CMPE283 : Virtualization

Assignment 1: Discovering VMX Features

Krishna K Jha (SJSU ID: 013803894)

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.

**Ans**:

The module necessary for this assignment was developed on Mac O/S

* Download and install VMWare Fusion on Mac.
* Download the image(iso) of 64 bit Ubuntu.
* Create Ubuntu VM using the image downloaded in setp 2. Allocated 8 GB of memory, 2 VCPU's, 200 GB of SSD storage and enabled nested virtualization under CPU settings.
* Run the Ubuntu VM.
* Execute cat /proc/cpuinfo | more to verify that nested virtualization is enabled in VM machine.

The following procedure describes the steps followed to develop and test the kernel module necessary for this assignment:

1. Clone the kernel sources from the master linux git repository:

>> git clone <https://github.com/torvalds/linux.git>

This clones the linux kernel sources to a directory named "linux".

1. Change to the cloned directory:

>> cd linux

# Module development

1. Create a new directory named “cmpe283” in the previously cloned “linux” source folder.

>> mkdir cmpe283

1. Copy the template “cmpe283-1.c” file and the template “Makefile” provided by the professor to the cmpe283 directory.
2. The functionality to query all the other MSRs as explained in the assignment description is added to cmpe283-1.c.

* By referring SDM, created structures with name (description) and bit positions for procbased, secondary procbased, entry and exit controls.
* In order to detect and print VMX capabilities of CPU, the function report\_capability ( ) is called with appropriate parameters passed in order to print pinbased, procbased, entry and exit controls.
* In order to determine if true controls are available, a new function has been written to check the 55th bit of IA32\_VMX\_BASIC MSR. If this bit is set, then true controls are available and another function will be called to print the corresponding true VMX capabilities.
* In order to determine if Secondary Procbased controls are available, , a new function has been written to check 63rd bit of IA32\_VMX\_PROCBASED MSR. If this bit is set, then secondary procbased controls are available and another function will be called to print the corresponding secondary procbased capabilities.

1. Change to the cmpe283 directory:

>> cd cmpe283

1. Build the module using the following command inside the cmpe283 directory:

>> make all

1. Load and unload the module using the following commands:

When a module is inserted into the kernel, the module\_init macro will be invoked, which will call the function init\_module.

Similarly, when the module is removed with rmmod, module\_exit macro will be invoked, which will call the cleanup\_module.

>> sudo insmod ./cmpe283­1.ko

1. The VMX features must now be logged in the kernel log and can be verified using the dmesg command:

>> dmesg

For example, on the VM which was used to test the developed module, the following info was printed:

[ 424.356535] CMPE 283 Assignment 1 Module Start

[ 424.356538] Pinbased Controls MSR: 0x3f00000016

[ 424.356538] External Interrupt Exiting: Can set=Yes, Can clear=Yes

[ 424.356539] NMI Exiting: Can set=Yes, Can clear=Yes

[ 424.356540] Virtual NMIs: Can set=Yes, Can clear=Yes

[ 424.356540] Activate VMX Preemption Timer: Can set=No, Can clear=Yes

[ 424.356541] Process Posted Interrupts: Can set=No, Can clear=Yes

[ 424.356542] Procbased Controls MSR: 0xf7f9fffe2401e5f2

[ 424.356543] Interrupt-window exiting: Can set=Yes, Can clear=Yes

[ 424.356543] Use TSC offsetting : Can set=Yes, Can clear=Yes

[ 424.356544] HLT exiting : Can set=Yes, Can clear=No

[ 424.356544] INVLPG exiting : Can set=Yes, Can clear=Yes

[ 424.356545] MWAIT exiting: Can set=Yes, Can clear=No

[ 424.356545] RDPMC exiting: Can set=Yes, Can clear=Yes

[ 424.356546] RDTSC exiting: Can set=Yes, Can clear=Yes

[ 424.356547] CR3-load exiting: Can set=Yes, Can clear=No

[ 424.356547] CR3-store exiting: Can set=Yes, Can clear=No

[ 424.356548] CR8-load exiting: Can set=Yes, Can clear=Yes

[ 424.356548] CR8-store exiting: Can set=Yes, Can clear=Yes

[ 424.356549] Use TPR shadow : Can set=Yes, Can clear=Yes

[ 424.356549] NMI-window exiting: Can set=Yes, Can clear=Yes

[ 424.356550] MOV-DR exiting: Can set=Yes, Can clear=Yes

[ 424.356550] Unconditional I/O exiting: Can set=Yes, Can clear=Yes

[ 424.356551] Use I/O bitmaps : Can set=Yes, Can clear=Yes

[ 424.356551] Monitor trap flag : Can set=No, Can clear=Yes

[ 424.356552] Use MSR bitmaps: Can set=Yes, Can clear=Yes

[ 424.356552] MONITOR exiting: Can set=Yes, Can clear=No

[ 424.356553] PAUSE exiting: Can set=Yes, Can clear=Yes

[ 424.356554] Activate secondary controls: Can set=Yes, Can clear=Yes

[ 424.356555] \*\*\*\* Secondary procbased controls are available !!! \*\*\*\*

[ 424.356557] Secondary procbased Controls MSR: 0x10182e00000000

[ 424.356557] Virtualize APIC accesses: Can set=No, Can clear=Yes

[ 424.356558] Enable EPT : Can set=Yes, Can clear=Yes

[ 424.356558] Descriptor-table exiting : Can set=Yes, Can clear=Yes

[ 424.356559] Enable RDTSCP : Can set=Yes, Can clear=Yes

[ 424.356559] Virtualize x2APIC mode: Can set=No, Can clear=Yes

[ 424.356560] Enable VPID: Can set=Yes, Can clear=Yes

[ 424.356560] WBINVD exiting: Can set=No, Can clear=Yes

[ 424.356561] Unrestricted guest: Can set=No, Can clear=Yes

[ 424.356561] APIC-register virtualization: Can set=No, Can clear=Yes

[ 424.356562] Virtual-interrupt delivery: Can set=No, Can clear=Yes

[ 424.356562] PAUSE-loop exiting: Can set=No, Can clear=Yes

[ 424.356563] RDRAND exiting : Can set=Yes, Can clear=Yes

[ 424.356564] Enable INVPCID: Can set=Yes, Can clear=Yes

[ 424.356564] Enable VM functions: Can set=No, Can clear=Yes

[ 424.356565] VMCS shadowing: Can set=No, Can clear=Yes

[ 424.356565] Enable ENCLS exiting : Can set=No, Can clear=Yes

[ 424.356566] RDSEED exiting : Can set=No, Can clear=Yes

[ 424.356566] Enable PML: Can set=No, Can clear=Yes

[ 424.356567] EPT-violation #VE: Can set=No, Can clear=Yes

[ 424.356567] Conceal VMX non-root operation from Intel PT: Can set=No, Can clear=Yes

[ 424.356569] Enable XSAVES/XRSTORS: Can set=Yes, Can clear=Yes

[ 424.356570] Mode-based execution control for EPT: Can set=No, Can clear=Yes

[ 424.356570] Use TSC scaling: Can set=No, Can clear=Yes

[ 424.356573] Entry Controls MSR: 0x1d3ff000011ff

[ 424.356574] Load debug controls: Can set=Yes, Can clear=No

[ 424.356574] IA-32e mode guest: Can set=Yes, Can clear=Yes

[ 424.356575] Entry to SMM: Can set=No, Can clear=Yes

[ 424.356575] Deactivate dual-monitor treatment : Can set=No, Can clear=Yes

[ 424.356576] Load IA32\_PERF\_GLOBAL\_CTRL: Can set=No, Can clear=Yes

[ 424.356576] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356577] Load IA32\_EFER: Can set=Yes, Can clear=Yes

[ 424.356577] Load IA32\_BNDCFGS: Can set=Yes, Can clear=Yes

[ 424.356578] Conceal VM entries from intel PT: Can set=No, Can clear=Yes

[ 424.356580] Exit Controls MSR: 0xbfefff00036fff

[ 424.356581] Save debug controls: Can set=Yes, Can clear=No

[ 424.356582] Host address-space size: Can set=Yes, Can clear=No

[ 424.356582] Load IA32\_PERF\_GLOB AL\_CTRL: Can set=No, Can clear=Yes

[ 424.356583] Acknowledge interrupt on exit : Can set=Yes, Can clear=Yes

[ 424.356583] Save IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356584] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356584] Save IA32\_EFER: Can set=Yes, Can clear=Yes

[ 424.356587] \*\*\*\* True VMX Capabilities are available !!! \*\*\*\*

[ 424.356588] True Pinbased Controls MSR: 0x3f00000016

[ 424.356589] External Interrupt Exiting: Can set=Yes, Can clear=Yes

[ 424.356590] NMI Exiting: Can set=Yes, Can clear=Yes

[ 424.356590] Virtual NMIs: Can set=Yes, Can clear=Yes

[ 424.356591] Activate VMX Preemption Timer: Can set=No, Can clear=Yes

[ 424.356591] Process Posted Interrupts: Can set=No, Can clear=Yes

[ 424.356593] True Primary Procbased Controls MSR: 0xf7f9fffe240065f2

[ 424.356593] Interrupt-window exiting: Can set=Yes, Can clear=Yes

[ 424.356594] Use TSC offsetting : Can set=Yes, Can clear=Yes

[ 424.356594] HLT exiting : Can set=Yes, Can clear=No

[ 424.356595] INVLPG exiting : Can set=Yes, Can clear=Yes

[ 424.356595] MWAIT exiting: Can set=Yes, Can clear=No

[ 424.356596] RDPMC exiting: Can set=Yes, Can clear=Yes

[ 424.356596] RDTSC exiting: Can set=Yes, Can clear=Yes

[ 424.356597] CR3-load exiting: Can set=Yes, Can clear=Yes

[ 424.356597] CR3-store exiting: Can set=Yes, Can clear=Yes

[ 424.356598] CR8-load exiting: Can set=Yes, Can clear=Yes

[ 424.356599] CR8-store exiting: Can set=Yes, Can clear=Yes

[ 424.356599] Use TPR shadow : Can set=Yes, Can clear=Yes

[ 424.356600] NMI-window exiting: Can set=Yes, Can clear=Yes

[ 424.356600] MOV-DR exiting: Can set=Yes, Can clear=Yes

[ 424.356601] Unconditional I/O exiting: Can set=Yes, Can clear=Yes

[ 424.356601] Use I/O bitmaps : Can set=Yes, Can clear=Yes

[ 424.356602] Monitor trap flag : Can set=No, Can clear=Yes

[ 424.356602] Use MSR bitmaps: Can set=Yes, Can clear=Yes

[ 424.356603] MONITOR exiting: Can set=Yes, Can clear=No

[ 424.356603] PAUSE exiting: Can set=Yes, Can clear=Yes

[ 424.356604] Activate secondary controls: Can set=Yes, Can clear=Yes

[ 424.356605] True Secondary Procbased Controls MSR: 0xf7f9fffe240065f2

[ 424.356606] Virtualize APIC accesses: Can set=No, Can clear=Yes

[ 424.356606] Enable EPT : Can set=Yes, Can clear=No

[ 424.356607] Descriptor-table exiting : Can set=Yes, Can clear=Yes

[ 424.356607] Enable RDTSCP : Can set=Yes, Can clear=Yes

[ 424.356608] Virtualize x2APIC mode: Can set=Yes, Can clear=No

[ 424.356609] Enable VPID: Can set=Yes, Can clear=No

[ 424.356609] WBINVD exiting: Can set=Yes, Can clear=No

[ 424.356610] Unrestricted guest: Can set=Yes, Can clear=No

[ 424.356610] APIC-register virtualization: Can set=Yes, Can clear=No

[ 424.356611] Virtual-interrupt delivery: Can set=Yes, Can clear=Yes

[ 424.356611] PAUSE-loop exiting: Can set=Yes, Can clear=No

[ 424.356612] RDRAND exiting : Can set=Yes, Can clear=Yes

[ 424.356612] Enable INVPCID: Can set=Yes, Can clear=Yes

[ 424.356613] Enable VM functions: Can set=Yes, Can clear=No

[ 424.356613] VMCS shadowing: Can set=Yes, Can clear=No

[ 424.356614] Enable ENCLS exiting : Can set=Yes, Can clear=Yes

[ 424.356614] RDSEED exiting : Can set=Yes, Can clear=Yes

[ 424.356615] Enable PML: Can set=No, Can clear=Yes

[ 424.356615] EPT-violation #VE: Can set=No, Can clear=Yes

[ 424.356616] Conceal VMX non-root operation from Intel PT: Can set=Yes, Can clear=Yes

[ 424.356616] Enable XSAVES/XRSTORS: Can set=Yes, Can clear=Yes

[ 424.356617] Mode-based execution control for EPT: Can set=Yes, Can clear=Yes

[ 424.356618] Use TSC scaling: Can set=Yes, Can clear=Yes

[ 424.356619] True Entry Controls MSR: 0x1d3ff000011fb

[ 424.356620] Load debug controls: Can set=Yes, Can clear=Yes

[ 424.356620] IA-32e mode guest: Can set=Yes, Can clear=Yes

[ 424.356621] Entry to SMM: Can set=No, Can clear=Yes

[ 424.356621] Deactivate dual-monitor treatment : Can set=No, Can clear=Yes

[ 424.356622] Load IA32\_PERF\_GLOBAL\_CTRL: Can set=No, Can clear=Yes

[ 424.356622] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356623] Load IA32\_EFER: Can set=Yes, Can clear=Yes

[ 424.356623] Load IA32\_BNDCFGS: Can set=Yes, Can clear=Yes

[ 424.356624] Conceal VM entries from intel PT: Can set=No, Can clear=Yes

[ 424.356625] True Exit Controls MSR: 0xbfefff00036ffb

[ 424.356626] Save debug controls: Can set=Yes, Can clear=Yes

[ 424.356626] Host address-space size: Can set=Yes, Can clear=No

[ 424.356627] Load IA32\_PERF\_GLOB AL\_CTRL: Can set=No, Can clear=Yes

[ 424.356628] Acknowledge interrupt on exit : Can set=Yes, Can clear=Yes

[ 424.356628] Save IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356629] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[ 424.356629] Save IA32\_EFER: Can set=Yes, Can clear=Yes

[ 431.937537] CMPE 283 Assignment 1 Module Exits

**\_end\_**