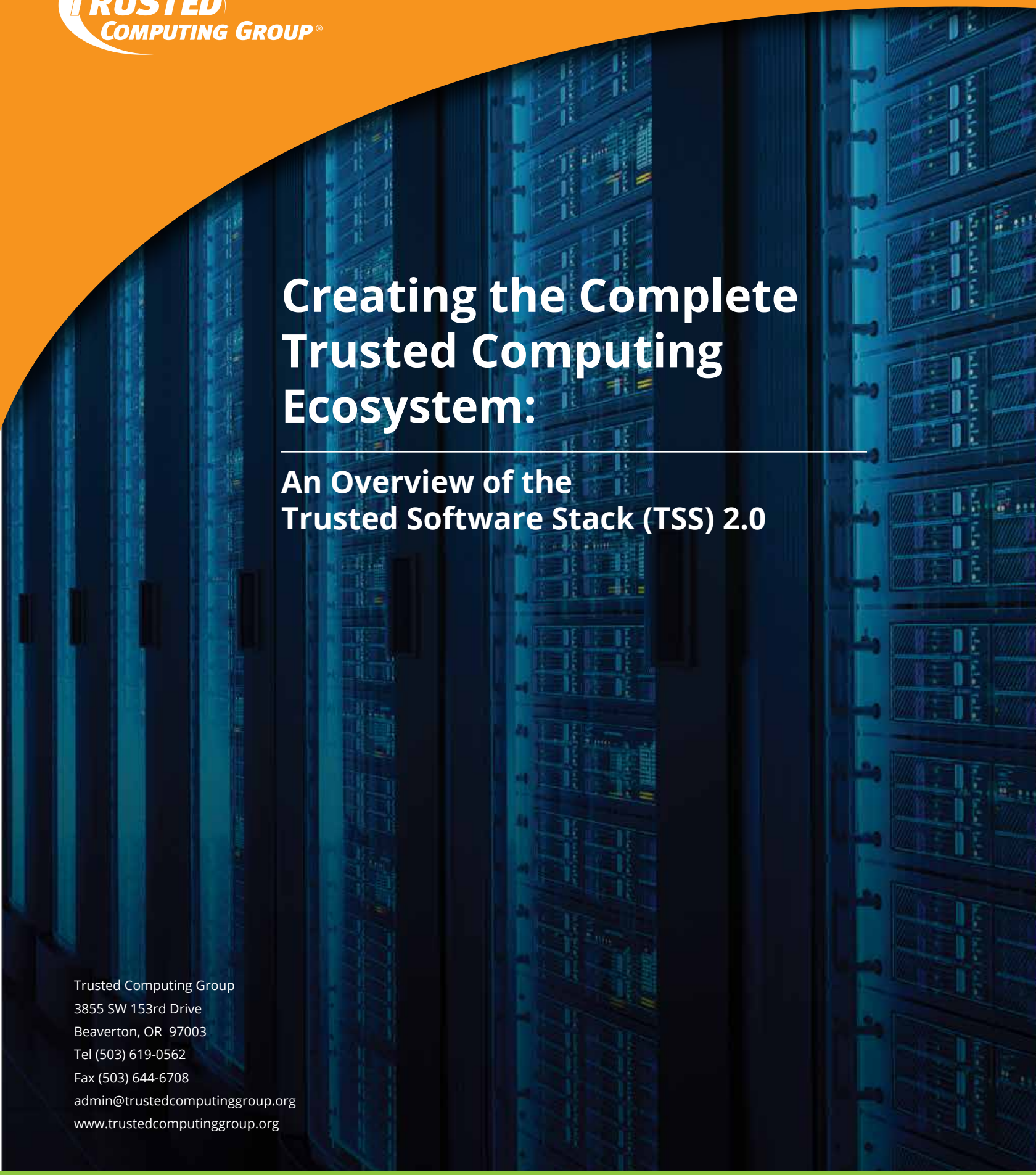
FEBRUARY 2018

TRUSTED COMPUTING GROUP®



Creating the Complete Trusted Computing Ecosystem:

An Overview of the Trusted Software Stack (TSS) 2.0

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97003
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

© 2018 Trusted Computing Group | All Rights Reserved

AN OVERVIEW OF THE TRUSTED SOFTWARE STACK (TSS) 2.0

High-end computing systems such as those used in financial institutions, critical industries (including healthcare), large data centers, and more require hardware-based security. These heavily regulated security applications must employ very expensive hardware security modules (HSMs).

In contrast, all the other (more cost sensitive) platforms in the world store keys and certificates in file systems and the user hopes that firewalls and software-only solutions provide sufficient protection.

Antivirus programs, firewalls, secure network links, compliance management and other software-based approaches provide "top down" security. Top-down security approaches essentially provide security on the perimeter of the system in an attempt to stop attackers from penetrating the system. These traditional top-down security approaches do not start running until well within the bootup of the system and they cannot protect the lower layers of the system software stack leaving the system vulnerable to serious and largely undetectable attacks (i.e., Rootkits and Bootkits).

Trusted computing implements bottom-up security which begins at the first instruction the system executes when booting and extends as far into the operating system and applications as system software designers desire it to go. A comprehensive security approach using top-down and bottom-up security provides protection for all the software in the system *(Figure 1)*. Trusted computing also can be used to ensure strong device identity for remote management and code updates.

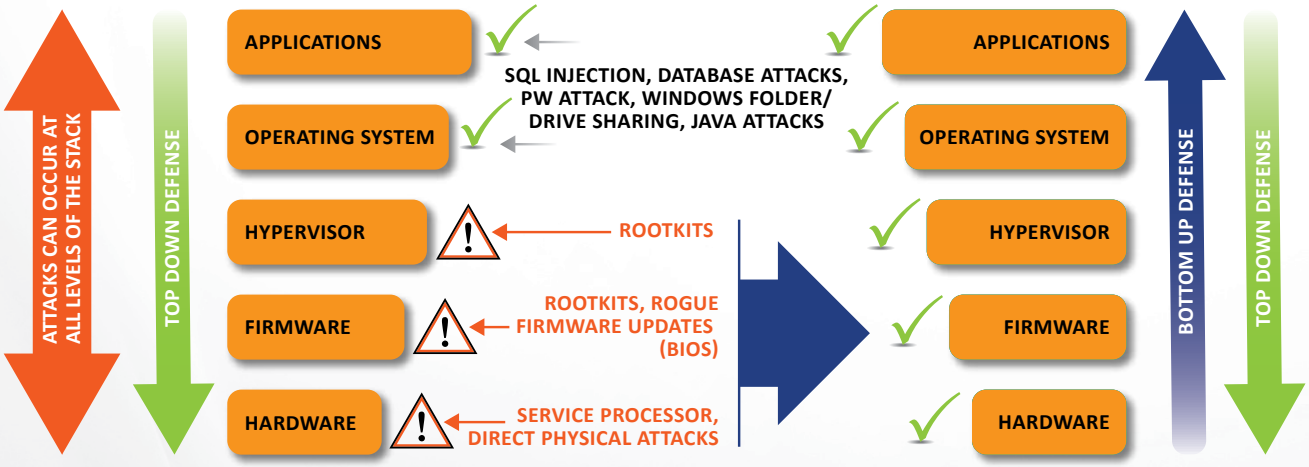


Figure 1. The shortcomings of a top-down only approach are corrected with a comprehensive (top down and bottom up) security solution.

The bottom up solution requires trusted hardware, firmware and software. To provide the most rigorous hardware protection, companies introduced the first hardware-based Trusted Computing Module (TPM) based on Trusted Computing Group (TCG) specifications more than a decade ago. With the recent announcement of TPM 2.0, TCG now has standards for discrete, integrated, firmware and software TPMs (listed in decreasing security order) offering different tradeoffs between cost, features, and security for essentially all applications.

Complementing TPM 2.0, TCG also recently announced the TCG Software Stack (TSS) 2.0 to complete the support infrastructure for trusted computing. Building on the foundation of TSS 1.2 that has been available since March 2009, TSS 2.0 addresses some of its missing pieces and simplifies the programming requirements for the software. The trusted computing-enabled firmware builds a "transitive trust chain" and establishes systems measurements from a Core Root of Trust for Measurement (CRTM) to launch bottom-up security.

With TSS 2.0, OSs, RTOSs, firmware become trusted applications that seal secrets to protect overall platform security to the TPM Programmable Configuration Registers (PCRs) and use the TPM as an HSM where appropriate.

Copyright© 2018 Trusted Computing Group | All Rights Reserved

BUILDING SOLUTIONS WITH TRUSTED COMPUTING

For those unfamiliar with the TPM, it Is best described in two pieces. It can be thought of as a code measurement / key sealing system combined with a HSM (hardware security module), but the HSM can be achieved at significantly lower cost points.

The TPM's trusted computing functions include PCRs for measuring code, key sealing and enhanced authorization. The HSM section contains key storage and a cryptographic acceleration engine. The TSS 2.0 specification defines several Application Programming Interfaces (APIs) that simplify implementing a TPM in an end product.

The TCG Software Stack 2.0 (TSS 2.0) was developed by the TCG to provide a trusted system utility that allows the operating system and applications to elegantly share the system's TPM. There are other pieces of software that have described themselves using the term TSS 2.0, but there is only one TCG Software Stack 2.0.

Middlewares such as Public-Key Cryptography Standards #11 (PKCS#11) can be interfaced to TSS 2.0 to allow legacy applications to use the TPM as if it was a traditional HSM or smartcard.

Two specific use case examples are shown in Figures 2 & 3 and demonstrate how TSS 2.0 enables the use of the TPM's capabilities.

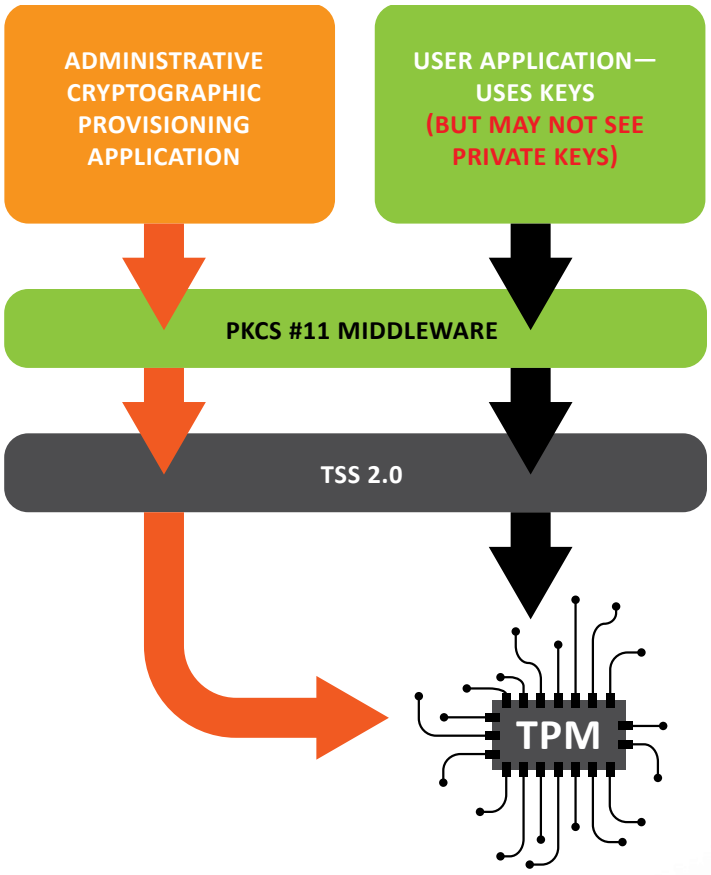


Figure 2. Use Case 1: HSM-style key store and use can be provided by a TPM.

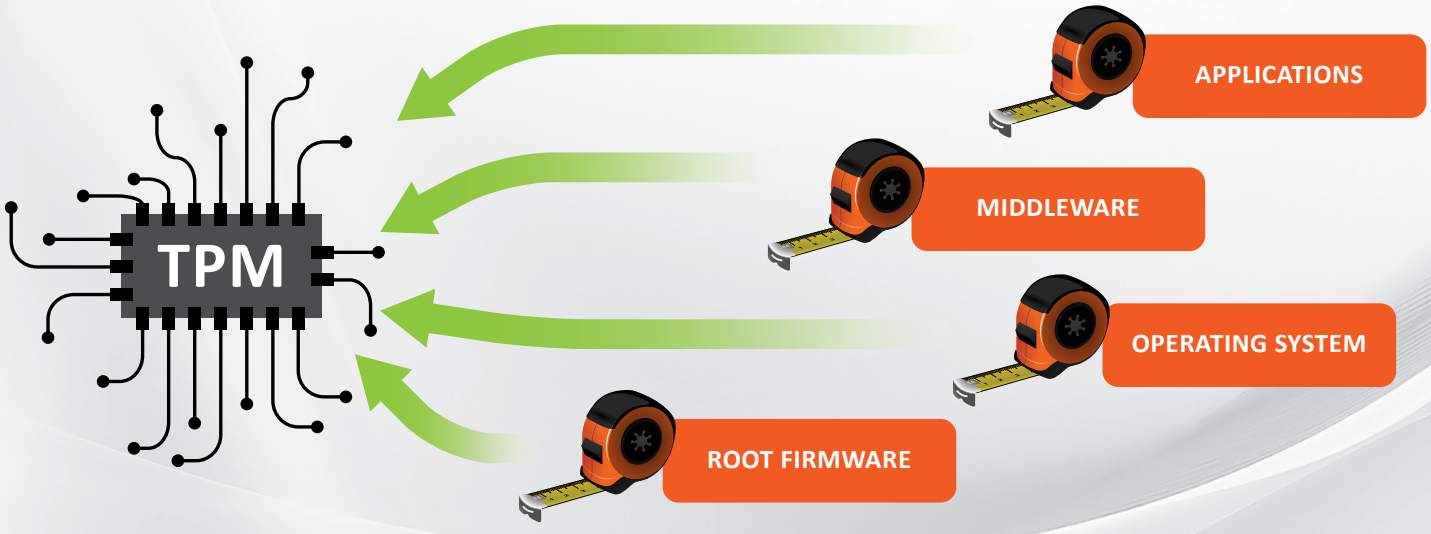


Figure 3. Use Case #2: With TSS 2.0, the TPM can measure software—seal keys, detect attacks, provide endpoint management and more.

Copyright© 2018 Trusted Computing Group | All Rights Reserved

TSS 2.0 BENEFITS

Together with the TPM 2.0, the TSS 2.0 helps programmers and significantly reduces their programming task by:

- Handling the marshalling/unmarshalling needed for communication with a TPM and handling multiple TPM applications
- Providing synchronous and asynchronous function call models for communicating with the TPM
- Encrypting the data stream from the software to the TPM stopping side-channel (hardware probing) attacks (achieving Common Criteria Evaluation Assurance Level (EAL) 4++)
- Simplifying context and session management needed when applications work with TPMs
- Providing varying levels of abstraction (depending on the TSS layer used) simplifying the task of using the TPM
- Providing "scalable solutions" that allow different code footprints from the smallest Internet of Things (IoT) device up to server applications

Using the official TCG Software Stack (TSS 2.0) specifically provides a standardized API which permits applications to use the same programming model across platforms with no need for completely different APIs on each platform.

For this reason, many governments and critical industries will specifically specify its use in their requests for proposals (RFPs) thus requiring the use of the official TSS 2.0 in your product to meet their procurement requirements.

To ensure that you meet these RFP requirements, make sure you are using the TCG Software Stack 2.0 (TSS 2.0) and not another solution describing itself as a TSS. TSS 2.0 complies with modern "clean programming" techniques to make code more maintainable and more secure. Its capabilities include:

- No function overloading—High semantic content
- Strong type checking—No variadic variables
- High semantic content—others (including yourself) will be able to read your code, understand it and maintain it over the lengthy product lifecycle that must be supported.
- No global variables
- Both synchronous and asynchronous call support.
- TSS 2.0 implementations are written in C99 in such a fashion as to make it easy to write language bindings.
- The TSS 2.0 API was created to be compatible with Motor Industry Software Reliability Association (MISRA) coding standards (required in embedded and IoT products where safety is an issue). Note: The implementation underlying the TSS 2.0 may or may not be MISRA compliant.

In addition to being developed and scrutinized by the TCG community at large, strong versioning and revision control is ensured by the design of the TSS 2.0. Your TSS 2.0 applications will tend to fail at compile time – not run time – with TSS 2.0's strong type checking and high semantic content. This is a powerful method of stopping errors from reaching the field. This supports a "fail early, fail fast and not at the customer" strategy. Figure 4 shows the interactions of the various TSS 2.0 defined structures.

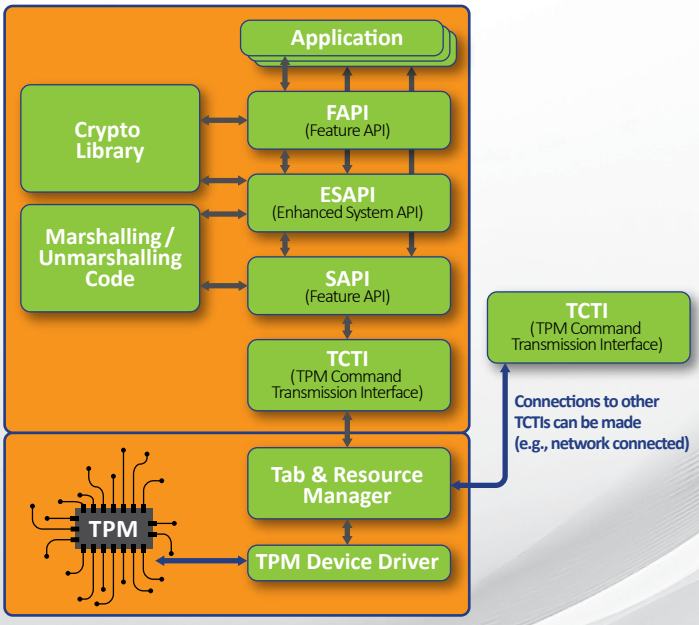


Figure 4. The TSS 2.0 software stack includes Marshalling/ Unmarshalling API (MUAPI), Feature API (FAPI), Enhanced System API (ESAPI), System API (SAPI), TPM Command Transmission Interface (TCTI) and more.

Copyright© 2018 Trusted Computing Group | All Rights Reserved

EASE OF USE WITH TSS 2.0

With the Feature API (FAPI), TSS 2.0 provides ease of use that was not available for TSS 1.2. It allows programmers to interface to the TPM without having to be TPM experts.

The Enhanced System API (ESAPI) is another new ease of use aspect to TSS 2.0. ESAPI provides easier context management and the ability to encrypt the data stream to the TPM stopping side-channel attacks (and essential to EAL4++).

The System API (SAPI) doesn't need a file system or a heap data structure. It can be integrated with boot firmware or used in the smallest IoT devices.

The TPM Command Transmission Interface (TCTI) significantly helps development programmers. It allows the use of TPMs other than the primary TPM on a platform. You can target TPM simulators and even remote TPMs with TCTI.

The Tab and Resource Manager will vary depending on the operating system. It allows multiple applications and the kernel to share TPM resources.

Drivers are available today in Linux and Windows but some I/O platforms may need a modified or custom driver. A brief summary of the code requirements for TSS Layers is shown in Table 1.

Code Requirements \ TSS Layers	SAPI	TCTI	ESAPI	FAPI	Tab and Resource Manager
File I/O	No	No	No	Yes	No[2]
Cryptographic function	No	No	Yes	No	No
Heap	No	No	Yes	Yes	Yes
External library dependency	No	No	No	No	No
Context base state	Yes	Yes	Yes	Yes	No
Able to do retries	No	No	No	Yes	No
Support possibility of reduced code size[1]	No	No	No	Yes	No
Abstract TPM details from programmers	No	No	No	Yes	No
Power management	No	No	No	No	Yes

[1]By offering static libraries

[2]Depends on power management

Copyright© 2018 Trusted Computing Group | All Rights Reserved

ENABLE TRUST—NOW

Since TSS 2.0 is now public, full scale deployment can begin today. The specifications can be reviewed at: https://trustedcomputinggroup.org/work-groups/software-stack/. Some implementations are available as well. An open source version of TSS 2.0 for Linux up including the lower portions of TSS 2.0 up through the SAPI layer is available now. Commercial implementations of the full TCG TSS 2.0 stack with support for multiple operating systems and ESAPI are available now. Commercial versions with FAPI support will available shortly after TCG releases the next version of the TSS 2.0 FAPI specification in the very near future.

Note: When looking for TSS 2.0 offerings, be sure the TSS 2.0 is TCG compliant. Some suppliers have used the term TSS 2.0 for products that do not conform to the TCG specifications.

With this final piece in place, it's time to get to work on adopting the trusted computing security model.

MORE INFORMATION

Open source software stack:
https://github.com/tpm2-software/tpm2-tss

Commercial solutions:
https://assets.onboardsecurity.com/static/downloads/TSS-2.0-Data-Sheet-05082017.pdf

Copyright© 2018 Trusted Computing Group | All Rights Reserved