

Creating a Secure Computing Environment

Hardware-based security features further protect against software-based attacks

Malicious software infiltrates a target system’s hardware and software resources and wreaks havoc by accessing sensitive information, stealing identities or committing other illegal actions. While anti-virus, encryption, firewall and other security products offer protection, these software solutions can be neutralized by malware that’s running at the same or higher privilege levels.

What are privilege levels? They are a hardware-based security hierarchy supported by Intel® processors, where the highest level has access to everything – all system memory and instructions – and the lower levels have limited access. This feature prevents critical software, like operating systems, from getting compromised by software running in lower privilege levels. Extending this hierarchy, Intel® Virtualization Technology¹ (Intel® VT) establishes a new high privilege level for deploying virtual machine monitors (VMMs), which provide even greater protection for operating systems and applications. As a result, software executing in a virtualized environment benefits from additional hardware-based protection designed to protect against malware or intrusion.

Trusted Execution Technology

Designed to help protect against software-based attacks, Intel® Trusted Execution Technology² (Intel® TXT) integrates new security capabilities into the processor, chipset and other platform components. These hardware-based security features, unalterable by rogue software, run mission-critical applications in a safe partition, protect crucial platform data and keep malware from launching in the first place:

- **Protected execution:** Runs critical applications in a virtualized, protected environment, which employs the highest processor privilege level.
- **Sealed storage:** Encrypts and stores system secrets, like VPN security keys, safely within the trusted platform module (TPM), which is a secure cryptoprocessor.
- **Protected launch:** Ensures all system software components are in a known state, referred to as “trusted,” before launching. This is accomplished with three mechanisms, as illustrated in Figure 1.

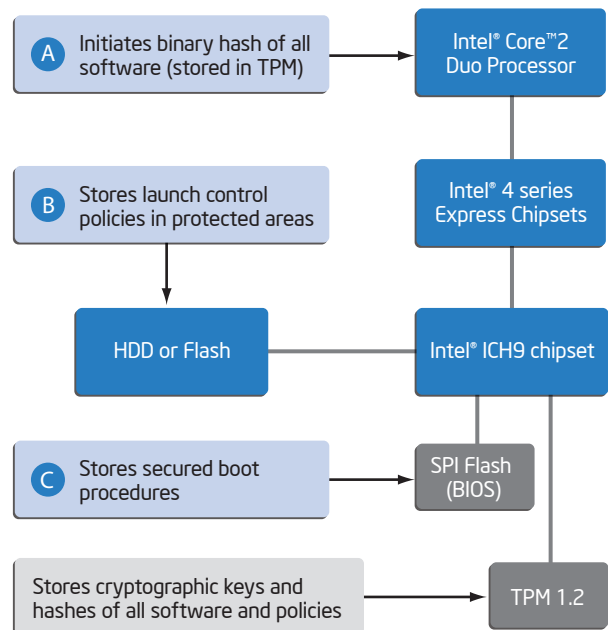


Figure 1. Protected Launch Mechanisms

- The processor executes new SMX (Safer Mode Extensions) instructions, which generate a binary hash (a number generated by a formula) of all system software, including operating systems, applications and VMMs. The hash is performed in a secure area of the processor and the results are stored in the TPM. The new hash values are verified with the previous values before any software is allowed to start execution, thus preventing system tampering.
- Launch control policies (LCP) define the trusted platform elements. The policies are written by the OEM or VAR and reside in a protected region on the hard disk drive. A hash of the LCP, stored in the TPM, is verified during system boot. Additional LCPs can be created by the system administrator.
- A BIOS authentication code module, consisting of signed binaries from Intel, is stored in the BIOS and helps secure the boot procedure.

Addressing Common Security Issues

Based on hardware-rooted security features, Intel TXT creates an additional layer of software and data protection and detects when a system deviates from its trusted state using hashing and verification functions. Some of the key features and benefits of Intel TXT are listed in Table 1. Intel TXT addresses many common security situations without sacrificing platform usability, as described in the next three sections.

Protect Critical Software from Malware

Cybercriminals looking to profit from reading and modifying sensitive information, like bank records, manufacturing recipes and military secrets, seek to breach application software and databases. Using Intel TXT, OEMs can put software and data out of reach of hackers by running applications, operating systems and VMMs in the highest privilege level, permission granted only by system developers. As a result, application code and data are stored in hardware-secured memory regions, inaccessible to malware. OEMs and system administrators can define a list of trusted, validated software, and only applications or device drivers on this list can be loaded.

Stop Unauthorized Access of Data

Spoofing and phishing – when a system or program masquerades as another – are fraudulent activities used to gain access to confidential information. Helping to prevent these attacks, Intel TXT provides sealed storage in the TPM for security codes, like VPN encryption keys, which keeps perpetrators from intercepting secured communications links. Intel TXT encrypts and stores critical security codes and ensures they are only released (decrypted) to the executing environment that originally encrypted them.

Features	Benefits
Protected execution environment	Safeguards critical applications and data
Encrypted keys and secrets (e.g., platform configuration registers)	Eliminates potential security holes
Launch control policies	Stops compromised systems from booting
Measured launch environment	Prevents execution of untrusted software

Table 1. Intel® Trusted Execution Technology (Intel® TXT) Features and Benefits

Prevent Booting a Compromised System

Compromised systems, possibly infected with a virus or connected to an illegal peripheral, need to be deactivated before they can cause harm. One solution is to stop these systems from booting whenever the software or hardware configuration differs from the trusted state. This is achievable with Intel TXT, which compares the hash of the trusted state with the current state and blocks system startup when differences are detected.

Deploying Intel® Trusted Execution Technology

Intel TXT is enabled by a number of hardware and software components, which are listed in Table 2. The hardware components comprise Intel TXT-enabled processors, chipsets and TPMs, such as the latest Intel® Core™2 Duo processors, the Intel® 4 Series Express chipsets and TCG 1.2-compliant TPMs. The software components include an Intel-approved BIOS, authentication code modules available from Intel and a VMM with Intel TXT support.

For more information on Intel Trusted Execution Technology, visit www.intel.com/technology/advanced_comm.

Additional information about Intel® embedded products can be found at www.intel.com/products/embedded/index.htm.

Intel® Trusted Execution Technology (Intel® TXT) Components

	Required Capability
Processor	Support for Intel® SMX instructions
Chipset	Intel TXT enabled
TPM Chip	TCG 1.2 compliant to the extent required by Intel
BIOS	From list of Intel-approved BIOS vendors
Authenticated Code Modules (ACMs)	BIOS ACM and System Initialization (SINIT) ACM
Measured Launch Environment (MLE)	An MLE can be implemented with a VMM available from software vendors, such as Green Hills, LynuxWorks, Citrix, Wind River and others

Table 2. Required Intel® Trusted Execution Technology (Intel® TXT) Components

¹Intel® 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.

²No 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>.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit Intel Performance Benchmark Limitations.

Copyright © 2009 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Core are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

