SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Establishing trust in an updatable fTPM using remote attestation

Andreas Korb

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Establishing trust in an updatable fTPM using remote attestation

Herstellung von Vertrauen in ein aktualisierbares fTPM durch Remote Attestierung

Author:	Andreas Korb
Supervisor:	Prof. Claudia Eckert
Advisor:	Albert Stark
Submission Date:	15.11.2023

I confirm that this master's thesis is my own work and I have documented all sources and material used.

Munich, 15.11.2023 Andreas Korb

Acknowledgments

Abstract

Contents

1 Introduction

1.1 Motivation

TPMs rise in their deployments and importance, e.g., in 2013 the President's Council of Advisors on Science and Technology encourages the adoption of TPMs [1], and Microsoft publicized that they require a TPM module for Windows 11 in 2021 [2].

1.2 Goal

1.3 Threat Model

The main threat is the modification of the binary of the fTPM before or during boot. For example, by exchanging the SD card storing the binary. However, we assume that the fTPM cannot be modified by malicious parties after the boot process (regardless of whether the fTPM is benign or compromised) because we trust the OP-TEE environment. Out-of-scope are hardware attacks, side-channel attacks, control-flow attacks, and Denial of Service attacks.

1.4 Environment

This work was created at the 'Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC' in Garching. It is part of the 'Fraunhofer Society for the Promotion of Applied Research e. V.', which is an organization distributed over Europe with main focus on applied research. In the roughly 35 years of its existence, it rose to become the largest research institute in Europe with around 30,000 employees.

1.5 Outline

2 Background

This chapter discusses the relevant background knowledge required to understand the remainder of this work.

2.1 Trusted execution environment

One of the core security concepts of operating systems are the privilege levels of processes. Thereby, processes are protected against other processes with the same or lower privilege level. However, they are not protected against more privileged processes. This bears problems for example for cloud computing and edge computing. In cloud computing, other services, the hypervisor, or the cloud provider in general could potentially access sensitive data of the cloud tenant. In edge computing, the edge applications deal with plain text data, while they are potentially running on insecure edge devices. Hence, protection against more privileged processes is desired.

A Trusted execution environment (TEE) is an integrated hardware extension to processors. Effectively, the execution environment is separated into the Rich execution environment (REE) and the TEE by hardware. The REE runs the common software, e.g., a Linux-based operating system and the user applications. The TEE is an isolated tamper-resistant execution environment that guarantees the authenticity of the executed code, and the integrity of runtime states (e.g., memory) [3]. Since a TEE is integrated into the processor, there is no separate chip required. Moreover, the TEE commonly follows the same user and kernel space separation as REE operating systems. The kernel space is running a trusted OS kernel, and the user space is running the trusted applications.

Previous technologies ensure protection of data-in-transit, and data-at-rest, while TEE additionally protects data-in-use. For example, smart cards are commonly used to store keys to identify users and keys to encrypt data-at-rest [4].

One such TEE is ARM's TrustZone [5, 6]. It partitions all software and hardware resources of the containing system into the Normal world (NW) and the Secure world (SW). While the SW can access the resources of the SW and the NW, the NW is restricted to its own resources. Since ARM is the dominant processor architectures for IoT devices with a market share of 86 % [7], many of the approaches in this field of research rely on ARM technology such as TrustZone. Our approach also leverages TrustZone to enable the execution and the remote attestation of an fTPM.

Other TEE technologies are Intel Software Guard Extensions (SGX), and AMD Secure Encrypted Virtualization (SEV), in the future also Intel Trusted Domain Extensions (TDX), and ARM Confidential Computing Architecture (CCA). Since we focus on the implementation of our concept with ARM TrustZone, we do not go into detail about these other technologies here. However, since our concept is not tied to ARM processors and can also be applied to others, they are mentioned for the sake of completeness.

2.2 Attestation

According to the Cambridge Dictionary an attestation is "a formal statement that you make and officially say is true". Specifically in our context, attestation is a mechanism for software to prove its identity. In the following, the two types are discussed.

2.2.1 Local attestation

Local attestation enables assertions between two environments on the same system [8]. The claim of an environment can be verified by another environment, usually with the help of message authentication codes (MAC) [9]. For example, Intel SGX uses this mechanism to establish assertions between two enclaves [8].

2.2.2 Remote attestation

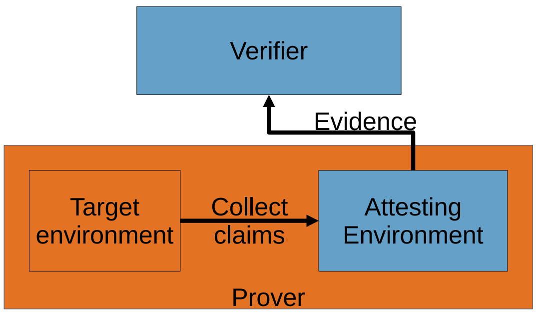


Figure 2.1: Data flow of remote attestation [10]. Initially, only the blue areas are trusted by the verifier. After the attestation, the verifier also trusts the target environment.

Remote attestation is a challenge-response protocol initiated by a remote attestor.

Figure 2.1 depicts a simplified overview of the data flow of a remote attestation. The process is initiated by a remote trusted party (called "verifier") to verify that a target environment on the end-device (called "prover") has not been tampered with [9, 11]. This challenge contains a nonce, enforcing a fresh response. The response must be an evidence of the challenged system that it is trustworthy. To build that, an attesting environment on the prover device generally inspects the following properties of a program: (i) its code and data has been correctly loaded into memory for execution, and (ii) its data has not been maliciously modified at runtime.

The attesting environment acts as a trust anchor for the verifier. A trusted anchor is required on the device to be attested because at least one trusted component is necessary to extract the data from the remote device to be verified. In many cases, TEE's act as a trust anchor because they are hardware-protected, making it an excellent candidate for a trust anchor.

2.3 Trusted Platform Module

The Trusted Computing Group (TCG) published the first TPM specification (v1.2) in 2009 [12], and the most current specification (v2.0 Revision 01.59) ten years later in 2019 [13]. It describes a cryptographic coprocessor that increases trust in the host platform. Specifically, this means that the platform exhibits the expected behavior and that this behavior can be trusted. For that, the TPM maintains a separated state from the host platform, which enables the TPM to take measurements of the host platform. It is also a passive device, meaning it only does something when prompted. Table 2.1 summarizes the main features of TPMs.

Table 2.1: TPM main features and exemplary use-cases.

Feature	Use-case
Device identification	for a network provider to identify a machine before granting it access to its VPN network
Encryption	file and folder encryption on a device
Key Storage	Store keys securely
Random Number Generator	Seed the key generation algorithms
Platform Configuration Registers	Store measurements of system components taken during the boot process

The Platform Configuration Register (PCR) values are the fundament for the remote system attestation. They are one-way registers, which values can never be written to an exact value, but only be extended. This is known as 'hash extend'. Its properties prohibit the removal of extensions, and the arbitrary writing of values, whether by a benign or malicious actor. The PCR value at index *i* can only be modified (i.e., extended) in the following way:

$$PCR(i)_0 \coloneqq 0, \quad PCR(i)_{t+1} \coloneqq hash(PCR(i)_t \parallel new\ value)$$

A PCR value holds a hash representing the platform state. Thereby, a remote attestor can request a so-called 'quote' from the TPM on the host in question. A quote contains the PCR values and is digitally signed.

Typically, a TPM contains 24 PCR values that form a bank, with the lower PCR values representing the system boot process and the higher ones representing the events after the kernel is booted [4]. The fixed length of the PCR values is important for memory-constrained TPMs [4].

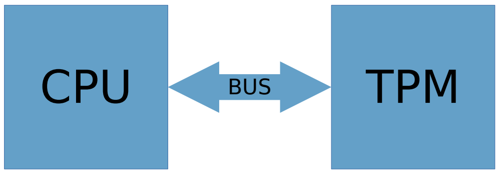
TPM 1.2 is limited to SHA-1 hashes which are considered broken [14–16]. Although the SHA-1 uses in TPM 1.2 were analyzed to be not affected [17], cryptographic algorithms only become weaker over time [4]. In reaction, TPM 2.0 offers crypto-agility and allows newer algorithms such as SHA-256. In general, TPM 2.0 is more flexible, and is always turned on, while a TPM 1.2 needed to be turned on manually. Also, TPM 2.0 is more consistent across different implementations because of broader specifications. TPM 2.0 is the focused version nowadays, e.g., Microsoft recommends TPM 2.0 over TPM 1.2 because of security advantages [18], and also requires TPM 2.0 for Windows 11 with SHA-256 PCR banks [2].

There are three types of TPMs, as illustrated in Figure 2.2. They all offer the same functionality, but with different security guarantees and performance characteristics.

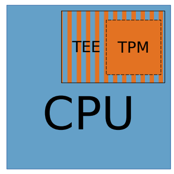
2.3.1 Discrete TPM

This is the classical form of a TPM. It is a dedicated piece of hardware, connected to the CPU via a bus. It is designed and manufactured to be highly temper-resistant against hardware attacks. The TPM specifications [13, 19] do not demand a specific bus system, however, they define the interfaces between the TPM and the following bus systems: LPC, I^2C, and SPI.

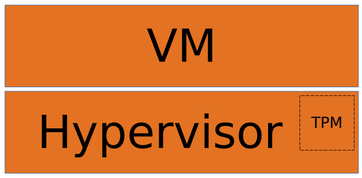
The well-known 'TPM Reset Attack' was independently described in [20, 21]. It requires minimal hardware, precisely only a wire connecting the reset line of the LPC bus [22] to ground. This results in a reset signal for the TPM, yielding predictable values for the PCR registers, i.e., 0. This allows an attacker to replay the measurement log of a benign boot process to achieve valid PCR values, even though a modified chain has been booted. Since TPM 1.2, TCG provides a mitigation specification for this reset



(a) Discrete TPM



(b) Firmware TPM



(c) Virtual TPM

Figure 2.2: Schematic illustration of the different TPM types in their pure form. Blue: Hardware, Orange: Software.

attack [23], requiring the BIOS to overwrite sensitive data after each unexpected reset, preventing an attacker to gain a valid measurement log. However, this mitigation is still vulnerable to cold boot attacks [24, 25].

Winter and Dietrich [25] demonstrate a bus modification attack at TPMs integrated with the LPC bus or the I^2C bus. Their approach, labeled 'Active LPC frame hijacking', allows them to "lift" commands to a higher locality than the one they were originally sent with. This allows them to evolve the 'TPM Reset attack' from being only usable for S-RTM, to also D-RTM systems. They also introduce a new approach of circumventing the TPM's measurement feature. Instead of resetting the TPM as previously described [20, 21], they reset the main device, i.e., the users' device like a desktop PC while preventing the TPM from receiving the reset signal. This keeps the state of the TPM, e.g., the valid PCR values of the previous boot procedure, and the attacker can hijack the boot procedure triggered by the platform's reset and boot a malicious operating system or firmware, while the TPM still stores the old and valid PCRs. While its conceptually easier since the attacker does not need to know the measurement log since the valid PCR values are already in-place, it requires active manipulation of bus transmissions to shield the TPM from the reset signal.

Seunghun Han et al. [26] report two attacks on discrete TPMs to reset the PCR registers. The first targets a gray area in the power management section of the TPM 2.0 specification. The TPM shall store its state into the (its?) non-volatile random access memory (NVRAM) before shutting down when the host platform goes to sleep, and restore it when it wakes up. However, the specification is missing a concrete description how to handle a lack of a stored state when waking up. Therefore, some implementations simply reset the state. Their second attack targets a DRTM, namely an implementation flaw in tboot [27], the most widely used measured boot environment used with Intel's Trusted Execution Technology. However, in their work, they found that some mutable function pointers are not measured, which allows attacks.

A time-based side-channel attack [28] during signature generation based on elliptic curves allows an attacker to recover 256-bit private keys for ECDSA and ECSchnorr signatures.

A passive sniffing attack is shown in [29]. It is applicable to TPM 1.1 connected to an LPC bus. They observed that the data of some operations like unsealing are transmitted via the bus in plain text. Since TPM 1.2, however, the modules no longer send sensitive data unencrypted [25].

That invasive hardware attacks against dTPMs are possible was already shown by Tarnovsky in 2010 [30]. However, this requires a lot of time, knowledge and resources, i.e., hardware and money.

2.3.2 Firmware TPM

As seen in the previous section about discrete TPMs, the bus between the CPU and a TPM can be considered as their biggest attack vector. An fTPM [31, 32] circumvents this by being directly executed within the CPU within a TEE, revealing no easily accessible bus. The trend is moving towards fTPMs, which can also been seen by the increasing efforts to bring an fTPM to the RISC-V processor family [33]. Also, since they require less hardware, they are cheaper for manufacturers.

Cheng et al. [34] conducted a detailed performance comparison between dTPMs and fTPMs. They found that fTPMs are faster overall. In addition, as is the nature of software, fTPMs are easier to update than dTPMs.

However, there are also disadvantages. First, they cannot provide true RNG, since hardware is required for that. Second, they are started later in the hosts' boot chain than a dTPM that is accessible from the beginning. This has the consequence that the hashes of the components booted before the fTPM cannot be sent to the fTPM. Last, fTPMs depend on more components for its security than single-component dTPMs, e.g., the TEE, and the boot chain.

Of course, there are also attacks against fTPMs. The previously mentioned side-channel attack [28] against dTPMs, can also be applied to fTPMs.

Jacob et al. [35] target proprietary AMD fTPMs by attacking their TEE, namely the AMD Secure Processor (AMD-SP). Thereby, they can expose the full internal state of the fTPM bypassing any authentication mechanisms. To do so, they leak the secret key from the BIOS flash chip which is used to derive the encryption and signature keys for the fTPMs non-volatile data. They achieve this by using a voltage fault injection that bypasses the authenticity check in the hosts' boot process and allows them to boot their own firmware component that leaks the required information.

Cfir Cohen from Google's cloud security team has uncovered an attack on fTPMS, which also runs on AMD-SP [36]. They store a maliciously crafted payload - a certificate - on the fTPM and trigger a function with a stack-based overflow error that accesses this payload, giving them full control over the program counter.

2.3.3 Virtual TPM

2.4 Secure Boot and Measured Boot

Secure boot is a concept of UEFI doing local attestation of components directly at boot-time. Based on signatures of next-to-boot components. It cancels the boot process as soon as deviations are detected. Binaries of components are first signed and then, deployed universally. Hence, binaries are not bound to the platform and can be considered portable in this context.

Measured Boot is a concept that is often implemented in interplay with a TPM. Measured Boot allows remote attestation to a later time. Uses sealing functionality of TPMs, therefore, bound to the exact platform. Its goal is to detect manipulated system configurations.

Both technologies are often used in conjunction.

3 Related Work

In the following, we describe defense mechanisms for fTPMs that can be seen as complementary to our approach. They all have in common that they offer no way for a third party to ensure that the hardened fTPM is actually running on the device under test, which is exactly what our work aims to cover.

One approach is to verify the code of fTPMs [37]. Here, the TPM 1.2 code is written in a functional programming language that enables automatic verification.

There exist efforts to improve the security of TPM by introducing the concept of hybrid TPMs [38, 39]. Kim and Kim [38] extend a hardware TPM with software support, which they name hTPM. This increases the defense of the TPM, e.g., circumventing side-channel attacks, and also enables more secure TPM functions, e.g., enabling true random number generation. Their hTPM implementation also shows significantly better performance due to the use of modern CPU features. Vice versa, Gross et al. [39] propose the reverse approach of backing an fTPM with hardware. While their implementation has similar properties to hTPM, it inherits some downsides of fTPMs. For example, their fTPM is still started later in the boot chain than a dTPM, which is not the case for hTPM. However, it is easier to update than hTPM since the lack of a dTPM, and the overall design is simpler.

Abbreviations

TEE Trusted execution environment

REE Rich execution environment

PCR Platform Configuration Register

TCG Trusted Computing Group

NW Normal world

SW Secure world

List of Figures

List of Tables

Bibliography

[1] P. C. of Advisors on Science and Technology. *Immediate opportunities for strengthening the nation's cybersecurity*. Nov. 2013.

[2] Microsoft. *Windows 11 Minimum Hardware Requirements*. June 2021. URL: https://learn.microsoft.com/en-us/windows-hardware/design/minimum/minimum-hardware-requirements-overview.

[3] M. Sabt, M. Achemlal, and A. Bouabdallah. "Trusted Execution Environment: What It is, and What It is Not." In: *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE, Aug. 2015. DOI: 10.1109/trustcom.2015.357.

[4] W. Arthur. *A Practical Guide to TPM 2.0 Using the New Trusted Platform Module in the New Age of Security. Using the New Trusted Platform Module in the New Age of Security*. Springer Nature, 2015, p. 392. ISBN: 9781430265849.

[5] ARM Limited. *ARM Security Technology - Building a Secure System using TrustZone Technology*. Issue C. 2009.

[6] B. Ngabonziza, D. Martin, A. Bailey, H. Cho, and S. Martin. "TrustZone Explained: Architectural Features and Use Cases." In: *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, Nov. 2016. DOI: 10.1109/cic.2016.065.

[7] E. foundation. *IoT & Edge Developer Survey Report*. (Accessed July 2022). 2022. URL: https://outreach.eclipse.foundation/iot-edge-developer-2021.

[8] I. Anati, S. Gueron, S. Johnson, and V. Scarlata. "Innovative Technology for CPU Based Attestation and Sealing." In: 2013.

[9] J. Ménétrey, C. Göttel, A. Khurshid, M. Pasin, P. Felber, V. Schiavoni, and S. Raza. "Attestation Mechanisms for Trusted Execution Environments Demystified." In: *Distributed Applications and Interoperable Systems*. Springer International Publishing, 2022, pp. 95–113. DOI: 10.1007/978-3-031-16092-9_7.

[10] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan. *Remote ATtestation procedureS (RATS) Architecture*. RFC 9334. Jan. 2023. DOI: 10.17487/RFC9334. URL: https://www.rfc-editor.org/info/rfc9334.

[11] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. "Principles of remote attestation." In: *International Journal of Information Security* 10.2 (Apr. 2011), pp. 63–81. DOI: 10.1007/s10207-011-0124-7.

[12] ISO/IEC 11889:2009. *Trusted Platform Module*. Standard. Geneva, CH: International Organization for Standardization, May 2009.

[13] Trusted Computing Group. *Trusted Platform Module Library Specification*. Family "2.0", Level 00, Revision 01.59. May 2019.

[14] V. Rijmen and E. Oswald. *Update on SHA-1*. Cryptology ePrint Archive, Paper 2005/010. https://eprint.iacr.org/2005/010. 2005. URL: https://eprint.iacr.org/2005/010.

[15] X. Wang, Y. L. Yin, and H. Yu. "Finding Collisions in the Full SHA-1." In: *Advances in Cryptology – CRYPTO 2005*. Springer Berlin Heidelberg, 2005, pp. 17–36. DOI: 10.1007/11535218_2.

[16] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. "The First Collision for Full SHA-1." In: *Advances in Cryptology – CRYPTO 2017*. Springer International Publishing, 2017, pp. 570–596. DOI: 10.1007/978-3-319-63688-7_19.

[17] K. Goldman and S. Potter. *SHA-1 Uses in TPM v1.2*. Apr. 2010.

[18] Microsoft. *TPM recommendations*. Feb. 2023. URL: https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations.

[19] Trusted Computing Group. *TCG PC Client Platform Firmware Profile Specification*. Level 00 Version 1.05 Revision 23. May 2021.

[20] B. Kauer. "OSLO: Improving the Security of Trusted Computing." In: *16th USENIX Security Symposium (USENIX Security 07)*. Boston, MA: USENIX Association, Aug. 2007. URL: https://www.usenix.org/conference/16th-usenix-security-symposium/oslo-improving-security-trusted-computing.

[21] E. R. Sparks. "A Security Assessment of Trusted Platform Modules." In: *Dartmouth College Undergraduate Theses* (2007).

[22] Intel. *Intel® Low Pin Count (LPC)*. Aug. 2002. URL: https://www.intel.com/content/dam/www/program/design/us/en/documents/low-pin-count-interface-specification.pdf.

[23] Trusted Computing Group. *TCG PC Client Platform Reset Attack Mitigation Specification*. Family "2.0", Version 1.10 Revision 17. Jan. 2019.

[24] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. “Lest we remember.” In: *Communications of the ACM* 52.5 (May 2009), pp. 91–98. DOI: 10.1145/1506409.1506429.

[25] J. Winter and K. Dietrich. “A hijacker's guide to communication interfaces of the trusted platform module.” In: *Computers & Mathematics with Applications* 65.5 (Mar. 2013), pp. 748–761. DOI: 10.1016/j.camwa.2012.06.018.

[26] S. Han, W. Shin, J.-H. Park, and H. Kim. “A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping.” In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1229–1246. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/han.

[27] Intel. *Trusted Boot*. URL: https://www.sourceforge.net/projects/tboot.

[28] D. Moghimi, B. Sunar, T. Eisenbarth, and N. Heninger. *TPM-FAIL: TPM meets Timing and Lattice Attacks*. 2019. DOI: 10.48550/ARXIV.1911.05673.

[29] K. Kursawe, D. Schellekens, and B. Preneel. “Analyzing trusted platform communication.” In: 2005.

[30] C. Tarnovsky. *Hacking the smartcard chip*. 2010. URL: http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html.

[31] H. Raj, S. Saroiu, A. Wolman, R. Aigner, J. Cox, P. England, C. Fenner, K. Kinshumann, J. Loeser, D. Mattoon, M. Nystrom, D. Robinson, R. Spiger, S. Thom, and D. Wooten. *fTPM: A Firmware-based TPM 2.0 Implementation*. Tech. rep. MSR-TR-2015-84. Nov. 2015. URL: https://www.microsoft.com/en-us/research/publication/ftpm-a-firmware-based-tpm-2-0-implementation/.

[32] H. Raj, S. Saroiu, A. Wolman, R. Aigner, J. Cox, P. England, C. Fenner, K. Kinshumann, J. Loeser, D. Mattoon, M. Nystrom, D. Robinson, R. Spiger, S. Thom, and D. Wooten. “fTPM: A Software-Only Implementation of a TPM Chip.” In: *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, pp. 841–856. ISBN: 978-1-931971-32-4. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/raj.

[33] M. Boubakri, F. Chiatante, and B. Zouari. “Towards a firmware TPM on RISC-V.” In: *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, Feb. 2021. DOI: 10.23919/date51398.2021.9474152.

[34] J. L. Cheng, K. C. Chen, H. W. Zhang, W. Y. Chen, and D. Y. Wu. "Emulating Trusted Platform Module 2.0 on Raspberry Pi 2." In: *International Journal of Security, Privacy and Trust Management* 9.3 (Aug. 2020), pp. 1–11. DOI: 10.5121/ijsptm.2020.9301.

[35] H. N. Jacob, C. Werling, R. Buhren, and J.-P. Seifert. *faulTPM: Exposing AMD fTPMs' Deepest Secrets*. 2023. DOI: 10.48550/ARXIV.2304.14717.

[36] C. Cohen. *AMD-PSP: fTPM Remote Code Execution via crafted EK certificate*. Jan. 2018. URL: https://seclists.org/fulldisclosure/2018/Jan/12.

[37] A. Mukhamedov, A. D. Gordon, and M. Ryan. "Towards a Verified Reference Implementation of a Trusted Platform Module." In: *Security Protocols XVII*. Springer Berlin Heidelberg, 2013, pp. 69–81. DOI: 10.1007/978-3-642-36213-2_11.

[38] Y. Kim and E. Kim. "hTPM." In: *Proceedings of the 1st ACM Workshop on Cyber-Security Arms Race*. ACM, Nov. 2019. DOI: 10.1145/3338511.3357348.

[39] M. Gross, K. Hohentanner, S. Wiehler, and G. Sigl. "Enhancing the Security of FPGA-SoCs via the Usage of ARM TrustZone and a Hybrid-TPM." In: *ACM Transactions on Reconfigurable Technology and Systems* 15.1 (Nov. 2021), pp. 1–26. DOI: 10.1145/3472959.