Trusted Platform Module (TPM)

2.0: A BRIEF INTRODUCTION

The Trusted Computing Group (TCG) has been addressing the trust issue – and related security benefits - for PCs, servers, networking gear and embedded systems for more than a decade, driven by the Trusted Platform Module (TPM) specification.

The TPM standard defines a hardware root of trust (HRoT) widely accepted as more secure than software that can be more easily breached by attackers.

The TPM is used with software to enable features; open source APIs are available and custom software can be developed. Additional resources for software support also are provided later in this paper.

In many systems, the TPM provides integrity measurements, health checks and authentication services.

TPM EVOLVES

While the earlier TPM 1.2 standard was incorporated into billions of PCs, servers, embedded systems, network gear and other devices, the evolving Internet of Things and increasing demand for security beyond traditional PC environment led TCG to develop a new TPM specification, which recently was adopted as an international standard ISO/IEC 11889:2015.

For more flexibility of application and to enable more widespread use of the specification, TCG created TPM 2.0 with a "library" approach. This allows users to choose applicable aspects of TPM functionality for different implementation levels and levels of security. Also, new features and functions were added, such as algorithm agility, the ability to implement new cryptographic algorithms as needed.

ATTRIBUTES OF THE TPM INCLUDE:

- Support for bulk (symmetric) encryption in the platform
- High quality random numbers
- Cryptographic services
- A protected persistent store for small amounts of data, sticky-bits, monotonic counters and extendible registers
- A protected pseudo-persistent store for unlimited amounts of keys and data
- An extensive choice of authorization methods to access protected keys and data
- Platform identities
- Support for platform privacy
- Signing and verifying digital signatures (normal, anonymous, pseudonymous)
- Certifying the properties of keys and data
- Auditing the usage of keys and data

IN A TRUSTED PLATFORM THE TPM ALSO PROVIDES:

- Attestation: reporting platform state
- Sealing: using platform state to authorize access to keys and data

A TPM FOR MANY APPLICATIONS

With TPM 2.0, TCG created a library specification that describes all the commands/features that could be implemented and might be needed in platforms from servers to laptops to embedded systems. Each platform can choose the features needed and the level of security or assurance required. In this way, TPM 2.0 is much more flexible than the original TPM specification. That flexibility allows the newest TPMs to be applied to many embedded applications, including automotive, industrial, smart home and many more – and for designers and developers to select with more granularity the appropriate TPM capabilities for the targeted use case.

Four types of TPM are popular today, offering different trade-offs between cost, features, and security. TCG continues to evaluate market requirements to further evolve the TPM.

1

DISCRETE TPM
Discrete TPM provides the highest level of security, as might be needed for a TPM used to secure the brake controller in a car. The intent of this level is to ensure that the device it's protecting does not get hacked via even sophisticated methods. To accomplish this, a discrete chip is designed, built and evaluated for the highest level of security that can resist tampering with the chip, including probing it and freezing it with all sorts of sophisticated attacks.

2

INTEGRATED TPM
Integrated TPM is the next level down in terms of security. This level still has a hardware TPM but it is integrated into a chip that provides functions other than security. The hardware implementation makes it resistant to software bugs, however, this level is not designed to be tamper-resistant.

3

FIRMWARE TPM
Firmware TPM is implemented in protected software. The code runs on the main CPU, so a separate chip is not required. While running like any other program, the code is in a protected execution environment called a trusted execution environment (TEE) that is separated from the rest of the programs that are running on the CPU. By doing this, secrets like private keys that might be needed by the TPM but should not be accessed by others can be kept in the TEE creating a more difficult path for hackers.

In addition to the lack of tamper resistance, the downside to the TEE or firmware TPM is that now the TPM is dependent on many additional aspects to keep it secure, including the TEE operating system, bugs in the application code running in the TEE, etc.

4

SOFTWARE TPM
Software TPM can be implemented as a software emulator of the TPM. However, a software TPM is open to many vulnerabilities, not only tampering but also the bugs in any operating system running it. It does have key applications: it is very good for testing or building a system prototype with a TPM in it. For testing purposes, a software TPM could provide the right solution/approach.

Many IoT systems include sensors and cloud processing, which means virtualization. In a cloud environment, one clever way to implement a TPM is through a virtual TPM. The virtual TPM is part of the cloud-based environment and it provides the same commands that a physical TPM would but it provides those commands separately to each virtual machine.

TPM SOLUTIONS FOR DIFFERENT NEEDS

The five variations of TPM, discussed roughly in order of security level and decreasing cost, are shown in Table 1. To get a better handle on the cost and security level impact, the TPM supplier needs to be consulted.

TRUST ELEMENT	SECURITY LEVEL	SECURITY FEATURES	RELATIVE COST	TYPICAL APPLICATION
DISCRETE TPM	HIGHEST	TAMPER RESISTANT HARDWARE	$$$	CRITICAL SYSTEMS
INTEGRATED TPM	HIGHER	HARDWARE	$$	GATEWAYS
FIRMWARE TPM	HIGH	TEE	$	ENTERTAINMENT SYSTEMS
SOFTWARE TPM	NA	NA	¢¢	TESTING & PROTOTYPING
VIRTUAL TPM	HIGH	HYPERVISOR	¢	CLOUD ENVIRONMENT

TPM RESOURCES

- **An "open access" book intended to get one started with TPMs: "A Practical Guide to TPM 2.0 - Using the Trusted Platform Module in the New Age of Security"; Arthur, Challener**
  - http://www.springer.com/us/book/9781430265832
- **A reference book intended to help explain TPMs: "Trusted Computing Platforms - TPM2.0 in Context"; Proudler, Chen, Dalton; Springer**
  - http://www.springer.com/us/book/9783319087436
- **Software**
  - https://sourceforge.net/projects/ibmswtpm2/
  - https://chromium.googlesource.com chromiumos/third_party/tpm2/
  - https://github.com/vbendeb/tpm2_server
  - http://research.microsoft.com/en-US/downloads/35116857-e544-4003-8e7b-584182dc6833/default.aspx
  - https://github.com/PeterHuewe/linux-tpmdd/tree/tpm-emulator
  - https://github.com/PeterHuewe/linux-tpmdd/commit/9329f13c403daf1f4bd1e715d2ba0866e089fb1d
  - https://github.com/PeterHuewe/linux-tpmdd/commit/bbf2f7064c1452b47f11dfad340326b1205d863a