Linux kernel and driver development training

Practical Labs

bootlin
https://bootlin.com

March 11, 2022

About this document

Updates to this document can be found on https://bootlin.com/doc/training/linux-kernel.

This document was generated from LaTeX sources found on https://github.com/bootlin/training-materials.

More details about our training sessions can be found on https://bootlin.com/training.

Copying this document

© 2004-2022, Bootlin, https://bootlin.com.

This document is released under the terms of the Creative Commons CC BY-SA 3.0 license . This means that you are free to download, distribute and even modify it, under certain conditions.

Corrections, suggestions, contributions and translations are welcome!

Training setup

Download files and directories used in practical labs

Install lab data

For the different labs in this course, your instructor has prepared a set of data (kernel images, kernel configurations, root filesystems and more). Download and extract its tarball from a terminal:

```
$ cd
$ wget https://bootlin.com/doc/training/linux-kernel/linux-kernel-labs.tar.xz
$ tar xvf linux-kernel-labs.tar.xz
```

Lab data are now available in an `linux-kernel-labs` directory in your home directory. This directory contains directories and files used in the various practical labs. It will also be used as working space, in particular to keep generated files separate when needed.

Update your distribution

To avoid any issue installing packages during the practical labs, you should apply the latest updates to the packages in your distro:

```
$ sudo apt update
$ sudo apt dist-upgrade
```

You are now ready to start the real practical labs!

Install extra packages

Feel free to install other packages you may need for your development environment. In particular, we recommend to install your favorite text editor and configure it to your taste. The favorite text editors of embedded Linux developers are of course *Vim* and *Emacs*, but there are also plenty of other possibilities, such as Visual Studio Code[1], *GEdit*, *Qt Creator*, *CodeBlocks*, *Geany*, etc.

It is worth mentioning that by default, Ubuntu comes with a very limited version of the `vi` editor. So if you would like to use `vi`, we recommend to use the more featureful version by installing the `vim` package.

More guidelines

Can be useful throughout any of the labs

- Read instructions and tips carefully. Lots of people make mistakes or waste time because they missed an explanation or a guideline.

[1] This tool from Microsoft is Open Source! To try it on Ubuntu: `sudo snap install code --classic`

© 2004-2022 Bootlin, CC BY-SA license

- Always read error messages carefully, in particular the first one which is issued. Some people stumble on very simple errors just because they specified a wrong file path and didn't pay enough attention to the corresponding error message.
- Never stay stuck with a strange problem more than 5 minutes. Show your problem to your colleagues or to the instructor.
- You should only use the `root` user for operations that require super-user privileges, such as: mounting a file system, loading a kernel module, changing file ownership, configuring the network. Most regular tasks (such as downloading, extracting sources, compiling...) can be done as a regular user.
- If you ran commands from a root shell by mistake, your regular user may no longer be able to handle the corresponding generated files. In this case, use the `chown -R` command to give the new files back to your regular user.
  Example: `$ chown -R myuser.myuser linux/`

 © 2004-2022 Bootlin, CC BY-SA license

Downloading kernel source code

Get your own copy of the mainline Linux kernel source tree

Setup

Create the `$HOME/linux-kernel-labs/src` directory.

Installing git packages

First, let's install software packages that we will need throughout the practical labs:

```
sudo apt install git gitk git-email
```

Git configuration

After installing `git` on a new machine, the first thing to do is to let `git` know about your name and e-mail address:

```
git config --global user.name 'My Name'
git config --global user.email me@mydomain.net
```

Such information will be stored in commits. It is important to configure it properly when the time comes to generate and send patches, in particular.

It can also be particularly useful to display line numbers when using the `git grep` command. This can be enabled by default with the following configuration:

```
git config --global grep.lineNumber true
```

Cloning the mainline Linux tree

To begin working with the Linux kernel sources, we need to clone its reference git tree, the one managed by Linus Torvalds.

However, this requires downloading more than 2.7 GB of data. If you are running this command from home, or if you have very fast access to the Internet at work (and if you are not 256 participants in the training room), you can do it directly by connecting to `https://git.kernel.org`:

```
git clone https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux
```

If Internet access is not fast enough and if multiple people have to share it, your instructor will give you a USB flash drive with a `tar.gz` archive of a recently cloned Linux source tree.

You will just have to extract this archive in the current directory, and then pull the most recent changes over the network:

```
tar xf linux-git.tar.gz
cd linux
git checkout master
```

© 2004-2022 Bootlin, CC BY-SA license

```
git pull
```

Of course, if you directly ran `git clone`, you won't have to run `git pull`, as `git clone` already retrieved the latest changes. You may need to run `git pull` in the future though, if you want to update a newer Linux version.

Accessing stable releases

Having the Linux kernel development sources is great, but when you are creating products, you prefer to avoid working with a target that moves every day.

That's why we need to use the *stable* releases of the Linux kernel.

Fortunately, with `git`, you won't have to clone an entire source tree again. All you need to do is add a reference to a *remote* tree, and fetch only the commits which are specific to that remote tree.

```
cd ~/linux-kernel-labs/src/linux/
git remote add stable https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable
git fetch stable
```

As this still represents many git objects to download (450 MiB when 5.9 was the latest version), if you are using an already downloaded git tree, your instructor will probably have fetched the *stable* branch ahead of time for you too. You can check by running:

```
git branch -a
```

We will choose a particular stable version in the next labs.

Now, let's continue the lectures. This will leave time for the commands that you typed to complete their execution (if needed).

 © 2004-2022 Bootlin, CC BY-SA license

Kernel source code

Objective: Get familiar with the kernel source code

After this lab, you will be able to:

- Create a branch based on a remote tree to explore a particular stable kernel version (from the `stable` kernel tree).
- Explore the sources and search for files, function headers or other kinds of information…
- Browse the kernel sources with tools like `cscope` and Elixir.

Choose a particular stable version

Let's work with a particular stable version of the Linux kernel. It would have been more logical to do this in the previous lab, but we wanted to get back to lectures while the `fetch` command was running.

First, let's get the list of branches on our `stable` remote tree:

```
cd ~/linux-kernel-labs/src/linux
git branch -a
```

As we will do our labs with the Linux 5.10 stable branch, the remote branch we are interested in is `remotes/stable/linux-5.10.y`.

First, execute the following command to check which version you currently have:

```
make kernelversion
```

You can also open the `Makefile` and look at the beginning of it to check this information.

Now, let's create a local branch starting from that remote branch:

```
git checkout -b 5.10.bootlin stable/linux-5.10.y
```

Check the version again using the `make kernelversion` command to make sure you now have a 5.10.y version.

Exploring the sources manually

As a Linux kernel user, you will very often need to find which file implements a given function. So, it is useful to be familiar with exploring the kernel sources.

1. Find the Linux logo image in the sources[2].
2. Find who the maintainer of the MVNETA network driver is.
3. Find the declaration of the `platform_device_register()` function.

[2] Look for files in `logo` in their name. It's an opportunity to practise with the `find` command.

© 2004-2022 Bootlin, CC BY-SA license

Tip: if you need the `grep` command, we advise you to use `git grep`. This command is similar, but much faster, doing the search only on the files managed by git (ignoring git internal files and generated files).

Use a kernel source indexing tool

Now that you know how to do things in a manual way, let's use more automated tools.

Try Elixir at https://elixir.bootlin.com and choose the Linux version closest to yours.

If you don't have Internet access, you can use `cscope` instead.

As in the previous section, use this tool to find where the `platform_device_register()` function is declared, implemented and even used.

 © 2004-2022 Bootlin, CC BY-SA license

Board setup

Objective: setup communication with the board and configure the bootloader.

After this lab, you will be able to:

- Access the board through its serial line.
- Configure the U-boot bootloader and a tftp server on your workstation to download files through tftp.

Getting familiar with the board

Take some time to read about the board features and connectors:

- If you have the original BeagleBone Black:
  https://www.elinux.org/Beagleboard:BeagleBoneBlack
- If you have the newer BeagleBone Black Wireless:
  https://beagleboard.org/black-wireless in addition to the above URL.

Don't hesitate to share your questions with the instructor.

Download technical documentation

We are going to download documents which we will need during our practical labs.

The first document to download is the BeagleBone Black System Reference Manual found at https://github.com/CircuitCo/BeagleBone-Black/blob/master/BBB_SRM.pdf?raw=true.

Even if you have the BeagleBoneBlack Wireless board, this is the ultimate reference about the board, in particular for the pinout and possible configurations of the P8 and P9 headers, and more generally for most devices which are the same in both boards. You don't have to start reading this document now but you will need it during the practical labs.

The second document to download is the datasheet for the TI AM335x SoCs, available on https://www.ti.com/lit/ds/symlink/am3359.pdf. This document will give us details about pin assignments.

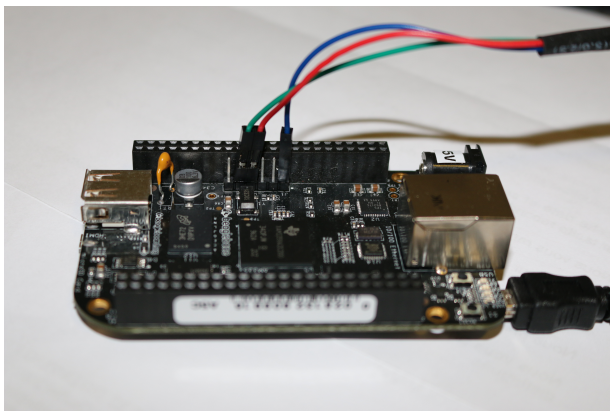
Last but not least, download the Technical Reference Manual (TRM) for the TI AM3359 SoC, available on https://www.ti.com/product/am3359, in the `User guides` section in the `Technical documents` tab. This document is more than 5100 pages big! You will need it too during the practical labs.

Setting up serial communication with the board

The Beaglebone serial connector is exported on the 6 pins close to one of the 48 pins headers. Using your special USB to Serial adapter provided by your instructor, connect the ground wire

(blue) to the pin closest to the power supply connector (let's call it pin 1), and the TX (red) and RX (green) wires to the pins 4 (board RX) and 5 (board TX)[3].

You always should make sure that you connect the TX pin of the cable to the RX pin of the board, and vice versa, whatever the board and cables that you use.



Once the USB to Serial connector is plugged in, a new serial port should appear: `/dev/ttyUSB0`. You can also see this device appear by looking at the output of `dmesg`.

To communicate with the board through the serial port, install a serial communication program, such as `picocom`:

```
sudo apt install picocom
```

If you run `ls -l /dev/ttyUSB0`, you can also see that only `root` and users belonging to the `dialout` group have read and write access to this file. Therefore, you need to add your user to the `dialout` group:

```
sudo adduser $USER dialout
```

Important: for the group change to be effective, you have to *completely log out* from your session and log in again (no need to reboot). A workaround is to run `newgrp dialout`, but it is not global. You have to run it in each terminal.

Now, you can run `picocom -b 115200 /dev/ttyUSB0`, to start serial communication on `/dev/ttyUSB0`, with a baudrate of `115200`. If you wish to exit `picocom`, press `[Ctrl][a]` followed by `[Ctrl][x]`.

There should be nothing on the serial line so far, as the board is not powered up yet.

It is now time to power up your board by plugging in the mini-USB (BeagleBone Black case) or micro-USB (BeagleBone Black Wireless case) cable supplied by your instructor to your PC.

See what messages you get on the serial line. You should see U-boot start on the serial line.

Bootloader interaction

Reset your board. Press the space bar in the `picocom` terminal to stop the U-boot countdown. You should then see the U-Boot prompt:

```
=>
```

[3] See https://www.olimex.com/Products/Components/Cables/USB-Serial-Cable/USB-Serial-Cable-F/ for details about the USB to Serial adapter that we are using.

 © 2004-2022 Bootlin, CC BY-SA license

You can now use U-Boot. Run the `help` command to see the available commands.

Type the `help saveenv` command to make sure that the `saveenv` command exists. We use it in these labs to save your U-Boot environment settings to the boards' eMMC storage. Some earlier versions do not support this.

If you don't have this U-Boot prompt, it's probably because you are doing these labs on your own (i.e. without participating to a Bootlin course), we ask you to install the U-Boot binary that we compiled and tested. See instructions at https://github.com/bootlin/training-materials/tree/master/lab-data/common/bootloader/beaglebone-black for a simple way to do this.

To avoid trouble because of settings applied in previous practical labs, we advise you to clear the U-Boot environment variables:

```
env default -f -a
saveenv
```

Setting up networking

The next step is to configure U-boot and your workstation to let your board download files, such as the kernel image and Device Tree Binary (DTB), using the TFTP protocol through a network connection.

As this course supports both the BeagleBone Black and BeagleBone Black Wireless boards, we're keeping things simple by using Ethernet of USB device as this works for both boards (as the Wireless board has no native Ethernet port). So, networking will work through the USB device cable that is already used to power up the board.

Network configuration on the target

Now, let's configure networking in U-Boot:

- `ipaddr`: IP address of the board
- `serverip`: IP address of the PC host

```
setenv ipaddr 192.168.0.100
setenv serverip 192.168.0.1
```

Of course, make sure that this address belongs to a separate network segment from the one of the main company network.

We also need to configure Ethernet over USB device:

- `ethprime`: controls which interface gets used first
- `usbnet_devaddr`: MAC address on the device side
- `usbnet_hostaddr`: MAC address on the host side

```
setenv ethprime usb_ether
setenv usbnet_devaddr f8:dc:7a:00:00:02
setenv usbnet_hostaddr f8:dc:7a:00:00:01
```

Save these settings to the eMMC storage on the board[4]:

[4] The U-boot environment settings are stored in some free space between the master boot record (512 bytes, containing the partition tables and other stuff), and the beginning of the first partition (often at `32256`). This is why you won't find any related file in the first partition of the eMMC storage.

```
saveenv
```

Network configuration on the PC host

To configure your network interface on the workstation side, we need to know the name of the network interface connected to your board.

Note that when the board is sitting at the U-Boot prompt, no network interface will show up on the workstation side. It is only when U-Boot is actively executing a network-related command (such as `ping` or `tftp`) that it brings up the USB network connection.

From the board, run `ping 192.168.0.1`, and while the `ping` command is running, you should see on your workstation a new network interface named `enx<macaddr>`. Given the value we gave to `usbnet_hostaddr`, it will therefore be `enxf8dc7a000001`. Note that pinging the board from your PC will not work: when U-Boot is sitting at its prompt, it is not able to reply to ping requests.

Then, instead of configuring the host IP address from NetWork Manager's graphical interface, let's do it through its command line interface, which is so much easier to use:

```
nmcli con add type ethernet ifname enxf8dc7a000001 ip4 192.168.0.1/24
```

Setting up the TFTP server

Let's install a TFTP server on your development workstation:

```
sudo apt install tftpd-hpa
```

Once the package is installed, view the contents of `/etc/default/tftpd-hpa`, and check what the TFTP server home directory (`TFTP_DIRECTORY` setting). If `/srv` exists on your system, it should be `/srv/tftp`, otherwise `/var/lib/tftpboot/`.

If you wish to make a change to this file, you will have to restart the TFTP server:

```
sudo /etc/init.d/tftpd-hpa restart
```

Testing the network connection

You can then test the TFTP connection. First, put a small text file in TFTP server home directory. Then, from U-Boot, do:

```
tftp 0x81000000 textfile.txt
```

The `tftp` command should have downloaded the `textfile.txt` file from your development workstation into the board's memory at location `0x81000000` (this location is part of the board DRAM). You can verify that the download was successful by dumping the contents of the memory:

```
md 0x81000000
```

We are now ready to load and boot a Linux kernel!

 © 2004-2022 Bootlin, CC BY-SA license

Kernel compiling and booting

Objective: compile and boot a kernel for your board, booting on a directory on your workstation shared by NFS.

After this lab, you will be able to:

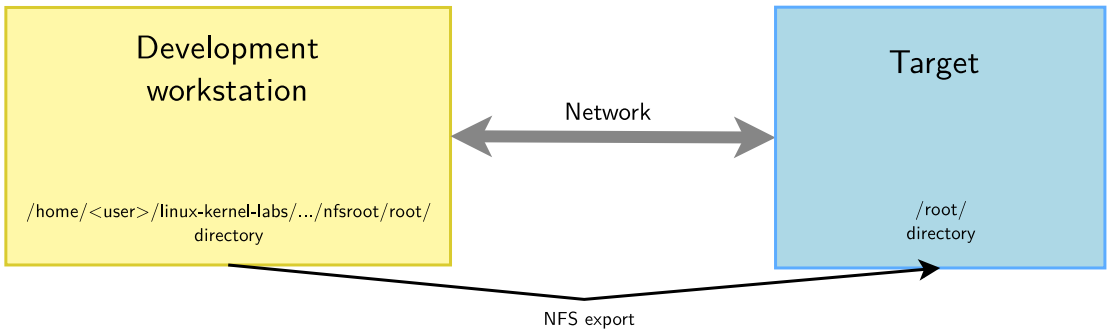
- Cross-compile the Linux kernel for the ARM platform.
- Boot this kernel on an NFS root filesystem, which is somewhere on your development workstation[5].

Lab implementation

While developing a kernel module, the developer wants to change the source code, compile and test the new kernel module very frequently. While writing and compiling the kernel module is done on the development workstation, the test of the kernel module usually has to be done on the target, since it might interact with hardware specific to the target.

However, flashing the root filesystem on the target for every test is time-consuming and would use the flash chip needlessly.

Fortunately, it is possible to set up networking between the development workstation and the target. Then, workstation files can be accessed through the network by the target, using NFS.



Setup

Go to the `$HOME/linux-kernel-labs/src/linux` directory.

Install packages needed for configuring, compiling and booting the kernel for your board:

```
sudo apt install libssl-dev bison flex
```

[5] NFS root filesystems are particularly useful to compile modules on your host, and make them directly visible on the target. You no longer have to update the root filesystem by hand and transfer it to the target (requiring a shutdown and reboot).

Cross-compiling toolchain setup

We are going to install a cross-compiling toolchain provided by Ubuntu:

```
sudo apt install gcc-arm-linux-gnueabi
```

Now find out the path and name of the cross-compiler executable by looking at the contents of the package:

```
dpkg -L gcc-arm-linux-gnueabi
```

Kernel configuration

Configure your kernel sources with the ready-made configuration for boards in the OMAP2 and later family which the AM335x found in the BeagleBone belongs to. Don't forget to set the `ARCH` and `CROSS_COMPILE` definitions for the `arm` platform and to use your cross-compiler.

Add the below options to support networking over USB device:

- `CONFIG_USB_GADGET=y`
- `CONFIG_USB_MUSB_HDRC=y` *Driver for the USB OTG controller*
- `CONFIG_USB_MUSB_GADGET=y` *Use the USB OTG controller in device (gadget) mode*
- `CONFIG_USB_MUSB_DSPS=y`
- Check the dependencies of `CONFIG_AM335X_PHY_USB` and find the way to set `CONFIG_AM335X_PHY_USB=y`
- Find the "USB Gadget precomposed configurations" menu and set it to *static* instead of *module* so that `CONFIG_USB_ETH=y`

Make sure that this configuration has `CONFIG_ROOT_NFS=y` (support booting on an NFS exported root directory).

To save about 1 second every time you boot or reboot, as shown in our Embedded Linux Boot Time Optimization course, you can also replace LZMA kernel compression by LZO compression (`CONFIG_KERNEL_LZO`). You will need to install the `lzop` package so that your machine has the appropriate tools to compress the kernel with the LZO compression algorithm:

```
sudo apt install lzop
```

Kernel compiling

Compile your kernel and generate the Device Tree Binaries (DTBs) (running 8 compile jobs in parallel):

```
make -j 8
```

Now, copy the `zImage` and `am335x-boneblack.dtb` or `am335x-boneblack-wireless.dtb` files to the TFTP server home directory (as specified in `/etc/default/tftpd-hpa`).

Setting up the NFS server

Install the NFS server by installing the `nfs-kernel-server` package. Once installed, edit the `/etc/exports` file as `root` to add the following lines, assuming that the IP address of your board will be `192.168.0.100`:

 © 2004-2022 Bootlin, CC BY-SA license

```
/home/<user>/linux-kernel-labs/modules/nfsroot 192.168.0.100(rw,no_root_squash,no_subtree_check)
```

Of course, replace `<user>` by your actual user name.

Make sure that the path and the options are on the same line. Also make sure that there is no space between the IP address and the NFS options, otherwise default options will be used for this IP address, causing your root filesystem to be read-only.

Then, restart the NFS server:

```
sudo exportfs -r
```

If there is any error message, this usually means that there was a syntax error in the `/etc/exports` file. Don't proceed until these errors disappear.

Boot the system

First, boot the board to the U-Boot prompt. Before booting the kernel, we need to tell it which console to use and that the root filesystem should be mounted over NFS, by setting some kernel parameters.

Do this by setting U-boot's `bootargs` environment variable (all in just one line):

```
setenv bootargs root=/dev/nfs rw ip=192.168.0.100:::::usb0 console=ttyS0,115200n8
  g_ether.dev_addr=f8:dc:7a:00:00:02 g_ether.host_addr=f8:dc:7a:00:00:01
  nfsroot=192.168.0.1:/home/<user>/linux-kernel-labs/modules/nfsroot,nfsvers=3,tcp
```

Once again, replace `<user>` by your actual user name.

Now save this definition:

```
saveenv
```

If you later want to make changes to this setting, you can type the below command in U-boot:

```
editenv bootargs
```

Now, download the kernel image through `tftp`:

```
tftp 0x81000000 zImage
```

You'll also need to download the device tree blob:

```
tftp 0x82000000 <board>.dtb
```

Now, boot your kernel:

```
bootz 0x81000000 - 0x82000000
```

If everything goes right, you should reach a login prompt (user: `root`, password: `root`). Otherwise, check your setup and ask your instructor for support if you are stuck.

If the kernel fails to mount the NFS filesystem, look carefully at the error messages in the console. If this doesn't give any clue, you can also have a look at the NFS server logs in `/var/log/syslog`.

Checking the kernel version

It's often a good idea to make sure you booted the right kernel. By mistake, you could have booted a kernel previously stored in flash (typically through a default boot command in U-Boot), or forgotten to update the kernel image in the TFTP server home directory.

This could explain some unexpected behavior.

There are two ways of checking your kernel version:

- By looking at the first kernel messages
- By running the `uname -a` command after booting Linux.

In both cases, you will not only know the kernel version, but also the date when the kernel was compiled and the name of the user who did it.

Similarly, you can also check the command line actually received by the kernel, either by looking at the first boot messages, or once you have reached a command line shell, by running `cat /proc/cmdline`.

Automate the boot process

To avoid typing the same U-boot commands over and over again each time you power on or reset your board, you can use U-Boot's `bootcmd` environment variable:

```
setenv bootcmd 'tftp 0x81000000 zImage; tftp 0x82000000 <board>.dtb; bootz 0x81000000 - 0x82000000'
saveenv
```

Don't hesitate to change it according to your exact needs.

We could also copy the `zImage` file to the eMMC flash and avoid downloading it over and over again. However, detailed bootloader usage is outside of the scope of this course. See our Embedded Linux system development course and its on-line materials for details.

 © 2004-2022 Bootlin, CC BY-SA license

Writing modules

Objective: create a simple kernel module

After this lab, you will be able to:

- Compile and test standalone kernel modules, which code is outside of the main Linux sources.
- Write a kernel module with several capabilities, including module parameters.
- Access kernel internals from your module.
- Set up the environment to compile it.
- Create a kernel patch.

Setup

Go to the `~/linux-kernel-labs/modules/nfsroot/root/hello` directory. Boot your board if needed.

Writing a module

Look at the contents of the current directory. All the files you generate there will also be visible from the target. That's great to load modules!

Add C code to the `hello_version.c` file, to implement a module which displays this kind of message when loaded:

```
Hello World. You are currently using Linux <version>.
```

... and displays a goodbye message when unloaded.

Suggestion: you can look for files in kernel sources which contain `version` in their name, and see what they do.

You may just start with a module that displays a hello message, and add version information later.

Caution: you must use a kernel variable or function to get version information, and not just the value of a C macro. Otherwise, you will only get the version of the kernel you used to build the module.

Building your module

The current directory contains a `Makefile` file, which lets you build modules outside a kernel source tree. Compile your module.

© 2004-2022 Bootlin, CC BY-SA license

Testing your module

Load your new module file on the target. Check that it works as expected. Until this, unload it, modify its code, compile and load it again as many times as needed.

Run a command to check that your module is on the list of loaded modules. Now, try to get the list of loaded modules with only the `cat` command.

Adding a parameter to your module

Add a `who` parameter to your module. Your module will say `Hello <who>` instead of `Hello World`.

Compile and test your module by checking that it takes the `who` parameter into account when you load it.

Adding time information

Improve your module, so that when you unload it, it tells you how many seconds elapsed since you loaded it. You can use the `ktime_get_seconds()` function to achieve this.

You may search for other drivers in the kernel sources using the `ktime_get_seconds()` function. Looking for other examples always helps!

Following Linux coding standards

Your code should adhere to strict coding standards, if you want to have it one day merged in the mainline sources. One of the main reasons is code readability. If anyone used one's own style, given the number of contributors, reading kernel code would be very unpleasant.

Fortunately, the Linux kernel community provides you with a utility to find coding standards violations.

First install the `python3-ply` and `python3-git` packages.

Then run the `scripts/checkpatch.pl -h` command in the kernel sources, to find which options are available. Now, run:

```
~/linux-kernel-labs/src/linux/scripts/checkpatch.pl --file --no-tree hello_version.c
```

See how many violations are reported on your code, and fix your code until there are no errors left. If there are many indentation related errors, make sure you use a properly configured source code editor, according to the kernel coding style rules in `process/coding-style`.

Adding the hello_version module to the kernel sources

As we are going to make changes to the kernel sources, first create a special branch for such changes:

```
git checkout 5.10.bootlin
git checkout -b hello
```

Add your module sources to the `drivers/misc/` directory in your kernel sources. Of course, also modify kernel configuration and building files accordingly, so that you can select your module in `make xconfig` and have it compiled by the `make` command.

 © 2004-2022 Bootlin, CC BY-SA license

Run one of the kernel configuration interfaces and check that it shows your new driver lets you configure it as a module.

Run the `make` command and make sure that the code of your new driver is getting compiled.

Then, commit your changes in the current branch (try to choose an appropriate commit message):

```
cd ~/linux-kernel-labs/src/linux
git add <files>
git commit -as
```

- `git add` adds files to the next commit. It is mandatory to use for new files that should be added under version control.
- `git commit -a` creates a commit with all modified files that already under version control
- `git commit -s` adds a `Signed-off-by:` line to the commit message. All contributions to the Linux kernel must have such a line.

Create a kernel patch

You can be proud of your new module! To be able to share it with others, create a patch which adds your new files to the mainline kernel.

Creating a patch with `git` is extremely easy! You just generate it from the commits between your branch and another branch, usually the one you started from:

```
git format-patch 5.10.bootlin
```

Have a look at the generated file. You can see that its name reused the commit message.

If you want to change the last commit message at this stage, you can run:

```
git commit --amend
```

And run `git format-patch` again.

© 2004-2022 Bootlin, CC BY-SA license

Device Model - I2C device

Objective: declare an I2C device and basic driver hooks called when this device is detected

Throughout the upcoming labs, we will implement a driver for an I2C device, which offers the functionality of an I2C Nunchuk.

After this lab, you will be able to:

- Add an I2C device to a device tree.
- Implement basic `probe()` and `remove()` driver functions and make sure that they are called when there is a device/driver match.
- Find your driver and device in `/sys`.

Setup

Go to the `~/linux-kernel-labs/src/linux` directory. Check out the `5.10.bootlin` branch.

Now create a new `nunchuk` branch starting from this branch, for your upcoming work on the Nunchuk driver.

During this lab, we will start to implement a driver for a Nunchuk I2C device, but at this stage we won't need to connect it yet, as we will enable I2C on the right board pins in the next lab.

Download a useful document sharing useful details about the Nunchuk and its connector:
https://bootlin.com/labs/doc/nunchuk.pdf

Create a custom device tree

To let the Linux kernel handle a new device, we need to add a description of this device in the board device tree.

As the Beaglebone Black device tree is provided by the kernel community, and will continue to evolve on its own, we don't want to make changes directly to the device tree file for this board.

The easiest way to customize the board DTS is to create a new DTS file that includes the Beaglebone Black or Black Wireless DTS, and add its own definitions.

So, create a new `am335x-customboneblack.dts` file in which you just include the regular board DTS file. We will add further definitions in the next sections.

Now, modify the corresponding `Makefile` to make sure the new DTS is compiled automatically.

Enable the second I2C bus

We are first going to enable and configure the second I2C bus (`i2c1`).

First, as an exercise, find the DTS include file defining (`i2c1`) for the SoC in our board.

 © 2004-2022 Bootlin, CC BY-SA license

Then, make a reference to this definition in your custom DTS and enable this bus. Also configure it to function at 100 KHz. That's enough so far!

Declare the Nunchuk device

As a child node to the `i2c1` bus, now declare an I2C device for the Nunchuk, choosing `nintendo,nunchuk` for its `compatible` property. You will find the I2C slave address of the Nunchuk on the nunckuk document that we have downloaded earlier[6]. The node name should be `joystick@addr`, the convention for node names is `<device-type>@<addr>`.

Checking the device tree on the running system

Now, just compile your DTB by asking the kernel Makefile to recompile only DTBs:

```
make dtbs
```

Now, copy the new DTB to the tftp server home directory, change the DTB file name in the U-Boot configuration[7], and boot the board.

Through the `/sys/firmware/devicetree` directory, it is possible to check the Device Tree settings that your system has loaded. That's useful when you are not sure exactly which settings were actually loaded.

For example, you can check the presence of a new `joystick` node in your device tree:

```
# find /sys/firmware/devicetree -name "*joystick*"
/sys/firmware/devicetree/base/ocp/interconnect@48000000/segment@0/target-module@2a000/i2c@0/joystick@52
```

As the base address of the I2C1 controller registers was not explicited in the DTSI file (at least not in the corresponding node), you can now compute this address from the above line: it's `0x48000000 + 0x2a000 = 0x4802a000`.

Also find the same address in the big processor Technical Reference Manual[8].

Back to `/sys/firmware/devicetree/`, you can also check the whole structure of the loaded Device Tree, using the Device Tree Compiler (`dtc`), which we put in the root filesystem. That's better than checking the source files and includes in the source directory:

```
# dtc -I fs /sys/firmware/devicetree/base/ > /tmp/dts
```

Look for `i2c1` and `joystick` in the output file, and see where the nodes are instantiated. Don't hesitate to ask your instructor for questions!

Implement a basic I2C driver for the Nunchuk

It is now time to start writing the first building blocks of the I2C driver for our Nunchuk.

In a new terminal, go to `~/linux-kernel-labs/modules/nfsroot/root/nunchuk/`. This directory contains a Makefile and an almost empty `nunchuk.c` file.

[6] This I2C slave address is enforced by the device itself. You can't change it.

[7] Tip: you just need to run `editenv bootcmd` and `saveenv`.

[8] Tip: to do your search, put an underscore character in the middle of the address, as in `FFFF_FFFF`... that's how addresses are written in this document.

Now, you can compile your out-of-tree module by running `make`. As the current directory is part of the NFS root that the board boots on, the generated `.ko` file will immediately be visible on the board too.

Relying on explanations given during the lectures, fill the `nunchuk.c` file to implement:

- `probe()` and `remove()` functions that will be called when a Nunchuk is found. For the moment, just put a call to `pr_info()` inside to confirm that these functions are called.
- Initialize a `i2c_driver` structure, and register the i2c driver using it. Make sure that you use a `compatible` property that matches the one in the Device Tree.

You can now compile your module and reboot your board, to boot with the updated DTB.

Driver tests

You can now load the `/root/nunchuk/nunchuk.ko` file. You need to check that the `probe()` function gets called then, and that the `remove()` function gets called too when you remove the module.

Once your new Device Tree and module work as expected, commit your DT changes in your Linux tree:

```
git commit -sa
```

Exploring /sys

Take a little time to explore `/sys`:

- Find the representation of your driver. That's a way of finding the matching devices.
- Find the representation of your device, containing its name. You will find a link to the driver too.

 © 2004-2022 Bootlin, CC BY-SA license

Using the I2C bus

Objective: make the I2C bus work and use it to implement communication with the Nunchuk device

After this lab, you will be able to:

- Declare pinctrl settings.
- Access I2C device registers through the bus.

Setup

Stay in the `~/linux-kernel-labs/src/linux` directory for kernel and DTB compiling (stay in the `nunchuk` branch), and in `~/linux-kernel-labs/modules/nfsroot/root/nunchuk` for module compiling (use two different terminals).

Remove debugging messages

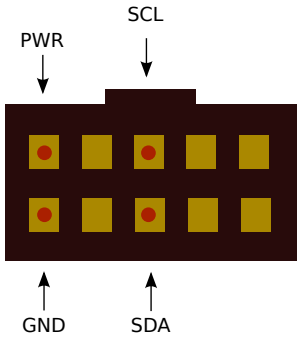
Now that we have checked that the `probe()` and `remove()` functions are called, remove the `pr_info()` messages that you added to trace the execution of these functions.

Connecting the nunchuk

Take the nunchuk device provided by your instructor.

We will connect it to the second I2C port of the CPU (`i2c1`), which pins are available on the `P9` connector.

Now we can identify the 4 pins of the nunchuk connector:

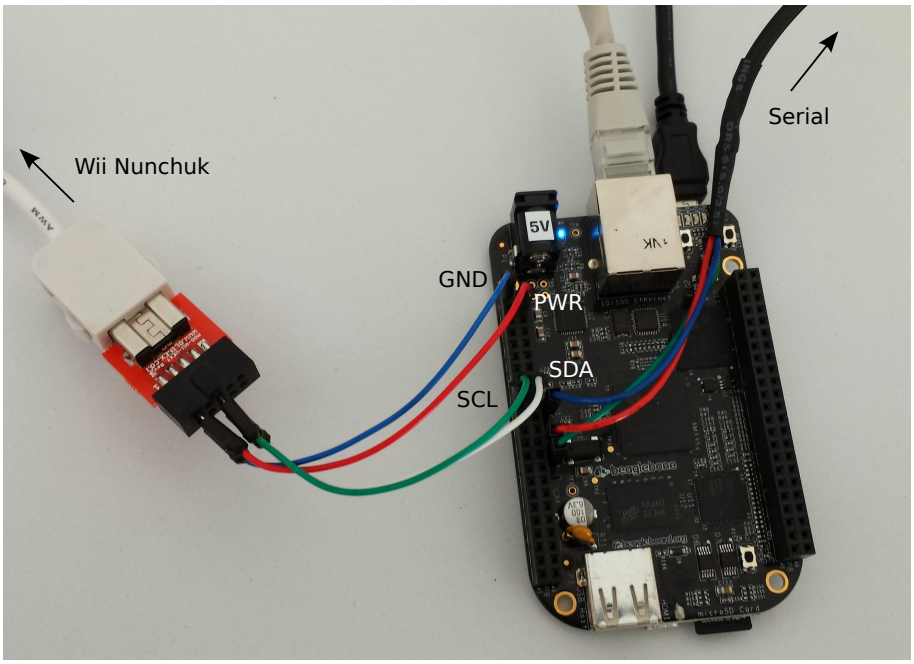


Nunchuk i2c pinout
(UEXT connector from Olimex, front view)

Open the System Reference Manual that you downloaded earlier, and look for "connector P9" in the table of contents, and then follow the link to the corresponding section. Look at the table listing the pinout of the P9 connector.

Now connect the nunchuk pins:

- The GND pin to P9 pins 1 or 2 (GND)
- The PWR pin to P9 pins 3 or 4 (DC_3.3V)
- The SCL pin to P9 pin 17 (I2C1_SCL)
- The SDA pin to P9 pin 18 (I2C1_SDA)



Find pin muxing configuration information for i2c1

As you found in the previous lab, we now managed to have our nunchuk device enumerated on the i2c1 bus.

However, to access the bus data and clock signals, we need to configure the pin muxing of the SoC.

If you go back to the BeagleBone Black System Reference Manual, in the *Connector P9* section, you can see that the pins 17 and 18 that we are using correspond to pins A16 and B16 of the AM335 SoC. You can also see that such pins need to be configured as MODE2 to get the functionality that we need (I2C1_SCL and I2C1_SDA).

The second step is to open the CPU datasheet (am3359.pdf), and look for pin assignment information (*Pin Assignments* section). You will find that the processor is available through two types of packages: ZCE and ZCZ. If you have an original BeagleBoneBlack board, you can have a very close look at the CPU (with your glasses on!) and you will see that the CPU has ZCZ written on its lower right corner. On BeagleBoneBlack Wireless with the Octavo System In Package, you can no longer find such information. Anyway, the ZCZ package information applies to both types of boards.

So, in the *ZCZ Package Pin Maps (Top View)* section[9], you can find hyperlinks to the descriptions of the A16 and B16 pins. That's where you can find reference pin muxing information for

[9] Caution: you won't be able to search the PDF file for this section name, for obscure reasons. At the time of this writing, this section is numbered 4.1.2.

 © 2004-2022 Bootlin, CC BY-SA license

these pins. You can find that the pin name for A16 is SPI0_CS0 and that the pin name for B16 is SPI0_D1. You can also get confirmation that to obtain the (I2C1_SCL and I2C1_SDA) signals, you need to configure muxing mode number 2. You can also see that both pins support pull-up and pull-down modes[10] (see the PULLUP /DOWN TYPE column).

The next thing to do is to open the big TRM document and look for the address of the registers that control pin muxing. First, look for *L4_WKUP Peripheral Memory Map* with your PDF reader search utility. You will find a table containing a Control Module Registers entry with its address: 0x44E1_0000.

Last but not least, look for the SPI0_CS0 and SPI0_D1 pin names, and you will find the offsets for the registers controlling muxing for these pins in the *CONTROL_MODULE REGISTERS* table: respectively 0x95c and 0x958.

We now know which registers we can write to to enable i2c1 signals.

Add pinctrl properties to the Device Tree

Now that we know the register offsets, let's try to understand how they are used in existing code. For example, open the the Device Tree for the AM335x EVM board (arch/arm/boot/dts/am335x-evm.dts), which is using i2c1 too. Look for i2c1_pins, and you will see how offsets are declared and what values they are given:

```
i2c1_pins: pinmux_i2c1_pins {
        pinctrl-single,pins = <
                /* spi0_d1.i2c1_sda */
                AM33XX_PADCONF(AM335X_PIN_SPI0_D1, PIN_INPUT_PULLUP, MUX_MODE2)
                /* spi0_cs0.i2c1_scl */
                AM33XX_PADCONF(AM335X_PIN_SPI0_CS0, PIN_INPUT_PULLUP, MUX_MODE2)
        >;
};
```

Here are details about the values:

- AM335X_PIN_SPI0_D1 and AM335X_PIN_SPI0_CS0 offsets in the Pin Controller registers to control muxing on the corresponding package pins.
- MUX_MODE2 corresponds to muxing mode 2, as explained in the datasheet.
- PIN_INPUT_PULLUP puts the pin in pull-up mode (remember that our pins support both pull-up and pull-down). By design, an I2C line is never actively driven high, devices either pull the line low or let it floating. As we plug our device directly on the bus without more analog electronics, we need to enable the internal pull-up.

Now that pin muxing settings have been explained, edit your board DTS file to add the same definitions to enable pin muxing for i2c1. Don't forget that you don't have to repeat definitions that are already present in the .dtsi files. Just add new declarations, or settings that override common definitions.

Rebuild and update your DTB, and eventually reboot the board.

I2C bus tests

We will use the i2cdetect command to make sure that everything works fine for i2c1:

[10] See https://en.wikipedia.org/wiki/Pull-up_resistor

```
# i2cdetect -l
i2c-0 i2c        OMAP I2C adapter                I2C adapter
i2c-2 i2c        OMAP I2C adapter                I2C adapter
i2c-1 i2c        OMAP I2C adapter                I2C adapter

# i2cdetect -F 1
Functionalities implemented by /dev/i2c-1:
I2C                              yes
SMBus Quick Command              no
SMBus Send Byte                  yes
SMBus Receive Byte               yes
SMBus Write Byte                 yes
SMBus Read Byte                  yes
SMBus Write Word                 yes
SMBus Read Word                  yes
SMBus Process Call               yes
SMBus Block Write                yes
SMBus Block Read                 no
SMBus Block Process Call         no
SMBus PEC                        yes
I2C Block Write                  yes
I2C Block Read                   yes
```

You can see that the *SMBus Quick Commands* are not available on this driver, yet `i2cdetect` uses them by default to scan the i2c bus. You can use `i2cdetect -r` to use the usual set of i2c commands, and be able to detect the devices on your bus.

To test if everything works fine, run `i2cdetect -r 1`. This will scan the `i2c1` bus for devices. You should see a device at the address `0x52`. This is your nunchuk.

If everything works as expected, commit your Device Tree changes. This will be required to switch to another branch later:

`git commit -as`

- `git commit -a` adds all the files already known to `git` to the commit.
- `git commit -s` adds a `Signed-off-by` line (required for all contributions to the Linux kernel).

Device initialization

The next step is to read the state of the nunchuk registers, to find out whether buttons are pressed or not, for example.

Before being able to read nunchuk registers, the first thing to do is to send initialization commands to it. That's also a nice way of making sure i2c communication works as expected.

In the probe routine (run every time a matching device is found):

1. Using the I2C raw API (`i2c_master_send()` and `i2c_master_recv()`), send two bytes to the device: `0xf0` and `0x55`[11]. Make sure you check the return value of the function you're

[11] The I2C messages to communicate with a wiimote extension are in the form: `<i2c_address> <register>` for reading and `<i2c_address> <register> <value>` for writing. The address, `0x52` is sent by the i2c framework so you only have to write the other bytes, the register address and if needed, the value you want to write. There are two ways to set up the communication. The first known way was with data encryption by writing `0x00` to register `0x40` of the nunchuk. With this way, you have to decrypt each byte you read from the nunchuk (not so

 © 2004-2022 Bootlin, CC BY-SA license

using. This could reveal communication issues. Using Elixir, find examples of how to handle failures properly using the same function.

2. Let the CPU wait for 1 ms by using the `udelay()` routine. Let's use Elixir again to find the right C headers to include...

   The Elixir results are a bit confusing here, because `udelay()` is defined in `arch/<arch>/include/asm/delay.h` files, but not in an `include/linux/<file>.h>` that is normally used in kernel code.

   However, look at `include/linux/delay.h` and you will see that it includes `asm/delay.h` which corresponds to the specific headers for the current architecture. So you need to include `linux/delay.h`.

   General rule: whenever the symbol you're looking for is defined in `arch/<arch>/include/asm/<file>.h`, you can include `linux/<file>.h` in your kernel code.

3. In the same way, send the `0xfb` and `0x00` bytes now. This completes the nunchuk initialization.

Recompile and load the driver, and make sure you have no communication errors.

Read nunchuk registers

As the nunchuk does not feature any type of external signaling nor any internal bit to advertize a possible end-of-conversion status, the user is required to regularly poll the registers, each read triggering the next conversion. This leads to a specific situation: the first read triggers the first conversion but returns some data which can be considered garbage and safely discarded.

As a consequence, we will need to read the registers twice the first time!

To keep the code simple and readable, let's create a `nunchuk_read_registers()` function to read the registers once. In this function:

1. Start by putting a `10 ms` delay by calling `usleep_range(10000, 20000)`, guaranteed to sleep between 10 and 20 ms.[12] Such waiting time is needed to add time between the previous i2c operation and the next one.
2. Write `0x00` to the bus. That will allow us to read the device registers.
3. Add another `10 ms` delay.
4. Read 6 bytes from the device, still using the I2C raw API. Check the return value as usual.

Reading the state of the nunchuk buttons

Back to the `probe()` function, call your new function twice.

After the second call, compute the states of the `Z` and `C` buttons, which can be found in the sixth byte that you read.

As explained on `https://bootlin.com/labs/doc/nunchuk.pdf`:

hard but something you have to do). Unfortunately, such encryption doesn't work on third party nunchuks so you have to set up unencrypted communication by writing `0x55` to `0xf0` instead. This works across all brands of nunchuks (including Nintendo ones).

[12] That's better than using `udelay()` because it is not making an active wait, and instead lets the CPU run other tasks in the meantime. You'll find interesting details on how to sleep or wait in kernel code for specified durations in the kernel documentation: `timers/timers-howto`.

- `bit 0 == 0` means that `Z` is pressed.
- `bit 0 == 1` means that `Z` is released.
- `bit 1 == 0` means that `C` is pressed.
- `bit 1 == 1` means that `C` is released.

Using boolean operators, write code that initializes a `zpressed` integer variable, which value is `1` when the `Z` button is pressed, and `0` otherwise. Create a similar `cpressed` variable for the `C` button[13].

The last thing is to test the states of these new variables at the end of the `probe()` function, and log a message to the console when one of the buttons is pressed.

Testing

Compile your module, and reload it. No button presses should be detected. Remove your module.

Now hold the `Z` button and reload and remove your module again:

```
insmod /root/nunchuk/nunchuk.ko; rmmod nunchuk
```

You should now see the message confirming that the driver found out that the `Z` button was held.

Do the same over and over again with various button states.

At this stage, we just made sure that we could read the state of the device registers through the I2C bus. Of course, loading and removing the module every time is not an acceptable way of accessing such data. We will give the driver a proper *input* interface in the next slides.

[13] You may use the `BIT()` macro, which will make your life easier. See Elixir for details.

 © 2004-2022 Bootlin, CC BY-SA license

Input interface

Objective: make the I2C device available to user space using the input subsystem.

After this lab, you will be able to:

- Expose device events to user space through an input interface, using the kernel based polling API for input devices (kernel space perspective).
- Handle registration and allocation failures in a clean way.
- Get more familiar with the usage of the input interface (user space perspective).

Add input event interface support to the kernel

For this lab, you need to rebuild your kernel with static input event interface (`CONFIG_INPUT_EVDEV`) support. With the default configuration, this feature is available as a module, which is less convenient.

Update and reboot your kernel.

Register an input interface

The first thing to do is to add an input device to the system. Here are the steps to do it:

- Declare a pointer to an `input_dev` structure in the `probe` routine. You can call it `input`. You can't use a global variable because your driver needs to be able to support multiple devices.
- Allocate such a structure in the same function, using the `devm_input_allocate_device()` function.
- Still in the `probe()` function, add the input device to the system by calling `input_register_device()`;

At this stage, first make sure that your module compiles well (add missing headers if needed).

Handling probe failures

In the code that you created, make sure that you handle failure situations properly.

- Of course, test return values properly and log the causes of errors.
- In our case, we only allocated resources with `devm_` functions. Thanks to this, in case of failure, all the corresponding allocations are automatically released before destroying the `device` structure for each device. This greatly simplifies our error management code!

© 2004-2022 Bootlin, CC BY-SA license

Implement the remove() function

In this function, we need to unregister and release the resources allocated and registered in the `probe()` routine.

Fortunately, in our case, there's nothing to do, as everything was allocated with `devm_` functions. Even the unregistration of the `input_dev` structure is automated.

Recompile your module, and load it and remove it multiple times, to make sure that everything is properly registered and automatically unregistered.

Add proper input device registration information

We actually need to add more information to the `input` structure before registering it. That's why we are getting the below warnings:

```
input: Unspecified device as /devices/virtual/input/input0
```

Add the below lines of code (still before device registration, of course):

```
input->name = "Wii Nunchuk";
input->id.bustype = BUS_I2C;

set_bit(EV_KEY, input->evbit);
set_bit(BTN_C, input->keybit);
set_bit(BTN_Z, input->keybit);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/input-device-attributes.c)

Recompile and reload your driver. You should now see in the kernel log that the `Unspecified device` type is replaced by `Wii Nunchuk`.

Implement a polling routine

The nunchuk doesn't have interrupts to notify the I2C master that its state has changed. Therefore, the only way to access device data and detect changes is to regularly poll its registers.

So, it's time to implement a routine which will poll the nunchuk registers at a regular interval.

Create a `nunchuk_poll()` function with the right prototype (find it by looking at the definition of the `input_setup_polling()` function.)

In this function, you will have to read the nunchuk registers. However, as you can see, the prototype of the `poll_fn()` routine doesn't carry any information about the `i2c_client` structure you will need to communicate with the device. That's normal as the input subsystem is generic, and can't be bound to any specific bus.

This raises a very important aspect of the device model: the need to keep pointers between *physical* devices (devices as handled by the physical bus, I2C in our case) and *logical* devices (devices handled by subsystems, like the input subsystem in our case).

This way, when the `remove()` routine is called, we can find out which logical device to unregister (though that's not necessary in our case as logical device unregistration is automatic). Conversely, when we have an event on the logical side (such as running the polling function), we can find out which I2C device this corresponds to, to communicate with the hardware.

 © 2004-2022 Bootlin, CC BY-SA license

This need is typically implemented by creating a per device, *private* data structure to manage our device and implement such pointers between the physical and logical worlds.

Add the below global definition to your code:

```
struct nunchuk_dev {
        struct i2c_client *i2c_client;
};
```

Now, in your `probe()` routine, declare an instance of this structure:

```
struct nunchuk_dev *nunchuk;
```

Then allocate one such instead for each new device:

```
nunchuk = devm_kzalloc(&client->dev, sizeof(struct nunchuk_dev), GFP_KERNEL);
if (!nunchuk)
        return -ENOMEM;
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/private-data-alloc.c)

Note that we haven't seen kernel memory allocator routines and flags yet.

Also note that here there's no need to write an "out of memory" message to the kernel log. That's already done by the memory subsystem.

Now implement the pointers that we need:

```
nunchuk->i2c_client = client;
input_set_drvdata(input, nunchuk);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/device-pointers.c)

Make sure you add this code before registering the input device. You don't want to enable a device with incomplete information or when it is not completely initialized yet (there could be race conditions).

So, back to the `nunchuk_poll()` function, you will first need to retrieve the I2C physical device from the `input_dev` structure. That's where you will use your private `nunchuk` structure.

Now that you have a handle on the I2C physical device, you can move the code reading the nunchuk registers to this function. You can remove the double reading of the device state, as the polling function will make periodic reads anyway[14].

At the end of the polling routine, the last thing to do is post the events and notify the `input` core. Assuming that `input` is the name of the `input_dev` parameter of your polling routine:

```
input_report_key(input, BTN_Z, zpressed);
input_report_key(input, BTN_C, cpressed);
input_sync(input);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/input-notification.c)

Now, back to the `probe()` function, the last thing to do is to declare the new polling function (see the slides if you forgot about the details) and specify a polling interval of 50 ms.

[14] During the move, you will have to handle communication errors in a slightly different way, as the `nunchuk_poll()` routine has a `void` type. When the function reading registers fails, you can use a `return;` statement instead of `return value;`

At this stage, also remove the debugging messages about the state of the buttons. You will get that information from the input interface.

You can now make sure that your code compiles and loads successfully.

Testing your input interface

Testing an input device is easy with the `evtest` application that is included in the root filesystem. Just run:

```
evtest
```

The application will show you all the available input devices, and will let you choose the one you are interested in (make sure you type a choice, `0` by default, and do not just type `[Enter]`). You can also type `evtest /dev/input/event0` right away.

Press the various buttons and see that the corresponding events are reported by `evtest`.

Going further

Stopping here is sufficient, but if you complete your lab before the others, you can try to achieve the below challenges (in any order):

Supporting multiple devices

Modify the driver and Device Tree to support two nunchuks at the same time. You can borrow another nunchuk from the instructor or from a fellow participant.

Making sure that your driver does indeed support multiple devices at the same time is a good way to make sure it is implemented properly.

Use the nunchuk as a joystick in an ascii game

In this optional, challenge, you will extend the driver to expose the joystick part of the nunchuk, i.e. x and y coordinates.

We will use the *nInvaders* game, which is already present in your root filesystem.

Connect through SSH

nInvaders will not work very well over the serial port, so you will need to log to your system through `ssh` in an ordinary terminal:

```
ssh root@192.168.0.100
```

The password for the *root* user is `root`.

You can already play the `nInvaders` game with the keyboard!

Note: if you get the error `Error opening terminal: xterm-256color.` when running `nInvaders`, issue first the `export TERM=xterm` command.

 © 2004-2022 Bootlin, CC BY-SA license

Recompile your kernel

Recompile your kernel with support for the joystick interface (CONFIG_INPUT_JOYDEV).

Reboot to the new kernel.

Extend your driver

We are going to expose the joystick X and Y coordinates through the input device.

Add the below code to the `probe` routine:

```
set_bit(ABS_X, input->absbit);
set_bit(ABS_Y, input->absbit);
input_set_abs_params(input, ABS_X, 30, 220, 4, 8);
input_set_abs_params(input, ABS_Y, 40, 200, 4, 8);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/declare-x-and-y.c)

See input/input-programming for details about the input_set_abs_params() function.

For the joystick to be usable by the application, you will also need to declare *classic* buttons:

```
/* Classic buttons */

set_bit(BTN_TL, input->keybit);
set_bit(BTN_SELECT, input->keybit);
set_bit(BTN_MODE, input->keybit);
set_bit(BTN_START, input->keybit);
set_bit(BTN_TR, input->keybit);
set_bit(BTN_TL2, input->keybit);
set_bit(BTN_B, input->keybit);
set_bit(BTN_Y, input->keybit);
set_bit(BTN_A, input->keybit);
set_bit(BTN_X, input->keybit);
set_bit(BTN_TR2, input->keybit);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-i2c-input-interface/declare-classic-buttons.c)

The next thing to do is to retrieve and report the joystick X and Y coordinates in the polling routine. This should be very straighforward. You will just need to go back to the nunchuk datasheet to find out which bytes contain the X and Y values.

Time to play

Recompile and reload your driver.

You can now directly play *nInvaders*, only with your nunchuk. You'll quickly find how to move your ship, how to shoot and how to pause the game.

Have fun!

© 2004-2022 Bootlin, CC BY-SA license

Accessing I/O memory and ports

Objective: read / write data from / to a hardware device

Throughout the upcoming labs, we will implement a character driver allowing to write data to additional CPU serial ports available on the BeagleBone, and to read data from them.

After this lab, you will be able to:

- Add UART devices to the board device tree.
- Access I/O registers to control the device and send first characters to it.

Setup

Go to your kernel source directory.

Create a new branch for this new series of labs. Since this new stuff is independent from the nunchuk changes, it's best to create a separate branch!

```
git checkout 5.10.bootlin
git checkout -b uart
```

Add UART devices

Before developing a driver for additional UARTS on the board, we need to add the corresponding descriptions to the board Device Tree.

First, open the board reference manual and find the connectors and pinmux modes for UART2 and UART4.

Using a new USB-serial cable with male connectors, provided by your instructor, connect your PC to UART2. The wire colors are the same as for the cable that you're using for the console:

- The blue wire should be connected `GND`.
- The red wire (`TX`) should be connected to the board's `RX` pin.
- The green wire (`RX`) should be connected to the board's `TX` pin.

Now, create again a new `arch/arm/boot/dts/am335x-customboneblack.dts` file including the standard board DTS file and create a pin muxing section with declarations for UART2 and UART4.

```
/* Pins 21 (TX) and 22 (RX) of connector P9 */
uart2_pins: uart2_pins {
        pinctrl-single,pins = <
                /* (A17) spi0_sclk.uart2_rxd */
                AM33XX_PADCONF(AM335X_PIN_SPI0_SCLK, PIN_INPUT_PULLUP, MUX_MODE1)
                /* (B17) spi0_d0.uart2_txd */
                AM33XX_PADCONF(AM335X_PIN_SPI0_D0, PIN_OUTPUT, MUX_MODE1)
        >;
};

/* Pins 11 (RX) and 13 (TX) of connector P9 */
uart4_pins: uart4_pins {
        pinctrl-single,pins = <
```

 © 2004-2022 Bootlin, CC BY-SA license

```
                /* (T17) gpmc_wait0.uart4_rxd */
                AM33XX_PADCONF(AM335X_PIN_GPMC_WAIT0, PIN_INPUT_PULLUP, MUX_MODE6)
                /* (U17) gpmc_wpn.uart4_txd */
                AM33XX_PADCONF(AM335X_PIN_GPMC_WPN, PIN_OUTPUT, MUX_MODE6)
        >;
};
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-serial-iomem/uarts-pinctrl.dts)

Then, declare the corresponding devices:

```
&uart2 {
        compatible = "bootlin,serial";
        status = "okay";
        pinctrl-names = "default";
        pinctrl-0 = <&uart2_pins>;
};

&uart4 {
        compatible = "bootlin,serial";
        status = "okay";
        pinctrl-names = "default";
        pinctrl-0 = <&uart4_pins>;
};
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-serial-iomem/uarts.dts)

This is a good example of how we can override definitions in the Device Tree. `uart2` and `uart4` are already defined in `arch/arm/boot/dts/am33xx.dtsi`. In the above code, we just override a few properties and add missing ones: duplicate the valid ones:

- `compatible`: use our driver instead of using the default one (`omap3-uart`).
- `status`: enable the device (was set to `disabled` in the original definition.
- `pinctrl-names`, `pinctrl-0`: add pinmux settings (none were defined so far).

Compile and update your DTB.

Operate a platform device driver

Go to the `~/linux-kernel-labs/modules/nfsroot/root/serial/` directory. You will find a `serial.c` file which already provides a platform driver skeleton.

Add the code needed to match the driver with the devices which you have just declared in the device tree.

Compile your module and load it on your target. Check the kernel log messages, that should confirm that the `probe()` routine was called[15].

Create a device private structure

In the same way as in the nunchuk lab, we now need to create a structure that will hold device specific information and help keeping pointers between logical and physical devices.

[15] Don't be surprised if the `probe()` routine is actually called twice! That's because we have declared two devices. Even if we only connect a serial-to-USB dongle to one of them, both of them are ready to be used!

As the first thing to store will be the base virtual address for each device, let's declare this structure as follows:

```
struct serial_dev {
        void __iomem *regs;
};
```

The first thing to do is allocate such a structure at the beginning of the `probe()` routine. Let's do it with the `devm_kzalloc()` function again as in the previous lab. Again, resource deallocation is automatically taken care of when we use the `devm_` functions.

So, add the below line to your code:

```
struct serial_dev *serial;
...
serial = devm_kzalloc(&pdev->dev, sizeof(*serial), GFP_KERNEL);
if (!serial)
        return -ENOMEM;
```

Get a base virtual address for your device registers

You can now get a virtual address for your device's base physical address, by calling:

```
serial->regs = devm_platform_ioremap_resource(pdev, 0);
if (IS_ERR(serial->regs))
        return PTR_ERR(serial->regs);
```

What's nice is that you won't ever have to release this resource, neither in the `remove()` routine, nor if there are failures in subsequent steps of the `probe()` routine.

Make sure that your updated driver compiles, loads and unloads well.

Device initialization

Now that we have a virtual address to access registers, we are ready to configure a few registers which will allow us to enable the UART devices. Of course, this will be done in the `probe()` routine.

Accessing device registers

As we will have multiple registers to read, create a `reg_read()` routine, returning an `unsigned int` value, and taking a `serial` pointer to a `serial_dev` structure and an `int` register offset.

Your prototype should look like:

```
static u32 reg_read(struct serial_dev *serial, unsigned int reg);
```

In this function, read from a 32 bits register at the base virtual address for the device plus the register offset multiplied by 4.

All the UART register offsets have standardized values, shared between several types of serial drivers (see `include/uapi/linux/serial_reg.h`). This explains why they are not completely ready to use and we have to multiply them by 4 for OMAP SoCs.

Create a similar `reg_write()` routine, writing an `int` value at a given register offset (don't forget to multiply it by 4) from the device base virtual address. The following code samples are using

 © 2004-2022 Bootlin, CC BY-SA license

the writel() convention of passing the value first, then the offset. Your prototype should look like:

```
static void reg_write(struct serial_dev *serial, u32 val, unsigned int reg);
```

In the next sections, we will tell you what register offsets to use to drive the hardware.

Power management initialization

Add the below lines to the probe function:

```
pm_runtime_enable(&pdev->dev);
pm_runtime_get_sync(&pdev->dev);
```

And add the below line to the remove() routine:

```
pm_runtime_disable(&pdev->dev);
```

Line and baud rate configuration

After these lines, let's add code to initialize the line and configure the baud rate. This shows how to get a special property from the device tree, in this case clock-frequency:

```
/* Configure the baud rate to 115200 */
ret = of_property_read_u32(pdev->dev.of_node, "clock-frequency",
                           &uartclk);
if (ret) {
        dev_err(&pdev->dev,
                "clock-frequency property not found in Device Tree\n");
        return ret;
}

baud_divisor = uartclk / 16 / 115200;
reg_write(serial, 0x07, UART_OMAP_MDR1);
reg_write(serial, 0x00, UART_LCR);
reg_write(serial, UART_LCR_DLAB, UART_LCR);
reg_write(serial, baud_divisor & 0xff, UART_DLL);
reg_write(serial, (baud_divisor >> 8) & 0xff, UART_DLM);
reg_write(serial, UART_LCR_WLEN8, UART_LCR);
reg_write(serial, 0x00, UART_OMAP_MDR1);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-serial-iomem/uart-line-init.c)

Declare baud_divisor and uartclk as unsigned int.

FIFOs reset

The last thing to do is to reset the FIFOs:

```
/* Clear UART FIFOs */
reg_write(serial, UART_FCR_CLEAR_RCVR | UART_FCR_CLEAR_XMIT, UART_FCR);
```

(Source code link: https://raw.githubusercontent.com/bootlin/training-materials/master/labs/kernel-serial-iomem/uart-line-reset.c)

We are now ready to transmit characters over the serial ports!

If you have a bit of spare time, you can look at section 19 of the AM335x TRM for details about how to use the UART ports, to understand better what we are doing here.

Standalone write routine

Implement a C routine taking a pointer to a `serial_dev` structure and one character as parameters, and writing this character to the serial port, using the following steps:

1. Wait until the `UART_LSR_THRE` bit gets set in the `UART_LSR` register. You can busy-wait for this condition to happen. In the busy-wait loop, you can call the `cpu_relax()` kernel function to ensure the compiler won't optimise away this loop.
2. Write the character to the `UART_TX` register.

Add a call to this routine from your module `probe()` function, and recompile your module.

Open a new `picocom` instance on your new serial port (not the serial console):

```
picocom -b 115200 /dev/ttyUSB1
```

Load your module on the target. You should see the corresponding character in the new `picocom` instance, showing what was written to UART2.

You can also check that you also get the same character on UART4 (just connect to the UART4 pins instead of the UART2 ones).

Driver sanity check

Remove your module and try to load it again. If the second attempt to load the module fails, it is probably because your driver doesn't properly free the resources it allocated or registered, either at module exit time, or after a failure during the module `probe()` function. Check and fix your module code if you have such problems.

 © 2004-2022 Bootlin, CC BY-SA license

Output-only misc driver

Objective: implement the write part of a misc *driver*

After this lab, you will be able to:

- Write a simple misc driver, allowing to write data to the serial ports of your Beaglebone.
- Write simple `file_operations` functions for a device, including `ioctl` controls.
- Copy data from user memory space to kernel memory space and eventually to the device.
- You will practice kernel standard error codes a little bit too.

You must have completed the previous lab to work on this one.

Misc driver registration

In the same way we added an input interface to our Nunchuk driver, it is now time to give an interface to our serial driver. As our needs are simple, we won't use the *Serial framework* provided by the Linux kernel, but will use the *Misc framework* to implement a simple character driver.

Let's start by adding the infrastructure to register a *misc* driver.

The first thing to do is to create:

- A `serial_write()` write file operation stub. See the slides or the code for the prototype to use. Just place a `return -EINVAL;` statement in the function body so far, to signal that there is something wrong with this function so far.
- Similarly, a `serial_read()` read file operation stub.
- A `file_operations` structure declaring these file operations.

The next step is to create a `miscdevice` structure and initialize it. However, we are facing the same usual constraint to handle multiple devices. Like in the Nunchuk driver, we have to add such a structure to our device specific private data structure:

```
struct serial_dev {
        void __iomem *regs;
        struct miscdevice miscdev;
};
```

To be able to access our private data structure in other parts of the driver, you need to attach it to the `pdev` structure using the `platform_set_drvdata()` function. Look for examples in the source code to find out how to do it.

Now, at the end of the `probe()` routine, when the device is fully ready to work, you can now initialize the `miscdevice` structure for each found device:

- To get an automatically assigned minor number.
- To specify a name for the device file in *devtmpfs*. We propose to use:

```
struct resource *res;
[...]
res = platform_get_resource(pdev, IORESOURCE_MEM, 0);
/* Error handling */
[...]
devm_kasprintf(&pdev->dev, GFP_KERNEL, "serial-\%x", res->start);
```

`devm_kasprintf()` allocates a buffer and runs `kasprintf()` to fill its contents. `platform_get_resource()` is used to retrieve the device physical address from the device tree. A much simpler solution to get a unique name for the device file would have been to use `&pdev->name`, but this would create unusual names for device files (e.g. `48024000.serial`).

- To pass the `file_operations` structure that you defined.
- To set the `parent` pointer to the appropriate value.

See the lectures for details if needed!

The last things to do (at least to have a *misc* driver, even if its file operations are not ready yet), are to add the registration and deregistration routines. That's typically the time when you will need to access the `serial_dev` structure for each device from the `pdev` structure passed to the `remove()` routine.

Make sure that your driver compiles and loads well, and that you now see two new device files in `/dev`.

At this stage, make sure you can load and unload the driver multiple times. This should reveal registration and deregistration issues if there are any.

Check in `/sys/class/misc` for an entry corresponding to the registered devices, and within those directories, check what the `device` symbolic link is pointed to. Check the contents of the `dev` file as well, and compare it with the major/minor number of the device nodes created in `/dev` for your devices.

Implement the write() routine

Now, add code to your write function, to copy user data to the serial port, writing characters one by one.

The first thing to do is to retrieve the `serial_dev` structure from the `miscdevice` structure itself, accessible through the `private_data` field of the open file structure (`file`).

At the time we registered our *misc* device, we didn't keep any pointer to the `serial_dev` structure. However, as the `struct miscdevice` structure is accessible through `file->private_data`, and is a member of the `serial_dev` structure, we can use a magic macro to compute the address of the parent structure:

```
struct serial_dev *serial =
container_of(file->private_data, struct serial_dev, miscdev);
```

See https://radek.io/2012/11/10/magical-container_of-macro/ for interesting implementation details about this macro.

This wouldn't have been possible if the `struct miscdevice` structure was allocated separately and was just referred to by a pointer in `serial_dev`, instead of being a member of it.

 © 2004-2022 Bootlin, CC BY-SA license

Another possibility, but more complicated, would have been to access the `parent` device pointer in `struct miscdevice`, which then through the `platform_get_drvdata()` function would have given us access to the `serial_dev` structure containing the virtual address of the device. There are always multiple possibilities in kernel programming!

Now, add code that copies (in a secure way) each character from the user space buffer to the UART device.

Once done, compile and load your module. Test that your `write` function works properly by using (example for UART2):

```
echo "test" > /dev/serial-48024000
```

The `test` string should appear on the remote side (i.e in the `picocom` process connected to `/dev/ttyUSB1`).

If it works, you can triumph and do a victory dance in front of the whole class!

Make sure that both UART devices work on the same way.

You'll quickly discover that newlines do not work properly. To fix this, when the user space application sends `"\n"`, you must send `"\n\r"` to the serial port[16].

Module reference counting

Start an application in the background that writes nothing to the UART:

```
cat > /dev/serial-48024000 &
```

Now, with `lsmod`, look at the reference count of your module: it is still 0, even though an application has your device opened. This means that you can `rmmod` your module even when an application is using it, which is not correct and can quickly cause a kernel crash.

To fix this, we need to tell the kernel that our module is in charge of this character device. This is done by setting the `.owner` field of `struct file_operations` to the special value `THIS_MODULE`.

After changing this, make sure the reference counter of your module, visible through `lsmod`, gets incremented when you run an application that uses the UART.

Ioctl operations

We would like to maintain a count of the number of characters written through the serial port. In order to do this, register a counter variable in the main driver structure, and increment it when appropriate. Then, we need to implement two `unlocked_ioctl()` operations:

- `SERIAL_RESET_COUNTER`, which as its name says, will reset the counter to zero
- `SERIAL_GET_COUNTER`, which will return the current value of the counter in a variable passed by address.

Two test applications (in source format) are already available in the `root/serial/` NFS shared directory. They assume that `SERIAL_RESET_COUNTER` is ioctl operation `0` and that `SERIAL_GET_COUNTER` is ioctl operation `1`.

Compile them:

[16] See https://en.wikipedia.org/wiki/Newline for details about the newline (`\n`) and carriage return (`\r`) characters

```
arm-linux-gnueabi-gcc -static -o serial-get-counter serial-get-counter.c
arm-linux-gnueabi-gcc -static -o serial-reset-counter serial-reset-counter.c
```

The new executables are then ready to run on your target. They take as argument the path to the device file corresponding to your UART.

 © 2004-2022 Bootlin, CC BY-SA license

Sleeping and handling interrupts

Objective: learn how to register and implement a simple interrupt handler, and how to put a process to sleep and wake it up at a later point

During this lab, you will:

- Register an interrupt handler for the serial controller of the Beaglebone.
- Implement the read() operation of the serial port driver to put the process to sleep when no data are available.
- Implement the interrupt handler to wake-up the sleeping process waiting for received characters.
- Handle communication between the interrupt handler and the read() operation.

Setup

This lab is a continuation of the *Output-only misc driver lab*. Use the same kernel, environment and paths!

Register the handler

Declare an interrupt handler function stub. Then, in the module probe function, we need to register this handler, binding it to the right IRQ number.

Nowadays, Linux is using a virtual IRQ number that it derives from the hardware interrupt number. This virtual number is created through the `irqdomain` mechanism. The hardware IRQ number to use is found in the device tree.

First, retrieve the unique IRQ number to request:

```
int irq;
irq = platform_get_irq(pdev, 0);
```

Then, pass the interrupt number to `devm_request_irq()` along with the interrupt handler to register your interrupt in the kernel.

Then, in the interrupt handler, just print a message and return `IRQ_HANDLED` (to tell the kernel that we have handled the interrupt).

You'll also need to enable interrupts. To do so, in the `probe()` function, write `UART_IER_RDI` to the `UART_IER` register.

Compile and load your module. Send a character on the serial link (just type something in the corresponding `picocom` terminal, and look at the kernel logs: they are full of our message indicating that interrupts are occurring, even if we only sent one character! It shows you that interrupt handlers should do a little bit more when an interrupt occurs.

© 2004-2022 Bootlin, CC BY-SA license

Enable and filter the interrupts

In fact, the hardware will replay the interrupt until you acknowledge it. Linux will only dispatch the interrupt event to the rightful handler, hoping that this handler will acknowledge it. What we experienced here is called an `interrupt flood`.

Now, in our interrupt handler, we want to acknowledge the interrupt. On the UART controllers that we drive, it's done simply by reading the contents of the `UART_RX` register, which holds the next character received. You can display the value you read to see that the driver will receive whatever character you sent.

Compile and load your driver. Have a look at the kernel messages. You should no longer be flooded with interrupt messages. In the kernel log, you should see the message of our interrupt handler. If not, check your code once again and ask your instructor for clarification!

Load and unload your driver multiple times, to make sure that there are no registration / deregistration issues.

Sleeping, waking up and communication

Now, we would like to implement the `read()` operation of our driver so that a user space application reading from our device can receive the characters from the serial port.

First, we need a communication mechanism between the interrupt handler and the `read()` operation. We will implement a very simple circular buffer. So let's add a device-specific buffer to our `serial_dev` structure.

Let's also add two integers that will contain the next location in the circular buffer that we can write to, and the next location we can read from:

```
#define SERIAL_BUFSIZE 16

struct serial_dev {
        void __iomem *regs;
        struct miscdevice miscdev;
        unsigned int counter
        char buf[SERIAL_BUFSIZE];
        unsigned int buf_rd;
        unsigned int buf_wr;
};
```

In the interrupt handler, store the received character at location `buf_wr` in the circular buffer, and increment the value of `buf_wr`. If this value reaches `SERIAL_BUFSIZE`, reset it to zero.

In the `read()` operation, if the `buf_rd` value is different from the `buf_wr` value, it means that one character can be read from the circular buffer. So, read this character, store it in the user space buffer, update the `buf_rd` variable, and return to user space (we will only read one character at a time, even if the user space application requested more than one).

Now, what happens in our `read()` function if no character is available for reading (i.e, if `buf_wr` is equal to `buf_rd`)? We should put the process to sleep!

To do so, add a `wait_queue_head_t` wait queue to our `serial_dev` structure, named for example `wait`. In the `read()` function, keep things simple by directly using `wait_event_interruptible()`

 © 2004-2022 Bootlin, CC BY-SA license

right from the start, to wait until `buf_wr` is different from `buf_rd`[17].

Last but not least, in the interrupt handler, after storing the received characters in the circular buffer, use `wake_up()` to wake up all processes waiting on the wait queue.

Compile and load your driver. Run `cat /dev/serial-48024000` on the target, and then in `picocom` on the development workstation side, type some characters. They should appear on the remote side if everything works correctly!

Don't be surprised if the keys you type in Picocom don't appear on the screen. This happens because they are not echoed back by the target.

[17] A single test in the `wait_event_interruptible()` function is sufficient. If the condition is met, you don't go to sleep and read one character right away. Otherwise, when you wake up, you can proceed to the reading part.

Locking

Objective: practice with basic locking primitives

During this lab, you will:

- Practice with locking primitives to implement exclusive access to the device.

Setup

Continue to work with the `serial` driver.

You need to have completed the previous two labs to perform this one.

Adding appropriate locking

We have two shared resources in our driver:

- The buffer that allows to transfer the read data from the interrupt handler to the `read()` operation.
- The device itself. It might not be a good idea to mess with the device registers at the same time and in two different contexts.

Therefore, your job is to add a spinlock to the driver, and use it in the appropriate locations to prevent concurrent accesses to the shared buffer and to the device.

Please note that you don't have to prevent two processes from writing at the same time: this can happen and is a valid behavior. However, if two processes write data at the same time to the serial port, the serial controller should not get confused.

 © 2004-2022 Bootlin, CC BY-SA license

Kernel debugging mechanisms and kernel crash analysis

Objective: Use kernel debugging mechanisms and analyze a kernel crash

In this lab, we will continue to work on the code of our serial driver.

dev_dbg() and dynamic debugging

Add a `dev_dbg()` call in the `write()` operation that shows each character being written (or its hexadecimal representation) and add a similar `dev_dbg()` call in your interrupt handler to show each character being received.

Check what happens with your module. Do you see the debugging messages that you added? Your kernel probably does not have `CONFIG_DYNAMIC_DEBUG` set and your driver is not compiled with `DEBUG` defined, so you shouldn't see any message.

Now, recompile your kernel with the following options:

- `CONFIG_DYNAMIC_DEBUG`: this will allow you to see debugging messages.
- `CONFIG_DEBUG_INFO`: this option will make it possible to see source code in disassembled kernel code. We will need it in a later part of this lab, but enabling it now will allow to avoid recompiling the whole kernel again.

Once this is done, in U-Boot, add `loglevel=8` to the kernel command line to get the debugging messages directly in the console (otherwise you will only see them in `dmesg`).

Now boot your updated kernel.

The dynamic debug feature can be configured using `debugfs`, so you'll have to mount the `debugfs` filesystem first. Then, after reading the dynamic debug documentation in the kernel sources, do the following things:

- List all available debug messages in the kernel.
- Enable all debugging messages of your serial module, and check that you indeed see these messages.
- Enable just one single debug message in your serial module, and check that you see just this message and not the other debug messages of your module.

Now, you have a good mechanism to keep many debug messages in your drivers and be able to selectively enable only some of them.

debugfs

After using `debugfs` for controlling the dynamic debug feature, let's add a new entry in this filesystem. Modify your driver to add:

© 2004-2022 Bootlin, CC BY-SA license

- A directory called after a unique name per device in the `debugfs` filesystem.
- And file called `counter` inside this directory of the `debugfs` filesystem. This file should allow to see the contents of the `counter` variable of your module.

Recompile and reload your driver, and check that in `/sys/kernel/debug/<unique name>/counter` you can see the amount of characters that have been transmitted by your driver.

Kernel crash analysis

Setup

Go to the `~/linux-kernel-labs/modules/nfsroot/root/debugging/` directory.

Compile the `drvbroken` in this directory, and load it on your board. See it crashing in a nice way.

Analyzing the crash message

Analyze the crash message carefully. Knowing that on ARM, the `PC` register contains the location of the instruction being executed, find in which function does the crash happen, and what the function call stack is.

Using Elixir or the kernel source code, have a look at the definition of this function. This, with a careful review of the driver source code should probably be enough to help you understand and fix the issue.

Locating the exact line where the error happens

Even if you already found out which instruction caused the crash, it's useful to use information in the crash report.

If you look again, the report tells you at what offset in the function this happens. Let's disassemble the code for this function to understand exactly where the issue happened.

That's where we need a kernel compiled with `CONFIG_DEBUG_INFO` as we did at the beginning of this lab. This way, the kernel is compiled with `$(CROSSCOMPILE)gcc -g`, which keeps the source code inside the binaries.

You could disassemble the whole `vmlinux` file and work with the `PC` absolute address, but it is going to take a long time.

Instead, using Elixir or `cscope`, you'll find that the crash happens in an function defined in assembly, called by a function implemented in C. Find the `.c` source file where the C function is implemented.

In the kernel sources, you can then find and dissassemble the corresponding `.o` file:

```
arm-linux-gnueabi-objdump -S file.o > file.S
```

Another way to do this is to use gdb-multiarch[18]:

[18] gdb-multiarch is a new package supporting multiple architectures at once. If you have a cross toolchain including gdb, you can also run arm-linux-gdb directly.

 © 2004-2022 Bootlin, CC BY-SA license

```
sudo apt install gdb-multiarch
gdb-multiarch vmlinux
(gdb) set arch arm
(gdb) set gnutarget elf32-littlearm
(gdb) disassemble function_name
```

Then, in the disassembled code, find the start address of the function, and using an hexadecimal calculator, add the offset that was provided in the crash output. That's how you can find the exact assembly instruction where the crash occured, together with the C code it was compiled from. Looking at the addresses handled by this code, you can now guess what is wrong in the data passed to the stack of kernel functions called by the broken module.

A little understanding of assembly instructions on the architecture you are working on helps, but seeing the original C code should answer most questions.

Note that the same technique works if the error comes directly from the code of a module. Just dissassemble the `.o` file the `.ko` file was generated from.

© 2004-2022 Bootlin, CC BY-SA license