System Firmware

Gives life to the silicon & your system

Goal is to get to the OS – Simple, right?

• Silicon initialization - CPU, DRAM controller, "uncore" logic
• Find and initialize peripherals
• Load target OS
• Provide runtime service availability (e.g. RAS handlers)

Increasing complexity over the years

• Drivers, networking, crypto, application support
• Millions of lines of code
• System firmware has become an OS
Where does System Firmware reside?

Control Plane
- Rack Manager FW
- NW Switch FW
- Storage Appliance FW

Data Plane
- Server FW
- BMC FW
- BIOS FW
- IO FW
- SSD FW
- PSU FW
- nVME FW
- SMM
- DXE
- Secure Boot
- Silicon Ref Code
- PEI
This has created a few problems...

Complex and important part of the software stack

Runs at highest level of privilege

Must integrate into company’s SW architecture

Very few engineers looking at it?
  • Much of it has remained stubbornly closed
  • Not many people trained to work on this code
  • Must support multiple generations,
    • otherwise creates obsolescence

Real Problem for companies with lots of Hardware
Opportunity leads to OSF

2016: Talks began for an open source firmware effort

Goals were laid out to enable:

- Innovations and customizations in the system firmware stack
- Closer collaboration with suppliers/vendors
- Better error handling, diagnostics, remediations
- Continuous integration and testing
- Auditable and traceable code, integration with authentication devices.
- Coordination with firmware for ASICs, BMCs, rack management, etc.
- Open tooling, Faster deployment
Mission: Develop an open source philosophy based ‘system firmware’ modules, to support different OS and different CPU silicon vendors.

Companies Contributing to OSF development: Intel, Microsoft, Google, Facebook, Lenovo, Two Sigma, Horizon, 9 Elements, Cavium, AMD, IBM, etc.

Work Streams: Open EDKII DXE core, Linux Boot, Core Boot, Intel FSP, AMD AGESA, ARM boot code, HW platform module, Build tools, Automated test support, HW requirements, etc.

GitHub Repositories Collateral link: https://github.com/opencomputeproject/OSF

Bi-weekly OSF discussions: Architectural reviews, workstream progress, agenda setting and other collaborative discussions on OSF development.
Current State of BIOS FW(initialization)

- Developer’s Kit will be available from Wiwynn
- LinuxBoot approach had working hardware at OCP Summit in March
- Facebook and Intel have a EDK II POC using Open Rack sled
- Demo planned for OCP Regional Summit in Amsterdam
- September 26th – Announcement Planned regarding OSF
Rack Manager Data Traffic Interfaces

openRMC Rack Manager

Fabric bound
- REDFISH
- SWORDFISH
- SSH
- Legacy REST
- Web GUI

Device bound
- REDFISH
- SWORDFISH
- SSH
- IPMI
- I2C
Integrated w/ Power Shelf

Server
Server
Server
Server
Server
Server

Rack Boundary

Switch

Power Shelf w/ RMC FW

Server
Server
Server
Server
Server
Server

Server
Server

Integrated w/Switch

Server
Server
Server
Server
Server
Server

Switch w/ RMC FW

Rack Boundary

Stand Alone

Server
Server
Server
Server
Server
Server

Server
Server

Rack Boundary

Switch

Rack Manager

Integrated w/Switch

Server
Server
Server
Server
Server
Server

Power Shelf w/ RMC FW

Server
Server

Server
Server

Current State of RMC FW

- Repo: https://github.com/opencomputeproject/Rack-Manager
- Developer’s Kit will be available from Wiwynn
- LinuxBoot approach had working hardware at OCP Summit in March
- Microsoft, Inspur, and Intel have made code contributions
- Demo planned for OCP Regional Summit in Amsterdam
Orchestration Software

Control Plane
- Rack Manager FW
- NW Switch FW
- Storage Appliance FW

Data Plane
- Server FW

Sub-systems:
- BMC FW
- BIOS FW
- IO FW
- SSD FW
- PSU FW
- nVME FW

- SMM
- DXE
- Secure Boot
- Silicon Ref Code
- PEI
OCP HW Management Strategy

Describe → Prescribe → Test → OCP Recognized Products

- OCP Redfish Profiles
- Redfish Interop Validator
- OCP Recognized Products

OCP Strategy: Redfish/Swordfish API’s for HW Management FW
End Goal: A Secure, maintainable platform with API’s to keep pace with open source software needs.

Open Source:
BMC, BIOS, Rack Resources across all the IT equipment
Thank You

Follow Up Links: opencompute.org