A Comprehensive Survey of TPM for Defense Systems

Cheol Ryu, Jae-Ho Lee, Do-Hyung Kim, Hyung-Seok Lee, Young-Sae Kim, Jin-Hee Han, and Jeong-nyeo Kim*

Cyber Security Research Division, ETRI, South Korea

[e-mail: ryuch, bigleap, hyslee, vincent, hanjh, jnkim@etri.re.kr]

*Corresponding author: Jeong-nyeo Kim

Received December 18, 2023; revised April 18, 2024; accepted June 27, 2024; published July 31, 2024

Abstract

Lately, there has been a notable surge in the defense industry's efforts to develop highly advanced intelligent systems. These systems encompass sophisticated computing platforms that boast an impressive level of autonomy. However, it's important to acknowledge that these very systems are not impervious to vulnerabilities stemming from both hardware and software tampering. Within the context of this discourse, our focus of the survey is directed towards the hardware security module. This component stands out for its capability to offer a significantly heightened level of protection when compared to conventional software-based techniques. Through the lens of this paper, we embark on a comprehensive survey of Trusted Platform Module (TPM), a hardware security module, shedding light on its potential to fortify the defense against threats that emerge from various vectors of attack.

Keywords: anti-tampering, trusted platform, TPM, TSS

This work was supported by KRIT - Grant funded by Defense Acquisition Program Administration (DAPA) (KRIT-CT-22-051)

http://doi.org/10.3837/tiis.2024.07.012 **ISSN : 1976-7277**

1. Introduction

As modern weapons are becoming more advanced, it has become necessary to prevent reverse engineering of HW and SW when a weapon system is lost or stolen. Computing platforms that operate weapon systems with functions of autonomous flight, autonomous navigation, and autonomous driving are widely introduced. The need to protect the platform and the information on it has increased in order to prevent incidents such as the U.S. unmanned aerial vehicle RQ-170 being hijacked and reverse-engineered by Iran [1].

In order to prevent attacks on the platform, a hardware security module that can safely protect cryptographic keys through physical attacks and prevent tampering of the platform has become necessary. In this paper, we look into the key functions, the standards and applications of TPM, and examine the needs of the defense field.

2. Overview of the TPM Standards

2.1 Overview of the TPM

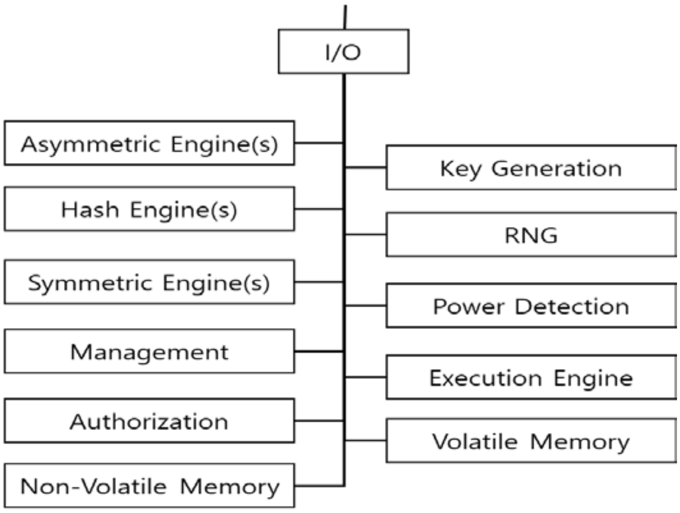

Fig. 1. TPM Architectural overview [2][3]

TPM (Trusted Platform Module) is a hardware-based security module designed to provide secure cryptographic functions and protect sensitive data in a computer system. It is a computer chip with a microcontroller which securely stores passwords, certificates, encryption keys. HSMs (Hardware Security Modules) are targeted towards delivering high-security and high-performance cryptographic operations and key management. In contrast, TPMs (Trusted Platform Modules) focus on securing individual devices and establishing a fundamental root of trust. TPM 2.0 is a specification developed by the Trusted Computing Group (TCG) and it was improved over the earlier TPM 1.2 by offering more features and enhanced security. The TPM 2.0 is designed to provide a strong foundation for building secure systems and supporting a wide range of security applications, including secure boot, data encryption, key management, and remote attestation. The following briefs the pivotal constituents found in TPM 2.0 [2].

- The I/O buffer: serves as the communication hub between a TPM and its host system. Command data is deposited in this buffer by the system, and the resulting response data is subsequently retrieved from it.

- Key Generation: generates cryptographic keys securely within the TPM.

- Random Number Generator (RNG): provides high-quality random numbers for cryptographic keys and nonces.

- Hash Engine: provides various hashing algorithms (e.g., SHA-1, SHA-256, SHA-384, SHA-512) for secure data hashing used in cryptographic operations like digital signatures and attestation.

- Cryptographic Engines: comprise two types, the Asymmetric module and the Symmetric module. The TPM uses asymmetric algorithms for attestation, identification, and secret sharing and uses symmetric encryption to encrypt some command parameters (typically, authentication information) and to encrypt protected objects stored outside it.

- Authorization subsystem: is called at the beginning and end of command execution. Before the command may be executed, it checks that proper authorization for use of each of the shielded locations has been provided

- Non-Volatile Memory: stores persistent data like Endorsement/Platform/Storage Seed and monotonic counters.

- Volatile Memory: temporarily stores PCRs, Sessions, etc. during the TPM power cycle.

- Power Detection: monitors TPM power state, taking appropriate actions during power transitions and ensuring proper shutdown.

- Execution Engine: processes commands, including unmarshaling the command and marshaling the response. It uses other modules to validate messages and to check authorities and

The command execution flow in the TPM could be divided into these steps;[3]

1. Command Decoding: It decodes the command to understand what operation is being requested.

2. Parameter Verification: It checks the parameters of the command to ensure they are valid and meet the necessary criteria for the requested operation.

3. Execution of Command: It carries out the specific cryptographic or management function that the command requests. This could involve tasks like key generation, encryption/decryption, signing operations, or updating TPM data structures.

4. Response Generation: After executing the command, the module generates a response. This response typically includes the result of the command execution, which could be data (like an encrypted message), a digital signature, or status

information.

5. Response Marshaling: Finally, it prepares the response in a format that can be sent back to the requester, ensuring that it adheres to the TPM communication protocols.

Overall, the components of TPM 2.0 work together to provide secure cryptographic functions, protect sensitive data, and establish a root of trust for measurement in a trusted computing environment. The TPM's architecture ensures the integrity and confidentiality of information, enabling a wide range of security applications, including secure boot, remote attestation, and data protection.

2.2 Standards for the TPM

In order to safely store sensitive information such as encryption keys in systems such as PCs, mobile phones, and automobiles, TPM chip technology, which is attached to a motherboard that is different from the general storage device structure and performs special security functions, was developed. The people who led this work created the TCG organization [4] for TPM standardization and are writing related specifications. Key participants included major tech companies, security experts, industry groups, and government agencies, ensuring a robust and versatile security standard.

Starting with TCPA main specification version 1.1b in 2002, TCG announced TPM main specification version 1.2 in 2009. TPM 1.2 laid the groundwork for the concept of trusted computing, introducing hardware-based security that was more robust than software-only solutions. And it was widely adopted in many devices, particularly in enterprise environments, providing a base level of security for numerous systems. TPM 1.2 established a hardware-based root of trust, offering a secure way to store cryptographic keys and perform critical security functions [5].

TCG released TPM specification version 2.0 in 2014. The transition from TPM 1.2 to TPM 2.0 brought several significant improvements and changes, making TPM 2.0 more flexible, robust, and capable. TPM 2.0 is algorithm-independent, meaning it can support a wider range of cryptographic algorithms. This is a major shift from TPM 1.2, which was largely built around specific algorithms (like SHA-1 and RSA). And it supports newer cryptographic standards, including SHA-256 and ECC (Elliptic Curve Cryptography), offering better security and efficiency. TPM 2.0 introduces a more flexible command structure, which allows for easier updates and enhancements. This adaptability makes it more future-proof against evolving security needs [6].

TPM 2.0 provides more sophisticated and flexible authorization mechanisms, including policy-based authorization, which allows for complex security policies. It improved privacy features in TPM 2.0 include Enhanced Authorization (EA), which provides more control over user data and better protection of user privacy. It also supports multiple hierarchy storage areas for keys, which enhances organizational control and management of keys. It introduced session management which handles more concurrent sessions compared to TPM 1.2, improving its multitasking capabilities. It also improved resource management which allows the TPM to handle more objects and sessions simultaneously, optimizing performance for complex operations.

In addition, TPM 2.0 provides four hierarchies (Endorsement, Storage, Platform, Null) so that various users can conveniently and safely utilize the functions, and introduces the concept of "Algorithm Agile" so that algorithms can be deleted or added without changing the specifications.

To be precise, the TPM 2.0 specification is a library specification which supports a wide variety of functions, algorithms and capabilities upon which future platform-specific specifications will be based.

2.3 Software Stack for the TPM

Other TCG specifications detail how the TPM can be implemented in variety of platforms through TCG platform specific specifications, such as TPM Software Stack (TSS) specification and separate specifications for PCs, cloud, server, storage, mobile, embedded, IoT, and virtualized platforms.

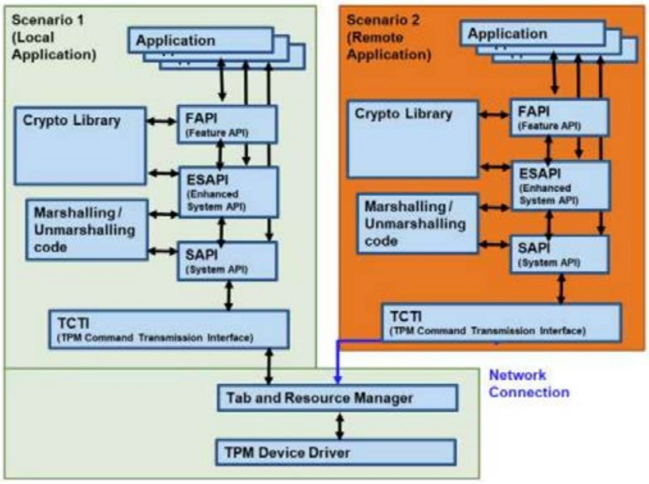
Scenario 1 (Local Application)
Application
Crypto Library
FAPI (Feature API)
ESAPI (Enhanced System API)
Marshalling / Unmarshalling code
SAPI (System API)
TCTI (TPM Command Transmission Interface)
Scenario 2 (Remote Application)
Application
Crypto Library
FAPI (Feature API)
ESAPI (Enhanced System API)
Marshalling / Unmarshalling code
SAPI (System API)
TCTI (TPM Command Transmission Interface)
Network Connection
Tab and Resource Manager
TPM Device Driver

Fig. 2. TCG Software Stack 2.0 [7]

TSS is vital for harnessing the full potential of TPM technology. It provides the necessary tools, interfaces, and management capabilities to integrate TPM security into a wide range of computing environments. It acts as the intermediary that allows software applications to communicate with the TPM. Without the TSS, applications would not be able to effectively utilize the TPM’s security functions. The TSS abstracts the complexity of the TPM's commands and responses, providing a more user-friendly interface for developers. This abstraction simplifies the process of integrating TPM functionalities into various applications.

It provides a standardized way to access TPM functionalities, ensuring consistency and compatibility across different applications and systems. This standardization is crucial for developers, as it simplifies the development process and ensures that applications can reliably interact with the TPM.TSS manages the execution of security protocols, such as authentication and encryption, which are fundamental to TPM operations. This includes handling complex tasks like cryptographic key generation, management, and secure storage.

It can enforce security policies, which are critical for applications that require stringent security measures. This includes managing authorization credentials and ensuring that TPM operations comply with predefined security rules. TSS effectively manages the limited resources of the TPM, such as memory and cryptographic keys. This management is crucial for the efficient and secure operation of the TPM, especially in systems where multiple applications may be accessing the TPM concurrently.

It provides robust error handling and logging capabilities, which are essential for diagnosing issues, maintaining system integrity, and ensuring reliable TPM operations. It makes it easier for system administrators and developers to integrate TPMs into existing systems, ensuring that the benefits of TPM security can be widely adopted without requiring deep technical expertise in TPM internals.

2.4 Standards Comparable to TPM and TPM-Like Hardware

ISO/IEC JTC1 approved and adopted TPM specification Version 1.2 and TPM Library Specification 2.0 as 11889:2009 and 11889:2015 standard [8], respectively. In the United States, TPM is not a universal regulatory requirement in the United States, its use is essential and often required in specific sectors and for particular applications. For certain government and defense-related applications, TPM may be required as part of broader security and compliance measures. The National Institute of Standards and Technology (NIST) guidelines often influence these requirements. federal systems or systems handling certain types of government data must comply with FIPS standards, which can include requirements for hardware-based security modules like TPM. Department of Defense, CMMC requirements may include standards that can be met using TPM technology.

NIST does not have a specific standard exclusively for TPM but it has related guidelines for BIOS, key managements, and firmware. NIST SP 800-147 provides guidelines for BIOS Protection, which is relevant for secure boot processes. NIST SP 800-88 guides for media sanitization, including methods for secure deletion of data, which can be relevant to secure key storage and destruction. NIST SP 800-193 is the guidelines for Platform Firmware Resiliency, which can involve TPM for ensuring the integrity and security of firmware.

In Europe, while the General Data Protection Regulation (GDPR) does not specifically mandate the use of TPM, it does require that personal data be processed securely. Using TPM can help organizations meet some of the technical requirements of GDPR by securing data at rest and in transit.

3. Implementations and Adaptions

3.1 TPM Chip Manufacturers

TCG has established certification programs with the aim of maintaining consistent quality standards across products developed in adherence to TCG specifications. Currently, the roster of TCG certified products includes TPM 2.0 chips that have been manufactured by key players such as Infineon Technologies, Nuvoton, and STMicroelectronics [9]. Intel and AMD also incorporated TPM capabilities into their products. In addition to the companies of which products are certified, TCG also assigned a number of vendor IDs to Advanced Micro Devices, Atmel, Broadcom, Cisco, Flyslice Technologies, Google, HPI, HPE, Huawei, IBM, Intel, Lenovo, Microsoft, National Semiconductor, Nationz Technologies, Qualcomm, Samsung, Sinosun, SMSC, Texas Instruments and Winbond [10].

Each of these TPM chips serves as a fully integrated security cryptoprocessor, meticulously designed for seamless integration into diverse systems such as personal computers, embedded systems, and IoT platforms.

This implementation can manifest in the form of a discrete TPM compliant with the TPM version 2.0 standards, or alternatively, it can be offered as a turnkey solution complete with the firmware seamlessly embedded within the TPM chip [11].

Additionally, Infineon Technologies, a notable manufacturer of TPM chips, has taken strides in advancing security measures. They offer the OPTIGA TPM 2.0 solution, complete with TSS host software, which simplifies the process of integrating TPM into Linux-based systems, starting from the year 2021. This solution holds the capacity to effectively safeguard sensitive data within interconnected devices, thus mitigating the potential risks of data breaches stemming from cyberattacks. This, in turn, empowers IoT system integrators to significantly enhance the security profile of their interconnected products. Moreover, the integration of software with TSS-FAPI carries several advantages. Notably, it reduces the necessity for extensive source code development, consequently leading to notable cost and time savings within the development cycle.

Nuvoton's TPMs are also prevalent, especially in many laptops and desktops. They have a strong presence in the personal computing market with the NPCT series. They offer the TrustSentinel TSS2.0 software through a partnership with OnBoard Security, providing a comprehensive TSS solution. STMicroelectronics is another key player whose TPM chips are used in diverse applications with the ST33 series or STSAFE-TPM from personal computing to more specialized industrial and automotive systems. STMicroelectronics ‘TPM product is compliant with the open-source TCG TPM 2.0 TSS implementation.

Intel's approach to TPM integration demonstrates their commitment to providing flexible and robust security solutions, accommodating both firmware-based and hardware-based TPM options. Intel implements TPM functionality directly into the chipset of the processor through firmware. This approach, known as fTPM, embeds TPM capabilities within the CPU, eliminating the need for a separate physical TPM chip on the motherboard. fTPM provides the same functionality as a discrete TPM chip, including secure boot, cryptographic operations, key storage, and integrity measurement. The advantage of fTPM is that it reduces the need for additional hardware, lowers costs, and simplifies the system design while providing the benefits of TPM security [12][13][14].

Intel's chipsets and motherboards also support discrete TPM chips. This means that motherboard manufacturers can include a physical TPM chip on their Intel-based motherboards. This support is important for users or organizations that prefer or require a discrete TPM for their security needs, such as for enhanced isolation of the TPM from the main CPU.

In addition to above two approaches, Intel integrates TPM support in their platform designs, ensuring that both fTPM and discrete TPM chips can function seamlessly with Intel processors and chipsets. This integration is a part of Intel’s broader security architecture, which includes hardware-assisted security features and is designed to provide robust security solutions for a range of applications, from personal computing to enterprise systems.

Intel provides support for TPM integration through software tools, SDKs (Software Development Kits), and documentation, facilitating developers and manufacturers in implementing TPM functionalities in their products. And It ensures that its TPM solutions, both fTPM and support for discrete TPMs, are compliant with the standards set by the Trusted Computing Group (TCG).

3.2 Platforms that adopted the TPM

On top of TPM, various extensions have been developed based on TPM technologies. The **Fig. 3** shows brief introduction of the extensions and adopters of them.

Extensions	**Descriptions**	**Adopters**
vTPM	Extends the functionality of TPM on virtual machine	Xen vTPM, VMware, Microsoft Hyper-V, IBM Cloud
fTPM	Software implantation of TPM within the firmware of a device	AMD, Intel PTT, Arm TrustZone, Qualcomm
Measured Boot	Applies TPM to boot securely with the recorded hashes of the hardware components	Microsoft Windows, VMware vSphere, Linux IMA, UEFI, TCG, Google Chrome OS
TXT	Trusted Execution Technology provides a trusted environment for the execution of code and protection of data on a computer.	Intel TXT, AMD-V, DRTM
DHA	Device Health Attestation ensures the integrity of devices, but not relies solely on TPM	Microsoft Windows, Google Android

Fig. 3. Extensions and adopters of TPM

TPM has been in use for over 20 years and has been part of PCs since around 2005. Several categories of platform vendors adopted TPM 2.0 and they can be shown as follows;

- PC and Laptop Manufacturers: Many leading computer manufacturers have incorporated TPM 2.0 in their devices. This includes companies like Dell, HP, Lenovo, and Microsoft (in their Surface line of devices), particularly in their business and enterprise-focused models.
- Motherboard Manufacturers: Major motherboard manufacturers, such as ASUS, Gigabyte, and MSI
- Server Manufacturers: Companies that produce servers for enterprise environments, like IBM, Dell EMC, and Hewlett Packard Enterprise
- Smartphone and Tablet Manufacturers: Some manufacturers of mobile devices may also adopt TPM 2.0
- Embedded Systems and IoT Devices: Manufacturers of embedded systems and IoT devices

- Automotive Industry: As vehicle systems become more connected and complex, some automotive manufacturers may integrate TPM 2.0 for enhanced security in vehicle communications and data systems.
- Enterprise Networking Equipment: Vendors producing networking equipment for enterprise environments
- Operating System Providers: Major OS providers like Microsoft with Windows and some Linux distributions support TPM 2.0.
- Hypervisor platforms: VMware, Microsoft Hyper-V [15], Citrix Hypervisor, KVM, Oracle Virtual Box, QEMU [16], Red Hat Virtualization and others support vTPM.

In 2016, TPM 2.0 became the standard for new PCs. Particularly Microsoft's Windows 11 requires TPM version 2.0 [17]. The Windows operating system deeply applies hardware-based security to many features and improves usability using TPM. For example, BitLocker drive encryption, Windows Virtual Smart Card functionality, Platform Crypto Provider, etc [18][19].

More specifically for the security for Windows operating system, Microsoft provides BitLocker [20], Secure Boot and Windows Hello. BitLocker, Windows' built-in drive encryption feature, uses TPM to securely store encryption keys. This ensures that the keys are not exposed to software attacks and that the drive cannot be read even if it is removed from the computer. Fore secure booting, TPM is used in conjunction with UEFI Secure Boot to ensure that a device boots using only software that is trusted by the PC manufacturer. Windows Hello is the biometric authentication, TPM securely stores the data used to recognize a user's face, iris, or fingerprint.

In enterprise environments Microsoft ensures devices are secure and unmodified before accessing resources. TPM is used to securely report the health and integrity of a device. This is called as Device Health Attestation.

In collaboration with chip manufacturers, Microsoft developed Pluton processor which is a chip-to-cloud security technology that provides hardware-based security features. Pluton is designed to provide the functionality of a TPM and additional security features. Microsoft Pluton is currently available on devices with Ryzen 6000 and Qualcomm Snapdragon 8cx Gen 3 series processors and can be enabled on devices running Windows 11 version 22H2 [21].

As a platform company, Intel provides a function that can detect software attacks and check system integrity by linking its Intel TXT Technology with TPM [22]. The StrongSwan, a VPN solution that runs on Linux and Android, utilizes TPM 2.0 through a plugin [23]. Google's Chrome OS uses TPM to protect user data encryption keys and provide functions to verify device mode [24][25][26].

VMware's vSphere [27] platform supports TPM for VMs which is called vTPM. vTPM emulates the functionality of a physical TPM but within a virtual machine. Each VM can have its own isolated and independent vTPM instance and provides the same capabilities as a physical TPM, including secure generation and storage of cryptographic keys, device authentication, and secure boot processes [28][29]. VMware provides Secure Boot by supporting Intel TXT and TPM 2.0 functions in vSphere 6.7 U1 and later versions [30].

Wind System has released a small boxed industrial computer unit with a TPM 2.0 chip built into the board to enhance security in various industrial applications [31]. Wind System integrated VxWorks, its real-time operating system, with TPM for secure boot, encryption, and protecting sensitive data.

Oracle's Solaris includes TPM device drivers, a TCG software stack, and TPM-related commands to utilize TPM features [32]. Winmagic has released MagicEndpoint, which allows users to easily authenticate without a password by utilizing TPM 2.0 [33].

4. Military Cybersecurity

In 2011, Iran claimed to have hijacked and reverse-engineered the U.S. unmanned aerial vehicle RQ-170. The Islamic Revolution Guard Corps stated that they had successfully extracted all the data from the drone and were in the process of constructing a replica of the aircraft [1]. A TPM could have served as an anti-tamper mechanism to deter the reverse engineering of the device. It could have ensured that the device boots securely, protected data by encrypting it, and prevented tampering or compromise.

The United States Department of Defense (DoD) specifies that new computer assets must be equipped with TPM 1.2 or higher, and the TPM will be used for equipment identification, authentication, encryption, and integrity verification [34]. In the instance of Raytheon, a prominent player in the defense sector, a noteworthy approach was taken. This defense company strategically acquired a dedicated set of NVRAM addresses within the TPM standards, effectively reserving them for their specific operational requirements [35].

Beyond its widespread adoption in PCs, the TPM extends its influence to an array of cutting-edge domains. These encompass cloud servers, storage systems, mobile devices, embedded systems, the Internet of Things (IoT), and virtualized platforms. These versatile commercial applications extend to defense systems as well. Security solutions for defense systems built from COTS (common off-the-shelf) components has long been demanded. If commercially off-the-shelf components can be obtained, significant financial savings could be realized. Even in the context of individual purchases for personal computing applications, the cost of a single TPM chip, intended as an add-on module, typically starts from $15. This pricing variation is influenced by several factors including the TPM version (either 1.2 or 2.0), the type of interface it employs (such as SPI or LPC), and whether the TPM is a discrete module or an integrated component of a motherboard. In light of bulk purchasing considerations, it may now be feasible to construct a defense system with a TPM as its central component.

For the defense systems, data on the system should be thoroughly erased both before and after usage and the system needs to have secure self-identification capabilities. Users must be able to identify themselves securely. Data transferred to the system should remain hidden during transmission. Private information stored on the system must be inaccessible to other running processes. TPM can offer security functionalities using the PCRs and the secure boot technique. Given these use cases, TPM is recognized as fulfilling the following requirements:

1. Tamper-Resistant Hardware: As a hardware-based security module, TPM should designed to be resistant to tampering, adding a layer of physical security.

2. Secure Boot with Hardware Roots of Trust: TPM should support secure boot processes, ensuring that the system boots from a trusted state and verifying software integrity.

3. Anti-Tamper Software and Firmware: TPM should help detect unauthorized changes to software and firmware, contributing to overall system integrity.

4. Robust Network Security Protocols: While TPM itself doesn’t define network protocols, it should provide secure key storage and identity services that can support robust network security.

5. Supply Chain Security: TPM should provide a secure boot and hardware attestation, helping to ensure that hardware and software haven’t been tampered with during the supply chain process.

However, TPM technology isn't inherently built for the harsh environments commonly encountered in defense systems. While TPM chips are inherently secure, they would need to undergo physical and environmental hardening to be fully prepared for the extreme conditions typical in defense applications. This additional hardening is essential to ensure that the TPMs meet the rigorous environmental specifications required for military use. it's important to note that TPMs are just one component of a comprehensive defense security strategy. Defense systems often face threats that are more sophisticated and varied than those encountered in commercial environments. It has the capability to securely safeguard the cryptographic keys essential for implementing data wiping protocols. Beyond this logical eradication, the integration of physical self-destruction features is also advisable. It means defense applications typically require additional layers of security, including specialized hardware and software, advanced encryption techniques, and rigorous physical protection measures.

FPGA (Field-Programmable Gate Array) is a prevalent and critical platform for modern military systems. But unlike ASICs (Application-Specific Integrated Circuits), FPGAs can be reconfigured after manufacturing. This allows defense systems to be updated or repurposed with new functionalities to adapt to evolving threats or mission requirements without needing new hardware. And FPGAs facilitate rapid prototyping, testing, and deployment of new system designs or updates. This is crucial in defense applications where speed and adaptability can be critical. FPGAs are capable of handling high-speed signal processing tasks, such as radar signal processing, image processing, and encrypted communications, which are common in military applications [36].

But FPGAs do not inherently include the same level of built-in security features those modern microprocessors might have. This is because FPGAs are essentially blank slates that can be programmed to perform a wide range of functions, including security-related ones. But FPGAs are susceptible to unique attack vectors such as bitstream tampering, where an attacker modifies the configuration of the FPGA. Physical attacks like side-channel attacks are also a concern. TPM provides hardware-based isolation, secure boot, and cryptographic capabilities for microprocessor-based systems.

The combination of FPGA's adaptability and performance with TPM's robust security features makes this integration highly suitable for the demanding and dynamic needs of military systems. the integration of TPM (Trusted Platform Module) enhances these systems. FPGA allows for the customization of hardware to meet specific military needs, which can range from signal processing to secure communications. Integrating TPM adds a layer of hardware-based security to these customized solutions. Military applications often require rapid adaptation to new technologies and threats. FPGAs can be reconfigured for new tasks or updated algorithms without needing new hardware, and TPM ensures that these updates are secure. FPGAs provide high-performance processing, crucial for applications like real-time data analysis, encryption/decryption, and signal processing in military systems. TPMs enhance this by securely managing the cryptographic functions. Security is paramount in military applications [37].

TPMs provide secure boot, hardware-based key storage, and integrity checks, ensuring that the system is protected from tampering and unauthorized access. TPM chips are designed to be tamper-resistant, adding an extra layer of security against physical attacks. They also protect against cyber threats by securely managing cryptographic keys and processes. Military systems need long-term reliability and support. FPGAs offer this through their longevity and adaptability, while TPMs provide consistent, reliable security over the system's lifespan. The reprogrammable nature of FPGAs, combined with the secure update and integrity verification capabilities of TPMs, reduces the risk of system obsolescence, allowing military hardware to stay current with evolving threats and technologies.

5. Conclusion

The preference for hardware security modules over software-based security methodologies is rooted in their inherent advantages. A prime example of this is the TPM, which boasts a well-developed feature set tailor-made to cater to the stringent demands of defense systems and a multitude of other applications. Its maturity is evident through a comprehensive range of capabilities that it offers, which have been rigorously tested and refined over time. This has been solidified by its extensive adoption across diverse industries, further underscoring its proven effectiveness and robustness.

Looking ahead, the standards governing military equipment are poised to assume a pivotal role in shaping the cohesion and collaboration among nations within military alliances. These standards will serve as a foundational framework, dictating the interoperability, compatibility, and effectiveness of military assets across diverse national defense forces. By adhering to unified standards, countries within military alliances can seamlessly integrate their capabilities, fostering enhanced coordination, communication, and strategic alignment.

References

[1] Simorgh: Iran’s Reproduced US Sentinel Spy Drone RQ-170 with Improved Features | Farsnews Agency. (n.d.). https://www.farsnews.ir/en/news/13941220000394/Simrgh-Iran39-s-Reprdced-US-Seninel-Spy-Drne-RQ-0-wih-Imprved-Feares
[2] Siani Pearson et al., “Trusted Computing Platforms,” Prentice Hall PTR, 2000
[3] Trusted Computing Group: TCG Specification Architecture Overview. Specification, Revision 1.4 Aug. 2, 2007, http://www.trustedcomputinggroup.org
[4] “Welcome to Trusted Computing Group | Trusted Computing Group,” Trusted Computing Group, Aug. 23, 2016. https://trustedcomputinggroup.org/
[5] *TPM 1.2 Main Specification*. Retrieved from https://trustedcomputinggroup.org/resource/tpm-main-specification/

[6] Trusted Computing Group Releases TPM 2.0 Specification for Improved Platform and Device Security. *Trusted Computing Group*. Retrieved from https://trustedcomputinggroup.org/trusted-computing-group-releases-tpm-2-0-specification-improved-platform-device-security/

[7] "TCG TSS 2.0 Overview and Common Structures Specification | Trusted Computing Group," Trusted Computing Group, Dec. 16, 2021. https://trustedcomputinggroup.org/resource/tss-overview-common-structures-specification/

[8] "ISO - International Organization for Standardization," ISO, Dec. 11, 2023. https://www.iso.org/

[9] "TPM | Certified | Products | Trusted | Computing | Group," Trusted Computing Group, Jul. 30, 2019. https://trustedcomputinggroup.org/membership/certification/tpm-certified-products/

[10] "Vendor ID Registry | Trusted Computing Group," Trusted Computing Group, Aug. 11, 2023. https://trustedcomputinggroup.org/resource/vendor-id-registry/

[11] I. T. Ag, "OPTIGATM TPM - Trusted Platform Module - InfineOn Technologies," Copyright Infineon Technologies AG - All Rights Reserved. https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/

[12] Raj, Himanshu et al., "fTPM: A Firmware-based TPM 2.0 Implementation," *Microsoft Research*, 2015. Article(CrossRefLink)

[13] Raj, Himanshu et al., "fTPM: A Software-Only Implementation of a TPM Chip," in *Proc. of 25th USENIX Security Symposium (USENIX Security 16)*, 2016. Article(CrossRefLink)

[14] Afzal Warsi, Shubham Malav, Vishal J. Rathod, Shrikrishna S Chippalkatti, Hari Babu Pasupuleti, and S D Sudarsan, "Secure Firmware based Lightweight Trusted Platform Module (FLTPM) for IoT Devices," in *Proc. of 2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp.738-743, 2023. Article(CrossRefLink)

[15] Velte, Anthony, and Toby Velte. Microsoft virtualization with Hyper-V. McGraw-Hill, Inc., 2009.

[16] Bellard, Fabrice, "QEMU, a fast and portable dynamic translator," in *Proc. of ATEC '05: Proceedings of the annual conference on USENIX Annual Technical Conference, FREENIX Track*, 2005. Article(CrossRefLink)

[17] "What is TPM? - Microsoft Support." https://support.microsoft.com/en-us/topic/what-is-tpm-705f241d-025d-4470-80c5-4feeb24fa1ee

[18] Microsoft, "GitHub - microsoft/TSS.MSR: The TPM Software Stack from Microsoft Research," GitHub. https://github.com/microsoft/TSS.MSR

[19] Vinaypamnani-Msft, "How Windows uses the TPM - Windows Security," Microsoft Learn, Nov. 17, 2023. https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/how-windows-uses-the-tpm

[20] Ritik Sharma, Sarishma Dangi, and Preeti Mishra, "A Comprehensive Review on Encryption based Open Source Cyber Security Tools," in *Proc. of 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp.614-619, 2021. Article(CrossRefLink)

[21] Vinaypamnani-Msft, "Microsoft Pluton security processor - Windows Security," Microsoft Learn, Jul. 31, 2023. https://learn.microsoft.com/en-us/windows/security/hardware-security/pluton/microsoft-pluton-security-processor

[22] W. Arthur and D. Challener, A practical guide to TPM 2.0: Using the Trusted Platform module in the new age of security. 2015. [Online]. Available: https://library.oapen.org/bitstream/20.500.12657/28157/1/1001837.pdf

[23] "Trusted Platform Module 2.0 : StrongSwan Documentation." https://docs.strongswan.org/docs/5.9/tpm/tpm2.html

[24] "TPM usage," https://www.chromium.org/developers/design-documents/tpm-usage/

[25] Wenli Shang, Xiule Zhang, Xin Chen, Xianda Liu, Chunyu Chen, and Xiaopeng Wang, "The research and application of trusted startup of embedded TPM," in *Proc. of 39th Chinese Control Conference (CCC)*, pp.7669-7676, 2020. Article(CrossRefLink)

[26] Devki Nandan Jha, Graham Lenton, James Asker, David Blundell, and David Wallom "Trusted Platform Module-Based Privacy in the Public Cloud: Challenges and Future Perspective," *IT Professional*, vol.24, no.3, pp.81-87, 2022. Article(CrossRefLink)

[27] Guthrie, Forbes, Scott Lowe, and Kendrick Coleman. VMware vSphere design. John Wiley & Sons, 2013.

[28] Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, and Leendert van Doorn, "vTPM: virtualizing the trusted platform module," in *Proc. of USENIX-SS'06: Proceedings of the 15th conference on USENIX Security Symposium*, vol.15, 2006. Article(CrossRefLink)

[29] Shohreh Hosseinzadeh, Samuel Laurén, and Ville Leppänen, "Security in container-based virtualization through vTPM," in *Proc. of 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC)*, pp.214-219, 2016. Article(CrossRefLink)

[30] "VMware Knowledge Base," https://kb.vmware.com/s/article/2148536

[31] J. Jenkins, "SWAP Enabled Rugged COTS Designs with TPM 2.0 for Embedded Systems," WINSYSTEMS, Jan. 18, 2021. https://www.winsystems.com/swap-enabled-rugged-cots-designs-with-tpm-2-0-for-embedded-systems/

[32] "Using trusted platform module - securing systems and attached devices in Oracle® Solaris 11.3," May 14, 2019. https://docs.oracle.com/cd/E53394_01/html/E54828/sysauth-tpm.html

[33] WinMagic Inc, You searched for magic endpoint | WinMagic Data Security Solutions, Protection Services and Software. [Online]. Available: https://winmagic.com/en/?s=magic+endpoint&lang=en

[34] M. McKernan, J. Riposo, J. A. Drezner, G. McGovern, D. Shontz, and C. A. Grammich, "Issues with Access to Acquisition Data and Information in the Department of Defense: A Closer Look at the Origins and Implementation of Controlled Unclassified Information Labels and Security Policy," *RAND Corporation*, 2016. Article(CrossRefLink)

[35] TCG EK Credential Profile Version 2.3 Revision 2, TCG, 23 July 2020

[36] "Special technology area review on FPGAs for Military Applications," *Office of the under secretary of defense acquisition, technology & logistics*, Jul. 2005. Article(CrossRefLink)

[37] Gross, M., Hohentanner, K., Wiehler, S., & Sigl, G., "Enhancing the security of FPGA-socs via the usage of ARM Trustzone and a hybrid-TPM," *ACM Transactions on Reconfigurable Technology and Systems*, vol.15, no.1, pp.1-26, 2021. Article(CrossRefLink)

Cheol Ryu is a senior researcher at the Electronics and Telecommunications Research Institute (ETRI). He graduated from Chungnam National University with both a Bachelor's and a Master's degree in Computer Engineering. His research interests include embedded systems, augmented and virtual reality, and cyber security.

Jae-Ho Lee, a principal researcher at the Electronics and Telecommunications Research Institute since 2001, earned his BS, MS, and PhD degrees in Computer Engineering from Chungnam National University. His research focuses on embedded systems, mobile platforms, D2D communications, and cybersecurity.

Do-Hyung Kim has been a principal researcher at the Electronics and Telecommunications Research Institute since 1995. He received his M.S degree in Computer Science and Engineering from POSTECH. His research interests include embedded systems, mobile platforms, and cyber security.

Hyung-Seok Lee received his M.S. and Ph.D. degrees in electronic engineering from the Korea Advanced Institute of Science and Technology (KAIST) and has been a principal researcher at the Electronics and Telecommunications Research Institute (ETRI) since 1998. His research interests include embedded systems, operating systems, and cybersecurity.

Young-Sae Kim received the B.S. and M.S. degrees in Electronics Engineering from Kyungpook National University, Korea, in 1999 and 2001 respectively. Currently, he is a principal researcher with the Electronics and Telecommunications Research Institute (ETRI), Korea. His research interests include embedded system security, mobile security, and IoT security.

Jin-Hee Han received her B.S. degree in Information and Communications Engineering from Soongsil University and received her M.S. degree in Information and Communications Engineering from Gwangju Institute of Science and Technology (GIST). She is a principal researcher with the Electronics and Telecommunications Research Institute (ETRI) since 1999. Her research interests include embedded system security, mobile security, IoT security, and cyber security.

Jeong-nyeo Kim received her M.S. and Ph.D. degree from Department of Computer Engineering at Chungnam National University. She is the head of the Cyber Security Research Division at ETRI, Korea. Since 2015, she is also a full-time professor in the Department of ICT Engineering at UST. Her research interests include IoT security, mobile security, system and network security, and secure OS