



Embedded Systems and Trusted Computing Security

Security has become a major challenge for designers and developers of most systems and applications. Whether the system is a PC, a kiosk, a gateway or an industrial system, attacks and unauthorized access can lead to critical loss of data, downtime of the network and loss of productivity and revenue. How can embedded systems designers add security to new designs?

One answer might be in industry standards that have been developed and deployed widely in enterprise computing, which has faced the same security challenges. An organization called the Trusted Computing Group (TCG) has been working for years to create building blocks for trusted hardware and enabling software for security that is less vulnerable to virtual and physical attack. The products implementing these standards are now readily available for embedded design.

Trusted Platform Module (TPM) Overview

The basis of Trusted Computing is the Trusted Platform Module, or TPM. The TPM is a small piece of silicon affixed in a device. It securely stores digital keys, certificates and passwords and is more difficult to attack virtually or physically. TPM functions include:

- Asymmetric key functions for on-chip key pair generation using a hardware random number generator; private key signatures; and public key encryption and private key decryption of keys enable more secure storage of files and digital secrets. This is accomplished through hardware-based protection of (1) the symmetric keys associated with software-encrypted files (data, passwords, credit card numbers, etc.) and (2) private keys used for digital signatures. This includes use of the TPM random number generator to create keys and performance of operations on private keys created by the TPM (digital signatures, public key encryption for storage, decryption) in the TPM. Private keys created in the TPM are protected by the TPM even when in use.
- Secure storage of HASH values representing platform configuration information in Platform Control Registers (PCRs) and secure reporting of these values, as authorized by the platform owner. These features allow and enable verifiable attestation of the platform configuration based on the chain of trust used in creating the HASH values. This includes creation of Attestation Identity Keys (AIKs) that cannot be used unless a PCR value is the same as it was when the AIK was created.
- An Endorsement Key which can be used by an owner to anonymously establish that identity keys were generated in a TPM, thus enabling confirmation of the quality of the key without identifying which TPM generated the identity key.

- Initialization and management functions that allow the owner to turn functionality on and off, reset the chip, and take ownership, with strong controls to protect privacy. The system owner is trusted and must opt-in. The user, if different from the owner, may opt-out if desired.

An Endorsement Credential, in conjunction with Conformance and Platform Credentials, can be used, as authorized by the owner, to create Attestation Identity Key (AIK) Credentials that can be attested to by a certificate authority. TCG specifications describe the creation of these credentials in order to enable their use, but TCG will not issue credentials itself.

Discrete TPMs and versions integrated with other functionality currently are available from semiconductor vendors, including Atmel, Broadcom, Sinosun, STMicroelectronics, Winbond and others. Software for various applications and applications development is available from other vendors, and the TPM is operating system agnostic.

Why Use a TPM in an Embedded Design?

The TPM offers several advantages over proprietary hardware security solutions, and inherently, hardware security is stronger than software-only approaches. TPM benefits include:

- *Flexibility:* the broad command architecture allows use in a wide array of application areas. chip experts, the commands and protocols have been widely analyzed.
- *Standards-based:* the TPM uses standard cryptographic algorithms and protocols that are widely accepted and will interoperate with other systems using software implementations.
- *Turnkey solution:* TPMs are sold complete with internal firmware so that the chip does not have to be programmed. More importantly for designers outside the security field, algorithmic expertise is not required.
- *Strong security:* the TPM has third party certification (Common Criteria EAL 3+, 4+). Because it has been developed with input from a variety of security and
- *Exportable:* the TPM and systems incorporating TPMs can be exported worldwide.

Embedded Applications

Any number of embedded applications can benefit from the security enabled by the TPM. Some of these include:

Confidence in Current State: modern equipment can be configured in many ways and typically works with a variety of software modules. Modules may be corrupted (maliciously or inadvertently). For safety or reliability reasons it may be necessary to do a real time-time audit or otherwise confirm the state. The TPM can:

- As each module is loaded, its value (hash) is added to the PCR registers. The core software or hardware ensures that nothing is loaded without being hashed.

- At any time, the system or a remote entity can ask the TPM to sign the PCR state with a TPM key. This can verify that at that particular time, that particular system was in that particular state.

Trusted Download of Software Updates: Systems are so complex that the use of flash memory to permit in-system updates is commonplace. A challenge is managing these downloads to prevent faulty software from being run or to require proper payment.

The TPM can help:

- Perform the asymmetric algorithm signature verification so that the system does not need to incorporate separate asymmetric cryptographic functions.
- Store the root of trust for the verification chain securely so that it cannot be modified.
- Authenticate the device to a download site and maintain audit trails of updates.

Secured Network Communications: an industrial control network needs to know that the nodes are authentic and that the communications channels are not being corrupted.

With modest computing capability and high volumes, sometimes it isn't practical to build in high security. The TPM can:

- Use signatures to authenticate nodes, relying on the Common Criteria certification process to provide the assurance that the underlying processes do not allow for cloned signatures and hence cloned nodes
- Use key exchange mechanisms to build dynamic session keys for communications.
- Result in lower costs – practical for a 10,000 node web.

Reliable peripheral identification: Especially in high-value systems, it's important to ensure that add-on or replacement parts are authentic. There's often no way for the system to achieve the necessary confidence. In this case, the TPM can help. For example:

- The OEM manufacturer includes a TPM in the part, along with a signature of a TPM key. When necessary, the system requests the new part to sign a random number to verify its authenticity.
- Parts can be personalized – either to work with a particular system or to be configured in a special way – by using the TPM to secure data that then requires some system secret to decode.

Local Secure Storage: Many embedded systems store, either permanently or temporarily, data that could be sensitive. For example, data stored could be later printed or faxed to unauthorized users. There is sensitive transaction information in point of sale and similar systems, as well. This equipment is connected over a network, making it vulnerable to a remote attack. The TPM can:

- Encrypt all stored information in disk/flash.
- Store keys in the TPM, where they are inaccessible.

Personnel authorization: Specific individuals may be authorized to perform varying operations on a piece of equipment. How does the system store both the identifiers (e.g. password) as well as protect the capability to authorize users? Systems with TPMs can enable:

- An authorization check can be done inside the TPM, so that passwords never need to be stored in the clear. The TPM can also support token or smart card authentication schemes.

- The authorized capability can be encrypted and only released when authorization validation happens correctly. (e.g. encrypt special program blocks).

TCG and Standards

The Trusted Computing Group is a not-for-profit corporation with international membership and broad industry participation from more than 110 semiconductor, system, software, networking and service provider companies. The purpose of TCG is to develop, define, and promote open specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.

TCG was created with an organization structure and governance model, as defined by the TCG bylaws, which is similar to many other computing industry standards bodies. This includes the following:

- An open membership model with multiple membership levels
- A board of directors consisting of Promoters and elected Contributor members
- Multiple work groups that are open to Promoter and Contributor members and seek active participation by these members
- A reciprocal reasonable and non-discriminatory (RAND) patent licensing policy between the members

This structure is designed to enable the expedient development of open, industry-standard specifications with broad industry participation and to foster widespread adoption of the organization's specifications.

Information on TCG, member products and specifications is located at www.trustedcomputinggroup.org.

All brands and trademarks are the properties of their respective owners.