OCP Initiatives and Intel Implementations

Mohan J. Kumar
Intel Fellow
Intel Corporation
Agenda

• Open Firmware
• Firmware at Scale
• Platform Attestation
• Summary
Open Firmware
UEFI-based Open Firmware (for Intel-based Server Platforms)

Platform interfaces tables to support OS boot
https://uefi.org

EDKII – existing upstream/open source core at
https://github.com/tianocore/edk2

Intel binaries for board invariant Si code at
https://github.com/intelfsp or
https://github.com/tianocore/edk2-non-osi

Platform (board) Specific Code at
https://github.com/tianocore/edk2-platforms

Mt. Olympus Xeon-based platform with UEFI-based open firmware available

Open source UEFI core

Intel Silicon Init

Server Platform

Open source Platform Package(s)

Platform Firmware Interface (ACPI, UEFI)
Intel support for OpenBMC

• **Market Direction**
  - Customer Desire
  - Security, Easy Access to Source Code

• **Collaboration**
  - Shared Efforts
  - Enabling ODMs and 3rd Party Vendors

• **Open Manageability Standards**
  - OCP, Redfish
Firmware Management at Scale
Platform Firmware Configuration

• Firmware Configuration in current model is based on BIOS Setup utility
• Current model does not allow for
  • remote configuration
  • At scale configuration
• Proposing a Redfish based model for BIOS configuration
• Allows BIOS configuration using a browser
• Supports Fleet configuration using scripts
• User communicates to BMC via Redfish
• BIOS configuration stored in BMC is pulled by BIOS at boot and converted to UEFI BIOS Configuration settings
• Submitted to Redfish SPMF Forum
Platform Firmware Configuration

Proposed Redfish model

BIOSAttributeRegistry*.json

```json
{
  "CurrentValue": null,
  "DisplayName": "Minimum Processor Idle Power Core C-State",
  "AttributeName": "MinProcIdlePower",
  "Value": [
    {
      "ValueDisplayName": "C6 State",
      "ValueName": "C6"
    },
    {
      "ValueDisplayName": "C3 State",
      "ValueName": "C3"
    }
  ],
  "AttributeDependencies": [
    {
      "AttributeDependency": {
        "$or": [
          {
            "$EQU": {
              "/PowerProfile/CurrentValue": "BalancedPowerPerf"
            }
          },
          {
            "$EQU": {
              "/PowerProfile/CurrentValue": "MinPower"
            }
          }
        ],
        "CurrentValue": "C6"
      }
    }
  ]
}
```

Set "MinProcIdlePower/CurrentValue" to "C6" if:

- "PowerProfile/CurrentValue" == "BalancedPowerPerf" ||
- "PowerProfile/CurrentValue" == "MinPower"
Platform Firmware Configuration in Action

Query BIOS Configuration via HTTP Get

Update BIOS Configuration via HTTP Patch

Log Console in Managed Server Platform
Firmware Version Dependency

- Dependency model for Platform Firmware Configuration also used to describe firmware update dependencies
- Submitted to Redfish SPMF Forum

For more details, please attend “Redfish OCP profile for Server Platforms” on March 21, 10:30AM
Platform Attestation
Intel is working to deliver the best implementation of OCP Platform Attestation principles (Cerberus) with Intel® Platform Firmware Resilience (Intel® PFR)

- Attestation of BIOS and BMC images before allowing firmware to run
- Intel further extends platform security with mutual attestation between CPU and additional platform root-of-trust solutions
- Can detect compromised firmware and automatically recover to known-good state
- Performs attestation during both warm and hard resets
- Monitors and filters SPI bus traffic during runtime to help further reduce attacks
- Attestation capabilities extendable to additional peripheral firmware
Platform Attestation Support
PCle* Device Firmware Measurement + Attestation

Platforms need mechanisms to determine the identity and capability of devices to make trust decisions
• Device Firmware Measurement to verify both immutable and mutable firmware versions
• Device Authentication mechanism to query a Device’s identities tied to a Device private key

PCI Express* Device Security Enhancements Proposal Draft Specification Posted (URL below)
• Defines register interfaces for Device Measurement and Authentication
• Follows established industry paradigms & builds on the industry architecture for USB Authentication


* All product names are trademarks, registered trademarks, or service marks of their respective owners.
Summary
Summary

Intel actively engaged in OCP Platform firmware and OCP Security WG
Intel and partners providing more Open UEFI firmware solutions
Intel OpenBMC solution underway (Visit the Intel Booth A12)
Intel driving firmware management at scale solutions via SPMF
Intel plans to support OCP platform attestation (Cerberus) with best implementation using PFR
Intel’s proposal for Device Security Enhancements further improves platform security for PCIe peripherals
Notices & Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. For more complete information about performance and benchmark results, visit http://www.intel.com/benchmarks.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/benchmarks.

Benchmark results were obtained prior to implementation of recent software patches and firmware updates intended to address exploits referred to as "Spectre" and "Meltdown." Implementation of these updates may make these results inapplicable to your device or system.

Intel® Advanced Vector Extensions (Intel® AVX)* provides higher throughput to certain processor operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you can learn more at http://www.intel.com/go/turbo.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

© 2018 Intel Corporation.
Intel, the Intel logo, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.
*Other names and brands may be claimed as property of others.