What is TPM 2.0? What does TPM do?

Trusted Computing Group (TCG) has been addressing trust and related security benefits for PCs, servers, network devices and embedded systems for over a decade, based on the Trusted Platform Module specification. (TPM).

A Trusted Platform Module is a microchip typically built into a computer to provide hardware-based security. It can be added later by diligent users who want to stick the chip in the motherboard. Not all motherboards offer a TPM connector, so you need to research your model first.

What does TPM do?

Picture 1 of What is TPM 2.0? What does TPM do?

Some, but not all, of the data you transmit during the day is sent unencrypted, in plain text. TPM chips use a combination of software and hardware to protect any important passwords or encryption keys when they are sent in this unencrypted form.

If the TPM chip finds that the integrity of the system has been compromised by a virus or malware, it can start in isolation mode to help troubleshoot. Some Google Chromebooks include a TPM, and during boot the chip scans the BIOS (the motherboard firmware that initiates the boot process) for unauthorized changes.

The TPM chip also provides secure storage of encryption keys, certificates, and passwords used to log into online services, which is a more secure method than storing them inside software. on the hard drive.

TPM chips in networked set top boxes enable digital rights management, so media companies can distribute content without worrying about it being stolen.

Who is TPM for?

Although initially targeted at businesses or large companies that want data security, TPM chips are now becoming a requirement for all laptops and desktops to keep them all secure. user.

How do you use TPM?

If you buy a PC with a TPM chip, you can enable its encryption to protect data by accessing the BIOS. IT departments typically manage TPM chips in enterprise devices.

Major laptop manufacturers - including Dell, HP and Lenovo - often include software applications that will help users access TPM features.

What can you do with TPM?

The most basic use for TPM is to set a login password for the system. The chip automatically protects that data, instead of keeping it stored on the hard drive. If a system has a TPM chip, its users can create and manage cryptographic keys used to lock the system or specific files.

Many people use TPM to enable Windows' BitLocker Drive encryption utility. When you boot a system with TPM and BitLocker, the chip runs a series of conditional tests to see if it's safe to boot. If TPM finds that the hard drive has been moved to another location, possibly stolen, it locks the system.

Laptops with built-in fingerprint readers often keep recorded fingerprints in the TPM, as the security of the TPM makes it a trusted storage location. The chip also enables smart card readers, which some companies require for user authentication and login.

Trusted Platform Module 2.0

Note: As of July 28, 2016, all new device models, series, or series (or if you are updating the hardware configuration of an existing model, series, or series with an update large, such as CPU, graphics card) must implement and enable TPM 2.0 by default. The TPM 2.0 activation requirement applies only to the manufacture of new devices.

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functionality. The TPM chip is a secure cryptographic processor that helps you perform actions such as generating, storing, and restricting the use of cryptographic keys. Many TPMs also include physical security mechanisms to prevent malware from tampering with the TPM's security functions.

Traditionally, TPMs were discrete chips soldered to a computer's motherboard. Such an implementation allows you as an original equipment manufacturer (OEM) to evaluate and certify the TPM separately from the rest of your system. Some newer TPM implementations integrate TPM functionality into the same chipset as other platform components while still providing the same logical separation as discrete TPM chips.

TPMs are passive: they receive commands and return responses. To realize the full benefits of TPM, you must carefully integrate the system hardware and firmware with the TPM to send commands and react to its responses. TPM provides security and privacy benefits to system hardware, platform owners, and users.

Starting with Windows 10, the operating system automatically initializes and takes ownership of the TPM. That means IT professionals don't need to configure or monitor systems anymore.

You finished reading the article "**What is TPM 2.0? What does TPM do?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com