

boot-popcorn

...

By Benjamin Bushnell, Michael Seeley, Zachary Taylor

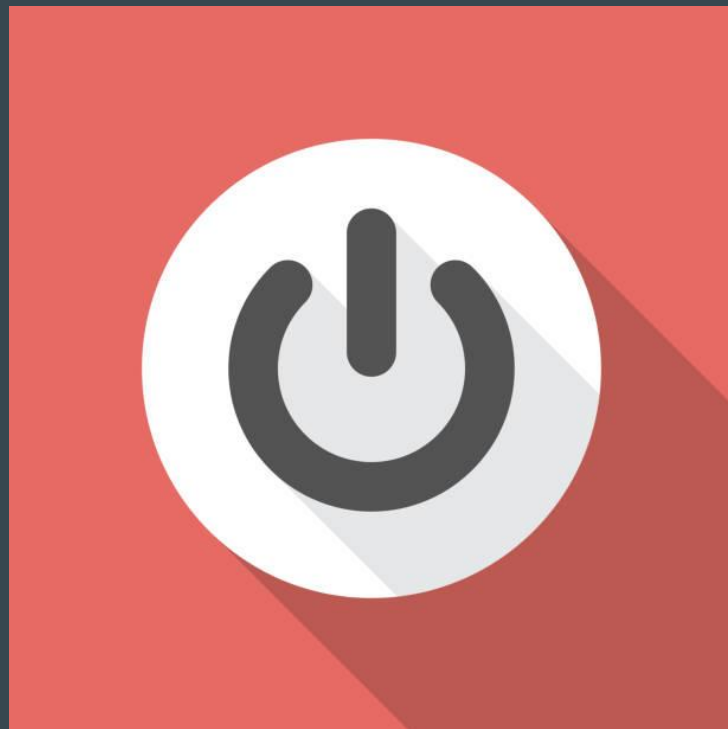
Boot Process

- POST
- Boot sector (first stage bootloader)
- Second stage bootloader
- Kernel



POST

- Power-On Self Test
- Part of BIOS (Basic Input Output System)
- Finds bootable device
- Loads first 512 bytes to 0x000:7C00



Boot Sector

- Also called 1st Stage Bootloader or Master Boot Record (MBR)
- Only 512 bytes!
- Loads either 2nd stage or kernel
- BIOS interrupts
- 16-bit real mode
- Assembly

Boot Sector hex dump:

```
00000000 e9 90 00 00 00 00 00 00 00 00 00 ff ff 00 00 00 |.....|
00000010 9a cf 00 ff ff 00 00 00 92 cf 00 18 00 03 7c 00 |.....|.|
00000020 00 42 6f 6f 74 20 73 65 63 74 6f 72 3a 20 45 78 |.Boot sector: Ex|
00000030 65 63 75 74 69 6e 67 20 53 74 61 67 65 20 31 2e |ecuting Stage 1.|
00000040 2e 2e 0d 0a 00 44 69 73 6b 20 72 65 61 64 20 65 |.....Disk read e|
00000050 72 72 6f 72 00 49 6e 63 6f 72 72 65 63 74 20 6e |rror.Incorrect n|
00000060 75 6d 62 65 72 20 6f 66 20 73 65 63 74 6f 72 73 |umber of sectors|
00000070 20 72 65 61 64 00 00 ac 08 c0 74 06 b4 0e cd 10 | read.....t.....|
00000080 eb f5 c3 be 45 7c e8 ee ff eb fe be 55 7c e8 e6 |....E|.....U|..|
00000090 ff eb fe b8 01 24 cd 15 b8 03 00 cd 10 bd 00 80 |.....$.|.....|
000000a0 89 ec be 21 7c e8 cf ff 88 16 76 7c b4 02 b0 10 |...!|.....v|....|
000000b0 b5 00 b6 00 b1 02 8a 16 76 7c bb 00 7e cd 13 fa |.....v|..~...|
000000c0 0f 01 16 1b 7c 0f 20 c0 66 83 c8 01 0f 22 c0 b8 |....|. .f...."..|
000000d0 10 00 8e d8 8e c0 8e e0 8e e8 8e d0 ea 23 7e 08 |.....#~..|
000000e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
000001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa |.....U.|
```

2nd Stage / Kernel

- Fuzzy distinction
- Much bigger than boot sector
- 32-bit protected mode
- Assembly and C, C++



Demo time...

Impressed?

OS Dev is hard...

- Assembly is hard
- No standard libraries!
- Sparse documentation

What did we learn?

- x86 Architecture history
- What the kernel needs to start
- Executable formats & linking
- Cross-compiling

Could it be better?

- Filesystem
- Multiboot, boot menu
- Standard library
- Interactivity

References

- Writing a Bootloader by Alex Parker - <http://3zanders.co.uk/2017/10/13/writing-a-bootloader/>
- os-tutorial on GitHub by Carlos Fenollosa - <https://github.com/cfenollosa/os-tutorial>
- OS Development Series by Mike from BrokenThorn Entertainment - <http://brokenthorn.com/Resources/OSDevIndex.html>
- OSDev Wiki - https://wiki.osdev.org/Main_Page
- The world of Protected Mode by Gregor Brunmar - <http://www.osdever.net/tutorials/view/the-world-of-protected-mode>

Any questions?