Contribution ID: **62** Type: **not specified**

System Firmware and Device Firmware Updates using Unified Extensible Firmware Interface (UEFI) Capsules

Thursday, 27 August 2020 07:35 (20 minutes)

Firmware is responsible for low-level platform initialization, establishing root-of-trust, and loading the operating system (OS). Signed UEFI Capsules define an OS-agnostic process for verified firmware updates, utilizing the root-of-trust established by firmware. The open source FmpDevicePkg in TianoCore provides a simple method to update system firmware images and device firmware images using UEFI Capsules and the Firmware Management Protocol (FMP).

This session describes the EFI Development Kit II (EDK II) capsule implementation, implementing FMP using FmpDevicePkg, creating Signed UEFI Capsules using open source tools, and an update workflow based on the Linux Vendor Firmware Service (fwupd.org).

I agree to abide by the anti-harassment policy

I agree

Primary author: HSIUNG, Harry (Intel)

Presenter: HSIUNG, Harry (Intel)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC