Notebook Advancements for Unified Extensible Firmware Interface (UEFI) Pre-boot Productivity

Chenhao Xia, Technical Marketing Engineer, Intel
Kangkang Shen, Executive Vice President, Byosoft
Dong Wei, Distinguished Technologist, HP

EFIS002
Agenda

• Overview of UEFI Pre-Boot Applications
• UEFI-based HP Innovations for Notebooks
• Byosoft Innovations for UEFI Pre-boot
Agenda

• Overview of UEFI Pre-Boot Applications
• UEFI-based HP Innovations for Notebooks
• Byosoft Innovations for UEFI Pre-boot
What is an UEFI Application?

• An UEFI Loadable Image
  – Loaded by UEFI loader just like UEFI drivers
  – Does not register protocols like UEFI drivers do
  – Consumes protocols
  – Typically user driven (exits when task completed)
  – Same set of interfaces available as drivers have

• Can be used for
  – Platform diagnostics
  – Factory diagnostics
  – Utilities
  – Driver prototyping
  – ‘Platform’ applications
Boot Execution Time Line

Security (SEC) | Pre EFI Initialization (PEI) | Driver Execution Environment (DXE) | Boot Dev Select (BDS) | Transient System Load (TSL) | Run Time (RT)

Power on → [ . . Platform initialization . . ] → [ . . Pre -OS boot . . ] → Shutdown

Pre – Boot UEFI Applications
UEFI Pre-boot Application Execution

- Abstractly Extend the Firmware without hardware or OS dependence
- Portable across platform and processor architectures

Pre-Boot UEFI Applications Extend Firmware
Agenda

• Overview of UEFI Pre-Boot Applications

• UEFI-based HP Innovations for Notebooks

• Byosoft Innovations for UEFI Pre-boot
UEFI-based HP Innovations for Notebooks

Dong Wei – HP Distinguished Technologist
April 14, 2010
HP Innovations for Notebooks based on UEFI Technology

• HP Diagnostics
• HP QuickLook
• HP DayStarter

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.
Enhanced Diagnostics

- Based on the UEFI Technology
- DIMM fault isolation
- Hard drive simultaneous test
- Concurrent memory, hard drive and batteries test
- Improve test coverage, optimize test cycles

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.
HP QuickLook

- Technology that lets you access your Outlook data in seconds when your notebook is off
- With HP QuickLook 3, you can edit your e-mail, calendar, contacts and tasks
  - Automatically synchronized the next time you start your computer.
  - Boasts updated security features, can authenticate your identity using the same password or fingerprint reader you use to log on to Microsoft® Windows®.
  - Can specify the frequency at which data is captured, the type of data that is captured (e-mail, calendar, contacts and tasks), and the range of data that is captured.

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.
WORK FASTER AND SIMPLIFY YOUR LIFE WITH HP QUICKLOOK 3.

Three-month rolling calendar
Current time and date
E-mail, calendar, contact and task creation and editing

Easy navigation
It's easy to access and edit information with HP QuickLook 3. When you push the HP QuickLook button, the Today page opens. It displays a three-month calendar, upcoming calendar events and your active tasks, along with the current date and time. You can then use intuitive icons to navigate to and edit more detailed information, including e-mail messages, calendar entries, contacts and tasks.
HP DayStarter

- Integral part of HP QuickLook 3.2 and above
- A new feature on the new HP commercial EliteBook and ProBook notebooks (selected models at first launch)
- Allow user to personalized information while the computer is booting

- Displays the following information:
  - Calendar summary
  - Battery icon
  - Windows status
  - Pause and escape buttons

- Supported in the HP Mobile Framework UEFI Codebase

See eWeek DayStarter Article:

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.
OutLook Plugins for HP QuickLook

HP QuickLook icons

When HP QuickLook is installed, the icons shown and described in the following table are displayed on the Outlook toolbar.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Configures HP QuickLook preferences.</td>
</tr>
<tr>
<td>📌</td>
<td>Manually initiates HP QuickLook information capture.</td>
</tr>
<tr>
<td>📌</td>
<td>Configures HP DayStarter preferences.</td>
</tr>
<tr>
<td>📌</td>
<td>HP DayStarter icon</td>
</tr>
</tbody>
</table>

Setting HP DayStarter preferences

To select HP DayStarter preferences, follow these steps:

1. Click the HP DayStarter icon on the Outlook toolbar.
2. The following note is displayed:
   - **NOTE:** Activation of HP DayStarter displays JPEG based images during system startup. These images may include personal calendar and event details that could be seen by other users of this system in a multi-user environment.
3. Click Yes.
4. Select the 12-hour calendar time period to be displayed when the computer restarts.
5. To save your changes, click OK.

UEFI enables faster and easier innovations

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.
Agenda

• Overview of UEFI Pre-Boot Applications
• UEFI-based HP Innovations for Notebooks
• Byosoft Innovations for UEFI Pre-boot
UEFI Pre-boot Application Development

- Use EDK/EDKII as development kit
- Development process as same as UEFI drivers
- Use UEFI Boot Services to implement functions
- Rich libraries support
  - EDK/EDKII libs
  - Other vendors, Byosoft GUI, Security libs
- Use “C” as main development language
  - Engineers pool is cheaper
  - Reuse C source code resource

Easy To Develop – Byosoft
Byosoft UEFI Pre-boot Application Examples

• Manufacture Tool
  – Ghost-like Tool
  – Flash Tool
  – Hide partition Tool

• Security Application
  – Pre-boot Anti-virus

• Value-Added
  – Pre-boot AD

• Debug Utility
  – UEFI Handle Dump
  – Driver Stack Dump
  – PCI/Memory Space Dump

• DOS Replacement Tool
  – HDD Partition
  – File management

Rich Pre-boot Applications Accumulation – Byosoft
UEFI Pre-boot Application - Build Description File

Set MODULE_TYPE in your module’s .INF file to UEFI_APPLICATION.

[Defines]
INF_VERSION = 0x00010005
BASE_NAME = MyApplication
FILE_GUID = 10C75C00-30
MODULE_TYPE = UEFI_APPLICATION
VERSION_STRING = 1.0
ENTRY_POINT = MyApplicationMain

This will cause the build tool to generate an UEFI Application image.
UEFI Pre-boot Application Development - Tips

- The UEFI Application runs on a UEFI Task Priority set at TPL_APPLICATION, which is the lowest priority. It may be interrupted by some DXE drivers.
- Do NOT use any of PI defined protocols because PI is only designed to be used by UEFI firmware itself.
- If you are implementing an OS loader, DO NOT call any of UEFI boot services after the ExitBootServices function is invoked.
- Always allocate memory which is boot service attribute.
- By default the DXE dispatcher will not dispatch this type of module.
Byosoft Pre-boot Innovation: Pre-boot AD

- Great Innovation in UEFI pre-boot applications
  - Play video and audio during system boot
    - Can be used to show advertisement, animation and other user selected video to bring great user experiences in notebook systems
  - User customizable
    - Provide edit utility to change the pre-boot video
- Integrated into Byosoft desktop and mobile product line
- Implemented as a set of UEFI pre-boot applications
  - Pre-boot Decoder
  - Pre-boot video player
- Support various multimedia formats
  - Native support AVI format
  - Provide video format convert tool support more multimedia formats

A Great Place to Innovate – Byosoft
Byosoft UEFI Pre-boot Example
Pre-boot AD Technology Cont.

PC boot Comparison
With Pre-boot AD VS Without Pre-boot AD
Summary

• UEFI leaves ample room for pre-boot applications
• Leading notebook provider HP has taken advantage of UEFI and delivered pre-boot applications on its new models
• UEFI technology is maturing and ready to use, but the room for innovation is unlimited.
• IBVs have worked on UEFI for many years and their year’s accumulation can be utilized by you right now.
Next Steps

• Using UEFI environment to host your pre-boot applications
• Differentiate your mobile products through UEFI pre-boot applications
• Contact Intel and IBVs for off the shelf pre-boot applications
• Contact IBVs for customized pre-boot applications
  kshen@byosoft.com.cn

UEFI enables faster and easier innovations
Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Whitepaper: “Installing UEFI-based Microsoft Windows Vista SP1* (x64) on HP EliteBook and Compaq Notebook PCs” on www.hp.com
- UEFI Plugfest Event at Intel in Dupont Washington, June 22-25, 2010 www.uefi.org or email: laurie.jarlstrom@intel.com
**IDF 2010 UEFI Spring Sessions**  
**April 14**

<table>
<thead>
<tr>
<th>EFI#</th>
<th>Company</th>
<th>Description</th>
<th>Time</th>
<th>RM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S001</td>
<td>Intel, IBM, HP</td>
<td>Using the Latest EFI Development Kit (EDK II) for UEFI Advanced Development and Innovation</td>
<td>11:10</td>
<td>302AB</td>
</tr>
<tr>
<td>S002</td>
<td>Intel, HP, Byosoft</td>
<td>Notebook Advancements for Unified Extensible Firmware Interface (UEFI) for Pre-boot Productivity</td>
<td>13:00</td>
<td>302AB</td>
</tr>
<tr>
<td>S003</td>
<td>Intel, Byosoft</td>
<td>Unified Extensible Firmware Interface (UEFI): Best Platform Security Practices</td>
<td>14:00</td>
<td>302AB</td>
</tr>
<tr>
<td>S004</td>
<td>Intel, Microsoft, Insyde</td>
<td>UEFI Fast Boot for Microsoft* Windows* 7 : Fast Boot Without Compromising your BIOS</td>
<td>15:00</td>
<td>302AB</td>
</tr>
<tr>
<td>S005</td>
<td>Intel, Inspur, Insyde</td>
<td>UEFI Firmware Solutions for Enterprise Servers: A Case Study in 8-way Processor Support</td>
<td>16:00</td>
<td>302AB</td>
</tr>
</tbody>
</table>

DONE
Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide
Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events
Q&A
Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.
- Intel, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
- Copyright © 2010 Intel Corporation.
Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel’s actual results, and variances from Intel’s current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation’s expectations.

Demand could be different from Intel’s expectations due to factors including changes in business and economic conditions; customer acceptance of Intel’s and competitors’ products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers.

Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast.

Additionally, Intel is in the process of transitioning to its next generation of products on 32nm process technology, and there could be execution issues associated with these changes, including product defects and errata along with lower than anticipated manufacturing yields.

Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel’s products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel’s response to such actions; defects or disruptions in the supply of materials or resources; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; product mix and pricing; start-up costs, including costs associated with the new 32nm process technology; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; the timing and execution of the manufacturing ramp and associated costs; and capacity utilization; Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel’s products and the level of revenue and profits. The majority of our non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management’s plans with respect to our investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other.

Intel’s results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates.

Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting our ability to design our products, or requiring other remedies such as compulsory licensing of intellectual property.

A detailed discussion of these and other risk factors that could affect Intel’s results is included in Intel’s SEC filings, including the report on Form 10-Q.

Rev. 1/14/10