Enterprise Security: Putting the TPM to Work

What is the best way to cost-effectively maximize enterprise information security? Consider a tool already at your disposal: the Trusted Platform Module, a security and cryptography chip installed in more than 100 million enterprise-class PCs. Learn how to put the TPM to work to unlock the full potential of 802.1X, VPNs, and authentication, and to improve your overall information security posture.

The Trusted Platform Module (TPM) Secures Endpoints

Want to dramatically improve the health and security of your enterprise endpoints? Many organizations already have a security tool at the ready: the Trusted Platform Module (TPM), a hardware-based security and cryptography chip built into virtually every enterprise-class desktop and laptop computer—PC or Mac—that ships today, as well as numerous consumer and SMB configurations. In fact, more than 100 million computers shipped to date have a TPM installed, and a number of RFPs from the Fortune 1000, as well as numerous government agencies, including the Department of Defense, explicitly require a TPM for all new computers.

Even though the chip is widely available, and dedicated management tools ship with enterprise PCs, many organizations have not yet put this valuable security tool to work. Perhaps that is because many IT managers report familiarity with the chip, but not its application.

In fact, an increasing number of hardware and software tools—with many more under development—now exploit the TPM. As a result, a growing number of enterprises have begun leveraging the TPM to provide crucial business capabilities, including protecting data at rest, making strong client authentication easier and more affordable, and implementing network access controls to improve overall endpoint security.

Hardware-Based PC Security

What exactly can the TPM do? For starters, the TPM can augment a PC with a secure hardware repository for safeguarding digital certificates, passwords, and other essential user credentials. The TPM also facilitates key management and escrow for verifying the identity of a PC; can securely sign, encrypt, and decrypt e-mails and digital documents; manages full-drive encryption; provides the second factor in multi-factor authentication; and helps assess the security and integrity of the host device.

Technology vendors are releasing products which utilize the TPM in ever more innovative ways. For example, many PC manufacturers, including HP, Lenovo and others, ship TPM-based PC security software tools, such as password vaults, as part of their standard enterprise client build, while Microsoft Vista BitLocker utilizes the TPM for secure start-up. On that front, the forthcoming HyperSpace platform from Phoenix Technologies will check PC security, pre-boot, to authenticate a device's identity, verify the integrity of trusted applications, and help minimize the threat of malware. Finally, the Secure Notebook full-disk encryption tool from Secude International AG secures access to the PC—and encrypted drives—using the TPM.

Foundation of Trust

The TPM creates a **hardware-based** foundation of trust, enabling enterprises to implement, manage, and enforce a number of *trusted* cryptography, storage, integrity management, attestation and other information security capabilities.

Prevent Data Breaches

In fact, many organizations are turning to full-disk encryption tools and self-encrypting hard drives, or planning to adopt Intel's new enterprise chipsets (codenamed Danbury) to fully encrypt any hard drive.

Simply having such capabilities, however, is not enough, either to secure personally identifiable information in the event it is lost or stolen, or for complying with numerous data privacy and security regulations. Rather, enterprises must actually enforce the use of these tools. On that front, Embassy Trust Suites from Wave Systems Corp. provides the requisite enforcement capabilities, as well as related key management tools, for organizations to manage a variety of strong authentication and data security tools—including full-disk encryption—and demonstrate compliance with numerous regulations.

Secure Servers

While initial TPM applications have focused on PCs, the TPM also secures servers, and numerous manufacturers, including IBM and Dell, now build the TPM into their servers to enable trusted, server-side computing, and to harden all client/software interactions. In fact, a recent Forrester Research report recommends enterprises now begin adopting servers containing a TPM to process all high-value transactions.

Future TPM Applications

As that suggests, software and hardware manufacturers are finding new ways to put the TPM to work. Yet numerous applications for the TPM already exist, to help enterprises improve overall information security, protect data at rest or in transit, and demonstrate compliance with numerous data security regulations. In other words, with the TPM already at large in the enterprise, why not put it to use now?

Top TPM Applications

Survey of current TPM users

Network Access	
• Access control	75%
• Wireless (802.1x)	74%
• VPN (IPsec)	74%
• Device authentication	71%
• Device attestation	48%
Data Protection	
• Secure email	75%
• Full-disk encryption	67%
• File/folder encryption	63%
• Key management	54%
User Authentication	
• PC login	88%
• User authentication	83%
• Secure boot sequence	79%
• Smart cards	45%
• Fingerprint biometrics	39%

Source: Aberdeen Group, 2008

TPM Success Stories

Organizations in a number of vertical industries already utilize the TPM to manage full-disk encryption, verify PC integrity, and safeguard data at rest:

- **Financial Services**: Publicly traded Fortune 500 firm determined that applying full-disk encryption costs far less than losing an unencrypted laptop, especially in this highly regulated industry. The CEO's data security mandate: Don't become a data breach headline.
- **Fast Food**: Pizza-maker Papa Gino's, with over 370 restaurants, uses Dell laptops and desktop with a built-in TPM to automatically encrypt all communications between stores and headquarters, and to secure passwords and bank account numbers. Ultimately, this helps it comply with multiple data security and privacy regulations, including the Payment Card Industry Data Security Standard (PCI DSS).
- **Big Pharma**: A leading Japanese pharmaceutical manufacturer with more than 20,000 seats deployed Lenovo PCs with a TPM, related digital certificate, and multifactor authentication software. This enables the company to restrict and monitor access to sensitive and regulated data via its Virtual Private Network (VPN).
- **Law Firm**: Practice with hundreds of personnel employs full-disk encryption to prevent data breaches, maintain attorney/client privilege, and avoid any damage to the firm's reputation resulting from lost or stolen PCs.
- **High-Technology**: World-renowned high-technology manufacturer's field force (2,000+ employees) carries laptops storing everything from client lists and product specifications to preferential sales prices and revenue forecasts. Using a TPM, all laptops are now automatically and completely encrypted, protecting this publicly traded company's confidential data.