Kernel Programming

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

ID1206 - OPERATING SYSTEMS

DECEMBER 6, 2023

KENAN DIZDAREVIC
kenandi@kth.se

NOAH PETTERSSON
noahpe@kth.se

Contents

1 Before we begin

We are running Ubuntu 20.04.3 LTS, which is a Debian based distribution.

1.1 CONFIG_MODVERSIONS

We first want to check that CONFIG_MODVERSIONS is enabled on our system. We execute:

```
zgrep CONFIG_MODVERSIONS /boot/config-$(uname -r)
```

This returns:

```
CONFIG_MODVERSIONS=y
```

We have now verified that CONFIG_MODVERSIONS is enabled.
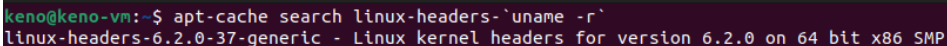
1.2 Disabling UEFI SecureBoot

When checking the settings of the `Oracle VM VirtualBox Manager` we see that Secure Boot is disabled.

1.3 Install Header Files

We install the header files by executing:

```
sudo apt-get update
apt-cache search linux-headers-`uname -r`
```

We get the following output:

We them run the following command:

```
sudo apt-get install kmod linux-headers-6.2.0-37-generic
```

We are now sure that we have the newest version of `kmod`.

2 The Simplest Module

2.1 Add hello-1.c

We have created a test directory and added the code into the file hello-1.c. We can see the code in the picture down below.

```c
/*
 * hello-1.c - The simplest kernel module.
 */
#include <linux/module.h> /* Needed by all modules */
#include <linux/printk.h> /* Needed for pr_info() */

int init_module(void)
{
    pr_info("Hello world 1.\n");

    /* A non 0 return means init_module failed; module can't be loaded. */
    return 0;
}

void cleanup_module(void)
{
    pr_info("Goodbye world 1.\n");
}

MODULE_LICENSE("GPL");
~
~
~
~
~
~
~
~
~
~
~
~
~
"hello-1.c" 20L, 397B
```

When trying to run `make` we get that the kernel configuration is invalid. This is solved by symlinking the build directory to the kernel soruce directory and upgrading the dependecnies. We used the following command to link the directories:

```
sudo ln -s /usr/src/linux-headers-$(uname -r) /lib/modules/6.2.0-37-generic/build
```

When executing `ls -alsh` we get the following output:

```
keno@keno-vm:~/workspace/kernel/hello-1$ ls -alsh
total 340K
4,0K drwxrwxr-x 2 keno keno 4,0K dec  9 17:03 .
4,0K drwxrwxr-x 3 keno keno 4,0K dec  9 16:33 ..
4,0K -rw-rw-r-- 1 keno keno  397 dec  9 16:36 hello-1.c
108K -rw-rw-r-- 1 keno keno 106K dec  9 16:58 hello-1.ko
4,0K -rw-rw-r-- 1 keno keno  281 dec  9 16:58 .hello-1.ko.cmd
4,0K -rw-rw-r-- 1 keno keno   46 dec  9 16:58 hello-1.mod
4,0K -rw-rw-r-- 1 keno keno  891 dec  9 16:58 hello-1.mod.c
4,0K -rw-rw-r-- 1 keno keno  202 dec  9 16:58 .hello-1.mod.cmd
 92K -rw-rw-r-- 1 keno keno  92K dec  9 16:58 hello-1.mod.o
 40K -rw-rw-r-- 1 keno keno  38K dec  9 16:58 .hello-1.mod.o.cmd
 16K -rw-rw-r-- 1 keno keno  16K dec  9 16:58 hello-1.o
 40K -rw-rw-r-- 1 keno keno  37K dec  9 16:58 .hello-1.o.cmd
4,0K -rw-rw-r-- 1 keno keno  175 dec  9 16:51 Makefile
4,0K -rw-rw-r-- 1 keno keno   46 dec  9 16:58 modules.order
4,0K -rw-rw-r-- 1 keno keno  170 dec  9 16:58 .modules.order.cmd
   0 -rw-rw-r-- 1 keno keno    0 dec  9 16:58 Module.symvers
4,0K -rw-rw-r-- 1 keno keno  218 dec  9 16:58 .Module.symvers.cmd
```

2.2   Loading The Module

We now need to load the newly added module. We load it by executing:

```
sudo insmod hello-1.ko
```

We can now see that the module is loaded successfully:

```
keno@keno-vm:~/workspace/kernel/hello-1$ sudo lsmod | grep hello
hello_1                    16384  0
```

We remove the module and check the `journalctl logs` and view the recent changes:

```
dec 09 17:36:56 keno-vm kernel: hello_1: loading out-of-tree module taints kernel.
dec 09 17:36:56 keno-vm kernel: hello_1: module verification failed: signature and/or required key missing - tainting kernel
dec 09 17:36:56 keno-vm kernel: Hello world 1.
dec 09 17:36:59 keno-vm sudo[4477]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/lsmod
dec 09 17:38:33 keno-vm kernel: audit: type=1400 audit(1702139913.332:72): apparmor="DENIED" operation="open" class="file" profile="snap.fir
efox.firefox" name="/etc/fstab" pid=2169 comm="firefox" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
dec 09 17:38:33 keno-vm kernel: audit: type=1107 audit(1702139913.448:73): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.118" pid=2169 label="snap.firefox.firefox" peer_pid=4728 peer_label="unconfined"
dec 09 17:38:33 keno-vm kernel: audit: type=1107 audit(1702139913.448:74): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.118" pid=2169 label="snap.firefox.firefox" peer_pid=4728 peer_label="unconfined"
dec 09 17:40:11 keno-vm sudo[4828]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/rmmod hel
lo_1
dec 09 17:40:11 keno-vm kernel: Goodbye world 1.
dec 09 17:40:22 keno-vm sudo[4836]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/bin/journalctl
 --since '1 hour ago'
```

3   Hello and Goodbye

3.1   Add hello-2.c

We add the new file in the same way as we added the previous file. We also update the `Makefile`, and make again. We get the following output with `ls -alsh`:

```
keno@keno-vm:~/workspace/kernel/hello-1$ ls -alsh
total 660K
4,0K drwxrwxr-x 2 keno keno 4,0K dec  9 17:45 .
4,0K drwxrwxr-x 3 keno keno 4,0K dec  9 17:45 ..
4,0K -rw-rw-r-- 1 keno keno  397 dec  9 17:33 hello-1.c
108K -rw-rw-r-- 1 keno keno 106K dec  9 17:36 hello-1.ko
4,0K -rw-rw-r-- 1 keno keno  281 dec  9 17:36 .hello-1.ko.cmd
4,0K -rw-rw-r-- 1 keno keno   46 dec  9 17:36 hello-1.mod
4,0K -rw-rw-r-- 1 keno keno  891 dec  9 17:36 hello-1.mod.c
4,0K -rw-rw-r-- 1 keno keno  202 dec  9 17:36 .hello-1.mod.cmd
 92K -rw-rw-r-- 1 keno keno  92K dec  9 17:36 hello-1.mod.o
 40K -rw-rw-r-- 1 keno keno  38K dec  9 17:36 .hello-1.mod.o.cmd
 16K -rw-rw-r-- 1 keno keno  16K dec  9 17:36 hello-1.o
 40K -rw-rw-r-- 1 keno keno  37K dec  9 17:36 .hello-1.o.cmd
4,0K -rw-rw-r-- 1 keno keno  553 dec  9 17:45 hello-2.c
108K -rw-rw-r-- 1 keno keno 107K dec  9 17:45 hello-2.ko
4,0K -rw-rw-r-- 1 keno keno  281 dec  9 17:45 .hello-2.ko.cmd
4,0K -rw-rw-r-- 1 keno keno   46 dec  9 17:45 hello-2.mod
4,0K -rw-rw-r-- 1 keno keno  891 dec  9 17:45 hello-2.mod.c
4,0K -rw-rw-r-- 1 keno keno  202 dec  9 17:45 .hello-2.mod.cmd
 92K -rw-rw-r-- 1 keno keno  92K dec  9 17:45 hello-2.mod.o
 40K -rw-rw-r-- 1 keno keno  38K dec  9 17:45 .hello-2.mod.o.cmd
 20K -rw-rw-r-- 1 keno keno  17K dec  9 17:45 hello-2.o
 40K -rw-rw-r-- 1 keno keno  37K dec  9 17:45 .hello-2.o.cmd
4,0K -rw-rw-r-- 1 keno keno  176 dec  9 17:45 Makefile
4,0K -rw-rw-r-- 1 keno keno   92 dec  9 17:45 modules.order
4,0K -rw-rw-r-- 1 keno keno  224 dec  9 17:45 .modules.order.cmd
   0 -rw-rw-r-- 1 keno keno    0 dec  9 17:45 Module.symvers
4,0K -rw-rw-r-- 1 keno keno  218 dec  9 17:45 .Module.symvers.cmd
```

3.2 Loading The Module

We load the new module in the same way as the previous module, and update `Makefile`. We see that it is loaded:

```
keno@keno-vm:~/workspace/kernel/hello-1$ sudo lsmod | grep hello
hello_2                16384  0
```

We remove the module and check the systemd journal again:

```
dec 09 17:51:58 keno-vm kernel: Hello, world 2
dec 09 17:52:07 keno-vm sudo[5308]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/lsmod
dec 09 17:52:58 keno-vm kernel: audit: type=1107 audit(1702140778.125:82): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.122" pid=2169 label="snap.firefox.firefox" peer_pid=5351 peer_label="unconfined"
dec 09 17:52:58 keno-vm kernel: audit: type=1107 audit(1702140778.125:83): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.122" pid=2169 label="snap.firefox.firefox" peer_pid=5351 peer_label="unconfined"
dec 09 17:52:58 keno-vm kernel: audit: type=1107 audit(1702140778.125:84): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.122" pid=2169 label="snap.firefox.firefox" peer_pid=5351 peer_label="unconfined"
dec 09 17:52:58 keno-vm kernel: audit: type=1107 audit(1702140778.125:85): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.122" pid=2169 label="snap.firefox.firefox" peer_pid=5351 peer_label="unconfined"
dec 09 17:52:58 keno-vm kernel: audit: type=1107 audit(1702140778.125:86): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.122" pid=2169 label="snap.firefox.firefox" peer_pid=5351 peer_label="unconfined"
dec 09 17:54:28 keno-vm sudo[5377]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/rmmod hel
lo_2
dec 09 17:54:28 keno-vm kernel: Goodbye, world 2
dec 09 17:54:40 keno-vm sudo[5385]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/bin/journalctl
 --since '1 hour ago'
dec 09 17:54:50 keno-vm sudo[5402]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/bin/journalctl
 --since '1 hour ago'
```

4 The init and exit Macros

4.1 Add hello-3.c

We load the new file in the same way as we previously did, and update `Makefile`. We see that the new file is loaded:

```
keno@keno-vm:~/workspace/kernel/hello-1$ sudo lsmod | grep hello
hello_3                16384  0
```

We remove the module and check the systemd journal again:

```
dec 09 17:59:13 keno-vm kernel: Hello, world 3
dec 09 17:59:23 keno-vm sudo[5813]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/lsmod
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:93): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:94): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:95): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:96): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:97): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.884:98): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 17:59:46 keno-vm kernel: audit: type=1107 audit(1702141186.888:99): pid=554 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freedesktop/hostname1" interface="org.freedesktop.DBus.Properties
" member="GetAll" mask="send" name=":1.124" pid=2169 label="snap.firefox.firefox" peer_pid=5847 peer_label="unconfined"
dec 09 18:00:28 keno-vm sudo[5890]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/sbin/rmmod hel
lo_3
dec 09 18:00:28 keno-vm kernel: Goodbye, world 3
dec 09 18:00:32 keno-vm sudo[5894]:     keno : TTY=pts/0 ; PWD=/home/keno/workspace/kernel/hello-1 ; USER=root ; COMMAND=/usr/bin/journalctl
 --since '1 hour ago'
```

5 Licensing and Module Documentation

5.1 Add hello-4.c

We repeat the same steps as with the previous modules, and update `Makefile` again. We see that the new module is loaded:

Again, we remove the module and check the systemd journal:

The updated Makefile The update `Makefile` looks like:

```
obj-m += hello-1.o
obj-m += hello-2.o
obj-m += hello-3.o
obj-m += hello-4.o

all:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

6 Passing Command Line Arguments to a Module

6.1 Add hello-5.c

We passed arguments in the command line and received these results.

We also tried passing a string as argument instead of a int and we received this error.

6.2 Add start.c and stop.c

We added two c files, start.c and stop.c and updated the `Makefile`.

We first create an object for our combined module by adding:

```
obj-m += startstop.o
```

Then we need to tell make what object files are a part of that kernel module by adding:

```
startstop-objs := start.o stop.o
```

When executing the kernel module we execute the combined kernel object file, which is `startstop.ko`.

We can see the two different messages printed out by the two different files by using:

```
sudo dmesg -t | tail -2
```

We get the following output:

7 Functions available to modules

We created a hello.c file which used the function `printf()` to print the string "hello". We could trace all the syscalls made with the use of strace.

The system call:

```
write(1, "hello", 5hello) = 5
```

is the one which prints out the string.

8 Character device drivers

We are going to work with the file `chardev.c`. The purpose of this section is to create a char driver.

We need to load the kernel module in the same way as we have done previously. We create the file `chardev.c`, and add the code. We update the `Makefile` by adding:

```
obj-m += chardev.o
```


The kernel module is now loaded correctly. We also need to verify that the driver has been created. We do that by executing:

```
cat /proc/devices | chardev
```

```
keno@keno-vm:~/workspace/kernel/hello-1$ cat /proc/devices | grep chardev
239 chardev
```

We have now verified that the driver has been added. We can also see that the file exists in the
/dev-folder.

```
keno@keno-vm:~/workspace/kernel/hello-1$ ls -l /dev | grep chardev
crw-------  1 root root    239,   0 dec 20 18:12 chardev
```

When we try to open the file we get the following output:

```
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 2 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 3 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 4 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 5 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 6 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 7 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 8 times Hello world!
keno@keno-vm:~/workspace/kernel/hello-1$ sudo cat /dev/chardev
I already told you 9 times Hello world!
```

We now want to try to write some text into chardev, by using echo. We need to update the
permissions, we do that by executing:

```
sudo chmod 777 /dev/chardev
```

We verify that we have updated the permissions correctly:

```
keno@keno-vm:~/workspace/kernel/hello-1$ sudo chmod 777 /dev/chardev
keno@keno-vm:~/workspace/kernel/hello-1$ ls -l /dev | grep chardev
crwxrwxrwx  1 root root    239,   0 dec 20 18:12 chardev
```

We see that every group has access to read, write, and execute the file.

When we try writing to the file, we get an error. We check the output of the kernel:

```
keno@keno-vm:~/workspace/kernel/hello-1$ echo "Hello, this is NOT the kernel speaking" > /dev/chardev
bash: echo: write error: Invalid argument
keno@keno-vm:~/workspace/kernel/hello-1$ sudo dmesg -t | tail -4
I was assigned major number 239.
Device created on /dev/chardev
Sorry, this operation is not supported.
Sorry, this operation is not supported.
```

We see that device has the major number 239, and that the device was created successfully. We also tried to write to the file twice, we see that the write operation is not supported.