Booting with UEFI Option

Contents

Introduction

This document contains notes for attempting to boot using the UEFI option, utilizing the Git repository available at `https://github.com/utshina/uefi-simple.git`.
When you finish the first two steps, you should be able to boot using the rEFInd manager and find the boot option with main.efi. Upon completing the third step, you should be able to boot directly with main.efi, which will display "Hello World!" when you boot your device.

Create EFI Partition

1. Partition the hard drive in GPT format and create a FAT32 formatted EFI System Partition (ESP). Use the gparted tool.

Compile main.c into Executable File

1. Use a toolchain that supports UEFI compilation (such as GCC or Visual Studio) to compile the code into a .efi file. You can use the gnu-efi library to assist with compilation:

   ```
   gcc -o main.efi main.c -I/usr/include/efi -I/usr/
       include/efi/gnu -L/usr/lib -lefi -lgnuefi
   ```

2. Use the following GCC command in the terminal to compile the main.c file:

   ```
   x86_64-w64-mingw32-gcc -shared -nostdlib -mno-red-
       zone -fno-stack-protector -Wall -e EfiMain main.c
        -o main.dll
   ```

3. Use the objcopy command to convert main.dll into main.efi:

   ```
   objcopy --target=efi-app-x86_64 main.dll main.efi
   ```

4. Place main.efi in the myboot directory:

   ```
   sudo mkdir -p /boot/efi/EFI/myboot
   ```

5. Use the cp command to copy the main.efi file to the EFI partition:

   ```
   sudo cp /home/huanhuanjiang/Documents/github/uefi-
       simple/main.efi /boot/efi/EFI/myboot/
   ```

6. Check if the file was successfully copied:

   ```
   ls /boot/efi/EFI/myboot/
   ```

7. Set file permissions to ensure it can be accessed by the UEFI boot loader:

```
sudo chmod 755 /boot/efi/EFI/myboot/main.efi
```

Set BIOS to Boot from the Hard Drive EFI Partition

1. Boot with CSM (Compatibility Support Module) for legacy BIOS.
2. Set NVRAM boot entries:
   (a) Install efibootmgr:

   ```
   sudo apt install efibootmgr
   ```

   (b) Add a new boot entry:

   ```
   sudo efibootmgr -c -d /dev/nvme0n1 -p 1 -L "
       MyBoot" -l "\EFI\myboot\main.efi"
   ```

   (c) Set the boot order:

   ```
   sudo efibootmgr -o Boot0002,0000,0001,0005
   ```

3. Disable secure boot by setting the "OS Type" option under "Secure Boot" to "Other OS".

Other Notes

1. The meaning of the command `sudo chmod 755 filename` is:
   - `sudo`: Execute the command with superuser (root) privileges.
   - `chmod`: Modify the read, write, and execute permissions of files or directories.
   - `755`: This is an octal number representing the file permission settings.
     - The first digit 7 represents the permissions for the file owner (u): 4+2+1=read+write+execute=7
     - The second digit 5 represents the permissions for the group (g): 4+0+1=read+execute=5
     - The third digit 5 represents the permissions for others (o): 4+0+1=read+execute=5
   - Therefore, the 755 permission can be symbolically represented as rwxr-xr-x, meaning:
     - The file owner has read, write, and execute permissions.
     - The group and other users have read and execute permissions, but no write permissions.

2. NVRAM (Non-Volatile Random Access Memory) is a type of non-volatile random-access memory. It has the following characteristics:

    - Definition: NVRAM is a type of random-access memory that retains data even when power is turned off or disconnected, unlike volatile memory such as DRAM and SRAM, which lose data when power is off.
    - Working Principle: NVRAM is typically powered by a battery. When the computer is powered on, NVRAM operates like regular RAM. When the power is turned off, NVRAM draws enough power from an internal battery to retain data.
    - Application Scenarios: NVRAM is commonly found in embedded systems. It is often used to store critical system information, such as BIOS settings, modem IPs, and routing table information. In Hackintosh systems, NVRAM is used to save parameters like Bluetooth, screen brightness, system volume, iMessage, FaceTime, etc., after rebooting. Clover and OpenCore bootloaders also require NVRAM support to set the system boot disk.
    - Advantages: Compared to flash memory, NVRAM offers faster data storage speeds. Compared to DRAM, NVRAM retains data even when power is turned off.