conceal VM entries from Intel PT: Can set=No, Can clear=Yes
[ 7854.270147]   Load IA32_RTIT_CTL: Can set=No, Can clear=Yes
[ 7854.270148]   Load CET state: Can set=No, Can clear=Yes
[ 7854.270149]   Load PKRS: Can set=No, Can clear=Yes
shreyaghotankar@ubuntu:~/Assignments$
```