TPM 2.0 Specification Provides Critical, Vendor Neutral Technology to Respond to Security Demands in Today’s Volatile Threat Landscape

TCG has announced the availability of the TPM (Trusted Platform Module) 2.0 library specification. TPM 2.0 provides a critical technology response to the global need for a more secure computing environment.

Based on contributions and feedback from TCG member companies and security technology experts representing the world’s leading silicon makers, device makers, software and solution providers as well as researchers, governments and academic institutions, TPMs provide a secure root of trust to protect data in computers and mobile devices from digital and physical attacks, theft or loss.

Hundreds of millions of TPMs are embedded into PCs, servers, networking gear, embedded systems and other computing devices, where they help protect computers against unauthorized changes from malware, rootkit attacks and similar malicious activities. TPMs enable more secure processes within the system, such as digital signatures and key exchanges. The TPM can help ensure that unsafe, unverified or out-of-date systems don’t connect to a corporate network and provides a cost effective, built in hardware root of trust that can be used to authenticate devices and users.

TCG Specification in Public Review

PC Client Platform TPM Profile (PTP)

This specification discusses the specifics regarding the
requirements of the TPM for PC Client but only the requirements for the TPM itself, not the requirements for a platform integrating the TPM. This document discusses the details of what interfaces and protocols are used to communicate with the TPM and the platform-specific set of requirements. This document includes the definitions of the items identified in the TPM Library specification as “Platform Specific” such as the minimum number of PCRs required and NV Storage available. The target audience for this document is the TPM manufacturers but platform manufacturers should review it as well.

TPM 2.0 Mobile Command Response Buffer Interface
This specification defines an interface between a TPM and software. This interface is the Command/Response Buffer Interface (CRB). The CRB design is intended to work with a large number of hardware implementation options. With this interface, it is possible to write a driver that can interact with a TPM whether it is implemented as a discrete component on a peripheral bus or in an execution mode in a Protected Environment.

TPM 2.0 Mobile Reference Architecture
This specification defines the reference architecture for the implementation of a TPM in modern mobile platforms. This TPM executes within a Protected Environment and is referred to as a TPM Mobile. The architecture allows any possible implementation of the Protected Environment that meets the security requirements defined in the specification. Several example implementations are included.

TPM 2.0 Library Profile for Automotive – Thin
This Profile specifies a TPM that can be deployed into a resource constrained embedded automotive application. A top down approach is taken, beginning with a discussion of the differences between resource constrained automotive use cases and more widely understood wireless applications (as an example).

Given the diverse use cases inside the vehicle, it is possible to describe a vehicle as a composite industrial control system network with an Internet connection and a human user interface. Based on the complexity of this model, this profile is limited to a definition of the functionality of a TPM that can be deployed into resource and cost constrained scenarios within the vehicle.

TPM 2.0 Library Specification
This specification provides updates to the previous published TPM main specifications. The changes and enhancements compared to the TPM 1.2 include:

- Support for additional cryptographic algorithms
- Enhanced authorization mechanisms
- Simplified TPM management
- Additional capabilities to enhance the security of platform services

Architect’s Guides Available
TCG has published a new series of architect’s guides that provide step-by-step blueprints with examples and tips on how to implement TCG technologies. In each case, companies worldwide have built on TCG’s specifications to provide tools that provide security. Now those in the trenches can learn how to turn on and use powerful trust-based solutions - and in many cases, they can use their existing equipment and infrastructure.

Topics covered include:
- BYOD (Bring Your Own Device)
- Comply to Connect
- Cybersecurity
- Data Security
- Industrial Control System Security
- Mobile Security
- Security Automation

Call For Participation: Marketing Work Group
TCG is actively seeking additional members to become engaged in the Marketing Work Group (MWG).

The MWG seeks to do the following activities and relies on the support of the membership and participants to help deliver on the goals and objectives:
1) Drive awareness of TCG throughout relevant vendor and customer market segments
2) Educate about and promote the adoption of the standards, specifications, and/or solutions created by TCG and encourage adoption of products that support TCG standards through all appropriate marketing media
3) Communicate use cases from the Market to the technical Work Groups and from the technical Work Groups to the Market
4) Drive membership recruitment through all appropriate marketing mediums. Join Today>

With its focus on professionals and growing number of discussion groups, LinkedIn is a great tool for sharing information, discussing topics and how-tos, and getting feedback on the industry. Click here to Join us!

Using the TPM to Solve Today’s Most Urgent Cybersecurity Problems
Tuesday, May 20, 2014 at 10:00 AM PDT
More Info >

SEDs Great for Business, Says Samsung Read More>
IF-MAP 2.2 - Learning from Experience Read More>
Storing Data in Secure Times Read More>