Hardware assisted Virtualization in Embedded

Tanveer Alam
Platform Architect – Embedded Virtualization

Sponsored by:

& CITRIX
Agenda

- Embedded Virtualization
  - What is embedded?
  - Embedded specific requirements
  - Key Embedded Use Cases
  - Hardware Virtualization Features Review

- Embedded Virtualization and Retail/Digital Signage—OS Soft Failover Proof-of-Concept Example

- Embedded Virtualization and Medical—Critical OS Isolation Proof-of-Concept Example

- Call to Action
Embedded Virtualization

Industrial

Medical

Energy

Retail

Automotive
Technical requirements for Embedded Virtualization

- Smaller code base – lesser points of failure
- Highly robust and reliable
- Remote management
- Certification
- Legacy code
- Consolidation + Critical function isolation/partitioning
- Real time
- Easy and fast to implement – “turnkey”
Embedded Virtualization Usage Models

Legacy OS Consolidation

- Legacy OS (Single threaded: RTOS e.g. VxWorks)
- Legacy OS (Single threaded: RTOS e.g. VxWorks)
- Guest OS

Thin Hypervisor

- VT-x & VT-d enabled Multi-Core Intel® Architecture

RTOS & GPOS Consolidation

- Linux* X-windows
- MS Windows*
- API
- Real Time Kernel
- Real Time Process

Hypervisor

- CPU 0
- CPU 1
- NIC
- Chipset
- VT-x & VT-d enabled Multi-Core Intel® Architecture

Trusted/Open Application Integration

- Media (Phone, Video) Application
- Embedded OS with GUI, calendar, voice mail, games etc.

Thin Hypervisor

- CPU 0
- CPU 1
- Antenna
- VT-x & VT-d enabled Multi-Core Intel Architecture

Performance-Critical Application Separation

- Modified NetBSD* SMP kernel
- IP Stack Changes
- User Space
- Standard NetBSD

Hypervisor

- CPU 0
- CPU 1
- NIC
- Chipset
- VT-x & VT-d enabled Multi-Core Intel Architecture

Notes:
- "Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture VT-x" and "Intel® Virtualization Technology (Intel® VT) for Directed I/O VT-d" are trademarks or registered trademarks of Intel Corporation.
- Other names and brands may be claimed as the property of others.

Copyright © 2010, Intel Corporation
Extended Page Tables (EPT)

Virtual Processor ID (VPID)

Preemption Timer / Pause Loop Exit

VT-d I/O Virtualization
- DMA remap
- PCIe pass-through
- Interrupt remap
Virtualization in Embedded: Soft Failover Proof-of-Concept
Virtualization in Embedded: Soft Failover

- Automatic System Recovery
- Real-time task pointer tracking and resume
- Requires No Network Connectivity
- Preserve Critical Data and State
Virtualization in Embedded: Soft Failover

- Xen DomU (P)
- Xen DomU (B)
- Primary VM
- Backup VM
- Blue Screen
- Recover
- Windows 7
- Intel® Embedded Virtualization Manager
- Intel® Platform
- Intel Platform with Intel® vPro™ technology
- Samba
- Xen Dom0 Host OS
- Heartbeat Mon daemon
- VGA Passthrough
## Virtualization in Embedded: Soft Failover

### Specifications:

<table>
<thead>
<tr>
<th>Software</th>
<th>Rev/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Kernel</td>
<td>2.6.32.26</td>
</tr>
<tr>
<td>Fedora</td>
<td>14 (64 bits)</td>
</tr>
<tr>
<td>Xen pvops</td>
<td>4.1</td>
</tr>
<tr>
<td>Video Player</td>
<td>Ryarc</td>
</tr>
<tr>
<td>File Share</td>
<td>Samba</td>
</tr>
</tbody>
</table>
Virtualization in Embedded: Medical Proof-of-Concept
Virtualization in Embedded: Critical Path Isolation (Medical)

CPU Utilization

Running Processes

- Windows
- Linux/RTOS
Virtualization in Embedded
Call to Action

- Few Embedded Challenges: real-time, simpler Dom0, fast path interVM comms

- Open to developing similar creative ideas using Xen and open source in the embedded domains.

- Explore Xen community collaboration possibilities to enable better embedded practical solutions.
## References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® HD Graphics Driver</td>
<td><a href="http://support.intel.com">http://support.intel.com</a></td>
</tr>
<tr>
<td>Xen how-to guide</td>
<td><a href="http://wiki.xensource.com">http://wiki.xensource.com</a></td>
</tr>
<tr>
<td>Xen VGA pass-through (using Intel® VT-d)</td>
<td><a href="http://wiki.xensource.com/xenwiki/XenPClpassthrough">http://wiki.xensource.com/xenwiki/XenPClpassthrough</a></td>
</tr>
<tr>
<td>Xen PCI pass-through (using Intel® VT-d)</td>
<td><a href="http://wiki.xensource.com/xenwiki/XenVGAPassthrough">http://wiki.xensource.com/xenwiki/XenVGAPassthrough</a></td>
</tr>
<tr>
<td>Intel Embedded Developer Site</td>
<td><a href="http://edc.intel.com">http://edc.intel.com</a></td>
</tr>
</tbody>
</table>