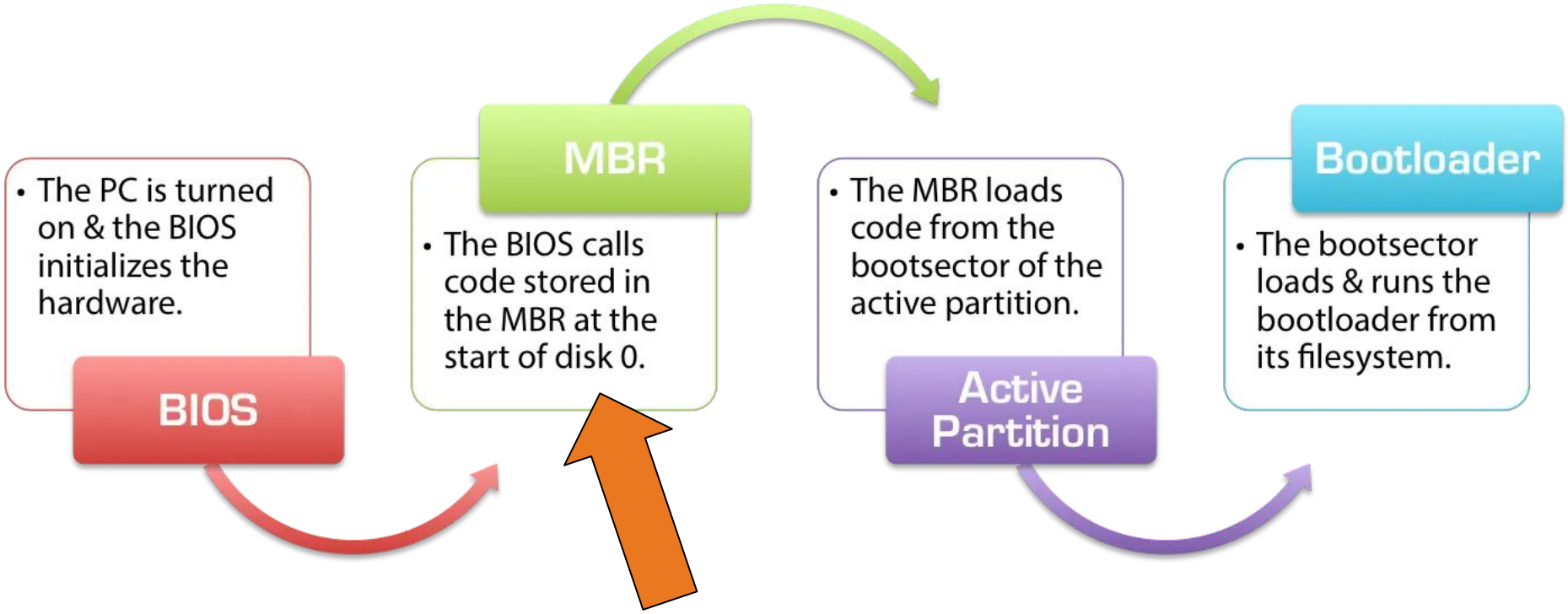
Embracing Open Firmware in HPC for Faster and More Secure Provisioning

Devon T. Bautista

USRC Showcase
12 August 2020

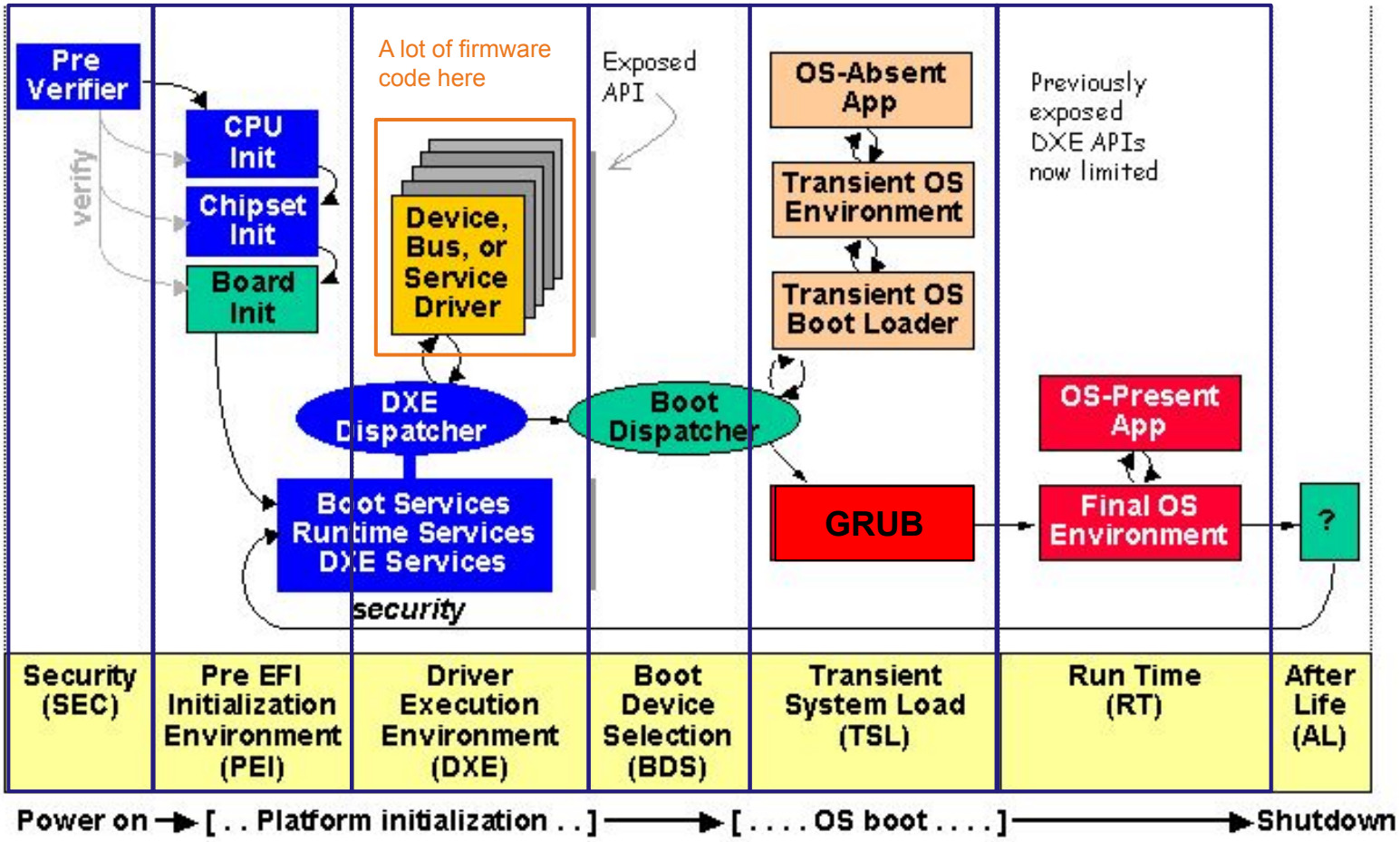
BIOS: The Old Way of Booting



Blindly executes code at CHS 0/0/1

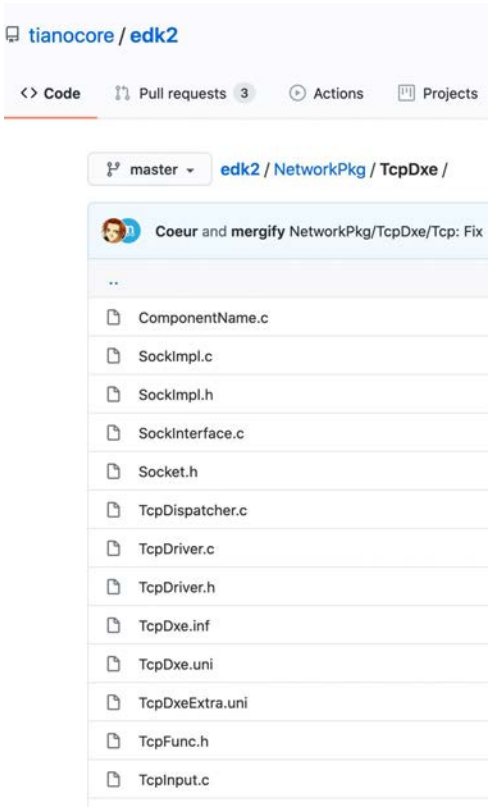
From: https://neosmart.net/wiki/mbr-boot-process/

UEFI: The Current Way of Booting

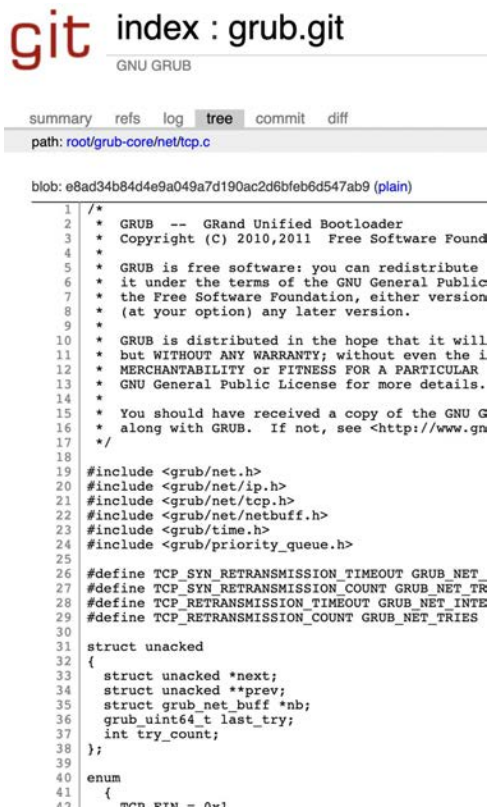


From: https://trmm.net/LinuxBoot_34c3

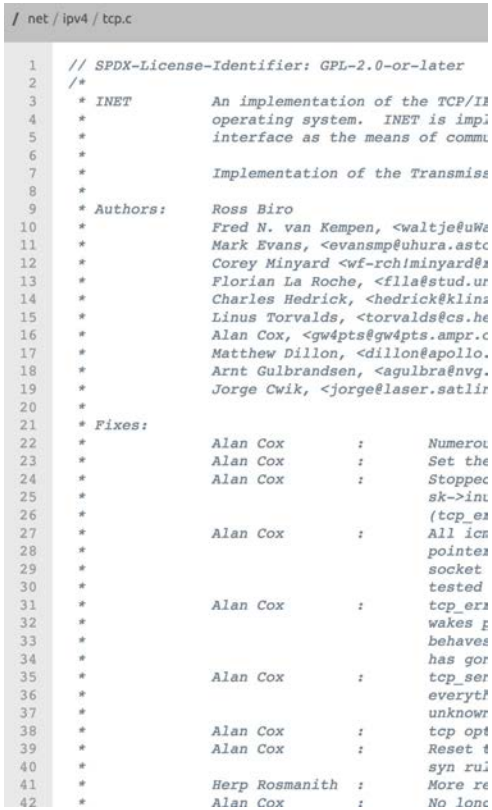
Network Drivers



Intel's EDKII Firmware

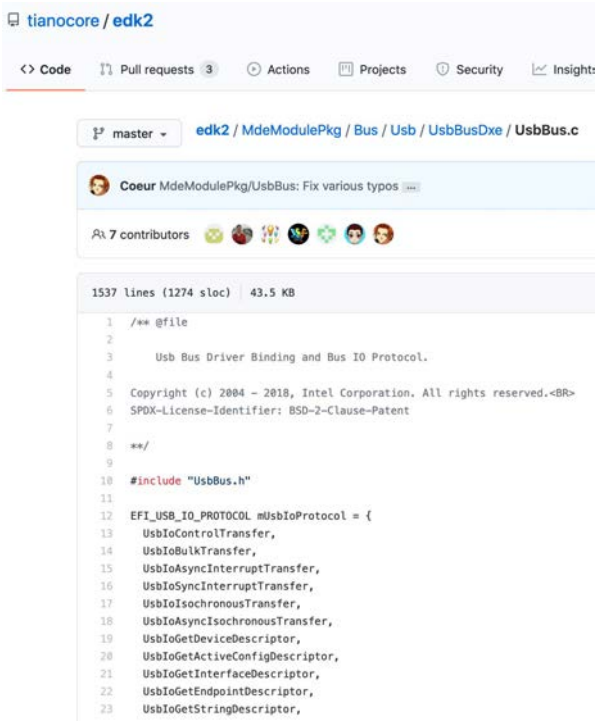


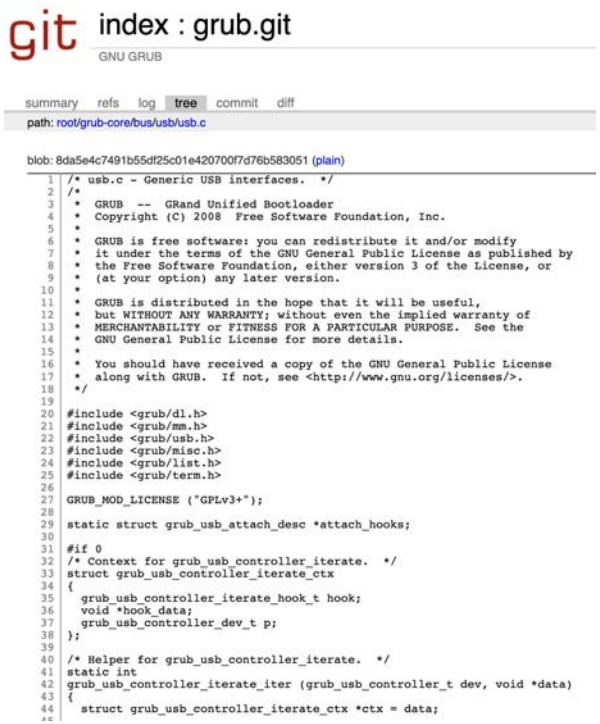
GRUB Bootloader



Linux

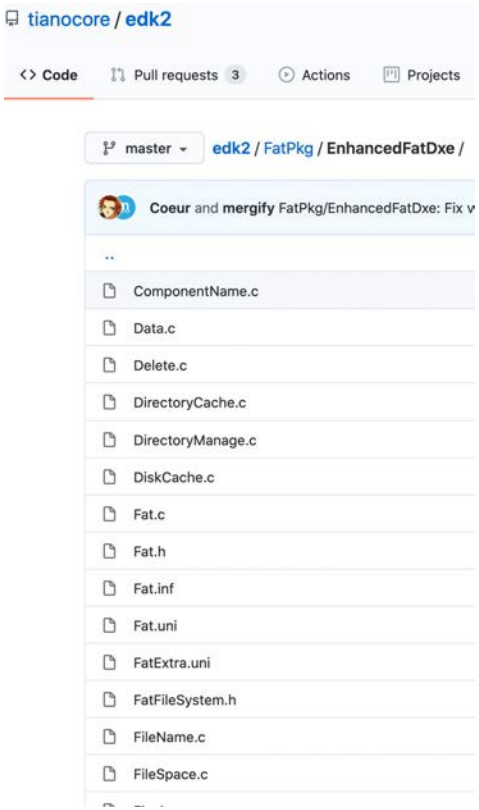
USB Drivers





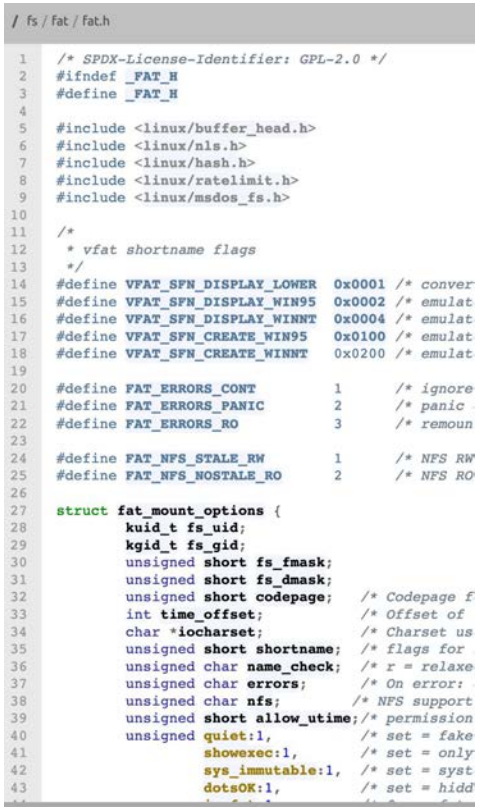
Intel's EDKII Firmware *GRUB Bootloader* *Linux*

Filesystem Drivers



Intel's EDKII Firmware

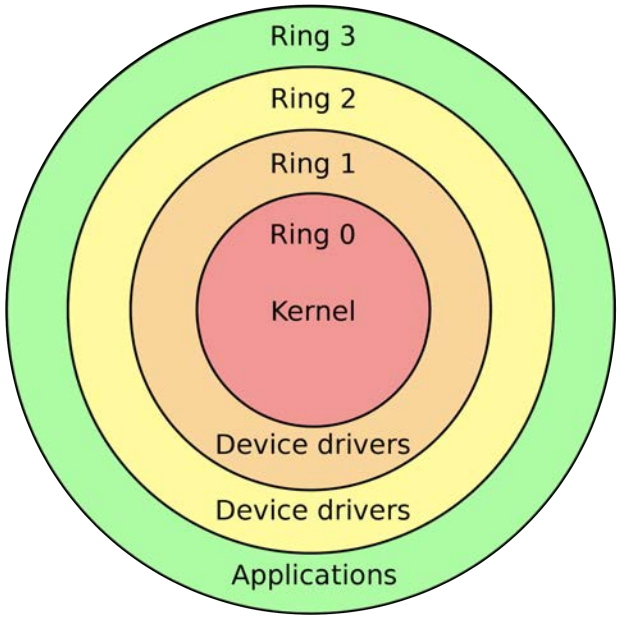
GRUB Bootloader

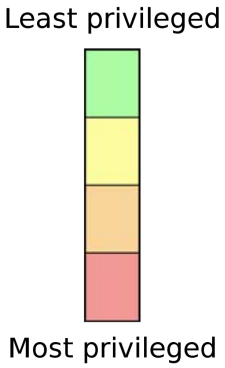


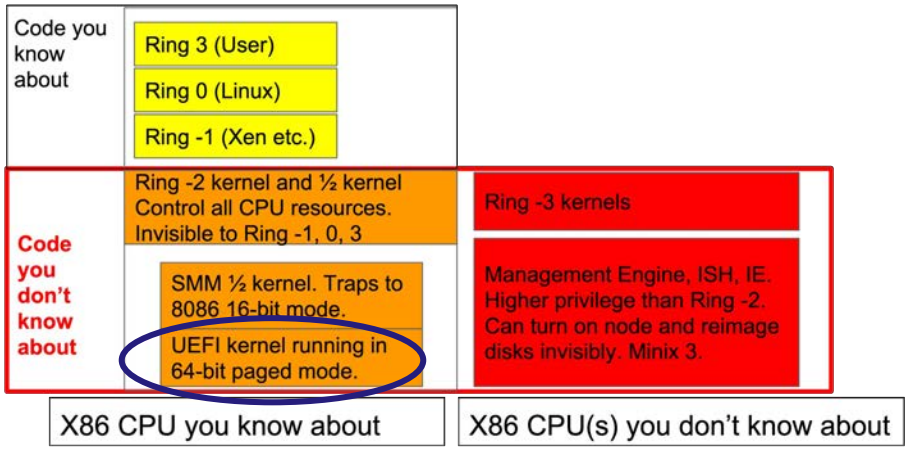
Linux

Privilege Rings

Traditional **vs.** **Modern**







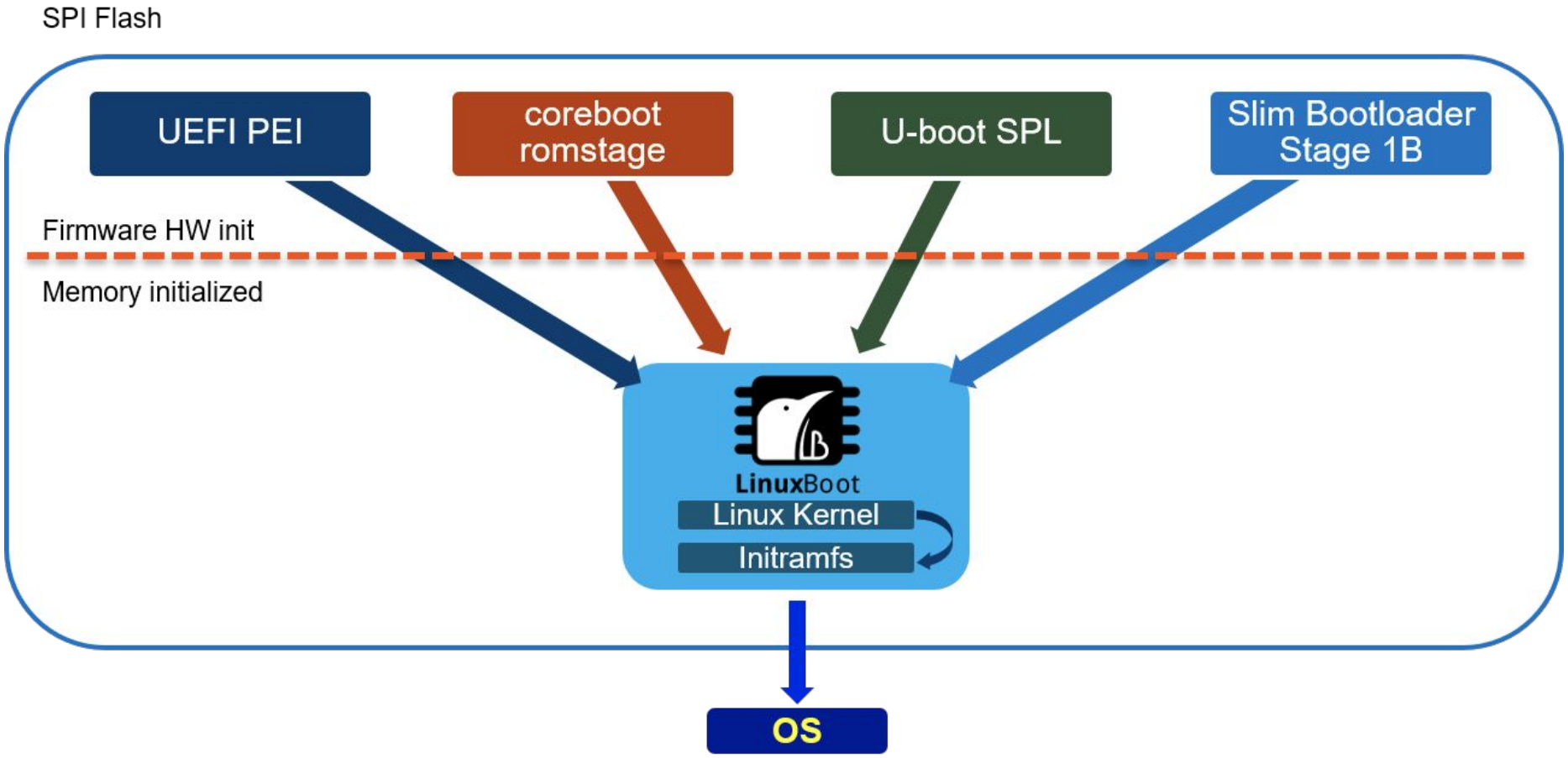
From: https://en.wikipedia.org/wiki/Protection_ring

From: https://www.youtube.com/watch?v=iffTJ1vPCSo

Problems

- Redundant drivers with different implementations
  - Increases attack surface
  - Too many unneeded or redundant drivers loading slows down boot
- Insufficiently audited code with the most privileged system access
  - Proprietary, closed-source
  - Reviewed by relatively small number of developers within company
- Reliant on vendor for updates and repairs

"Let Linux Do It"

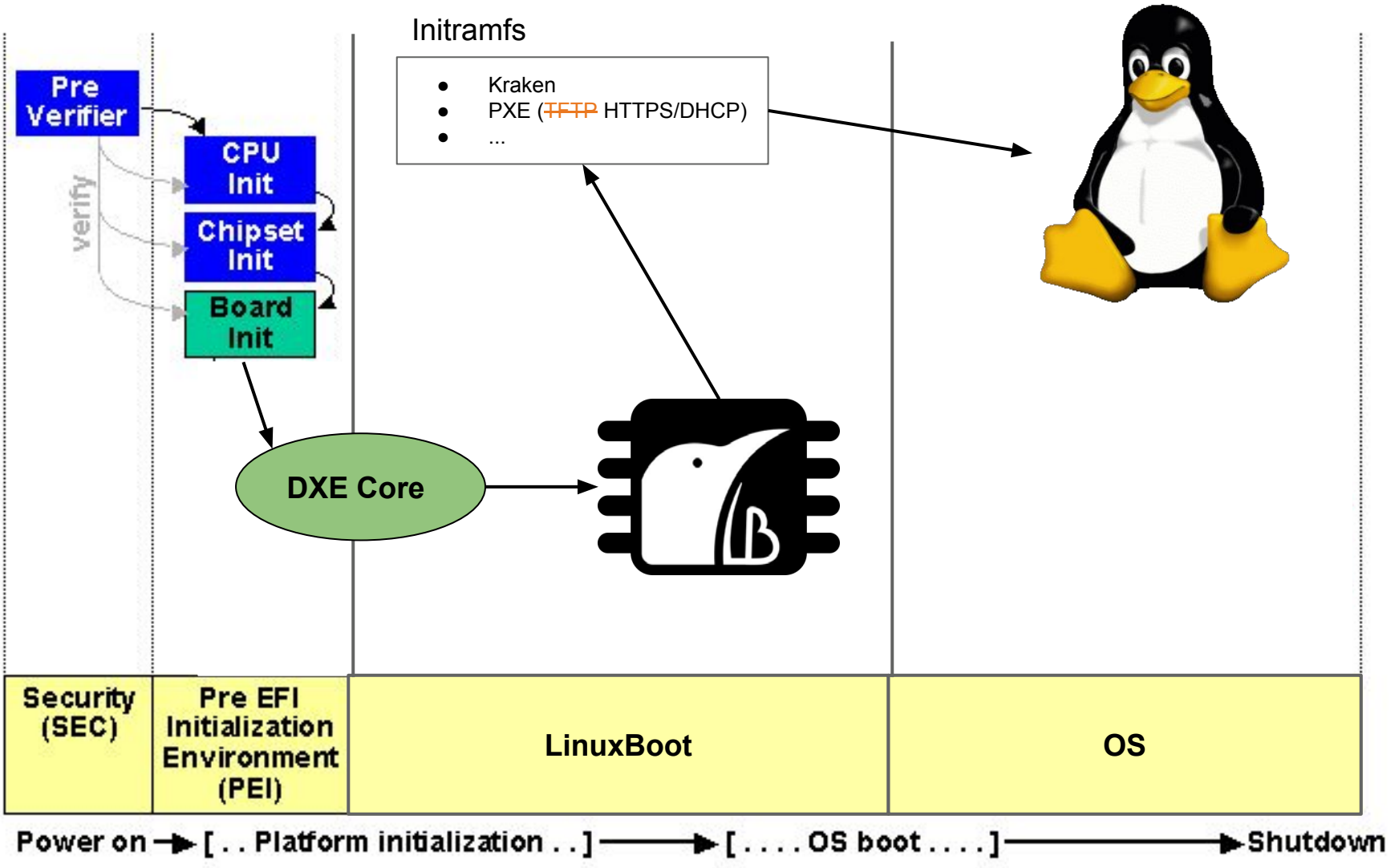


From: https://www.linuxboot.org/

Benefits of Linux in Firmware

- Improves boot reliability
  - Replaces lightly-tested firmware drivers with hardened Linux drivers
- Improves boot time (up to 20 times faster in some cases)
  - Removes unnecessary/insecure code
- Allows customization of the initrd runtime to support site-specific needs (both device drivers as well as custom executables)
  - **Use Case:** Custom provisioning tools in the boot process
  - e.g. Replace TFTP with HTTPS for PXE booting
- Proven approach for almost 20 years in military, consumer electronics, and supercomputing systems – wherever reliability and performance are paramount

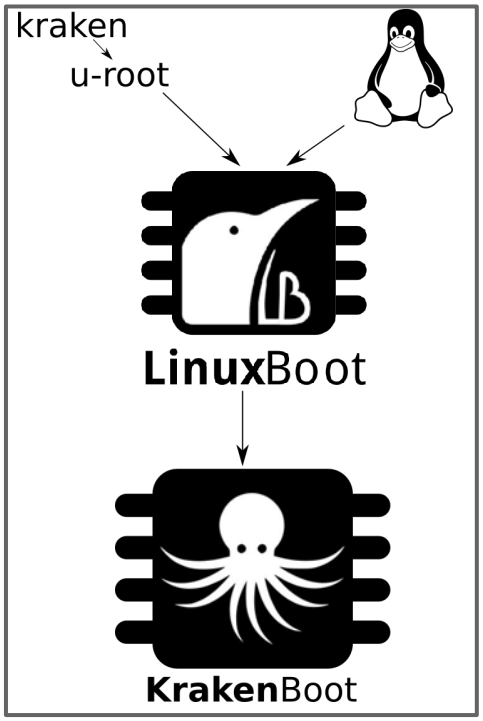
HIGH PERFORMANCE COMPUTING


Initramfs
Kraken
PXE (~~TFTP~~ HTTPS/DHCP)
...
Pre Verifier
verify
CPU Init
Chipset Init
Board Init
DXE Core
Security (SEC)
Pre EFI Initialization Environment (PEI)
LinuxBoot
OS
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown

USRC's Research Into Provisioning with Open Firmware

Done

- Emulate a modified firmware image running a Linux kernel and custom initramfs
- Provision a VirtualBox cluster using kraken in a custom initramfs
  - Not a firmware image, but through VirtualBox



LA-UR-20-26019

Doing

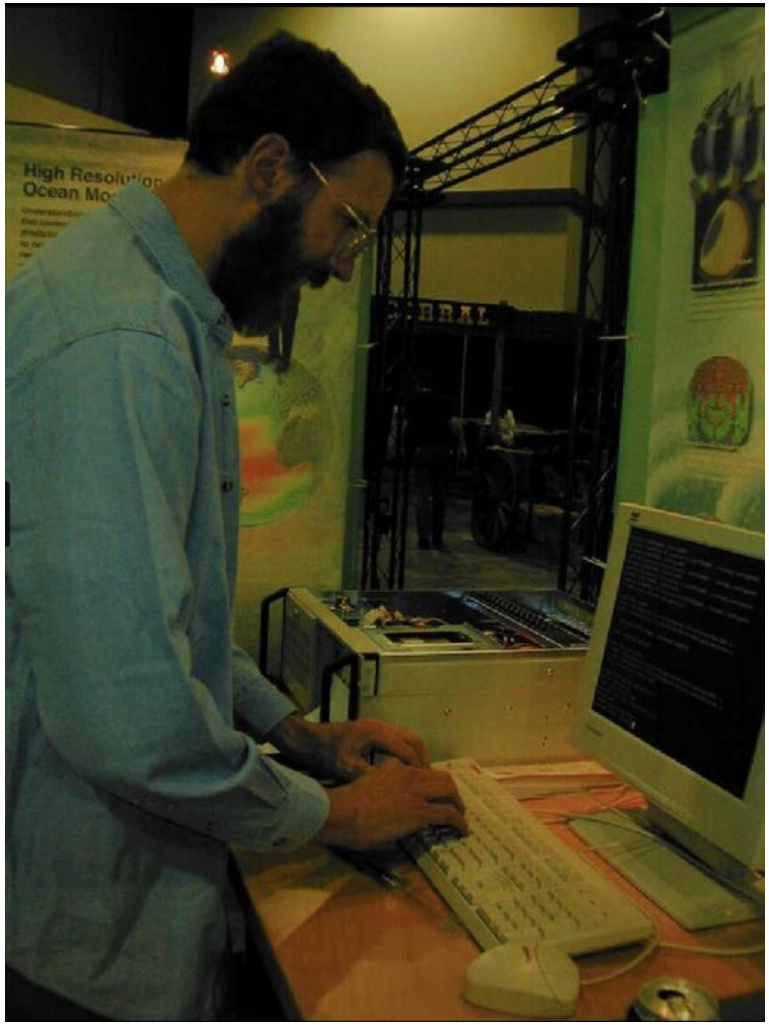
- Create a working example of provisioning using emulatable firmware images
- Provision on *real* hardware in firmware

Problems Solved

Firmware Until Now	Firmware Now and Beyond
Contains an OS	Let Linux do it
Opaque, understood by few	Open, well-understood by many
Proprietary ecosystem	Auditable, debuggable
Product-specific	Portable, reusable
Vendor-specific tooling	Open source tools
Locked down	Customizable

“The vendors will never support this.”

Open Firmware: Not a New Idea



Ron Minnich, creator of Coreboot (formerly LinuxBIOS), at LANL in 1999

coreboot

HIGH PERFORMANCE COMPUTING

Facebook

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

LISA18

LinuxBoot in provisioning

- LinuxBoot can simplify provisioning a lot
  - Tested DHCP/TFTP implementations
  - Better protocols: HTTPS instead of TFTP
  - Consistent firmwares everywhere
  - We know and control what that we run

OPEN Compute Project

OpenBMC

HIGH PERFORMANCE COMPUTING

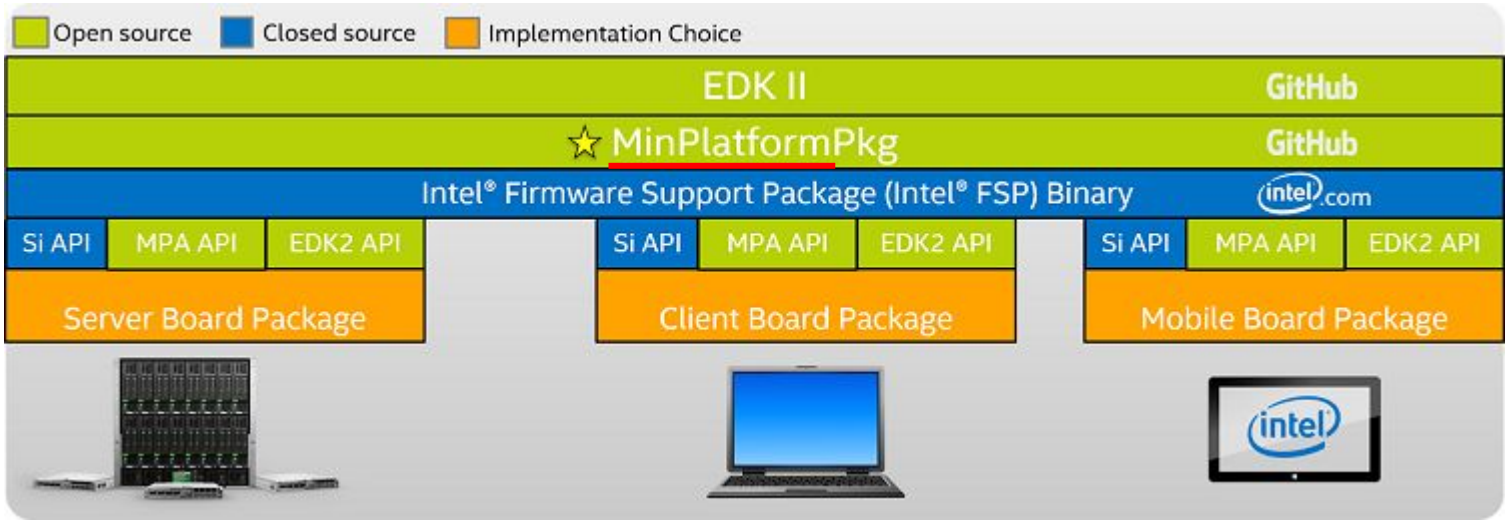
Google

OPEN SOURCE FIRMWARE CONFERENCE
2019 SEPTEMBER 03–06

https://osfc.io/

Intel

tianocore



See: https://www.youtube.com/watch?v=x3NFbUC3hkA
and: https://edk2-docs.gitbook.io/edk-ii-minimum-platform-specification

HIGH PERFORMANCE COMPUTING

ARM

arm Developer

IP PRODUCTS TOOLS AND SOFTWARE ARCHITECTURES SOLUTIONS COMMUNITY SUPPORT DOCUMENTATION DOWNLOADS

Overview | Building EDKII Firmware | Dynamic tables framework

Overview

Arm is an active contributor to the EDKII project hosted by the Tianocore community.

The EDKII project is an open source project that provides a modern, feature-rich, cross-platform firmware development environment for the UEFI and PI specifications developed and maintained by the UEFI Forum.

Arm contributions make sure the EDKII project constantly keeps an up to date implementation of a UEFI compliant firmware on Arm systems.

Arm contributes to both the EDKII main repository, maintaining some core packages like DynamicTablesPkg and StandaloneMMPkg, and the EDKII platforms repository, hosting support for various Arm reference platforms as well as other 3rd party Arm-based platforms maintained by either Linaro or partners.

UNIFIED EXTENSIBLE FIRMWARE INTERFACE

HIGH PERFORMANCE COMPUTING

Questions?

Acknowledgements

J. Lowell Wofford
Cory Lueninghoener

Over 70 years at the forefront of supercomputing