

Evolution of Integrity Checking with Intel® Trusted Execution Technology: an Intel IT Perspective

Periodic integrity checks with Intel TXT could help Intel IT detect attacks more quickly, contain the spread of malware, and reduce the need to rebuild hypervisors if a compromise is detected.

Sudip Chahal

Principal Engineer, Intel IT

Das Kamhout

Engineer, Intel IT

Toby Kohlenberg

Senior Information Security Specialist, Intel IT

Mohan Kumar

Senior Principal Engineer, Intel Architecture Group

Steve Mancini

Senior Security Specialist, Intel IT

Dennis Morgan

Senior Security Specialist, Intel IT

Stacy Purcell

Enterprise Architect, Intel IT

Alan Ross

Senior Principal Engineer, Intel IT

Cindy Smith

Enterprise Architect, Intel IT

Executive Overview

Intel IT is transitioning to a private cloud-computing environment to improve efficiency and agility. This highly virtualized multi-tenant environment creates new security challenges, including those presented by emerging threats such as rootkit attacks.

We carefully examine these security concerns and analyze technologies that can potentially address them. As part of this effort, we evaluated Intel® Trusted Execution Technology (Intel® TXT), a new security technology in Intel® processors. Intel TXT enables hardware-enforced integrity checks of hypervisors and other key system components at server startup.

Our evaluation highlighted a potential use case that utilizes Intel TXT to conduct periodic hypervisor integrity checks across a server cluster, without interrupting business applications. This could let us detect attacks more quickly, contain the spread of malware, and reduce the need to rebuild hypervisors if a compromise is detected.

We envision this use case as a key step in an evolution of integrity-checking capabilities built on Intel TXT. The evolution begins with one-time integrity checks at system startup, progresses to more frequent periodic integrity checks, and culminates in runtime integrity checks on individual virtual machines.

We analyzed the performance and power-management implications of this use case, as well as the ecosystem support required. Our analysis suggests that all servers in a large cluster could be checked within a few hours and that the use case has considerable potential synergy with virtualization power-management schemes.

With appropriate ecosystem enabling for Intel TXT, we believe that this use case could significantly enhance security in our virtualized environment. Intel is working with suppliers to encourage this support. We are deploying Intel® Xeon® processor 5600 series-based servers, which include Intel TXT, as a core element of our private cloud infrastructure.

Intel TXT is a foundation technology that can be applied to enhance security in multiple usage models; the use case described here is only one of these, and we expect to continue exploring other applications in the future.

Contents

Executive Overview.....	1
Background.....	2
Root of Trust.....	2
Evolution of Integrity Checking.....	3
Use Case for Intel® TXT.....	4
Scalability.....	5
Implementation Considerations.....	6
Synergy with Power Management.....	6
Ecosystem Requirements and Other Concerns.....	6
Summary.....	7

IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel IT is undertaking a major transition to an enterprise private cloud that will support our office and enterprise computing applications. This multi-year initiative is designed to enable greater agility and efficiency; we plan a phased implementation, progressively moving more-important applications to the cloud over time.

We are building this multi-tenant environment on virtualized infrastructure as a service (IaaS), based on clusters of Intel® Xeon® processor-based servers. Management of these clusters will be automated and policy-driven. A key capability of this architecture is live migration, which enables virtual machines (VMs) with applications running in them to be moved between servers without downtime. Live migration is the basis of advanced services such as automated dynamic load-balancing within a cluster.

The security of Intel's data and applications remains a critical focus as we develop and implement our cloud strategy. Our enterprise private cloud architecture addresses key security challenges, including software, platform, and infrastructure security, as shown in Figure 1.

In a non-virtualized environment, the separation provided by physical infrastructure is assumed to provide a level of protection for applications and data. In

the cloud, this traditional physical isolation between applications no longer exists. Our cloud infrastructure is multi-tenant, with multiple applications utilizing a shared common physical infrastructure. This provides the benefit of much more efficient resource utilization. However, because the physical barriers between applications have been eliminated, it is important to establish compensating security controls to minimize the potential for malware to spread through the cloud.

Newer types of malware threats, such as rootkit attacks, can be increasingly difficult to detect using traditional antivirus products. These threats use various methods of concealment to remain undetected as they infect key system components such as hypervisors and drivers. This increases the likelihood that the malware can operate in the background, spread through a cloud environment, and cause greater damage over time.

Root of Trust

These security concerns increase the importance of helping assure system integrity by establishing a root of trust—a hardware-based security foundation—within each system. This trusted foundation can then be used to perform regular integrity checks of key components, such as hypervisors, to verify that they have not been compromised. The trusted foundation can be provided by Intel® Trusted Execution Technology (Intel® TXT), a hardware-based security technology that conducts integrity

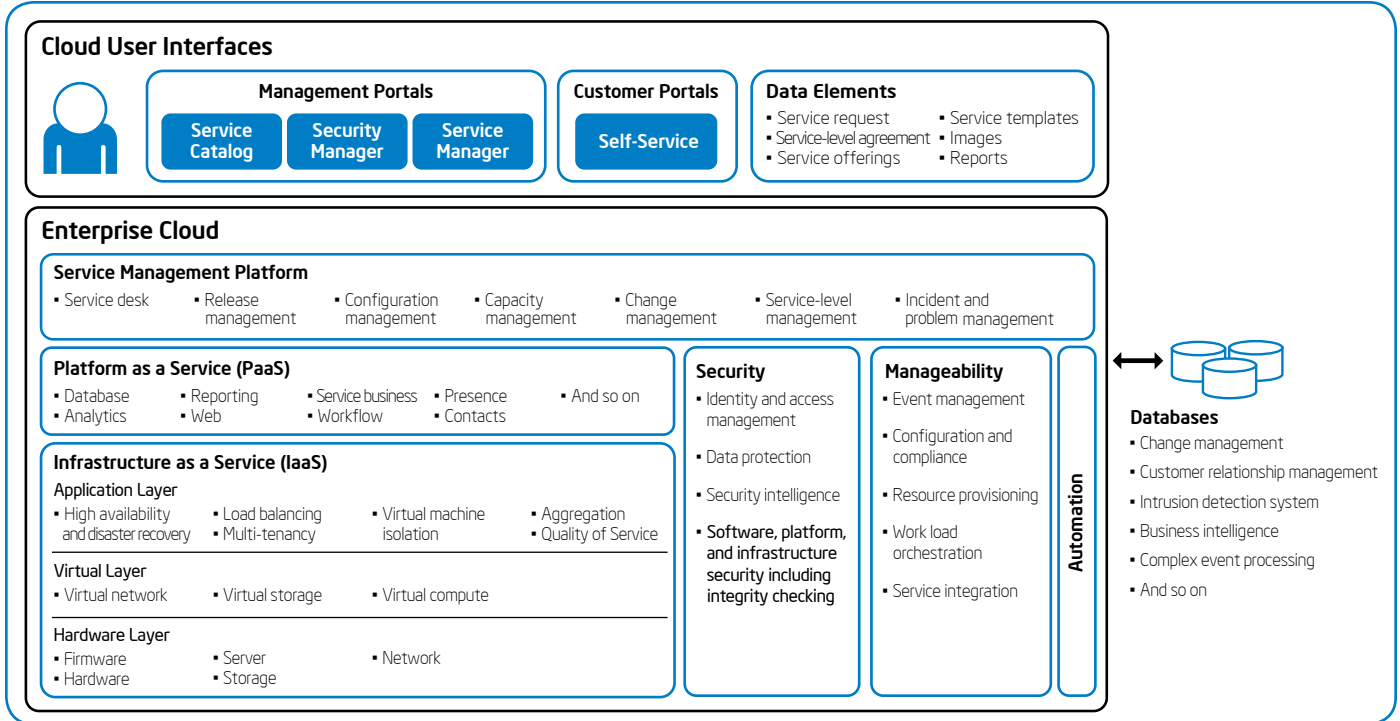


Figure 1. Intel IT's enterprise private cloud architecture.

checks at hypervisor launch, which is typically at server startup (see sidebar “Intel® Trusted Execution Technology”).

Evolution of Integrity Checking

We view system integrity checking as a key capability within the software, platform, and infrastructure security focus area of our private cloud architecture.

Our vision for helping assure ongoing system integrity in a virtualized environment includes an evolution of integrity-checking capabilities. Each phase in this evolution provides an increasing level of assurance and relies on secure startup enabled by Intel TXT.

This evolution begins with one-time integrity checks at system or hypervisor startup, progresses to more frequent periodic integrity checks, and culminates in runtime integrity checks, as shown in Figure 2.

In the longer term, we believe that significant protection could be provided by conducting integrity checks on individual VMs at runtime. Given a trusted foundation, it is possible that the integrity of the VMs operating on top of the hypervisor may someday be open to inspection and verification as well. However, this is not feasible with technology that is available today.

We are therefore exploring periodic integrity checking. By increasing the frequency of server restarts and using Intel TXT to check integrity at each restart, this approach could enable faster detection of compromises.

In a traditional computing environment, increasing restart frequency is difficult because applications are tied to physical servers; restarting a production server can result in unacceptable application downtime.

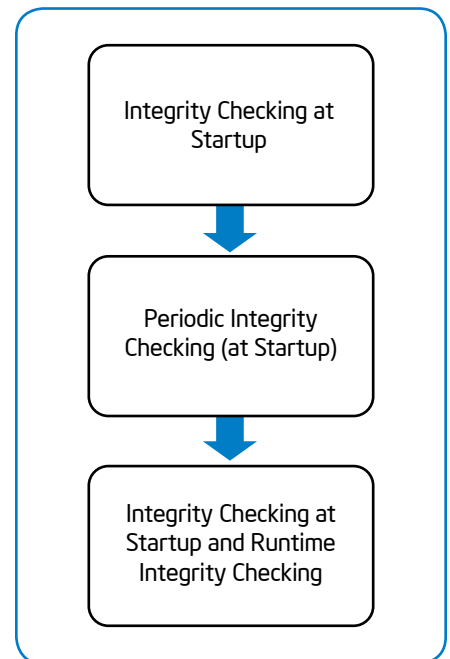


Figure 2. Evolution of integrity checking.

Intel® Trusted Execution Technology

Intel® Trusted Execution Technology (Intel® TXT) is a hardware-based security technology specifically designed to harden platforms against attacks to the hypervisor and BIOS, malicious rootkit installations, and other firmware and software attacks. It is currently available in servers based on Intel® Xeon® processor 5600 series and on business PCs with Intel® Core™ vPro™ processors.

Intel TXT establishes a root of trust—a hardware-based security foundation that can be used to verify the integrity of other system components, such as the hypervisor.

At startup, Intel TXT measures the code of the hypervisor and compares it with a known good value, as shown in Figure 3. If the measurements do not match, indicating that the hypervisor may have been compromised, launch can be blocked.

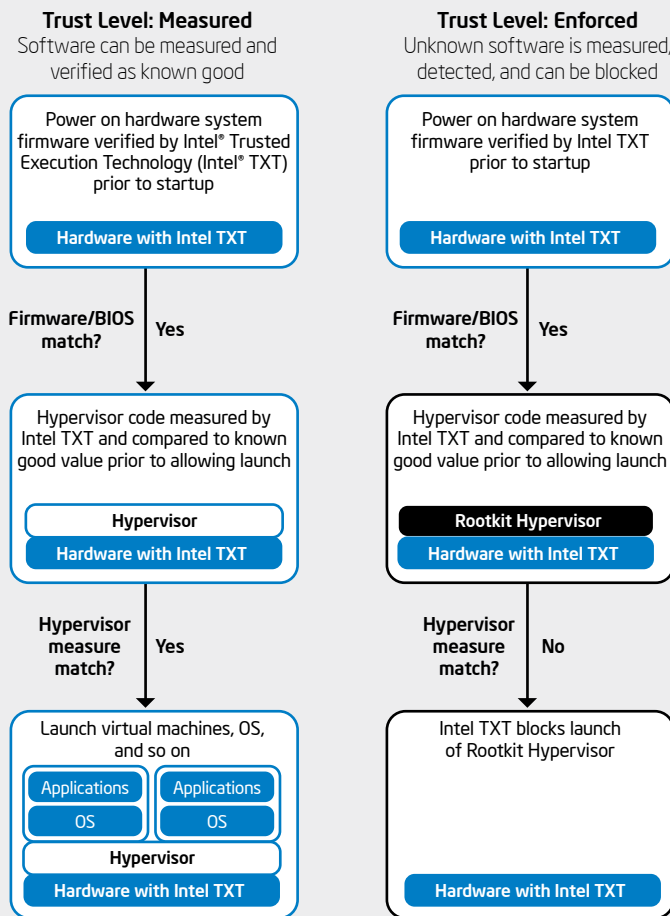


Figure 3. Intel® Trusted Execution Technology helps protect virtualized server environments.

In a virtualized environment, increasing restart frequency becomes much more feasible. We can use live migration to relocate workloads within a cluster, enabling individual servers to be rebooted without interruption to applications.

To assess the potential of this approach, we identified a use case that takes advantage of the capabilities of Intel TXT as a root of trust to conduct periodic integrity checks in a virtualized environment. We analyzed the benefits, implementation considerations, possible impacts, and the ecosystem support required.

USE CASE FOR INTEL® TXT

Our use case, shown in Figure 4, employs live migration to move all VMs off each server within a cluster in turn, allowing us to restart the server and conduct an integrity check without application downtime. This use case assumes that the servers in the cluster are Intel TXT-capable and enable a hypervisor to be launched securely.

For each server, the steps are:

1. Live migrate all VMs running on the server to other servers in the cluster.
2. Restart the server, with an Intel TXT-enabled integrity check to verify that the hypervisor has not been compromised.
3. If the hypervisor code is verified as good, live migrate the VMs from other servers back to this server. If the hypervisor code is bad, then corrective action is taken immediately on all servers, hypervisors, and VMs involved in this specific series of VM migrations.

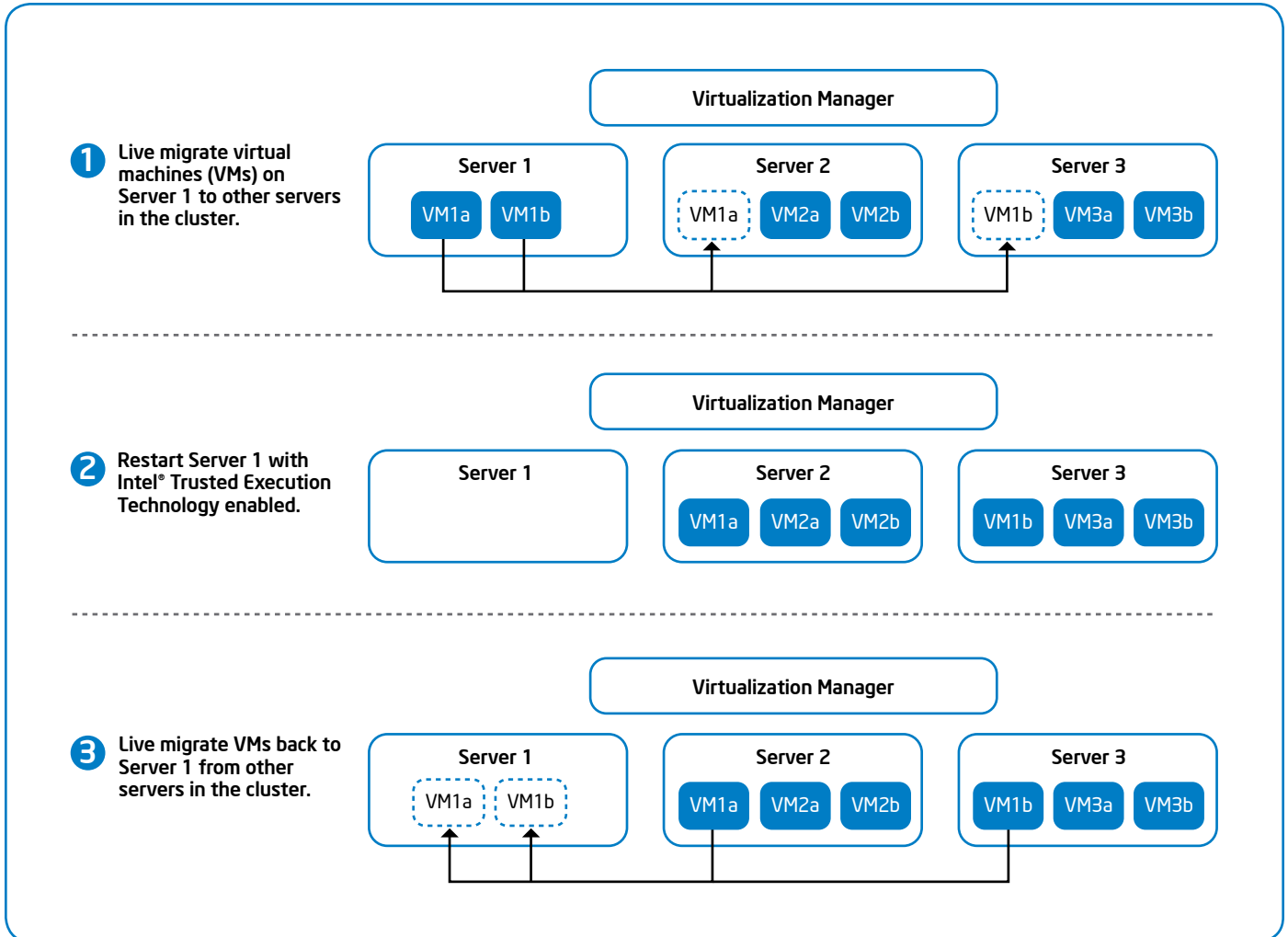


Figure 4. Proposed use case: Integrity check in a virtualization server cluster.

This process is repeated for all servers in the cluster.

The use case should be a policy-driven, automated activity that can be scheduled to run at night or at other times of low activity. In a large cluster, several servers could be executing the use case concurrently.

Scalability

We conducted preliminary analysis to assess whether our use case could scale to support large production clusters.

Our analysis was partly based on existing Intel IT live migration data. This included tests in which a representative enterprise reporting application, comprising six VMs, was live migrated between several servers based on different generations of Intel Xeon processors. The average time required to migrate all six VMs was between three minutes 20 seconds and four minutes—an average of about 33 to 40 seconds per VM. In our scalability analysis, we estimated how long it would take to complete the use

case for all servers in a 20-server cluster running a total of 200 VMs. We created a range of projections based on the following assumptions:

- A conservative range of live migration times, from 30 seconds to two minutes per VM
- Server restart time of five minutes
- One to four concurrent live migrations within the cluster

With four concurrent migrations, the entire process could be completed within a few

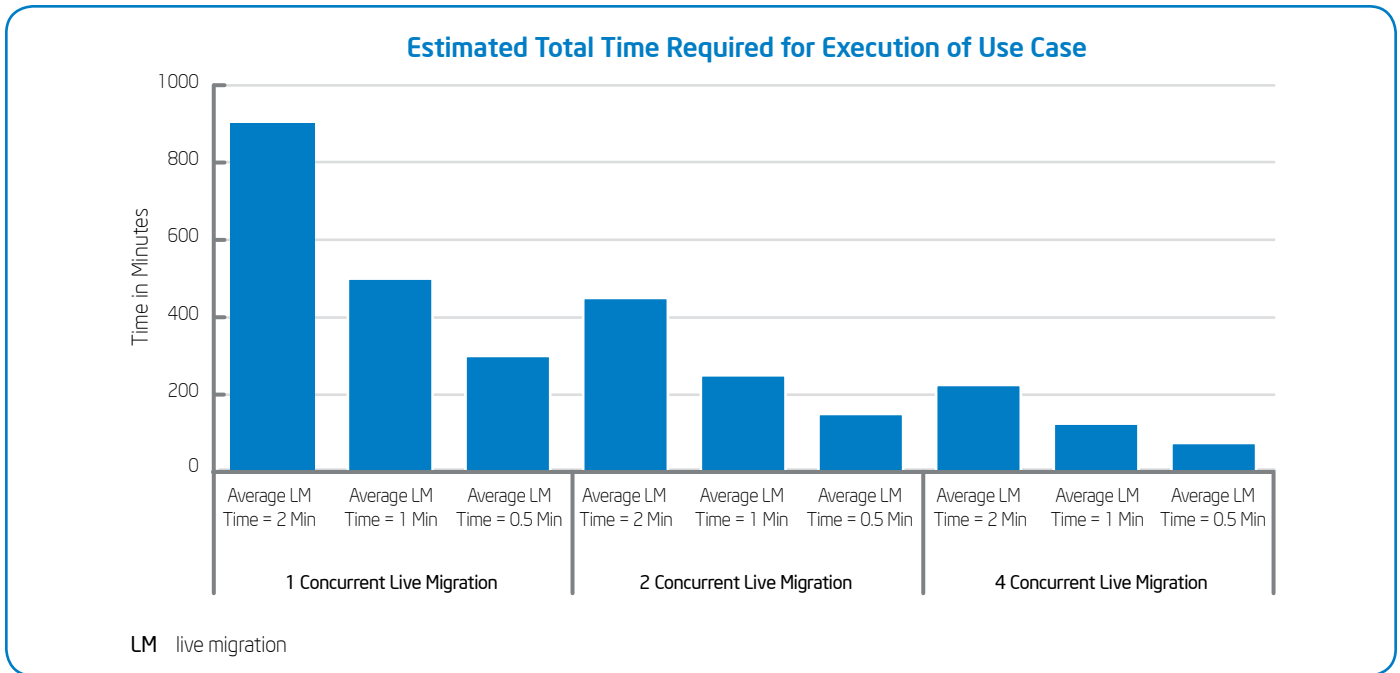


Figure 5. Estimates of total time required to execute the use case, resulting in integrity checks for all servers in a large (20-server) cluster with 200 virtual machines and a five-minute server restart time.

hours, as shown in Figure 5. This suggests that the proposed use case could scale to accommodate large clusters by executing concurrently on multiple servers.

Implementation Considerations

Key implementation considerations include enforcement, logging, and frequency of integrity checks.

ENFORCEMENT

The integrity check must not be bypassed as a result of modifications to the server configuration, such as firmware or BIOS updates.

LOGGING

Comprehensive logging is required for this security process.

- All integrity checks and changes to the integrity checksum must be logged to a remote server.

- Only authorized personnel should be able to update the checksum.

FREQUENCY OF INTEGRITY CHECKS

The frequency with which servers are checked will depend on the environment and any other existing controls.

- Development clusters.** Clusters used for software development will require more frequent integrity checks, perhaps nightly, because they are less likely than production clusters to be rigorously secured or trusted.
- Production clusters running internal applications.** Clusters that are running internal applications and are within corporate firewalls will need less frequent checks since they are highly secured.
- Production clusters running externally facing applications.** These will require more frequent checks because they are likely to be more accessible and targeted by attackers.

Synergy with Power Management

There is substantial synergy between our proposed use case and the power management approach provided by some virtualization management software. Both use live migration to move VMs off some servers within a cluster during periods of low activity. As a result, the mechanisms used for power management could be applied to implement our use case as well, without requiring additional hardware or software.

This synergy provides an opportunity to address two business requirements, security and power management, with a unified automated, policy-based virtualization software architecture.

Ecosystem Requirements and Other Concerns

Implementation of our proposed use case will require ecosystem support for Intel TXT.

An Alternative Approach to Conducting Periodic Integrity Checks

Intel IT continues to explore other usage models that could further simplify the process of conducting periodic integrity checks. One approach that we are researching is “offline” startup and integrity checking. The concept is to copy the hypervisor executables from an operational server to an isolated standby server that is used to execute the startup process and associated integrity check. This approach would enable checks to be conducted more frequently and more quickly. There would also be even less risk of impacts to application performance, since this approach would not require live migration of virtual machines. Considerations include the need to help assure secure transfer of the hypervisor copy.

Intel is working closely with suppliers, including OS and hypervisor providers, to encourage them to develop Intel TXT-enabled products.

The desired ecosystem support could enable orchestration and automation of the full sequence of steps. Ideally, this orchestration could be supported by virtualization management software, enabling synergy with power management.

Ecosystem support could also help ensure adequate logging and auditing of all integrity checks, to help identify anomalous behavior and provide robust forensic capabilities.

Further support would allow extension of the chain of trust to enable runtime checking at the level of each VM, thus identifying individual compromised VMs. This may obviate the need to rebuild an entire cluster from bare metal if a VM is found to be compromised.

Other areas of concern include the need to evaluate whether frequent live migrations have application performance impacts or require additional network bandwidth. Additionally, there is a concern that automated live migration can propagate malware within a cluster; however, this can happen in any virtualized environment, and the use of Intel TXT-enabled integrity checks may help contain the malware before it spreads to other clusters.

SUMMARY

Our analysis suggests that this use case is feasible and could offer significant benefits in the future, as shown in Table 1.

Using Intel TXT, we could periodically check for compromised hypervisors without interruption to business applications. This could enable faster detection of compromises, helping to contain the spread of malware, and reduce the need to rebuild hypervisors if a compromise is detected.

Limitations of this approach include the fact that integrity checks occur only at server startup. In addition, ecosystem support for Intel TXT is required to orchestrate and automate the use case. Ecosystem support could also extend the chain of trust to enable runtime integrity checks of each VM.

With the appropriate ecosystem enabling for Intel TXT, we believe that this use case could significantly enhance security in our virtualized environment. We are deploying Intel Xeon processor 5600 series-based servers, which include Intel TXT, as a core element of our private cloud infrastructure.

Intel TXT is a foundation technology that can be applied in multiple usage models to enhance IT security; the use case described here is only one of these. As ecosystem support evolves, we expect to continue exploring other uses of Intel TXT within our environment.

Table 1. Benefits and Limitations of Use Case: Periodic Integrity Checking in a Virtualized Environment with Intel® Trusted Execution Technology

Potential benefits
<ul style="list-style-type: none"> Proactively detect compromised hypervisors more quickly No application downtime Help contain spread of malware Reduce the need to the rebuild hypervisors in a cluster if compromise is detected Synergy with power management techniques; possibility of an automated framework addressing both security and power management
Concerns and limitations
<ul style="list-style-type: none"> Integrity check occurs only at startup Ecosystem support will be required to automate the use case and to enable runtime checking of individual virtual machines and applications

FOR MORE INFORMATION

- "Intel® Trusted Execution Technology: Hardware-based Technology for Enhancing Server Platform Security" www.intel.com/Assets/en_US/PDF/whitepaper/323586.pdf
- "Testing Live Migration with Intel® Virtualization Technology FlexMigration" http://download.intel.com/it/pdf/Testing_Live_Migration_with_FlexMigration.pdf
- "An Enterprise Private Cloud Architecture and Implementation Roadmap" http://download.intel.com/it/pdf/Entrprse_Priv_Cloud_Arch_final.pdf

ACRONYMS

IaaS	infrastructure as a service
Intel® TXT	Intel® Trusted Execution Technology
PaaS	platform as a service
VM	virtual machine

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.


This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel, the Intel logo, Intel Core, 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.

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA
0810/KAR/KC/PDF

 Please Recycle
323953-001US

