Intel® Trusted Execution Technology

Hardware-based Technology for Enhancing Server Platform Security

James Greene
Intel Corporation

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 regular 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 key to maintaining the high assurance required to meet the security needs in the data center.

This paper describes a highly scalable architecture called Intel® Trusted Execution Technology (Intel® TXT) that provides hardware-based security technologies to build a solid foundation for security. Built into Intel's silicon, these technologies address the increasing and evolving security threats across physical and virtual infrastructure 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 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 future 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

The Threats to Data Keep Growing

Attacks on IT infrastructure continue to grow in volume, complexity, sophistication, and stealth. According to the Symantec* Internet Security Threat Report, the release rate of malicious code and other unwanted programs "may be exceeding that of legitimate software applications."[1] For another opinion on the matter, consider that a few years ago, Kaspersky Lab forecast a ten-fold increase in malicious programs, from 2.2 million to 20 million in 2008.[2] This was far from exaggeration. The specialists at Kaspersky Lab detected the 25 millionth malicious program and added it to the company's antivirus databases in June 2009.[3]

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."[4] Security experts consulted by Georgia Tech Information Security Center (GTISC) believe cyber warfare will accompany traditional military interaction more often in the years ahead.[5] 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.[6] 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 programming skills.[7] Nearly anyone can do it thanks to an increased availability of prepackaged "kits" that allow for the easy definition of malware.

Servers are a particularly alluring target. For instance, in 2008, hackers took control of Federal Aviation Administration (FAA) critical network servers and could have shut them down.[8] They also took advantage of interconnected networks, installed malicious codes, and gained access to more than 40,000 FAA user IDs, passwords, and other data used to control a portion of the mission-support network.[9] In Virginia, an online thief compromised the network of the Commonwealth of Virginia's Department of Health Professions, allegedly stealing healthcare data on nearly 8.3 million patients and demanding $10 million for the data.[10] These breaches are just the tip of the iceberg. And even more recently, Google and as many as 30 other major companies disclosed that they had suffered significant breaches to their infrastructure. While the details from such breaches will continue to emerge, the basic trend is alarming—a trend of sophisticated, orchestrated and highly targeted attacks. Unfortunately, there are far too many such breaches of equal significance to report here. Making matters worse, the cost of a data breach is increasing as well. The average organizational costs of a data breech have gone from $4.7 million in 2006 to $6.6 million in 2008[11], with lost business as the largest percentage of this cost. It's no wonder that according to Enterprise Innovation, IT security is the number one worry of Fortune 1000 companies[12] and in 2009, CIOs of state governments across the United States ranked security in the top four of their concerns.[13]

The net 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. For this, 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. 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, Virtual Machine Managers, and more). The root also provides a trusted position to evaluate the integrity of any other components —enabling assurance through a secure comparison against expected measurements. By allowing such comparison 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 is established, it becomes 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 wide variety of personal, financial, governmental and other data, and are under increased attack, the time has arrived 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 will be available on servers with the introduction of the Intel® Xeon® processor 5600 series, formerly code-named Westmere-EP. Hardened for server environments (particularly virtual server environments), Intel TXT gives IT managers the opportunity 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

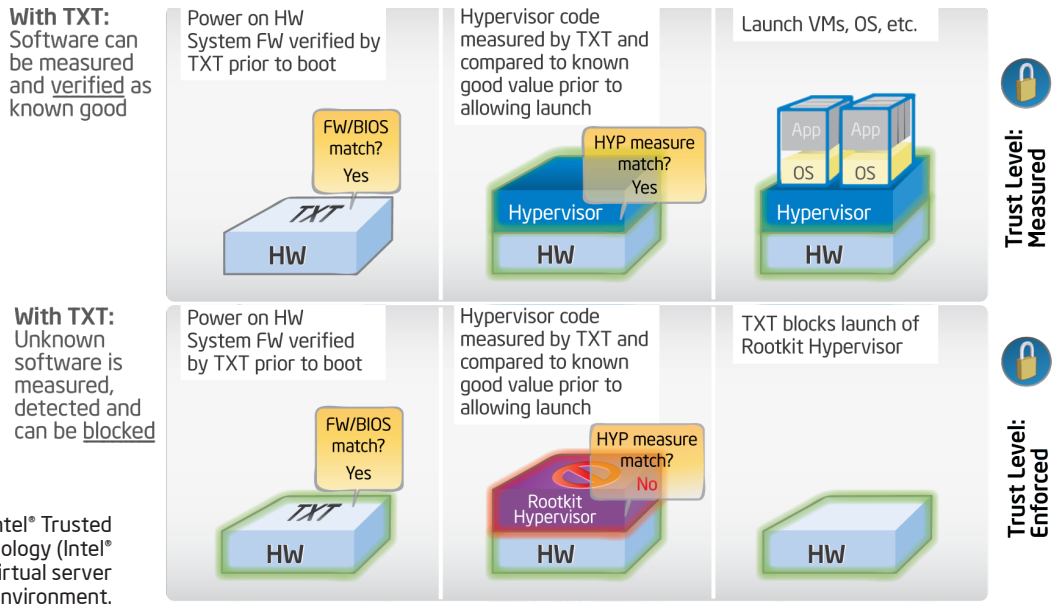

Figure 1. How Intel® Trusted Execution Technology (Intel® TXT) protects a virtual server environment.

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 infrastructure.

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 via 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/systems to complete the trust verification process and support compliance and audit activities.

Figure 1 shows two model cases for the Intel TXT launch process. The first 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 this case, the assumption is that the measurements (hashes) of the components match the expected "known good" configurations and the launch is allowed. 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 second case, the assumptions and results are different. As before, the early BIOS and system firmware are measured in the first step, but this time the system has been compromised by a rootkit hypervisor such as the "Blue Pill"—which is 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 since it has been modified (through the insertion of the rootkit) it therefore cannot match the "known good" configuration. In this case TXT would be able to abort the launch per the launch policy. This demonstrates the benefit of the greater control Intel TXT provides over the launch configuration and how it can help to mitigate 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 run-time malware protections (anti-virus software, intrusion detection systems, etc.). This is a valuable usage model for helping reduce support and remediation costs for the enterprise.

While this basic protection and enhanced control is good 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

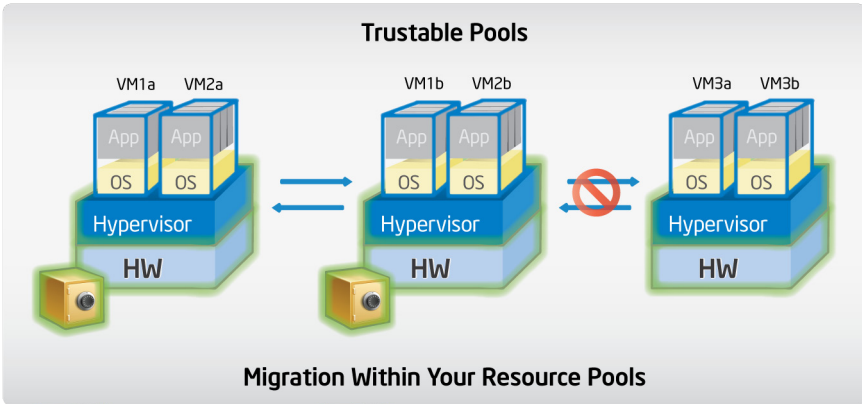

Figure 2. Ensuring safe migration between hosts through trustable pools created using Intel® Trusted Execution Technology (Intel® TXT)-enabled platforms.

more than traditional perimeter-oriented security techniques.

Take virtual machine (VM) migration, for instance. 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 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 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 was demonstrated by Intel, VMware (http://www.vmware.com), and HyTrust (http://www.hytrust.com) at the Intel Developer Forum in September 2009.[14] (See: http://www.youtube.com/watch?v=RB1UGtkY4wM.)

Of course, all usage models require a complete solution stack of hardware and software components. Intel is working closely with leading operating system (OS), Virtual Machine, 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 chipset)
- Authenticated Code Modules (ACM)
- Launch Control Policy (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)
- 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.

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 all the way 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

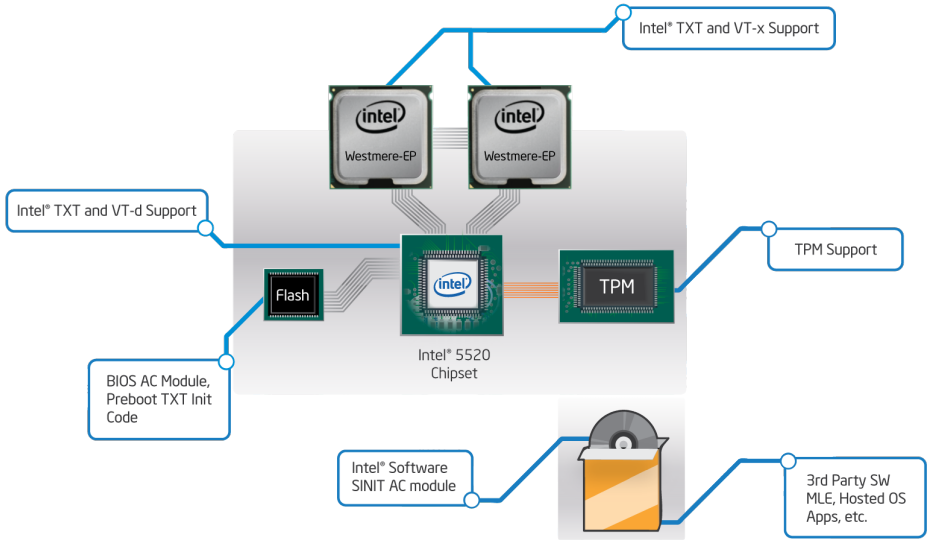

Figure 3. Intel® Trusted Execution Technology (Intel® TXT) Components.

process change (or get updated) after the trust is established, then the system will require 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 very 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, Authenticated Code Module (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.

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 TPM), enable 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 to replace it with their own choice of MLE. The details of developing or implementing an MLE and Launch Control Policies are detailed in the document *Intel Trusted Execution Technology Software Development Guide* available at http://www.intel.com/technology/security.

Intel TXT will be available on server platforms based on the Intel Xeon processor 5600 series in early 2010. Because it takes time to grow ecosystems for new technologies—especially those with multiple touchpoints (HW, SW, BIOS)—not all features or solutions and use models will be immediately supported by all vendors at product launch. System and software vendors will individually disclose the specific product Intel TXT support capabilities. Intel will also provide a list of platforms and software products that have announced support for Intel TXT on its Web site. As enabled platforms proliferate in the market, we expect

increased software support for the features and more solutions built on these capabilities. In short, there will be a growing ecosystem of support for Intel TXT as 2010 progresses.

Summary

Most malware prevention tools execute only once the system is booted 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 grows ever 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.

Overall, Intel is enabling a significant opportunity for IT organizations to "future proof" their infrastructures. Using Intel TXT-enabled solutions, they can get ahead of the curve of emerging threats. IT organizations can gain important security instrumentation 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 growing requirements for compliance auditing. 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 "raising the bar" for data center security over time.

Through Intel TXT and other new features in the Intel Xeon processor 5600 series, Intel is taking a leading role in delivering solutions that mitigate current and emerging attacks and 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:
  - http://www.intel.com/technology/security
  - http://download.intel.com/technology/security/downloads/315168.pdf
  - http://communities.intel.com/docs/DOC-3833
- 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, Launch Control Policy tools, and more):
  - http://sourceforge.net/projects/tboot

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

[1] "Symantec Internet Security Threat Report," July-December 2007.

[2] "Kaspersky Lab detects 25 millionth malicious program," Kaspersky Lab press release, June 12, 2009.

[3] Ibid.

[4] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, Office of the Press Secretary, Mary 29, 2009.

[5] "Emerging Cyber Threats Report for 2009," report from GTISC annual Security Summit on Emerging Cyber Threats, October 18, 2009.

[6] "Cisco 2008 Annual Security Report," Cisco, February 2009.

[7] "Malware Discussion," Norman ASA, July 10, 2009. (http://www.norman.com/security_center/security_center_archive/2009/70364/en)

[8] "Report: Hackers broke into FAA air traffic control systems," CNET news, May 7, 2009.

[9] Ibid.

[10] "Reports: Thief holds Virginia medical data ransom," SecurityFocus, May 5, 2009.

[11] "Data-breach costs rising, study finds," Network World, February 2, 2009.

[12] "IT security is No. 1 worry of Fortune 1000 companies," Enterprise Innovation, July 14, 2008.

[13] As reported on the National Association of State Chief Information Officers (NASCIO) Web site. (http://www.nascio.org/publications/documents/NASCIO-CIOPriorities2008-2009.pdf)

[14] Intel, VMware, Hytrust video from Intel Developer Forum 2009. (http://www.youtube.com/watch?v=RB1UGtkY4wM)

Printed in USA 0110/JG/EMC/PDF Please Recycle 323586-001US