Chapter 4

# Overview of Intel® vPro™ Technology

*Computers are useless. They can only give you answers.*

—Pablo Picasso (1881–1973)

Intel® vPro™ technology is a collection of high performance, energy efficient, and robust out-of-band management capabilities that enable IT professionals to monitor, manage, and repair computers remotely, regardless of operating system health or computer power state. The same techniques that have been used to lower the cost of ownership and power use, and to increase the reliability and security of large servers, are built into platforms with the Intel vPro technology.

Intel vPro technology is more than Intel Active Management Technology (Intel AMT). While Intel AMT is the main focus of this book, computers marked with the Intel vPro technology brand include a dual core 64-bit processor or better, gigabit Ethernet, RAID controller for storage speed and reliability, Wake-on-LAN, and power saving features such an Ethernet adapter capable of dropping to lower speeds when the computer is sleeping. All these features allow IT professionals to identify platforms that meet the manageability and security requirements of today's business computing.

## Intel® vPro™ Technology Value Vectors

Manageability, security, and energy-efficient performance are three key value vectors of Intel vPro technology.

The manageability capabilities embedded in the platform with Intel vPro technology allow the IT system administrator to carry out manageability operations like collecting system inventory and asset information, detecting the act of disabling of critical system software like virus scanners by malware or the users, remotely diagnosing and repairing issues with software or firmware on the platform. Having this capability embedded in the hardware allows the IT system administrator to perform these actions remotely, irrespective of the state of operating system or the system power state, and thereby considerably reducing the number of desk side visits.

For home users, Intel vPro technology means that they can press a Help button (or a key sequence) when they need support, rather than making a phone call. PCs can "phone home" for help or for regular maintenance even if located outside the firewall.

The security benefits for platforms with Intel vPro technology lie in the capabilities to detect and isolate infected systems from the network to prevent the infection from spreading. Once isolated, the infected systems can be placed on a quarantined network allowing the IT system operator to remotely repair and update the critical security agents. Platforms with Intel vPro technology can automatically run heuristics to determine if the system is infected, take policy-based actions to automatically isolate them from the network and notify the IT system administrator.

System hardware can take part in network authentication even prior to start of the operating system, allowing administrators to be sure that their network access protections are in place before allowing systems on the network.

Intel vPro technology provides hardware-based data encryption capabilities providing the end users protection from theft.

While providing the manageability and security benefits, Intel vPro technology provides energy efficiency in core silicon and other hardware components, leading to reduced power consumption and longer battery life. Additional remote power control operations allow systems to stay longer on standby power while maintaining emergency contact with the remote system

administrator. In certain areas of the world (such as Japan) and specific installations (such as schools) people like to turn the systems off in the evening and turn them on in the morning. Providing a way to do this in an automated fashion helps in saving power.

## Intel® vPro™ Technology Ingredients

In this chapter, we look at the overall capabilities of platforms equipped with Intel vPro technology and how these capabilities are exposed through standards-based interfaces, which allows a wide variety of management applications to use them. This open architecture allows greater interoperability and provides flexibility to IT systems administrators to deploy manageability and security solutions.

### Intel® Core™2 Processor with Intel vPro™ Technology

The Intel Core™2 Quad processor or Intel Core2 Duo processor (or later versions as the products evolve) are essential parts of the Intel vPro technology ingredients. These are built on Enhanced Intel Core microarchitecture. The 45-nm technology used in these processors brings higher performance and lower power usage than the previous generations with up to a 12 MB L2 cache and a 1333 MHz Front Side Bus. These processors include several technologies that are essential to deliver many of the capabilities of Intel vPro technology.

Enhanced Intel SpeedStep® technology brings a unique combination of power-optimized performance. This technology allows automatic switchover from high performance mode to power-optimized mode by adjusting the processor speed and voltage as the system is switched from AC power to battery power. The smooth transitions make it completely transparent to the operating system and the user. Furthermore, the power adjustments are done on a per-core basis to further enhance efficiency.

Processor features support Intel Virtualization Technology (Intel VT) and Intel Trusted Execution Technology (Intel TXT) to bring unique benefits for creating secure virtual partitions. We describe these features in more detail later in this chapter.

New Intel Streaming SIMD Extensions 4 (Intel SSE4) instructions bring improved performance for multimedia and graphics and enhanced video

encode and decode capabilities. Intel SSE4 brings over 50 new instructions to the IA instruction set. The general concept behind these instructions is to combine certain common operations into one smooth operation: rather than a series of *multiple* instructions required for, say, discovering the dot product of two vectors, Intel SSE4 provides one dedicated instruction. Intel SSE4 reduces complex operations into native instructions, and this can greatly improve the efficiency of the processor in certain applications. Most of the new instructions are related to vector operations, which are the core of graphics and multimedia processing. Also included are primitives that increase the speed of streaming and improves access to device memory.

### Chipsets

The Intel Q45 Express Chipset and Intel Q43 Express Chipset (and later versions as the products evolve) work in conjunction with Intel Core 2 processors to provide key parts of the ingredients in Intel vPro technology. Intel AMT is the heart of these capabilities delivered by these chipsets and is the main focus of this book.

Intel Anti-Theft Technology allows encryption of user data and makes sure that the data cannot be retrieved if the system is stolen. Statistics indicate that thieves are usually after the data rather than the system itself, and the thief is less likely to steal a system if he knows that the data is locked.

Intel Matrix Storage Technology provides the reliability and performance for building RAID solutions.

Integrated DVI and display port as well as dual independent digital displays provide enhanced graphics performance and usability and productivity.

### Gigabit Ethernet

In addition to the obvious speed and performance benefits of Gigabit Ethernet, an additional capability that the Intel Gigabit Ethernet controller brings is the packet filtering. There are two types of filters. One type, Out-of-Band filter, allows delivering the manageability traffic received from the network to the manageability engine. This capability allows Intel AMT to be connected over the network to the IT system administrator at all times irrespective of the state of the host operating system. The other type of filter allows Intel AMT to create policies to detect certain anomalous network

patterns, thereby detecting a condition such as outbreak of a network worm. In such conditions an Ethernet controller can be instructed to stop all or some of the traffic going to or from the host. These packet filters in the Integrated Gigabit Ethernet controller are key elements of the network security capabilities provided by the Intel AMT technology. This capability is discussed more in detail in later chapters.

### Wireless Networking

Faster wireless networking with 802.11n in Intel Centrino® platforms provides high throughput connectivity options for multiple environments. It provides flexibility to connect to wireless home network and public wireless LAN hotspots located in airports, hotels, restaurants, and coffee shops around the world. Intel AMT capabilities are accessible via wireless networks in the same way as through the wired LAN. TCO filters in the wireless controller work the same way as described above.

### Platform BIOS

Platform BIOS is an important ingredient that enables the features in the processors and chipsets. The BIOS has been used traditionally on desktop and mobile client platforms to configure and enable key platform features for use by the operating system. On some platforms, a management controller can directly configure certain features and provide an interface to the user to set a configuration parameter.

In platforms with Intel vPro technology, the BIOS must be able to enable and configure the following capabilities such that they can be used by the operating system and applications:

- Intel® Virtualization Technology
- Intel® Trusted Execution Technology and the Intel® Trusted Platform Module
- Intel® Active Management Technology

### Software Applications

Software applications which use Intel AMT are another important part of managing platforms with Intel vPro technology. The capabilities of Intel vPro technology are exposed using standards-based interfaces allowing easy interoperability and integration with wide variety of manageability and security solutions. Intel has done significant work in collaborating with independent software vendors (ISVs) to create the ISV manageability ecosystem.

## Key Intel® vPro™ Technologies

Three key set of ingredient technologies are fundamental to Intel vPro technology: Intel Active Management Technology (Intel AMT), Intel Virtualization Technology (Intel VT) and Intel Trusted Execution Technology (Intel TXT).

Out of these three, Intel AMT is the most user-visible and it is described further in the remainder of the book. The following sections provide an overview of Intel VT and Intel TXT.

### Intel® Virtualization Technology

Intel Virtualization Technology provides hardware support that simplifies processor virtualization, enabling reductions in virtual machine monitor (VMM) software size and complexity. Resulting VMMs can support a wider range of legacy and future operating systems on the same physical platform while maintaining high performance.

To understand the concepts of Intel VT, let's first briefly understand the challenges associated with virtualizing the processor. In order to virtualize the processor, the VMM needs to:

- Protect itself from the guest operating system and applications
- Isolate guest operating systems from each other
- Present a virtual platform to the guest operating system

To achieve this, the VMM must be able to control and virtualize the CPU, memory, and devices on the platform. This requires the VMM to be executing as the most-privileged software on the processor. Intel processors provide protection based on the concept of a privilege level, using 0 for most-

privileged software and 3 for least-privileged. The privilege level determines whether privileged instructions, which control basic CPU functionality, can execute without fault. It also controls address-space accessibility based on the configuration of the processor's page tables and segment registers.

For an OS to control the CPU, some of its components must run with privilege level 0. Because a VMM cannot allow a guest OS such control, a guest OS cannot execute at privilege level 0. Thus, VMMs must use ring de-privileging, a technique that runs all guest software at a privilege level less than 0 (numerically greater).

However, since the guest OS is not written to run at this privilege level, it introduces inefficiencies and security problems. A number of Intel Architecture (IA) instructions like LAR, LSL, SIDT, and CPUID when executed at lower-privilege rings (rather than ring 0 as intended) do not fault. Hence the VMM, even though running at ring 0, cannot intercept and virtualize them. In order to effectively switch the context between multiple guest operating systems, the VMM needs mechanisms to save and restore the processor state. Some of the IA processor state, like the hidden segment states, cannot be easily saved and restored. Additionally, executing operating systems in higher privilege levels can lead to excessive and un-necessary faulting leading to inefficient execution. Numerous problems, such as interrupt virtualization, inefficient transitions back and forth from VMM to guest OS, and so on, make this software approach problematic.

To address the virtualization challenges VMM designers developed creative techniques for modifying guest software (source or binary). The source-level modifications technique is called paravirtualization. Developers of these VMMs modify the source code of a guest OS to create an interface that is easier to virtualize. Paravirtualization offers high performance and does not require changes to guest applications. A disadvantage of paravirtualization is that it limits the range of supported operating systems. VMMs that rely on paravirtualization cannot support an OS whose source code the VMM's developers have not modified.

A VMM can support unmodified operating systems by transforming guest-OS binaries on-the-fly to handle virtualization-sensitive operations. Such VMMs support a broader range of operating systems than VMMs that use paravirtualization.

Intel VT eliminates the need for CPU paravirtualization and binary translation techniques, simplifying the implementation of robust VMMs that can support a broad range of unmodified guest operating systems while maintaining high levels of performance.

Intel VT consists of two main components. Intel VT for IA-32 Intel Architecture (Intel VT-x) provides processor extensions for CPU virtualization, and Intel VT for Directed I/O (Intel VT-d) provides processor extensions for device virtualization.

Intel VT-x augments IA-32 with two new modes of CPU operation: VMX root mode intended for use by a VMM and VMX non-root mode intended for guests' virtual machines. Both modes of operation support all four privilege levels, allowing guest software to run at its intended privilege level, and providing a VMM with the flexibility to use multiple privilege levels.

Intel VT-x defines two new transitions: a transition from VMX root operation to VMX non-root operation is called a VM entry, and a transition from VMX non-root operation to VMX root operation is called a VM exit. VM entries and VM exits are managed by a new data structure called the virtual-machine control structure (VMCS). The VMCS includes a guest-state area and a host-state area, each of which contains fields corresponding to different components of processor state. VM entries load processor state from the guest-state area. VM exits save processor state to the guest-state area and then load processor state from the host-state area.

Processor operation is changed substantially in VMX non-root operation. An important change is that many instructions and events cause VM exits. Some instructions, such as INVD, cause VM exits unconditionally when executed in VMX non-root operation. Other instructions, such as INVLPG, can be configured to cause VM exits conditionally using VM-execution control fields in the VMCS.

VM entry and VM exit provide an efficient way of switching the context from a VMM to a guest and back. The result is better performance without sacrificing the security while running unmodified guest OS.

Intel VT-d extends Intel VT to include support for I/O device virtualization. It is important to have protected access to I/O resources from a given virtual machine (VM), such that it cannot interfere with the operation of another VM on the same platform. This isolation between VMs is essential

for achieving availability, reliability, and trust. The second major requirement is the ability to share I/O resources among multiple VMs. In many cases, it is not practical or cost-effective to replicate I/O resources (such as storage or network controllers) for each VM on a given platform.

In the case of the enterprise client, virtualization can be used to create a self-contained operating environment, or *virtual appliance*, that is dedicated to capabilities such as manageability or security. These capabilities generally need protected and secure access to a network device to communicate with down-the-wire management agents and to monitor network traffic for security threats. For example, a security agent within a VM requires protected access to the actual network controller hardware. This agent can then intelligently examine network traffic for malicious payloads or suspected intrusion attempts before the network packets are passed to the guest OS, where user applications might be affected.

The virtualization of I/O resources is an important evolution of usage models in the data center, the enterprise, and the home. VT-d support on Intel platforms provides the capability to ensure improved isolation of I/O resources for greater reliability, security, and availability.

To help with this, Intel VT-d supports the remapping of I/O DMA transfers and device-generated interrupts. The architecture of Intel VT-d provides the flexibility to support multiple usage models that may run unmodified, special-purpose, or virtualization-aware guest operating systems. The Intel VT-d hardware capabilities for I/O virtualization complement the existing Intel VT capability to virtualize processor and memory resources. Together, this offers a complete solution to provide full hardware support for the virtualization of Intel platforms.

Readers who need more information on Intel VT will be interested in the book *Applied Virtualization Technology* By Sean Campbell and Michael Jeronimo (Intel Press 2006)

### Intel® Trusted Execution Technology

Intel Trusted Execution Technology (Intel TXT) is a hardware extension that is intended to provide users and enterprises with a higher level of trusted platform while accessing, modifying, or creating sensitive data and code. It is useful as a way to defend against software-based attacks aimed at stealing sensitive information.

Intel TXT consists of a series of hardware enhancements that allow for the creation of multiple separated execution environments, or partitions. One critical component is the Intel® Trusted Platform Module (Intel® TPM), which allows for secure key generation and storage, and authenticated access to data encrypted by this key. The private key stored in the Intel TPM is not available to the owner of the machine, and never leaves the chip. Intel TXT comprises of the following capabilities.

The processor allows creation of a segregated private environment for applications, so that the hardware resources (such as memory pools) are locked to the calling applications and cannot be accessed by any other process running on the platform.

User input paths (keyboard, mouse) are protected, allowing users to interact with trusted platform applications without the risk of their inputs being observed or modified by other software. Secure display interface enables trusted platform applications to send display data securely on output devices without the risk of their output being observed or modified by other software.

The Intel TPM allows the system administrator to configure a launch control policy and in conjunction with the Intel TXT allows the performance of a measured and verified launch of the system software. The Intel TPM also provides secure storage and sealing for keying material and other secrets such that the secrets are made available to only trusted applications. The Intel TXT and Intel TPM can be used to securely record various system measurements and provide trusted attestation of the system status.

Thus Intel TXT capability helps reduce IT support costs with improved services, enables decentralized or remote computing, and verifies platform configuration with a higher level of assurance.

Intel TXT allows local or remote verification of the platform state. Local verification uses the measurement capability of Intel TXT to allow the local user to have confidence that the platform is executing in a known state. The confidence comes from the hardware ability of Intel TXT to properly measure the launched configuration and store the measurement in the Intel TPM. Remote verification takes the measurements obtained by Intel TXT and stored in the Intel TPM, and uses the Intel TPM to inform remote entities (those not executing on the platform) about the current platform

configuration. The essence of this use model is that the remote entity can rely on the protective properties of Intel TXT.

Readers who need more information on Intel TXT will be interested in the book *Dynamics of a Trusted Platform: A building block approach* by David Grawrock (Intel Press 2009).

## Summary

Intel vPro technology provides manageability, security, and energy efficient computing capabilities using technologies like Intel AMT, Intel VT and Intel TXT. A number of ingredients in the platforms, such as CPU, chipset, LAN, and BIOS work together to provide the capabilities of Intel vPro technology. The rest of the book focuses on Intel AMT and the ingredients that are specifically used in delivering these capabilities.