UEFI and U

Or, how I learned to stop worrying and love UEFI

Or, baby bye-bye-BIOS

But really:

And end user’s perspective

First: what's a BIOS?

Something like that.

A BIOS:

- Lives on your MOBO
- Looks for and tests devices on boot (keyboard, cpu, RAM, floppy drive)
- Finds your bootloader on a disk and hands off control to it

Bootloader

- Lives in a special part of your hard disk
- Loads your OS
- e.g.
  - Grub
  - SYSLINUX
  - Windows Boot Manager

In summary:

The thing loads the thing which loads the thing which loads the thing
(BIOS -> GRUB -> Linux Kernel)

Limitations!

- MBR
  - Partitions
  - Disk size
  - Flakiness
- 16-bit
- 1MB address space

Enter UEFI

The “new” kid on the block

UEFI

- Intel Boot Initiative (1998 (!))
- UEFI (2005)
- UEFI 2.1 (2007)
  - Crypto
  - Network Authentication
  - UI

First, GPT

- MBR compatible-ish!
- Redundant headers/tables!
- Address up to 2 ZiB (2.147 * 10^9 TiB)
- 128 Partitions
  - ...by default
- Labels!

UEFI Booting

- Embeded? That’s silly.
- EFI Boot Partition (FAT32)
- Loads an EFI application
- Can hand off useful information (systemd-analyze)

EFI Application

- e.g.
  - Gummiboot
  - REFind
  - GRUB
  - Windows’s thing
  - Linux (no, really)

In summary:

(UEFI -> Linux Kernel)
(easy!)

Compare...

grub-install --target=i386-pc --recheck **/dev/sda**

grub-mkconfig -o /boot/grub/grub.cfg

- hope grub / your distro set everything up correctly

efibootmgr -d /dev/sd**a** -c -L "Arch Linux" -l /vmlinuz-linux -u "root=**/dev/sda2** rw initrd=/initramfs-linux.img"

- hope your hardware manufacturers follow a now universal standard

No more windows overwriting GRUB!

They live side-by-side in your EFI Boot Partition!

Unnecessary Complexity?

Well...

Speaking of windows...

SecureBoot

- Verifies that the EFI application has been signed by a trusted key

Who controls the keys?

Your manufacturer decides...

Microsoft the nice guy?

Secure if you want it!

Repeat after me:

- UEFI != Secure Boot
- UEFI != Secure Boot
- UEFI != Secure Boot

coreboot as an alternative

Chromebooks!

What say you?


ASUS EFI BIOS Utility - EZ Mode
Exit/Advanced Mode
06:06
Tuesday[11/16/2010]
P8P67 DELUXE
BIOS Version : 0304
CPU Type : Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz
Total Memory : 2048 MB (DDR3 1333MHz)
English
Build Date : 10/21/2010
Speed : 3100 MHz
Temperature
CPU +116.6°F/+47.0°C
MB +96.8°F/+36.0°C
Voltage
CPU 1.200V
5V 5.120V
3.3V 3.408V
12V 12.288V
Fan Speed
CPU_FAN 1034RPM
PWR_FAN1 N/A
CHA_FAN1 N/A
CHA_FAN2 N/A
System Performance
Quiet
Performance
Energy Saving
Normal
Boot Priority
UEFI
UEFI
Use the mouse to drag or keyboard to navigate to decide the boot priority.
Boot Menu(F8)
Default(F5)