for Mere Mortals
About Us

• Stephano Cetola
  • TianoCore Community Manager
  • Open Source Firmware (& Hardware) Advocate

• Alexander Graf
  • KVM and QEMU developer for SUSE
  • Founding member of SUSE ARM team
What is UEFI?

“This Unified Extensible Firmware Interface (hereafter known as UEFI) Specification describes an interface between the operating system (OS) and the platform firmware.”

-- UEFI Specification 2.7A, August 2017
What is Defined?

• Platform Initialization
• Boot & Runtime Interfaces
• Advanced Configuration & Power Interface (ACPI)
• UEFI Shell
What is the Point?
Hardware Init to Payload Handoff

- Reset Vector
- Memory Initialization
- Boot Media Initialization
- Initialize Silicon Features
  (USB, Network, PCIe, UART, …)

- Standards Driven Interfaces
- Signed Capsule Update
  Linux Vendor Firmware Service (LVFS)
- HTTP/HTTPS Boot
- Graphics Output Protocol (GOP)
coreboot & Slim Bootloader

- Minimal initialization
- Quickly handoff to a payload
  (Bootloaders & OS’s)
- Boot the OS you care about

https://github.com/coreboot/coreboot
https://github.com/slimbootloader/slimbootloader
UEFI Implementation Examples

- Full Hardware Initialization
- Provide Boot-time Services
- Allow Firmware to be updated easily

https://github.com/tianocore/edk2
https://github.com/u-boot/u-boot
UEFI Implementation Examples

- Open Source Since 2004
- PI & UEFI Implementations
- Numerous Platforms (Emulation)
- UEFI Shell

- Open Source from Day 1
- "UEFI Lite" Implemented
- Large Selection of Hardware
- UEFI Shell
EFI Development Kit (EDK II)

- Build your own scalable UEFI implementation
- Open source firmware code
- Multiple corporations working together
- Growing community involvement
- Work from master repo or stable release
- Fully validated UEFI Development Kit (UDK)
- Stable tags created every three months

https://github.com/tianocore/edk2
• Monthly Community Meetings

• https://www.tianocore.org/community-meeting

• Improving our mailing list with Groups.io

• Working on building a community continuous integration (CI) environment
edk2-platforms repo

- Platforms actively maintained against edk2
- Default branch (master) contains platforms actively validated against edk2/master
- **stable**- branches track UDK releases
- **devel**- branches host works in progress

https://github.com/tianocore/edk2-platforms
EDK2-Platforms In Progress

- BeagleBone Black
- Aaeon Up² Board
- Marvell MACCHIATObin
- MinnowBoard Max / Turbot

https://github.com/tianocore/tianocore.github.io/wiki/EDK-II-Platforms
Example: Aaeon Up2 Board


https://github.com/tianocore/edk2-platforms/tree/devel-IntelAtomProcessorE3900
<table>
<thead>
<tr>
<th>License</th>
<th>GPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>100s kb</td>
</tr>
<tr>
<td>Market</td>
<td>Embedded, Integrated</td>
</tr>
<tr>
<td>Coding Style</td>
<td>Linux</td>
</tr>
<tr>
<td>Payload Interface</td>
<td>“UEFI Lite”, Direct Linux, U-Boot API</td>
</tr>
<tr>
<td>License</td>
<td>GPL</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Size</td>
<td>100s kb</td>
</tr>
<tr>
<td>Market</td>
<td>Embedded, Integrated</td>
</tr>
<tr>
<td>Coding Style</td>
<td>Linux</td>
</tr>
<tr>
<td>Payload Interface</td>
<td>“UEFI Lite”, Direct Linux, U-Boot API</td>
</tr>
</tbody>
</table>
“UEFI Lite”

UEFI

tianocore
"UEFI Lite"
Contributions Welcome

https://www.tianocore.org/contrib/
edk2-devel@lists.01.org
@stephano
stephano.cetola@intel.com

https://www.denx.de/wiki/U-Boot/Patches
u-boot@lists.denx.de