Lab8

ID: 11912614

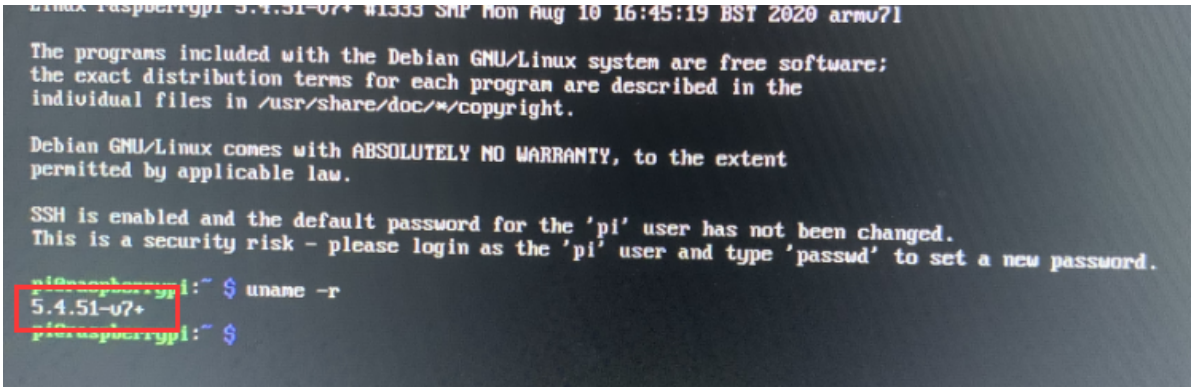
Name: 张睿豪

Q1 & Q2 are finished with my project members: 谢岳臻，李家奥，刘晟淇，王奕童

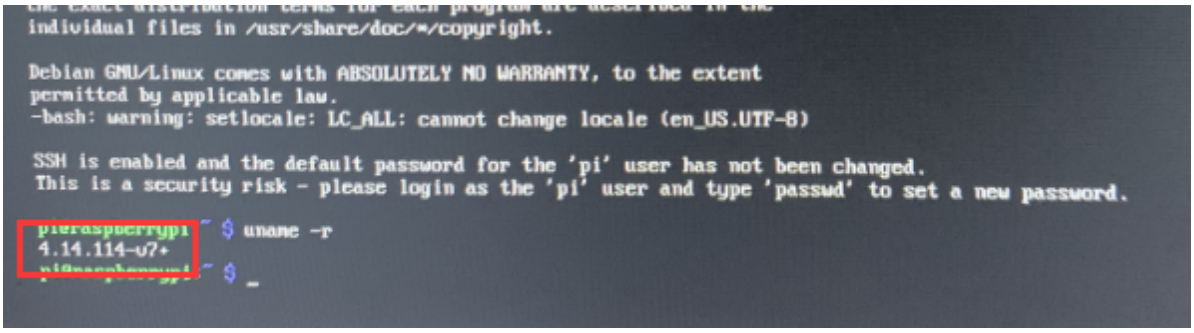
Q1

> Prove that you have replaced the kernel

Before replacement



After replacement

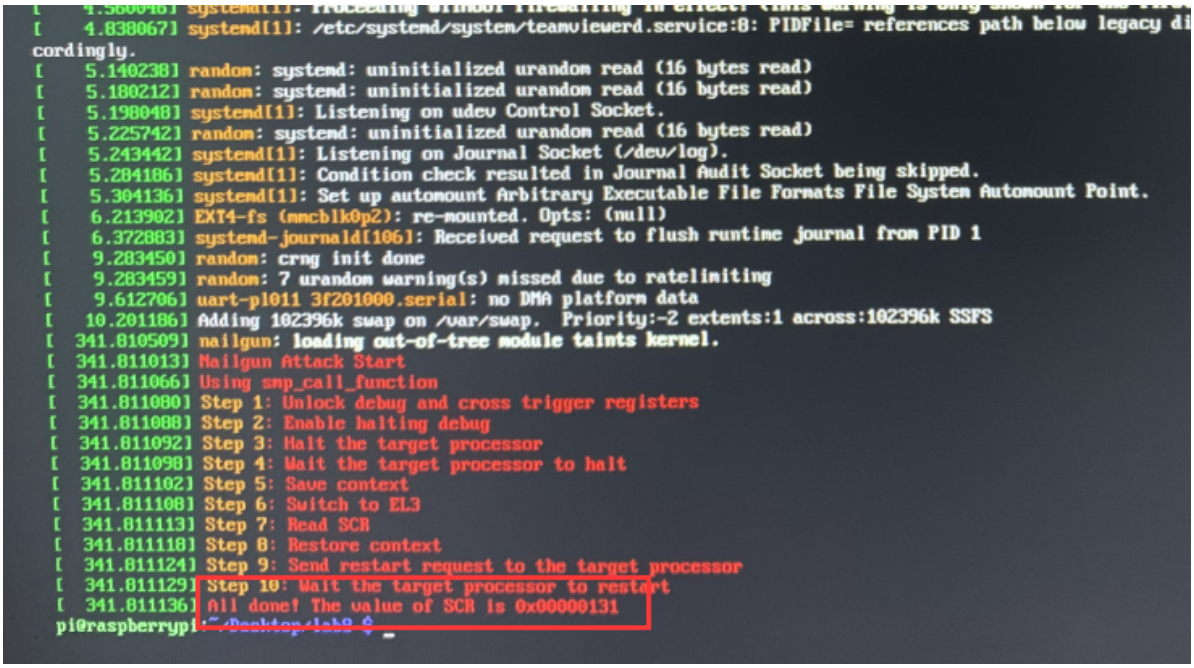


> Prove that you have built the nailgun module with new headers

We complie the nailgun module successfully

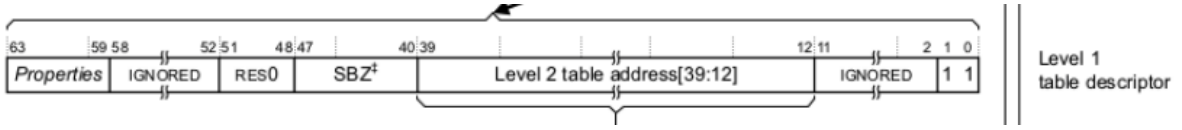
Q2

The Nailgun Attack works.



Q3 & Q4

The translation table base address is VTTBR: `0x32000000`



As the picture above shows, size of a descriptor is 2^3 B.

According to structure of IPA, I know followings:

1. The number of entries for each page table:
   - level-1 page table: $2^{31-30+1} = 2^2$
   - level-2 page table: $2^{29-21+1} = 2^9$
   - level-3 page table: $2^{20-12+1} = 2^9$
2. Space (B) needed to store each level page table:
   - level-1 page table

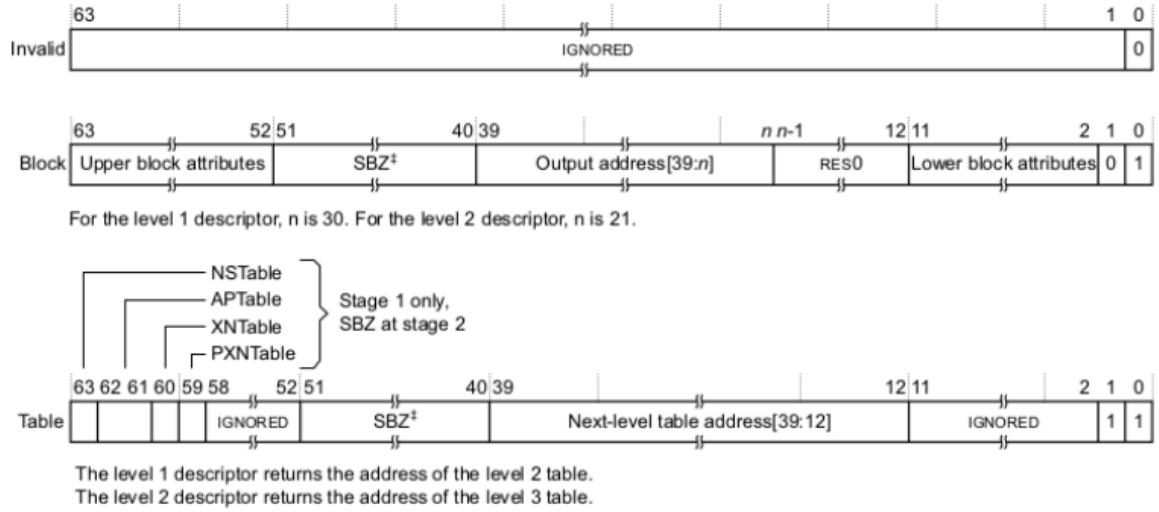
     Since $2^3 \times 2^2 = 2^5 < 4KB$, it needs $4KB = 2^{12}B$
   - level-2 and level-3 page table

     $2^3 \times 2^9 = 2^{12}B$

Design

Descriptor's value

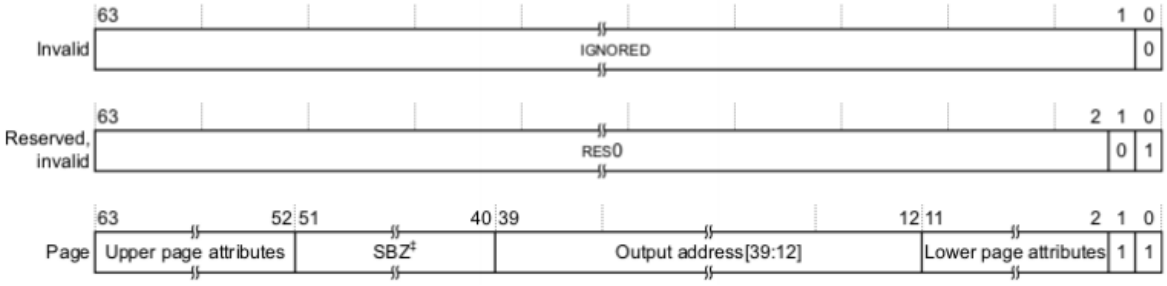
1. For level-1 & level-2 descriptor:



For simplicity, if it is

- invalid: value is 0
- block: only care about output address , value is $\text{output address} << 30 + 1$ for level 1 and $\text{output address} << 21 + 1$ for level 2
- table: only care about next-level table address, value is $\text{next-level table base address} << 12 + 3$

2. For level-3 descriptor:



For simplicity, if it is

- invalid: value is 0
- page: only care about output address , value is $\text{output address} << 12 + 3$

Address range of each page table

1. Level-1 Page Table: [`0x3200 0000`, `0x3200 0000` + 2^{12}) =

$$[0x32000000, 0x32001000)$$

   Base of level-1 page is VTTBR.

2. Level-2 Page Table: [`0x3200 1000`, `0x3200 1000` + $2^2 \times 2^{12}$) =

$$[0x32001000, 0x32005000)$$

   Base of level-2 page is `0x3200 1000`, called BA2.

3. Level-3 Page Table:

Theoretically, the range should be [`0x3200 5000`, `0x3200 5000` + $2^2 \times 2^9 \times 2^{12}$) = [`0x3200 1000`, `0x3280 5000`) but `0x3280 5000` > `0x321f ffff` (upper bound of the reserved space). Therefore, actual range is

$$[0x32005000, 0x321fffff)$$

Base of level-3 page is `0x0x3200 5000`, called BA3.

Q3

What I know:

- VTTBR: `0x3200 0000`
- input IPA: `0x40030614` = `0b0100 0000 0000 0011 0000 0110 0001 0100`
  - Level-1 Page Table Number: IPA[31:30] = `0b01`
  - Level-2 Page Table Number: IPA[29:21] = `0b0`
  - Level-3 Page Table Number: IPA[20:12] = `0b0011 0000`
  - offset (4kb): IPA[11:0] = `0b0110 0001 0100`
- output PA (PA== IPA): `0x40030614` = `0x40030` << 12 + `0x614`

According to my design,

1. level 1:
   - address of descriptor:

     concat(VTTBR[39:5], IPA[31:30], 0b000) = `0x3200 0008`
   - value of descriptor:

     it points to the second (index is IPA[31:30]==1) level-2 table, so address of the table is $A2 = (\mathrm{BA2} + 1 \times 2^{12}) = 0\mathrm{x}3200\ 2000$

     $$\mathrm{A2}[39{:}12] << 12 + 3 = 0\mathrm{x}3200\ 2003$$
2.
2. level 2 (base `0x3200 1000`):
   - address of descriptor:

     concat(A2[39:12], IPA[29:21], 0b000) = `0x3200 2000`
   - value of descriptor:

     it points to the first (index is IPA[29:21]==0) level-3 table, so address of the table is $A3 = (\mathrm{BA3} + 0 \times 2^{12}) = 0\mathrm{x}3200\ 5000$

     $$\mathrm{A3}[39{:}12] << 12 + 3 = 0\mathrm{x}3200\ 5003$$
3. level 3 (base `0x3200 5000`):
   - address of descriptor:

     concat(A3[39:12], IPA[20:12], 0b000) = `0x3200 5180`
   - value of descriptor:

     it points to output address PA, so the value is

$$\mathrm{PA}[39{:}12] << 12 + 3 = \mathrm{0x4003\ 0003}$$

Q4

What I know:

- VTTBR: `0x3200 0000`
- input IPA: `0x41912614` = `0b0100 0001 1001 0001 0010 0110 0001 0100`
  - Level-1 Page Table Number: IPA[31:30] = `0b01`
  - Level-2 Page Table Number: IPA[29:21] = `0b1100`
  - Level-3 Page Table Number: IPA[20:12] = `0b1 0001 0010`
  - offset (4kb): IPA[11:0] = `0b0110 0001 0100`
- output PA (PA== IPA): `0x41912614` = `0x41912` << 12 + `0x614`

According to my design,

1. level 1:
   - address of descriptor:

     concat(VTTBR[39:5], IPA[31:30], 0b000) = `0x3200 0008`
   - value of descriptor:

     it points to the second (index is IPA[31:30]==1) level-2 table, so address of the table is $A2 = (\mathrm{BA2} + 1 \times 2^{12}) = \mathrm{0x3200\ 2000}$

     $$\mathrm{A2}[39{:}12] << 12 + 3 = \mathrm{0x3200\ 2003}$$
2. level 2 (base `0x3200 1000`):
   - address of descriptor:

     concat(A2[39:12], IPA[29:21], 0b000) = `0x3200 2060`
   - value of descriptor:

     it points to the 12th (index is IPA[29:21]==12) level-3 table, so address of the table is $A3 = (\mathrm{BA3} + 12 \times 2^{12}) = \mathrm{0x3201\ 1000}$

     $$\mathrm{A3}[39{:}12] << 12 + 3 = \mathrm{0x3201\ 1003}$$
3. level 3 (base `0x3200 5000`):
   - address of descriptor:

     concat(A3[39:12], IPA[20:12], 0b000) = `0x3201 1890`
   - value of descriptor:

     it points to output address PA, so the value is

     $$\mathrm{PA}[39{:}12] << 12 + 3 = \mathrm{0x4191\ 2003}$$