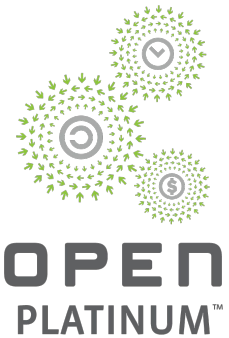
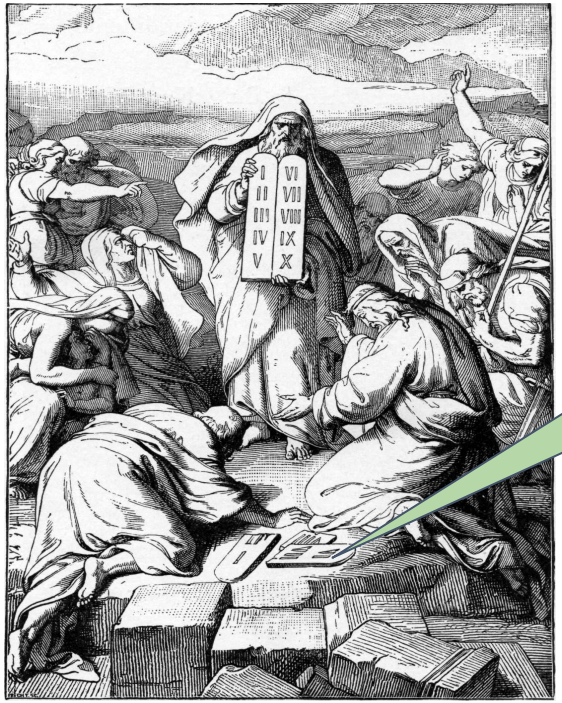
coreboot on OCP systems

Ron Minnich
co-creator, Open System Firmware workstream



How BIOS/UEFI are delivered to customers today:
Silicon tablets, from the heavens, engraved with software, unchangeable.



Customer’s firmware attempts that did not work out

How’s that working for ya? [not so well]

https://eclypsium.com/2018/08/27/uefi-remote-attacks/

https://www.bleepingcomputer.com/news/security/uefi-firmware-vulnerabilities-affect-at-least-25-computer-vendors/ (FEB 2022)

HP Patches UEFI Vulnerabilities Affecting Over 200 Computers (May 12 2022)

coreboot: 20 years, 1 vuln? Still not sure.

Old Model: chip provider knows best, not the customer
“you’re gonna eat it and you’re gonna like it”

- That’s how kernels, compilers, and systems software used to be distributed
- Software came with unfixable “Bugs Inside™”
- Customers could not fix a bug, or share a fix
- Or even talk about a bug!
- Or even get a confirmation that it *was* a bug
  - “nobody else is reporting this problem”
- Sound familiar?
- New model: collaborative creation, i.e. sometimes customers do know best!

Open System Firmware
also
Open Source?

- **Multi-generation and multi-vendor data center fleet mgmt. at scale**
  - Modular firmware with high degree of reuse
  - Open-source tool chain
  - Customization and Provisioning at scale
- **Security and Ownership**
  - Customer control over reset vector and attestation flows
  - “open” firmware reduces attack surface
  - Runtime firmware visibility & control
- **Community driven** collaboration
  - Lifts all boats
  - Faster development, backporting and bug fixing
  - “Chosen few” to broader firmware talent pool
  - Proven quality (e.g., Linux drivers)

Meta Path: Why?

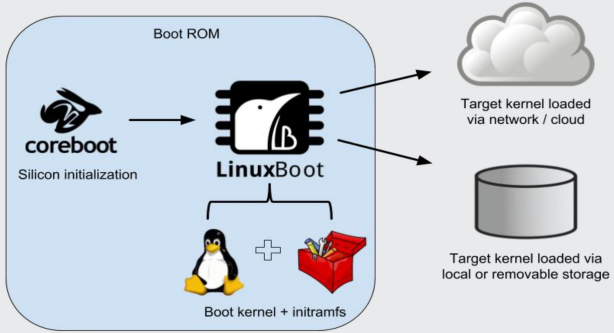
Booting is hard

- Ever-increasing amount of hardware
  - Many local/removable storage media and networking devices
  - Complex setup, complex protocols
- Firmware has become an operating system
- More demands for firmware security
  - Verified/secure boot, measured/trusted boot, attestation
  - Secure network protocols, crypto
- Provisioning is hard

Problems with closed firmware

- Archaic, complex, often quite buggy
  - Even open firmwares are often unfamiliar and difficult to extend
- Reactive instead of Proactive debugging
- Hard to maintain, can't forward/backport features and fixes
- Vendor-specific tools
- "Dimensions" of supporting firmware at scale
  - Robustness, flexibility, debugging, build and deployment...

How we're addressing the problem

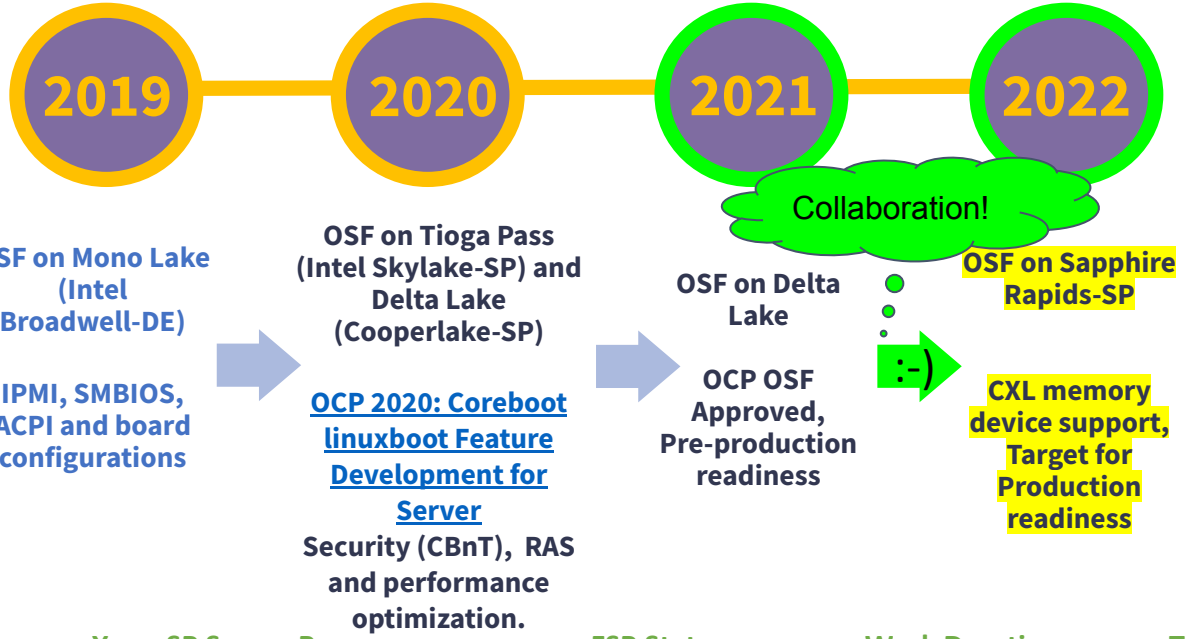


Why LinuxBoot

- We use Linux... a lot
- Production-quality drivers, networking, crypto
- Versatility
  - Can be used on anything that is intended to run Linux.
- We have engineering teams who understand Linux very well
  - Leverage talent we already have
- General goodness that open source brings
  - Auditability, portability, modern development, collaboration, ...

***source**: **Open Source Firmware @ Facebook,** 2018 open source firmware conference*
(David Hendricks, Andrea Barberio)

Meta Path: Status



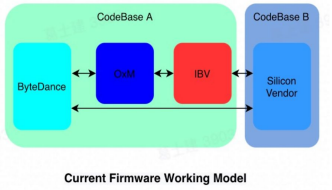
OCP Server	Xeon SP Server Processor	FSP Status	Work Duration	Test Pass Rate
TiogaPass	SkyLake - SP	Prototype	Jan. 2019 - Feb. 2020	38%
DeltaLake	CooperLake – SP(6UPI)	Statement Of Work	Mar. 2020 - July 2021	95%
Next Generation single socket server	SapphireRapids - SP (SPR-SP)	Included in Intel Reference Platform BIOS as platform POR	Jan. 2021 on-going	Trending better than DeltaLake

ByteDance Path: Why?

Firmware Defects

- Comparing Linux community, UEFI community is NOT active
- Can't fix UEFI issue immediately since some key modules are controlled by IBV
- Working Model is NOT efficient.

OPEN SYSTEM FIRMWARE



Current Firmware Working Model

Hardware improvement:
- Core Count
- Memory Capacity
- Flash Size
- …

Next Generation Firmware?

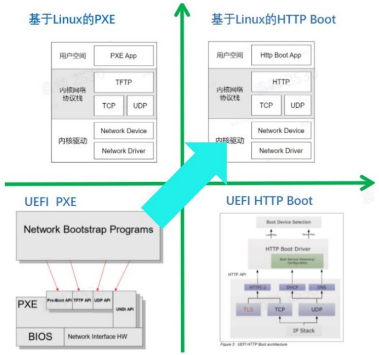
OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Key Example in LinuxBoot

UEFI Disadvantage
- UEFI network stack is not powerful
- Hard to optimize
- etc

LinuxBoot Advantage
- Linux Network Stack is powerful
- Independent of firmware vendor
- There are more linux network experts



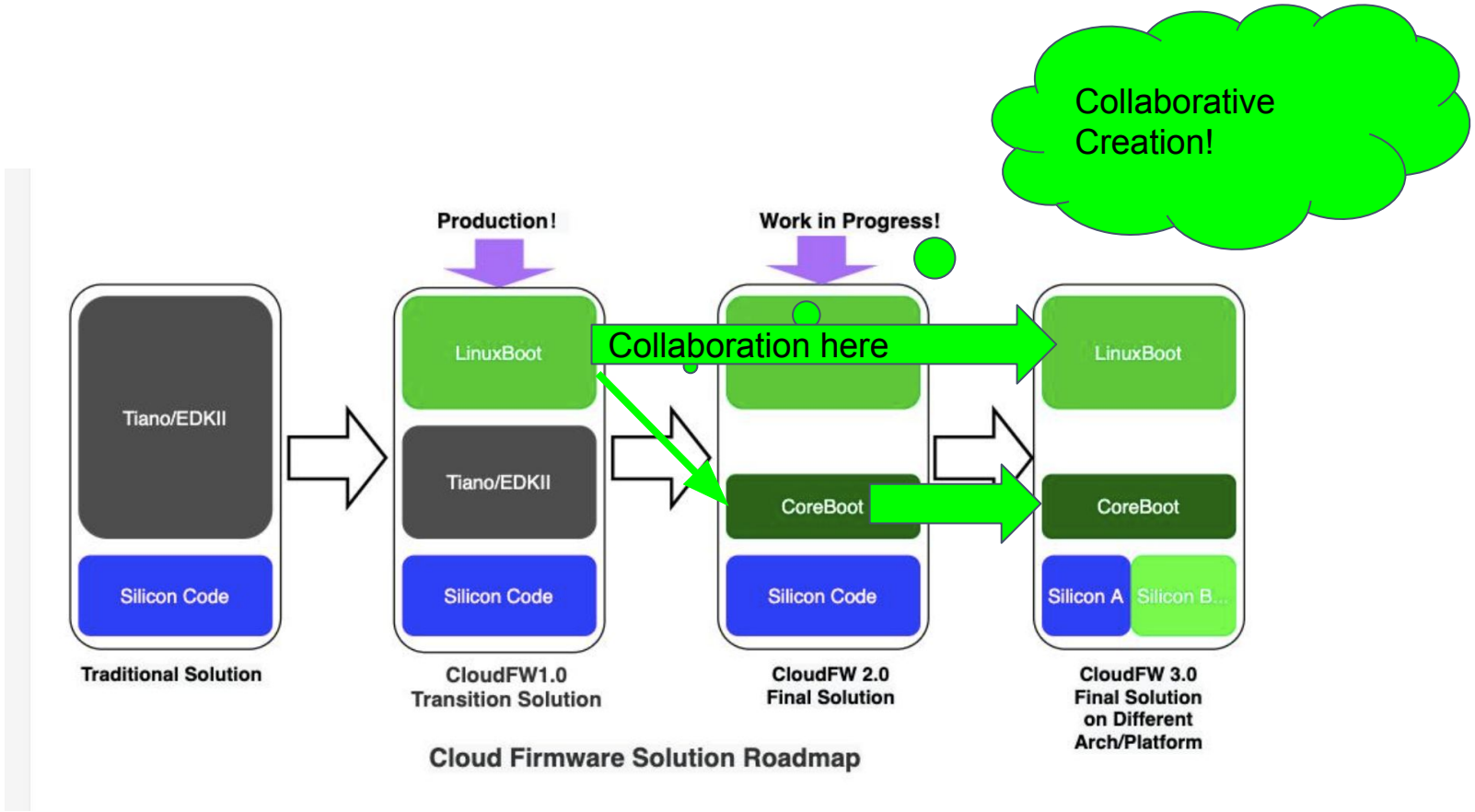
OPEN SYSTEM FIRMWARE

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

***source**: **Cloud Firmware in ByteDance,** 2021 OCP Global Summit*

ByteDance Path: Status (coreboot)



OCP Open System Firmware Project

Enabling collaborative creation

https://www.opencompute.org/projects/open-system-firmware

Owner can modify, build, flash and **share** system firmware.

Publicly redistributable binary blobs are accepted (but not liked!)

“OCP Accepted” badge requires system supporting OSF.

Wiwynn Yosemite v3 (SV7100G4) has been accepted by OCP, and got the “OCP Accepted” badge.

Collaborative creation of coreboot for SPR

- Intel -- foundational software (FSP) on which to build
- Hyperscalers (build coreboot on top of FSP)
  - Meta
  - ByteDance
  - AWS
- ODMs / OEMs
  - Inspur
  - Quanta
  - SuperMicro
  - WiWynn
- Independent Firmware Vendors
  - 9Elements
  - SysPro

- Creating a broad “culture of competence” in coreboot
- Future ports are easier/faster

Call to Action

- open system firmware slack: https://slack.osfw.dev/, linuxboot.org
- coreboot for OCP DeltaLake server based on Intel Xeon Scalable processor:
    - https://github.com/opencomputeproject/OpenSystemFirmware
        - /tree/master/Wiwynn/deltalake
- Coming for 2022:
    - Launch of OCP OSF for Intel SPR-SP based platform
    - Launch of OCP community lab
- Both will foster more collaborative creation