presented by

Challenges, Solutions and Benefits of Integrating Wireless Drivers in UEFI Firmware

UEFI 2024 Webinar Series

March 13, 2024

Hemanth Venkatesh Murthy

Meet the Presenter

Hemanth Venkatesh Murthy
Software Senior Principal Engineer
Dell Technologies

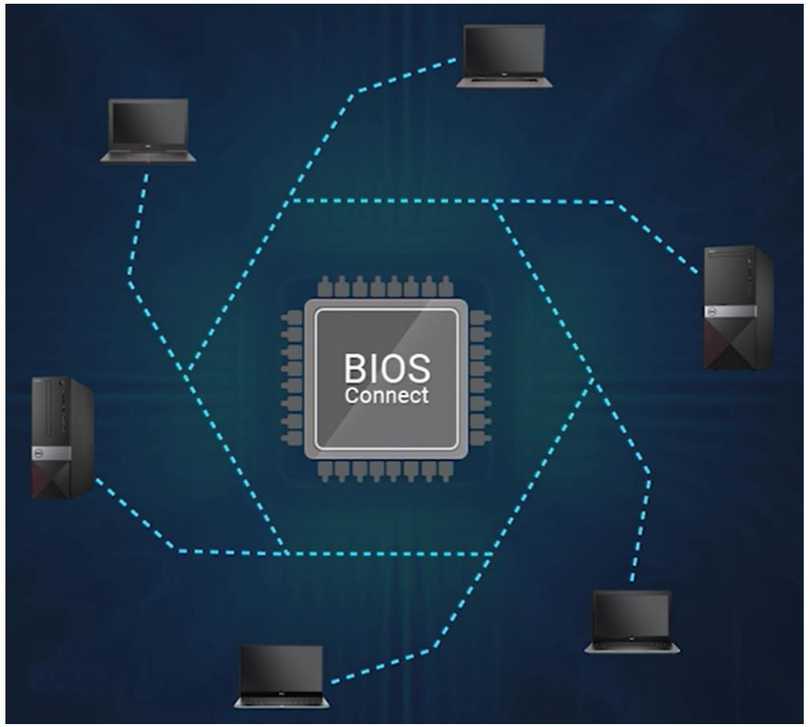
25+ years of experience working on embedded software stacks. Member of Dell Technologies Client BIOS & Firmware Architecture team with focus on Connectivity use cases.

Agenda

- Introduction
- Need for Wireless in BIOS
- BIOS FW Challenges
- Solutions

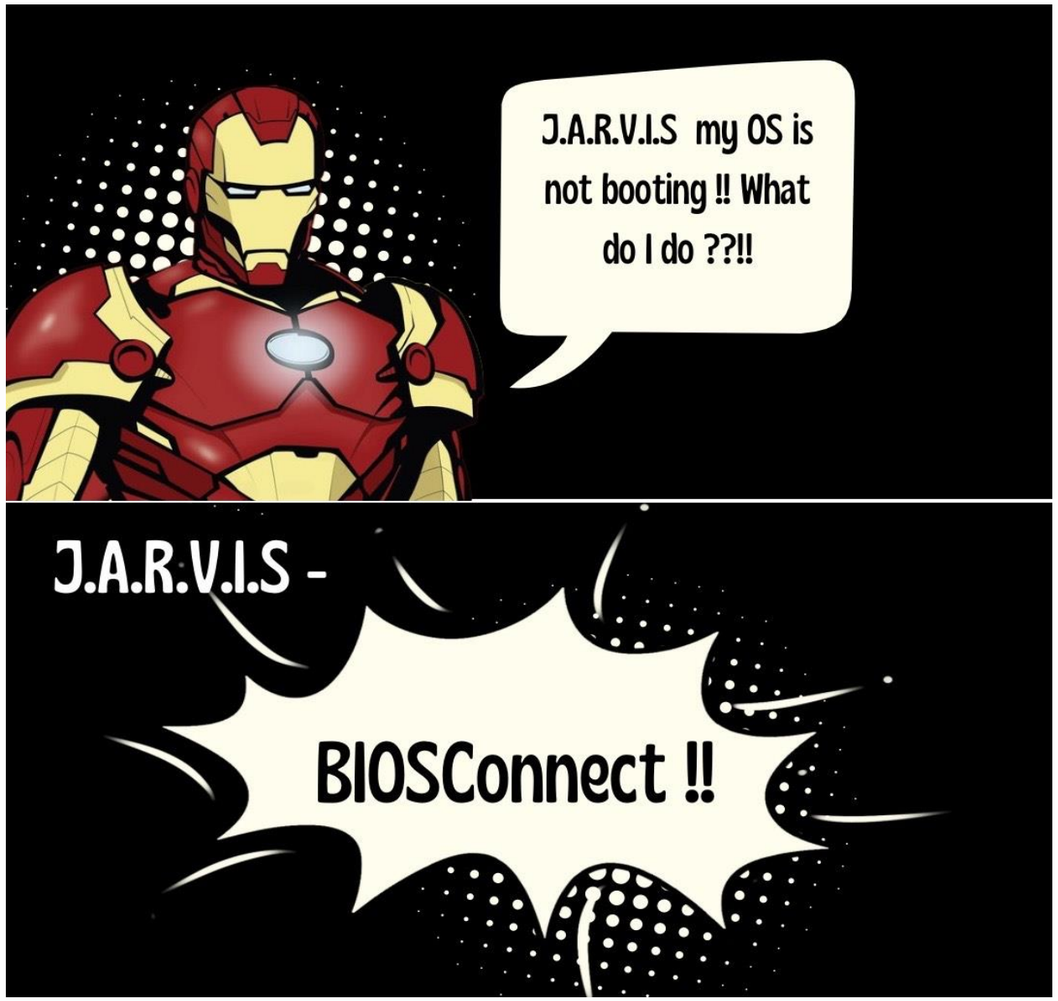
Introduction

- UEFI Firmware
  - Part of BIOS
  - Initialization of the system
- BIOS
  - Dedicated Flash device
  - Independent of Storage drive
  - Capable of initializing the system even if storage drive is not present
- Talk focusses on utilizing BIOS capabilities for improving serviceability



Bare Metal Operating System (OS) Recovery

- OS Recovery Scenarios
  - Corrupted OS
  - Malware infection
  - Storage Drive Replaced
  - Motherboard Replaced
  - Remote IT Admin
- Above scenarios BIOS is unaffected
- BIOS can be used to recover OS by downloading from Internet
- Wi-Fi is the preferred connectivity option

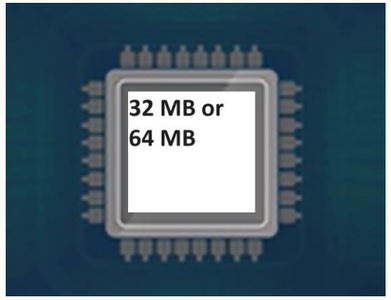


Bare Metal Firmware Update

- Firmware Update Scenarios
  - Motherboard replaced in field
  - Manufacturing process in factory
  - OS agnostic firmware update for users

Storage Space Challenges

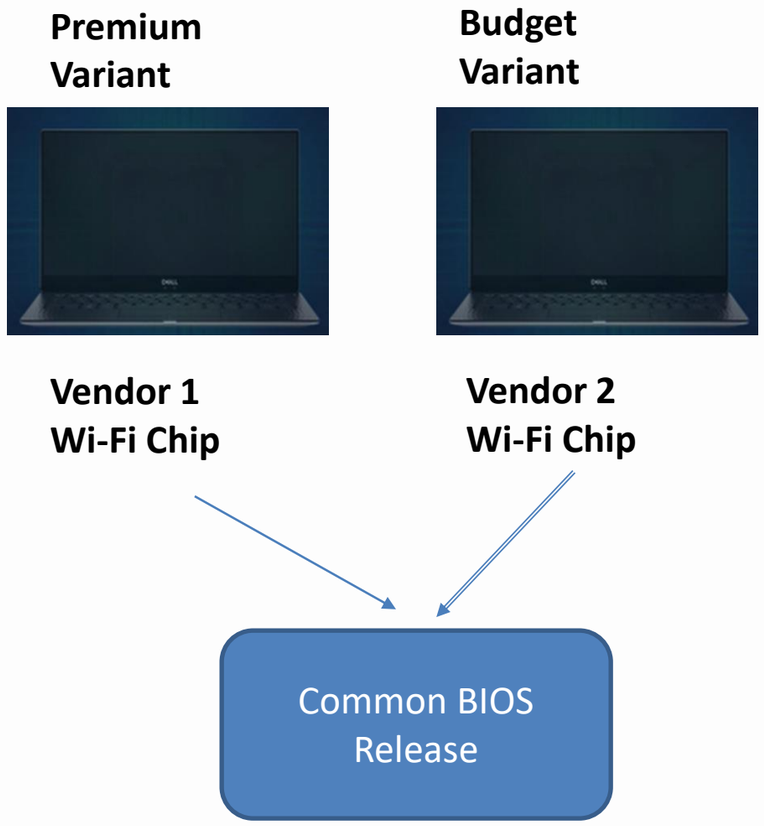
- Platforms support
  - 32 MB or 64MB Flash Chip
- Wireless Components
  - SNP DXE Driver
  - Supplicant DXE Driver
  - Firmware
  - Rest of Network stack part of EDK II
- Features & Typical size
  - WPA3 and Wi-Fi 6/6E
  - Personal & Enterprise Network Support
  - ~1.5 – 2.5 MB uncompressed
  - Business Logic for OS Recovery and Firmware-Over-The-Air (FOTA)



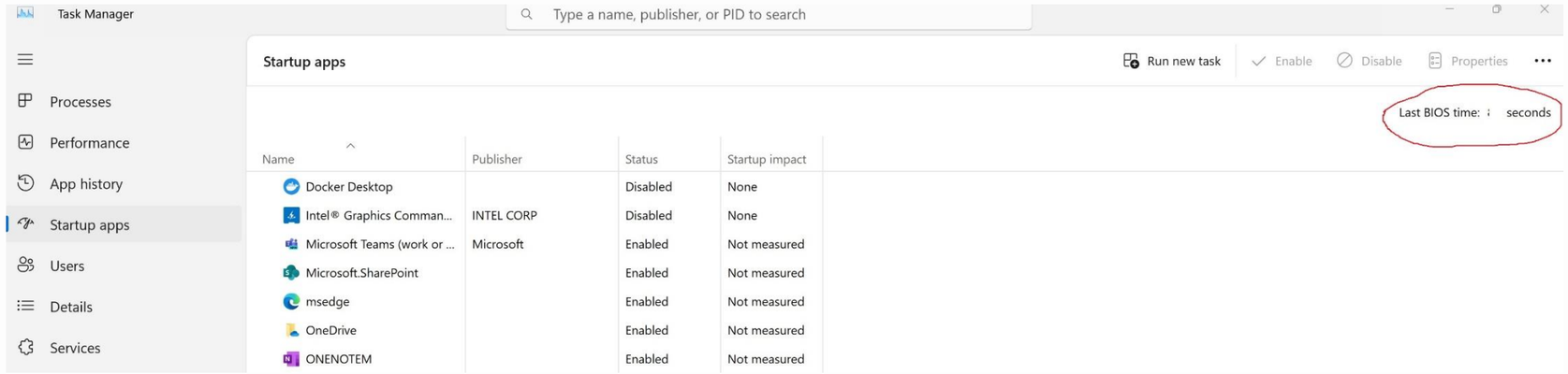

```
09-01-2024  01:07 PM          459,864 IntelFmacDxe.efi
09-01-2024  01:07 PM          549,148 IntelFW.bin
09-01-2024  01:07 PM          117,848 IntelSupplicantDxe.efi
09-01-2024  01:07 PM        1,329,810 QcaFW.bin
09-01-2024  01:07 PM          280,952 QcaWifiDxe.efi
09-01-2024  01:07 PM        1,051,736 QcaWlanSupplicantDxe.efi
```

Platform Variant Challenges

- Typically, platform variants share same BIOS
- There could be multiple variants of a particular platform that support different vendor chipsets
- In such scenarios multiple Wi-Fi Drivers need to be integrated into BIOS



Boot Time Impact Challenges

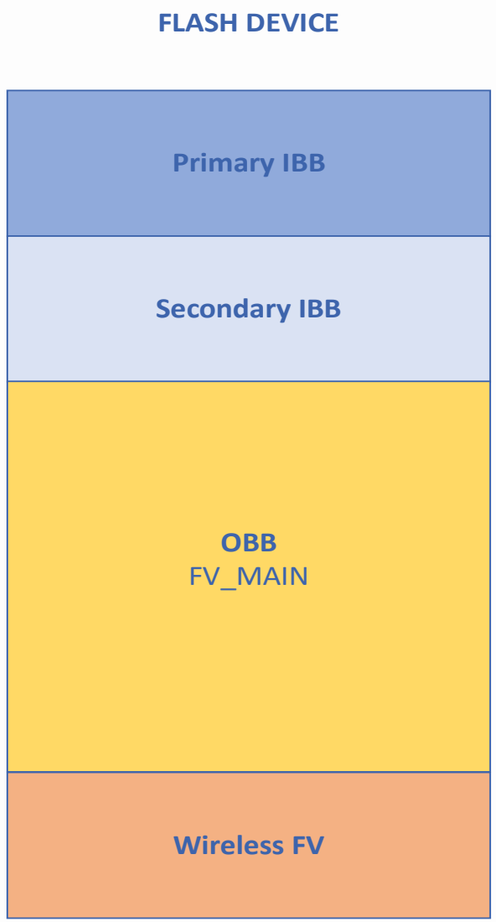


- Expectation is to have minimum BIOS Boot time
- Only components required for normal boot to be loaded and initialized
- Wi-Fi Controller initialization not required in UEFI during normal boot process

Security Challenges

- BIOS is root of trust for the system
- If BIOS is compromised, whole system could be compromised
- Wi-Fi connectivity should not become target for backdoor attacks

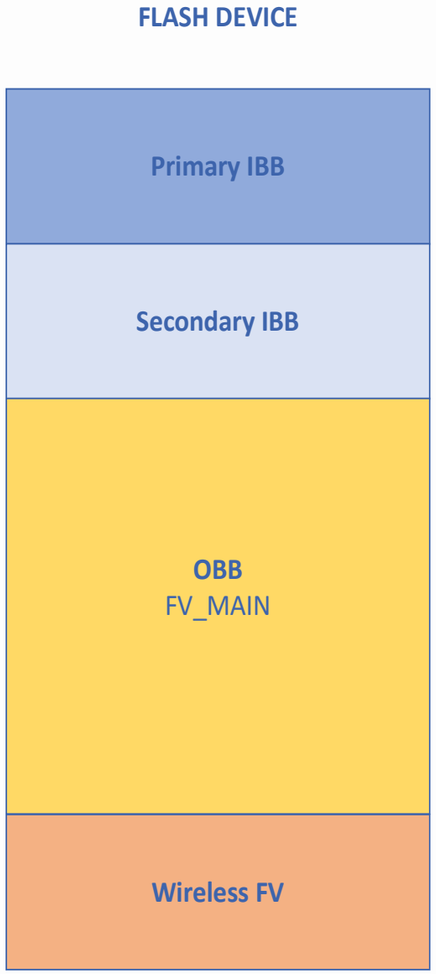
Separate Wireless Region

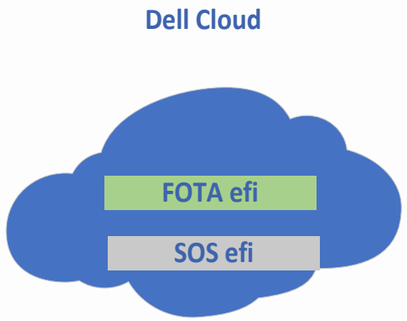


- BIOS flash map layout shown
- FV_MAIN
  - DXE Drivers
  - Dispatched during normal boot
- Wireless FV
  - Wireless Drivers
  - Not Dispatched during normal boot
  - Only Dispatched during Recovery or FW update
  - Optimizes boot time

Cloud BIOS

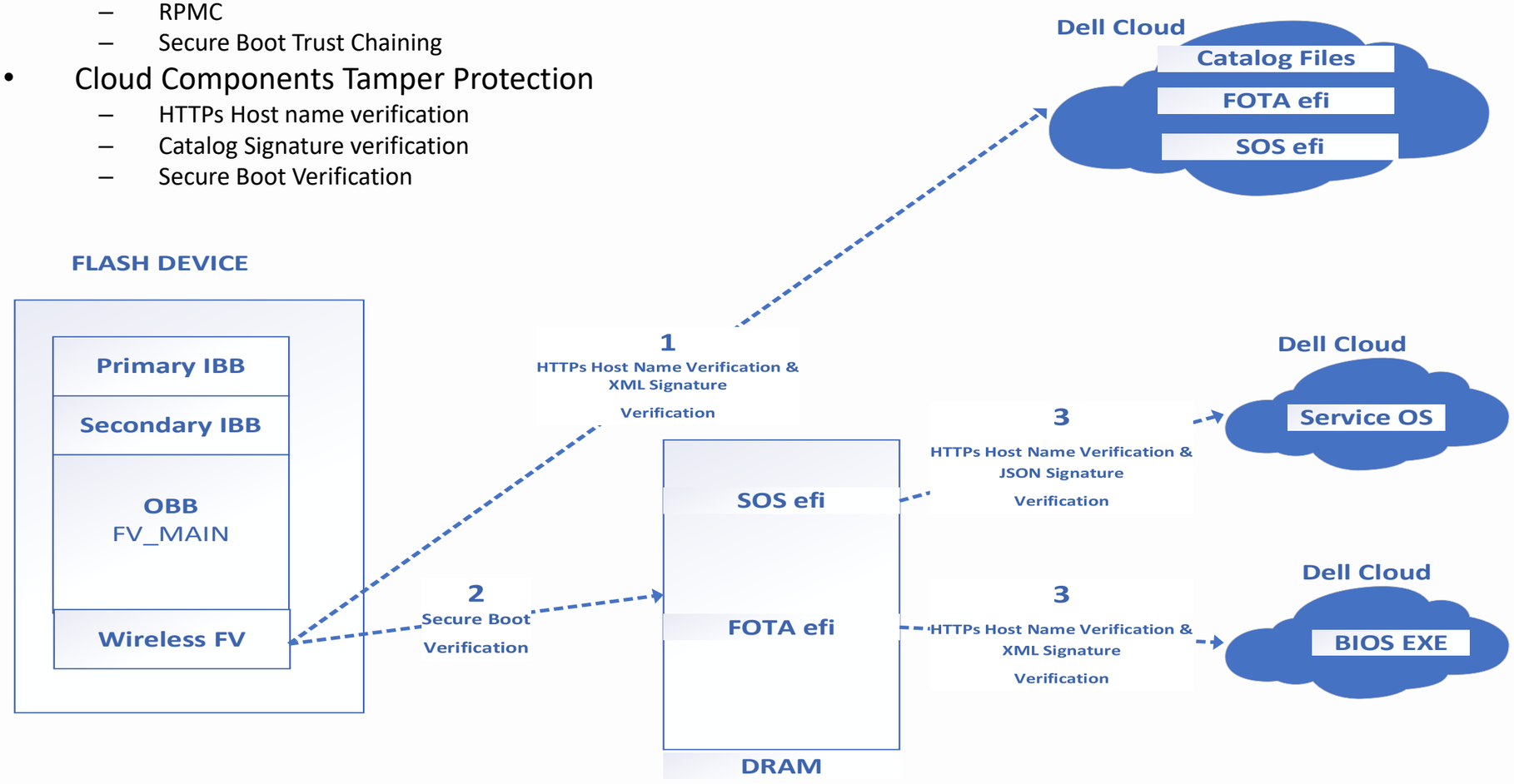
- Split BIOS
  - Flash Components
  - Cloud Components
- UEFI Applications for OS Recovery & FOTA
  - Not required during normal Boot
  - Hosted on Cloud
  - Downloaded and executed during OS Recovery & FW update
- Network Connectivity Drivers
  - Integrated in Flash Device
- Storage Space & Boot time Optimization
- Easy and quick upgrade for UEFI Application
  - Does not require BIOS update on the system





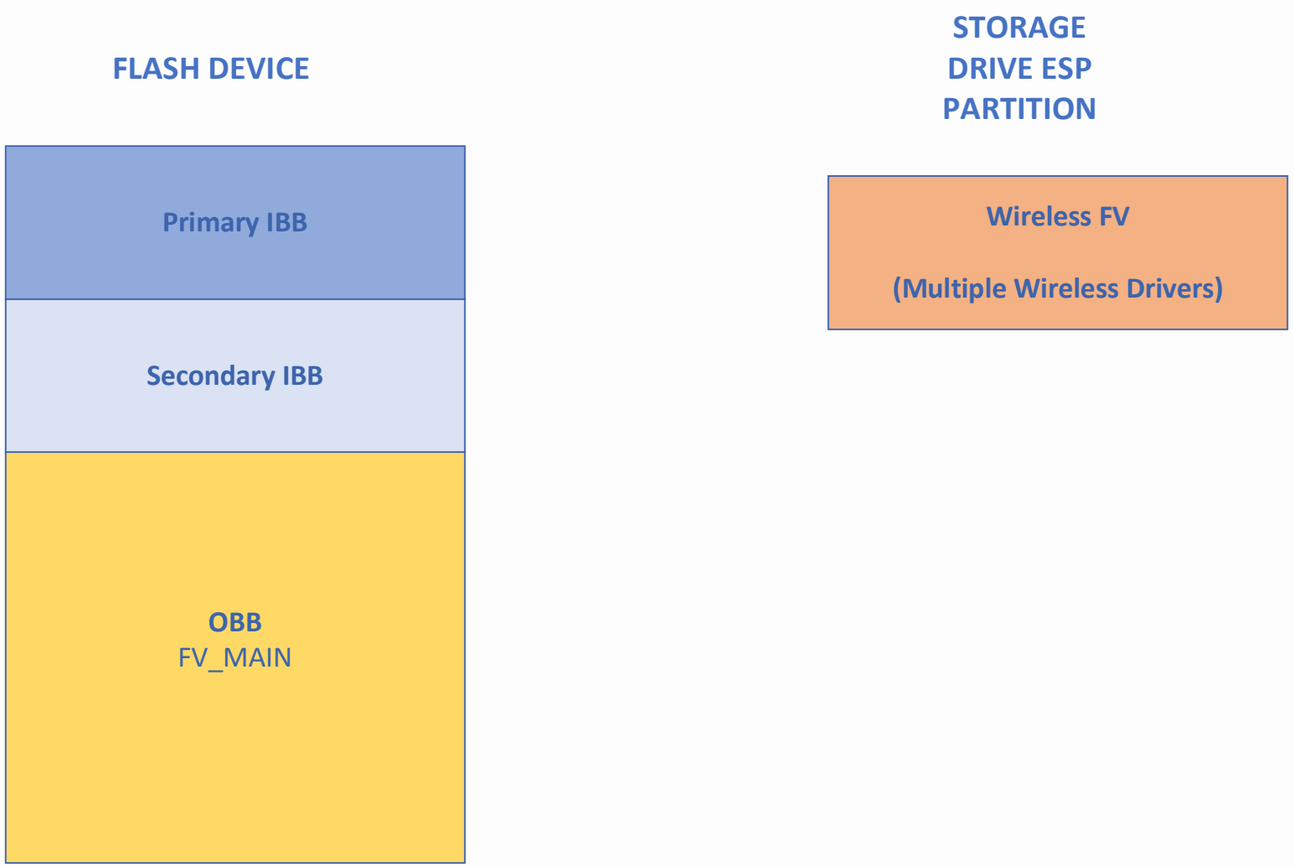
Cloud BIOS Security

- Flash Device Tamper Protection
  - Intel BIOS Guard
  - RPMC
  - Secure Boot Trust Chaining
- Cloud Components Tamper Protection
  - HTTPs Host name verification
  - Catalog Signature verification
  - Secure Boot Verification



Wireless Drivers in ESP

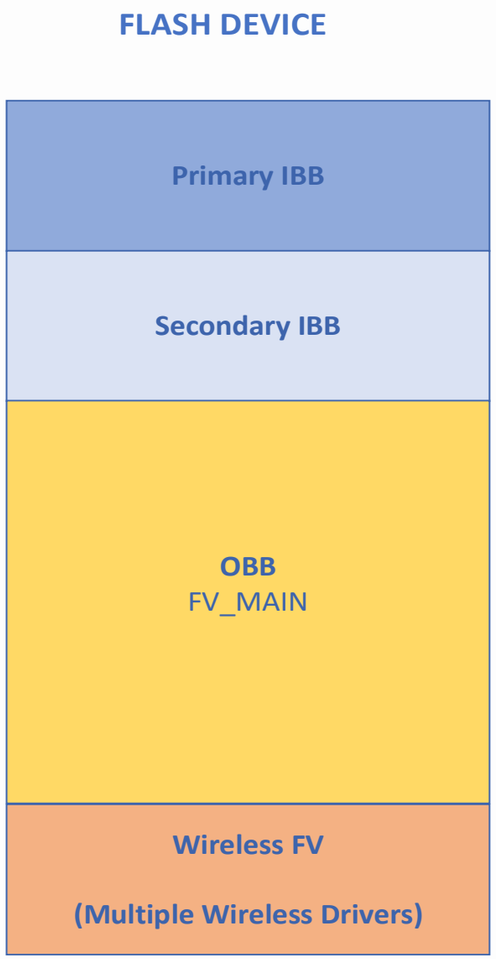
- Wireless Drivers hosted in Encapsulating Security Payload (ESP)
  - Security verification
  - Loaded and dispatched on demand
- Pros Vs Cons
  - Lower SPI Flash size
  - All required drivers are compiled into the image on ESP
  - Wireless feature not available when Storage Drive replaced
  - Wireless feature not available when Storage Drive is fully formatted & re-imaged



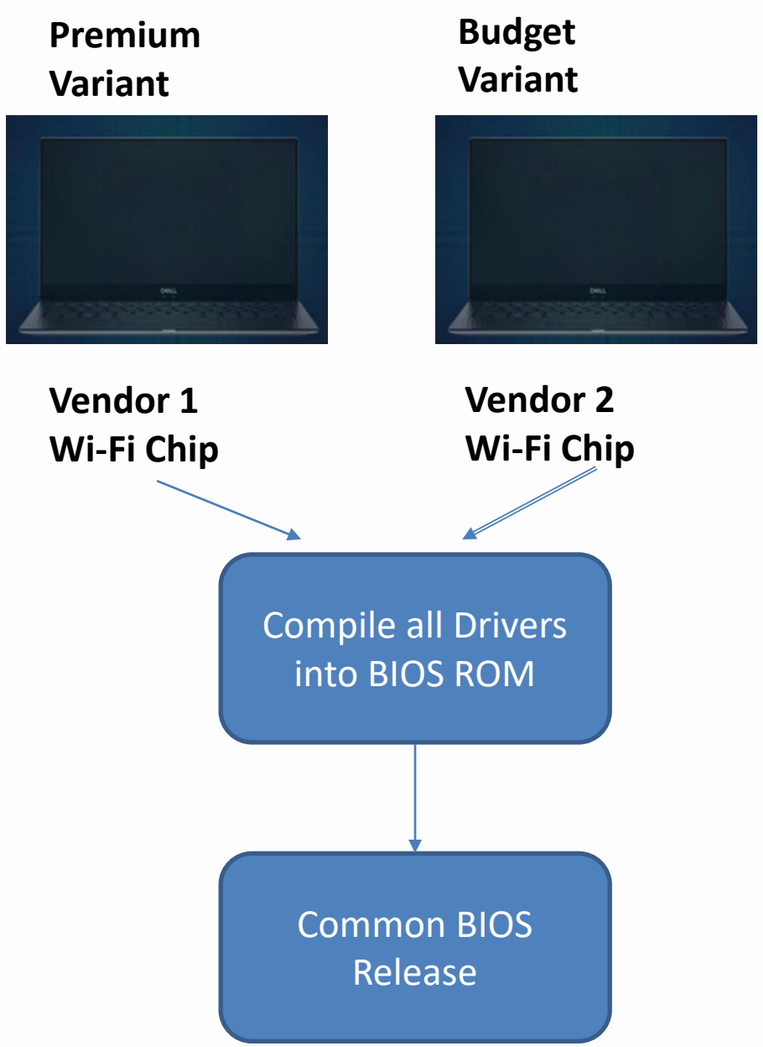
Wireless Drivers in Flash

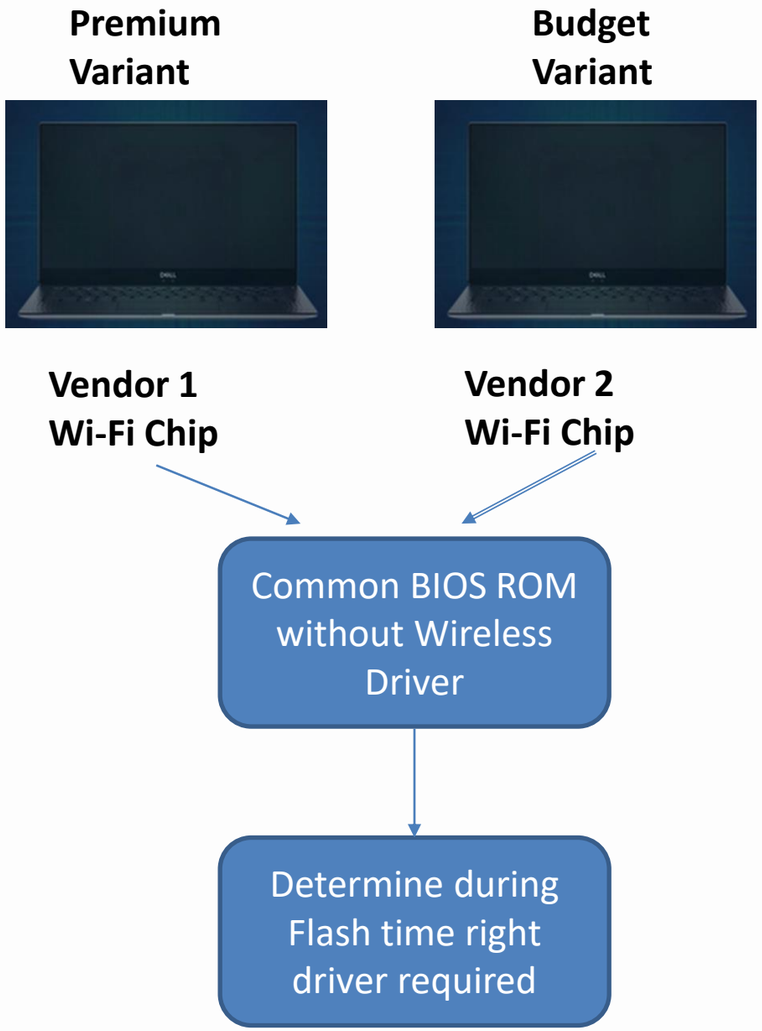
- Wireless Drivers embedded in Flash Device
  - Multiple Drivers embedded as required for the platform BIOS

- Pros Vs Cons
  - All required drivers are compiled into the BIOS image and flashed
  - Wireless feature are available when Storage Drive replaced or re-imaged
  - Larger Flash Drive requirement since multiple drivers need to be embedded
  - For any new feature to be added like UEFI BLE Support, the storage size requirement gets compounded

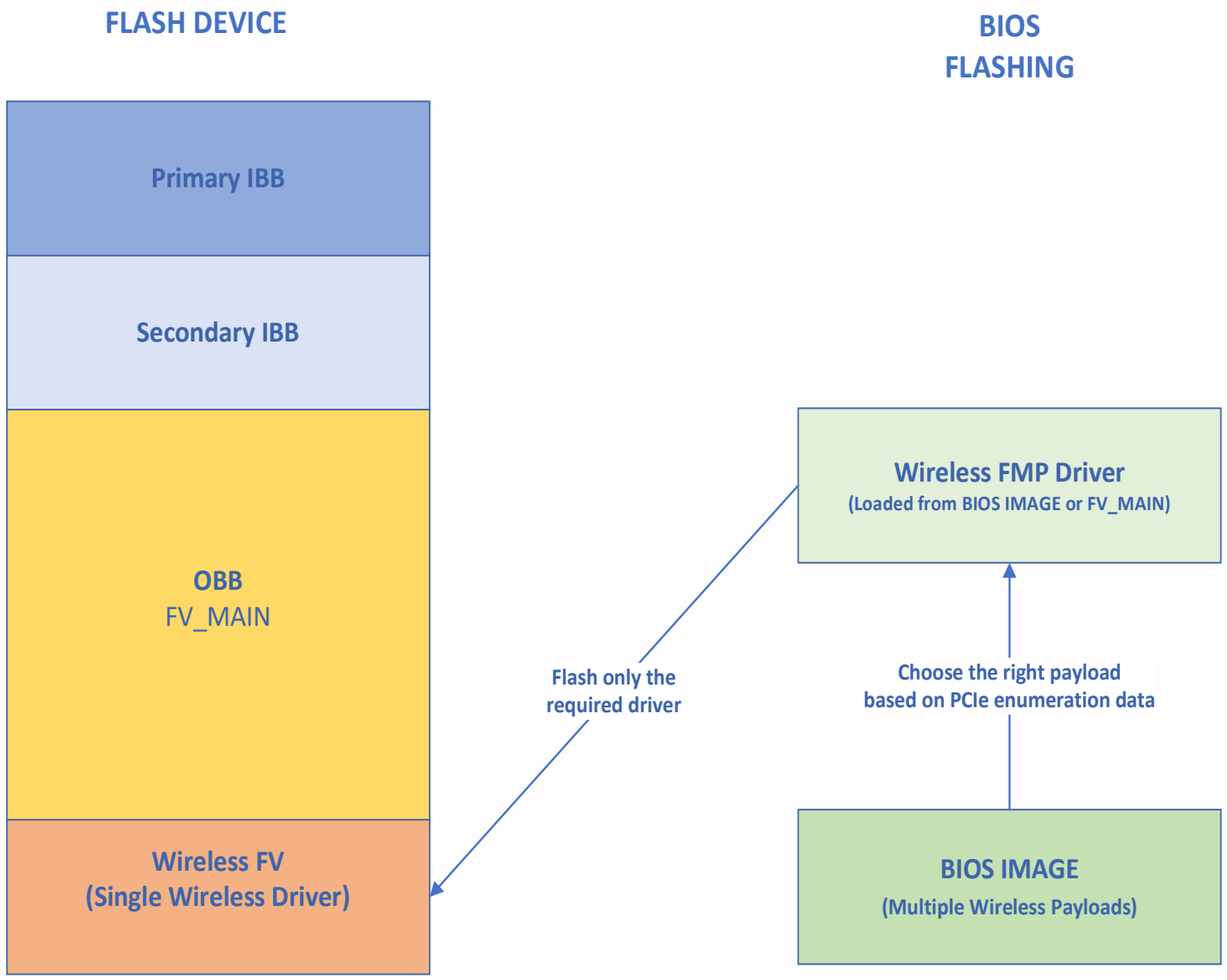


Applying Lazy Algorithm



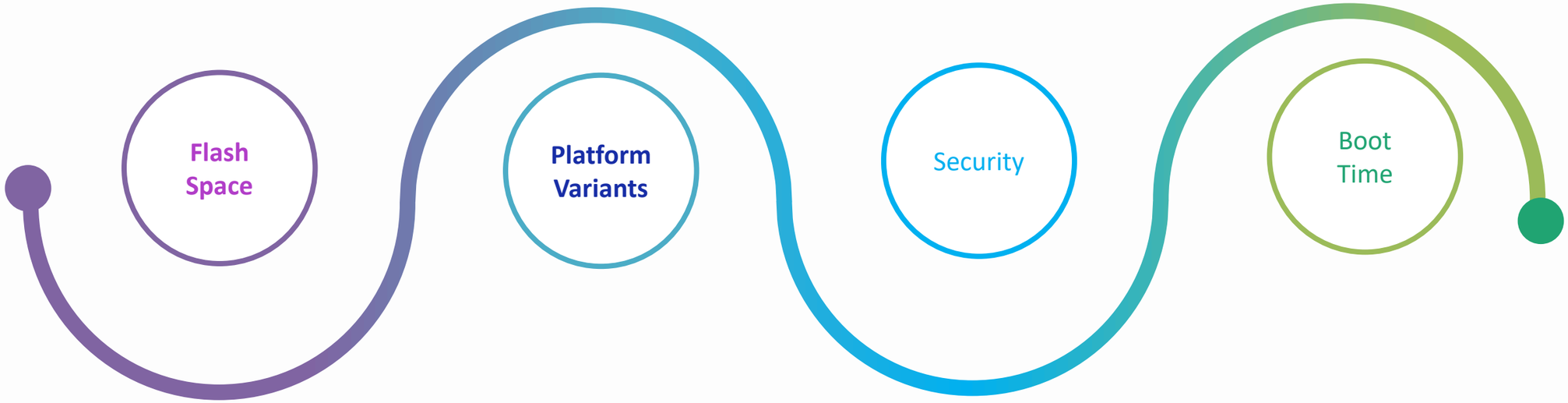


Applying Lazy Algorithm



- Delaying the decision to Flashing time from compile time
  - Wireless FMP Driver can determine the Wi-Fi chipset installed using PCIe enumeration data
  - Wireless FMP Driver Flashes only the required driver
  - Can include Both Wi-Fi & BLE UEFI Drivers
  - Satisfies Bare Metal recovery requirements
- Factory Process Updated
  - Manufacturing Process updated to Flash Wireless Drivers during production
  - All systems coming out of factory will have the right wireless driver in FV Region

Challenges & Solutions: Summary



Flash Space

- Cloud BIOS
- Lazy Algorithm

Platform Variants

- Separate Wireless Region
- Lazy Algorithm

Security

- Flash Tamper Protection
- Cloud Tamper Protection

Boot Time

- Cloud BIOS
- Separate Wireless Region

Questions?

Thanks for attending a UEFI Forum 2024 Webinar

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by