Intel® Virtualization Technology [VT]

Sunil Saxena
Intel Corporation
INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. 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 MAY MAKE CHANGES TO SPECIFICATIONS, PRODUCT DESCRIPTIONS, AND PLANS AT ANY TIME, WITHOUT NOTICE.

ALL DATES PROVIDED ARE SUBJECT TO CHANGE WITHOUT NOTICE.
Scope of this Session

- Intel® Virtualization Technology (VT)
  - Challenges of IA CPU virtualization today
  - VT closes virtualization holes by design
  - VT-x Technical Overview
  - Intel® LaGrande Technology (LT)
  - VT-i Technical Overview
  - Status / Plans Xen with VT

- VT Roadmap

- Additional Resources
Challenges of Running a VMM

OS and Apps in a VM don’t know that the VMM exists or that they share CPU resources with other VMs.

VMM should isolate Guest SW stacks from one another.

VMM should run protected from all Guest software.

VMM should present a virtual platform interface to Guest SW.
**SW Solution: Guest Ring Deprivileging**

Run Guest OS above Ring-0 and have privileged instructions generate faults...

Run VMM in Ring-0 as a collection of fault handlers

Top IA Virtualization Holes:
- Ring Aliasing
- Non-trapping instructions
- Excessive Faulting
- Interrupt Virtualization Issues
- CPU state context switching
- Addr Space Compression

Sophisticated Software Techniques:
- Source guest OS Modifications
- Binary guest OS Modifications

Current IA CPUs require sophisticated software techniques
Guest SW runs deprivileged in a new operating mode:
- Apps run deprivilegated in ring 3
- OS runs deprivilegated in ring 0
- VMM runs in new mode with full privilege

VMM preempts execution of Guest OS via new HW-based transition mechanism

By design, VT closes virtualization holes and the need for complex software workarounds
VM Entry and VM Exit

• VM Entry
  – Transition from VMM to Guest
  – Enters VMX non-root operation
  – Loads Guest state and Exit criteria from VMCS
  – `VMLAUNCH` instruction used on initial entry
  – `VMRESUME` instruction used on subsequent entries

• VM Exit
  – `VMEXIT` instruction used on transition from Guest to VMM
  – Enters VMX root operation
  – Saves Guest state in VMCS
  – Loads VMM state from VMCS
VT-x Operations

VMX Non-root Operation

VMX Root Operation

Build Foil

VM Exit

VM CS 1

VM CS 2

VM CS n

Ring 0

Ring 3

Ring 0

Ring 3

Ring 0

Ring 3

Ring 0

Ring 0

*Third party marks and brands are the property of their respective owners
LaGrande Technology* (LT)

LT builds on Intel® Virtualization Technology

Protected Execution Environments
(Protected Launch, DMA Protections)

Protected Key Operations & Sealed Storage

Protected Data Paths
(Keyboard, Mouse, Graphics)

LT interoperates with an enabled OS to better defend against software based attacks

*Third party marks and brands are the property of their respective owners
Itanium® Virtualization VT-i

Virtualization-supported CPU

Host Virtual Address

Privileged Resources

Non-privileged Resources

Guest Software (Virtualized)

Host Software/ VMM

Processor Status Register

PSR.vm=1

PSR.vm=0

Intercepts

• TLB Accesses
• Privileged Registers (PSR, Control, Debug)
• Register Stack Engine (RSE)
Intel® Virtualization Technology and Xen

Enhanced Xen capability with Legacy Linux support
Status/Plans – Xen with VT

• Completed Xen 3.0 items
  – 32-bit VT, UP Linux guest, UP host
  – 64-bit xenolinux and 32-bit VT domain

• Additional items for Xen 3.0
  – 64-bit VT domain, PCI/IOAPIC/ACPI in domain 0, guest FW, para-virtualized drivers, xenolinux in VT domain

• Plan for Xen 4.0
  – Performance Optimization, SMP guests, Windows guest, Security, Management
VT Client Roadmap

2005 Lyndon
Intel® Pentium® 4 Processor
945G Chipset
HT, XD, EM64T, EIST, Intel AMT, VT

2006 Averill
Intel Pentium 4 Processor & DC
Broadwater Chipset
2005 features plus Intel AMT2, LT

2006 Napa
Mobile Dual Core Processor code-named “Yonah”
Chipset code-named “Calistoga”
Wireless LAN solution code-named “Golan”
XD, EIST, VT, Intel AMT
VT Server Roadmap

2005 - 2006
Millington / DP Montvale
Intel® 8870, Enabled
Dual Core, MT, Foxton, Pellston, VT

2005 - 2006
Montecito / Montvale
Intel® 8870 / Enabled
MT, Foxton, Pellston, VT

2006 Bensley, Glidewell
Dempsey
Blackford & Greencreek
2005 features plus VT, IAMT, I/OAT

Copyright Intel Corporation
Third party marks and brands are the property of their respective owners.
Additional Resources

• For specs / whitepapers / web resources:
  WWW.INTEL.COM/TECHNOLOGY/VT

• For discussions on VT:
  Sunil.Saxena@Intel.Com
Thank You