

# Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age


*Sponsored by Trusted Computing Group (TCG)*

# Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age

*June 2013*

**A SANS Whitepaper**

*Written by Gal Shpantzer*

*Advisor: John Pescatore*

# Introduction
# A New Look at an Established Security Mechanism

When the specification for the Trusted Platform Module (TPM) was introduced more than 10 years ago, it held the promise of a real breakthrough in information security, especially for defense agencies and other organizations with critical data to protect. Because its security is hardware based, systems containing TPMs can be scanned at boot for signs of change and attest to whether or not the machine meets security requirements, before boot is executed. This makes advanced malware such as bootkits (formerly known as "rootkits") detectable, and on well-managed endpoints, it reduces the risk of data compromises.

Since the TPM working group formed under IBM and then formalized under the Trusted Computing Group (TCG), TPM has gained the backing of industry heavy hitters including AMD, Cisco, Dell, Infineon, Intel, Infineon and Juniper Networks.[1] One of its most active and long-standing supporters is Microsoft, which has historically used TPM to support its Windows BitLocker and which has now embedded TPM support in its Windows 8 and Windows Server 2012 operating systems (OSes) for increased security and ease of administration. TPMs have also shipped in more than a billion devices, set-top boxes and smaller devices since the first version came out in 2003.[2]

Yet even though TPM capabilities have penetrated the markets for PCs, servers and other, nontraditional devices, TPM has to date not been adopted on a large scale by enterprises. Why? The delay is related to a mix of issues with manufacturers, the nature of upgrade cycles, compatibility with other security software and the change of mindset needed to look at threats and protect devices at a lower level. Now, however, an increasingly complex threat landscape, coupled with the widespread availability and increased maturity of the TPM technology, as well as other factors such as cost reduction, makes TPM ready for prime time. The TPM 2.0 specification was recently published for additional protections, such as protected storage and shielded execution (secure operational states for different uses on the same machine). Intel's x86 and ATOM processors, for example, provide TPM 2.0 in their firmware. And it is available in phone firmware, such as Nokia Windows 8 phones.

In this paper, we discuss the trends that are driving adoption of TPM, with advice on how to take advantage of this increasingly commonplace technology without disrupting your security infrastructure.

1 TCG board members, http://www.trustedcomputinggroup.org/about_tcg/board_of_directors

2 TPM specification history, http://www.trustedcomputinggroup.org/resources/tpm_main_specification

# Why TPM Is Ready for Prime Time

Ten years is a long time in the IT and security worlds, and a lot has changed in those years—from both an integration/maturity and a threat perspective—that is driving increased adoption of TPM. Today, a number of key factors is driving intense interest in TPM among enterprise security professionals and IT managers. One of the biggest drivers is its increasing integration with Windows and Windows Mobile systems, making acquisition costs lower. Meanwhile, threats that take advantage of software-based protections are driving security lower in the stack.

## Timing Is Everything

Here are five top reasons why TPM is ready for prime time:

1. **Embedded in Windows systems.** One of the key drivers of renewed adoption is Microsoft's embedded support for TPM in its Windows 8 systems. Windows 8 and Windows Server 2012 are much more tightly integrated with TPM, supporting it natively and working with the latest central deployment and management tools in Server 2012. But TPM is no longer reserved for expensive business-class desktops, and TPMs can be found in everything from smartphones and tablets to inexpensive consumer-oriented Chromebooks. The software and tools needed to manage TPM are easier to use and are integrated with Microsoft System Center 2012 system-management capabilities. TPM is also a strong component with Windows Phone 8 and Windows RT (a variant of Windows 8 systems designed for smaller devices).
2. **Growing need to secure mobile devices.** In addition to securing data on Windows Mobile devices, TPM is embedded in numerous smart devices, which is indicative of a strong push coming from defense and intelligence agencies, as underscored by National Institute of Standards and Technology (NIST) SP 800-164.[3] For example, Motorola's AME 2000 and the Samsung Knox feature roadmaps that use these platforms. Nokia Windows 8 phones that support Connected Standby (in fact, all Windows 8 devices that support Connected Standby) use TPM 2.0 (for protected storage and operational states, which are needed for mobile devices accessing business applications).
3. **New threats.** Changes in the threat landscape, particularly from bootkit-based threats, represent another factor that now makes the TPM ready for prime time. These threats—like the 2011 Mebromi attack,[4] the first BIOS rootkit found in the wild—usually can't be detected by software-based tools, because they're situated so low in the hardware/firmware/software stack. And as far back as the 2009 Black Hat conference, a then-18-year-old researcher presented the Stoned Bootkit, which seemed to revive the old Master Boot Record (MBR) rootkits of the late 1980s.[5] If the lessons of the past still apply—and experience suggests they do—these threats will be increasingly "commoditized" and widely circulated on the Internet, including the criminal underground using the dark Web.
4. **Deep, wide industry support.** The TPM standards-based technology has had 10 years to mature and is now embedded—at very low cost—in the products of almost every major device manufacturer. All ARM and Intel ATOM devices have TPM 2.0 embedded, and Intel's release of Haswell in the near future will mean TPM technology resides in all new versions of the Intel processors. As TPM becomes more and more pervasive, it also has become more affordable, adding nominal costs to the price of systems the chips are installed in (including the $250 Chromebook).

3 http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf

4 http://mason.gmu.edu/~msherif/isa564/fall11/projects/bios.pdf

5 http://www.blackhat.com/presentations/bh-usa-09/KLEISSNER/BHUSA09-Kleissner-StonedBootkit-SLIDES.pdf

5. **Lower acquisitions and operations costs.** While hardware acquisition costs are important, enterprises are even more sensitive to annual operations and support costs. Improvements in GUIs and management tools by PC manufacturers and OS vendors have also greatly reduced the ongoing costs of managing TPM functions. With TPM now embedded in devices of virtually every type, and from most major vendors, its cost has dropped dramatically. TPM now comes standard in some surprising packages, including highly commoditized consumer-grade devices like Google Chrome OS Chromebooks from Samsung,[6] convertible Windows 8 Ultrabooks from Sony[7] and Windows 8 tablets from Dell.[8] With TPM already installed in devices costing as little as $250 for Chromebooks and $1,200 for the high-end Ultrabooks, organizations can now take advantage of embedded hardware-based security, for which they used to pay a premium.

New vendors—including Gemalto, General Dynamics and Oracle—are joining the TCG initiative all the time. Chip manufacturers recognize that improvements must be understood and supported by the BIOS companies. Storage vendors recognize an opportunity in the universal requirement for protection of data at rest by compliance mandates all over the world.

## Example of Embedded Architecture

The Chromebook, a $250 consumer-grade netbook offered by Google and made by Samsung, among others, is one example of a consumer-oriented product that has a TPM built in. Google's process is illustrated in Figure 1.

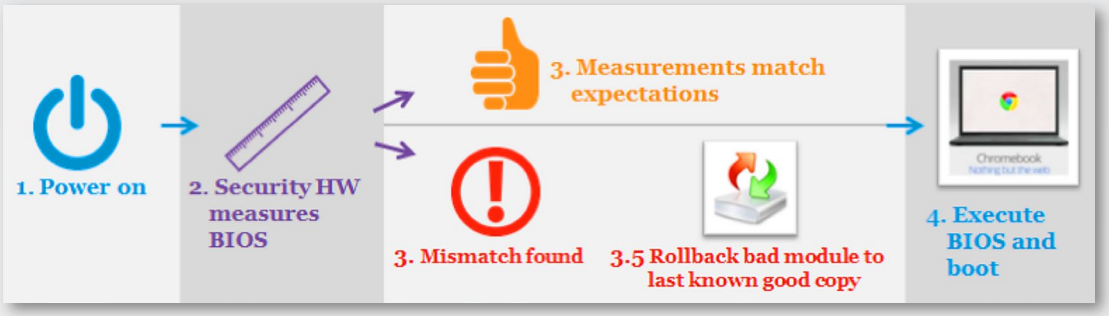


*Figure 1. TPM Root of Trust Attestation on Chromebook Architecture*

The Chromebook is powered on, and the TPM's Core Root of Trust Measurement (CRTM) measures the BIOS. This measurement either matches expectations, in which case the Chromebook continues to execute the BIOS to boot, or, in the case of a mismatch between the measurement and the reference, the Chromebook performs a rollback of the bad module to the last known good state and then executes the BIOS to boot.

6 http://www.samsung.com/us/computer/chrome-os-devices/XE303C12-A01US-specs
(The Samsung Chromebook is about $250 as of late May 2013.)

7 http://store.sony.com/c/VAIO-Duo-11-Ultrabook-Laptops/en/c/S_D_SERIES_PAGE
(The Sony Ultrabook is about $1,200 as of late May 2013.)

8 http://www.dell.com/us/business/p/latitude-10-tablet/fs
(The Dell Latitude 10 with TPM is about $500 as of late May 2013.)

# Meets Today's Demands

The increasing complexity of systems and the deeply embedded nature of today's threats means that security must extend deeper into the technology stack. TPM-enabled devices can check the integrity of the machine during the boot process, enabling protection and detection mechanisms to function in hardware, at pre-boot and in the secure boot process.

TPM processes and functions include:

- Pre-boot authentication (PBA). PBA allows the drive to be unlocked only when legitimate credentials (or a hardware token/personal identification number) are entered.
- The pre-boot encrypted drive. This protects the confidentiality of the data, as well as the configuration of the OS and applications on the drive.

Without encryption and PBA, an unauthorized user could try to boot the machine with a bootable disk or USB drive and hacking tools and then copy the drive's contents—or even just the Security Accounts Manager (SAM) file—for offline password cracking. While the TPM's main importance is to embed a hardware root of trust for integrity measurements, the TPM can also more securely manage encryption keys.

## Meets NIST Definitions for Trust at the Platform Level

TPM can be used to protect secrets and data that are worth money to cybercriminals (for example, intellectual property and personal financial information). Software-based security is regularly defeated. The National Institute for Standards and Technology (NIST) acknowledges the risk with software and software-based security in SP 800-164, "Guidelines on Hardware-Rooted Security in Mobile Devices."[9] In fact, NIST defines three trusted computing requirements in NIST SP 800-147, 800-155, and 800-164. To NIST, "trusted" means that the platform behaves as it's expected to behave: The software inventory is what we think it is, the configurations and security are in place and operating as they should, and so on.

This means that we must know that no unauthorized person has tampered with the software or its configuration. According to the NIST documentation, the currently available way to do this is to:

- Measure firmware, software and configuration data before it's executed
- Store those measurements in a hardware root of trust, like a TPM
- Validate that the measurements made actually match the measurements that were expected (if so, it can be attested that the platform can be trusted to behave as expected)

9 http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf

## Security to Scale

Hardware encryption mechanisms like TPM are well suited for organizations with scale and complexity of systems and systems management. This is one of the reasons the National Security Agency (NSA)[10] and NIST both recommend the concept of hardware-based security. As an NSA representative noted in a recent article, "TPM capabilities represent a shift against today's attackers who are embedding rootkits beneath the notice of today's software-based security solutions… We found TPM works very well for our high-assurance platforms."[11]

## Supports Audit

The TPM enhances security and the security audit process—and confidence in the audit process—which is a critical concern for many organizations today, particularly those with rigorous regulatory compliance requirements or valuable intellectual property. Because the system can attest to the state of the device and whether or not it blocked access based on that attestation, this data can be drawn from the platform management system for use in audit and investigations. For example, attestation to encryption and system state would be of value to auditors and is available in Windows 8 as Measured Boot.[12] The TPM signs a report with a key that exists only within TPM and uses its own integrity measurements to attest to that, providing evidence for auditors and system administrators, evidence upon which one makes the decision about whether to trust the platform.

In today's market, Wave Systems offers a product that may make these reports available and TCG's Trusted Network Connect (TNC) specifications describe how TNC-enabled networking gear (as from Juniper) can be used to get those reports from TNC-enabled endpoints (use the Integrity Measurement Client on the endpoint).

## Beating Bootkits and Other Malware

While no security is 100 percent tamperproof, the security processes enabled by TPM present far stronger protections of endpoints and their data than anything currently offered by software security. The good news is: Attacks conducted in labs still require physical access to the device to get the key, and even then they have to physically delaminate the chip or put sensors around the chip to read the electromagnetic radiation (DPA). We know that the population of "black hat" hackers capable of a serious, sustained threat against TPM-protected hardware is far smaller than those bent on breaking software security and encryption for OSes and applications.

Bitlocker takes into consideration that attackers will continue to up their game against hardware-based security. As such, Windows takes advantage of the TPM anti-hammering capabilities to prevent brute force attacks during pre-boot authentication. For devices that are designed to be secure from cold boot attacks without the need for pre-boot authentication, BitLocker can be used to prevent brute force attacks on Windows sign-in. If a brute force attack is detected, the device will automatically reboot in recovery mode and will require a 48-digit recovery key password to gain access to the disk.[13]

---

10 http://www.scmagazine.com/delayed-reaction/article/276462/2

11 http://www.scmagazine.com/delayed-reaction/article/276462/3

12 video.ch9.ms/teched/2012/na/SIA309.pptx, Slide 16

13 http://technet.microsoft.com/en-us/library/jj679889.aspx

## Enhanced Encryption

With the growing use of mobile devices to process company information, along with collaborative applications shared between devices, encryption is more important than ever. However, ease of use is a critical factor in encryption for today's on-the-go user population.

TPM also greatly enhances the software-based encryption key management mechanisms of Windows BitLocker, which otherwise requires that encryption keys be offloaded to a USB drive, introducing significant cost and management issues.[14] TPM supports the software-based encryption mechanisms used to encrypt the contents of desktop and notebook hard drives, including Microsoft's BitLocker drive encryption, which is included in most of the current corporate versions of Microsoft Windows. BitLocker is a form of software-based full-disk encryption that relies on a TPM to verify the integrity of the platform at boot. BitLocker on Windows 7 uses the TPM to validate boot integrity and to secure encryption keys. For Windows 8, boot-level protection is now handled through Microsoft's Unified Extensible Firmware Interface (UEFI) instead, although TPM is used for securing encryption keys. Through these changes, Microsoft has significantly enhanced the BitLocker back-end management product, MBAM,[15] for central deployment and administration of BitLocker keys, including unlocking encrypted computers—for example, when users have forgotten their PINs or passwords.[16]

### TPMs and Self-Encrypting Drives

**One increasingly popular approach to protection in today's fast-changing threat environment is the use of hardware-based encryption—for example, self-encrypting devices (SEDs)—to protect data at rest.[17] SEDs are drives (both traditional hard drives and solid-state drives) for desktops, notebooks and servers that encrypt all data written to the drive constantly, not via third-party software, but using a bulk data encryption co-processor built into the electronics of the drive controller electronics. SEDs for laptops/desktops conform to the TCG/OPAL standard for deployment and management and to the TCG/Enterprise standard for the data center. SEDs are widely used by organizations with strong data-protection requirements, such as law enforcement agencies, and other government bodies and businesses (for example, in health care) with rigorous regulatory compliance requirements.[18]**

**SEDs offer many benefits over software-based encryption.[19] For example, SEDs create their encryption keys internal to the device, and the keys are never exported from the drive, which is a security advantage over generating keys manually. Another value is that the drive has the compute resources to do encryption at bus speed, which results in an extremely low performance cost to encryption done by these devices, compared to software encryption, which relies on the laptop's CPU and RAM.**

**Another highly pragmatic benefit of self-encrypting technology is fast, inexpensive, end-of-life preparation for secure disposal. Companies that process credit card information, for example, are bound by the PCI DSS, which mandates that storage devices that contain or have contained credit card information must be wiped before they leave the building at end of life. Conventional data-wipe techniques are expensive and can take hours, but with any type of full drive encryption—including SEDs—a drive can be wiped in a mere 100 milliseconds using a process called "crypto-erase."**

**Even SEDs still need third-party support for key management issues such as secure key issuance and exchange, which has opened a market to companies like Absolute Software, Cryptomill, McAfee, WinMagic and Wave Systems to participate as key authorities.**

14 http://ctogonewild.com/2009/08/28/10-things-you-dont-want-to-know-about-bitlocker
15 https://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/mdop/mbam.aspx
16 SED management vendors include Absolute Software, Cryptomill, McAfee, WinMagic and Wave Systems.
17 http://www.scmagazine.com/delayed-reaction/article/276462
18 http://www.scmagazine.com/delayed-reaction/article/276462
19 http://www.trustedstrategies.com/papers/fde_samsung_ssd.pdf

## Support for Virtualization

Upgrade cycles—and especially hardware upgrade cycles—can take years, but factors like virtualization and cloud computing, consumerization and bring your own device (BYOD) policies are rapidly shortening the typical upgrade cycle. For this reason, TCG also supports security of virtual machines at the pre-boot level. One example of security for virtualization is the SecureView[20] desktop virtualization effort, originally designed for use by the Department of Defense. SecureView uses a hardware root of trust (a TPM and Intel's Trusted eXecution Technology [TXT]) to launch virtual machines in a carefully controlled environment. SecureView verifies the integrity of the XenClient hypervisor and detects offline tampering of the installed software or of the configuration of the device. See Figure 2.

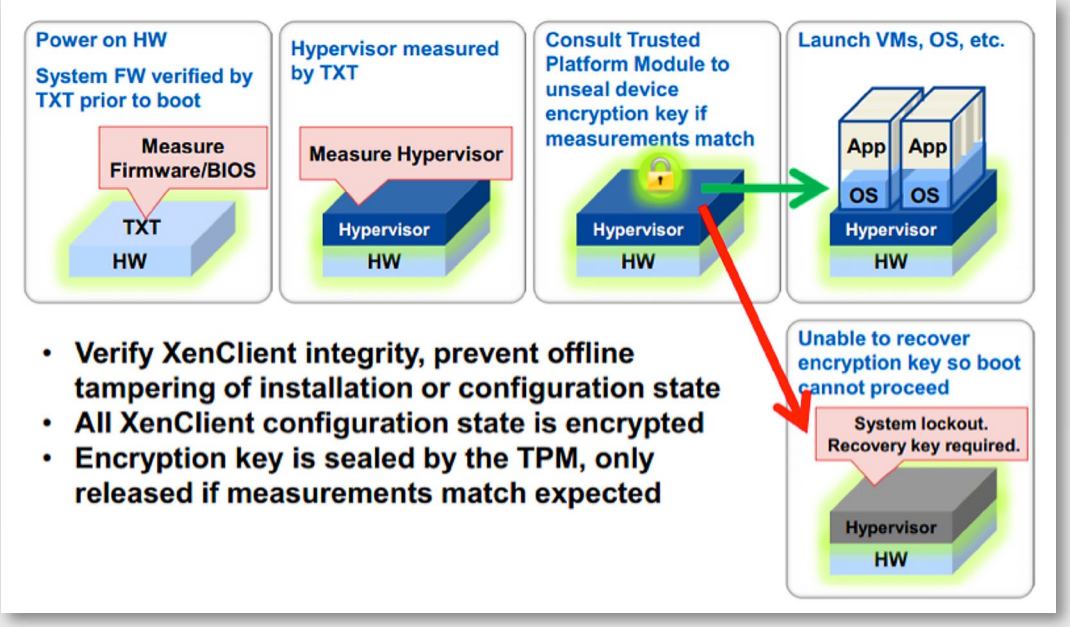


*Figure 2. TPM in Virtual Environment*

SecureView uses a feature of the TPM specification called "sealing" to ensure that secret data is decrypted and used only when there is no doubt the platform has not been compromised. When the system boots up, integrity measurements are taken and stored in Platform Configuration Registers (PCRs) in the TPM. It's possible to order the TPM to encrypt data and tie decryption to a conditional state of the device, so it is decrypted only if the values stored in the PCR match specified values and the platform is in a verified clean state. Since the XenClient configuration files are encrypted and the encryption key is sealed to PCRs in the TPM, the hypervisor will launch only when the PCR measurements match the expected values for a system that has not been compromised.[21]

20 http://www.ainfosec.com/wp-content/uploads/2013/05/AIS-SecureView-Overview.pdf

21 https://www.ncsi.com/nsatc11/presentations/thursday/real_world/durante.pdf, Slides 25–26

## Also Supports Post-Boot Processes

There are also use cases for TPM that take advantage of post-boot hardware security. One large enterprise that uses TPM for post-boot authentication is PwC (Price Waterhouse Coopers), an 180,000-employee audit, tax and consulting firm that has a global presence. A public case study from 2010, further discussed at an NSA hardware-based security conference in 2011, reveals that PwC wanted to strengthen the security of the VPN authentication process, which, until the use of the TPM, was handled in software.

Though they already had a working PKI, PwC wanted to eliminate the threat of stolen keys. Their requirement was thus to find hardware to protect the X.509 certificates for the VPN login, ideally in an inexpensive and hassle-free manner. PwC considered USB or smart-card solutions, but passed on them due to high Total Cost of Ownership (TCO), as well as being yet another token for the user base to carry and protect from loss or theft. PwC went with TPM because it is an open standard with multiple vendor support and was already present in 95% of PwC laptops.

PwC ended up taking advantage of a user-entered PIN to authorize TPM to release the certificate for login to PwC networks. PwC deployed 35,000 endpoints in 2010 (first public mention of this deployment), which means that in 2013 and beyond, other enterprises can be more confident of success, given the greater availability of devices with TPM, for less cost and with better tools for deployment and manageability.

# Implementation Advice

Key to making the TPM work on an organizationwide level is showing senior decision makers the value of using this mature technology that's already present in their systems—or will be after specific upgrade cycles. This value must be shown to both the security/IT (CSO/CIO) and the business (CFO/COO) decision makers. SANS recommends that security professionals working to leverage TPM capabilities consider the following.

## Make the Case

The business typically wants to either increase revenue or reduce costs. A convincing business case for TPM could, for example, be based on savings from reduced data breach recovery costs, because better credential management results in fewer breaches. It could also be argued that costs of administration go down when compared to various forms and versions of software encryption in use. It can also be determined that standardization on the TPM can reduce administrative costs overall and even enable complex onboarding of new systems in a secure manner—for example, in the case of a merger.

TPM will also be attractive to organizations that are planning to upgrade to Windows 8, which makes extensive use of the TPM. Windows makes the TPM available to enterprise and independent software vendor (ISV) applications through an API. One interesting use case that Windows 8 enables is the virtual smart card. Windows 8 uses the TPM to protect secrets that can also be protected on a smart card, eliminating issues related to deployment and management of cards, as well as user resistance to keeping track of them. Enterprises considering the use of smart cards might find the Windows 8-supported, TPM-based virtual smart card an attractive business case, especially if the TPM is already paid for and embedded in the hardware being used.

## Conduct a Cost Analysis

Because TPMs are an industry standard, and not exclusive to any one vendor, there's plenty of room for the competitive bids a procurement department is likely to request. And, of course, the TPMs may already be in place as a result of upgrades and on mobile endpoints. This helps with requests for specific vendor products that can take advantage of the tools you already have in place. This is, for example, an important driver for the use of BitLocker: An enterprise that needs to protect data at rest can use BitLocker, licensed through Windows, for $10 per seat.[22] BitLocker is a feature of Windows Ultimate and Windows Enterprise. With Windows 8, BitLocker is part of Windows Pro and Enterprise. In addition, Windows RT and Windows Phone 8 use device encryption based on BitLocker technology.

In a 2012 report, the Aberdeen Group also makes a financial case for using TPM as a hardware root of trust.[23] In this report, the cost per endpoint was $56 as opposed to the cost of other encryption/disk protections at $71 per device. It also showed reduced security-related incidents (4 versus 8). At an average cost of $130 per incident, they concluded this to be a $520 cost avoidance.

---

22 Microsoft MDOP, a paid service, includes MBAM for managing BitLocker, which sells for about $10 per seat for Software Assurance customers.

23 "Endpoint Security: Hardware Roots of Trust," by Derek Brink, June 2012. http://www.aberdeen.com/Aberdeen-Library/7080/RA-trusted-computing-security.aspx

## Have an Action Plan

Security professionals planning new or expanded TPM deployments should develop a concise action plan involving the following steps:[24]

- Conduct a survey of the devices that connect to the network for access and data transfer. Determine what applications and processes they are running and create a baseline of approved behaviors.
- Determine what TPM and SED capabilities are already in place on endpoints that can potentially be leveraged and how.
- Check for compatibility issues. This will involve, for example, checking for version and hardware compatibility, virtual TPMs in smartphones (also known as Mobile Trusted Modules [MTMs]) and SEDs in notebook computers and even servers.
- Establish a working group to determine near- and long-term use cases for TPMs and/or SEDs. The working group should coordinate with the IT professionals responsible for hardware replacement life cycles, so TPMs and SEDs are included in future acquisition requirements, where appropriate.
- Monitor the TCG's actions and the evolving standards of the TCG and its partners for more uses of the TPM modules (such as the virtual TPM in Arm's TrustZone, in addition to those in the desktops/laptops), combined with other modules for encryption (SED/BitLocker), mobile computing and virtualized environments.

In most cases, TPM deployments should begin with a small pilot project, focusing on a particular use case that has been identified. Still, it's essential to keep an eye on the bigger picture. For example, security and IT professionals will need to work together to determine what infrastructure, software and hardware will be needed to make effective use of TPMs in an increasingly heterogeneous enterprise computing environment. This is a key consideration when leveraging TPMs to create a baseline hardware root of trust.

It will also be important to understand where TPM activation and enablement are best placed in the overall process of IT procurement, deployment, management and disposal. This means understanding how hardware is purchased, and whether some of the steps in activation and enablement can be performed at the factory. It also means understanding how central management of the TPM will work with the identified use case—for example, whether it can be managed with existing central management tools—and whether upgrades or additions will be necessary.

In some cases, OEMs providing devices with TPMs onboard will activate and provision TPMs on behalf of their customers. As an example, PC OEMs will ship with TPMs turned on or off, per customer specifications.

24 TCG, "How to Use the TPM: A Guide to Hardware-Based Endpoint Security," http://www.trustedcomputinggroup.org/resources/how_to_use_the_tpm_a_guide_to_hardwarebased_endpoint_security

## Prepare for Tomorrow

As computing environments become more complex, many more security functions will rely on a hardware root of trust. This will be the case not only in the original TPM target platforms of desktop and notebook deployments, but also in the mobile, virtual and cloud server environments, as well as further use in the embedded computing space.

There are many components of TCG where future research would be of value. This includes interactions with "hard" TPM modules, as well as virtual and mobile TPM (like ARM architecture for mobile phones). At the network layer, for example, networking vendors are beginning to implement TCG's TNC architecture, as well.

We're already seeing Hardware Security Modules (HSMs), standalone TPM-like appliances dedicated to secure key storage and cryptographic operation, being deployed in major public cloud environments. This type of adoption by the largest public cloud vendor further cements the concept that hardware roots of trust belong in the data center, as well as the office.[25]

25 Safenet, a TCG member, is the supplier of HSMs to Amazon Web Services (AWS), which announced the CloudHSM product in April of 2013. http://aws.amazon.com/cloudhsm

# Conclusion

Even though the TPM's presence is growing rapidly, it's important to note that hardware security—the underlying concept of the hardware root of trust—has matured and is ready for deployment in a wide range of use cases.

Over the course of more than a decade, some of the most important players in the technology industry have committed to research and development of TCG standards-based solutions. These solutions are now fully mature and can be applied to protecting information across networks, on mobile devices, and in the cloud.

The hardware root of trust is already a critical component of the security architecture of enterprise and government networks, allowing for efficiently deployed and managed data protection across the entire data life cycle. For all these reasons, the TPM will be a major area of attention for security professionals today and tomorrow.

# Appendix and Links to Further Research

How to Use the TPM (for deployment advice for how to use TPM TODAY [not tomorrow]):
http://www.trustedcomputinggroup.org/resources/how_to_use_the_tpm_a_guide_to_hardwarebased_endpoint_security

TCG BYOD Architect's Guide:
http://www.trustedcomputinggroup.org/resources/tcg_byod_architects_guide

TPM:
http://www.trustedcomputinggroup.org/developers/trusted_platform_module

Virtualized Platform: One hardware TPM to work with the Virtual Machine Manager (VMM):
http://www.trustedcomputinggroup.org/developers/virtualized_platform

Remote "attestation" of endpoint with Platform Trust Services, tying TPM as hardware root of trust to TNC IF-M specification:
http://www.trustedcomputinggroup.org/resources/endpoint_security_hardware_roots_of_trust

SANS Reading Room paper for GREM Gold certification on UEFI security:
http://www.sans.org/reading_room/whitepapers/services/analysis-building-blocks-attack-vectors-unified-extensible-firmware_34215

# About the Author

**Gal Shpantzer** has 12 years' experience as an independent security professional and is a trusted advisor to chief security officers of large corporations, technology and pharmaceutical startups, Ivy League universities and nonprofits. He has been involved in multiple SANS Institute projects since 2002, including co-editing the SANS Newsbites, revising the e-warfare course and presenting SANS@Night talks on cyberstalking, CAPTCHA and endpoint security. In 2009, Mr. Shpantzer founded and led the privacy subgroup of the NIST Smart Grid Cybersecurity Coordination Task Group. He is a co-author of the "Managing Mobile Device Security" chapter in the *Information Security Management Handbook* (2010), and he has collaborated in presenting the ongoing Security Outliers project at RSA, CSI, BSides and Baythreat conferences. Most recently, he was a subject-matter expert in the development of the U.S. Department of Energy's Electric Sector Cybersecurity Capability Maturity Model (ESC2M2) in 2012, and he is currently working with the PACS-WG to alert and advise industrial controls system asset owners exposed on the Internet.

## About the Advisor

**John Pescatore** joined SANS as director of emerging security trends in January 2013. He has 35 years' experience in computer, network and information security. Prior to joining the SANS Institute, Mr. Pescatore was Gartner's lead security analyst for 13 years, working with global 5000 corporations and major technology and service providers. Before joining Gartner, Mr. Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and Public Key Infrastructures. Prior to that, Mr. Pescatore spent 11 years with GTE developing secure computing and telecommunications systems.

Mr. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a Bachelor's degree in Electrical Engineering from the University of Connecticut and is a NSA Certified Cryptologic Engineer. He is also an Extra class amateur radio operator, callsign K3TN.

*SANS would like to thank its sponsor:*

TRUSTED COMPUTING GROUP™

Last Updated: August 21st, 2017

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Tampa - Clearwater 2017 | Clearwater, FLUS | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Network Security 2017 | Las Vegas, NVUS | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| SANS Dublin 2017 | Dublin, IE | Sep 11, 2017 - Sep 16, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MDUS | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, DK | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, GB | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Data Breach Summit & Training | Chicago, ILUS | Sep 25, 2017 - Oct 02, 2017 | Live Event |
| Rocky Mountain Fall 2017 | Denver, COUS | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS SEC504 at Cyber Security Week 2017 | The Hague, NL | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Oslo Autumn 2017 | Oslo, NO | Oct 02, 2017 - Oct 07, 2017 | Live Event |
| SANS DFIR Prague 2017 | Prague, CZ | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| SANS Phoenix-Mesa 2017 | Mesa, AZUS | Oct 09, 2017 - Oct 14, 2017 | Live Event |
| SANS October Singapore 2017 | Singapore, SG | Oct 09, 2017 - Oct 28, 2017 | Live Event |
| SANS AUD507 (GSNA) @ Canberra 2017 | Canberra, AU | Oct 09, 2017 - Oct 14, 2017 | Live Event |
| Secure DevOps Summit & Training | Denver, COUS | Oct 10, 2017 - Oct 17, 2017 | Live Event |
| SANS Tysons Corner Fall 2017 | McLean, VAUS | Oct 14, 2017 - Oct 21, 2017 | Live Event |
| SANS Tokyo Autumn 2017 | Tokyo, JP | Oct 16, 2017 - Oct 28, 2017 | Live Event |
| SANS Brussels Autumn 2017 | Brussels, BE | Oct 16, 2017 - Oct 21, 2017 | Live Event |
| SANS Berlin 2017 | Berlin, DE | Oct 23, 2017 - Oct 28, 2017 | Live Event |
| SANS San Diego 2017 | San Diego, CAUS | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Seattle 2017 | Seattle, WAUS | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Gulf Region 2017 | Dubai, AE | Nov 04, 2017 - Nov 16, 2017 | Live Event |
| SANS Miami 2017 | Miami, FLUS | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| SANS Amsterdam 2017 | Amsterdam, NL | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| SANS Milan November 2017 | Milan, IT | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| Pen Test Hackfest Summit & Training 2017 | Bethesda, MDUS | Nov 13, 2017 - Nov 20, 2017 | Live Event |
| SANS Paris November 2017 | Paris, FR | Nov 13, 2017 - Nov 18, 2017 | Live Event |
| SANS Sydney 2017 | Sydney, AU | Nov 13, 2017 - Nov 25, 2017 | Live Event |
| SANS San Francisco Fall 2017 | OnlineCAUS | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |