Sudha Amarnath

CMPE283 Assignment 1

First I tried to this assignment on my ubuntu guest VM that was run using the Oracle Virtual box on host Windows 10. I was able to compile the code given in assignment on the Ubuntu VM, but after inserting kernel object the module, the dumps in the dmesg were showing all the MSRs set to 0. Later I found that guest Ubuntu VM does not support nested virtualization in my laptop, so I installed Ubuntu
on my hard disk drive next to windows 10. After booting laptop with Ubuntu I could see the VMX support in /proc/cpuinfo.
Following are the steps that were done to setup the environment to compile and load the modules to the kernel.
1. sudo apt-get update
2. sudo apt-get upgrade
3. sudo apt-get install git build-essential kernel-package libncurses5-dev bison flex libssl-dev ccache
4. reboot - Enter BIOS and disable Secure Boot in UEFI (BIOS) settings - Otherwise the third party complied ko cannot be inserted using insmod by default. Save BIOS and reboot
5. Download latest source code using "git clone git://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git"
6. Compile the new kernel code.
   (a) 1. Change the directory to where the linux is downloaded
   (b) 2. make clean && make mrproper
   (c) 3. cp /boot/config-$(uname -r) .config
   (d) 4. make menuconfig - save and exit
   (e) 5. make
   (f) 6. make modules
   (g) 7. sudo make modules_install
   (h) 8. sudo make install
   (i) 9. sudo update-grub
   (j) 7. Reboot and verify new kernel is chosen (uname -r)
8. Compile the new code for the assignment using the Makefile provided in the assignment
9. sudo dmesg -C
10. sudo insmod cmpe283-1.ko
11. sudo lsmod | grep cmpe283
12. sudo rmmod cmpe283_1
13. dmesg
Terminal Logs
==========
sudha@sudhalinux:~/cpuvmmko$ uname -r
4.19.0-rc4+

sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ make
make -C /lib/modules/4.19.0-rc4+/build M=/home/sudha/cpuvmmko modules
make[1]: Entering directory '/home/sudha/kernels/linux'
Makefile:958: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel"
CC [M] /home/sudha/cpuvmmko/cmpe283-1.o

Building modules, stage 2.
MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/sudha/cpuvmmko/cmpe283-1.o
see include/linux/module.h for more information
CC /home/sudha/cpuvmmko/cmpe283-1.mod.o
LD [M] /home/sudha/cpuvmmko/cmpe283-1.ko
make[1]: Leaving directory '/home/sudha/kernels/linux'
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ sudo dmesg -C
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ ls
cmpe283-1.c cmpe283-1.ko cmpe283-1.mod.c cmpe283-1.mod.o cmpe283-1.o cmpe283-1.o.ur-safe
Makefile modules.order Module.symvers
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ sudo insmod cmpe283-1.ko
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ lsmod | grep cmpe283
cmpe283_1 16384 0
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ sudo rmmod cmpe283_1
sudha@sudhalinux:~/cpuvmmko$
sudha@sudhalinux:~/cpuvmmko$ dmesg
[184.436285] cmpe283_1: loading out-of-tree module taints kernel.
[184.436288] cmpe283_1: module license 'unspecified' taints kernel.
[184.436289] Disabling lock debugging due to kernel taint
[184.436330] cmpe283_1: module verification failed: signature and/or required key missing - tainting kernel
[184.436490] CMPE 283 Assignment 1 Module Start
[184.436491] VMX Basic MSR: 0x00da040000000012
[184.436491] VMX Basic MSR Bit 55 is set. Getting True MSR values:
[184.436492] TRUE Pinbased Controls MSR: 0x0000007f00000016
[184.436493] External Interrupt Exiting: Can set=Yes, Can clear=Yes
[184.436494] NMI Exiting: Can set=Yes, Can clear=Yes
[184.436495] Virtual NMIs: Can set=Yes, Can clear=Yes
[184.436496] Activate VMX Preemption Timer: Can set=Yes, Can clear=Yes
[184.436497] Process Posted Interrupts: Can set=No, Can clear=Yes
[184.436498] TRUE Processor Based Controls MSR: 0xfff9fffe04006172
[184.436499] Interrupt-window exiting: Can set=Yes, Can clear=Yes
[184.436500] Use TSC offsetting: Can set=Yes, Can clear=Yes
[184.436501] HLT exiting: Can set=Yes, Can clear=Yes

[184.436502] INVLPG exiting: Can set=Yes, Can clear=Yes
[184.436503] MWAIT exiting: Can set=Yes, Can clear=Yes
[184.436504] RDPMC exiting: Can set=Yes, Can clear=Yes
[184.436505] RDTSC exiting: Can set=Yes, Can clear=Yes
[184.436506] CR3-load exiting: Can set=Yes, Can clear=Yes
[184.436507] CR3-store exiting: Can set=Yes, Can clear=Yes
[184.436508] CR8-load exiting: Can set=Yes, Can clear=Yes
[184.436509] CR8-store exiting: Can set=Yes, Can clear=Yes

[184.436509] Use TPR shadow: Can set=Yes, Can clear=Yes
[184.436510] NMI-window exiting: Can set=Yes, Can clear=Yes
[184.436511] NMI-window : Can set=Yes, Can clear=Yes
[184.436512] Unconditional I/O exiting: Can set=Yes, Can clear=Yes
[184.436513] Use I/O bitmaps: Can set=Yes, Can clear=Yes
[184.436514] Monitor trap flag: Can set=Yes, Can clear=Yes
[184.436515] Use MSR bitmaps: Can set=Yes, Can clear=Yes
[184.436516] MONITOR exiting: Can set=Yes, Can clear=Yes
[184.436517] PAUSE exiting: Can set=Yes, Can clear=Yes
[184.436518] Activate secondary controls: Can set=Yes, Can clear=Yes
[184.436519] TRUE Exit Controls MSR: 0x007fffff00036dfb
[184.436520] Save debug controls: Can set=Yes, Can clear=Yes
[184.436521] Host address-space size: Can set=Yes, Can clear=Yes
[184.436522] Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[184.436523] Acknowledge interrupt on exit: Can set=Yes, Can clear=Yes
[184.436524] Save IA32_PAT: Can set=Yes, Can clear=Yes
[184.436525] Load IA32_PAT: Can set=Yes, Can clear=Yes
[184.436526] Save IA32_EFER: Can set=Yes, Can clear=Yes
[184.436527] Load IA32_EFER: Can set=Yes, Can clear=Yes
[184.436528] Save VMX-preemption timer value: Can set=Yes, Can clear=Yes
[184.436529] Clear IA32_BNDCFGS: Can set=No, Can clear=Yes
[184.436530] Conceal VMX from PT: Can set=No, Can clear=Yes
[184.436531] TRUE Entry Controls MSR: 0x0000ffff000011fb
[184.436532] Load debug controls: Can set=Yes, Can clear=Yes
[184.436533] IA-32e mode guest: Can set=Yes, Can clear=Yes
[184.436534] Entry to SMM: Can set=Yes, Can clear=Yes
[184.436535] Deactivate dual-monitor treatment: Can set=Yes, Can clear=Yes
[184.436536] Load IA32_PERF_GLOBAL_CTRL: Can set=Yes, Can clear=Yes
[184.436537] Load IA32_PAT: Can set=Yes, Can clear=Yes
[184.436538] Load IA32_EFER: Can set=Yes, Can clear=Yes
[184.436540] Load IA32_BNDCFGS: Can set=No, Can clear=Yes
[184.436541] Conceal VMX from PT: Can set=No, Can clear=Yes
[184.436542] Activate secondary controls bit31 is set. Secondary Processor Based Controls MSR: 0x00057cff00000000
[184.436543] Virtualize APIC accesses: Can set=Yes, Can clear=Yes
[184.436544] Enable EPT: Can set=Yes, Can clear=Yes
[184.436545] Descriptor-table exiting: Can set=Yes, Can clear=Yes
[184.436546] Enable RDTSCP: Can set=Yes, Can clear=Yes
[184.436547] Virtualize x2APIC mode: Can set=Yes, Can clear=Yes

[184.436548] Enable VPID: Can set=Yes, Can clear=Yes
[184.436549] WBINVD exiting: Can set=Yes, Can clear=Yes
[184.436550] Unrestricted guest: Can set=Yes, Can clear=Yes
[184.436552] APIC-register virtualization: Can set=No, Can clear=Yes
[184.436553] Virtual-interrupt delivery: Can set=No, Can clear=Yes
[184.436554] PAUSE-loop exiting: Can set=Yes, Can clear=Yes
[184.436554] RDRAND exiting: Can set=Yes, Can clear=Yes
[184.436555] Enable INVPCID: Can set=Yes, Can clear=Yes
[184.436556] Enable VM functions: Can set=Yes, Can clear=Yes

[184.436557] VMCS shadowing: Can set=Yes, Can clear=Yes
[184.436558] Enable ENCLS exiting: Can set=No, Can clear=Yes
[184.436559] RDSEED exiting: Can set=Yes, Can clear=Yes
[184.436560] Enable PML: Can set=No, Can clear=Yes
[184.436561] EPT-violation #VE: Can set=Yes, Can clear=Yes
[184.436562] Conceal VMX from PT: Can set=No, Can clear=Yes
[184.436563] enable XSAVES/XRSTORS: Can set=No, Can clear=Yes
[184.436564] Mode-based execute control for EPT: Can set=No, Can clear=Yes
[184.436565] Use TSC scaling: Can set=No, Can clear=Yes
[233.773829] CMPE 283 Assignment 1 Module Exits

sudha@sudhalinux:~/kernels/linux$
sudha@sudhalinux:~/kernels/linux$
sudha@sudhalinux:~/kernels/linux$ git status
On branch master
Your branch is up to date with 'origin/master'.

Changes to be committed:
(use "git reset HEAD <file>..." to unstage)

new file: cpuvmmko/Makefile
new file: cpuvmmko/cmpe283-1.c

sudha@sudhalinux:~/kernels/linux$ git commit -m "cmpe283-1.c assignment" cpuvmmko/
[master 0b3632b7d12b] cmpe283-1.c assignment
2 files changed, 285 insertions(+)
create mode 100755 cpuvmmko/Makefile
create mode 100755 cpuvmmko/cmpe283-1.c
sudha@sudhalinux:~/kernels/linux$ git log
commit 0b3632b7d12b038288b09f5a0cb0e94e3e0e9f7e (HEAD -> master)
Author: SudhaAmarnath <sudha04.a@gmail.com>
Date: Sun Sep 23 13:19:13 2018 -0700

cmpe283-1.c assignment

commit 10dc890d4228cd17ddfd09ba9aaa9221627e29b2 (origin/master, origin/HEAD)
Merge: a27fb6d983c7 96147db1e1df
Author: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
Date: Fri Sep 21 20:01:16 2018 +0200

Merge tag 'pinctrl-v4.19-3' of git://git.kernel.org/pub/scm/linux/kernel/git/linusw/linux-pinctrl

Linus writes:
"Pin control fixes for v4.19:
- Two fixes for the Intel pin controllers than cause
problems on laptops."

** tag 'pinctrl-v4.19-3' of git://git.kernel.org/pub/scm/linux/kernel/git/linusw/linux-pinctrl:*
pinctrl: intel: Do pin translation in other GPIO operations as well

pinctrl: cannonlake: Fix gpio base for GPP-E

commit a27fb6d983c7b5bb0129ae4d7a7c81758173bfab
Merge: 0eba8697bce1 26b471c7e2f7
Author: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
Date: Fri Sep 21 16:21:42 2018 +0200

Merge tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kvm/kvm

Paolo writes:
"It's mostly small bugfixes and cleanups, mostly around x86 nested virtualization. One important change, not related to nested virtualization, is that the ability for the guest kernel to trap CPUID instructions (in Linux that's the ARCH_SET_CPUID arch_prctl) is now masked by default. This is because the feature is detected through an MSR; a very bad idea that Intel seems to like more and more. Some applications choke if the other fields of that MSR are not initialized as on real hardware, hence we have to disable the whole MSR by default, as was the case before Linux 4.12."

** tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kvm/kvm: (23 commits)*
KVM: nVMX: Fix bad cleanup on error of get/set nested state IOCTLs
sudha@sudhalinux:~/kernels/linux$