UEFI and Linux Interoperability

Harry Hsiung

11/3/2016

Presentation will be posted at

http://www.uefi.org under Education

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

- Who does 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 (12 Promoters)

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

12 Promoters
41 Contributors
221 Adopters
36 Individual Adopters
Total: 310
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

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

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 Specification 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
Plugfest gatherings of all UEFI members once a year in USA (Seattle) and usually in Taipei.

http://www.uefi.org/events

Some presence also at Linuxcon and OCP summit.
Specifications and code

http://uefi.org

- UEFI 2.0
- PI 1.0
- UEFI 2.1
- PI 1.1
- UEFI 2.2
- PI 1.2
- Shell 2.0
- Packaging 1.0
- UEFI 2.3
- PI 1.3
- UEFI 2.3.1
- PI 1.4
- ACPI 6.1
- UEFI 2.6
- PI 1.5

EDK 1.01:
- UEFI 2.0
- PI 1.0

EDK 1.04:
- UEFI 2.1
- PI 1.1

EDK 1.06:
- UEFI 2.1+
- PI 1.2

EDK II*:
- UEFI 2.1+
- PI 1.3

SCT UEFI
- 2006
- 2007
- 2008
- 2009
- 2010
- 2011-16

UDK2010:
- UEFI 2.3
- PI 1.4

UDK2016:
- UEFI 2.6
- PI 1.5

http://tianocore.org
https://github.com/tianocore/edk2
Latest UEFI & ACPI Specifications (Q3 2016)

http://uefi.org/specifications

- UEFI 2.6
- ACPI 6.1
- UEFI Shell 2.2
- UEFI PI 1.4
- UEFI PI Packaging 1.1
What’s Not So New UEFI 2.5 … needs coding

- But needs to be tested
  - UEFI 2.5 Network Enhancements
    - Boot from HTTP
      - HTTP API
      - HTTP Helper API
      - DNS v4/6
      - RAM Disk Device Path
      - Code in staging area of EDK2 Tianocore.org
  - WiFi
    - EAP Support
  - TLS (Https)
  - Bluetooth (BLE for hid only)
  - REST Protocol (Redfish DMTF) [http://redfish.dmtf.org/]
What’s New in UEFI 2.6

- UEFI v2.6
  - Network Enhancements
    - Wireless MAC Connection II Protocol
    - RAM Disk Protocol
  - RAS
    - CPER Extension for ARM
  - User Interface
    - HII Font Ex, Glyph Generator, Image Ex and Image Generator Protocols
  - IO
    - SD/eMMC Pass Thru Protocol
    - Non-identity Mapped Address Translations in PCI Root Bridge and IO Protocols
What’s New besides UEFI

- ACPI v6.1
  - Persistent Memory
    - NFIT Updates
    - NFIT Root Device _DSM
  - RAS
    - APEI Extension for ARM
    - ERST/EINJ max wait time
- Management
  - Graceful Shutdown Clarifications
  - Wireless Power Calibration Device
- IO
  - Interrupt-signaled Events
UEFI Secure Boot vs. TCG Trusted Boot

- 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

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

- Incumbent upon other software to make security decision using attestation
Secure Boot Implementation

UEFI firmware

boot shim

bootloader

kernel

verify & execute

verify & execute

verify & execute

ExitBootServices()

Legend

-cert Microsoft* UEFI CA certificate

-sig Signature generated from Microsoft UEFI CA

-cert Fedora* CA certificate

-sig Signature generated from Fedora CA
SUSE* Approach to UEFI Secure Boot

- SUSE has to balance two goals
  - Improving enterprise security by adopting UEFI Secure Boot
  - Reconcile UEFI Secure Boot with Linux developer’s need to run a custom boot loader & kernel
- Aiming to support Secure Boot in SLE11 SP3* and openSUSE*
- Working with Linux* community and other vendors
  - Building on the shim loader created by Matthew Garrett
  - Extending it to allow machine owner to securely boot other kernels
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
- 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_TPM_2_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
Trusted Execution Environment
TrEE (1.0)

- EFI protocol to allow OS (bootloader) to:
  - Check TPM related firmware capabilities
  - Obtain TCG measured boot log
  - Add measurements to log and extend into TPM PCRs
  - Pass TPM commands to TPM device
TrEE 1.0 -> TCG2.0

- Added support for crypto-agile functionality
  - Switch active TPM PCR banks
  - Obtain crypto-agile TCG measured boot log
- Same GUID as TrEE 1.0 protocol
- Get capability API reports new version number
  - Allowing firmware to implement one protocol
  - Caller can use different subset of functionality based on reported version
Customized UEFI Secure boot
Starting in UEFI 2.5/2.6 versions

https://github.com/tianocore/edk2-staging/tree/Customized-Secure-Boot

### Deployment

<table>
<thead>
<tr>
<th></th>
<th>Initial</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Platform Specific</td>
<td>Standardized solution to customize the secure boot keys</td>
</tr>
<tr>
<td>Specific PK</td>
<td>PK\textsubscript{pub} Clear</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Setup Mode</td>
<td>Setup Mode</td>
</tr>
<tr>
<td></td>
<td>User Mode</td>
<td>User Mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit Mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deployed Mode</td>
</tr>
</tbody>
</table>

### Benefits

- No specific solution
- Higher utilization
- Verification status
- Security
- Flexibility
- Extensibility

Customized UEFI Secure Boot reduces the security risk introduced by platform specific solutions. Working w/ OS vendors on interoperability and readiness.
Customized Deployment of Secure Boot

- Configure Secure Boot options programmatically
- Enterprise admins can set and deploy PK/KEK/db/dbx/[future Secure Boot variables]
- Uses new Secure Boot modes from UEFI 2.5 Section 30.3
  - Setup, User, Deployed, Audit
- Relies on PCR[7] in TPM 2.0
## Customized Deployment of Secure Boot
tentative timeline

<table>
<thead>
<tr>
<th>Estimate</th>
<th>Checkpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>09-2016</td>
<td>UEFI spec fix ECR drafted</td>
</tr>
<tr>
<td>11-2016</td>
<td>TCG spec stabilized</td>
</tr>
<tr>
<td>12-2016</td>
<td>UEFI spec fix published</td>
</tr>
<tr>
<td>02-2017</td>
<td>Tianocore production branch stabilized and verified</td>
</tr>
<tr>
<td>03-2017</td>
<td>IBVs receive Tianocore</td>
</tr>
<tr>
<td>05-2017</td>
<td>IBVs ready to support Customized Deployment of Secure Boot</td>
</tr>
<tr>
<td>08-2017</td>
<td>OEMs start shipping devices with the Customized Deployment of Secure Boot</td>
</tr>
</tbody>
</table>
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
HTTP Stack

https://github.com/tianocore/edk2-staging/tree/HTTPS-TLS
https://github.com/tianocore/edk2/tree/master/NetworkPkg

New Modules

<table>
<thead>
<tr>
<th>Driver</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Boot Driver</td>
<td>HTTP Library</td>
</tr>
<tr>
<td>HTTP Driver</td>
<td>TlsLib Library</td>
</tr>
<tr>
<td>HTTP Utilities Driver</td>
<td>OpenslTlsLib Library</td>
</tr>
<tr>
<td>TLS Driver</td>
<td></td>
</tr>
</tbody>
</table>

- Flexible Network Deployment
- Home Environment Support
- Corporate Environment Support

BDS (Display boot option HTTP_BOOT)

Load File

Device Path

HTTP Boot Driver

Boot Service Discovery/Configuration

HTTP API

HTTP(S)

DNS

DHCP

TLS

TCP

UDP

IP Stack

MNP Driver

SNP

UNDI/NII
HTTP-S boot

https://github.com/tianocore/edk2-staging/tree/HTTPS-TLS
https://github.com/tianocore/edk2/tree/master/NetworkPkg

Booted!
Boot recovery

https://github.com/UEFI/uefiproto/tree/master/OsRecovery

- What’s new
  - OS defined recovery
  - Platform defined recovery
  - Recovery policy protected by authentication
    - OsRecoveryOrder
    - dbrDefault, dbr
  - Default platform recovery supported

Security enhancements help in accelerating the system startup stage
What’s New in Shell 2.2

- UEFI Shell v2.2
  - Network updates (for https boot)
  - Allow Execute() to not nest new shells
  - Add command line parameter to auto exit
  - New dh features
  - Setvar command re-factor
  - New command features for disconnect, comp, dmem, cls, reset, pci, bcfg, dmpstore
  - Nvdimm support – mm
Putting it all together

- Having platforms with the features
  - Including
    - OVMF
    - Minnow
    - Galileo
    - Others…
  - UEFI Specification cannot prescribe ‘how’ to build (i.e., ‘where is my NIST 800-147 reference) but platforms can demonstrate
    - Windows Logo, Android CDD, NIST XYZ, …. 

- Security Bugs
  - in EDKII code ->
  - In other code and/or specification ->
    [http://uefi.org/security](http://uefi.org/security)
Bringing in other scenarios

- Network based recovery
  - HTTP, Wireless, Recovery -> have OS’s and platforms doing it

- Updates
  - Capsule, network, REST – harmonize payload between in-band and out of band
    - [http://www.dmtf.org/sites/default/files/standards/documents/DSP0267_1.0.0a.pdf](http://www.dmtf.org/sites/default/files/standards/documents/DSP0267_1.0.0a.pdf)

- IPXE scenarios – evolve UEFI Shell to provide parity to IPXE scripting?
Linux work list for UEFI

- ESRT (signed) firmware capsule update
  - OS passes payload of firmware to update in system
- Https network
  - OS install from https server (instead of pxe)
    - Ipxe support for scripting
  - OS booting from https server (instead of pxe)
  - OS recovery (ie cloud recovery) to restore OS and firmware
  - All of the above on Wifi networks for client
- Security
  - Measured boot static root of trust with TPM 2.0 support
  - UEFI secure boot audit and deployment mode
- Redfish support for Rest api (out of band deployment and support)
Where do you get UEFI

- Code lives on [www.tianocore.org](http://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
- GCC/Clang/llvm tool chain added
- Security reporting mechanism
- Training documents for EDK2
Open source hardware designs

- **MinnowboardMax (Baytrail-I)**
  - [http://wiki.minnowboard.org/MinnowBoard_MAX](http://wiki.minnowboard.org/MinnowBoard_MAX)
- New Turbot ADI board version
- Lures (plugin cards) [www.tincantools.com](http://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.)


- ARM UEFI platforms

[https://wiki.linaro.org/ARM/UEFI](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 Fall Plugfest - September 20-22, 2016**
  
  [http://www.uefi.org/learning_center/presentationsandvideos](http://www.uefi.org/learning_center/presentationsandvideos)

- **Redfish Configuration of UEFI HII Settings** - Mike Rothman (Intel) and Samer El Haj Mahmoud (Lenovo)
- **Innovative Software Tools & Methods to Profile, Test and Optimze UEFI Firmware Improving Test Coverage and Debug Results** - Kevin Davis (Insyde Software)
- **Out of Band BIOS Remote Management** - Matthew Krysiak (AMI)
- **UEFI Forum Update** - Dong Wei (HPE)
- **Microsoft UEFI Security Updates** - Scott Anderson, Suhas Manangi, Nate Nunez, Jeremiah Cox, and Michael Anderson (Microsoft)
- **UEFI Open Source Community: tianocore.org update** - Brian Richardson (Intel) and Leif Lindholm (Linaro)
- **UEFI Network and Security Update** - Vincent Zimmer (Intel)
- **Updated TCG TPM 2.0 Specs** - Dick Wilkins (Phoenix Technologies Ltd.)
- **ARM Trusted Firmware ARM UEFI SCT Update** - Charles Garcia-Tobin (ARM)