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]


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

### 2019
- **OSF on Mono Lake** (Intel Broadwell-DE)
  - IPMI, SMBIOS, ACPI and board configurations

### 2020
- OSF on Tioga Pass (Intel Skylake-SP) and Delta Lake (Cooperlake-SP)
  - **OCP 2020: Coreboot linuxboot Feature Development for Server Security (CBnT), RAS and performance optimization.**

### 2021
- OSF on Delta Lake
  - OCP OSF Approved, Pre-production readiness
  - Collaboration!
  - CXL memory device support, Target for Production readiness

### 2022
- OSF on Sapphire Rapids-SP

### OCP Server
- **TiogaPass**
- **DeltaLake**
- Next Generation single socket server

### Xeon SP Server Processor
- **SkyLake - SP**
- **CooperLake – SP(6UPI)**
- **SapphireRapids - SP (SPR-SP)**

### FSP Status
- Prototype
- Statement Of Work
- Included in Intel Reference Platform BIOS as platform POR

### Work Duration
- Mar. 2020 - July 2021
- Jan. 2021 on-going

### Test Pass Rate
- 38%
- 95%
- 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.

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

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

source: Cloud Firmware in ByteDance, 2021 OCP Global Summit
ByteDance Path: Status (coreboot)

Collaborative Creation!

Collaboration here
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/](https://slack.osfw.dev/), linuxboot.org
- coreboot for OCP DeltaLake server based on Intel Xeon Scalable processor:
  - [https://github.com/opencomputeproject/OpenSystemFirmware](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