Plug-Ins: Added value for PCs
June 22, 2010

Dick Wilkins, Office of the CTO
Agenda

- Plug-Ins! Past, Present, and Future
- UEFI is Making BIOS Plug-Ins Possible!
- Plug-In Examples
- Taking Plug-Ins to the Next Level
- Call to Action
Plug-Ins: Added Value for PCs

- Plug-Ins are added value for PCs installed by:
  - The OEM
  - The End User

- What plug-ins do we use today?
  - For MP3 players, it’s earphones, power supplies, etc.
  - For PDAs & Smart Phones, it’s app store software
  - For PCs, plug-ins extend functionality too
Plug-Ins: Added Value for PCs

- **OEM Plug-Ins:**
  - Likely to exist in source code form
  - Require technical integration into the BIOS in some way (source, adaptation, etc.)
  - Integrated as part of system test

- **User Plug-Ins:**
  - Need seamless binary installation
  - Lots of issues (security, storage, configuration, compatibility, etc.)
  - Must just work without any “system test” on the user’s part
Plug-Ins: Added Value for PCs

- In the legacy BIOS days, plug-ins made hardware operational—ROM BIOS extensions (OpROMs)
- Today’s add value is less about new hardware options, and more about other things:
  - Virus/Malware Protection
  - Enterprise Management
  - OS Installation
  - Geo-Fencing
  - Instant-On environments
  - Diagnostics
Plug-Ins Past and Present

Today’s computing is trending towards enclosed systems with limited hardware expansion

1981-1989
Expansion via hardware plug-ins (i.e. LAN, Modem, Graphics)

1990-1999
Expansion via standards (USB, PCI)
Early Notebooks with limited expansion
Connectivity: Network, Internet

2000-2009
Accelerated Transition to Mobility
(Notebooks, Netbooks, PDAs, etc.)
Limited Expansion: Closed Systems

©Phoenix Technologies Ltd.
What forces are driving plug-ins now?

- **2010**: UEFI Notebooks: SW Door Opens
  - 2008-2009: Steady growth in UEFI adoption
  - 2010*: Broad adoption of UEFI: ~>50% notebooks shipped

- **2012**: Form Factor Mobile UEFI Adoption
  - i.e. PDAs, Mobile Phones, MP3 players, etc.

* Source, UEFI Forum
** Source, Phoenix Technologies
What forces are driving plug-ins down the road?

- 2015*: The Cloud: Unlimited storage and services
- 2015*: The Grid: Unlimited computing power
- 2020*: Shift from “press this to cause the device to do that” to peer interaction with the device

* Source, Phoenix Technologies
- Focus on Mobile Devices
- All new systems shipping with some form of UEFI
- Phoenix creating UEFI solutions for all new silicon solutions
- Green H: Formal packaging of executable entities, run-order, flow control
  - Does away with hooking and patching
### Green H/UEFI Transforms Plug-Ins

#### Legacy

<table>
<thead>
<tr>
<th>Category</th>
<th>Legacy Services</th>
<th>UEFI Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Allocation</td>
<td><img src="image" alt="BDA Editing" /> <img src="image" alt="INT 15h" /></td>
<td><img src="image" alt="Allocate Pages" /> <img src="image" alt="Allocate Memory" /></td>
</tr>
<tr>
<td>I/O to Screen</td>
<td><img src="image" alt="INT 10h/INT 16h" /> <img src="image" alt="Painting video memory" /></td>
<td><img src="image" alt="ConIn/ConOut handles" /></td>
</tr>
<tr>
<td>Hotkeys</td>
<td><img src="image" alt="Hook INT 09h, INT 08h, INT 1ch" /></td>
<td><img src="image" alt="Hotkey protocols" /></td>
</tr>
<tr>
<td>Security</td>
<td><img src="image" alt="None" /></td>
<td><img src="image" alt="Well Defined Protocols" /></td>
</tr>
<tr>
<td>Configuration</td>
<td>!<a href="image">^S to enter special setup program in ROM</a></td>
<td><img src="image" alt="Human Interface (HII) Protocols" /></td>
</tr>
<tr>
<td>Packaging</td>
<td><img src="image" alt="ROM extension on PC card" /></td>
<td><img src="image" alt="UEFI DXE Driver" /> <img src="image" alt="UEFI Application" /></td>
</tr>
</tbody>
</table>

**UEFI offers Standard services & Interfaces vs. ad-hoc legacy implementation**
Plug-In Examples

- **SecureGuard**
  - Plug-in to anchor critical software components to a PC device
  - Provides tamper protection and trust from root
  - BIOS can insert and up-sell after-market solutions (simple as presenting and offer or as complex as download and install of an application)
  - Windows agent works with BIOS plug-in to trigger actions or behaviors

- **ServiceMeter**
  - Carriers like Verizon, AT&T and Vodafone are offering subsidized netbook and slate PCs with their 2.5G and 3G plans.
  - Carriers need the ability to address account delinquency for PC devices and discontinue the wireless service and disable the system for delinquent accounts
  - ServiceMeter is a BIOS plug-in and Windows service that converts a standard netbook PC or slate PC into a subscription-based metered device
Taking Plug-Ins to the Next Level

- Preparation for transition from OEM “Push” to End User “Pull” in the market
- Solve User-Level problems, not OEM problems
- Make Mobile Systems Plug-In Friendly (OEM/ODMs)
  - Need to create concept vehicles
- Make Tools that are Plug-In Friendly (IBVs)
  - Create SDKs for ODMs and OEMs
  - Create SDKs for Plug-In Makers
  - Development environment that abstracts the complexities of BIOS from the Plug-In makers

  i.e., You don’t need Windows source code to create a Windows application
Taking Plug-Ins to the Next Level

- IBVs to collaborate with UEFI forum and define a path to move to binary distribution (i.e. app store level)

- All IBVs will have their own ideas

Phoenix is working on:
- Installation – Installer
- Discovery – Defining firmware volume assignments for plug-In storage
- Compatibility – UI form and function
- Storage – Read/Write firmware volume assignments and QoS for data storage
- Isolation – Adding protection around apps for security and reliability
- Performance – One second POST
- Power Management – Best practices for maximizing battery life
- Configuration – Best practices to simplify user experience
Plug-Ins are going to take off, as the role of the BIOS/Pre-Boot is standardized and stabilized

Importance of Plug-Ins will increase
- Allows for differentiation and expandability in otherwise closed systems

IBVs, ODMs, OEMs, and SVs will pave the way for plug-In manufacturers to add value:
- First at the source code level as they sell to OEMs
- Finally at the binary level as end users install their own plug-ins
Questions?

Dick Wilkins
dick_wilkins@phoenix.com