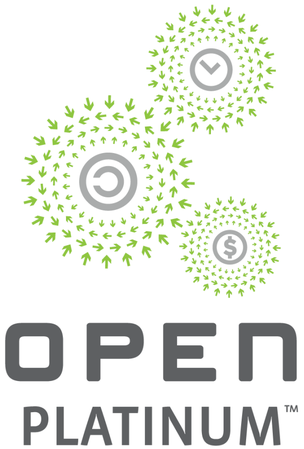

Open. Together.
OCP
SUMMIT

OSF/Security

Improving Cloud System Uptime with Runtime Firmware Update and Activation

Murugasamy (Sammy) Nachimuthu
Sr. Principal Engineer, Intel Corporation

Mallik Bulusu
Principal Firmware Engineering Manager
Microsoft Corporation

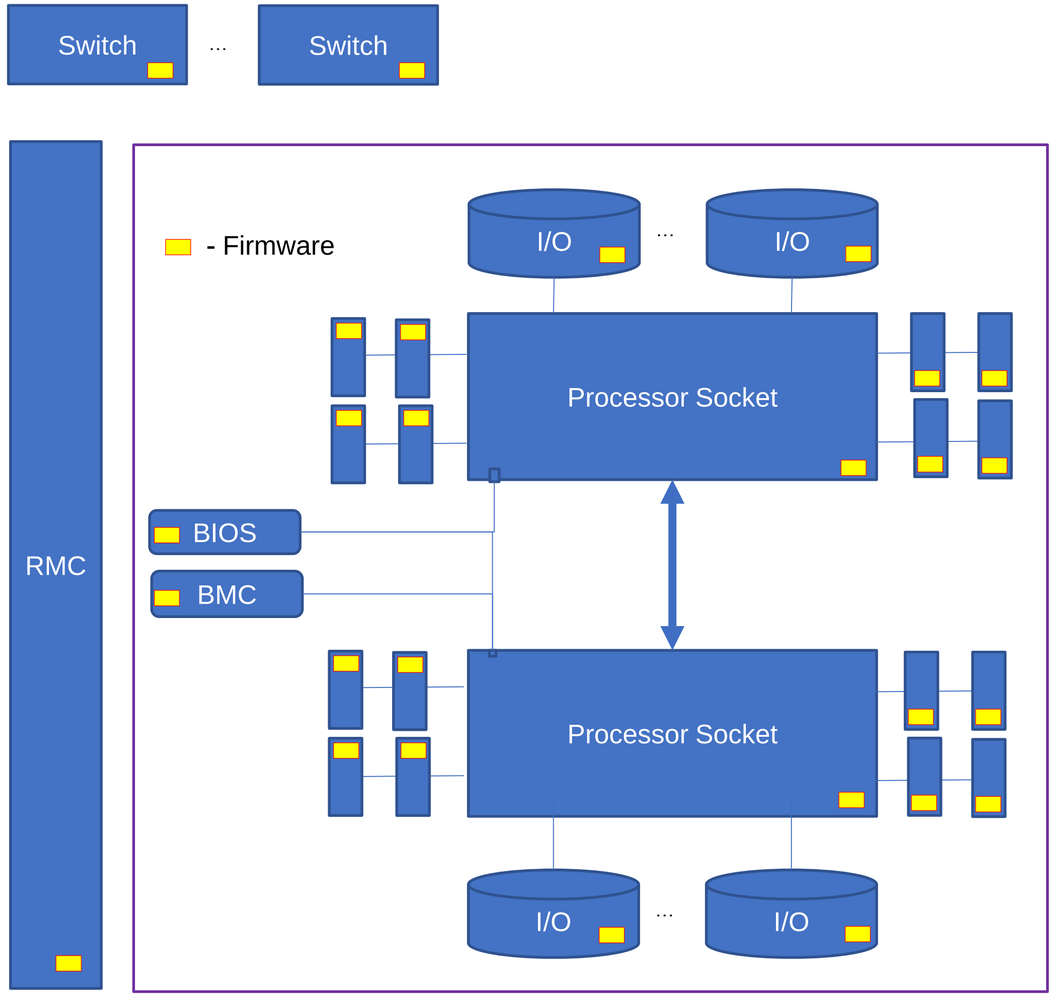


Cloud Demands High Service Availability

System reboot affects the service availability

Cloud Demands High Service Availability (cont…)

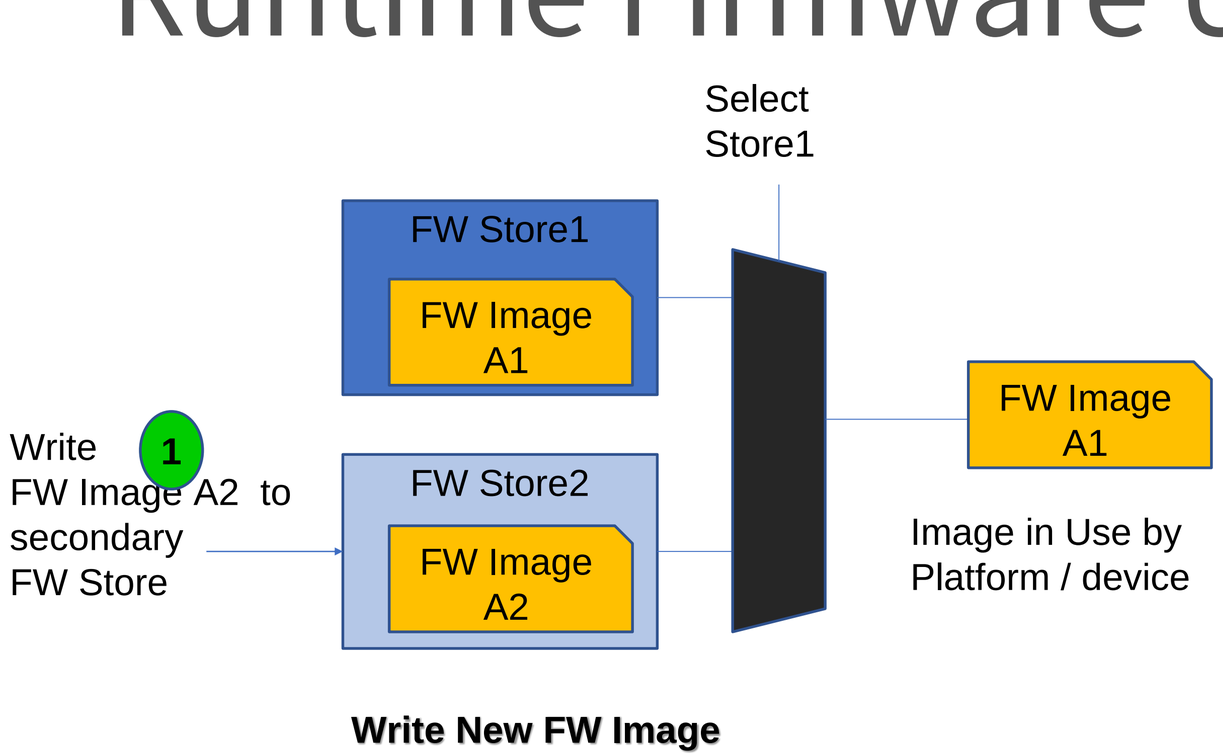
- Today's OCP system contains many hardware components with firmware
  - System Firmware – BIOS, BMC, etc.
  - Device Firmware – Microcode, Network, TPM, Storage, SCM, Custom FPGA, PSU etc.
- Over life time of the system, the firmware components are updated to address:
  - Security, Power, Performance, debug, bug fixes, fleet freshness, fleet hygiene, etc.
- In most cases, system is rebooted to activate new firmware



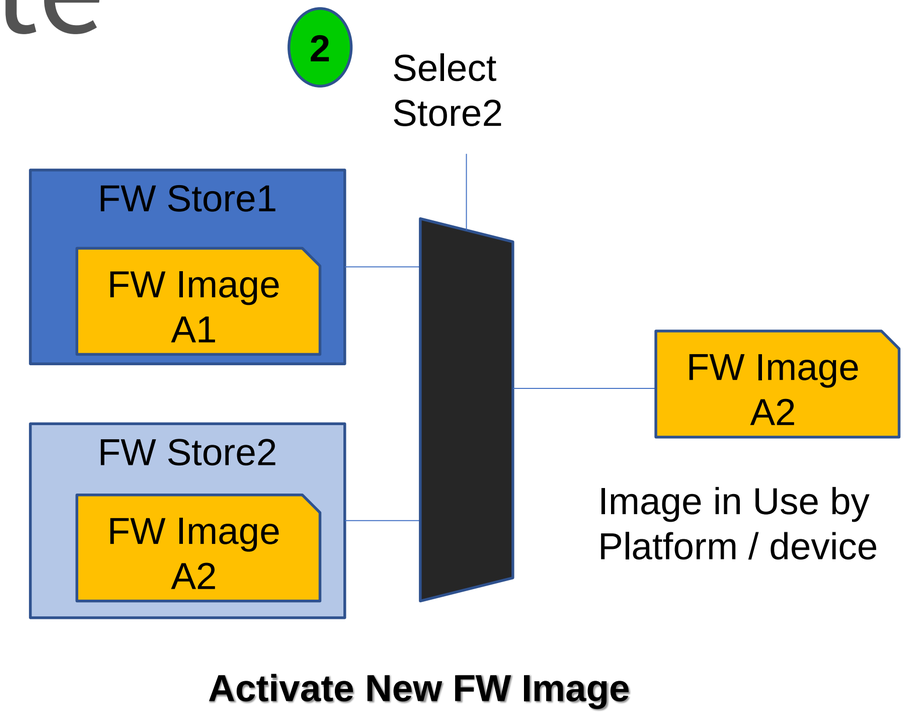
Key Aspects to Cloud Firmware Updates

- Supply Chain Integrity
- Ease of Deployment at Scale
- Impactless Updates
- Automatic Recovery / Rollback
- Audit Trails
- Root of Trust
- Low Boot Time
- Configuration / Policy Management

Runtime Firmware Update



Write New FW Image



Activate New FW Image

Typically, do not overwrite in-use copy of firmware – for high availability, ease of firmware update and security reasons

Two step process consisting of writing new FW image to secondary store and then activating it (making it the primary)

Firmware update copy can be written at runtime but activation requires a System Reset

Gaps in Runtime Firmware Activation

- Firmware is delivered as monolithic package today
- Lack of Platform, OS primitives for runtime activation
- Runtime attestation capabilities

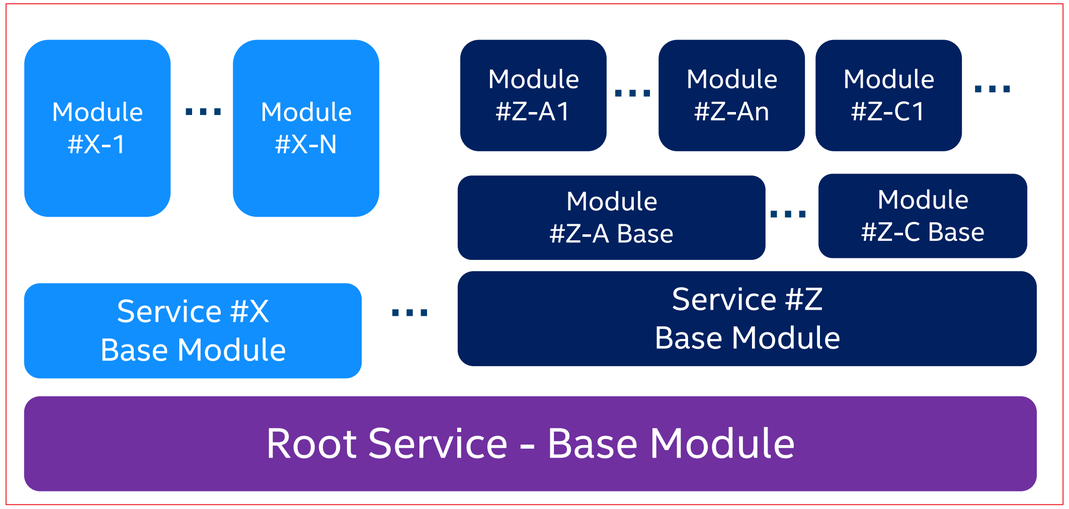
OCP System Firmware Project and OCP Security Project well scoped to solve …

Modular FW

Monolithic FW

Independently updateable
≠ Independently activated

Independently updateable module & activation hierarchy

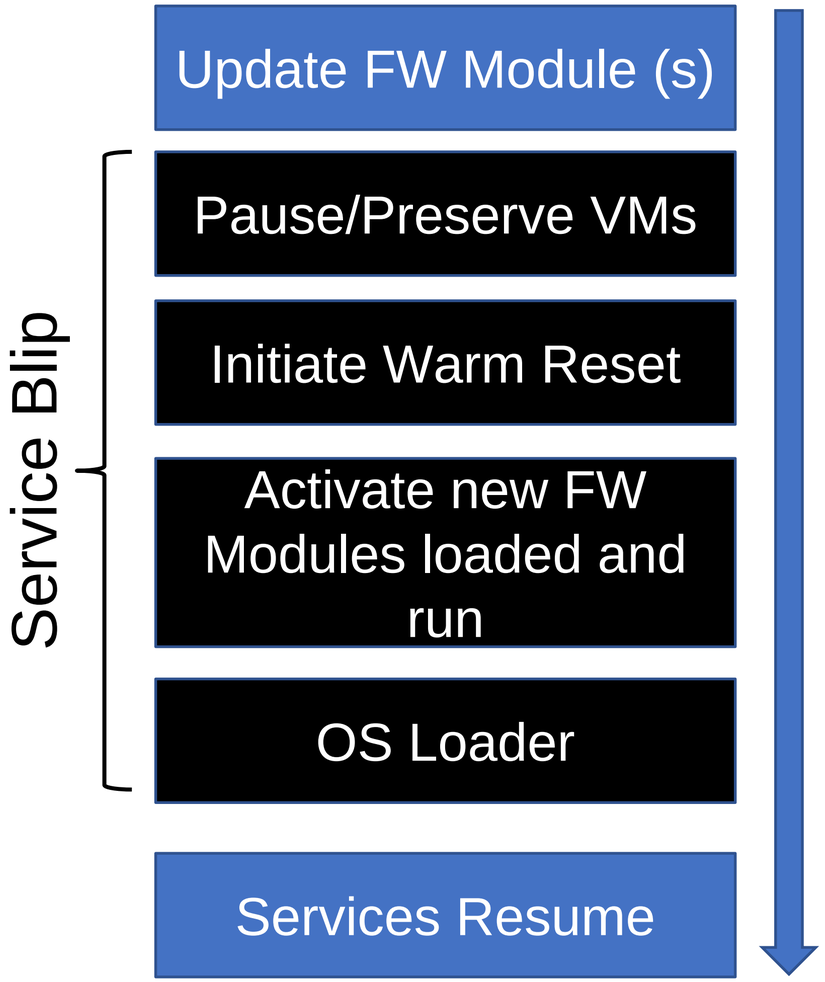


Design Considerations:

- Modularity as a means for nimble firmware updates
- Module Authentication
- Auditing & Versioning

Ideally, Modules should be designed for independent update and activation

Runtime Firmware Activation Flow



- OS Constructs for Runtime Updates
  - Unix/Linux – kexec
  - Windows – Memory Preserving Maintenance
- Firmware Activation Mechanics
  - Pause/Preserve VMs
  - Invoke Modified Reset flow
  - Activate new FW Modules
  - Load OS (memory contents still valid)
  - Resume services

Runtime Firmware Activation Security

- Need runtime attestation as part of Security Project
- Cerberus provides RoT and attestation
- New firmware additions are added to the Platform Firmware Manifest (PFM) and reported as Platform Active RoT (PA-ROT)

Summary & Call to Action

OCP's Open System Firmware project aims to address specifications for OCP firmware needs.

OCP System Firmware and Security Project Collaboration for runtime attestation

OCP systems are used in cloud that require high service availability.

Drive the OS changes through partnership

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

https://www.opencompute.org/projects/security

https://www.uefi.org

https://www.openbmc.org

https://www.dmtf.org/


Open. Together.
OCP Global Summit | March 14–15, 2019
OCP
SUMMIT