Benefits of User-Controlled Firmware in Production Systems

OPEN SYSTEM FIRMWARE

Embedded Software

Ryan O'Leary
with Jean-Marc Eurin

Google
Google

OCP Taipei Workshop
October 23, 2019

with Ron Minnich, Chris Koch, Gan Shun Lim, Prachi Laud, Xuan Chen
with Max Shegay
with Trammell Hudson
with Julien VdG, Guillaume Giamarchi
with Jean-Marie Verdun
with David Hendricks, Andrea Barberio, Tobias Fleig
with Łukasz Siudut, Anatole Denis
with Philipp Deppenwiese
with Loic Prylii

Google
ex-Google Intern

ITRenew

Facebook
Facebook
9elements Cyber Security
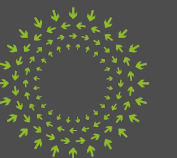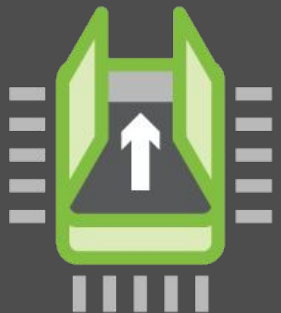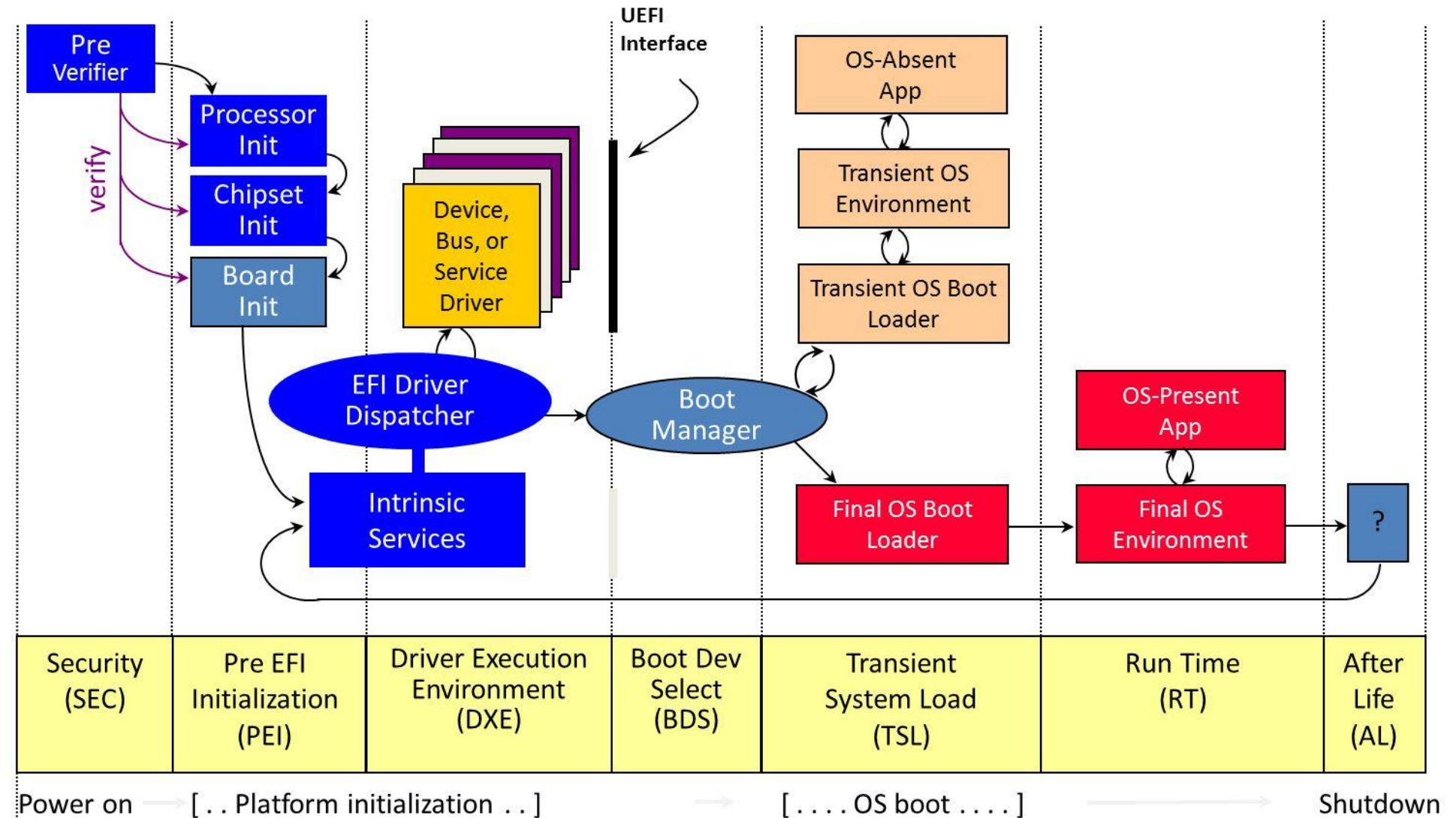Netflix

Consume. Collaborate. Contribute.

Overview

Consume. Collaborate. Contribute.

UEFI Boot

OS-like features:

- Drivers
  - Network
  - Disk
  - USB
- Dispatching / Scheduling
- Filesystem
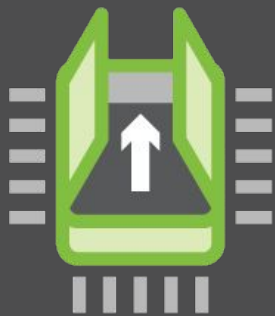- Applications
- Events
- ...
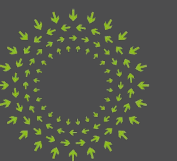
Today's System Firmware

- UEFI Implementations
    - are mostly closed source,
    - written in C,
    - share an address space in ring 0.
- Vendors are incentivized to ship it and forget.
- **Owners do not own their system.**
    - **Even when it is open-source**

OPEN SYSTEM FIRMWARE

Embedded Software

*Consume. Collaborate. Contribute.*

Today's System Firmware

- 20+ vendors involved in shipping firmware
  - IBVs (BIOS vendors),
  - silicon manufacturers,
  - ODMs, OEMs,
  - NIC, disk, BMC, … vendors,
  - OS vendors (Windows, RHEL, Debian)
- Black boxes that wrap black boxes.
- What happens with vulnerabilities?
  - Who owns fixing it?
  - How to integrate it?
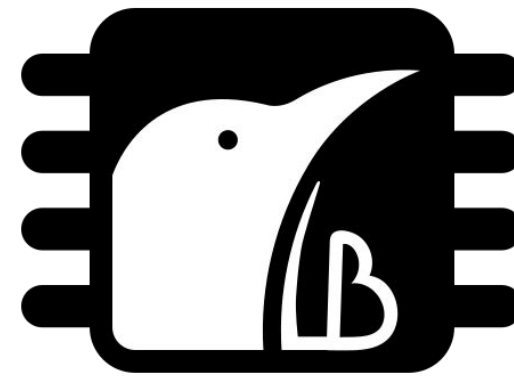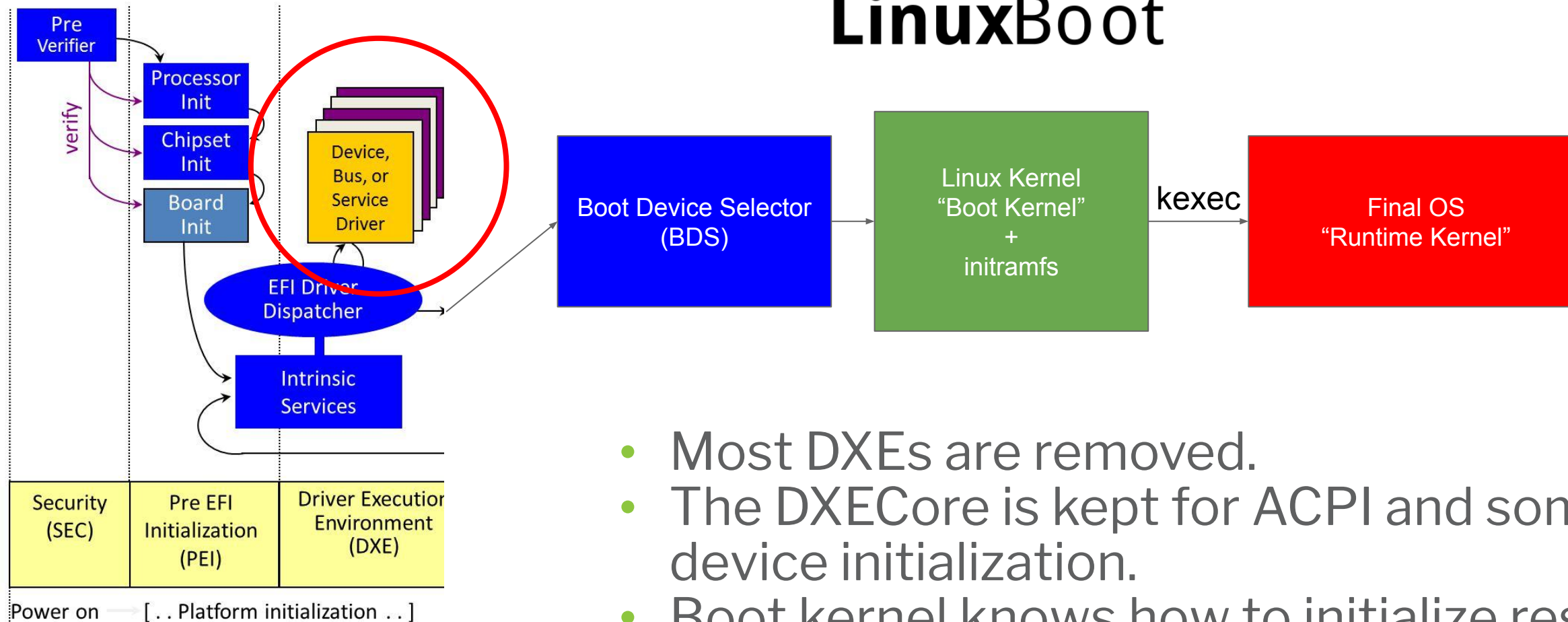
OPEN SYSTEM FIRMWARE

Embedded Software

OPEN

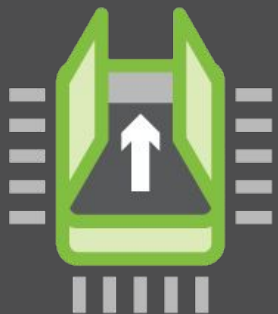*Consume. Collaborate. Contribute.*
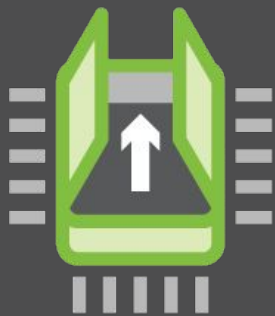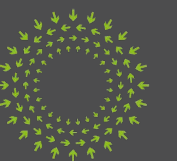
LinuxBoot

- Most DXEs are removed.
- The DXECore is kept for ACPI and some device initialization.
- Boot kernel knows how to initialize rest of devices.
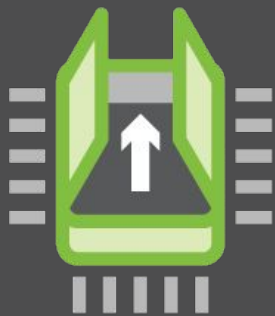- The boot kernel kexec's the runtime kernel.

Consume. Collaborate.
*Contribute.*

What have we gained?

- Linux already has drivers for everything
  - No need to reimplement drivers in firmware
- Some applications and drivers can be written as a userspace program in Linux
- Speed
  - Winterfell boot time: **8 minutes down to 20 seconds**
  - Boots faster than iPXE/grub/etc. (measured for 20 years)
- Are we simply replacing GRUB?
  - Remove grub and replace what was used to run GRUB.
- Why have Linux boot another Linux?
  - Can use limited kernel to boot more feature-full kernel
 - Kiosk mode: The firmware linux is the final linux.

OPEN SYSTEM FIRMWARE

Embedded Software

OPEN

Consume. Collaborate. Contribute.
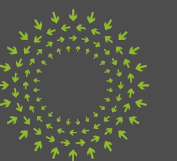
Linux + what's in the initramfs?

- Whatever you want.
  - We provide tools, not policy.
- Busybox?
- Systemd-boot?
- Petiteboot?
- HEADS? trmm.net/Heads
  - Security-focused busybox LinuxBoot runtime
- Stages of firmware we are replacing…
  - Drivers
  - Bootloaders
  - Debugging shells
  - …

initramfs + Linux

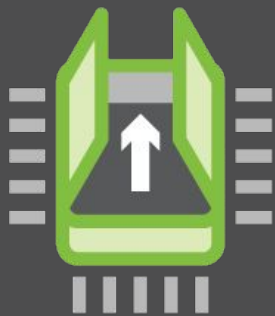OPEN SYSTEM FIRMWARE

Embedded Software
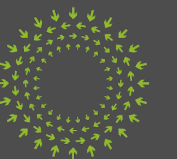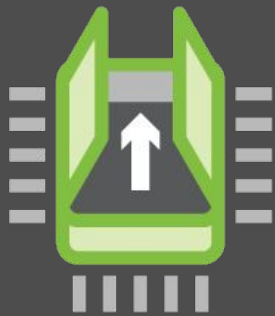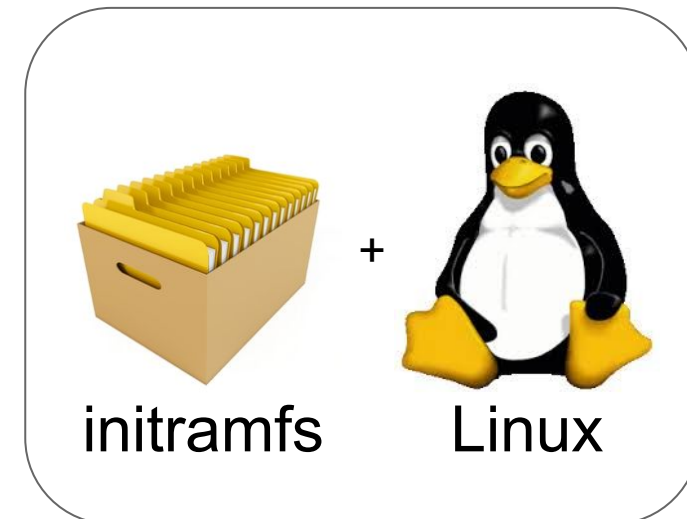
u-root: Why Golang for firmware?

- Use Go static analysis tools
  - go vet, golint, gofmt, ineffassign, ...
- Race detector, memory sanitizer, etc...
  - go test -race
- Continuous Integration (CI) testing
- Open documentation (https://godoc.org/)
- Language is safer than C or shell scripts
- Well designed and secure standard library
  - Easy cross-compilation: GOOS= and GOARCH=
  - Supports amd64, arm, arm64, and ppc64
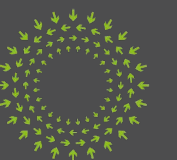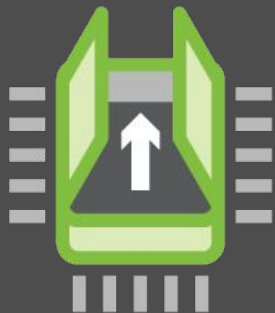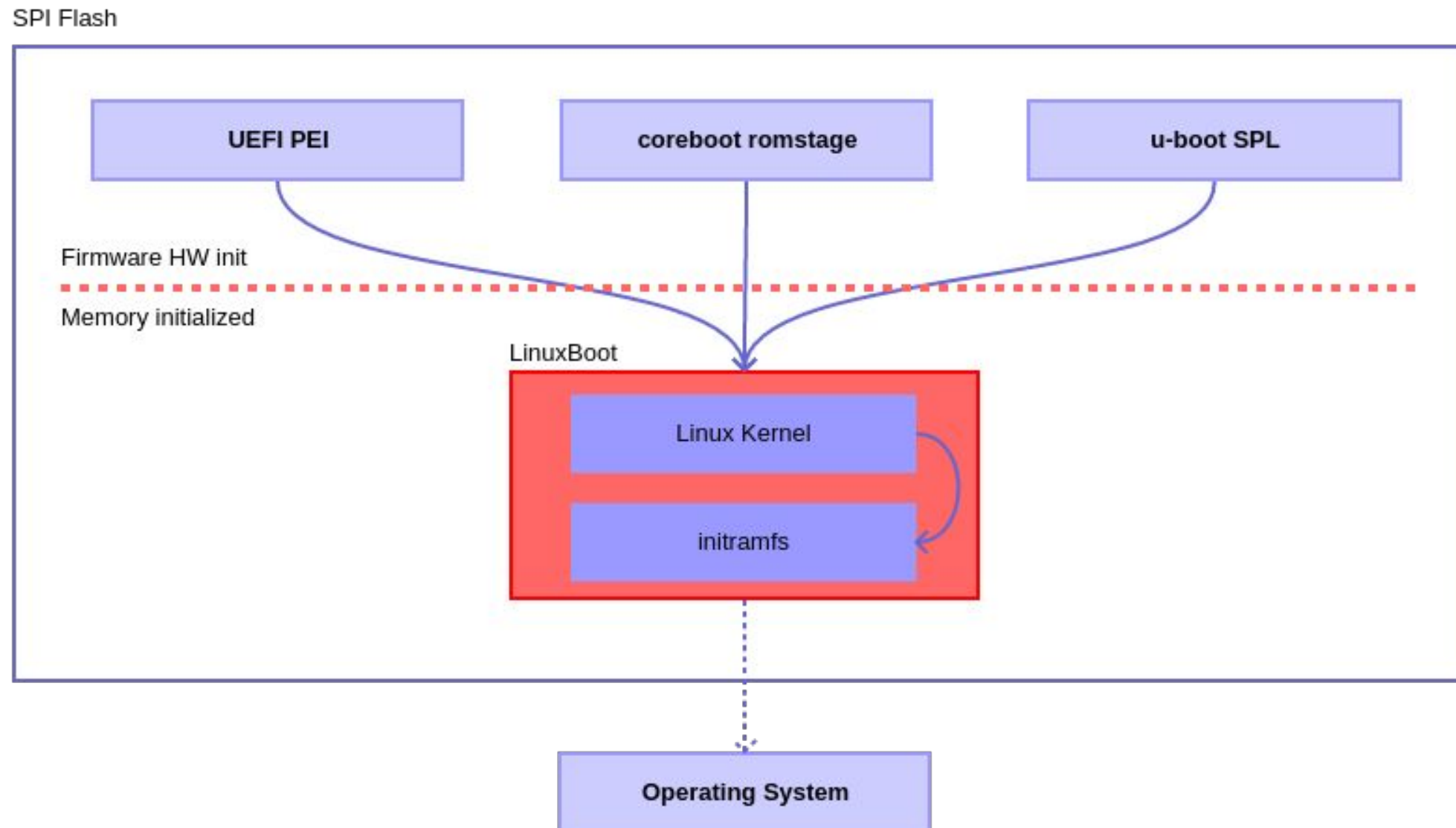- Fast compilation (on the order of seconds)

Embedded
Software

Consume. Collaborate.
Contribute.
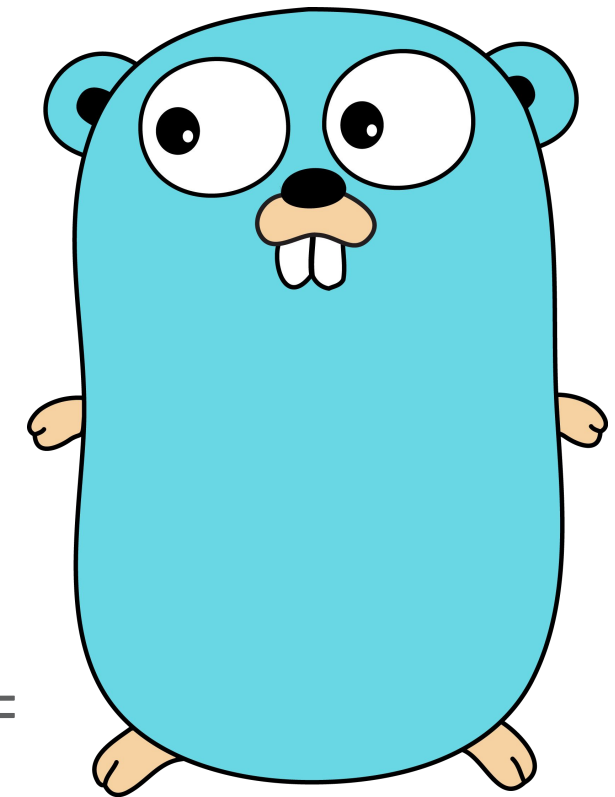
OPEN

More Bootloader Options
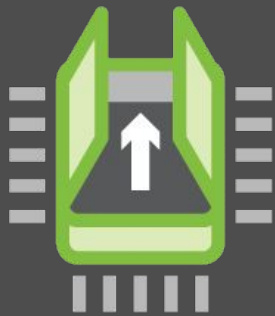
Consume. Collaborate. Contribute.

Booting Multiboot OSes from LinuxBoot

- The work of Max Shegai
- Supports booting OSes using the Multiboot standard
- Open-source and available on GitHub
- Can now boot:
  - Akaros
  - Harvey
  - tboot
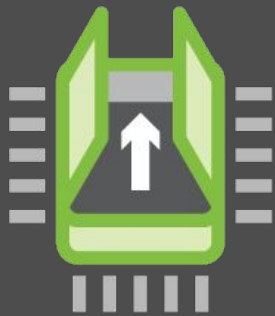 - VMware ESXi
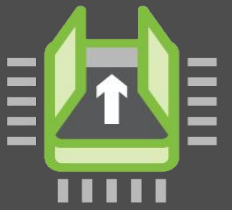
OPEN SYSTEM
FIRMWARE

Embedded
Software

OPEN

Booting Windows from LinuxBoot

- The work of Ofir Weisse
- Still a proof of concept
- Open-source and available on GitHub

OPEN SYSTEM FIRMWARE
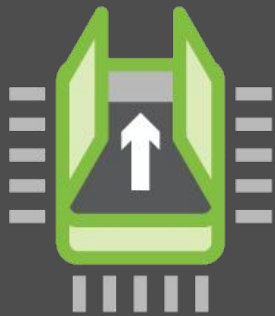
Embedded Software

OPEN

Case Study #1: Google

- Substantial contributions to LinuxBoot open-source projects
  - u-root, fiano, dhclient, ...
- Substantial presence in conferences and communities
- **LinuxBoot is now running on Google's production servers!**
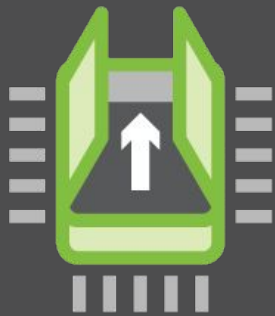
OPEN SYSTEM FIRMWARE

Embedded Software

Case Study #2: ChromeOS

- Chromebooks have been running Coreboot for **almost a decade**
  - Accounts for 50 million machines
- Supports arm32, arm64 and x86
- Coreboot has existed for over **2 decades!**
- Firmware is open-source and user-controlled
  - Some leeway in terms of FSP blobs
- Large open-source community contributing to Coreboot
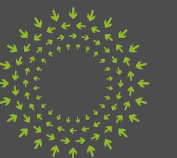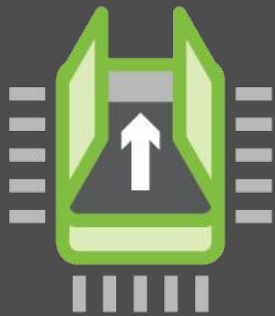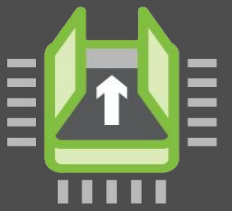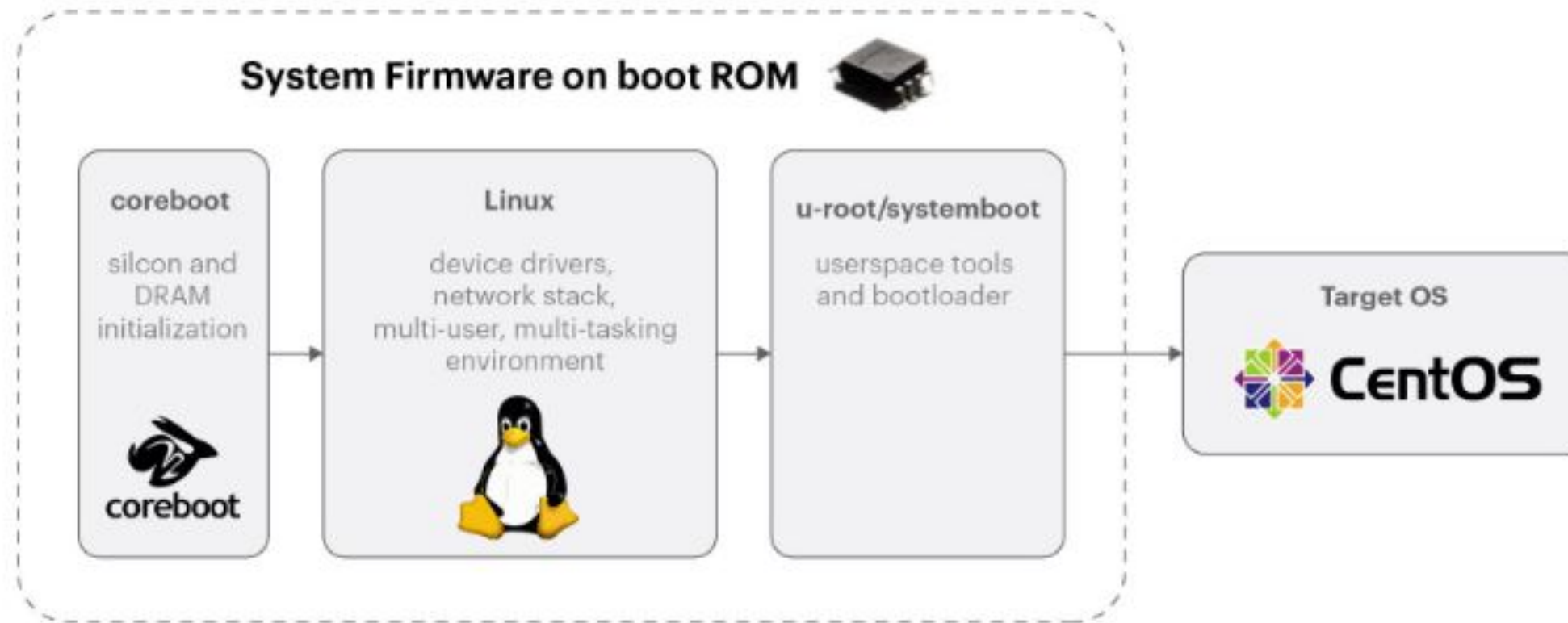- Very passionate engineers and active open-source community

Embedded Software

Consume. Collaborate. Contribute.

Case Study #3: Facebook

Embedded Software

Case Study #4+: Others

- Netflix
- HPE
- Wiwynn
- ITRenew

Embedded
Software

*Consume. Collaborate.
Contribute.*
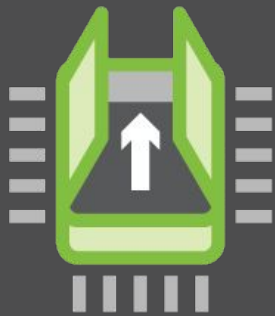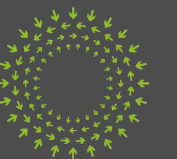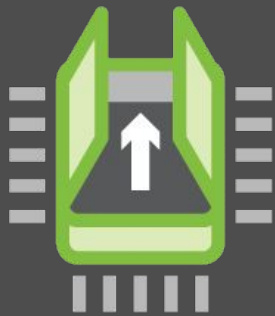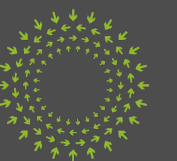
The Future

- More and more vendors are using LinuxBoot
- Shipping more hardware with LinuxBoot
- Modern bootloaders implemented in Go
- Firmware tools in Go (cbfs support, self-flashing capabilities, …)
  - cbfs support
  - self-flashing capabilities
  - improved ACPI and device tree support
  - …
- Documentation
  - Linuxboot Book, technical writers are onboard

OPEN SYSTEM
FIRMWARE

Embedded
Software

Consume. Collaborate.
Contribute.

Call to Action

Join Open Source Firmware Slack

https://u-root.slack.com

Join using https://slack.u-root.com

LinuxBoot

https://www.linuxboot.org

https://github.com/linuxboot/linuxboot

u-root

https://github.com/u-root/u-root

Bi-weekly OSF Calls

https://www.opencompute.org/wiki/Open_System_Firmware
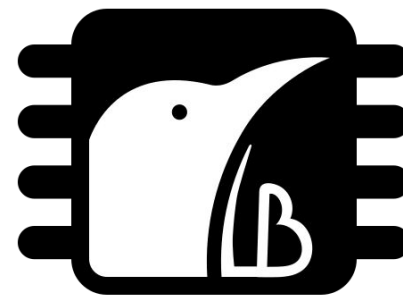
Consume. Collaborate.
Contribute.

LinuxBoot Book

https://github.com/linuxboot/book

New Hardware
We'll help get LinuxBoot working on your hardware.

Laptop Stickers

Susanne Nähler

LinuxBoot

BIOS HAZARD
INFECTED SYSTEM

OPEN SYSTEM
FIRMWARE

Embedded
Software

OPEN