State of UEFI Technology

Harry Hsiung

9/14/2017

Presentation will be posted at

http://www.uefi.org under Education, Presentation and videos

http://www.uefi.org/learning_center/presentationsandvideos/

Agenda

- Who is in UEFI
- Latest specifications
- Latest efforts in the code
  - Work to be done
- Where do you get UEFI
- Testing UEFI for Linux

The UEFI Forum

Board of Directors (13 Promoters)

Officers:
President: Mark Doran (Intel); VP (CEO): Dong Wei (ARM)
Secretary: Jeff Bobzin (Insyde); Treasurer: Bill Keown (Lenovo)

- Industry & Communications (ICWG)
- UEFI Specification (USWG)
  - Security Subteam (USST)
  - Configuration Subteam
  - Network Subteam (UNST)
  - Shell Subteam
  - ARM Binding Subteam
- Platform Initialization (PIWG)
  - Security Subteam
- Test (UTWG)
- ACPI Specification (ASWG)
  - NVDIMM Subteam
- Security Response Team (USRT)

Mark Doran President Intel	Dong Wei Vice President ARM	Jeff Bobzin Secretary Insyde Software	Bill Keown Treasurer Lenovo
Gary Simpson Advanced Micro Devices, Inc.	Stefano Righi American Megatrends, Inc.	Andrew Fish Apple	Richard Holmberg Dell
Dick Wilkins Phoenix Technologies	Kevin Depew Hewlett Packard Enterprise	Lan Wang HP, Inc.	Jeremy Kerr IBM	Toby Nixon Microsoft

13 Promoters
42 Contributors
245 Adopters
37 Individual Adopters
Total: 337

UEFI membership

Join the Forum

Membership is open to any company, organization or individual interested in contributing to the evolution of UEFI specifications.

General membership benefits:

- Access to the UEFI Forum Members-only web area
- Invitations to member events
- Access to UEFI technical tools and design guides

Membership Levels

The UEFI Forum offers two standard membership levels: Adopter and Contributor.

Adopter Membership:

- Complimentary membership
- General membership benefits listed above

Contributor Membership:

- $2,500 USD annual membership
- General membership benefits listed above, in addition to:
  - Participation in UEFI Work Groups, by invitation
  - Participation in email reflectors
  - Access to draft specifications

Full Membership Benefits

Benefit	Contributor	Adopter
Chairperson Candidacy	Yes	No
Voting Rights	Yes	No
Work Group Participation	Yes	No
Work-in-Progress Specification Access	Yes	No
Published Specification Access	Yes	Yes
Marketing Programs Access	Yes	No
Plugfest Attendance	Yes	Yes
Technical Expert Access	Yes	Yes
Members-only Collaboration Site Access	Yes	Yes
Email List Subscription	Yes	Yes
Listed as Member on Forum Website	Yes	Yes
Number of Participants	Unlimited	Unlimited

Did You Know?

- Founded in 2005
- Supported by 280+ members
- Develops and maintains
  - Advanced Configuration and Power Interface (ACPI) Specification
  - Unified Extensible Firmware Interface (UEFI) Specification
  - UEFI Shell Specification
  - UEFI Platform Initialization (PI) Specification
  - UEFI PI Distribution Packaging Specification
  - UEFI Self-Certification Test

Working Groups

- ACPI Specfiication Work Group
- Industry Communications Work Group
- Platform Initialization Work Group
- UEFI HII/Configuration Subteam
- UEFI Networking Subteam
- UEFI Security Subteam
- UEFI Specification Work Group
- UEFI Test Work Group

Event Location: Capital Hotel. No. 7 Jianguo North Road Sec. 2 Taipei, Taiwan
http://www.capital-hotel.com.tw
Meeting/Testing Dates: October 30-November 3
Only UEFI Forum members may attend UEFI Plugfests. If your company is not a member, please go to http://www.uefi.org/join
To register, UEFI Forum members should visit: http://bit.ly/2t2GDKy.
http://www.uefi.org/fallplugfest2017

Save the date

UEFI plugfest USA – March 26-30th TBD (Seattle or Portland OR)

UEFI plugfest in Nanjing China March 28-30th, 2017

- State of UEFI - Mark Doran (Intel)
- Keynote: China Information Technology Ecosystem - Guangnan Ni (Chinese Academy of Engineering).
- The Role of UEFI Technologies Play in ARM Platform Architecture - Dong Wei (ARM)
- ARM Server's Firmware Security - Zhixiong (Jonathan) Zhang, Cavium
- SMM Protection in EDK II - Jiewen Yao (Intel)
- Server RAS and UEFI CPER - Mao Lucia and Spike Yuan (Intel)
- A More Secure and Better User Experience for OS-based Firmware Update - David Liu (Phoenix)
- UEFI and IoT: Best Practices in Developing IoT Firmware Solutions - Hawk Chen (Byosoft)
- Establishing and Protecting a Chain of Trust with UEFI - David Chen (Insyde)
- Implementation of Hypervisor in UEFI Firmware - Kangkang Shen (Huawei)
- Lessons Learned from Implementing a Wi-Fi and BT Stack - Tony Lo (AMI)
- UEFI Development Anti-Patterns - Chris Stewart (HP)

http://uefi.org/learning_center/presentationsandvideos

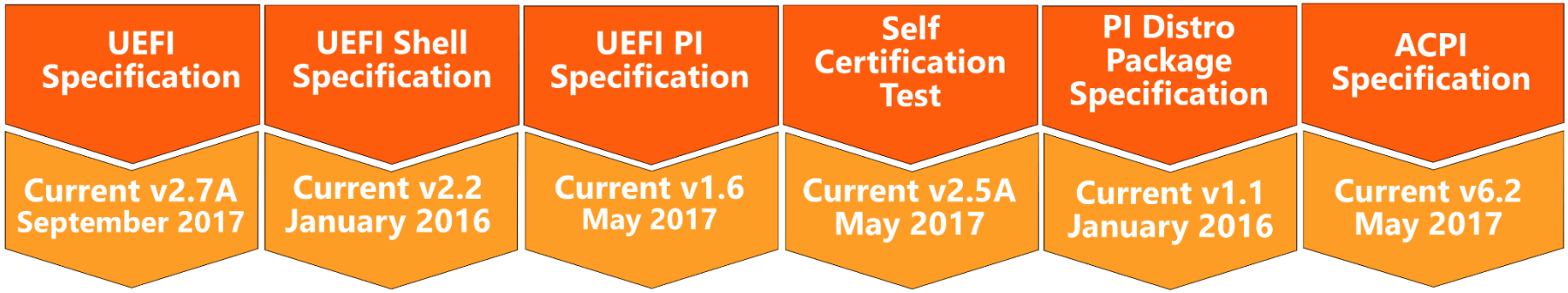
UEFI plugfest in Nanjing China March 28-30th, 2017

- UEFI - What is it?- Dong Wei (ARM)
- TianoCore, the Open Source UEFI Community - Brian Richardson (Intel)
- General Firmware Overview of Recommendations for Windows OS- Fei Zhou (Microsoft)
- Code Coverage in Firmware Automation Testing - Liu Zhi (Intel)

http://uefi.org/learning_center/presentationsandvideos

Latest UEFI & ACPI Specifications (Sept. 2017)

http://uefi.org/specifications



Related Trusted Computing Group(TCG) specifications

PC Client Work Group EFI Platform Specification, Version 1.22, Revision 15

PC Client Work Group EFI Protocol Specification, Family “2.0”, Level 00, Revision 00.13

New features added to Linux Distros for current UEFI features

- UEFI Http(s) boot (in addition to pxe boot)
  - Network boot using webpage URL instead of PXE servers. Ideally no need for touching DHCP servers or using UDP packets anymore (switch support?)
  - SUSE SLES 12 sp2/sp3 with ramdisk support
  - Redhat Rhel 7.4(checked in but not tested?)

- ESRT firmware capsule update
  - Update system firmware from Linux os runtime from a site like fwupd.org or oem site.
  - Requires cert signing for Linux
  - What about device firmware (option roms) for plugin cards?

ESRT capsule update

- **Security guideline for firmware to allow for in the field secure updates**
- **NIST Draft SP 800-193, Platform Firmware Resiliency Guidelines**
- http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-193

- New bill in Congress on cybersecurity https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017
- Requires devices on the internet to provide a properly authenticated firmware update method as specified by NIST (see above draft document).
- A more Secure and Better User Experience for OS-based Firmware Update

New features added to Linux Distros for current UEFI features cont.

- Secure boot audit and deployment mode
  - Code put on hold until OS is available that supports deployment of cert keys to blank systems with no keys.
  - Firmware code versions pending on Tianocore.org staging area when an OS shows up.

OS Recovery from Firwmare

- UEFI feature allowing for network boot (ie Https + nvram feature) to restore a system from firmware
- Missing OS utilities for UEFI Http(s) boot/install
  - Could be done via pxe but not secure
- Restore UEFI nvram variables securely

Legacy BIOS removal

- Roadmap for legacy bios support removal
  - UEFI defines 3 classes
    - Legacy bios only (Pre UEFI) Class 0

      3 variations of this class of systems with UEFI + Legacy

      Class 1 & 2
    - Legacy bios + UEFI (legacy bios default on first during boot)
    - UEFI + legacy bios (UEFI default on first legacy bios still present and executed)
    - UEFI + legacy bios (UEFI default on first, legacy bios in system but never dispatched)

    - UEFI only (no legacy bios in system at all) Class 3

Legacy BIOS removal

- Attrition
  - No new features coming out with legacy bios support
    - NVDIMM, NVME, RST raid, 100gig network, etc.
      - New technologies introduced in 2018
  - Security requirement for Windows
    - Legacy bios must be disabled for UEFI Windows 8.1/10 etc.
  - Hardware roadmaps from 2018-2020
  - No more validation with Legacy BIOS phasing out in 2020
  - Impact to supply chain
    - Ie mfg test, DOS utilities, firmware update/testing utilities OS pxe legacy deployment -> UEFI pxe or http installation

What's New in UEFI 2.7

- UEFI v2.7
  - Secure boot new Nvram variable X509 cert
    - New private authenticated_3 variable that can be X509 cert signed. Clarify interfaces for Private Authenticated variables
  - EFI HII Pop up protocol
    - Added protocol to provide services for pop windows (ie in setup)
  - External Cert management capability for secure boot
    - Allows for external management of UEFI certs (ie secure boot, hypervisor or OS keys) via out of band management like BMCs
  - EFI HTTP Boot Callback Protocol (added)
    - Can be used for HTTP boot debugging and packet inspection.
      - This allows for printing status updates to the console during a long download during handoff to network boot file over HTTP

What's New in UEFI 2.7

- Added ABI calling convention for RISC-V UEFI images
- New Reset Notification Protocol
  - Registers a function to be called before gRT->ResetSystem() is executed

    Allows for a common way of intercepting the reset vector for making sure hardware is shut down correctly before a reset (ie TPM, NVME storage device etc.)

UEFI 2.7 errata A (9/7/2017)

- EFI NVDIMM label flags local updated
  - When set, the complete label set is local to a single NVDIMM Label Storage Area. When clear, the complete label set is contained on multiple NVDIMM Label Storage Areas. **New**-If NLabel is 1 then setting this flag is optional and it is implied that the EFI_NVDIMM_LABEL_FLAGS_LOCAL flag is set as the complete label set is local to a single NVDIMM Label Storage Area.
- UEFI 2.7 Label Protocol Section
  - Missing define for EFI_NVDIMM_LABEL_FLAGS_UPDATING
- Modifications to UEFI option rom image combination examples:
  - Legacy Option ROM image
    IA-32 UEFI driver
    x64 UEFI driver
    AArch32 UEFI driver
    AArch64 UEFI driver
    Legacy Option ROM image + x64 UEFI driver
    Legacy Option ROM image + x64 UEFI driver + AArch64 UEFI driver
    x64 UEFI driver + AArch64 UEFI Driver
  - Itanium and EBC images not really relevant these days

UEFI 2.7 errata A (9/7/2017)

- Modified the requirement to enable PCI bus mastering
  - UEFI firmware will not longer be required to enable the BME bit for PCI bus mastering downstream devices. If it is not a boot device then various entities have recommended that BME be disabled.
  - Should go test this to see if this breaks your OS boot/install

What's New besides UEFI

- ACPI v6.2
  - 5.2.26 Secure Devices (SDEV) ACPI Table
    - New SDEV ACPI table, a list of devices that are allowed/denied to be hand-off by secure OS to a normal one.
  - 5.2.27 Heterogeneous Memory Attribute Table (HMAT)
    - New HMAT ACPI table, memory attributes for systems with heterogenous memory architecture
  - 5.2.28 Platform Debug Trigger Table (PDTT)
    - New PDTT ACPI table, a standard way to notify all debuggers connected to the system of a fatal crash.
  - 5.2.29 Processor Properties Topology Table (PPTT)
    - New PPTT ACPI table, a description of CPU topology, available cache types and sizes.
  - Windows SMM Security Mitigations Table
    - Reserved WSMT ACPI table, Microsoft's invention for system firmware to report its SMM security measures
    - Linux does not have a WSMT ACPI table equivalent so it does not have this SMM protection

UEFI testing

- UEFI Self certification test
  - Compliance testing of your firmware implementation with the UEFI spec. Up to UEFI 2.5a. 2.6 SCT about to be released
  - http://uefi.org/testtools
- FWTS – linux firmwFunctional tests for UEFI and ACPI are test suite from Ubuntu and community
  - Release note: https://wiki.ubuntu.com/FirmwareTestSuite/ReleaseNotes/17.03.00
  - Source Package: https://launchpad.net/ubuntu/+source/fwts/17.03.00-0ubuntu1
  - Tarball: http://fwts.ubuntu.com/release/fwts-V17.03.00.tar.gz
  - Live-image: http://fwts.ubuntu.com/fwts-live/fwts-live-17.03.00.img
- Forum looking for more participation in test generation

UEFI and Security

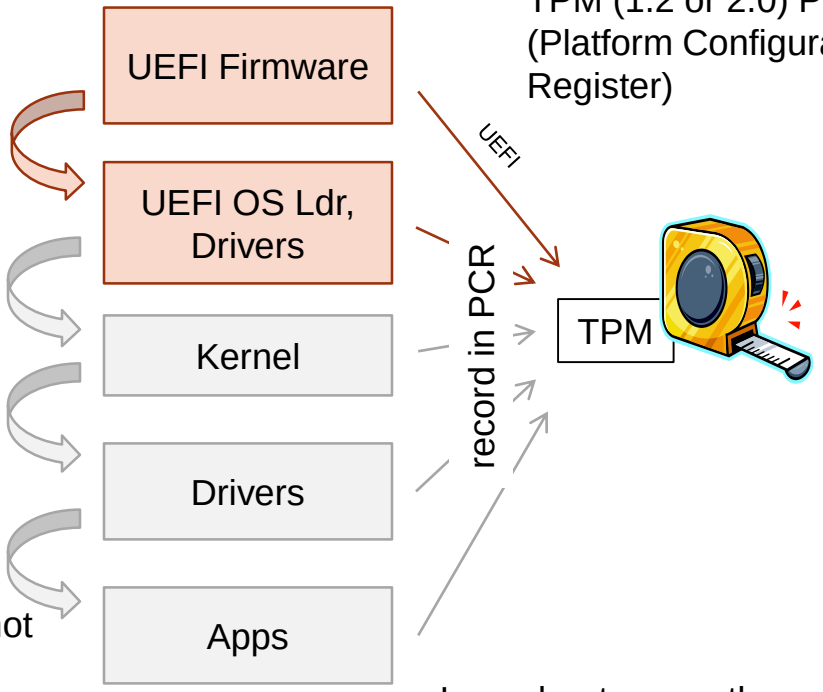
1. Secure boot (bare min)
2. Measure boot (TCG trusted boot)
3. Measured boot with hardware enforcing signed modules (ie Intel Bootguard, TXT, Trousers etc.)

- Most major Linux distros support 1
- Missing 2 with attestation and 3 for std shrink wrap Linux builds.

UEFI Secure Boot vs. TCG Trusted Boot

UEFI PI will measure OS loader & UEFI drivers into TPM (1.2 or 2.0) PCR (Platform Configuration Register)

UEFI authenticate OS loader
(pub key and policy)



Check signature of before loading

- UEFI Secure boot will stop platform boot if signature not valid (OEM to provide remediation capability)
- UEFI will require remediation mechanisms if boot fails

- Incumbent upon other software to make security decision using attestation

TCG 2.0 (trusted computing group)

- UEFI only specifies a signed boot (secure boot)
- TCG provides spec for measured boot (static root of trust)
  - PC client Specific Platform Firmware Profile spec

https://www.trustedcomputinggroup.org/wp-content/uploads/PC-ClientSpecific_Platform_Profile_for_TPM_2p0_Systems_v21.pdf

- Pc client work group EFI protocol specification

https://www.trustedcomputinggroup.org/tcg-efi-protocol-specification/

- Today systems ship with 1.2 TPMs
- Updated specs now provided for 2.0 TPMs

http://www.uefi.org/sites/default/files/resources/Phoenix_Plugfest_Fall_2016.pdf

http://www.uefi.org/sites/default/files/resources/Phoenix_Plugfest_TPM2_March_2016.pdf (delta of changes for UEFI)

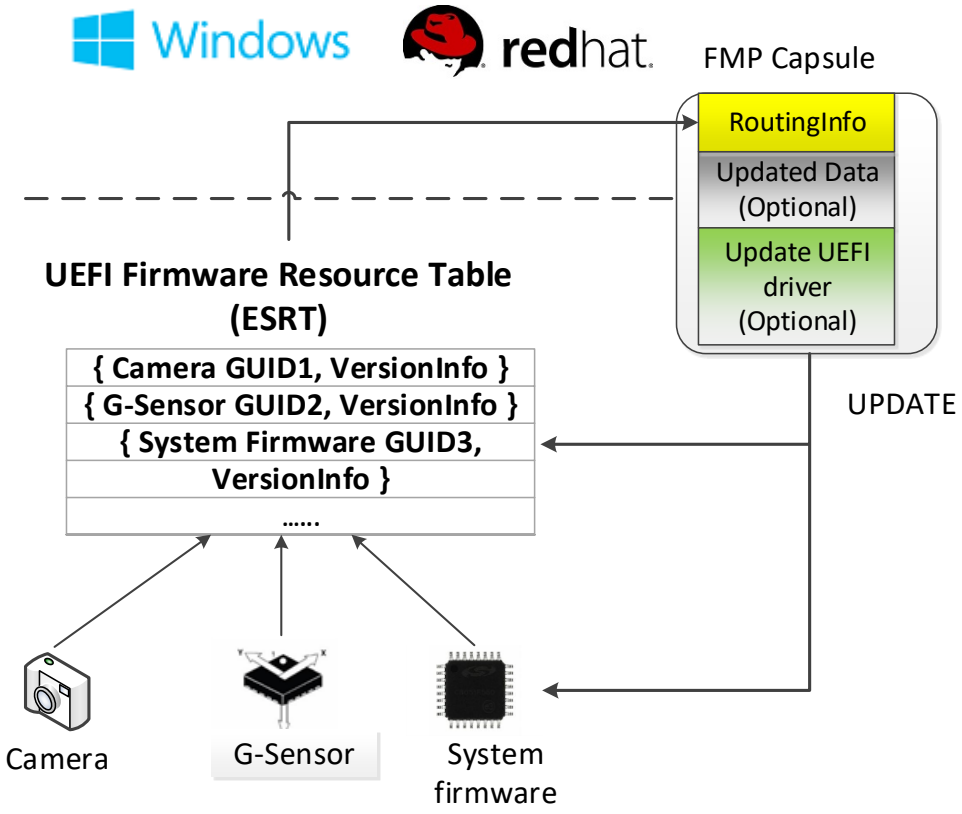
- Still in public review

  https://www.trustedcomputinggroup.org/specifications-public-review/

- TPM Specification, Version 2.0, Revision 135

Secure firmware update (ESRT capsule)

- Firmware update protected by:
  - OS verify the update driver when creating capsule
  - UEFI secure boot verify capsule payload before performing update
- What's new:
  - ESRT
  - FMPv3
  - FMP capsule



Where do you get UEFI

- Code lives on www.tianocore.org EDKII project
- Snapshots labelled as UDK2015, UDK2016 ….
- Mainly core code (UEFI protocols common to all implementations)
  - Not complete trees for platforms
  - OVMF/QEMU and NT32 trees for development
  - New Bugzilla database
  - GCC5 tool chain added
  - Security reporting mechanism
  - Training documents for EDK2

Open source hardware designs

- MinnowboardMax (Baytrail-I)
  - http://wiki.minnowboard.org/MinnowBoard_MAX
  - New Turbot ADI board version
  - http://www.adiengineering.com/products/minnowboard-turbot/
  - Lures (plugin cards) www.tincantools.com
    - Spi hook flash re-program/debug $29
  - Firmware source at Firmware.intel.com + tianocore.org (Valleyview pkg).
  - Other firmware now available(Uboot,coreboot, FSP etc.)

http://Firmware.intel.com/projects/minnowboard-max

- ARM UEFi platforms

https://wiki.linaro.org/ARM/UEFI

More UEFI hardware

- Rainbowpass S1200V3RPS (Haswell workstation)

http://www.Tunnelmountain.net

UEFI 2.5/2.6 code

Https support (wired lan only)

Ramdisk support

ESRT capsule update

TPM 2.0/1.2 support (LPC only)

Firmware at

https://firmware.intel.com/develop/server-development-kit

UEFI firmware testing

- FWTS – linux firmware test suite from Ubuntu
  - Tests both UEFI and ACPI in a platform

  https://wiki.ubuntu.com/FirmwareTestSuite

UEFI SCTs

- UEFI org tests for spec compliance

  http://www.uefi.org/testtools

- Linux UEFI validation

  https://01.org/linux-uefi-validation

References

- UEFI papers
  - http://www.uefi.org/learning_center/papers
  - Beyond BIOS **Developing with the Unified Extensible Firmware Interface, 3rd edition**
  - **Harnessing the UEFI Shell: Moving the Platform Beyond Dos, 2nd edition**
  - **The Chain of Trust: Keeping Computing Systems More Secure**
  - **The Chain of Trust: Keeping Computing Systems More Secure**