Capsule update with MM

Fall 2018 UEFI Plugfest
October 15 – 19, 2018
Presented by:
Meenakshi Agrawal (NXP Semiconductor)
Udit Kumar (NXP Semiconductor)
Agenda

• Introduction
• Arm® boot flow
• Capsule Structure
• Updating capsule with MM
• Advantage
• Questions
Introduction

• Why we need capsule update
  – New features
  – Bug fixes
• How to update firmware
  – OS
  – UEFI Runtime
  – Some Service processor
• Thing to take care
  – Security
  – Reliability
Arm Boot flow

Who should own the flash BL3 runtime or UEFI
- BLx is also stored on flash
- Security ??
MM mode

Can secure side of UEFI own flash driver ???
Arm : Set Variable

MM Communication Head
- Header GUID
  - Message Length
- Variable Communication Head
  - Function Id
  - Return Status
- VarAccess Comm Data
  - GUID
  - Data Size
  - Name Size
  - Attributes
  - Name []
  - Data []

Normal World
- EL0
  - Guest App1
- EL1
  - Linux Kernel A
  - Linux Kernel B

Secure World
- Secure Partition
  - Variable access
- TBB BL2
  - S-EL0
  - S-EL1

UEFI FIRMWARE – BL33
- Arm MM Interface
- Arm Trusted Firmware – BL31

Crypto service
- Secure Partition Manager
- TBB BL1
  - S-EL1

Secured world
- MM handler
- MM SetVariable ()

FVB Protocol
- ROTPK
  - SHA-256

Flash Driver#
- I2C driver#
Capsule Structure
How to build capsule

FmpPayloadSystemFirmwarePkcs7 # gEfiFmpCapsuleGuid

FmpPayload.FmpPayloadSystemFirmwarePkcs7
CERTIFICATE : # PKCS7
# PcdSystemFmpCapsuleImageTypeIdGuid##

F/W data : FILE_RAW # PcdEdkiiSystemFirmwareFileGuid
Driver (SystemFirmwareUpdateDxe.inf) # gEdkiiSystemFmpCapsuleDriverFvFileGuid

UEFI FIP Image, Signed with ARM cert_create tool
Traditional Update flow

1. CheckCapsuleUpdate()
   - PlatformPei
   - Coalesce()
   - CreateState()
   - MrcWrapper

2. CAPSULE_PPI
   - EFI_HOB
   - UEFI CAPSULE

3. ProcessCapsules()
   - DxeCapsuleLib

0. UpdateCapsule
   - OS
   - Capsule RuntimeDxe
   - ResetSystem RuntimeDxe
Traditional Update flow

0. Install
1. Locate & SetImage()
2. Parse & Verify
3. Dispatch()
4. PassThru
5. Parse & Verify
6. Update

SysFirmReport.efi in BIOS
CapsuleLib in BIOS
FMP capsule
Payload
SysFirmUpdate.efi in FMP capsule
Flash
Few rules/OEM specific

- Flash Storage should accommodate two copies of firmware
- One latest copy and another copy for fallback
- BL2 Image should choose between latest/recovery firmware
- Fip image will be updated (BL31, BL32 and BL33) combined (Consider as RAW FILE)
Updating capsule with MM

1. OS
2. UpdateCapsule()
3. ProcessCapsuleImage()
4. FmpSetImage()
5. SetFmpImageData()
6. StartFmpImage()
7. LoadImage()
8. StartImage()
Updating capsule with MM

1. CapsuleAuthenticateSystemFirmware()
   - Authenticate System Firmware Image

2. ExtractSystemFirmwareImage()
   - Extract System Firmware Image and update pointers with System Image information

Make SMC call to inform TF-A to use new image.
Advantage

- Security
- Can be used with thin PrePei way of working
References/Acknowledgment

- UEFI Specification 2.7

- ARM TF-A (https://github.com/ARM-software/arm-trusted-firmware/tree/master/docs)


- Microsoft Walkthrough on Firmware Updates (http://www.uefi.org/sites/default/files/resources/Microsoft_Spring%202018%20UEFI_Plugfest_Template_Day3.pdf)

- EDK-II source code

- ARM TZ
QUESTIONS?
Thanks for attending the Fall 2018 UEFI Plugfest

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

presented by

NXP, NXP SECURE CONNECTIONS FOR A SMARTER WORLD are trademarks of NXP B.V. All other product or service names are the property of their respective owners. Arm is a registered trademark of Arm Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. ©2018 NXP B.V.