Intel® Technologies for Information Assurance

For the first time, the military and government agencies can build on the significant investments of the enterprise sector to establish a cost-effective commercial off-the-shelf (COTS) computing foundation for classified information.

Mission-critical and high-value data faces continuous threats ranging from espionage, malicious hackers, and unauthorized internal access to viruses, worms, blue-pill malware and back-door attacks. The need for effective data isolation, multi-user access and information assurance is greater than ever.

Historically, information assurance computing systems – those with advanced data protection techniques supporting multiple and simultaneous independent levels of security – were highly complex and expensive. These systems were often based on purpose-built hardware and operating systems.

Now there is a cost-effective alternative. Intel® processors and chipsets, together with validated third-party hardware ingredients and software solutions, enable information assurance computing systems based on COTS solutions. These systems promise to be far more cost effective to develop, validate and support than legacy systems, while preventing the compromise of data security.

Intel® Virtualization Technology[1] (Intel® VT) and Intel® Trusted Execution Technology[2] (Intel® TXT) are the key technologies which enable Multi-Level Security (MLS) while improving system performance, robustness, security and trust.

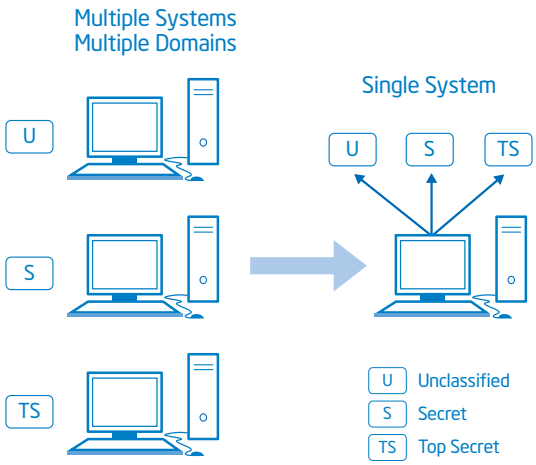

Figure 1. Simplifying information assurance: replacing multiple systems with multiple domains on a single system

Intel® Virtualization Technology (Intel® VT)

Intel® VT enables multiple independent operating systems and applications to share system resources in a controlled manner. Discrete applications and operating systems run independently in protected, isolated environments. A third-party trusted separation kernel, or hypervisor layer, creates and manages these independent "virtual machines," each running in a separate security domain. Intel VT has the additional benefit of enabling simple and small hypervisors.

Figure 2 shows how Intel VT enables multiple security domains on a single system. "Top Secret," "Secret" and "Unclassified" domains each have their own "guest" operating system and applications.

The separation kernel controls how the separate domains share system resources, assigning processor cores, separate I/O devices and protected areas of physical memory to each domain.

Hardware-assisted virtualization helps reduce the size and complexity of the separation kernel, which facilitates safety and security certification processes and also enables near-native performance of guest applications and operating systems. It can also be used to create a backup partition so that applications can be updated and run there, while keeping the previous configuration intact in the event a fall-back is required.

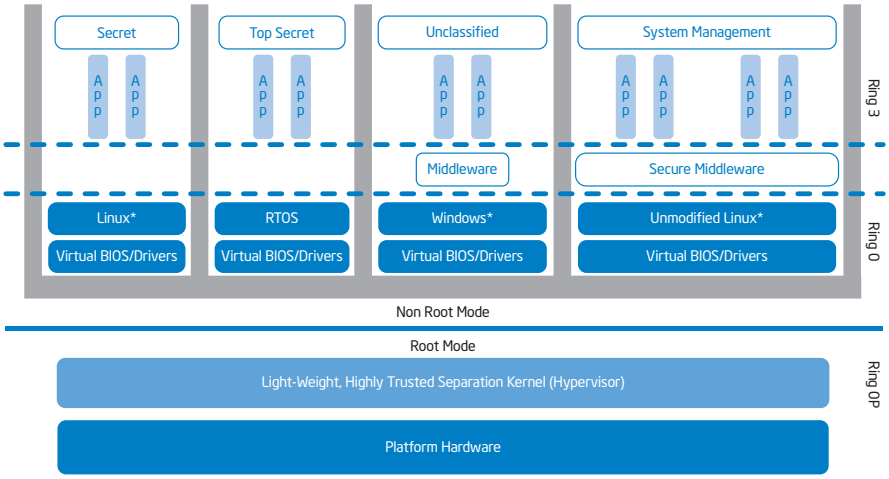

Figure 2. Examine multi-level security architecture using Intel® Virtualization Technology

Intel® Trusted Execution Technology (Intel® TXT)

Intel® TXT and third-party Trusted Platform Management (TPM) silicon provide the hardware-hardened framework that enables a system's hardware and software to be trusted, by ensuring that the system's hardware and software elements have not been tampered with. The TPM silicon provides sealed storage for encryption keys, software measurements and configuration policies to enable hardware and software lockdown.

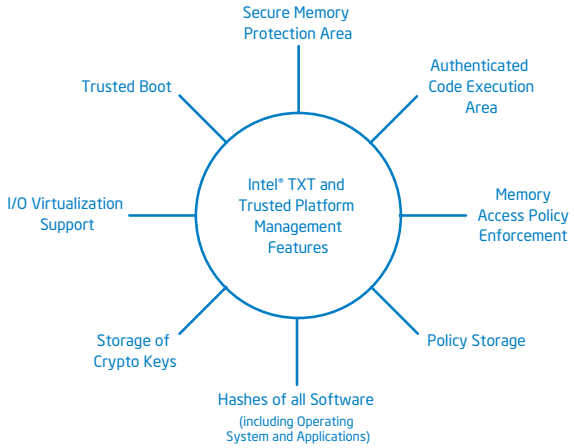

Figure 3. Intel® TXT and Trusted Platform Management features

Reduce platform complexity and cost

Intel's information assurance technologies replace complex and expensive multiple purpose-built computers, communications hardware and operating systems with standard COTS platforms built using standard tools. This greatly reduces the cost to develop and support trusted systems.

The framework provides the foundation for several use cases that enable security and trust, including the ability to:

- Replace discrete "Unclassified," "Secret," and "Top Secret" systems with multiple security domains on a single system and limit individual user access to authorized domains
- Isolate systems management from applications to allow for software updates and fail-over mechanisms
- Simplify development efforts to meet safety-critical and high-assurance evaluations
- Increase trust and assurance through onboard integrity measurement, key storage and memory and bus protection

Ecosystem support

Intel is engaging with our customers and with a broad ecosystem of third-party vendors to enable complete information assurance platform solutions for military, aerospace and government applications. We assist our customers by facilitating platform certification in compliance with the requirements of the Department of Defense, NIST, NSA and other agencies.

Intel helps our customers meet the challenges of long-term spiral technology insertion with technologies and products that combine industry-leading technologies, embedded lifecycle support and cost efficiency.

The following are some of the companies that provide separation kernel or Virtual Machine Monitor software components which enable the implementation of information assurance technologies:

Green Hills

INTEGRITY PC*
www.ghs.com/integritypc

LynuxWorks

LynxSecure Separation Kernel
www.lynuxworks.com/rtos/secure-rtos-kernel.php

VirtualLogix

VirtualLogix VLX Real-Time Virtualization* for Connected Devices
www.VirtualLogix.com

Learn more

For more information, visit www.intel.com/go/military or contact your Intel representative. To find an Intel representative visit www.intel.com/buy/networking/design.htm

[1]Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, Virtual Machine Monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[2]No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible Measured Launched Environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security.

Printed in USA 0907/LS/OCG/XX/PDF ♻ Please Recycle 318386-001US