Technology Overview

Intel® Trusted Execution Technology

Introduction

Intel® Trusted Execution Technology[†] (Intel® TXT), formally code-named LaGrande, is a highly versatile set of hardware extensions to Intel® processors and chipsets that, with appropriate software, enhance the platform security capabilities. Trusted Execution Technology will provide a hardware-based security foundation that will help enable greater levels of protection for information stored, processed and exchanged on the PC. For the PC industry, Intel Trusted Execution Technology creates a new value category in addition to traditional performance improvements.

Intel® Trusted Execution Technology

Designed to help protect against software-based attacks, Intel Trusted Execution Technology integrates new security features and capabilities into the processor, chipset and other platform components. The hardware rooted security enables the ability to increase the confidentiality and integrity of sensitive information from software-based attacks, protect sensitive information without compromising the usability of the platform, and deliver increased security in platform-level solutions through measurement and protection capabilities. It provides a general-purpose safer computing environment capable of running a wide variety of operating systems and applications. When used in conjunction with Intel® Virtualization Technology,[A] Intel Trusted Execution Technology provides hardware rooted trust in which a chain of trust for your execution environment can be built upon.

Intel Trusted Execution Technology capabilities include:

- Protected execution and memory spaces where sensitive data can be processed out of view of any other software.
- Sealed storage shields encryption keys and other data from attack while in use or stored.
- Attestation enables a system to provide assurance that it has correctly invoked the Intel Trusted Execution Technology environment, as well as enable a verified measurement of the software running in the protected space.
- Measured launch capability to help:
  - Reduce IT support costs with improved services
  - Enable decentralized or remote computing
  - Verify platform configuration with a higher level of assurance
- Memory protection to help:
  - Enhance protection of system resources
  - Increase confidentiality and integrity of data
  - Improve assurance of data transfers and resources
  - Improve protection of sensitive information

These Intel Trusted Execution Technology capabilities enable more secure platforms to address the increasing frequency and sophistication of software-based attacks.

Benefits of Trusted Execution Technology

Three use models can help illustrate the flexibility and benefits of Trusted Execution Technology. The use models are

- Local verification
- Remote verification
- Multi-level operation

Local Verification

Local verification uses the measurement capability of Trusted Execution Technology 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 Trusted Execution Technology to properly measure the launched configuration and store the measurement in the platform Trusted Platform Module (TPM).

Remote Verification

Remote verification takes the measurements obtained by Trusted Execution Technology and stored in the TPM, and uses the TPM to inform remote (not executing on the platform) entities about the current platform configuration. Of essence in this use model is that the remote entity can rely on the properties of Trusted Execution Technology to provide the protections listed above.

Multi-level Operation

Multi-level operation takes advantage of the memory protections provided by Trusted Execution Technology to run two or more applications or operating systems that require strict separation and managed communication between the entities. Those wishing to rely on these properties make use of either local or remote verification to ensure that the proper environment is setup and executing.

Intel Trusted Execution Technology Privacy and Policy

Intel recognizes that many aspects of successful policy implementation depend on software and hardware development from third-party providers whose implementations are outside Intel's direct control. Intel believes adherence to these or equivalent policies is critical to delivering the full benefits of Intel Trusted Execution Technology and other complementary security technologies, and will vigorously encourage our fellow travelers in the industry to internalize and implement these policies. For details on these policies visit http://www.intel.com/technology/security.

Summary and Plans

A Technology Enabling Platform (TEP) began shipping in 2006 and is available directly from an OEM. TEP includes TXT capabilities for the purpose of enabling the developer and security community to innovate and build ecosystem momentum towards more secure solutions.

This Technology Enabling Platform is a production-level platform with Intel Trusted Execution Technology capabilities for the security community to evaluate and innovate new platform-level solutions. The TEP is a hardware, BIOS and Authenticated Module solution to enable the ecosystem community to provide more secure platform solutions.

TXT in Client Intel® vPro™ processor technology-based platforms in 2007

Intel Trusted Execution Technology will extend to the broader security community targeted at enterprise, government, finance, banking, insurance, health care, and academia. In 2007, a select number of desktop Intel vPro processor technology-based platforms will include both the Intel Trusted Execution Technology and the Intel® Virtualization Technology for Directed I/O (Intel® VT-d). This will enable developers and the security community to begin delivering higher levels of system security and information assurance into PC computing solutions.

In addition to the protection provided by current software solutions, Intel Trusted Execution Technology-enabled solutions provide hardware-based mechanisms that help protect against software-based attacks and protect the confidentiality and integrity of data stored or created on the client PC. It does this by enabling an environment where applications can run within their own space, protected from all other software on the system. These capabilities provide the protection to mechanisms, rooted in hardware, that are necessary to provide trust in the application's execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform.

Throughout 2008 and 2009, Intel will continue to expand delivery of Intel TXT and Intel VT into Intel's next generation of mobile, server and embedded processors and chipsets.

Also available is the Intel® Safer Computing Initiative book. This book covers the fundamentals of Intel's Trusted Execution Technology and key Trusted Computing concepts such as security architecture, cryptography, trusted computer base, and trusted channels.

For more information on Intel Trusted Execution Technology, visit http://www.Intel.com/technology/security

[1] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology is a security technology under development by Intel and requires for operation a computer system with Intel® Virtualization Technology, an Intel Trusted Execution Technology-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel or other compatible measured virtual machine monitor. In addition, Intel Trusted Execution Technology requires the system to contain a TPMv1.2 as defined by the Trusted Computing Group and specific software for some uses. See http://www.intel.com/technology/security/ for more information.

[Δ] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform 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.

Printed in USA 0907/JAN/OCG/XX/PDF ♻ Please Recycle 325415-004US