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)

- 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)

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

BOARD OF DIRECTORS

MARK DORAN President Intel	**DONG WEI** Vice President Hewlett Packard Enterprise	**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
LAN WANG HP, Inc.	**JEREMY KERR** IBM	**TOBY NIXON** Microsoft	**DICK WILKINS** Phoenix Technologies

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?

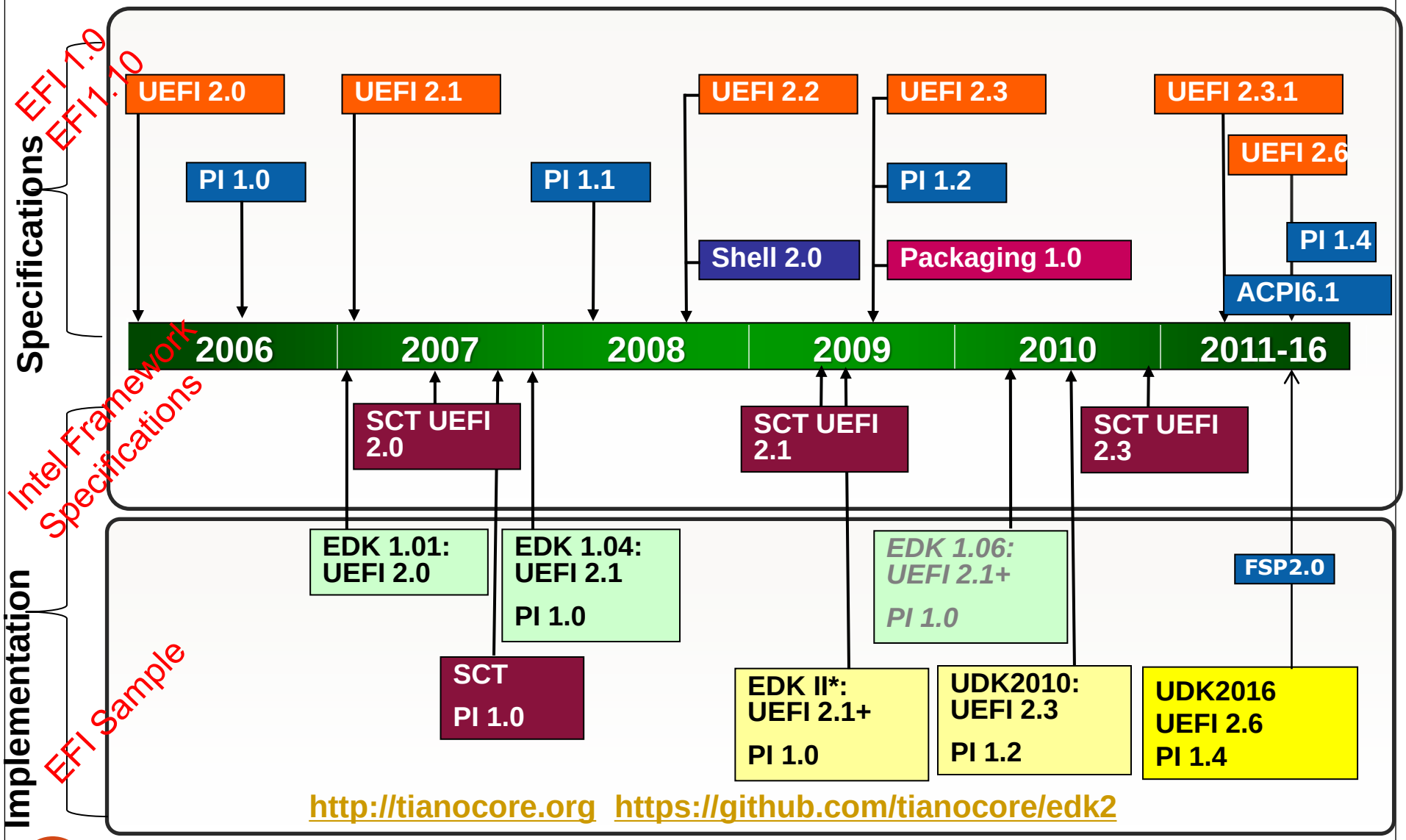
- Founded in 2005
- Supported by 280+ members
- Develops and maintains
  - Advanced Configuration and Power Interface (ACPI) Specification
  - Unified Extensible Firmware Interface (UEFI) Specification
  - UEFI Shell Specification
  - UEFI Platform Initialization (PI) Specification
  - UEFI PI Distribution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

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



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 Protcol
    - Non-identity Mapped Address Translations in PCI Root Bridge and IO Protocols

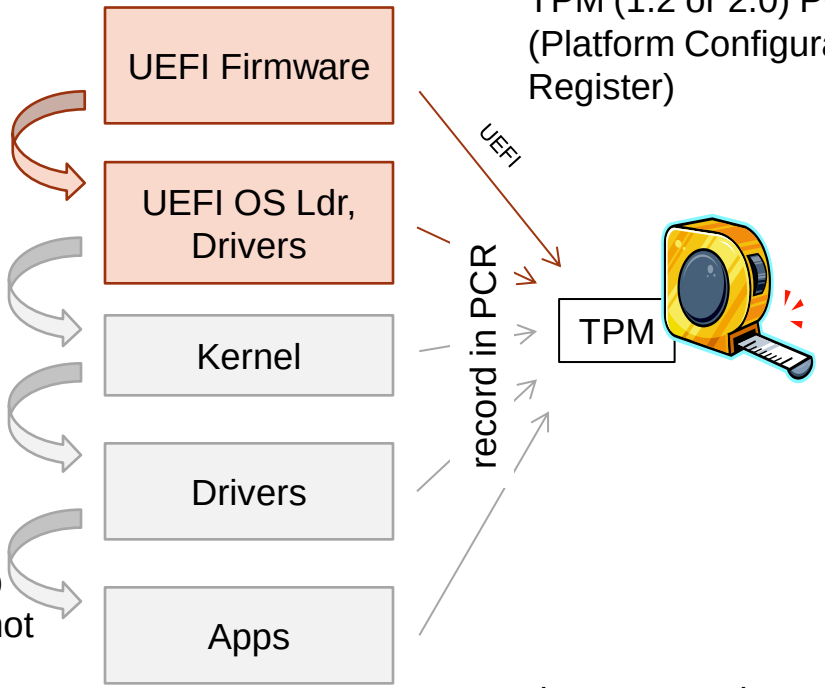
What’s New besides UEFI

- 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 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)

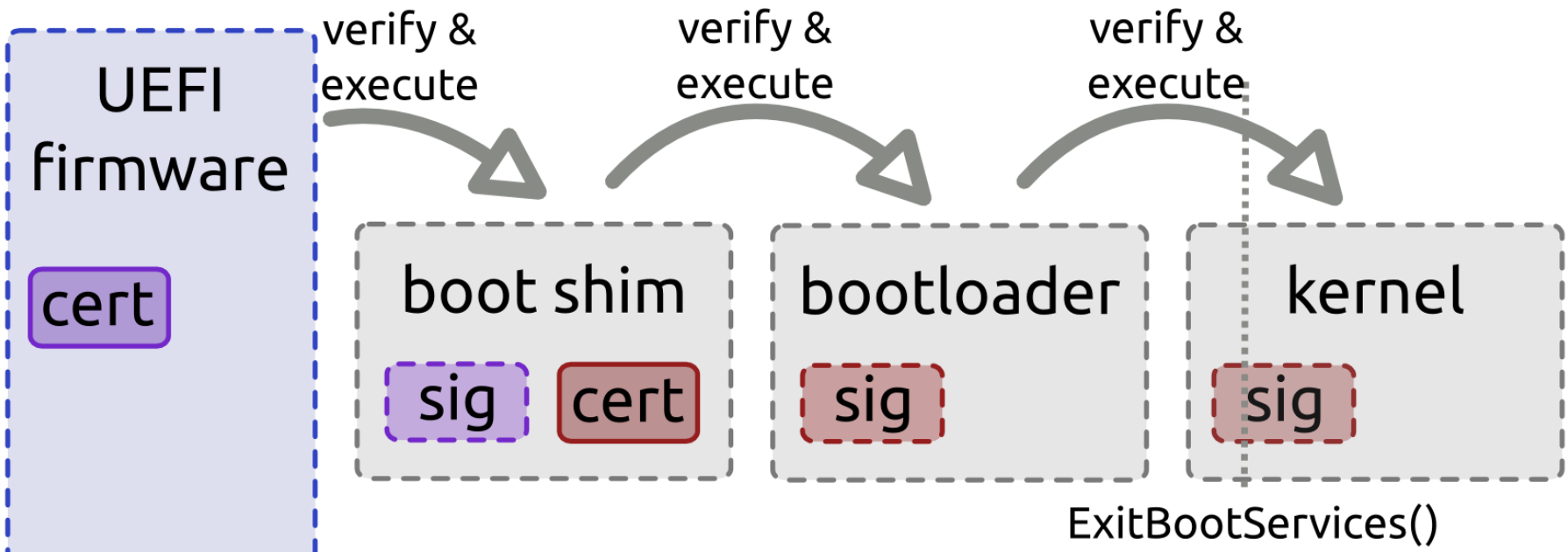


Check signature of before loading

- 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

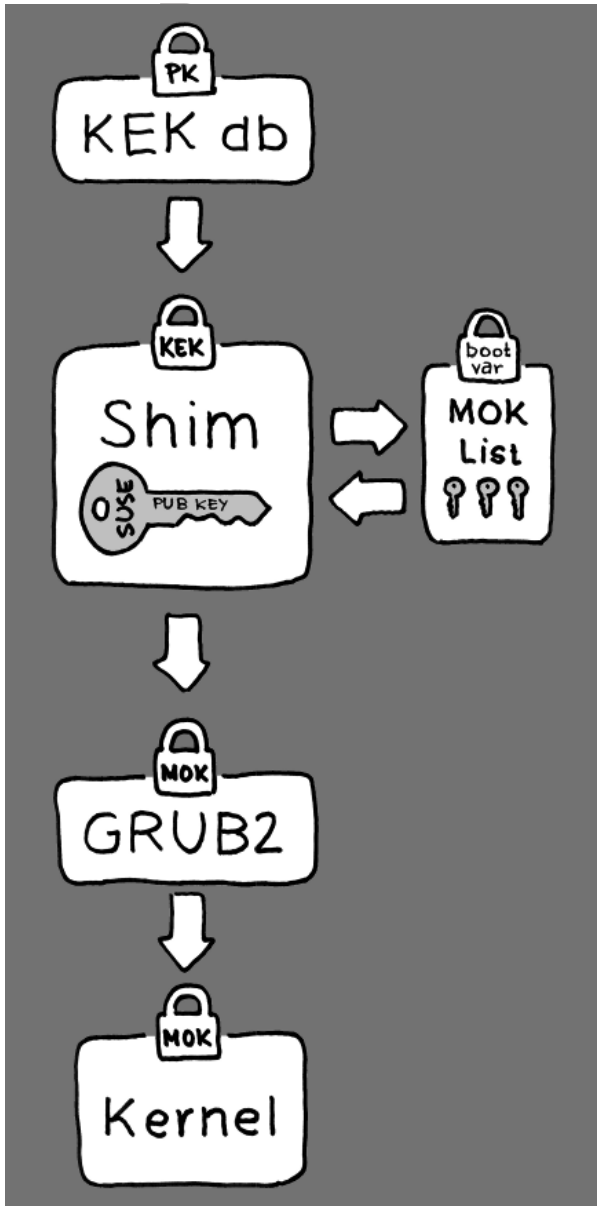
Secure Boot Implementation



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



- 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

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

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

Initial	Advanced
Platform Specific PK_{pub} Clear	Standardized solution to customize the secure boot keys
Setup Mode User Mode	Setup Mode User Mode Audit Mode Deployed Mode

Benefits

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

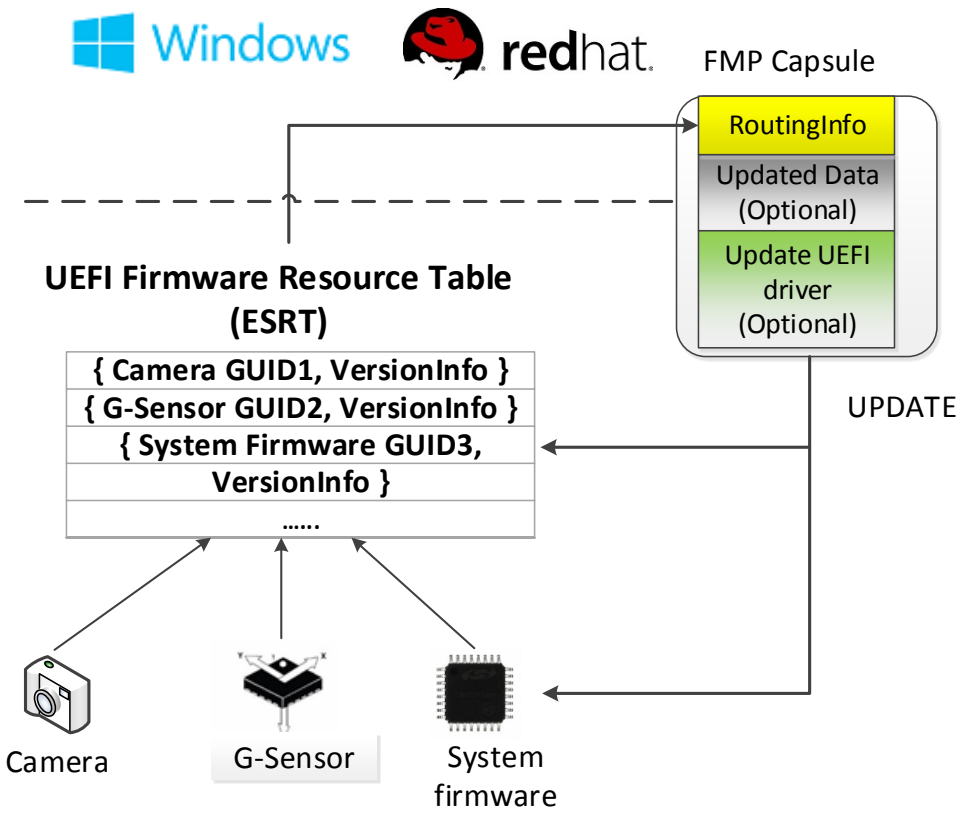
- Configure Secure Boot options programmatically
  - Enterprise admins can set and deploy PK/KEK/db/dbx/[future Secure Boot variables]
  - Uses new Secure Boot modes from UEFI 2.5 Section 30.3
    - Setup, User, Deployed, Audit
- Relies on PCR[7] in TPM 2.0

Customized Deployment of Secure Boot tentative timeline

Estimate	Checkpoint
09-2016	UEFI spec fix ECR drafted
11-2016	TCG spec stabilized
12-2016	UEFI spec fix published
02-2017	Tianocore production branch stabilized and verified
03-2017	IBVs receive Tianocore
05-2017	IBVs ready to support Customized Deployment of Secure Boot
08-2017	OEMs start shipping devices with the Customized Deployment of Secure Boot feature

Secure firmware update (ESRT capsule)

- Firmware update <u>protected</u> 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



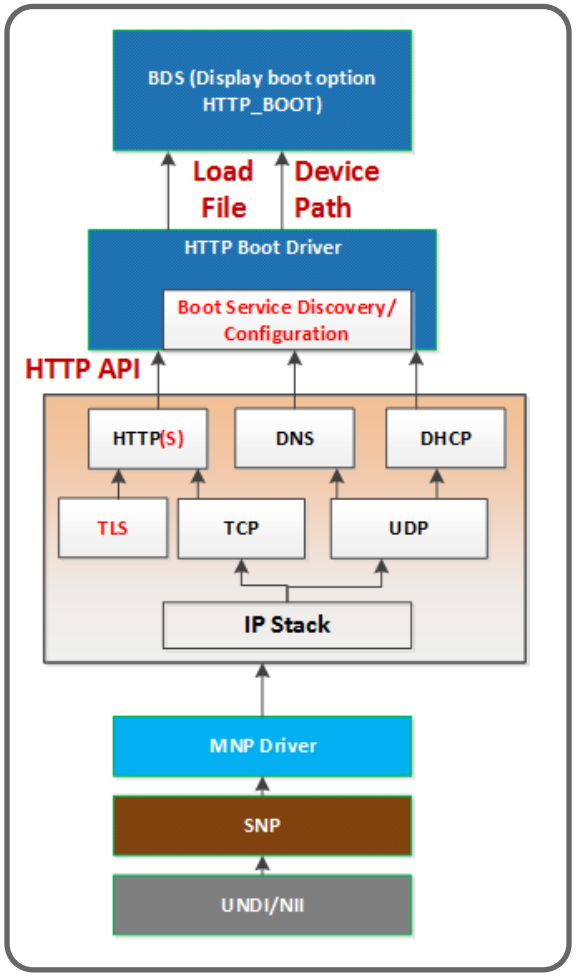
HTTP Stack

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

New Modules

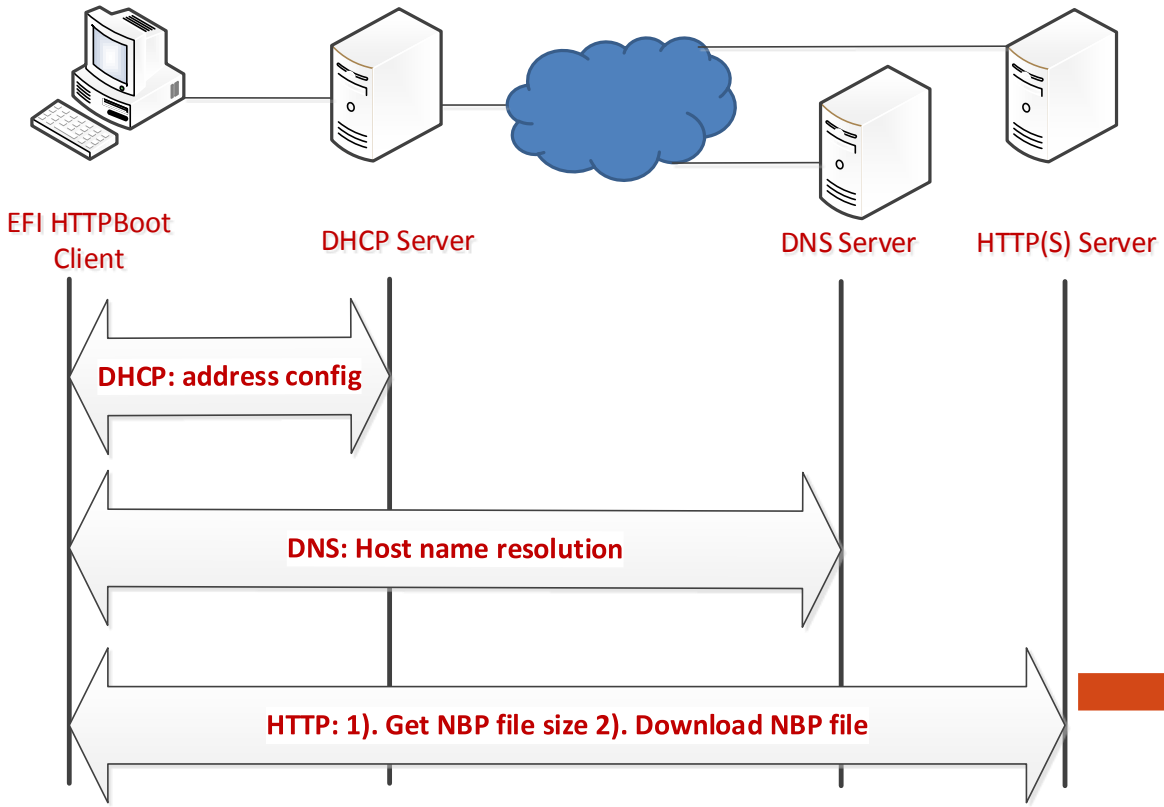
Driver	Library
HTTP Boot Driver HTTP Driver HTTP Utilities Driver TLS Driver	HTTP Library TlsLib Library OpenslTlsLib Library

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



HTTP-S boot

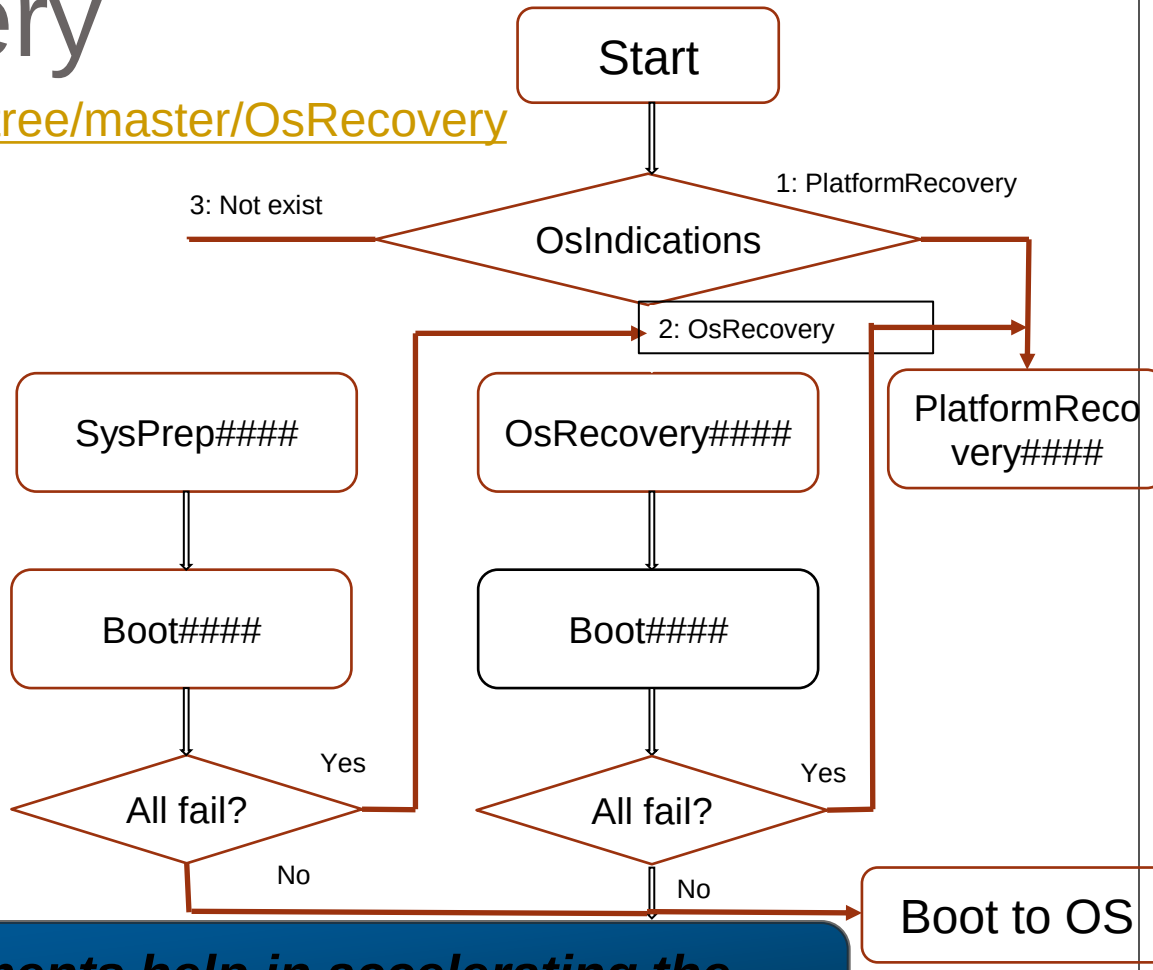
https://github.com/tianocore/edk2-staging/tree/HTTPS-TLS
https://github.com/tianocore/edk2/tree/master/NetworkPkg



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 -> https://github.com/tianocore/tianocore.github.io/wiki/Reporting-Security-Issues
  - In other code and/or specification -> 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.uefi.org/sites/default/files/resources/OCPsummit2016_Towards%20a%20Firmware%20Update%20Standard.pdf and 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 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
  - 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 Fall Plugfest - September 20-22, 2016**

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)