Ubuntu with UEFI and Hardware Enablement
December 8th 2011

Alex Hung
BIOS Engineer, Hardware Enablement
Agenda

- UEFI Introduction
- Ubuntu's UEFI Readiness
- Firmware Test Suite
UEFI Introduction
UEFI - Unified Extensible Firmware Interface

- UEFI is an interface between the operating system (OS) and the system firmware (BIOS).
- UEFI intends to replace the “legacy BIOS”.
- UEFI provides boot-time and runtime services - a standard environment for booting an OS.
- UEFI is a pure interface specification. Common implementation includes:
  - Intel EDK2 (Tiano)
  - AMI’s Aptio
  - Phoenix SecureCore
  - Insyde H20
UEFI's Advantages

Faster Boot Time

UEFI can only execute necessary (UEFI) drivers to speed up the boot time.
UEFI's Advantages

Support for Larger Disk Size

UEFI defines GPT (GUID Partition Table). Traditional MBR supports up to 2.2TB, and the we have reached the limit today.

- Support GPT
- Supports up to 9.4 ZB ($2^{73}$ bytes).
UEFI's Advantages

Processor Compatibility

Legacy BIOS is limited to 16-bit mode and 1 MB of memory address.

UEFI defines the CPU modes before handing off the power to OS.

- Protected Mode
- 128 KiB, or more, of available stack space
- Preserve memory for runtime services
- Etc...
UEFI Services

UEFI define a common boot environment abstraction for use by loaded UEFI images, including UEFI drivers, UEFI applications, and OS loaders.

- Boot-time services
- Runtime services
UEFI's Advantages

UEFI Shell

A shell environment for efi applications (i.e. grub.efi or firmware update utilities).

- Pre-boot environment.
- DOS replacement.
- Standard functions (Boot-time and Runtime services) for application development.
### UEFI's Advantages

#### UEFI Driver Model

UEFI defines the driver model that is CPU-independent.

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Simplify the design and implementation of device drivers</td>
</tr>
<tr>
<td>✔️</td>
<td>Produce small executable image sizes</td>
</tr>
<tr>
<td>✔️</td>
<td>Define CPU-independent environment (EFI Byte Code - EBC)</td>
</tr>
</tbody>
</table>
Ubuntu's UEFI Readiness
Ubuntu's UEFI Readiness

What is the status of Ubuntu's UEFI supports?

UEFI will eventually replace traditional legacy BIOS. How are we doing with UEFI now?

- Boot Loader (grub.efi) is ready.
- GOP driver is supported with Grub 1.99
- Ubuntu (64-bit) can be installed.
- Ubuntu (64-bit) can run.
- Suspend/Resume passes(*).
- Hibernate/ Resume passes(*).
# Test Results from UEFI Plugfest

<table>
<thead>
<tr>
<th>Machine</th>
<th>UEFI Version</th>
<th>Boot</th>
<th>Video</th>
<th>S3</th>
<th>S4</th>
<th>S5</th>
<th>Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMD Opteron</td>
<td>EFI v2.31 by American Megatrends</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>N/A</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>TunnelMountain</td>
<td>EFI v2.30 by EDK II</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Sandy Bridge</td>
<td>EFI v2.31 by Phoenix Technologies Ltd.</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Sandy Bridge</td>
<td>EFI v2.31 by Phoenix Technologies Ltd.</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Ivy Bridge</td>
<td>EFI v2.10 by HPQ</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Sandy Bridge</td>
<td>EFI v2.10 by HPQ</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Centaur VIA Nano processor</td>
<td>EFI v2.31 by Insyde Corp.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Celpella</td>
<td>EFI v2.31 by Insyde Corp.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Intel Ivy Bridge</td>
<td>EFI v2.31 by Insyde Corp.</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Ubuntu's UEFI Readiness

- Ubuntu supports UEFI mode.
- Boot loader, grub.efi, supports GOP drivers.
- There are some systems fails to install/boot Ubuntu in UEFI mode (no problems in legacy mode).
- UEFI is complex and we keep working on it.
- There might be other bugs, but we will find them and fix them along the way.
Firmware Test Suite (fwts)
Firmware Test Suite (fwts)

What is fwts?

fwts is a Linux tool that automates firmware checking. It aims to detect bugs and to get firmware fixed.

- Automatically detect errors
- Sanity check core functionality
- Ensure interactions between Linux and firmware
- Catch kernel warnings
- Suggest possible workarounds
- Gather firmware data for debug
Firmware Test Suite (fwts)

Key features

Command line
- Designed to be used by other test tools
- ...or to be run stand alone
- ...and to gather data for a developer

Batch tests – run without supervision

Interactive tests – e.g. hotkey, lid, AC power.

Extensive logging
- Per test PASS/FAIL results
- Explain reasons for failures (ADVICE lines)
- Classify failures (CRITICAL, HIGH, LOW..)

Summarise results
- Output log format can be configured

Soak testing (suspend/resume, hibernate/resume)
Firmware Test Suite (fwts)

Case Studies – What errors can fwts detects?

DMI (SMBIOS) Checks:
Identify incorrect DMI data, ex. Invalid UUID.

ACPI Control Methods:
Check return data and identify missing methods (ex. _BQC).

CPU Features Disables:
Detect CPU virtualization disabled when CPU supports the feature.

ACPI table Checks:
Discover multiple instances of APIC/MADT tables.

Linux Log Scanning:
Eyeball the kernel log and detect and give advice when it finds firmware related errors or warnings, ex. EC time-out.

And so on...
Firmware Test Suite (fwts)

fwts Demonstration

Run all batch tests
  sudo fwts

Extract system information (acpi table, dmesg, dmi and lspci)
  sudo fwts -d

Run suspend/resume stress tests 10 times
  sudo fwts s3 --s3-device-check

Run suspend/resume tests with device check
  sudo fwts s3 --s3-device-check

and a lot more!
Firmware Test Suite Live (fwts-live)

What is fwts-live?
fwts-live is a bootable USB image that will boot and run the firmware test suite without the need to install Linux/Ubuntu. Results of the tests are saved on the USB drive to be analysed later.

- No Installation necessary
- Easy to use
- Release with latest Ubuntu
Firmware Test Suite Live (fwts-live)

- Insert USB with fwts-live.
- Boot-up and load fwts-live
Firmware Test Suite Live (fwts-live)

- Executing tests is only a few key strokes.
- Customizing tests is also easy.
Firmware Test Suite Live (fwts-live)

- On-screen shows the current test and overall progress.

Running Batch Tests
So far: 7 passed, 0 failed, 0 warnings, 3 aborted, 0 skipped, 1 info only
Test ACPI Wakealarm.
Running test #0: Multiple wakealarm firing tests.
Firmware Test Suite Live (fwts-live)

- The results will be saved to USB disk (named by date)
Firmware Test Suite Live (fwts-live)

- It can be viewed right away.
Firmware Test Suite

Looking for more information?

fwts:
https://wiki.ubuntu.com/Kernel/Reference/fwts

fwts-live:
https://wiki.ubuntu.com/HardwareEnablementTeam/Documentation/FirmwareTestSuiteLive
References

- UEFI Specification 2.3.1
- https://help.ubuntu.com/community/UEFIBooting
Thank you