Replacing Vulnerable Software with Secure Hardware

The Trusted Platform Module (TPM) and How to Use It in the Enterprise

With the support of over 140 leading hardware, component, software, service, computing, networking, storage, and mobile phone companies, the Trusted Computing Group (TCG) has developed and continues to develop open industry standards to deliver products and services with a higher level of trust to users. This trust is based upon a hardware element called a Trusted Platform Module (TPM).

In systems such as PCs and servers, the TPM is typically a microcontroller that securely stores passwords and digital keys and certificates that can provide unique identification. The TPM can be a separate integrated circuit (IC) or an embedded portion of another IC, such as an Ethernet controller. Using standard software interfaces, the TPM works with other security methodologies to ensure deployment of secure applications.

In the TPM, a co-processor handles cryptographic operations such as asymmetric key generation (RSA), asymmetric encryption/decryption (RSA), hashing (Secure Hash Algorithm (SHA-1)), and random number generation (RNG).

With increasing threats to security and the increasing cost of security breaches, the TPM provides privacy protection and interoperability across multiple platforms. Based on open, vendor-neutral specifications, the architecture of TPM ICs provides flexible implementation by system and device manufacturers as well as flexible deployment by the owners of these solutions. An organization that uses TPM-capable computing and communication products obtains greater security without lowering productivity or introducing new obstacles in manageability.

In addition to computers, hardware-based, embedded security subsystems that use TCG technology and include TPM capabilities can provide reliable and cost-effective protection for cell phones and PDAs and enable the enforcement of strong security policies to ensure trustworthy transactions for these wireless devices. In storage systems, the TPM can enable disk encryption and capabilities for trusted drives and network security.

Companies that have previously developed and currently market TPM chips, software, TPM-capable motherboards, and system-level products that comply with TCG specifications include: Atmel, Broadcom, Dell Computer, Fujitsu, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, National Semiconductor, NTRU, Softex, STMicroelectronics, Utimaco Safeware AG, Wave Systems and many others. In addition to PCs, the TPM provides security in voting machines, set top boxes, POS terminals, and ATMs.

One of the major TPM successes in 2007 was its use in Microsoft's Windows Vista operating system as part of the BitLocker Drive Encryption feature. In the Ultimate and Enterprise editions of Windows Vista, BitLocker encrypts the computer's boot volume and provides integrity authentication for a trusted boot pathway. Built-in command-line tools allow the encryption of other volumes as well. TPM and BitLocker support for additional cryptographic features and expanded volume encryption are expected to proliferate in future Windows versions.

Prior to Microsoft’s utilization of the TPM’s capabilities, over 70 million desktop and portable PCs with TPMs were estimated as shipped. This number is expected to increase to over 200 million in 2008. The TPM can also be found in servers and with the recent publication of TCG’s Mobile Trusted Module Specification that uses a subset of TPM commands, mobile phones and other types of mobile devices may include a TPM in the future.

Using the TPM

In addition to the TPM’s well-established role in desktop computers and use in Microsoft’s Vista operating system, it has demonstrated its value in several other applications. In the enterprise environment, one of its critical and unique roles is eliminating deceptive endpoints in Network Access Control (NAC). In NAC, an endpoint infected by a virus or other malware may lie about its health status, gain access to the network, and infect other machines. While software can

provide a level of protection, software is vulnerable to attacks as well. The limitations of software-based approaches can be overcome by using the TPM with its hardware-based security. In TCG's Trusted Network Connect (TNC) architecture, the TPM is used for integrity measurement and remote attestation.

During the boot process, the TPM measures (hashes) all the critical software and firmware components, including the BIOS, boot loader, and operating system kernel, before they are loaded. By making these measurements before the software runs and storing them on the TPM, the measurements are isolated and secure from subsequent modification attempts. When the PC connects to the network, the stored measurements are sent to the TNC server, checked against the server's list of acceptable configurations, and quarantined as an infected endpoint if a non-match occurs. However, this is just one example of the TPM's usage.

Based on the efforts of TCG's Storage Work Group, the group has implemented security protocols to enable trusted storage, such as on hard disk drives. Under one user scenario for trusted drives, when the authentication screen is displayed, the user simply selects their User ID and then enters their Password similar to normal software-only protection schemes. But, the User is confirmed by the drive and, once confirmed, the drive unlocks and the OS boots normally. Another example of a trusted storage function is Full Disk Encryption (FDE), which encrypts everything on the drive using drive hardware. FDE provides protection against loss or theft, as well as re-purposing and end-of-life. An FDE drive can be rapidly erased by simply deleting the key under administrator control.

Organizations that have applied TPM-based trusted computing include: pharmaceutical companies to protect trade secrets and authenticate remote access, a pizza franchise chain to transmit and receive sensitive financial data and employee records, a car rental company to secure PCs in thousands of locations that handled confidential customer personal information and financial data, and even the U.S. government's National Security Agency (NSA) is evaluating full disk encryption, with associated credentials stored in the computer TPM.

In spite of overwhelming indication of the need for improved protection for users of a variety of computing-based systems, including the enterprise network itself, a few remaining naysayers continue to voice skepticism for TCG's efforts. Among the misperceptions for the TPM are:

- It will take years before enough large companies and ISVs utilize the TPM
- There is insufficient justification for implementing a TPM
- Software can do the job without new hardware

However, Microsoft and other leading companies' use of the TPM and its ability to provide an improved solution to issues, such as the deceptive endpoint problem should dispel these misconceptions and accelerate the acceptance of the TPM to increase security in products and the entire network at the enterprise level.

Building on the foundation of the Trusted Platform Module, TCG members have invested extensive effort to develop open, industry-wide specifications for essentially every software aspect that impacts the enterprise and requires security. When TCG's specifications are implemented in PCs, servers, storage devices, mobile phones, PDAs, and the network, the enterprise-wide protection will essentially create a trusted enterprise.

For more information about the TPM Work Group, the TPM specifications, white papers, FAQs, and more go to: https://www.trustedcomputinggroup.org/groups/tpm/

The Trusted Computing Group's home page provides direct links to its efforts in PCs, servers, the software stack, infrastructure, networking, mobile phones, storage, and hard copy as well as the TPM: https://www.trustedcomputinggroup.org

For links to the member companies' products information: https://www.trustedcomputinggroup.org/about/members/