How to secure network equipment using Infineon OPTIGA™ TPM hardware-based security solutions, the TPM Software Stack and Lanner security expertise

www.infineon.com

Contents

Abstract

Computers, servers and the people that operate them used to be the primary target of attackers. Today, because of increasing connectivity and dependence on networks, network equipment has become a frequent target for attacks, especially more sophisticated attacks on large industrial and commercial organizations and even government agencies. As a result, unprotected routers, switches, firewalls, gateways and wireless access points provide the newest targets for attackers.

The Trusted Computing Group's (TCG's) open document "TCG Guidance for Securing Network Equipment Using TCG Technology" describes how architects and designers can secure this equipment.[1] While this TCG document provides the theory, additional effort is required to implement this protection. Using the techniques described in the TCG document, developers can employ Infineon's OPTIGA™ Trusted Platform Module (TPM) and TCG's TPM Software Stack (TSS) to provide enhanced security to protect network equipment. This white paper describes the concepts and steps that must be understood to achieve the trust and security required for network equipment in commercial, industrial and government networks:

- Threats to network equipment and resulting risks
- Recommended countermeasures
- Practical implementation steps

With a thorough understanding of these concepts and steps, the reader can proceed with confidence.

Threats to network equipment and resulting risks

Commercial enterprises, industrial organizations, and governments experience frequent attacks. Most commonly, these attacks target computer servers and end-user equipment such as laptops and phones. However, attackers are increasingly seeking out less traditional and therefore less guarded targets, such as network equipment. If successful, their attacks can compromise the network equipment by replacing the proper hardware, firmware, software, or configuration with a malicious alternative.

Compromised network equipment can be especially dangerous for several reasons. First, compromised network equipment can be used to spy on communications. Second, messages sent through the network equipment can be silently modified to disrupt normal operations. Third, messages can be dropped to hide notifications of an attack in progress. Fourth, critical configuration data such as DHCP messages, DNS responses, and software updates can be altered to infect systems that receive the maliciously altered data. Fifth, supposedly private networks such as VPNs and VLANs can be penetrated. Rarely does anybody suspect that the network equipment might be compromised.

Network equipment may become compromised in many ways. First, the equipment may be counterfeit from the start. Second, the equipment may become compromised in the supply chain. This is especially likely with used or "gray market" equipment.[2] Third, external attacks after deployment may cause network equipment to become infected. Fourth, a trusted insider may alter the network equipment.

The risks caused by compromised network equipment are substantial. Confidential data can be stolen, leading to data breaches. Building automation systems such as door locks and fire alarms that operate on separate VLANs can be impacted. Firewalls can be breached. Even industrial control systems today are often based on Transmission Control Protocol/Internet Protocol (TCP/IP) over Ethernet or legacy networks. These systems have network equipment such as switches and routers. Because industrial systems are rarely updated, they are often vulnerable to well-known attacks so they depend on network equipment to isolate them from attacks. As we have seen, this isolation can be pierced by compromising the network equipment itself.

Fortunately, network equipment makers are starting to deploy Trusted Computing technologies for securing their products against attacks. The rest of this document describes these Trusted Computing technologies and how they can be used to restore confidence in the security and integrity of network equipment.

Recommended countermeasures

Standards for trusted computing

The Trusted Computing Group, an organization consisting of computing, networking, software and other security experts, has been developing open standards for Trusted Computing for nearly two decades. The foundation for these standards is a secured component called a Trusted Platform Module or TPM. The first widely used TPM specifications date to 2003 so they are not exactly new. In fact, TPMs are widely used in many domains (e.g., PCs) and have become an international standard (ISO/IEC 11889). One of the more surprising aspects of TPM is that some equipment manufacturers already have a TPM in their equipment but they do not take advantage of its capabilities. A better understanding of the problem and the solution can change this.

The TPM provides a hardware-based root of trust that is far more resistant to attacks than software-only approaches. Today, with the most recent TPM 2.0 specification, a TPM can take as many as five different forms but the most common form is a hardware security chip.

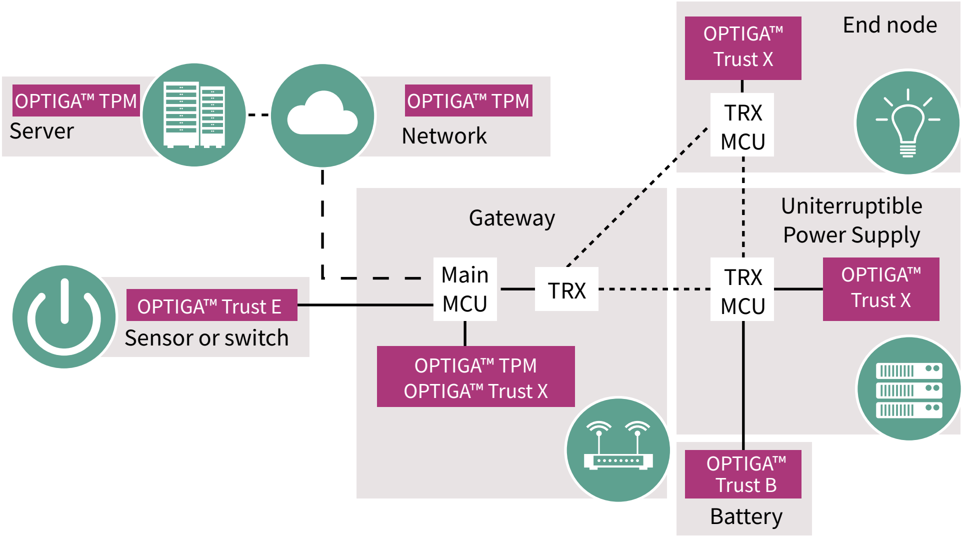
Leading semiconductor suppliers, like Infineon, offer TPM chips that conform to the TCG TPM 2.0 specification. Using these chips, manufacturers and users can implement trusted computing in computers, embedded systems, cloud services and networks - including network equipment. All TPMs support the same commands but there are subtle, and not so subtle, differences. Only a top quality TPM can provide the security needed to resist sophisticated attacks.

The Infineon OPTIGA™ TPM product line

Infineon offers a wide range of TPMs with different interfaces, different temperature ranges and different versions depending on the needs of the customer. One of the most important differentiators for Infineon OPTIGA™ TPMs is the range of different versions to address specific applications, including a standard line of TPM products suitable for use in typical computing devices like laptops and also special TPM products designed for automotive and industrial applications, which offer higher reliability, longer lifetime and an extended temperature range.

People who build or deploy network equipment may need to have extended temperature range and extended product lifetime because the network equipment may be mounted in an outside location where it will experience temperature extremes and where reliability is key because replacing equipment is problematic. As an additional differentiator, all OPTIGA™ TPMs are tested against TCG's TPM test suites to achieve highly compatible operation and interoperability, certified by the TCG, and listed on the TCG list of certified products.[3]

Infineon OPTIGA™ TPMs have been independently evaluated and certified to Common Criteria Evaluation Assurance Level (CC EAL) 4+. This is also a mandatory requirement of the TCG to achieve the approval of a TPM product. They include 6 kilobytes of user-accessible non-volatile memory and support Elliptic Curve Cryptography (ECC-256) and RSA cryptographic algorithms, with the private key stored in secured hardware (HW). As shown in Figure 1, Infineon also offers a line of OPTIGA™ Trust products with other security feature sets (not TPMs) that can be used to address a variety of system trust requirements.



Note: TRX indicates communications function

Figure 1. Infineon provides a variety of OPTIGA™ Trust products for different applications in networks, servers and connected devices.

Additional Infineon OPTIGA™ TPM product differentiation comes from expert support based on direct TCG specification involvement, a global network of trained support engineers and more than a dozen different technology partners that provide products and services complementing the TPM chips.

Lanner is an excellent example of the synergy that results from partnering. Lanner customers with engineering activity in locations such as India, Taiwan and other global locations will find a wide variety of hardware platforms to choose from with support from local experts who can help with any problem that could occur, whether it concerns the Infineon OPTIGA™ TPM hardware or any software issues.

TPM Software Stack

TCG’s TPM Software Stack specification[4] (currently TSS 2.0) was developed to provide a standard set of Application Programming Interfaces (APIs) that application software can use to communicate easily with the TPM (see Figure 2). While other basic TPM API software and application software are already integrated in computers with Microsoft Windows, all other platforms require the addition of TPM APIs software such as TSS and application software for the integration of the TPM functionality in the system.

Common examples where TSS may be used include:

- Network equipment
- Embedded systems
- Internet of Things (IoT) devices and gateways
- Automotive applications
- Industrial systems

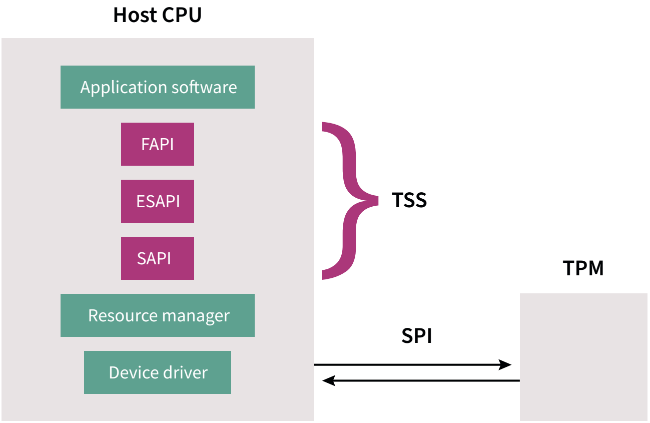


Figure 2. Interfacing to the TPM through the TSS using a Serial Peripheral Interface (SPI).

With the FAPI API of the TSS, the programmer does not need to know the details of the TPM or (in some cases) even know specific TPM commands. To provide this convenience in the high-level FAPI layer, the TSS defines two lower levels of APIs for the TPM, the ESAPI and SAPI. Underlying these three APIs are several lower level layers such as the Device Driver for the TPM but these layers provide only a connection for the command transmission to the TPM so they are not emphasized here.

The lowest level of the TSS is called the System API (SAPI). SAPI provides mainly a basic method to create TPM function calls and a way to translate function calls into encoded TPM 2.0 commands. The SAPI code turns the function calls into byte streams that are sent to the TPM and then converts the byte streams coming back from the TPM into the expected return values which are returned from the function calls.

The Enhanced System API or ESAPI is the next level up. ESAPI helps to reduce the complexity of the application software by handling housekeeping tasks such as session management and protection of the communication between the TPM that an average programmer likes to use by default in most applications.

The highest level of TSS APIs that is still under development is called the Feature API (FAPI). FAPI provides higher level software abstractions that provide functional capabilities such as automatic key loading, data encrypt and sign.

The open-source TPM stack TPM2-TSS[5] distributed via GitHub includes SAPI and ESAPI and it has been tested with many TPMs and software simulators. Because the TSS APIs are an open standard, similar TSS libraries are available from other sources.[6] [7]

To reduce the effort required to use the TPM even further, many commonly used application software libraries such as OpenSSL have been enhanced to support the TPM by interfacing those libraries to the TSS APIs. In Figure 3, the TPM is below the line. Above the line are the host CPU and the layers of software that run on it. The dark green layers show the many security packages that are implemented by Infineon partners on top of the TSS.

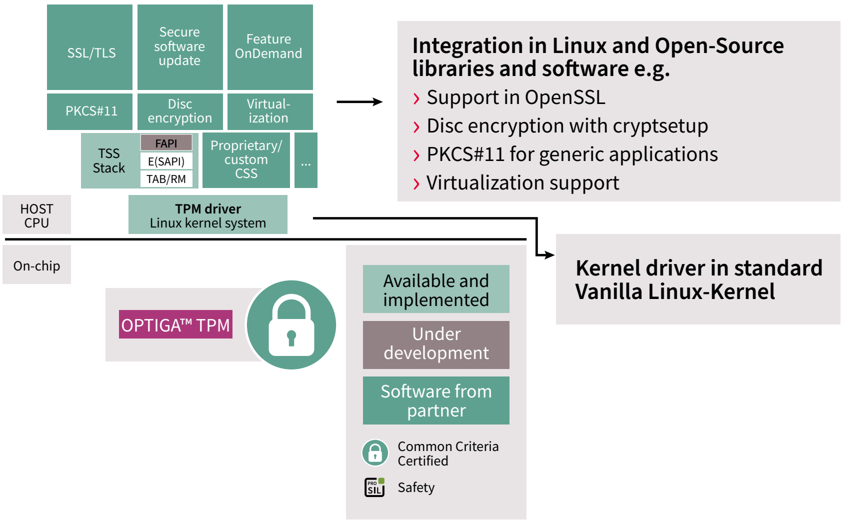


Figure 3. The TSS enables many software packages to interface to the TPM.

The application layer software packages can have other security software built on top of them. For example, Apache Web Server installations typically use OpenSSL for communications security.

TCG network equipment guidance

TCG's network equipment sub group (a group of network equipment makers) developed "Guidance for Securing Network Equipment Using TCG Technology"[1] to explain how TPM 2.0 and TSS can be used to address the rapidly expanding network security threat posed by unprotected routers, switches, firewalls, gateways and wireless access points. This specification defines prime use cases that are commonly implemented when securing network equipment such as securing secrets, protection of configuration data, and integrity-protected logs. The business case for each use case is explained and then technical advice is given about how to implement it using TPM and TSS.

Lanner SDK – a set of APIs to accelerate software development

Information technology in the IoT and especially the Industrial Internet of Things (IIoT) requires secured communications. As a provider of secured hardware platforms and consultant services for security, Lanner uses its expertise to help clients solve specific security/ trust problems. Simplifying the implementation of TPM capabilities is one aspect.

To enable secured communication from both device-to-gateway and gateway-to-IT layers, Lanner offers products with comprehensive firmware security features, encrypted platform identity and TSS 2.0 compliant middleware.[8] Beyond the hardware platform provided by Lanner, the SDK provides a set of solid designed and validated APIs to make sure that:

- › Software code execution is being measured
- › Data-at-rest is protected
- › Data-in-transit is encrypted
- › Confidential secrets are being sealed

With TCG's Network Equipment Guidance document defining the common architecture, Lanner APIs provide the enabling tools to protect network devices by using the integrated cryptographic features in the Infineon OPTIGA™ TPM that is an integral part of Lanner's platforms. Supporting TCG's TPM 2.0 specifications, the Open Source TSS included by Lanner provides source code, binaries, sample code and a simple set of APIs for developers to leverage TPM capabilities to build trusted solutions. Figure 4 shows how a secured end application is developed based on Lanner's hardware and software, combined with a developer's additional contributions. The solution stack is defined by the green components provided by Lanner and the yellow components provided by the developer who may include open source software as well as their own application code.

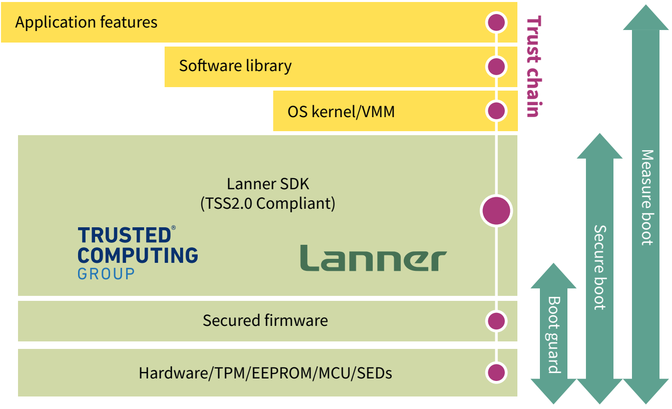


Figure 4. Building a secured solution based on Lanner hardware and software using the TPM 2.0 and TSS 2.0 specifications.

In a given network, if there are 100 security appliances, there could be 500 other appliances doing other functions in the network that are not necessarily security devices. The goal of the Lanner-implemented platform with a TPM chip and TSS stack is to enable all of these appliances and other devices to become more inherently secure by using a simple open -source standard TSS to access to the TPM chip to make their system more secure. Security companies already have ideas for how to make a device more secure, but programmable logic controller (PLC) vendors, analytics vendors, router vendors and similar equipment suppliers may have dozens of functions that need to be secured by the Hardware Root of Trust in the TPM. By including the TPM and TSS, Lanner offers a simple way to make a system far more secure than could be achieved by simply adding a layer of software.[9]

Practical implementation steps

As described in the last section, TCG's Network Equipment Guidance describes many different use cases that can be implemented to improve the security of network equipment:

- Device identity
- Secured zero touch provisioning
- Securing secrets*
- Protection of configuration data*
- Remote device management
- Software inventory
- Attestation of integrity for network devices (health check)
- Composite networking devices
- Integrity-protected logs
- Entropy generation*
- Deprovisioning

Due to limited space, this document will focus on only a few of the most critical use cases, marked with a * above. For information on the other use cases, the reader is referred to the TCG document.

Securing secrets

Network equipment and industrial gateways may need to manage and store many different kinds of secrets: passwords, cryptographic authentication keys, file or disk encryption keys, etc. TPM and TSS can be used to protect all of these secrets against a variety of attacks: physical tampering, exploitation of application software bugs, etc.

The easiest way to securely create and use cryptographic authentication keys with the TPM is to use the OpenSSL libraries with the tpm2-tss-engine, which adds TPM support to OpenSSL. Follow these steps:

1. Generate a new asymmetric key pair using the `tpm2-tss-genkey` command.
2. Obtain a certificate for the new key pair by generating a Certificate Signing Request (CSR) with the `openssl req` command and using a Certification Authority (CA) to get a certificate from the CSR.
3. Use the certificate and private key with other OpenSSL commands, such as the `openssl s_client` command that can be used to securely connect to a remote server.

If you prefer, you can call the TSS directly to create a key pair (e.g. with `Esys_Create`), generate the CSR, and perform cryptographic operations (e.g. with `Esys_Sign`). But why bother with those low-level commands when OpenSSL and tpm2-tss-engine can do it for you?

To protect confidential data or other kinds of secrets such as a password, you have several options:

- Store the secret in the TPM's non-volatile memory (with `Esys_NV_Write`), where it can be protected with policies and other protections (with `Esys_NV_DefineSpace`) and read (with `Esys_NV_Read`) when those policies are satisfied..
- Use the TPM to "seal" the secret (with `Esys_Create`), generating a blob that can be stored on local storage and unsealed by the TPM later (with `Esys_Unseal`) if the proper policies are satisfied.
- Use the TPM to generate an asymmetric key (using `Esys_Create`) and then use that key pair to encrypt and decrypt the secret (with `Esys_RSA_Encrypt` and `Esys_RSA_Decrypt`).
- Use the TPM to generate a symmetric key (using `Esys_Create`) and then use that key for key derivation (e.g. with `Esys_HMAC_Start`).
- Use OpenSSL's "`openssl pkeyutl`" command to encrypt and decrypt the secret with an asymmetric key pair.
- Use cryptsetup/luks or a similar Linux disk encryption package that supports TPM to encrypt the drive that holds the secret.[10] .

Each of these approaches has its own special pros and cons. You can study these pros and cons using books like [11] or [12] or you can consult TPM experts such as Lanner to get their advice about what's best for your situation.

Protection of configuration data

Configuration data for network equipment must be secured. Otherwise, network communications may fail or even be compromised (e.g., if an attacker can change firewall rules to permit attacks to flow through the firewall). For this reason, configuration data must be protected in transit (when it's sent to the network equipment) and at rest (when it's stored on the network equipment).

To protect the configuration data in transit, the best and easiest approach is to use OpenSSL or a similar secured communications library that supports TPM. The instructions above apply here as well.

To protect the configuration data at rest, any of these techniques can be used:

- Store the secret in the TPM's non-volatile memory (with `Esys_NV_Write`), where it can be protected with policies and other protections (with `Esys_NV_DefineSpace`) and read (with `Esys_NV_Read`) when those policies are satisfied
- Use the TPM to "seal" the secret (with `Esys_Create`), generating a blob that can be stored on local storage and unsealed by the TPM later (with `Esys_Unseal`) if the proper policies are satisfied.
- Use the TPM to generate an asymmetric key (using `Esys_Create`) and then use that key pair to sign and verify the secret (with `Esys_Sign` and `Esys_Verify`) and optionally to encrypt and decrypt the secret (with `Esys_RSA_Encrypt` and `Esys_RSA_Decrypt`).
- Use the TPM to generate a symmetric key (using `Esys_Create`) and then use that key to hash and verify the secret (with `Esys_HMAC`) and/or to encrypt and decrypt the secret (with `Esys_EncryptDecrypt2`).
- Use OpenSSL's "`openssl pkeyutl`" command to encrypt and decrypt and integrity protect the secret with an asymmetric key pair.
- Use luks or a similar Linux disk encryption package that supports TPM to encrypt and integrity protect the drive that holds the secret.[10]

Again, each of these approaches has its own special pros and cons. You can study these pros and cons using books like [11] or [12] or you can consult TPM experts such as Lanner to get their advice about what's best for your situation.

Entropy generation

Entropy (randomness) is under-appreciated but essential for security. For example, whenever a new secured communications session is established, a new session key must be generated. This requires cryptographically strong randomness so that attackers cannot guess which key will be generated. The TPM can fill this gap by providing a strong source of entropy. In fact, the OPTIGA™ TPM is certified to do so.

To obtain random data from the TPM, you can use the `Esys_GetRandom` function from ESAPI. But if you're using a new version of Linux, it will automatically feed entropy from the TPM into `/dev/random`, which is used by most programs that need strong entropy on Linux. Older versions of Linux can use `rng-tools`[13] to connect the TPM into `/dev/random`.

Other firmware security measures

In addition to the TPM's features, Lanner hardware platforms provide additional basic security measures often overlooked by industrial and networking computer systems. Since the Baseboard Management Controller (BMC) (an out-of-band management subsystem) is often an overlooked attack surface, Lanner ensures that it has the tightest security possible, while maintaining its usefulness. With this hardware:

- Lanner's BMC has a login block feature to avoid trial and error login attacks
- Lanner's BMC will ask the user to change their password at the first login
- Lanner's BMC uses strong ciphers and encryption algorithms to protect its own code and settings
- Lanner's new codebase encrypts all virtual media connections to external elements
- Lanner's documentation clearly shows how to disable port 623 (remote management) when unused

Conclusion

Unprotected network equipment provides new targets for attackers. Preventing those types of attacks needs to be high on the must-do list of IT, network and security experts as well as many levels of enterprise management. With Trusted Computing Group standards defining the enabling technology, Infineon and companies like Lanner provide the tools needed to easily implement the required trust and security with OPTIGA™ hardware-based security products. Now, network equipment security threats can be handled directly to avoid persistent, subtle infections as well as to control problems in industrial, military and other enterprises. Doing nothing is not an option, because the consequences are too great. In contrast, implementing protection is made easy based on the combined efforts of Infineon and its technology partners.

About Infineon Technologies
Infineon Technologies is a world leader in semiconductor solutions that make life easier, safer and greener. Microelectronics from Infineon is the key to a better future. For more information, please visit www.infineon.com or follow us on Twitter @Infineon

About Lanner
Lanner Electronics Inc is a world leading provider of design, engineering and manufacturing services for advanced network appliances and rugged applied computing platforms for system integrators, service providers and application developers. For more information, please visit http://www.lanner-america.com or follow us on Twitter at @LannerAmerica

OPTIGA™ is a trademark of Infineon.

References

[1] Guidance for Securing Network Equipment Using TCG Technology, https://trustedcomputinggroup.org/resource/tcg-guidance-securing-network-equipment/
[2] “FBI Worried as DoD Sold Counterfeit Cisco Gear”, https://www.infoworld.com/article/2653167/fbi-worried-as-dod-sold-counterfeit-cisco-gear.html
[3] TPM Certified Products List, https://trustedcomputinggroup.org/membership/certification/tpm-certified-products
[4] TPM Software Stack (TSS), https://trustedcomputinggroup.org/work-groups/software-stack/
[5] TPM2-TSS, https://github.com/tpm2-software/tpm2-tss
[6] IBM TSS, https://sourceforge.net/projects/ibmtpm20tss/
[7] Microsoft TSS, https://github.com/Microsoft/TSS.MSR
[8] IIoT Edge Security, http://www.lannerinc.com/news-and-events/latest-news/iiot-edge-security
[9] “Secure IIoT Gateways Ensure Visibility, Security and Manageability in Industrial Networks”, https://www.lannerinc.com/applications/industrial-automation/secure-iiot-gateways-ensure-visibility-security-and-manageability-in-industrial-networks
[10] https://gitlab.com/AndreasFuchsSIT/cryptsetup
[11] A Practical Guide to TPM 2.0, https://www.apress.com/gp/book/9781430265832
[12] Trusted Platform Modules: Why, When and How to Use Them, https://www.amazon.com/Trusted-Platform-Modules-Computing-Networks/dp/1849198934
[13] rng-tools, https://wiki.archlinux.org/index.php/Rng-tools