

Intel® Trusted Execution Technology

Hardware-based Technology for Enhancing Server Platform Security

Executive Summary

A building is only as good as its foundation. The same is true for a computer architecture's information security. In an age where security breaches in IT infrastructure are increasingly common front page news, it's imperative that organizations use the most secure building blocks for the foundations of their IT solutions. This is of growing importance today, as IT managers are being asked to evolve their data centers into new and more demanding uses that challenge existing security practices. For example, as the data center gets increasingly virtualized, high-value or highly sensitive workloads from different lines of business will be shared across common physical infrastructure. Where traditional physical isolation is no longer possible a more trusted infrastructure is the key to maintaining the high assurance and control required to meet the security needs in the data center. The increased interest in cloud computing will only further emphasize the need for more visibility into the security status of workloads and systems and new control capabilities to meet compliance mandates.

This paper describes a highly scalable architecture called Intel® Trusted Execution Technology (Intel® TXT) that provides hardware-based security technologies to help build a solid foundation for security.¹ Built into Intel's silicon, these technologies address the increasing and evolving security threats across physical and virtual infrastructures by complementing runtime protections such as anti-virus software. Intel TXT also can play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification useful in compliance efforts.

Intel TXT is specifically designed to harden platforms from the emerging threats of hypervisor attacks, BIOS, or other firmware attacks, malicious root kit installations, or other software-based attacks. It increases protection by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual Machine Extensions (VMX) environment of Intel® Virtualization Technology (Intel® VT), permitting a verifiably secure installation, launch, and use of a hypervisor or operating system (OS).

Intel TXT gives IT and security organizations important enhancements to help ensure more secure platforms; greater application, data, or virtual machine (VM) isolation; and improved security or compliance audit capabilities. Not only can it help reduce support and remediation costs, but it can also provide a foundation for more advanced solutions as security needs change to support increasingly virtualized or "multi-tenant" shared data center resources. This paper describes the basic uses of Intel TXT, the core components, how they operate, and critical enabling requirements for the technology in server implementations.

Table of Contents

Executive Summary	1
The Threats to Data Keep Growing	2
Root of Trust: A Foundation for Safer Computing	3
Intel® TXT: From Client to Server	3
How Intel TXT Works	3
Additional Usage Models	4
How to Get There: Intel TXT Components	5
Details: Establishing a Root of Trust with Intel TXT for Servers	6
Enabling Intel TXT	7
Summary	8
Additional Resources	8

The Threats to Data Keep Growing

Attacks on IT infrastructure continue to grow in volume, complexity, sophistication, and stealth. According to the McAfee Threat Report of 2Q 2012, “the number of new unique malicious code and other unwanted programs grew by over 8 million samples between the first and second quarter of 2012 alone.”² These include a growing number of nasty, sophisticated rootkits, with more than a 100,000 new rootkit variants discovered in each of the last 14 quarters. For another opinion on the matter of growth, consider that a few years ago, Kaspersky Lab forecast a 10-fold increase in malicious programs, from 2.2 million to 20 million in 2008.³ This was far from exaggeration. The specialists at Kaspersky Lab detected the 25 millionth malicious program and added it to the company’s anti-virus databases in June 2009.⁴ Today, the experts at McAfee are expecting the identification of the 100 millionth malware sample some time in 3Q 2012. Clearly, the malware tide is rising unabated.

Awareness of the dangers malicious threats pose to modern societies’ information and communications infrastructure has reached the top levels of government and industry leadership. In a 2009 speech, U.S. President Barack Obama noted, “It’s the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy.”⁵ Security experts consulted by Georgia Tech Information Security Center (GTISC) believe cyber warfare will accompany traditional military interaction more often in the years ahead.⁶ Organized crime is also involved. Cybercrime is so profitable for organized crime that they use it to fund other underground exploits, and U.S. law enforcement is reaching around the world in an attempt to reel it in.⁷ Other new threats appear daily from social networking sites, Web mashups (integrated applications or content from web sites that can contain viruses),

drive-by downloads, virtualization attacks, and a growing number of other sources. More frightening still, creating a malicious program is possible without any significant programming skills.⁸ Nearly anyone can do it thanks to an increased availability of prepackaged “kits” that allow for the easy definition, manipulation, and deployment of malware.

Servers are a particularly alluring target. For instance, in 2012 alone hackers have breached server systems at Yahoo, LinkedIn, and Sony with hundreds of thousands of records jeopardized.⁹ 2012 also saw breaches in the servers at the University of Rhode Island, University of Maine, University of North Florida, University of Nebraska, and other academic institutions.¹⁰ And it is not only academia that is at risk. Payment processing facilities, storage facilities, medical records providers, enterprises, and even government entities have also been compromised in recent times. Hundreds of thousands of records have been exposed, and control over facilities has been jeopardized.¹¹ While the details from such breaches will continue to emerge, the basic trend—sophisticated, orchestrated, and highly targeted attacks—is alarming. Unfortunately, there are far too many such breaches of equal significance to report here.

Making matters worse, the cost of a data breach is daunting. The average organizational costs of a data breach in the United States remained a stubbornly high USD 5.5 million in 2011,¹² with lost business as the largest percentage of this cost. According to the same study, the cost on a per-record basis is a challenging USD 194 per record—so a large-scale breach can be very damaging. In 2012 Global Payments, a U.S.-based payment processing firm, cited costs of USD 84.8 million related to a recent data breach.¹³ It’s no wonder that according to a 2012 study by FTI Consulting and Corporate Boardroom both Corporate Directors and General Counsel cited

Data Security as their top concern.¹⁴

The growth of low-level attacks is also a major motivator behind the U.S. National Institute of Standards and Technologies (NIST) to create new guidelines to focus on addressing vulnerabilities in BIOS and other key system firmware.¹⁵

The result is that security considerations can play a significant role in hindering the way that companies can use technology to expand or improve the efficiency of their operations, and new solutions are needed.

Root of Trust: A Foundation for Safer Computing

The penalties and costs for lost or compromised customer, employee, or financial data make it imperative that IT managers not lose control of their systems. This means they must implement the best tools available for protecting their infrastructure and validating the integrity of the computing environment on an ongoing basis. Establishing a root of trust is essential. Each server must have a component that will always behave in the expected manner and contain a minimum set of functions enabling a description of the platform characteristics and its trustworthiness.

The power of Intel® Trusted Execution Technology (Intel® TXT) is establishing this root of trust that provides the necessary underpinnings for successful evaluation of the computing platform and its protection.¹ The root is optimally small and difficult to defeat or alter, and allows for flexibility and extensibility to measure platform components in the boot and launch environment (such as BIOS, OS Loader, and Virtual Machine Managers (VMMs)). The root also provides a trusted, tamper-resistant position to evaluate the integrity of any other components, enabling assurance through a secure comparison against expected measurements. By allowing such comparisons during the boot and launch sequence, IT managers can stop the launch of unrecognized software and enforce “known good” launch-time configurations.

Once a basic root of trust and a secure basis for measurement and evaluation are established, it is possible to further extend these capabilities and the technologies that enable them. For example, to protect other aspects of the system, mechanisms can be created to seal and protect secrets in memory, as well as provide local or remote attestation (proof) of system configuration.

Intel® TXT: From Client to Server

Initially delivered to market with Intel® vPro™ technology-based client platforms in 2007, Intel TXT has been extended to mobile platforms as well. Because servers hold a variety of personal, financial, governmental, and other data, and are under increased attack, it was imperative to expand this multi-layered protection approach into the server infrastructure. With the advent of cloud computing and consolidated virtualized data centers, the potential harm from a single successful attack has increased dramatically, particularly in edge-of-the-network servers such as web servers, portals, and smaller databases.

Intel TXT on servers was launched with the 2010 introduction of the Intel® Xeon® processor 5600 series systems. Hardened for server environments (particularly virtual server environments), Intel TXT helps enable IT managers to provide higher levels of system security and information assurance in enterprise computing architectures. Through hardware-based technologies such as Intel TXT—and other Intel security technologies built into selected server platforms—Intel is setting an industry benchmark for secure processing in data centers. These building blocks will facilitate better regulatory compliance and increase the security and availability of infrastructures by addressing the ever-growing security threats across physical and virtual infrastructures.

How Intel TXT Works

Intel TXT works by creating a Measured Launch Environment (MLE) that enables an accurate comparison of all the critical elements of the launch environment against a known good source. Intel TXT creates a cryptographically unique identifier for each approved launch-enabled component and then provides hardware-based enforcement mechanisms to block the launch of code that does not match approved code. This hardware-based solution provides the foundation on which trusted platform solutions can be built to protect against the software-based attacks that threaten integrity, confidentiality, reliability, and availability of systems. Such attacks, when successful, create costly downtime and remediation expenses, as well as potentially large costs related to data breaches.

Intel TXT provides:

- **Verified Launch.** A hardware-based chain of trust that enables launch of the MLE into a “known good” state. Changes to the MLE can be detected through cryptographic (hash-based or signed) measurements.
- **Launch Control Policy (LCP).** A policy engine for the creation and implementation of enforceable lists of “known good” or approved, executable code.
- **Secret Protection.** Hardware-assisted methods that remove residual data at an improper MLE shutdown, protecting data from memory-snooping software and reset attacks.
- **Attestation.** The ability to provide platform measurement credentials to local or remote users or systems to complete the trust verification process and support compliance and audit activities.

Figure 1 shows the decision points and processes of the Intel TXT launch. The model outlines the high-level steps of an Intel TXT-enabled system evaluating launch components from the early BIOS and system firmware to the hypervisor. In each step, the outcome may be that the measurements (hashes) of the components match the expected “known good” configurations and the launch is allowed and indicated as trusted, or that there is a mismatch, and an action can be taken and the launch indicated as untrusted. In the case of the trusted launch, the benefit here is the assurance that the environment has launched as expected, without compromise. This would be a valuable ability to demonstrate in compliance-centric environments or industries.

In the case of a mismatch, one can get an indication of an untrusted launch. For example, a rootkit hypervisor such as the “Blue Pill” compromises the system by attempting to install itself underneath the hypervisor to effectively gain control of the platform. In this case, the Intel TXT-enabled system hashes the code, but because it has been modified (through the insertion of the rootkit) it cannot match the “known good” configuration. In this case Intel TXT would be able to indicate an absence of trust, and action can be taken. This demonstrates the benefit of the greater control Intel TXT provides over the launch configuration and how it can help to mitigate the impact of low-level malware attacks.

Additional Usage Models

By providing controls to ensure only a trustable hypervisor is run on a platform, Intel TXT helps protect a server prior to virtualization software booting and adds launch-time protections that complement runtime malware protections, such as anti-virus software and intrusion detection systems. This is a valuable usage model for helping reduce support and remediation costs for the enterprise.

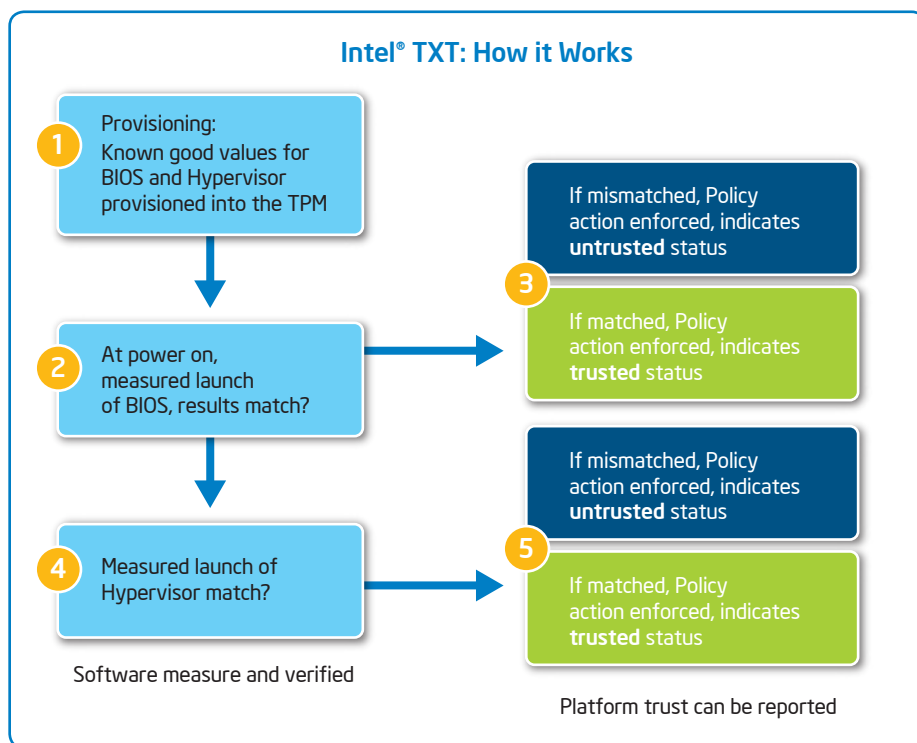


Figure 1. Intel® Trusted Execution Technology (Intel® TXT) protects a virtual server environment data center. Source: Intel Corporation

While this basic protection and enhanced control is effective on individual systems, it becomes even more powerful when one considers aggregated resources and dynamic environments such as today’s virtualized and cloud-based implementations. These implementations, because of their abstraction of physical hardware and multi-tenancy movement across shared infrastructure, require more than traditional perimeter-oriented security techniques.

For example, with VM migration there is a real concern of moving a compromised VM from one physical host to another and potentially compromising that different host and possibly impacting the VMs and workloads on that platform. Intel TXT can help combat this issue in VM migration by helping create something known as “trusted pools.” In this model, Intel TXT is used as a foundation to create pools of trusted hosts, each with Intel TXT enabled

and by which the platform launch integrity has been verified. A policy is then created that restricts the migration of VMs such that only those on trusted platforms can be migrated to other trusted platforms. In the same vein, VMs that were created on untrusted or unverified platforms could be prevented from migrating into trusted pools. This is analogous to an airline passenger clearing an airport checkpoint and then being able to move freely between gates.

Figure 2 shows how VM migration can be controlled across resource pools using trust as control instrumentation for migration policy. This enables IT managers to restrict confidential data or sensitive workloads to platforms that are better controlled and have had their configurations more thoroughly evaluated through the use of Intel TXT-enabled platforms. The ability to restrict VM migration to only trusted hosts has been

demonstrated by Intel, VMware (www.vmware.com), and HyTrust (www.hytrust.com) and captured in a video at YouTube.¹⁶ This new concept for virtualized environments is generating a great deal of interest from enterprises and cloud provider customers seeking new tools to provide insights and controls for virtual and cloud systems.

If this is to be a meaningful control point, IT and security managers need a common way to monitor and report on trust-related events in their infrastructure. This capability lies at the heart of addressing the visibility and compliance challenges exacerbated by virtualization and cloud architectures. Operationally, this requires that trust status can be provided through virtualization management consoles and delivered into Security Information Event Management (SIEM) and Governance, Risk, and Compliance (GRC) systems for more automated logging, reporting, and audit.

Of course, all usage models require a complete solution stack of hardware and software components. Intel is working closely with leading OS, VMM (or hypervisor), and other independent software vendors to include support for Intel TXT to deliver safer, more secure server platforms and data center solutions through these and other innovative usage models.

How to Get There: Intel TXT Components

Intel® server platforms with Intel TXT include several new secure processing innovations. As shown in Figure 3, these include:

- Trusted extensions integrated into the silicon (Intel Xeon processor and Intel® chipset)
- Authenticated Code Modules (ACMs)
- LCP tools

Not all of the components needed for an Intel TXT platform come directly from Intel. Important components also come from third parties, including:

- Trusted Platform Module (TPM) 1.2 (third-party silicon)¹⁷
- Intel TXT-enabled BIOS, and hypervisor or OS environment

A platform must include all of these components to be enabled for Intel TXT. If one of these components is missing or defective, the platform will launch into a traditional, untrusted state. Note that Intel TXT also makes extensive use of Intel® Virtualization Technology (Intel® VT) when utilized in a virtualized environment to provide protections from unauthorized direct memory accesses (DMAs) and to enforce application and data isolation on the system.¹⁸

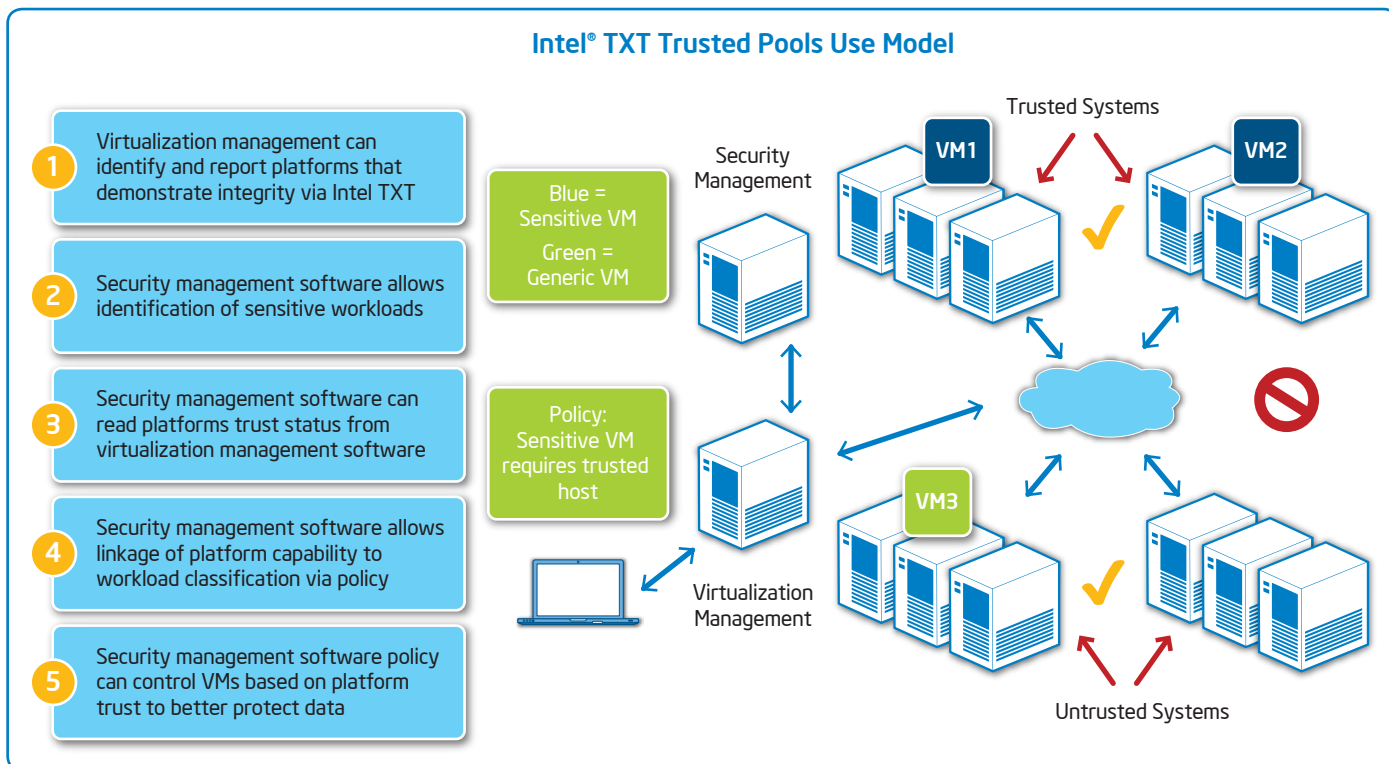


Figure 2. Trustable pools created using Intel® Trusted Execution Technology (Intel® TXT)-enabled platforms help ensure safe migration between hosts. Source: Intel Corporation

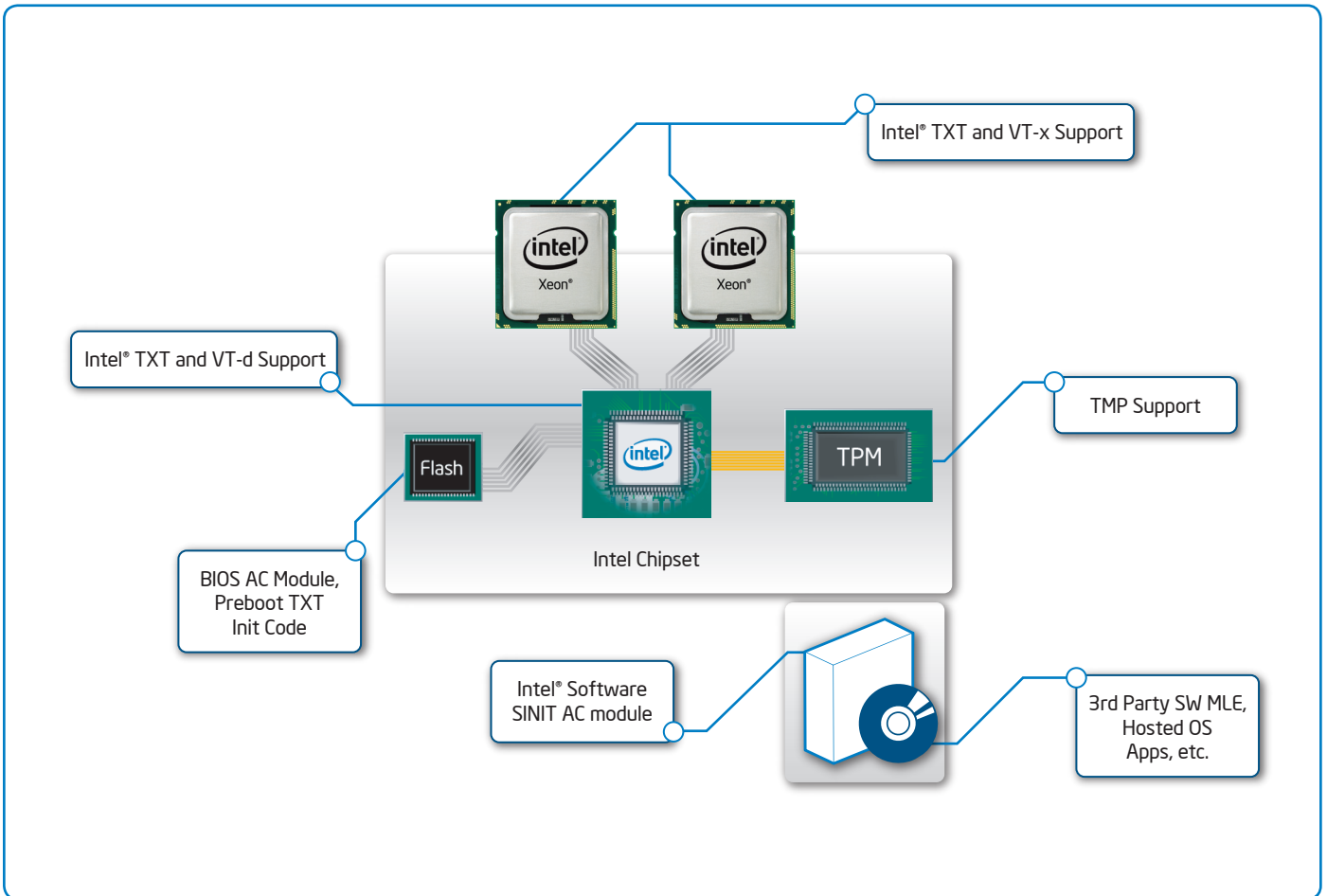


Figure 3. Intel® Trusted Execution Technology (Intel® TXT) components.

Details: Establishing a Root of Trust with Intel TXT for Servers

There are two distinct methods of establishing trust in a computing environment. The first method is called Static Root of Trust for Measurement (S-RTM). In S-RTM models, the measurement starts at a platform reset event and an immutable root (such as a BIOS boot block) and continues into the OS and its components. The major advantage

of S-RTM is its simplicity. Its shortcoming is that S-RTM alone on a complex system can result in a large and unmanageable Trusted Computing Base (TCB)—the set of components required to consider the platform trustable. If any of the components in the boot/launch process change (or get updated) after the trust is established, the system requires migration or re-sealing of secrets.

The other method of establishing trust in a computing environment is Dynamic Root of Trust for Measurement (D-RTM). D-RTM generally results in a smaller TCB—which is desirable. In D-RTM, the trust properties of the components can be ignored until a secure event (for example, an enabled hypervisor launch) triggers and initializes the system, starting the initial root of measurement. Components that were staged before the D-RTM secure event will be excluded from the TCB and cannot execute after the trust properties of the system are established.

Intel developed Intel TXT architecture for servers because server environments present challenging boot scenarios. Therefore, in servers it is essential to bring into the TCB some parts of the early BIOS that initialize the system fabric and the runtime BIOS components (also called system management code). These are needed to implement server reliability, availability, and serviceability (RAS) features. Consequently, because a pure D-RTM implementation excludes these items, a true D-RTM implementation with its smaller TCB falls short.

To create a more suitable implementation for servers, Intel TXT takes key features from both approaches. In any computer system, certain components (both hardware and software) need to be inside the trust boundary of the TCB to detect launch status. In the Intel TXT trust model, some of the system boot firmware is allowed within the trust boundary of the hardware-protected environment. In fact, Intel TXT allows just enough of the system firmware within the trust boundary so that all of the current or projected RAS features can be supported. In addition, Intel TXT architecture borrows from the S-RTM model, providing methods for measuring and recording in the TPM any of the system firmware that is within the trust boundary—providing additional ability to detect attacks against this sensitive platform component.

In Intel TXT architecture, the trusted firmware will most frequently include the BIOS components that initialize the system fabric, modules that participate in implementing system RAS features that would require modification to the system fabric, and any system service processor (SSP) code.

Enabling Intel TXT

Intel is working closely with industry partners to deliver safer, more secure server platforms and data centers. As noted earlier, Intel TXT-enabled solutions require components from multiple vendors to provide the relevant platform protection. Intel TXT requires a server system with Intel VT, an Intel TXT-enabled processor, chipset, ACM, enabled BIOS, and an Intel TXT-compatible MLE (OS or hypervisor). In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group (<http://www.trustedcomputinggroup.org>), and specific software for some uses. And more advanced Trusted Pools and compliance-oriented use models also require security policy engines and security management and compliance tools and more.

Intel's enabling effort spans all of the components above. We are working with system vendors to provide guidance on the required hardware components (including compatible TPM), enabling BIOS for TXT through the integration of ACMs, and providing LCP and LCP tools to facilitate the test and validation of Intel TXT components.

Similarly, we are working with OS and hypervisor vendors to help them develop Intel TXT-enabled software packages. Our work here is focused on providing the ACM required to enable trusted boot. We are also providing validation guidance and access to an LCP tool.

LCP is a component that deserves particular attention. It is touched and usable by nearly all Intel TXT components and component providers. It is also a tool IT managers will use to help control their environments.

As a policy engine, LCP operates on the policy data structures that are rooted in and protected by the platform TPM component. The TPM contains server-manufacturer-stored policy and owner-stored policy. These policies specify what values represent the “known good” or desired software load digests. Policy engine rules dictate that the platform owner's set policy overrides the stored set policy. This allows a server manufacturer to point to an MLE that is installed in the factory and at the same time provides an opportunity for the platform owner (such as an IT manager) to update or override it in order to replace it with their own choice of MLE. The details of developing or implementing an MLE and LCPs are detailed in the document Intel Trusted Execution Technology Software Development Guide available at www.intel.com/txt.

Intel TXT is available on a growing number of server platforms based on the Intel Xeon processor family from a variety of system vendors. And there is a growing ecosystem of supporting hypervisor and security software products that are now trust-aware for enabling trusted pools and compliance use models. While system and software vendors will individually disclose Intel TXT support for their specific products, Intel also provides on its web site a comprehensive list of platforms, software products, and service providers that have announced support for Intel TXT. As enabled platforms proliferate in the market, we expect increased software support for the features and more solutions and reference architectures built on these capabilities. In short, there will be a growing ecosystem of support for Intel TXT over time.

Summary

Most malware prevention tools execute only after the system boots into the runtime environment. In an age of ever-growing threats from hypervisor attacks, BIOS and other firmware attacks, malicious root kit installations, and more, Intel TXT helps to close an important security gap by providing evaluation of the launch environment and enforcing “known good” code execution. Complementing runtime security protection solutions, Intel TXT adds a foundational (hardware-based) protection capability to server systems by allowing greater control of the launch stack and isolation in boot process.

More than ever, today’s businesses and organizations need this kind of protection to help secure critical customer, employee, and financial data, and preserve systems infrastructure. This is becoming more crucial as companies adopt more virtualized, shared, and multi-tenant infrastructure models. With Intel TXT-enabled solutions you can:

- Address the increasing and evolving security threats across your physical and virtual infrastructure.
- Facilitate compliance with government and industry regulations and data protection standards.

- Reduce malware-related support and remediation costs.
- Establish visibility into the integrity of physical and virtual infrastructure

Overall, Intel is enabling a significant opportunity for IT organizations to future proof their infrastructures. Using Intel TXT-enabled solutions can help them stay ahead of emerging threats. IT organizations can gain important security instrumentation and visibility for their growing virtualized environments to allow them to better control the flow of confidential, privileged, or sensitive workloads or data by restricting these to more thoroughly evaluated or trusted platforms. They also gain the capability to have hardware-protected mechanisms for reporting on the integrity of the platform configuration, which will help meet the growing requirements for compliance auditing and provide a new control point in virtual and cloud infrastructures. While the near-term model will be the creation of “trustable pools” amid their legacy systems, increasingly, platform trust will grow to be a baseline level of assurance for platforms as systems are refreshed—essentially increasing the expectations for data center security over time.

Through Intel TXT and other new features in the Intel Xeon processor families, Intel is taking a leading role in delivering solutions that help mitigate current and emerging attacks and help reduce the overhead of securing data. Talk to your server supplier today to start making security a foundational part of your IT architecture and server planning.

Additional Resources

You can learn more about Intel Trusted Execution Technology using the following resources:

- More web-based info:
 - www.intel.com/technology/security
 - download.intel.com/technology/security/downloads/315168.pdf
- A book on this topic:
David Grawrock, Dynamics of a Trusted Platform: A Building Block Approach, Intel Press, ISBN#978-1-934053-17-1
- Source code for Trusted Boot (open source MLE code, LCP tools, and more):
 - sourceforge.net/projects/tboot

For more information on Intel® Trusted Execution Technology, visit www.intel.com/txt

¹ No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security

² McAfee Threat Report, 2Q 2012.

³ Kaspersky Lab detects 25 millionth malicious program, Kaspersky Lab press release, June 12, 2009.

⁴ Ibid.

⁵ Remarks by the President on Securing Our Nation's Cyber Infrastructure, The White House, Office of the Press Secretary, May 29, 2009.

⁶ Emerging Cyber Threats Report for 2009, report from GTISC annual Security Summit on Emerging Cyber Threats, October 18, 2009.

⁷ Cisco 2008 Annual Security Report, Cisco, February 2009.

⁸ Malware Discussion, Norman ASA, July 10, 2009. (www.norman.com/security_center/security_center_archive/2009/70364/en)

⁹ Yahoo confirms server breach, over 400k accounts compromised, Engadget, July 12, 2012. www.engadget.com/2012/07/12/yahoo-security-breach

¹⁰ SC Magazine. www.scmagazine.com/data-breaches/topic/3225/

¹¹ Reports: Thief holds Virginia medical data ransom, SecurityFocus, May 5, 2009.

¹² 2011 Annual Study: U.S. Cost of a Data Breach, Symantec, Ponemon Group, March 2012. www.slideshare.net/symantec/2011-annual-study-us-cost-of-a-data-breach-march-2012

¹³ Global Payments: data breach cost a whopping \$84.8 million, Network World, July 26, 2012. www.networkworld.com/news/2012/07/27/12-global-payments-data-breach-cost-261204.html

¹⁴ Legal Risks on the Radar. www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf

¹⁵ NIST BIOS Protection Guidelines. csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

¹⁶ YouTube: www.youtube.com/watch?v=VWw_XFFtjM4

¹⁷ The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

¹⁸ Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit www.intel.com/go/virtualization

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. 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. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2010-2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel vPro, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

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

Printed in USA ♻️ Please Recycle
0113J/R/MESH/PDF 323586-003US

