Traceable Firmware Bill of Materials

Overview

UEFI 2021 Virtual Plugfest
December 8, 2021
Amy Nelson, Jiewen Yao & Vincent Zimmer
Amy Nelson

- **Amy Nelson** is Distinguished Member Technical Staff, Software Engineering in Dell’s Modern Computing Solutions Group. She has been a Security Architect in Dell Client Solutions Group for the last 15 years focused on hardware, firmware and software.

- Amy co-chairs the PC Client Working Group and the TCG Technical Committee. Amy is the editor of the PC Client Firmware Integrity Measurement Specification and the PC Client Platform Firmware Profile Specification.
Jiewen Yao

- **Jiewen Yao** is a principal engineer in the Intel Software and Advanced Technology Group. He has been engaged as a firmware developer for over 15 years. He is a member of the UEFI Security Sub Team and the TCG PC Client Working Group, and chairing the DMTF SPDM Code Task Force.
Vincent Zimmer

- Vincent Zimmer is a senior principal engineer in the Intel Software and Advanced Technology Group. He has been engaged as a firmware developer for over 25 years and leads the UEFI Security sub team.
Agenda

• Background
• Firmware BOM
• Example
• Summary / Call to Action
Background – Supply Chain

Supply Chain Risk
– build tool, signing service, assembling, preinstallation, shipping

Software Bill of Material (BOM)

Bill of material (BOM): a list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, parts, and the quantities of each needed to manufacture an end-product.

Software BOM Today

**Software Package Data Exchange (SPDX)** – Low-level details of components
- Standard: ISO/IEC 5962:2021
- Examples: [https://github.com/swinslow/spdx-examples](https://github.com/swinslow/spdx-examples)
- Tools: [https://github.com/lfscanning](https://github.com/lfscanning)

**Software Identification (SWID) Tag** – describe Software Product

**Common Platform Enumeration (CPE)** – Describe application, OS, hardware
- Examples: [https://nvd.nist.gov/products/cpe](https://nvd.nist.gov/products/cpe)

**CycloneDX Software BOM** – Lightweight SBOM used in application security
- Standard: [https://github.com/CycloneDX/specification](https://github.com/CycloneDX/specification)
- Examples: [https://github.com/CycloneDX/sbom-examples](https://github.com/CycloneDX/sbom-examples)
- Tools: [https://cyclonedx.org/tool-center/](https://cyclonedx.org/tool-center/)
Complexity of Firmware

Quiz: How many firmware exist in this platform?

<table>
<thead>
<tr>
<th>UEFI FW</th>
<th>ME FW</th>
<th>Microcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS ACM</td>
<td>SINIT ACM</td>
<td>BMC</td>
</tr>
<tr>
<td>1Gb NIC FW</td>
<td>PXE OROM</td>
<td>RST OROM</td>
</tr>
<tr>
<td>ASPEED Video</td>
<td>Optane DIMM</td>
<td>NVMe</td>
</tr>
<tr>
<td>PCIE Device</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

www.uefi.org
And the supply chain issue in Firmware

* Source: https://www.blackhat.com/us-21/briefings/schedule/index.html#safeguarding-uefi-ecosystem-firmware-supply-chain-is-hardcoded-23685
Host Integrity at Runtime and Startup (HIRS):
Source: https://github.com/nsacyber/HIRS

Attestation Certificate Authority (PrivacyCA)

TPM Provisioning

Version 2.0 added support for the PC Client Reference Integrity Manifest (RIM) Specification to provide firmware validation capability to the HIRS ACA. This requires that the manufacturer of a device provide a digitally signed RIM "Bundle" for each device. The HIRS ACA has a new page for uploading and viewing RIM Bundles and a policy setting for requiring Firmware validation.
Attestation for Firmware

Appraiser

System Firmware

Endorser

Reference Provider

Policy Owner

TCG Platform Certificate / DICE Certificate

TCG RIM (SWID, CoSWID, CoRIM/CoMID)

Reference Manifest

Appraisal Policy

Appraisal

Endorsement

Manifest

TPM PCR

Evidence

TCG Event Log (including SPDM measurement)

Attestation Result

Relying Party

System Firmware as Lead Attester!
What is gap today?

• BIOS is measured as a chunk.

  Question: How to know info for each BIOS embedded component?

• Only BIOS and UEFI driver/application are measured.

  Question: How to know info for each device embedded firmware?
Firmware Bill of Material (BOM)

• **Firmware BOM**: A list of the firmware components and their hashes which are embedded or attached to the motherboard and play roles during system boot and runtime usage.

• **Firmware Related Guideline**
  – NIST SP800-155 (BIOS Integrity Measurement)
  – TCG PC Client Firmware Integrity Measurement (FIM)
  – TCG PC Client Reference Integrity Measurement (RIM)
  – TCG PC Client Platform Firmware Profile (PFP)
  – IETF CoSWID
  – IETF CoMID
Firmware BOM
Firmware Classification

• Type-I firmware
  – Loaded and executed in host environment.

• Type-II firmware
  – Loaded and executed NOT in host environment.

• More detail in next page ...
# Firmware Classification

<table>
<thead>
<tr>
<th>Type</th>
<th>SubType</th>
<th>Loader (Loaded by)</th>
<th>Location (Loaded From)</th>
<th>Execution Env</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type-I</td>
<td>I-A</td>
<td>Host</td>
<td>System Firmware</td>
<td>Host</td>
<td>BIOS, Intel FSP, CPU Microcode</td>
</tr>
<tr>
<td></td>
<td>I-B</td>
<td>Host</td>
<td>Peripheral Device</td>
<td>Host</td>
<td>PCI Option ROM, PXE</td>
</tr>
<tr>
<td>Type-II</td>
<td>II-A</td>
<td>Non-Host</td>
<td>Non-Host Firmware</td>
<td>Non-Host</td>
<td>BMC, EC, Intel CSME, PFR</td>
</tr>
<tr>
<td></td>
<td>II-B</td>
<td>Peripheral</td>
<td>Peripheral Device</td>
<td>Peripheral Device</td>
<td>NIC, NVMe, NVDIMM, Graphic Card.</td>
</tr>
</tbody>
</table>
System Firmware’s Role

• Type-I firmware handling:
  – Load and measure other Type-I firmware.
  – Ensure each firmware component have one or more dedicated entries in the event log.

• NOTE:
  – The system firmware itself can be measured and verified by a platform RoT.
Type-I firmware (today)

- **System Firmware RIM**
- **Platform Certificate**
- **Verifier**
- **OEM**
- **System Firmware (Type I-A)**
- **Device OROM (Type I-B)**
- **TPM / EventLog**

Authentication + Measurement
Type-I firmware

- Intel FSP
- 3rd Party FW
- OEM
- System Firmware (Type I-A)
- Device OROM (Type I-B)
- Authentication + Measurement
- Intel FSP RIM
- 3rd Party FW RIM
- Device RIM
- System Firmware RIM
- Platform Certificate
- TPM / EventLog

Verifier
System Firmware’s Role

• Type-II firmware handling:
  – Collect measurement of Type-II firmware from other RoT (device or platform).
  – Ensure each firmware component have one or more dedicated entries in the event log.

• NOTE:
  – The system firmware might not have access to some device RoT directly, but may get the Type-II firmware measurement from other RoT source (device or platform).
Type-II firmware (today)
Type-II firmware

Platform RoT

Non-Host Firmware(s) (Type II-A)

System Firmware (Type I-A)

Device Firmware (Type II-B)

Authentication + Measurement

Platform Certificate

Non-Host Firmware RIM

System Firmware RIM

Device RIM

TPM / EventLog (SPDM Measurement)

Verifier

Authentication + Measurement

SPDM

www.uefi.org
Example
Type-I Firmware - Intel FSP

- Intel Firmware Support Package (FSP)
  - A binary to perform silicon initialization.
  - Released by Intel.
  - Can be integrated into OEM BIOS.

- Question
  - Is the FSP binary in OEM BIOS from Intel?
  - Is it the latest FSP binary with known bug fix?
Type-I Firmware - Intel FSP

**Base RIM (SWID Tag)**

- **Name**: AmberLakeFspBin
- **version**: 3.7.6
- **tagID**: CC92BA16-8450-4C4B-8EFA-F34D5299D5E0
- **Link**: [here](http://...)
- **Role**: softwareCreator tagCreator
- **BindingSpec**: PC Client RIM
- **BindingSpecVersion**: 1.2
- **SupportRIMFormat**: TCG_EventLog_Assertion
- **SupportRIMURL**: [here](http://...)
- **DigitalSignature**: XXXXXXXX

**Support RIM**

- **EV_EFI_PLATFORM_FIRMWARE_BLOB2**:  
  - **Description**: FSPT  
  - **Base**: 0x00000000FFED0000  
  - **Length**: 0x0000000000130000  
  - **Digest**: AAAAAAAA  
- **EV_EFI_PLATFORM_FIRMWARE_BLOB2**:  
  - **Description**: FSPM  
  - **Base**: 0x00000000FFDF0000  
  - **Length**: 0x0000000000066000  
  - **Digest**: BBBB BBBB  
- **EV_EFI_PLATFORM_FIRMWARE_BLOB2**:  
  - **Description**: FSPS  
  - **Base**: 0x00000000FFD90000  
  - **Length**: 0x000000000002E000  
  - **Digest**: CCCCCCCC

*Source: Intel FSP 2.x Measurement and Attestation, [https://cdrdv2.intel.com/v1/dl/getContent/644001](https://cdrdv2.intel.com/v1/dl/getContent/644001)*
Type-I Firmware - Intel FSP

TCG Event Log
==========

TCG_Sp800_155_PlatformId_Event2:
  ManufactureId: <OEM_ID>
  ManufactureStr: <OEM>
  RimGuid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

TCG_Sp800_155_PlatformId_Event2:
  ManufactureId: 343
  ManufactureStr: Intel
  RimGuid: CC92BA16-8450-4C4B-8EFA-F34D5299D5E0

EV_EFI_PLATFORM_FIRMWARE_BLOB2:
  Description: FSPT
  Base: 0x00000000FFED0000
  Length: 0x0000000000130000
  Digest: AAAAAAAA

EV_EFI_PLATFORM_FIRMWARE_BLOB2:
  Description: FSPM
  Base: 0x00000000FFDF0000
  Length: 0x0000000000066000
  Digest: BBBBBBBB

EV_EFI_PLATFORM_FIRMWARE_BLOB2:
  Description: FSPS
  Base: 0x00000000FFD90000
  Length: 0x000000000002E000
  Digest: CCCCCCCC

* Reference:
https://github.com/tianocore/edk2/blob/master/IntelFsp2WrapperPkg/Include/Library/FspMeasurementLib.h
Type-I Firmware - Intel FSP

Base RIM
=========
tagID
SupportRIMURL

Support RIM
==========
FSPT: Hash: AAAA
FSPM: Hash: BBBB
FSPS: Hash: CCCC

System Firmware RIM

Intel FSP

System Firmware (Type I-A)

Platform Certificate

PCR/Event Log
==============
800_155_PlatformId: RimGuid
FSPT: Hash: AAAA
FSPM: Hash: BBBB
FSPS: Hash: CCCC

Verifier

TPM / EventLog

www.uefi.org
Type-I Firmware – UEFI Image

- uswid tool - [https://github.com/hughsie/python-uswid](https://github.com/hughsie/python-uswid)
  - A tool to create CoSWID tag for **UEFI image**

```
[uSWID]
tag-id = acbd84ff-9898-4922-8ade-dd4bbe2e40ba
software-name = HughskiColorHug.efi
software-version = 1.2.3
product = ColorHug
summary = Open Source Display Colorimeter
colloquial-version = b2ed6f1ed8587bf01a2951d74512a70f1a512d38
edition = v2021+
revision = 2

[uSWID-Entity:TagCreator]
name = Hughski Limited
regid = hughski.com
```
Type-II Firmware – Device

- Device includes
  - Firmware running in the device
  - Option ROM running in the host

- Question
  - How do we know the device firmware info?
  - How do we know the device option ROM info?
Type-II Firmware – Device

Base RIM

Type: corim
Vendor: XXX
Model: A.B.C
Id: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Role: tagCreator

Tag: coswid
Payload1: Digest: EEEEEEEE

Tag: comid

Fw1:
Vendor: XXX
Digest: AAAAAAAA

Fw2:
Vendor: XXX
Digest: BBBBBBBB

Fw3:
Vendor: XXX
Digest: CCCCCCCC
Type-II Firmware – Device

TCG Event Log

- **EV_EFI_SPDM_FIRMWARE_BLOB:**
  - Device Path: PCI Device
  - SPDM Measurement Block
    - Type 0: ImmutableROM
    - Device Measurement: AAAAAAAA
    - Device Context: PCI VID/DID

- **EV_EFI_SPDM_FIRMWARE_BLOB:**
  - Device Path: PCI Device
  - SPDM Measurement Block
    - Type 1: MutableFirmware
    - Device Measurement: BBBBBBBB
    - Device Context: PCI VID/DID

- **EV_EFI_SPDM_FIRMWARE_CONFIG:**
  - Device Path: PCI Device
  - SPDM Measurement Block
    - Type 2: HardwareConfig
    - Device Measurement: CCCCCCCC
    - Device Context: PCI VID/DID

- **EV_EFI_BOOT_SERVICES_DRIVER:**
  - Image Device Path: PCI Device/Option ROM
  - Digest: EEEEEEEE

* Reference:
  - https://github.com/DMTF/libspdm
Type-II Firmware – Device

Base RIM
==========
Payload0: Digest: EEEEEEEE
Vendor Info
Fw1: Digest: AAAAAAAA
Fw2: Digest: BBBBBBBB
Fw3: Digest: CCCCCCCC

PCR/Event Log
============= 
OptionROM Measurement: EEEEEEEE
PCI Info: VID/DID
SPDM Measurement: AAAAAAAA
SPDM Measurement: BBBBBBBB
SPDM Measurement: CCCCCCCC

Device RIM

TPM / EventLog

Verifier

System Firmware (Type I-A)

Device Firmware (Type II-B)

Device OROM (Type I-B)

SPDM

Authentication + Measurement
Future items (Challenge)

• Hot Plug device
  – If we need measure/attest the hot plug device?
  – If yes, how do we notify the device hot added or removed?

• Runtime Update
  – If we need measure/attest the new runtime firmware?
  – If yes, how do we notify the runtime firmware change?
Summary & Call for Action
Summary & Call for Action

• The industry is preparing support chain identification.

• System firmware plays a role to report firmware measurement information.

• We should get our firmware prepared.
Reference

• **General Supply Chain Guideline**
  – ISO/IEC 28000:2007 - Specification for security management systems for the supply chain
  – UK NCSC – Supply Chain Security Guideline

• **Standard / Guideline**
  – NIST SP800-155 (draft) – BIOS Integrity Measurement Guideline
  – TCG PC Client Platform Firmware Profile (PFP)
  – TCG PC Client Firmware Integrity Measurement (FIM)
  – TCG PC Client Reference Integrity Manifest (RIM)
  – TCG Platform Certificate Profile
  – TCG DICE Attestation Architecture
  – TCG DICE Layering Architecture
  – TCG DICE Certificate Profile
  – IETF RATS Remote Attestation Architecture
  – IETF SACM Concise SWID
  – IETF RATS Concise RIM
  – DMTF Secure Protocol and Data Model
Questions?
Thanks for attending the UEFI 2021 Virtual Plugfest

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