TianoCore, the Open Source UEFI Community

Spring 2017 UEFI Seminar and Plugfest
March 27 - 31, 2017
Presented by Brian Richardson (Intel)
Agenda

- Why is Firmware Important?
- Introducing tianocore.org
- Organization & Workflow
- Key Features & Changes
Why is Firmware Important?

TianoCore - UEFI Open Source Community

Why is Firmware Important?
Why is Firmware Important?
(“why you don’t want other people messing with your product firmware”)

• First code to execute at boot …
  – Initialize the hardware
  – Establish root-of-trust
  – Hand-off to the operating system

• Commonly known as “BIOS”
  – Basic Input Output System

• Critical part of digital infrastructure
Why is Firmware Important?

(“why you don’t want other people messing with your product firmware”)

- Initialize hardware
- Establish root-of-trust
- Hand-off to the OS

UEFI Plugfest – March 2017
Why is Firmware Important?

(“why you don’t want other people messing with your product firmware”)
Improving on BIOS concepts

**The Good**
- Abstraction for the OS/app layer
- Add-in cards carry 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?”

Depiction of Brian’s five year career as an assembly programmer
Hackers find a new place to hide rootkits

A pair of security researchers has developed a new kind of rootkit, called an SSM, that hides in an obscure part of the processor that is invisible to antivirus apps.

Lenovo ThinkPwn UEFI exploit also affects products from other vendors

The same critical vulnerability was found in the firmware of an HP laptop and several Gigabyte motherboards.
Standards Are Important

... otherwise this might happen
TianoCore, the Open Source UEFI Community

Introducing tianocore.org
Supporting EDK II, a BSD open source UEFI implementation, since 2004

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
Latest UEFI 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
TianoCore - UEFI Open Source Community

Organization & Workflow
Workflow – based on git

EDK II [http://www.tianocore.org/edk2/](http://www.tianocore.org/edk2/)

- 19,943 commits
- 8 branches
- 0 releases
- 105 contributors

- 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
Platforms

• Usable example code
  – Simplifies validation
  – Greater visibility for impact of changes

• Simulator platforms
  – OVMF (for QEMU)

• Cheap, public platforms
  – MinnowBoard Turbot
  – Intel® Galileo
  – More in the pipeline
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
bugzilla.tianocore.org

- For core/platform issues & requests
- Security issues follow a special process
  https://github.com/tianocore/tianocore.git
  hub.io/wiki/Reporting-Security-Issues
  - Never use e-mail to discuss a security issue
  - Use Bugzilla (“Tianocore Security Issues”)
  - Never use e-mail to discuss a security issue!
TianoCore - UEFI Open Source Community

Key Features & Changes
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 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

### EDK II OVMF x64

<table>
<thead>
<tr>
<th>Release Mode</th>
<th>GCC5</th>
<th>CLANG38</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEIFV</td>
<td>26%</td>
<td>-15%</td>
</tr>
<tr>
<td>DXEFV</td>
<td>4%</td>
<td>-4%</td>
</tr>
<tr>
<td>FvMainCompact</td>
<td>2%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Intel® Galileo IA32

<table>
<thead>
<tr>
<th>Release Mode</th>
<th>GCC5</th>
<th>CLANG38</th>
</tr>
</thead>
<tbody>
<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>
Plans for the future

• Improve website structure and content, including wiki & gitbooks
• Added open test cases for edk2
  https://github.com/tianocore/edk2-staging/tree/edk2-test
• More emphasis on open platforms
  https://github.com/tianocore/edk2-platforms
• Releases on a regular cadence
Summary

• Firmware is critical to today’s digital infrastructure
• TianoCore supports open source UEFI development using EDK II
• Recent improvements include a move to github and compiler optimizations
• Future improvements will improve code quality and open platform availability
Thanks for attending the Spring 2017 UEFI Seminar and Plugfest

For more information on the UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

* tianocore