

CS315 Lab8

Name: 王奕童

SID: 11910104

2 Background

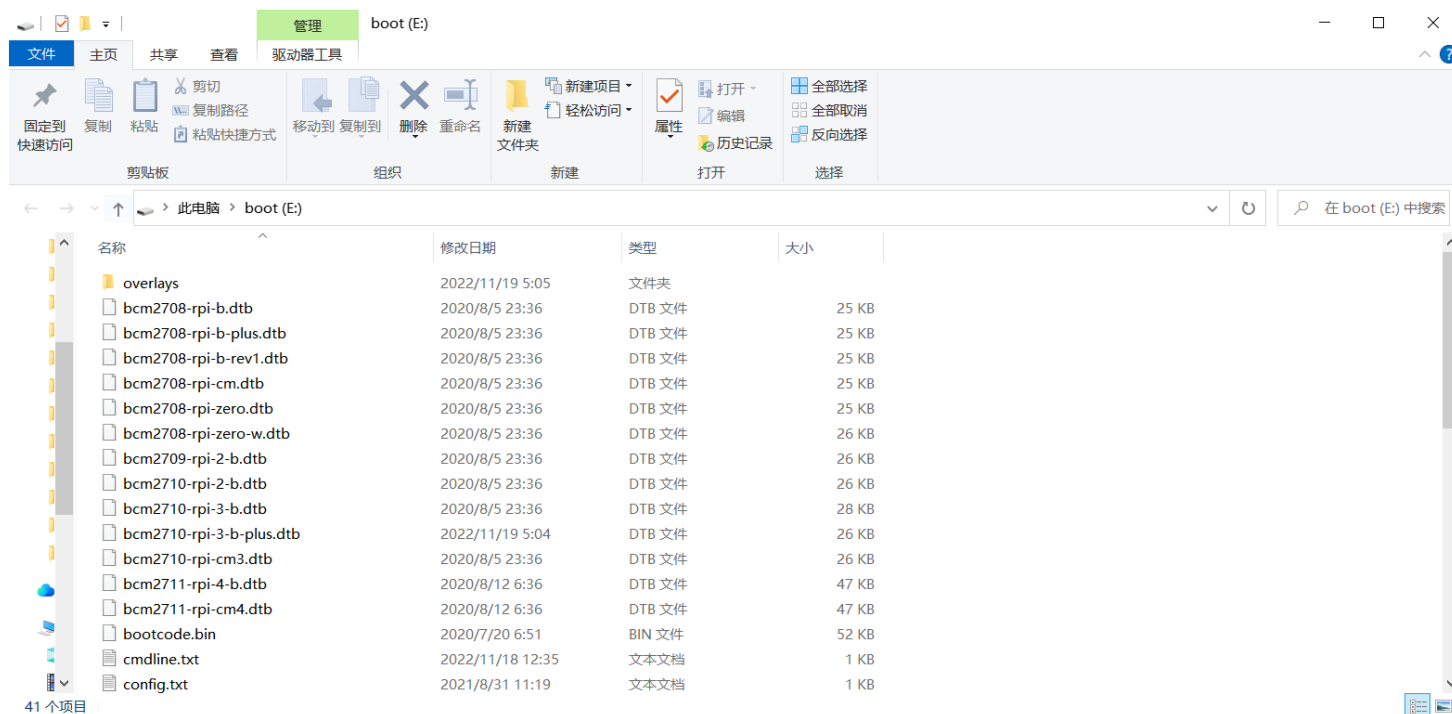
2.1 Your Tools

2.1.1 Hardware

我做这个实验使用了张睿豪同学的树莓派板子。

2.1.2 Boot directory

我将树莓派的sd卡拔出来放到电脑上连接，可以正确显示boot目录。



2.1.3 Source Code of Linux Kernel

已clone至ubuntu虚拟机中：

```
cs315@ubuntu: ~/Desktop
remote: Enumerating objects: 10286559, done.
remote: Total 10286559 (delta 0), reused 0 (delta 0), pack-reused 10286559
Receiving objects: 100% (10286559/10286559), 3.13 GiB | 4.83 MiB/s, done.
Resolving deltas: 100% (8613860/8613860), done.
Checking objects: 100% (33554432/33554432), done.
Updating files: 100% (61894/61894), done.
cs315@ubuntu:~/Desktop$ git clone git://github.com/raspberrypi/tools.git
Cloning into 'tools'...
fatal: unable to connect to github.com:
github.com[0: 20.205.243.166]: errno=Connection refused

cs315@ubuntu:~/Desktop$ git clone git://github.com/raspberrypi/tools.git
Cloning into 'tools'...
^C
cs315@ubuntu:~/Desktop$ git clone https://github.com/raspberrypi/tools.git
Cloning into 'tools'...
remote: Enumerating objects: 25415, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 25415 (delta 23), reused 22 (delta 14), pack-reused 25374
Receiving objects: 100% (25415/25415), 610.89 MiB | 6.36 MiB/s, done.
Resolving deltas: 100% (14904/14904), done.
Updating files: 100% (19060/19060), done.
cs315@ubuntu:~/Desktop$
```

2.1.4 Cross-compile Tools

已clone至ubuntu虚拟机中:

```
cs315@ubuntu: ~/Desktop
remote: Enumerating objects: 10286559, done.
remote: Total 10286559 (delta 0), reused 0 (delta 0), pack-reused 10286559
Receiving objects: 100% (10286559/10286559), 3.13 GiB | 4.83 MiB/s, done.
Resolving deltas: 100% (8613860/8613860), done.
Checking objects: 100% (33554432/33554432), done.
Updating files: 100% (61894/61894), done.
cs315@ubuntu:~/Desktop$ git clone git://github.com/raspberrypi/tools.git
Cloning into 'tools'...
fatal: unable to connect to github.com:
github.com[0: 20.205.243.166]: errno=Connection refused

cs315@ubuntu:~/Desktop$ git clone git://github.com/raspberrypi/tools.git
Cloning into 'tools'...
^C
cs315@ubuntu:~/Desktop$ git clone https://github.com/raspberrypi/tools.git
Cloning into 'tools'...
remote: Enumerating objects: 25415, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 25415 (delta 23), reused 22 (delta 14), pack-reused 25374
Receiving objects: 100% (25415/25415), 610.89 MiB | 6.36 MiB/s, done.
Resolving deltas: 100% (14904/14904), done.
Updating files: 100% (19060/19060), done.
cs315@ubuntu:~/Desktop$
```

2.2 Armv8-A Exception Levels

2.3 Armv8-A Address Translation

3 Implementation

3.1 Compile the Kernel

3.1.1 Warn

张睿豪同学已经配置树莓派为命令行模式。

3.1.2 Compile

执行课件上的命令：

```
make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabi-
make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabi-
```

```
cs315@ubuntu: ~/Desktop/linux
make: *** [Makefile:520: menuconfig] Error 2
cs315@ubuntu:~/Desktop/linux$ make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/
gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf- menuconfig
scripts/kconfig/mconf Kconfig

*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.

cs315@ubuntu:~/Desktop/linux$ make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/
gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf- bcm2709_def
config
#
# configuration written to .config
#
cs315@ubuntu:~/Desktop/linux$ make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/
gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf- menuconfig
scripts/kconfig/mconf Kconfig

*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.

cs315@ubuntu:~/Desktop/linux$
```

```
mkdir ../modulespath
```

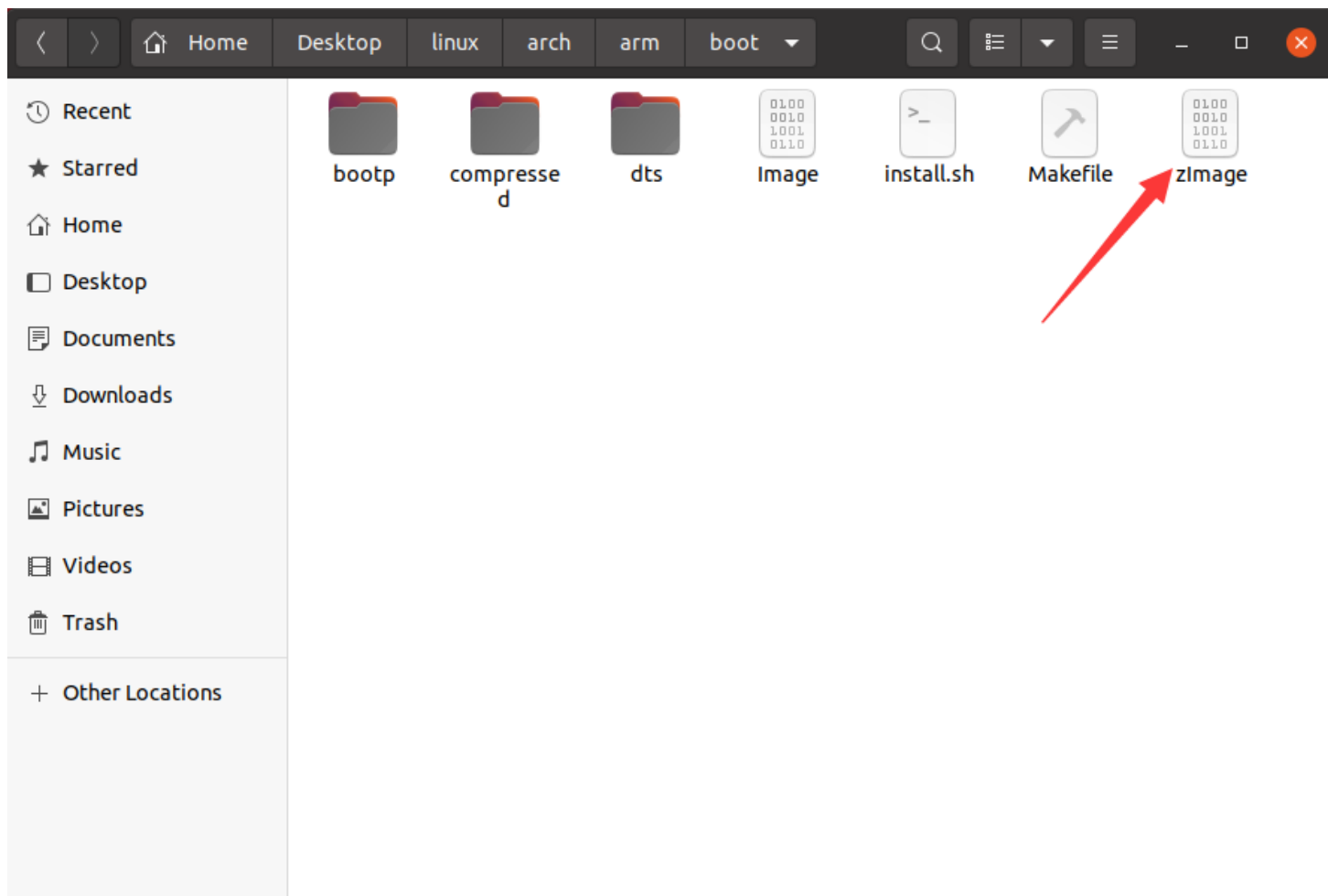
```
make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf-
```

```
make -j8 ARCH=arm CROSS_COMPILE=tools/arm-bcm2708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf-
```

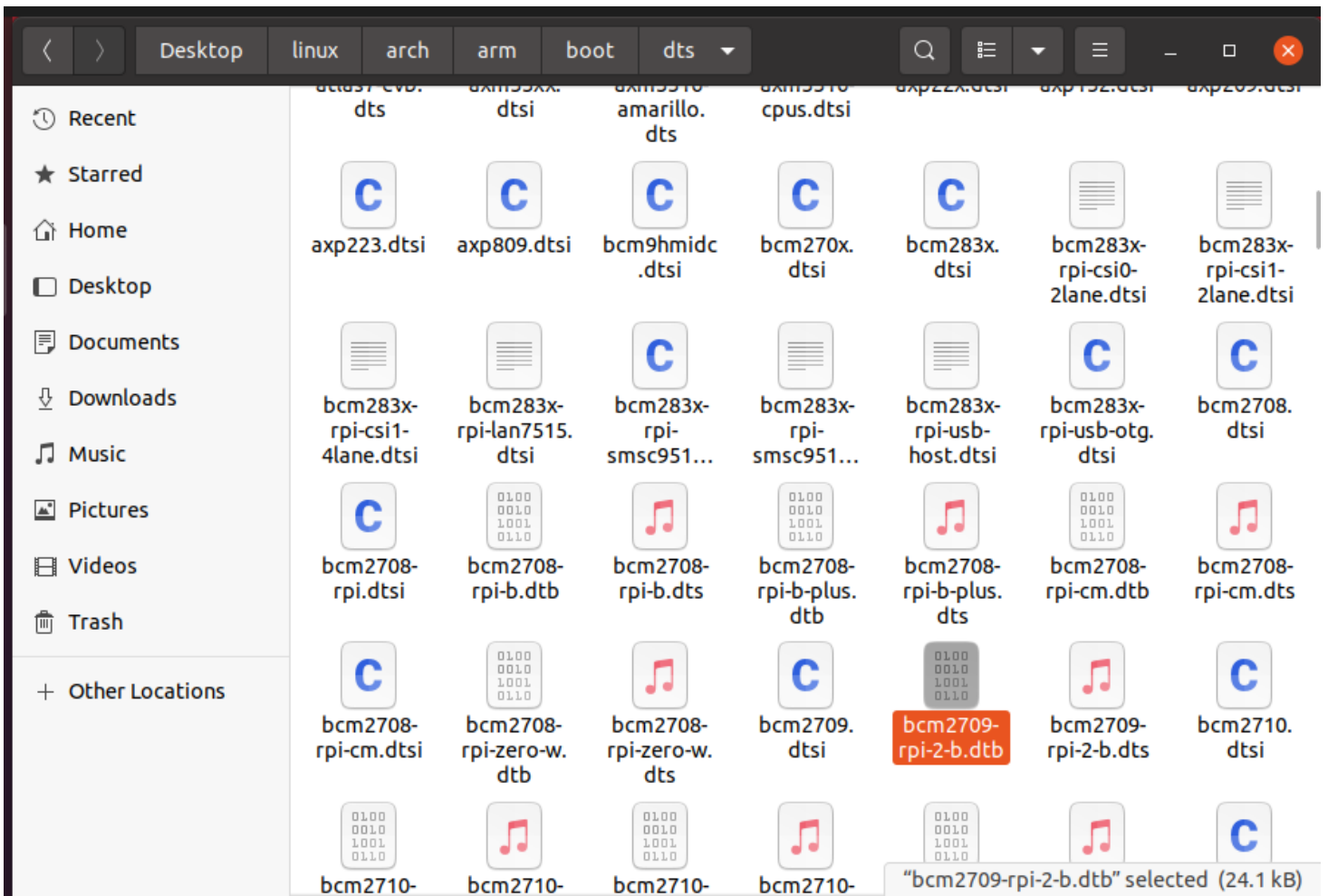
```
cs315@ubuntu: ~/Desktop/linux
INSTALL sound/soc/codecs/snd-soc-sigmadsp.ko
INSTALL sound/soc/codecs/snd-soc-spdif-rx.ko
INSTALL sound/soc/codecs/snd-soc-spdif-tx.ko
INSTALL sound/soc/codecs/snd-soc-tas5713.ko
INSTALL sound/soc/codecs/snd-soc-tlv320aic32x4-i2c.ko
INSTALL sound/soc/codecs/snd-soc-tlv320aic32x4.ko
INSTALL sound/soc/codecs/snd-soc-wm-adsp.ko
INSTALL sound/soc/codecs/snd-soc-wm5102.ko
INSTALL sound/soc/codecs/snd-soc-wm8731.ko
INSTALL sound/soc/codecs/snd-soc-wm8741.ko
INSTALL sound/soc/codecs/snd-soc-wm8804-i2c.ko
INSTALL sound/soc/codecs/snd-soc-wm8804.ko
INSTALL sound/soc/generic/snd-soc-audio-graph-card.ko
INSTALL sound/soc/generic/snd-soc-simple-card-utils.ko
INSTALL sound/soc/generic/snd-soc-simple-card.ko
INSTALL sound/soc/snd-soc-core.ko
INSTALL sound/usb/6fire/snd-usb-6fire.ko
INSTALL sound/usb/caiaq/snd-usb-caiaq.ko
INSTALL sound/usb/hiface/snd-usb-hiface.ko
INSTALL sound/usb/misc/snd-ua101.ko
INSTALL sound/usb/snd-usb-audio.ko
INSTALL sound/usb/snd-usbmidi-lib.ko
DEPMOD 4.14.114-v7+
cs315@ubuntu:~/Desktop/linux$
```

3.1.3 Replace

zImage文件:



dtb文件:



以下命令的执行必须先创建 BOOTDIR 目录：

```
./scripts/mkknlimg ./arch/arm/boot/zImage BOOTDIR/kernel7.img
cp BOOTDIR/kernel7.img BOOTDIR/kernel.img
cp ./arch/arm/boot/dts/bcm2710-rpi-3-b-plus.dtb BOOTDIR/
cp ./arch/arm/boot/dts/overlays/*.dtb* BOOTDIR/overlays/
```



```
cs315@ubuntu: ~/Desktop/linux
283x: y
* Failed to create 'BOOTDIR/kernel7.img'
cs315@ubuntu:~/Desktop/linux$ ./scripts/mkknlimg ./arch/arm/boot/zImage BOOTDIR/
kernel7.img
Version: Linux version 4.14.114-v7+ (cs315@ubuntu) (gcc version 4.8.3 20140303 (
prerelease) (crosstool-NG linaro-1.13.1+bzr2650 - Linaro GCC 2014.03)) #1 SMP We
d Nov 23 05:12:24 PST 2022
DT: y
DDT: y
270x: y
283x: y
cs315@ubuntu:~/Desktop/linux$ cp BOOTDIR/kernel7.img BOOTDIR/kernel.imgcp BOOTDI
R/kernel7.img BOOTDIR/kernel.img^C
cs315@ubuntu:~/Desktop/linux$ ^C
cs315@ubuntu:~/Desktop/linux$ ^C
cs315@ubuntu:~/Desktop/linux$ cp BOOTDIR/kernel7.img BOOTDIR/kernel.img
cs315@ubuntu:~/Desktop/linux$ cp ./arch/arm/boot/dts/bcm2710-rpi-3-b-plus.dtb BO
OTDIR/
cs315@ubuntu:~/Desktop/linux$ cp ./arch/arm/boot/dts/overlays/*.dtb* BOOTDIR/ove
rlays/
cp: target 'BOOTDIR/overlays/' is not a directory
cs315@ubuntu:~/Desktop/linux$ cp ./arch/arm/boot/dts/overlays/*.dtb* BOOTDIR/ove
rlays/
cs315@ubuntu:~/Desktop/linux$
```

在开发板上 `uname -r` 查看kernel版本


```

pi@raspberrypi:~ $ uname -r
4.14.114-v7+
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ks
-bash: ks: command not found
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ ls
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
pi@raspberrypi:~ $ uname -r
4.14.114-v7+
pi@raspberrypi:~ $

```

3.1.4 About the Nailgun module

```
cs315@ubuntu: ~/Desktop/nailgundefense/Read_SCR
make[1]: *** /home/cs315/CS315-NailgunDefense/CS315-NailgunDefense/codes/modules
path/lib/modules/4.14.114-v7+/build: No such file or directory. Stop.
make: *** [Makefile:10: all] Error 2
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$ make
make ARCH=arm -C ~/Desktop/linux/modulespath/lib/modules/4.14.114-v7+/build M=/h
ome/cs315/Desktop/nailgundefense/Read_SCR CROSS_COMPILE=~/.tools/arm-bcm2
708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf- modules
make[1]: Entering directory '/home/cs315/Desktop/linux'
  CC [M]  /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.o
/home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.c: In function 'nailgun_init
':
/home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.c:222:5: warning: ISO C90 fo
rbids mixed declarations and code [-Wdeclaration-after-statement]
    struct nailgun_param *param = kmalloc(sizeof(t_param), GFP_KERNEL);
    ^
Building modules, stage 2.
MODPOST 1 modules
  CC      /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.mod.o
  LD [M]  /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.ko
make[1]: Leaving directory '/home/cs315/Desktop/linux'
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$ ls
Makefile      Module.symvers  nailgun.ko      nailgun.mod.o
modules.order  nailgun.c       nailgun.mod.c   nailgun.o
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$
```

Question 1(20%) Can you prove that (1) you have replaced the kernel (with "uname -r" or other approaches), and (2) you have built the nailgun module with new headers? Please provide a figure.

前面的截图已经能够回答该问题。在此重复一次截图：

(1)在开发板上 `uname -r` 查看kernel版本

```
Raspbian GNU/Linux 10 raspberrypi tty2
```

```
raspberrypi login: pi
```

```
Password:
```

```
Last login: Thu Sep 2 15:59:40 CST 2021 on tty1
```

```
Linux raspberrypi 5.4.51-v7+ #1333 SMP Mon Aug 10 16:45:19 BST 2020 armv7l
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

```
pi@raspberrypi:~$ uname -r
```

```
5.4.51-v7+
```

```
pi@raspberrypi:~$
```

```
pi@raspberrypi:~$ uname -r
```

```
4.14.114-v7+
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ks
```

```
-bash: ks: command not found
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ ls
```

```
Bookshelf Desktop Documents Downloads Music Pictures Public Templates Videos teanview
```

```
pi@raspberrypi:~$ uname -r
```

```
4.14.114-v7+
```

```
pi@raspberrypi:~$
```

(2)创建nailgun的module。


```
cs315@ubuntu: ~/Desktop/nailgundefense/Read_SCR
make[1]: *** /home/cs315/CS315-NailgunDefense/CS315-NailgunDefense/codes/modules
path/lib/modules/4.14.114-v7+/build: No such file or directory. Stop.
make: *** [Makefile:10: all] Error 2
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$ make
make ARCH=arm -C ~/Desktop/linux/modulespath/lib/modules/4.14.114-v7+/build M=/h
ome/cs315/Desktop/nailgundefense/Read_SCR CROSS_COMPILE=~/.tools/arm-bcm2
708/gcc-linaro-arm-linux-gnueabihf-raspbian-x64/bin/arm-linux-gnueabihf- modules
make[1]: Entering directory '/home/cs315/Desktop/linux'
  CC [M] /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.o
/home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.c: In function 'nailgun_init
':
/home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.c:222:5: warning: ISO C90 fo
rbids mixed declarations and code [-Wdeclaration-after-statement]
    struct nailgun_param *param = kmalloc(sizeof(t_param), GFP_KERNEL);
    ^
Building modules, stage 2.
MODPOST 1 modules
  CC /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.mod.o
  LD [M] /home/cs315/Desktop/nailgundefense/Read_SCR/nailgun.ko
make[1]: Leaving directory '/home/cs315/Desktop/linux'
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$ ls
Makefile      Module.symvers  nailgun.ko      nailgun.mod.o
modules.order  nailgun.c       nailgun.mod.c   nailgun.o
cs315@ubuntu:~/Desktop/nailgundefense/Read_SCR$
```

Question 2(20%) Can you run the Nailgun Attack on your new kernel? Please provide a figure.
You can use "dmesg" to show the execution result of Nailgun Attack.

使用如下命令进行执行：

```
sudo insmod nailgun.ko
dmesg
uname -r
```

其中如果需要再次执行，需要卸载之前的安装：

```
sudo rmmod nailgun
```

```
[ 3041.567031] Step 6: Switch to EL3
[ 3041.567037] Step 7: Read SCR
[ 3041.567042] Step 8: Restore context
[ 3041.567047] Step 9: Send restart request to the target processor
[ 3041.567053] Step 10: Wait the target processor to restart
[ 3041.567061] All done! The value of SCR is 0x00000131
[ 3045.111460] Under-voltage detected! (0x00050005)
[ 3055.511415] Voltage normalised (0x00000000)
[ 3089.311889] Goodbye!
[ 3134.551430] rpi_firmware_get_throttled: 1 callbacks suppressed
[ 3134.551437] Under-voltage detected! (0x00050005)
[ 3138.711426] rpi_firmware_get_throttled: 1 callbacks suppressed
[ 3138.711431] Voltage normalised (0x00000000)
[ 3176.120313] Nailgun Attack Start
[ 3176.120380] Using smp_call_function
[ 3176.120396] Step 1: Unlock debug and cross trigger registers
[ 3176.120402] Step 2: Enable halting debug
[ 3176.120407] Step 3: Halt the target processor
[ 3176.120412] Step 4: Wait the target processor to halt
[ 3176.120417] Step 5: Save context
[ 3176.120423] Step 6: Switch to EL3
[ 3176.120427] Step 7: Read SCR
[ 3176.120432] Step 8: Restore context
[ 3176.120438] Step 9: Send restart request to the target processor
[ 3176.120443] Step 10: Wait the target processor to restart
[ 3176.120450] All done! The value of SCR is 0x00000131
[ 3188.631444] Under-voltage detected! (0x00050005)
[ 3194.871424] Voltage normalised (0x00000000)
[ 3195.590581] Goodbye!
[ 3209.939037] Nailgun Attack Start
[ 3209.939097] Using smp_call_function
[ 3209.939112] Step 1: Unlock debug and cross trigger registers
[ 3209.939118] Step 2: Enable halting debug
[ 3209.939122] Step 3: Halt the target processor
[ 3209.939127] Step 4: Wait the target processor to halt
[ 3209.939132] Step 5: Save context
[ 3209.939138] Step 6: Switch to EL3
[ 3209.939142] Step 7: Read SCR
[ 3209.939147] Step 8: Restore context
[ 3209.939152] Step 9: Send restart request to the target processor
[ 3209.939158] Step 10: Wait the target processor to restart
[ 3209.939166] All done! The value of SCR is 0x00000131
[ 3213.591460] Under-voltage detected! (0x00050005)
pi@raspberrypi:~/Desktop/lab8 $ uname -r
4.14.114-v7+
pi@raspberrypi:~/Desktop/lab8 $ _
```


3.2 Implementation of the Defense

3.3 Codes of Defense

Question 3(30%) With the provided source codes, can you explain the process of translating an IPA, $0x40030000 + \text{"last 3 numbers of your student ID"}$, to the same value of PA? (e.g., if your ID is 12150073, then you should translate $0x40030073$). In this question, you should mention the (1) address of each descriptor, and (2) value of each descriptor.

我的SID是11910104, (我假定都是104是16进制数) 因此要翻译的IPA是:

$0x40030000 + 0x104 = 0x40030104$

翻译为二进制为:

0b 0100_0000_0000_0011_0000_0001_0000_0100

我的设计直接参考了大课课件上的内容, 分为三个部分:

Design: Example



Here is one example of the table layout in $0x0 \sim 0xFFFF_FFFF$ (only invalid dbg)

VTTBR: point to area0

area0:

$0x0000_0000 \sim 0x3FFF_FFFF$: 1GB block
 $0x4000_0000 \sim 0x7FFF_FFFF$: table, point to area1
 $0x8000_0000 \sim 0xBFFF_FFFF$: 1GB block
 $0xC000_0000 \sim 0xFFFF_FFFF$: 1GB block

area1:

$0x4000_0000 \sim 0x401F_FFFF$: table, point to area2
 $0x4020_0000 \sim 0x403F_FFFF$: 2MB block
 $0x4040_0000 \sim 0x405F_FFFF$: 2MB block
...
 $0x7E00_0000 \sim 0x7FFF_FFFF$: 2MB block

area2:

$0x4000_0000 \sim 0x4000_0FFF$: 4KB Page
...
 $0x4002_F000 \sim 0x4002_FFFF$: 4KB Page
 $0x4003_0000 \sim 0x4003_0FFF$: Invalid (0x0)
 $0x4003_1000 \sim 0x4003_1FFF$: 4KB Page
 $0x4003_2000 \sim 0x4003_2FFF$: 4KB Page
...
 $0x401F_0000 \sim 0x401F_FFFF$: 4KB Page

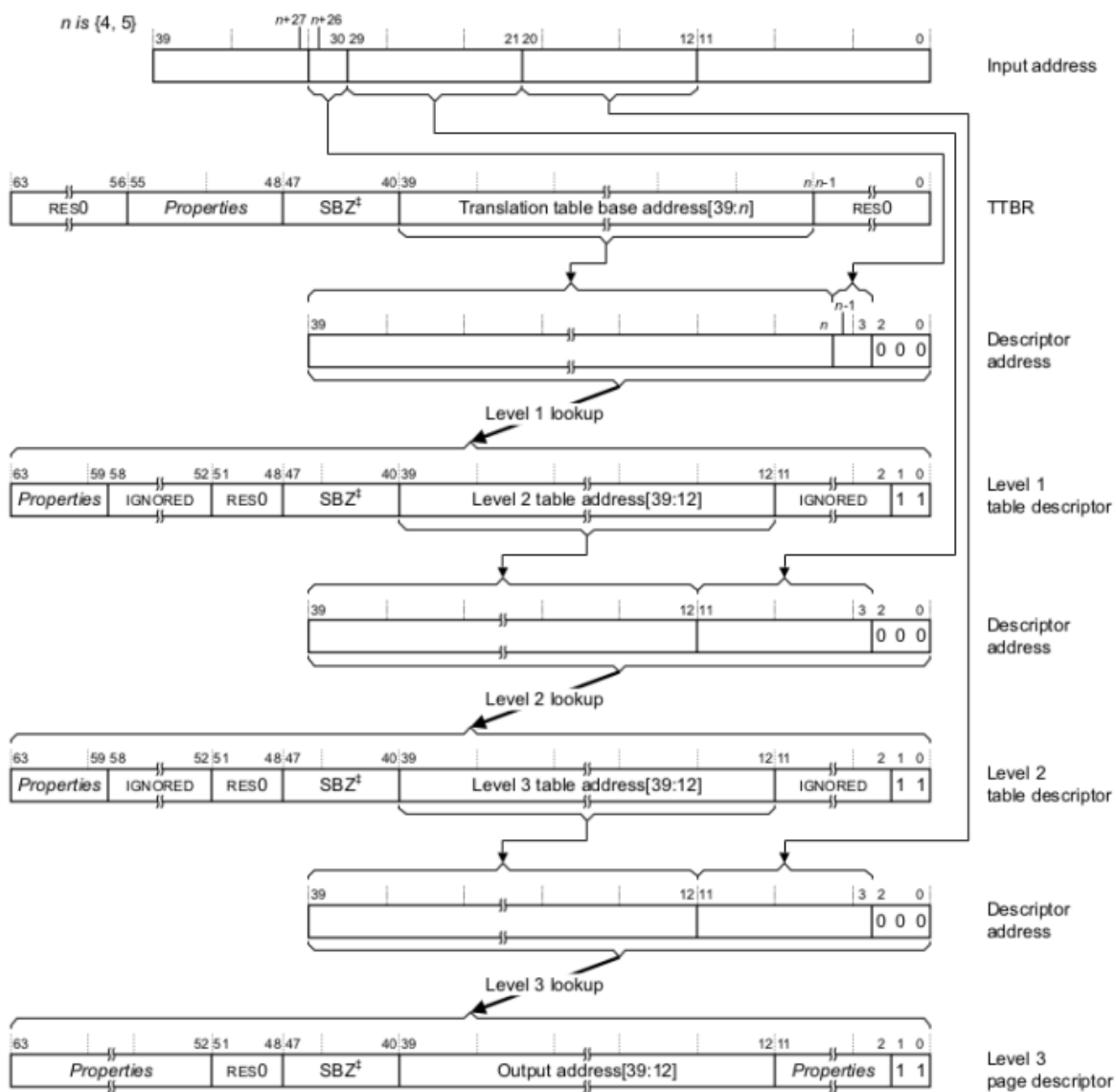


Figure 13: A translation example

VTTBR的数值是 0x32000000

First, we fill the VTTBR register, we directly put the start address (0x32000000) into the BADDR bits:

```
ldr r0,=0x32000000
ldr r1,=0x0
mcr p15, 6, r0, r1, c2
```

这个二进制需要分为好几个部分：

- 一级页表项，31-30位：01
- 二级页表项，29-21位：00_0000_000
- 三级页表项，20-12位：0_0011_0000

- offset项, 11-0位: 0001_0000_0100

在翻译之前, 还要算一下各个页表的首地址, 计算结果如下:

- 一级页表: area0, 首地址是0x32000000
- 二级页表: area1, 首地址是0x32001000
- 三级页表: area2, 首地址是0x32005000

页表翻译流程: (翻译过程中有加0b11的操作, 这个是手册上规定的数值)

- Step 1: 一级页表项为01

跳转至area1, 地址区域范围是0x4000_0000至0x7FFF_FFFF

(1)address: (VTTBR[39:5], IPA[31:30], 0b000) = (0x32000000, 0b01, 0b000)
= 0x32000008

(2)value: 它指向area2区域, 地址是:

$A2 = \text{area1} + \text{offset} * \text{block_size} + 0b11 = 0x32001000 + 1 * 2^{12} + 0x3 = 0x32002003$

最末两位是11

- Step 2: 二级页表项为全0

跳转至area2, 地址区域范围是0x4000_0000至0x401F_FFFF

(1) address: 考虑其为二级页表项的首项, 因此即为Step 1中的value, 为0x32002000

(2) value: 它指向area3区域, 地址是:

$A3 = \text{area2} + \text{offset} * \text{block_size} + 0b11 = 0x32005000 + 0 * 2^{12} + 0x3 = 0x32005003$

最末两位是11

- Step 3: 三级页表项为0_0011_0000

跳转至area3, 地址区域范围是0x4003_0000至0x4003_0FFF

(1) address: (A3[39:12], IPA[20:12], 0b000) = 0x32005180

(2) value: 它指向的地址是:

$0x40030 \ll 12 + 0b11 = 0x40030003$, 最末两位是11

- Step 4: offset项是0001_0000_0100

翻译结果就是 $0x40030 \ll 12 + 0001_0000_0100 = 0x40030104$ ，和原来的IPA地址相同。

Question 4(30%) With the provided source codes, can you explain the process of traslating an IPA, $0x40000000 + \text{"last 7 numbers of your student ID"}$, to the same value of PA? (e.g., if your ID is 12150073, then you should translate $0x42150073$). In this question, you should mention the (1) address of each descriptor, and (2) value of each descriptor.

该题流程和Question 3类似，设计保留Question 3的想法。

我的SID是11910104，（我假定都是1910104是16进制数）因此要翻译的IPA是：

$$0x40030000 + 0x1910104 = 0x41940104$$

翻译为二进制为：

$$0b\ 0100_0001_1001_1000_0000_0001_0000_0100$$

这个二进制需要分为好几个部分：

- 一级页表项，31-30位：01
- 二级页表项，29-21位：00_0001_100
- 三级页表项，20-12位：1_1000_0000
- offset项，11-0位：0001_0000_0100

页表翻译流程：

- Step 1: 一级页表项为01

跳转至area1，地址区域范围是 $0x4000_0000$ 至 $0x7FFF_FFFF$

$$(1) \text{ address: } (VTTBR[39:5], IPA[31:30], 0b000) = (0x3200000, 0b01, 0b000) \\ = 0x32000008$$

(2) value: 它指向area2区域，地址是：

$$A2 = \text{area1} + \text{offset} * \text{block_size} + 0b11 = 0x32001000 + 1 * 2^{12} + 0x3 = 0x32002003$$

最末两位是11

- Step 2: 二级页表项为1100

跳转至第12个2 MB block，地址区域范围是 $0x4180_0000$ 至 $0x419F_FFFF$

(1) address: (A2[39:12], IPA[29:21], 0b000) = 0x32005C00

(2) value:

$A3 = \text{area2} + \text{offset} * \text{block_size} + 0b11 = 0x32005000 + 12 * 2^{12} + 0x3 = 0x32011003$

最末两位是11

- Step 3: 三级页表项为0_0011_0000 1_1000_0000

跳转至area3，地址区域范围是0x4194_0000至0x4194_0FFF

(1) address: (A3[39:12], IPA[20:12], 0b000) = 0x32011C00

(2) value: 它指向的地址是：

$0x41940 \ll 12 + 0b11 = 0x41940003$ ，最末两位是11

- Step 4: offset项是0001_0000_0100

翻译结果就是 $0x41940 \ll 12 + 0001_0000_0100 = 0x41940104$ ，和原来的IPA地址相同。

Acknowledgement

本次实验感谢张睿豪同学提供开发板环境配置，谢岳臻同学提供Q3和Q4的设计与算法讲解。

我这次是和刘晟淇同学一起完成了本次实验。