TianoCore – UEFI Open Source Community

Brian Richardson

Intel Corporation, Technical Evangelist

TianoCore, Community Evangelist
Agenda

• Introduction
• Recent changes
• Plans for the future
• Why is firmware so important?
Introduction

TianoCore - UEFI Open Source Community
**Mission**
- Improve contribution
- Increase code quality
- Provide regular updates
- More end-to-end solutions

**Vision**
- A more active EDK II developer community
- Decisions based on community feedback

Supporting EDK II, a BSD open source UEFI implementation
Improving on BIOS concepts

The Good
• Abstraction for the OS/app layer
• Expansion cards carry their firmware drivers (Option ROM)
• Ubiquitous

The Bad
• x86 16-bit model
• Not extensible
• Not standardized
• Not open
“We have a solution ... why don’t we just patch it?”
Standards Matter
Latest Specifications

Unified Extensible Firmware Interface (UEFI) v2.6
Advanced Configuration & Power Interface (ACPI) v6.1
UEFI Platform Initialization (PI) v1.4
UEFI PI Packaging v1.1
UEFI Shell v2.2
Recent changes

TianoCore - UEFI Open Source Community
Governance

Andrew Fish  
Michael Kinney  
Leif Lindholm
Transition to git

Edk II http://www.tianocore.org/edk2/

19,943 commits
8 branches
0 releases
105 contributors

Latest commit acc3a37 5 days ago

- AppPkg: AppPkg/.../Python: Clean up and document how to escape the -# option.
- ArmPkg: ArmPkg/ArmGicLib: use correct loop variable
- ArmPlatformPkg: ArmPlatformPkg/NorFlashDxe: use strictly aligned CopyMem!
- ArmVirtPkg: ArmVirtPkg: restrict mapping attributes of normal memory to EFI_MEMOR...
- BaseTools: BaseTools/EfiRom: supply missing machine type lookup strings
Staging branch workflow

- [https://github.com/tianocore/edk2-staging](https://github.com/tianocore/edk2-staging)
  - Branch maintainers sync to edk2/master
  - Use edk2 review to submit branch to master
- Main branch is focused on product quality
UEFI FAT license

- Very big deal for Linux, ovmf & aavmf
- As of March 2016, Microsoft removed the ‘use clause’ from UEFI FAT sources
- FatPkg/FatBinPkg now under 2-clause BSD with no field of use restriction
LLVM/Clang & GCC

• EDK II now enables link time optimization (LTO) for LLVM Clang 3.8 & GCC 5.3
  • Good example of community collaboration
• Enables a platform for code analysis tools
  • Ex: http://clang-analyzer.llvm.org/
• Validated on Linux
## Binary Sizes vs VS2015

<table>
<thead>
<tr>
<th></th>
<th>GCC5</th>
<th>CLANG38</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEIFV</td>
<td>26%</td>
<td>-15%</td>
</tr>
<tr>
<td>DXEFFV</td>
<td>4%</td>
<td>-4%</td>
</tr>
<tr>
<td>FvMainCompact</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>FVRECOVERY</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>FVMAIN</td>
<td>5%</td>
<td>16%</td>
</tr>
<tr>
<td>FvMainCompact</td>
<td>9%</td>
<td>15%</td>
</tr>
</tbody>
</table>

*EDK II OVMF x64*

*Intel® Galileo IA32*
bugzilla.tianocore.org

• For core/platform issues & requests

• Security issues follow a special process

  1. Never use e-mail to discuss a security issue
  2. Use Bugzilla (“Tianocore Security Issues”)
  3. Never use e-mail to discuss a security issue
Plans for the future

TianoCore - UEFI Open Source Community
Plans for the future

• Improve website structure and content
• Add open test cases for edk2
• More emphasis on open platforms
• Releases on a regular cadence
Release Management

Requirements

Fixes

Validation

Release

platform

staging

edk2

platform fix

fix

fix

fix

UDK

UEFI Development Kit (stable snapshot)

requirement / design reviews
Implement / integrate feature
validation
UDK2017 Highlights (Q1 2017)

**UEFI 2.6 Features**
- eMMC/SD Stack
- MemoryAttributesTable
- IPv6 HTTP Boot
- RamDisk
- URI Configuration

**UEFI PI 1.4a Errata**

**EDK II Implementation**
- OpenSSL 1.0.2h
- Transition to NASM
- CPU MP init library
Why is firmware so important?

TianoCore - UEFI Open Source Community
It’s not really about building standards …
It’s about building infrastructure
Tacoma Narrows Bridge
Seriously, "rock stars" are arrogant narcissists. Plumbers keep us all from getting cholera. Build functional infrastructure. Be a plumber.

The Blue Collar Coder

Much of the conversation about the shortage of technology talent in the United States focuses on how we can encourage more young people to go to college to become Computer Science graduates. Those programs are admirable and should be encouraged, but I suggest we need to focus on some other key areas in order to encourage the sustainability of our tech industry:

- Education which teaches mid-level programming as a skilled trade, suitable for apprenticeship and advancement in a way that parallels traditional trade skills like HVAC or welding
- Less of a focus on "the next Zuckerberg", in favor of encouraging solid middle-class tech jobs that may be entrepreneurial, but are primarily focused on creating and maintaining technology infrastructure in non-tech companies
“FIRMWARE ISN’T SEXY. IT’S PLUMBING.

Me (just now)
BUT OUR PRINCESS IS IN ANOTHER CASTLE!
Like plumbing, firmware works best as a solid, standardized framework.

“FIRMWARE ISN’T SEXY. IT’S PLUMBING.”
So ... In Summary ...
So ... In Summary ...

1. TianoCore is making UEFI more open
2. We want your contributions to EDK II
3. It’s OK to be a plumber *(most of the time)*