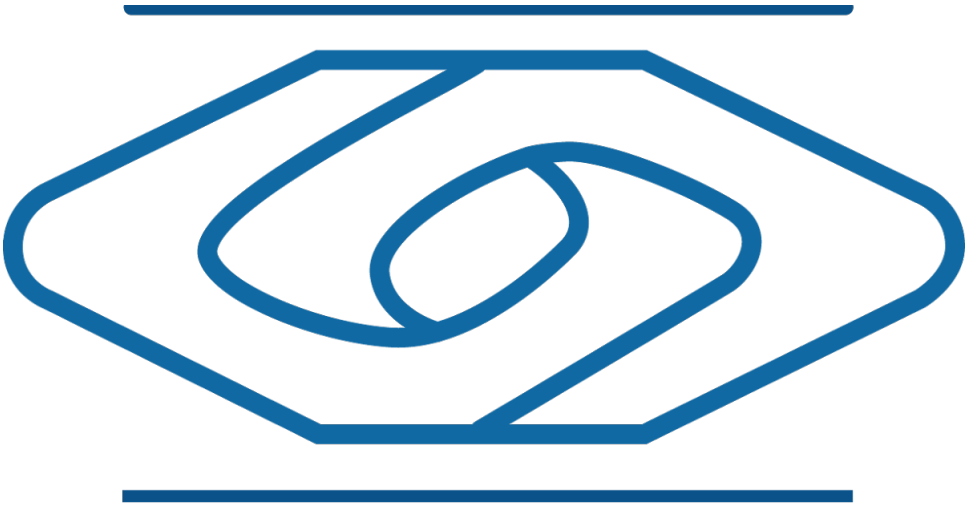


Instituto Politécnico Nacional
Escuela Superior de Computo

Práctica 1: Mi primer bootloader

Reporte
Profesor: Ulises Velez Saldaña
Alumno: Meza Madrid Raúl Damián
Clase: Sistemas operativos
Grupo: 2CM7

Introducción

A la hora de encender una computadora se ejecuta una secuencia de procesos y eventos, uno de ellos es la ejecución del BIOS que se encarga de revisar el funcionamiento del hardware (que usualmente ya ha sido revisado por la motherboard) para posteriormente buscar el cargador de sistema, bootloader. El bootloader es aquel que,después de ser cargado, busca y carga el sistema operativo; en ocasiones re-escribe parte del BIOS. Para que el bootloader funcione, es necesario que este cumpla ciertos de requisitos.

- Debe encontrarse en el primer segmento dentro del disco duro
- Debe cargarse en el primer segmento de la memoria RAM
- Debe dejar libres los primero 512 [1] bytes del mismo segmento.
- Al final del segmento debe escribir el Magic Number[2] para informar al BIOS mostrará un mensaje o leerá el siguiente disco.[2]

1.1 Programas y herramientas utilizados

Esta práctica fue desarrollada en el sistema operativo Ubuntu 18.04.1 LTS. Los programas y herramientas utilizados, junto con el comando de instalación, en caso de que no estuvieran instalados ya.

- NASM : $ apt-get install nasm
- QEMU : $ apt-get install qemu
- dd

Objetivo

Que el alumno aplique la teoría vista en clase, conozca el proceso y las herramientas necesarias para construir el cargados.

[1] El documento p1-minimum-bootloader.pdf especifica un tamaño de 10 bytes mas grandes al especificado por el profesor en clase. Se decidió seguir este ultimo porque tiene mas sentido.

[2] El Magic Number es 0xAA55 en hexadecimal y 0b1010101001010101 en binario

Desarrollo

3.1 Crear el archivo bootloader.asm

El archivo bootloader.asm debe cumplir con las siguientes espeficicaciones

- Un ciclo infinito.
- Compilar en 16 bits.
- Rellenar el segmento con ceros hasta una longitud de 510 bytes.
- Colocar el magic number 0xAA55 en la posición 511 y 512.

El archivo resultante es el siguiente

```
[bits 16]
loop:
  jmp loop
times 510 - ($-$$) db 0
dw 0xAA55
```

3.2 Ensamblar

Ensamblar cargador generando un ejecutable de código máquina plano. Para esto se usara NASM. Los parámetros -f bin especifican el formato de salida como flat binary y se guardan dentro de la carpeta bin con el nombre bootloader. El parámetro resultante es:

```
nasm src/bootloader.asm  -f bin bin/bootloader
```

3.3 Crear el disco

Crear el disco con el cargador en el sector cero. En este caso se usara un floppy disk (extinción flp) lleno con ceros (if=/dev/zeros) con 1440 (count=1440) segmentos de tamaño de un megabyte; 1024 bytes (bs=1024).

```
dd if=/dev/zero of=images/escomos.flp bs=1024 count=1440

 1440+0 records in
 1440+0 records out
 1474560 bytes (1.5 MB, 1.4 MiB) copied,
 0.00708728s, 208 MB/s
```

Despues se agrega la información del bootloader que creamos (if = bin/bootloader)

```
dd if=bin/bootloader of=images/escomos.flp seek=0 count=1 conv=notrunc
```

```
1+0 records in
1+0 records out
512 bytes copied, 0.000413659 s, 1.2 MB/s
```

3.4 Correr el sistema

Correr el sistema operativo en un emulador, en este caso QEMU en un sistema con la arquitectura i386, se especifica el formato -fda como un floppy disk y se carga la imagen creada anteriormente.

```
qemu-system-i386 -fda images/escomos.flp
```

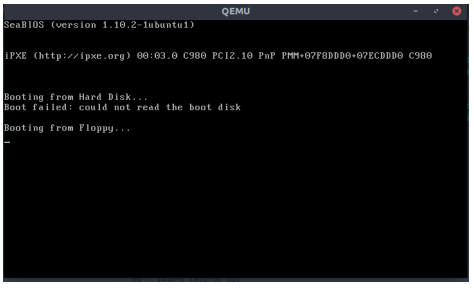
El primer resultado es un mensaje en consola que dice:

```
WARNING: Image format was not specified for
    'images/escomos.flp'and probing guessed raw.
    Automatically detecting the format is dangerous
    for raw images, write operations on block 0
    will be restricted. Specify the 'raw' format
    explicitly to remove the restrictions.
```

y después vemos una pantalla que dice:

SeaBIOS (version 1.10.2-1ubuntu1)

iPXE (...)
Booting from Hard Disk...
Boot failed: could not read the boot disk
booting from Floppy
-



3.5 Errores y problemas

La primera vez que se uso el comando NASM, decía que habia mas de una entrada,

```
nasm src/bootloader.asm -f bin bin/bootloader
```

```
nasm: error: more than one input file specified
type 'nasm –h' for help
```

Lo primero que hice fue quitar los argumentos extras, pero recibí el mismo mensaje. Trate de borrar espacios extras, pero tampoco. Termine haciéndolo directo desde la carpeta para después solo copiar el archivo ha la carpeta correspondiente

```
nasm bootloader.asm -f bin
```

References

[1] Alex Kolesnyk. How to develop your own Boot Loader. https://www.codeproject.com/KB/tips/boot-loader.aspx?fid=1541607&df=90&mpp=25&noise=3&sort=Position&view=Quick&fr=1#_Toc231383187. [Online; consultado en 9-Febrero-2019].

[2] Paul de Weerd, UNIX and network engineer. Re: fdisk / signature: 0xAA55. https://www.mail-archive.com/misc@openbsd.org/msg18029.html. [Online; consultado en 9-Febrero-2019].