LUG@UCLA TECH TALK

BOOTLOADING - BIOS/UEFI

Presented by Vincent Wong

lain@linux.ucla.edu

CONNECT TO THE LAN

WiFi SSID: *Kanye's iPhone*

These slides can then be accessed: `xxxx:8000`

Follow along in the web tty by: `xxxx:8001`

BOOTING

- You press power button --> kernel loads
- First performs power-on-self-test (**POST**)
  - Initializes hardware components, looks for problems
- Then, firmware (BIOS xor UEFI) does bootloading

BOOTLOADING

- Process of firmware executing **bootloader(s)** that eventually loads the operating system.
- This is where traditional BIOS systems and UEFI systems differ the most

BASIC INPUT/OUTPUT SYSTEM

BIOS

- Handles POST and executing bootloader, and provides BIOS call interface
  - But usually not relevant beyond booting
- Not really a standard, more like a convention in IBM PC compatible computers

BIOS BOOTING OVERVIEW

- Look for disks (CD/DVD, HDD, usb) that contain a bootable **MBR**
  - User can configure which disk to try booting from first
- If found, simply executes the code in the MBR

MASTER BOOT RECORD

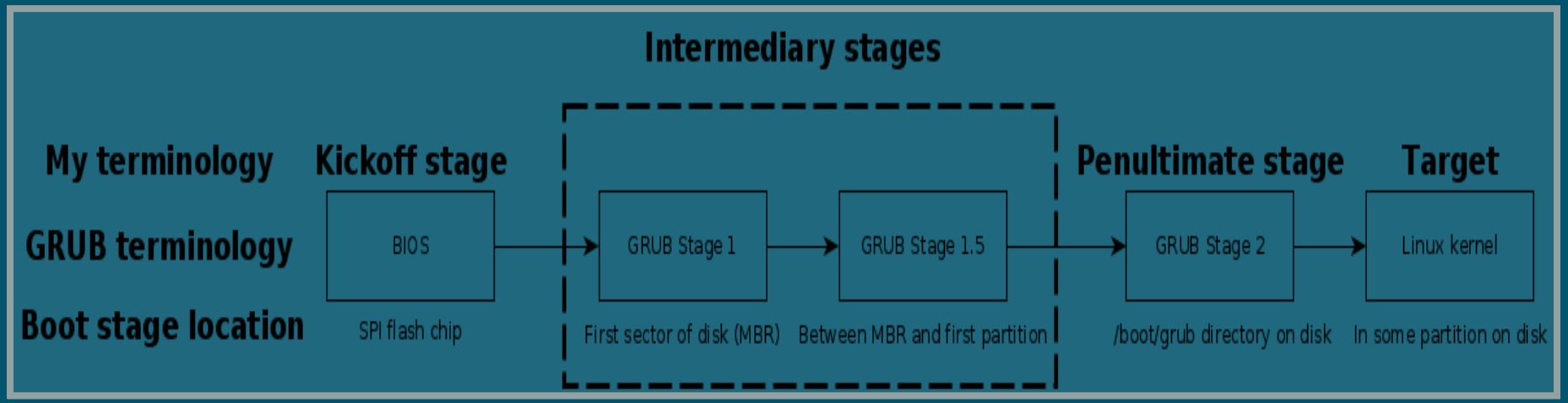
MBR

- A disk layout format
  - i.e. how to lay out partitions
- A convention for where to put bootloader code
- The first 512 bytes (first sector) of disk

MASTER BOOT RECORD

MBR

- Only supports 4 primary partitions, 2.2 TB disk
- Bootloaders chain-load region between MBR and first partition, then into /boot/grub in a real partition



Credit: Rebecca “.bx” Shapiro

DEMO

UNIFIED EXTENSIBLE FIRMWARE INTERFACE

UEFI

- Standard for firmware (not only for IBM PCs). The future.
- Originally developed by Intel (EFI), now managed by committee (UEFI)
- Macs use some hybrid abomination between EFI, UEFI, and their own thing

UEFI BOOTING OVERVIEW

- Supports BIOS "legacy" booting from MBR disk
  - But most often used with GPT-formatted disks
- Looks for a "EFI system partition" within each disk, which contains bootloaders
- Loads `/efi/boot/bootx64.efi` by default
- Configurable UEFI boot manager (like a boot menu)

GUID PARTITION TABLE

GPT

- New standard for laying out disk format
- Supports a minimum of 128 partitions and 2^64 sectors of disk space
- Practically limitless namespace ("GUIDs") for partition types
- Redundant GPT header for recovery

DEMO

FEATURES AND NOTES

BOOT MODE

- OSes are installed in UEFI or legacy mode
- *Why this matters*: It affects how the distro makes itself bootable, by writing to MBR or by creating a new loader in the ESP (and configuring the boot manager)
- Possible to "convert" afterwards, if you're willing to do disk surgery

HYBRID MBR

- Contains an MBR and an ESP, can be booted by BIOS and UEFI
  - GPT requires a "protective MBR"
- Used by modern live CDs so distros can be installed in either mode

SECURE BOOT

- Requires bootloaders in the ESP to be signed
- Not actually Microsoft being evil, surprisingly
- shim as a weird hack for signed 1st stage loader for grub

ADDITIONAL READING

- https://www.happyassassin.net/2014/01/25/uefi-boot-how-does-that-actually-work-then/
- http://www.cs.dartmouth.edu/~bx/blog/2015/09/03/a-toure-of-bootloading.html
- http://www.linux-kvm.org/downloads/lersek/ovmf-whitepaper-c770f8c.txt
- http://www.rodsbooks.com/refind/secureboot.html

THANKS FOR COMING!

linux.ucla.edu