

One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization

Robert Buhren
robert.buhren@sect.tu-berlin.de
Technische Universität Berlin - SECT

Thilo Krachenfels
tkrachenfels@sect.tu-berlin.de
Technische Universität Berlin - SECT

Hans Niklas Jacob
hnj@sect.tu-berlin.de
Technische Universität Berlin - SECT

Jean-Pierre Seifert
jpseifert@sect.tu-berlin.de
Technische Universität Berlin - SECT
Fraunhofer SIT

ABSTRACT

AMD Secure Encrypted Virtualization (SEV) offers protection mechanisms for virtual machines in untrusted environments through memory and register encryption. To separate security-sensitive operations from software executing on the main x86 cores, SEV leverages the AMD Secure Processor (AMD-SP). This paper introduces a new approach to attack SEV-protected virtual machines (VMs) by targeting the AMD-SP. We present a voltage glitching attack that allows an attacker to execute custom payloads on the AMD-SPs of all microarchitectures that support SEV currently on the market (Zen 1, Zen 2, and Zen 3). The presented methods allow us to deploy a custom SEV firmware on the AMD-SP, which enables an adversary to decrypt a VM's memory. Furthermore, using our approach, we can extract endorsement keys of SEV-enabled CPUs, which allows us to fake attestation reports or to pose as a valid target for VM migration without requiring physical access to the target host. Moreover, we reverse-engineered the Versioned Chip Endorsement Key (VCEK) mechanism introduced with SEV Secure Nested Paging (SEV-SNP). The VCEK binds the endorsement keys to the firmware version of TCB components relevant for SEV. Building on the ability to extract the endorsement keys, we show how to derive valid VCEKs for arbitrary firmware versions. With our findings, we prove that SEV cannot adequately protect confidential data in cloud environments from insider attackers, such as rogue administrators, on currently available CPUs.

KEYWORDS

Secure Encrypted Virtualization, SEV, Secure Nested Paging, SNP, hardware fault attack, voltage glitching

1 INTRODUCTION

Introduced in 2016, AMD's Secure Encrypted Virtualization (SEV) technology is the first commercially available solution aiming to protect virtual machines (VMs) from higher-privileged entities [29]. Prominent use cases for SEV are cloud environments, where the high-privileged hypervisor has direct access to a VM's memory content. In this scenario, a VM without SEV is unprotected from an administrator with malicious intentions. By encrypting a VM's memory, SEV aims to protect customers' data even when threatened by such an insider attack.

"... SEV protects data-in-use enabling customer workloads to be protected cryptographically from each other as well as protected from the hosting software. Even an

administrator with malicious intentions at a cloud data center would not be able to access the data in a hosted VM." [29, p. 9]

SEV leverages AES encryption to ensure the confidentiality of data-in-use by transparently encrypting a VM's memory with a VM-specific key. The memory encryption is carried out by a dedicated memory encryption engine embedded in the memory controller [2]. Recently presented extensions to SEV, SEV Encrypted State (SEV-ES) and SEV Secure Nested Paging (SEV-SNP), expand the encryption to the VM's register content and introduce software-based integrity protection using memory ownership tracking [3, 28]. Besides runtime protection, SEV provides a remote attestation feature allowing VM-owners to validate the correct instantiation of VMs even if the hypervisor is not fully trusted.

To ensure the confidentiality of VM memory encryption keys and the integrity of the remote attestation feature, AMD CPUs contain a dedicated security co-processor, the AMD Secure Processor (AMD-SP)¹. The AMD-SP constitutes the root-of-trust for modern AMD CPUs [35] and manages SEV-related VM life-cycle tasks such as deployment and migration [2]. The AMD-SP uses its own local memory and executes a firmware provided by AMD. While the hypervisor, executing on the main x86 cores, is still in control of the VMs, i.e., it is responsible for scheduling VMs, only the AMD-SP can access a VM's memory encryption key. This separation guarantees that a malicious or compromised hypervisor cannot access a VM's data.

Previous research revealed that the AMD-SP is a single point of failure for the SEV technology [14, 15, 18]. However, the presented issues are either limited to a specific CPU type, e.g., the issues presented in [14, 15] only affect the first generation of AMD Epyc CPUs (Zen 1), or are effectively mitigated by firmware updates [18]. To the best of our knowledge, no AMD-SP-related security issues that affect SEV are known for the current and last generation of AMD Epyc CPUs (Zen 2 and Zen 3).

Given the criticality of the AMD-SP for the security properties of the SEV technology, the question can be raised if there is a systematic way to mount attacks against SEV-protected VMs by targeting the AMD-SP. Particularly, one could consider fault attacks that do not depend on the presence of software issues but instead force genuine code to enter an unintended state. Recently, researchers applied this attack technique to Intel CPUs and mounted attacks against SGX enclaves [17, 38].

¹Formerly known as Platform Security Processor (PSP)

Due to its crucial role in the SEV technology, targeting the AMD-SP instead of the protected VMs potentially allows an attacker to circumvent any protection guarantees of SEV, independent from the targeted VM. Consequently, in this work, we answer the following research question: What are the implications of fault injection attacks against the AMD-SP for the SEV technology?

1.1 Contributions

In this work, we analyze the susceptibility of the AMD SEV technology towards physical attacks targeting the AMD-SP. By manipulating the input voltage to AMD systems on a chip (SoCs), we induce an error in the read-only memory (ROM) bootloader of the AMD-SP, allowing us to gain full control over this root-of-trust. This type of attack is commonly referred to as *voltage fault injection* attacks.

Building on this capability, we show that we can extract SEV-related secrets, i.e., Chip Endorsement Keys (CEKs), that can be leveraged to mount fully remote attacks as previously presented in [15]. In contrast to their work, our approach does not depend on firmware issues and re-enables the attacks presented in their work on all SEV-capable CPUs. Additionally, we reverse-engineered the new key-versioning scheme introduced by the SEV Secure Nested Paging (SEV-SNP) extension that binds the CEK to TCB component versions. This new key, called Versioned Chip Endorsement Key (VCEK), is cryptographically bound to firmware versions of the target system. Our glitching attack enables us to extract seeds for the VCEK that allow an attacker to derive the valid VCEKs for all possible combinations of firmware versions. This attack is the first – publicly known – attack against the recently released SEV-SNP extension.

We present our approach to determine the CPU-specific glitching parameters, i.e., the length and the depth of the voltage drop. After determining these parameters in an initial characterization phase, our attack can be mounted fully automatic and requires no knowledge of the internal structure of the ROM bootloader.

Both the attack and the characterization of the target CPU require only a cheap (~30 \$) μ Controller [40] and a flash programmer (~12 \$), making this attack feasible even for attackers with no access to special equipment. We successfully mounted the attack on AMD Epyc CPUs of all microarchitectures that support the SEV technology, i.e., Naples (Zen 1), Rome (Zen 2), and Milan (Zen 3). We publish our firmware to mount the glitching attack, the code of our payloads and our implementation of SEV’s key-derivation functions under an open-source license at (*Reference not yet available*). To prove the successful extraction endorsement keys, we publish valid signatures over the title of this paper at (*Reference not yet available*). The signatures can be validated using public keys, retrieved from AMD key servers at [4, 6].

We responsibly disclosed our findings to AMD, including our experimental setup and code.

2 RELATED WORK

Voltage glitching attacks targeting security-sensitive operations on CPUs have been subject to extensive analysis in the past. The majority of reported attacks have been carried out on small embedded systems and SoCs, where typically crowbar circuits (see Section 3.3

for details) are used to inject the fault, e.g., in [12, 21, 48]. A more thorough list of voltage glitching attacks can be found in [22].

More recently, voltage glitching attacks against Intel desktop and server CPUs have been reported, which use available interfaces to voltage regulators (VRs) for glitching the supply voltage.

Several authors demonstrated how code running in the Intel SGX enclaves can be faulted by injecting glitches through a software-based voltage scaling interface [30, 38, 41]. Thereby, SGX’s integrity properties are violated, and keys from cryptographic operations running inside the secure enclave can be extracted.

The work most related to our attack is presented by Chen et al. in [17]. The authors demonstrate the first physical attack targeting SGX enclaves entitled *VoltPillager*. VoltPillager improves the timing precision of software-based fault attacks and leverages direct hardware access to the VR for injecting glitches. By connecting wires to the bus between the CPU and the VR, the authors could inject commands causing voltage glitches with higher timing precision than the previously mentioned software-based fault injection methods. Furthermore, the attack is also applicable on patched systems, where the software interfaces for controlling the voltage are not accessible to an adversarial process. Although our attack uses the same mechanism to alter the input voltage to the SoC, namely the external VR, several factors distinguish our approach from theirs. We, therefore, compare our approach with VoltPillager in Section 4.

Since its introduction in 2016, several attacks against SEV have been published. Previous attacks predominantly target the runtime protection of SEV or SEV-ES protected systems [20, 24, 33, 36, 37, 51, 54]. These attacks either rely on the ability to write to encrypted guest memory, the ability to access the guest’s general-purpose register, or the ability to alter the mapping between guest-physical and host-physical pages of a SEV-protected VM. SEV-ES effectively mitigates attacks that require access to a guest’s register state, and SEV-SNP mitigates attacks that alter a guest’s memory layout or content. A different direction is explored in [42]. The authors present issues inside the Linux kernel of SEV-enabled guests that allow the circumvention of SEV’s security properties. By manipulating the result of the `cpuid` instruction, they show how an attacker could trick the guest into not enabling the SEV protection at all. To counter this issue, SEV-SNP introduces a “Trusted CPUID” feature that prevents a hypervisor from reporting an invalid CPU feature set.

In [15], the authors analyze SEV’s remote attestation mechanism. They revealed security issues in the AMD-SP’s firmware that enable an attacker to deploy a custom SEV firmware and extract keys critical to the remote attestation. Using a manipulated SEV firmware, an attacker can override the debug policy of SEV-enabled VM’s and thereby decrypt its memory. The extracted keys can be used to fake the presence of SEV during deployment or migration. These attacks require the presence of firmware issues in the AMD-SP. Although the work shows that the AMD-SP is crucial for the security properties of SEV, the presented firmware issue is only present on the first generation of SEV capable CPUs, i.e., Zen 1 (Naples). To the best of our knowledge, no comparable firmware issue for later generations of AMD CPUs has been published. Besides allowing to attack SEV-SNP, our new attack re-enables the attacks presented

in [15] for CPUs of all microarchitectures that support SEV (Zen 1, Zen 2, and Zen 3), without relying on firmware issues.

3 BACKGROUND

This section introduces the Secure Encrypted Virtualization (SEV) technology, voltage fault injection as means to induce errors in security-sensitive operations, and the VR communication protocol.

3.1 Secure Encrypted Virtualization

The SEV technology offers protection mechanisms for VMs in untrusted environments, such as cloud environments [29]. In contrast to Intel's Software Guard Extensions (SGX), which focus on protecting *parts* of an application, SEV protects full VMs. The *runtime protection* of VMs is achieved by transparently encrypting a VM's memory. The *remote attestation* feature of SEV allows cloud customers to validate the correct deployment of the VM. Since its introduction in 2016, AMD has introduced two extensions to SEV that add additional protection features to SEV. While SEV-ES adds encryption for guest VM registers [28], SEV-SNP introduces, amongst others, *software-based* integrity protection and an enhanced Trusted Computing Base (TCB) versioning feature for the Chip Endorsement Key (CEK) [3]. The CEK cryptographically links the target platform to the AMD root of trust.

Both the runtime protection and the remote attestation feature require the hypervisor to use an interface provided by a dedicated firmware running on the AMD-SP. The API for SEV and SEV-ES is specified in [2], whereas SEV-SNP uses a dedicated API specified in [8]. The SEV firmware is responsible for managing the memory encryption keys of the VMs and implementing the remote attestation feature of SEV.

Our approach re-enables the previously presented attacks by Buhren et al. by allowing the execution of custom code on the AMD-SP. Therefore, for details on SEV and SEV-ES protected systems, we refer to their paper [15], while the remainder of this section focuses on the SEV-SNP technology.

3.1.1 SNP Runtime Protection. In addition to the memory encryption introduced by SEV and the register encryption introduced by SEV-ES, SEV-SNP adds software-based memory integrity protection. For SEV-SNP enabled VMs, the CPU will track ownership of memory pages using the Reverse Mapping (RMP) table. Memory accesses are subject to an RMP check to ensure that, e.g., the hypervisor cannot access encrypted guest memory or manipulate the mapping between guest-physical and host-physical. The RMP access check mitigates previously presented attacks that rely on the hypervisor's ability to write or remap a VM's memory.

3.1.2 SNP Remote Attestation. With SEV-SNP, a VM can request an attestation report at an arbitrary point in time. To that end, the VM communicates with the AMD-SP via an encrypted and integrity-protected channel. The SEV firmware will generate an attestation report that includes a measurement of the initial VM state and additional information about the host platform. A VM can also include 512 bits of arbitrary data in the report, e.g., a hash of a public key generated in the VM. The VM can then provide this attestation report to a third party, such as the guest owner. The attestation report is signed with platform specific endorsement key,

the VCEK. Using an ID provided by the AMD-SP, a guest owner can retrieve a signed VCEK for a specific AMD SoC from an AMD key server [6]. The VCEK is signed by the AMD Root Key (ARK) which can be retrieved from an AMD website [5]. For each AMD Zen microarchitecture, there exists a different ARK. Using the obtained VCEK and the ARK, the guest owner can validate that an authentic AMD-SP has issued the report. The signed attestation report links the data in the report provided by the guest to the respective VM. If the VM provided the hash of a public key within the attestation report, a genuine report proves that the VM owns the corresponding key pair.

3.1.3 SNP Versioned Chip Endorsement Key. SEV and SEV-ES rely on a static, non-revocable ECDSA key (the CEK), to authenticate a remote AMD SoC. Firmware issues that enable CEK extraction, as presented in [15], have severe implications for SEV. An extracted CEK allows an attacker to fake attestation reports or pose a valid target for VM migration. As it is impossible to revoke a CEK, firmware updates are not sufficient to mitigate these attacks.

SEV-SNP, therefore, introduces the Versioned Chip Endorsement Key (VCEK). A VCEK is derived on the AMD-SP from chip-unique fused secrets and bound to firmware security versions of components which are part of SEV's TCB. These security version numbers (SVNs) are combined in a single TCB version string as shown in Table 1. In case of a known firmware issue, an update of a single

Byte(s)	0	1	2-5	6	7
Field	BOOT_LOADER	TEE	RSVD	SNP	MICROCODE

Table 1: SEV-SNP's TCB version string [8, Chapter 2.2].

TCB component will result in a different VCEK. To retrieve the signed VCEK, the user has to provide the ID of the target platform, as well as the SVNs for which the signed VCEK should be retrieved.

SEV-SNP allows to downgrade the SVN of the TCB components to provide backward compatibility. To that end, SEV-SNP provides the `SNP_SET_REPORTED_TCB` API call. The firmware ensures that the call can only be used to set a lower TCB version. Providing higher SVNs than the current counter values results in an error.

In contrast to the CEK, the VCEK is cryptographically bound to specific firmware versions. Hence, previously extracted VCEKs are no longer valid after a firmware upgrade. Any party involved in the attestation process can now enforce minimum TCB component versions.

3.1.4 SNP Migration. Migration of SEV-protected VMs requires a dedicated mechanism, as the VM memory encryption key is solely accessible by the AMD-SP. For SEV and SEV-ES, the AMD-SP is involved in the migration processes and policy enforcement. Using a Diffie-Hellman key exchange, the involved AMD-SPs on the source and target of the migration derive shared transport keys to migrate the memory.

To allow more complex migration schemes, SEV-SNP introduces Migration Agents (MAs). A MA is a dedicated VM associated with one or multiple VMs and is responsible for migrating a VM. In the first step, the hypervisor uses the `SNP_PAGE_SWAP_OUT` SEV-SNP

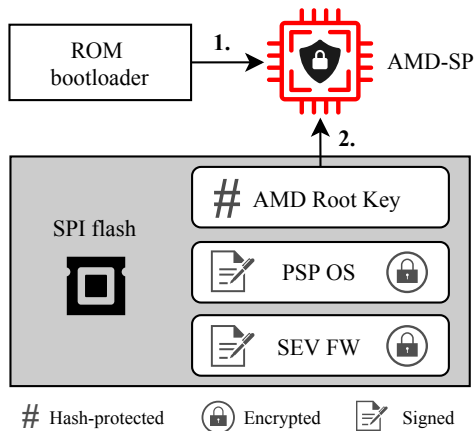


Figure 1: Overview of the AMD-SP's firmware components relevant to the TCB of SEV protected VMs.

API command to export a VM's memory. The AMD-SP will re-encrypt the memory using a dedicated key, the Offline Encryption Key (OEK). The AMD-SP generates the OEK during the initial launch of a VM.

Then the hypervisor calls the MA, which will retrieve the *guest context* of the respective VM using the VM Export AMD-SP API command. The context represents the internal VM state for SEV-SNP and contains, amongst others, the OEK used to re-encrypt a VM's memory pages during migration. The AMD-SP ensures that the context is only exported to MAs that are associated with the respective VM. The MA can now enforce arbitrary policies for the migration process, as only the MA can decrypt the memory pages. To re-import a VM, a MA on the target host can re-create the VM using the guest context and the encrypted guest memory.

The MA associated with a VM is part of a VM's TCB, as it can retrieve the guest context including the OEK. To enable guest owners to validate the MA associated with their VM, the AMD-SP remote attestation reports include the measurement of the MA.

Alternatively, SEV-SNP supports a guest-assisted migration mode where the memory pages are transferred by trusted component within the guest itself.

3.2 AMD Secure Processor

Initially introduced in 2013 under the name Platform Security Processor (PSP) [31], the AMD-SP is a dedicated security processor and contained within AMD CPUs. The AMD-SP is an ARMv7 core with dedicated SRAM executing a firmware provided by AMD and is the root-of-trust for the AMD SoC. The AMD-SP executes a firmware that implements the SEV-related functions defined in the SEV-API [2], respectively the SEV-SNP-API [8]. The firmware is loaded from an SPI-attached flash chip and is stored alongside the UEFI firmware [14].

AMD-SP Boot Procedure. [15] analyzes the AMD-SP's boot procedure on AMD Epyc Naples (Zen 1) CPUs. Figure 1 depicts AMD-SP's firmware components relevant for SEV. On these systems, the AMD-SP initially starts executing from a non-updatable ROM bootloader, see Figure 1 Step 1. The ROM bootloader is responsible for

loading and verifying an RSA public key from a modifiable SPI flash. This public key is used to validate the integrity of files loaded from the SPI flash. The public key itself is verified using hashes stored within the bootloader ROM, Step 2 of Figure 1.

In the following steps, the ROM bootloader loads another boot stage, called the *PSP OS* by Buhren et al. [15], from the SPI attached flash. This boot stage contains a proprietary operating system and will later load and verify the SEV firmware from flash. Both this second boot stage and the SEV firmware are validated using the public key loaded by the ROM bootloader. The public key used to authenticate the PSP OS and the SEV firmware is identical to the ARK of the corresponding microarchitecture.

We confirmed that the described boot procedure is present in all CPUs we analyzed. However, on Epyc Milan (Zen 3) systems, both the PSP OS, as well as the SEV firmware component are encrypted and the SEV firmware is validated using a public key embedded in the PSP OS instead of the ARK. In Section 5.6, we describe how we decrypt these components to enable further analysis.

3.3 Fault Injection by Voltage Glitching

Integrated circuits (ICs) need to be operated under the specified conditions to function as intended, e.g., within rated supply voltage, clock stability, temperature, and electromagnetic field ranges [11]. This dependency can be misused to force faulty behavior during the chip's operation. Glitches on the supply voltage line, i.e., short supply voltage variations, can be used to produce computational errors on CMOS circuits at low cost [19]. Unintended bit flips, corrupted instructions, and skipping of instructions in a microprocessor are examples of such errors. If these errors are forced during the execution of cryptographic algorithms, information about the secret key or plaintext might be leaked [11]. On the other hand, faults can be used to skip security checks, enter protected code paths, or gain code execution [34, 48].

Depending on the design of the target, different approaches can be used to inject faults into the supply voltage rail. In case the voltage is supplied externally to the printed circuit board (PCB), an external power supply can introduce glitches through that interface. If the voltage is generated directly on the PCB using a voltage regulator (VR), the injection of glitches becomes more complex. On the one hand, glitches can be injected using a so-called crowbar circuit, which creates a short circuit between the voltage line and GND, effectively enforcing a voltage drop [39]. On the other hand, on more advanced systems, such as SoCs, the VRs typically offer communication interfaces to adjust the voltage on demand. These interfaces, if not adequately protected, can also be leveraged to inject voltage glitches [17, 38, 41].

3.4 SVI2 Protocol

The demand for processors trimmed for high performance which at the same time show deterministic behavior, has put increased requirements on the power management of x86 processors [1]. The power consumption of a processor is directly linked with its current consumption and supply voltage. To maximize performance gain, the power consumption in modern processors is managed by dedicated on-chip μ Controllers, which measure voltage/current in real time. Recent AMD processors dynamically monitor and adjust their

primary (Core and SOC) voltage rails, which is also known as dynamic voltage scaling [1]. Through the serial voltage identification interface 2.0 (SVI2), the processor can directly communicate with a VR to monitor and alter the supply voltages. The AMD SVI2 is a three-wire interface with clock (SVC), data (SVD), and telemetry (SVT) lines. Although the corresponding specification by AMD is not publicly available, all the necessary information on SVI2 can be gathered from datasheets of different VRs implementing the interface, e.g., from [26, 27, 44, 45].

The SVI2 protocol is similar to the I²C bus concept. The CPU acts as master and sends control packets via the SVC and SVD lines to the VR. SVI2 control packets consist of 3 bytes transmitted conforming to the *SMBus send byte* protocol: 1 byte for selecting the voltage domain (Core or SOC) followed by an acknowledgement (ACK) bit, and then 2 bytes containing the voltage to be applied and other configuration parameters, each byte followed by an ACK bit [44]. Due to the configuration encoding, the voltage can be configured with a step size of 6.25 mV. Through the telemetry function (TFN) configuration bits, periodic voltage (and current) reports from the VR to the CPU via the SVC and SVT lines can be enabled. Details about the telemetry package format can be found in [45].

4 ATTACK SCENARIO

One of the most prominent use cases for the SEV technology, are cloud environments. In cloud environments, the physical systems hosting the VMs are under full control of a cloud service provider (CSP). In our attack scenarios, the attacker aims to access a SEV-protected VM's memory content by attacking the AMD-SP. We make no assumptions on whether SEV-ES, SEV-SNP, or just SEV is active. We consider an attacker who has either access to the physical hosts that execute the targeted VM or access the CSP's maintenance interfaces that allow to, e.g., migrating a VM to another physical system. Examples for attackers with these capabilities are maintenance or security personnel or system administrators of the CSP. We do not assume the presence of firmware or software bugs in the targeted host or VM for our attack scenarios. Based on these capabilities, we showcase two different approaches to access a SEV-protected VM's data. The attack scenarios are inspired by the attacks presented in [15], but are adapted to SEV-SNP. We want to emphasize that these scenarios are merely two examples of possible attacks. Due to the AMD-SP's critical role for the SEV technology, targeting the AMD-SP potentially enables several other attack scenarios.

Scenario 1: Debug Override. As previously presented in [15], the SEV API provides debug features that allow the de- and encryption of a VM's memory [2, Chapter 7]. A similar feature exists for SEV-SNP [8, Section 8.23]. Both SEV's and SEV-SNP's debug features are subject to a policy check enforced by the SEV firmware. Only if a guest owner explicitly enabled debugging during the initial deployment, the SEV firmware will allow the debug API commands.

By altering the SEV firmware, an attacker could override this policy enforcement to allow the debug commands regardless of a guest owner's policy. To that end, the attacker must replace the SEV firmware on the physical machine that hosts the target VM. Alternatively, the attacker could first migrate the targeted VM to



Figure 2: SPI bus traces during the initial boot. CS and MISO lines only. The upper part depicts SPI bus activity for the original flash image (“CS original” and “MISO original”). The lower part shows the corresponding SPI signals for a flash image with a manipulated ARK.

a previously prepared system. The attacker can then use the previously mentioned debug API calls to decrypt a VM's memory regardless of the policy specified by the guest owner.

Scenario 2: Forge Attestation. In this second scenario, the attacker has access to the control interface of the hypervisor to initiate migrations of SEV-protected VMs. However, in contrast to the first scenario, the attacker does not need to alter the firmware of the targeted host. Instead, the attacker needs to extract the CPU-specific endorsement keys of the same CPU microarchitecture as the targeted host's CPU. These endorsement keys play a central role in the remote attestation feature of the SEV technology, see Section 3.1.1. To decrypt a VM's memory, the attacker could fake the attestation report during deployment or migration to trick a VM into accepting a malicious MA. The MA is part of a VM's TCB and has access to the Offline Encryption Key (OEK) of exported VMs, see Section 3.1.4. Using the OEK, a malicious MA can decrypt a VM's memory. For pre-SEV-SNP systems, a similar attack has been proposed in [15].

Both presented example scenarios require the attacker to gain code execution on the AMD-SP. Therefore, in the following sections, we present our analysis of the AMD-SP's susceptibility towards voltage fault injection as means to execute attacker-controlled code.

4.1 Targeting the AMD-SP

For the attack scenarios presented in the previous section, the attacker needs to execute custom code on the AMD-SP, either to provide a custom SEV firmware, or to extract the endorsement keys. As described in Section 3, the AMD-SP loads an RSA public key, the ARK, from the SPI attached flash to validate the authenticity of subsequent loaded firmware components. If an attacker would be able to replace the original ARK, all firmware components would be validated using the attacker-controlled key, thereby enabling the attacker to execute code directly after the ROM bootloader stage.

To better understand the ARK verification, we analyzed the traffic on the Serial Peripheral Interface (SPI) bus during the boot process of an AMD Epyc CPU. We conducted two experiments: first we recorded the SPI traffic during a normal boot, i.e., a boot with the original flash content. The upper part of Figure 2 shows the activity on the chip select (CS) and MISO lines of the SPI bus for this first experiment.

In a second experiment, we flipped a single, non-functional bit of the ARK. While the flipped bit would still allow validating signatures, the hash comparison by the ROM bootloader would fail. The corresponding trace is shown in the lower part of Figure 2. The CS signal will be pulled low if the SPI master, in our case the AMD-SP, transmits data on the bus; otherwise the CS signal is high.

Our analysis revealed a small period of time after the ARK is loaded without SPI traffic. As we could not observe further SPI traffic when providing a manipulated ARK, we inferred that the AMD-SP validates the ARK's integrity during this window. Furthermore, we could observe that the amount CS line changes prior to this gap only depends on the ARK size.

We identified this time period as a promising window of opportunity to inject our fault due to the following reasons:

- Injecting a fault during the validation of the ARK potentially enables us to coerce the AMD-SP into accepting our own public key. By re-signing the flash image, we can manipulate all existing firmware components signed with that key.
- The ARK validation happens at an early stage in the AMD-SP's boot process. The fault injection might render the target system non-responsive which forces us to reset the target. By focusing on a very early security check we increase the number of glitches we can inject.
- According to our observation, the amount of SPI traffic prior to the ARK validation only depends on the size of the ARK. This enables us to leverage the SPI traffic as a trigger for our fault injection.

To inject a fault during the ARK validation, we chose a similar approach as presented by Chen et al. in their attack called *VoltPillager* [17]. We explain the similarities and differences to their approach in the following section.

4.2 Glitching the AMD-SP

To inject a fault, we leverage a CPU-external VR to manipulate the input voltage of AMD SoCs. The VR is an external controller that communicates via a dedicated bus, the SVI2 bus, with the AMD SoC to allow the SoC to dynamically change the input voltage, e.g., when CPU-frequency changes require a different input voltage. Our analysis of the AMD SVI2 bus revealed that the external VR not only controls the input voltage of the main x86 cores, but also the input voltage of the AMD-SP. Although the SVI2 protocol allows a single VR to handle both input voltages, we observed that AMD Epyc systems leverage two independent VRs to handle the input voltages. As described in Section 3.4, the AMD SoC uses two different voltage domains, Core and SoC. We verified that we can manipulate the AMD-SP's input voltage via the SoC voltage domain. Using a similar hardware setup as presented by Chen et al. [17], we injected our own packets into the SVI2 bus leveraging a *Teensy* μ Controller.

However, in contrast to the approach taken by Chen et al., where the authors target the protected entity, i.e., code executing in the SGX enclave, we target the AMD-SP. To overcome the protections imposed by SEV, targeting the AMD-SP instead of the SEV-protected VM has several benefits for the attacker:

- System stability - If our fault attack renders the target unusable, we can simply reset the target and try again as the

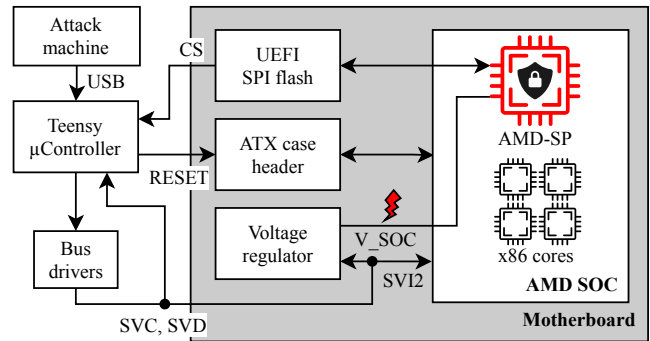


Figure 3: Schematic of the attack setup.

AMD-SP rom-bootloader will immediately execute once the SoC powers on. We don't need to fully instantiate the SEV-protected VM.

- Attack effectiveness - Once our fault injection is successful, the decryption of VM memory is 100% effective.
- Independence from target VM - Our approach works for all SEV-protected VMs, regardless of the type of operating system or application used inside the VM.
- Key extraction - Targeting the AMD-SP allows us to extract SEV-related secrets which can be used to target remote systems. For these systems, we don't require physical access.
- Automation of the attack - Once the target CPU is characterized, i.e., the glitching parameters are determined, subsequent attacks require no manual intervention.
- Blinded glitching - Our glitching attack solely relies on observing an *external* trigger, the chip select (CS) signal of the SPI bus. We don't require code execution on the target to determine our glitching parameters.

In the following section we present our experimental setup that allows us to inject faults into the AMD-SP's ROM bootloader.

5 GLITCH ATTACK

To overcome the boot protection mechanisms of the AMD-SP, we target the ROM bootloader's signature verification of the ARK with our glitching attack. Figure 3 depicts our glitching setup and the components involved. Inspired by the *VoltPillager* attack [17], we use a *Teensy* 4.0 μ Controller [40] for all communication with the low-level hardware and to run the time-critical attack logic. The *Teensy* is responsible for monitoring the chip select (CS) line of the target motherboard's SPI bus to identify the precise time to perform the glitch and whether a glitch was successful or not, see Section 4.1. In order to drop the voltage of the AMD-SP, the *Teensy* is connected to the SVI2 bus of the target. By injecting packets into this bus, the *Teensy* programs the VR to apply the corresponding voltage levels. For resetting the target SoC after a failed attack, the *Teensy* is connected to the ATX Reset line.

The *Teensy* is controlled from an attack machine via a serial-over-USB interface. This attack machine is responsible for selecting attack parameters and orchestrating the glitching attacks. We want to emphasize that the *Teensy* μ Controller is capable of performing the attack on its own with only minor firmware modifications.

Using the described setup, we were able to successfully execute custom payloads on the CPUs shown in Table 2. We used the *Supermicro H11DSU-iN* motherboard² for all targeted CPUs. In the following sections, we describe the required steps to mount our glitching attack.

CPU	μArchitecture	Previously Exploited
72F3	Milan (Zen 3)	No
7272	Rome (Zen 2)	No
7281	Napels (Zen 1)	Yes [15]

Table 2: AMD-SPs successfully attacked.

5.1 Payload Preparation

As a pre-requisite for our attack, we prepare the SPI flash image of the target so that our payload replaces the PSP OS component in the target's flash image, see Section 3.2. Then we replace the ARK with our own public key and re-sign the payload with this key. In case of a successful glitch, the AMD-SP accepts our public key and executes our payload instead of the original PSP OS component. As a proof-of-concept payload, we use a simple "Hello World" application, which outputs the string "Hello World" on the SPI bus. After the attack, we can verify that we gained code execution by reading "Hello World" from the SPI bus using a logic analyzer.

5.2 Attack Cycle

To coerce the AMD-SP into accepting our public key, we need to inject a fault during the hash verification of the ARK. The attack can be split into several steps, executed in a loop until a successful glitch was detected. For each targeted CPU, we first determine static glitch parameters: *delay* and *duration*. In Section 5.5, we explain our approach for identifying these parameters in detail.

Figure 4 depicts the output of the relevant signals of a successful glitch cycle. In each cycle, the following steps are executed:

- A1 The Teensy detects the SVI2 bus becoming active, starting the attack logic (5.3.2)
- A2 - A4 To avoid later SVI2 packet collisions, we inject two commands to disable the telemetry reports and set default voltages (5.3.3).
- B1 - B2 Using the number of CS pulses and the *delay* parameter we determined for the targeted CPU, we precisely trigger the voltage drop (5.4.1).
- B3 - B5 By injecting two SVI2 commands (B3 and B4), we cause the voltage drop. The lowest voltage (B5) is determined by the *duration* parameter (5.4).
- B6 - B7 We observe further SPI traffic to distinguish between successful and failed attack attempts (5.4.2).

After each failed attempt, we start the next one by resetting the AMD SoC using the ATX reset line (see Figure 3). Our attack cycle takes 3.14 (± 2 ms) seconds, which amounts to just above 1100 attempts per hour. This attack rate is limited by the ATX reset line timeout, which allows us to reset the AMD SoC only after around 3 seconds have passed since the last reset.

²Although the H11DSU-iN does not officially support the 72F3 CPU, we still could successfully boot the AMD-SP.

5.3 SVI2 Bus Injection

On all AMD CPUs that we tested, the AMD-SP is powered by the SoC voltage rail, which is controlled by a dedicated VR and a dedicated SVI2 bus on CPUs with an SP3 socket [53]. To inject packets onto this SVI2 bus, we soldered two wires to its SVC and SVD lines. While the bus is idle, both lines are permanently pulled to a logical high level by the CPU, which we use to inject packets by pulling the lines low. We used an 8-channel open-drain driver (the LVC07A [47]) for this task. Per bus line, we connected two channels of the driver in parallel to reliably achieve a logical low level accepted by the *IR35204* VR [27] present on our motherboard.

The driver's inputs are connected to one of the Teensy's I²C hardware interfaces and are pulled high with a 150 Ω resistor. Together with the Teensy's own open-drain drivers, this enables us to inject SVI2 commands at a baudrate of 4.6 Mbit/s. This is within the 0.1 to 21 Mbit/s range commonly supported by the VRs [26, 27, 44, 45], but faster than the 3.3 Mbit/s that we measured for our CPUs.

5.3.1 SVI2 Protocol. The SVI2 bus packet format is best described in [44] and [45]. An SVI2 command contains many configuration values, of which the following are of interest to us: The voltage domain selection bits, the voltage identification (VID) byte, the power state bits, and the telemetry function (TFN) bit. All other values have a "no change" setting, which we choose for every injected packet. Each SVI2-compliant VR can regulate two voltage rails. On motherboards with a single VR (e.g., with AM4 socket [52]), both the Core and SoC voltage rails (aka VDD and VDDNB, respectively) are regulated by that VR. The voltage domain selector bits are used to select which voltage rail is affected by an SVI2 packet. For Epyc CPUs, there is one voltage regulator for each voltage rail. Our experiments have shown that the Core (VDD) settings are used for both rails.

The VID byte sets the main parameter of the VR: the voltage of the selected voltage rail. As there is no "no change" VID, we must set a reasonable value every time we inject a command. The default values we use for the Core and SoC voltage rails are the first values we observed on the bus. The VRs use different power states for increased efficiency in low-power phases [26, 27, 44, 45]. We always choose the highest power state for our injections, as we noticed more significant voltage switching ripples in the lower power states, which cause our voltage faults to be less predictable.

5.3.2 Boot Detection. When the CPU starts its boot sequence (after a power on or a reset), there is a period when the VR is already providing power to the CPU, but is not controlled via the SVI2 bus [26, 27, 44, 45]. This period ends when the CPU signals the VR to use the SVI2 bus. For all CPUs that we tested, the SVD line are constantly pulled low when the SVI2 bus is inactive. However, when the SVI2 communication is activated, SVD transitions to a high state (A1 in Figure 4). When the SVI2 bus becomes deactivated again (e.g., when the SoC is reset), the SVD line constantly remains at a low level, which we use to arm our SVI2 startup detection again.

5.3.3 Avoiding Packet Collisions. Once the SVI2 bus is active, the CPU immediately sends two SVI2 commands, configuring defaults for the two voltage rails (A2 in Figure 4). No more commands are sent on the SVI2 bus until the ARK has been verified. Therefore,

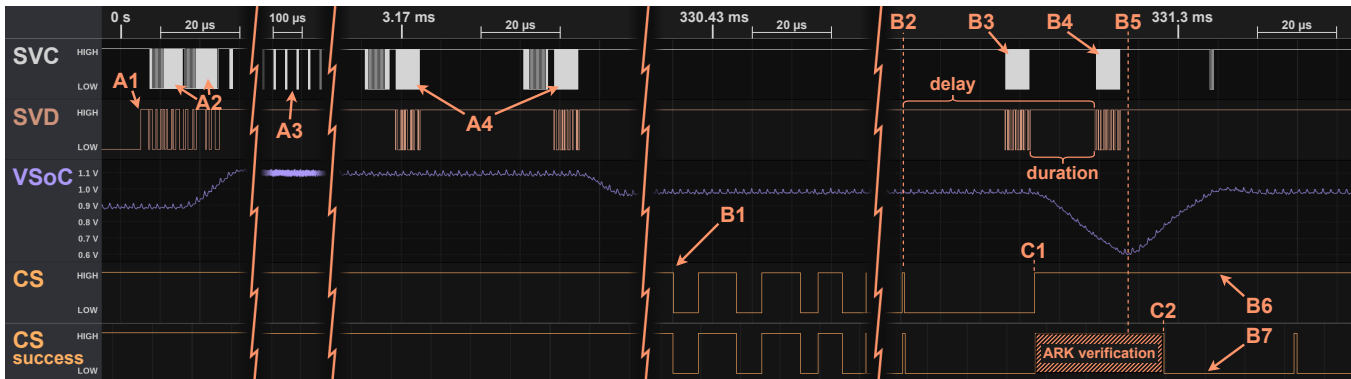


Figure 4: Logic traces of a complete Attack Cycle including CS traces of a successful and a failed attempt. The “A”-labels mark the SVI2 bus activation, periodic telemetry reports, and disabling the telemetry reports, as described in Section 5.3. Labels starting with “B” mark trigger events, the voltage drop injections, and the feedback mechanism described in Section 5.4. The CS edges marked with “C” are used to determine the initial window for the *delay* parameter.

we are not affected by interfering SVI2 commands from the CPU during the packet injection.

In contrast, the periodic telemetry reports sent from the VR to the CPU use the SVC line as a shared clock (A3 in Figure 4). This can cause packet collisions if left unattended. To avoid possible interference with our packet injection, we disable the telemetry reporting shortly after the SVI2 bus becomes active (A4 in Figure 4).

5.4 Voltage Drop

To lower the voltage level of the AMD-SP, we inject two commands into the SVI2 bus (B3 and B4 in Figure 4). First, we configure a low voltage identification (VID) setting, and secondly, we inject the same VID that was configured before the voltage drop (see 5.3.3). The voltage set by the first packet is too low for the AMD-SP to operate correctly and would cause non-recoverable errors, even if configured for only a short time. However, due to the limited voltage regulation speed of the VR, we inject the second command before the configured voltage is reached. This way, we can control the depth and shape of our voltage drop with only one parameter, the *duration*. Another advantage is that the voltage rail reaches its minimum for only a short moment, which we call the *fault time* (B5 in Figure 4). The *fault time* occurs directly after the second command injection, which allows us to trigger the fault injection precisely.

5.4.1 Trigger. As discussed in Section 4.1, counting the number of active low (negative) CS pulses allows us to determine the time window for the ARK verification. To more precisely control the *fault time* (B5 in Figure 4) within the ARK verification window, we use a *delay* parameter, which is the time between the last counted CS pulse and the *fault time*. Both timings are implemented on the Teensy μ Controller using a busy loop where one iteration corresponds to 12.5 ns. The complete trigger process proceeds as follows, see Figure 4:

- A1 Starting with the boot detection, we count the number of CS pulses.

- B1 The first CS pulse is counted.
- B2 After counting the last CS pulse³, we start the busy loop counter.
- B3 After (*delay* – *duration*) busy loop cycles we inject the first SVI2 command.
- B4 *Duration* many busy loop cycles later – exactly *delay* busy loop cycles after B2 – we inject the second SVI2 command.
- B5 The *fault time* is precisely determined by the CS pulse count and *delay*.

5.4.2 Fault Feedback. We can use the CS line to infer what effect our voltage drop had on the execution of the AMD-SP. Two different behaviors can be observed, see Figure 2:

- B6 No further accesses to the SPI flash occur.
- B7 The AMD-SP continues to load data from the SPI flash.

For our attack firmware image with an invalid ARK, B6 means that the attack failed. The reason is either that our key was correctly identified as invalid, or that we caused an unrecoverable fault in the ROM bootloader’s operation. In this case, the Teensy resets the target using the ATX reset line. Since the ROM bootloader only continues to load data from the SPI flash when the loaded key was accepted as valid, B7 means that our attack succeeded.

5.5 Determining the Attack Parameters

To successfully mount the glitching attack, we first need to determine the glitching parameters: The *delay*, responsible for the precise timing of our voltage drop, and the *duration*, which sets the depth of the voltage drop (see Figure 4). As a first step, we limit both parameters to windows containing all sensible values (Sections 5.5.1 and 5.5.2). This is done manually using the serial interface of the Teensy μ Controller, which took us around 30 minutes for each CPU. These windows are then searched and refined using automated attacks (see Section 5.5.3).

³To achieve a certain voltage drop depth within the ARK verification window, the first SVI2 command has to be issued before the last CS pulse (B3 Figure 4). In these cases we have to decrease the number of CS pulses that we count.

5.5.1 Delay Window. In the beginning, we limit the *delay* parameter such that the *fault time* always lies in the ARK verification window. This is done by measuring the CS line at *fault time* for varying *delay* parameters and firmware images. With the *duration* set to zero and an invalid ARK on the flash image, we can use the last CS pulse to determine the first *delay* value in the ARK verification window (C1 in Figure 4).

Then we flash the original firmware image to the SPI flash. Since this image’s ARK is valid, our attack attempts – with *duration* set to zero – will now always “succeed”. By again measuring the CS line at *fault time*, we now find the last *delay* inside the ARK verification window (C2 in Figure 4). According to our observation, the resulting *delay* window is about 2000 parameters wide.

5.5.2 Duration Window. As a next step, we want to limit the *duration* parameter, i.e., the voltage depth, so that we can search the resulting parameter space. To do this, we use the already flashed original firmware image and run our attack with varying *duration* parameters and a *delay* that is inside the window specified above. For shorter *durations*, our attacks will mostly “succeed”, but for longer *durations*, it will transition to mostly “failing” (see Figure 5). Using a binary search, we can identify the window of transition between these two extremes.

We expect to cause functional faults with *duration* parameters inside this transition window, which our experiments confirm, see Figure 5. This observation aligns with other works that analyze voltage faults on ARM processors with respect to the depth and length of a voltage drop [48].

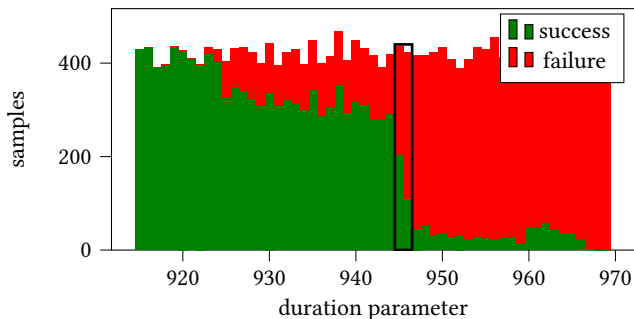


Figure 5: Attack samples for *duration* parameters in the transition window between always succeeding and always failing. The attacks target the original firmware image on the AMD Epyc 72F3 CPU. The final *duration* window is marked in black and contains the values deemed most likely to cause a fault by the refinement process.

5.5.3 Refining Parameters. To limit both parameters further, we repeatedly attempt our attack with randomly selected values from the two windows. On each CPU we tested, it took us less than 6 hours to archive a first successful attempt. The parameter space can now be limited further, e.g., to a window of ± 50 *delay* parameters and ± 10 *duration* parameters around the successful attempt’s values. With these smaller windows, we have an increased chance of achieving successes, which we use to limit the parameter space further.

	Total	72F3 (Zen 3)	7272 (Zen 2)	7281 (Zen 1)
Succ./Attempts		170/486695	17/15459	144/110382
Success Rate		0.035 %	0.11 %	0.130 %
Final Window				
Succ./Attempts		6/4653	6/3467	36/18309
Success Rate		0.129 %	0.173 %	0.197 %
Δ Delay/ Δ Dur.		4/2	14/3	20/10

Table 3: Attack results per CPU

5.5.4 Results. We summarize the overall results in Table 3, together with the final parameter windows we used. Our attack gains code execution reliably with an average waiting time between 13.5 min (Zen 1) and 46.5 min (Zen 3) for our final parameters. However, the calculated success rates cannot be translated into a reliable worst-case time-to-exploit metric since the successful attempts are not uniformly distributed over time.

5.6 Payloads

In this section, we present the attack payloads we executed leveraging the glitching of the AMD-SP’s ROM bootloader. We briefly describe our approach to re-enable the attacks presented in [15]. For further details regarding these attacks, we refer to the original paper.

Dumping the ROM bootloader and extracting secrets. To analyze the endorsement key derivation process, we build a payload that extracts the ROM bootloader and SRAM contents of all targeted CPUs. The payload writes the respective components to the SPI bus including the VCEK secrets. The CEK secrets were extracted from the crypto co-processor (CCP) using a similar payload.⁴ In Section 6, we use these secrets to derive the CEK and VCEK key of the exploited CPUs.

SEV Policy Override. In [15], the authors present attacks against SEV-protected VMs based on firmware issues present in the first generation of AMD Epyc CPUs, i.e., Zen 1 Naples. We successfully mounted these attacks on an AMD Epyc Zen 2 Rome system, running the latest SEV firmware available from [7]. Similarly to [15], we patched the SEV firmware to ignore the guest’s policy for the DBG_DECRYPT command. The target host was booted with a modified PSP OS firmware, which allowed us to update any SEV firmware signed with our own key.

AMD-SP Firmware Decryption. Our analysis of the AMD-SP’s firmware images for AMD Epyc Milan CPUs showed that firmware components, such as the PSP OS and the SEV firmware, are encrypted, see Section 3. In contrast to that, the analyzed AMD Epyc Rome and Naples images did not contain encrypted firmware images. For AMD Epyc Milan CPUs, we inferred the encryption mechanism by analyzing the ROM bootloader.

To detect whether a firmware component is encrypted, the ROM bootloader parses the header of the respective firmware component. If the component is encrypted, the ROM bootloader first loads an encrypted key from the SPI flash, the *IKEK*. The *IKEK* is decrypted

⁴There is no public documentation available for the CCP. However, its functionality is described in the corresponding Linux kernel driver: [32].

using a key present in a non-readable register of the CCP. The decrypted IKEK is then used to decrypt the component’s key, which is also part of its header. While we cannot access the IKEK decryption key directly, we were able to use the CCP to decrypt the IKEK, and with that, all encrypted components of the firmware image.

6 CEK & VCEK DERIVATION

Through the attacks presented in Section 5.6, we have access to the firmware components that implement the key derivation for SEV’s endorsement keys and the corresponding secrets. The CEK and VCEK are fundamental for the security properties of SEV (see Section 3.1.2). Both are derived from secret values burned into the fuses of the AMD SoC. Each AMD SoC has a unique 256-bit identifier (ID) that can be used to retrieve certificates for the CEK and VCEK keys from AMD [2, 4].

6.1 Key Derivation Algorithms

In this section we present our analysis of the derivation algorithms for the CEK and the VCEK.

6.1.1 CEK Derivation. The CEK is generated from a 32-byte secret. This secret is expanded to 56 pseudorandom bytes using NIST’s *Key Derivation Function in Counter Mode* (KDF), specified in [16], with HMAC-SHA256 as *Pseudorandom Function*. The KDFs inputs for the CEK derivation are an empty context, the label “sev-chip-endorsement-key” and, as key, the SHA256 digest of the secret. These 56 pseudorandom bytes can then be converted into an ECDSA key on the *secp384r1* curve [13]. The algorithm used for this is NIST’s *Key Pair Generation Using Extra Random Bits*, specified in [9].

6.1.2 ID Derivation. The ID of the AMD SoC is generated from the same secret as the CEK. This secret is interpreted as the private part of an ECDSA key on the elliptic curve *secp256k1*, specified in [13]. The public part of this key, encoded as the concatenation of its two 32-byte coordinates, is then used as the ID.

6.1.3 VCEK Derivation. To derive the VCEK, a 48-byte secret value is used. This secret is modified to incorporate the Trusted Computing Base (TCB) version string (see Section 3.1.3). The TCB version string consists of eight different one-byte security version numbers (SVNs), four of which are currently reserved (see Table 1). We use v_0, v_1, \dots, v_7 to denote these SVNs and sec_{255} to denote the initial secret. To incorporate v_0 into this secret, we use $255 - v_0$ successive SHA384 operations:

$$sec_{255} \xrightarrow{SHA384} sec_{254} \xrightarrow{SHA384} \dots \xrightarrow{SHA384} sec_{(v_0 + 1)} \xrightarrow{SHA384} sec_{v_0}$$

By prefixing sec_{v_0} with eight zero-bytes and applying SHA384 again, the algorithm “locks” the first SVN and prepares it for the incorporation of the next SVN:

$$sec_{v_0_255} := SHA384('\0\0\0\0\0\0\0\0' || sec_{v_0})$$

As suggested by this notation, we now apply $255 - v_1$ successive SHA384 operations to $sec_{v_0_255}$ to generate $sec_{v_0_v_1}$ and “lock” the second SVN using the prefix and SHA384 operation:

$$sec_{v_0_255} \xrightarrow{SHA384} sec_{v_0_254} \xrightarrow{SHA384} \dots \xrightarrow{SHA384} sec_{v_0_v_1}$$

$$sec_{v_0_v_1_255} := SHA384('\0\0\0\0\0\0\0\0' || sec_{v_0_v_1})$$

This process is continued with the remaining six SVNs, and we are left with the secret $sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7}$, which is hashed one more time with SHA384 to obtain the final secret

$$sec_final = SHA384(sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7})$$

$$(\ = sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7}) . \quad (1)$$

We then use sec_final to generate the VCEK similarly to how the CEK is derived from its secret. Using the label “sev-versioned-chip-endorsement-key” and the key sec_final as inputs to the same KDF as described in Section 6.1.1, we again derive 56 pseudorandom bytes, which are turned into an ECDSA key on the *secp384r1* curve using the same algorithm used in Section 6.1.1.

6.2 VCEK Design

The goal of the VCEK, as described in Section 3.1.3, requires that from a given secret (e.g. $sec_{(v_0 - 1)}$), we are not able to derive a secret for a higher SVN (e.g. sec_{v_0}). The cryptographic properties of SHA384 assure this, since SHA384 is practically infeasible to invert.

The SEV-SNP API allows TCB downgrades (see Section 3.1.3). If, for example, we want to downgrade sec_final ’s last SVN by one, we can apply one SHA384 operation to sec_final and generate the ECDSA key from the resulting secret. However, this mechanism can only be used to downgrade the last SVN. To allow downgrades of all SVNs, the SEV firmware has access to all of the secrets in (2).

$$sec_{(v_0 - 1)}$$

$$sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7}$$

$$sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7}$$

$$\dots$$

$$sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7} = sec_final \quad (2)$$

For example, to derive the VCEK for the TCB version string

$$(v_0, v_1 - 2, v'_2, \dots, v'_7),$$

we can apply one SHA384 operation to $sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7}$ and then continue the VCEK derivation algorithm with the SVNs v'_2, \dots, v'_7 . A potential issue is that we can choose values for v'_2, \dots, v'_7 , which are higher than the original values v_2, \dots, v_7 . We can, for example, derive the secret

$$sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7} \xrightarrow{SHA384} sec_{v_0_v_1_v_2_v_3_v_4_v_5_v_6_v_7} \quad (3)$$

which would result in a valid VCEK with the SVN 255 for both the SEV application and μ Code patch level. However, this does not constitute a security vulnerability as the downgraded SVN belongs to an insecure firmware component with a higher privilege level than the firmware components with upgraded SVNs. In the example above, the SVN $v_1 - 2$ refers to an insecure PSP OS firmware, whose security vulnerabilities could potentially be used to leak the secret (3).

6.3 Implementation on the AMD-SP

Both the ID and the CEK derivation algorithms described above are implemented by the SEV application. Their shared secret value is derived by the ROM bootloader, which passes the secret to the PSP OS in a readable buffer of the CCP. The SEV application can then access the secret through the syscall interface of the PSP OS.

The SEV application is also responsible for deriving the VCEK, but the secrets derivation algorithm is split up between ROM boot-loader, the PSP OS, and the SEV application. The ROM boot-loader derives the initial VCEK secret sec_255 from the fuses of the AMD-SP. The first SVN, i.e., the SVN labeled `BOOT_LOADER` in Table 1, is part of the header of the PSP OS binary on the SPI flash. The ROM boot-loader uses this first SVN v_0 to derive the secrets:

$$sec_v_0_255 \quad \text{and} \quad sec_v_0 - 1 . \quad (4)$$

Once it has verified the PSP OS signature (the header is included in this signature), both secrets (4) are passed onto the PSP OS.

According to the SEV-SNP API specifications [8], the second SVN corresponds to the “trusted execution environment.” In the firmware image we analyzed, the PSP OS binary was responsible for the boot process and acted as an operating system running on the AMD-SP. As a result, this second SVN and the next four “reserved” SVNs are set to zero by the PSP OS. Every time a SEV application is loaded, its SVN, v_6 , and the hardcoded SVNs, v_1 to v_5 , are used to derive all the first seven secrets of (2) and

$$sec_v_0 \dots v_6_255 .$$

These secrets are then passed to the SEV application, which incorporates the last SVN – the μ Code patch level.

6.4 CEK/VCEK Derivation and Fault Attacks

With the glitching attack presented in Section 5, an attacker can not only execute an arbitrary PSP OS firmware component, but also, choose an arbitrary SVN for its header. By creating a payload with the highest possible SVN, 255, the attacker forces the ROM boot-loader to derive the secrets

$$sec_255_255 \quad \text{and} \quad sec_254 .$$

We extracted these secrets, together with the CEK secret, using payloads described in Section 5.6. With these secrets and the algorithms described in Section 6.1, we were able to derive the CEKs and IDs for all our target CPUs, as well as the VCEKs of our Milan (Zen 3) CPU for all possible TCB component versions.

7 DISCUSSION

In this section we evaluate the feasibility and impact of our attack, and propose potential mitigations.

7.1 Attack Evaluation

To evaluate the real-world applicability of our attack, we compare an attacker’s capabilities with the attack requirements. We focus on attack scenarios relevant in cloud environments, as presented in Section 4.

For the “Debug Override” attack, the attacker first replaces the original SEV firmware with a custom firmware and re-signs the firmware image, see Section 5.6. To mount the glitching attack described in the previous sections, the attacker then prepares the target host as described in Section 5. As the Teensy μ Controller is small enough to fit into a standard server enclosure, the physical setup introduces no additional requirements regarding the installation into the datacenter. This initial preparation, including the

determination of the glitching parameters, does not pose a serious challenge for the attacker. We were able to prepare our target system for attacking the Epyc 72F3 in under four hours.

The attacker will then boot the target system, and the μ Controller will perform the actual glitching via the SVI2 packet injection. The μ Controller will automatically reset the target if the glitch attempt failed, leading to an increased boot time of the target. Once the target is fully booted, the attacker can leverage SEV’s debug API to decrypt a VM’s memory. As described in Section 5, a attack machine is required to control the μ Controller. While in a cloud scenario, a neighboring host could be used to control the μ Controller. However, with minor firmware modifications, the Teensy μ Controller would be capable of automatically performing the glitching attack on its own. As the manipulation of the SEV firmware image does not change a VM’s measurement, the validation of attestation reports will succeed even though the target host does not execute a genuine AMD SEV firmware.

For the second scenario, instead of preparing a system to host the targeted VMs, the attacker prepares and then extracts the endorsement key of an arbitrary SEV capable CPU. The endorsement key is then used to fake attestation reports. In the case of SEV-SNP, the faked attestation report allows an attacker to migrate the victim VM to a host with a malicious MA, see Section 3.1.4. Using the exported Offline Encryption Key (OEK), the malicious MA can decrypt the victim’s memory pages. For pre-SEV-SNP targets, the extracted endorsement key allows to mount the migration attack as described in [15]. Compared to the first scenario, this approach relaxes the requirements for the attacker as the glitching attack can be performed in a controlled environment, and the extracted keys can then be used to target remote systems.

Either attack scenario poses a threat for SEV-protected VMs, as they can be carried out by insider attackers such as system administrators and require only cheap and easily available hardware.

7.2 Potential Mitigations

We see two different strategies that can be pursued to mitigate our attack. On the one hand, one could try to prevent the adversary from achieving code execution (Section 7.2.1). On the other hand, one could try to protect the architecture keys from being extracted, even if the adversary manages to achieve code execution (Section 7.2.2).

7.2.1 Prevent adversarial code execution. The threat of fault injection for gaining adversarial code execution can be tackled from different directions. One could try to detect malicious voltage drops/glitches, and as a consequence, shut down the system to prevent further damage. Alternatively, one could try to prevent faulty execution in the presence of glitches, for instance, by introducing redundancy. Both approaches might imply the need for changes in the hardware or software design.

Hardware-based detection/prevention. Voltage monitoring circuits – as commonly implemented in modern smartcards – could help to detect glitches. A recent patent by NVIDIA [43] proposes a cross-domain voltage glitch detection circuit, which can be implemented into a SoC. The main idea is that circuits in different independent voltage domains monitor the voltage levels in the other domains, and if there is a glitch on a specific rail, an alert signal is asserted.

In our opinion, this is a promising approach. However, it should be kept in mind that there might exist voltage glitch shapes that can cause faulty behavior but can not be detected by a particular protection circuit.

We share the opinion with the authors of the *VoltPillager* attack [17] that voltage glitching can not be prevented by protecting the VR bus/protocol through cryptographic authentication. Furthermore, although the VR bus is an easy access point for injecting voltage glitches, the adversary could also inject glitches by other means, e.g., by altering the PWM signal output of the VR or entirely replacing the VR with a custom injection setup.

One might think that fully integrating the VR into the SoC could be the ultimate solution. However, faults can not only be induced by glitching the supply voltage. In the past couple of years, electromagnetic (EM) fault injection techniques against modern CPUs have been examined to inject faults in a more targeted and contactless way [49, 50]. Consequently, a holistic view is necessary to prevent all kinds of fault injection techniques that can lead to code execution on the target device.

Software-based detection/prevention. Hardening the ROM bootloader might be another option to prevent the adversary from gaining code execution. However, this is a complex task since the characteristics and potentials of faults are not well understood. Particularly, there is no model which covers all possible faults.

Though, there are generic countermeasures that can decrease the probability of successful attacks [10, 55]. For instance, constants with large hamming distance make it hard to flip one valid value to another, double checks protect branch conditions, loop integrity checks make sure that the loop exits as intended, and a global counter can be used to monitor the program flow and detect anomalies. For assessing software countermeasures against fault attacks, different simulation-based frameworks have been proposed [25, 46]. In our opinion, the general approach of software-based mitigations is promising because they can protect not only against fault attacks by voltage glitching. Nevertheless, these countermeasures come at the cost of some overhead in execution time, and therefore, performance reduction.

7.2.2 Prevent key extraction. One of the key insights from [15] is that the CEK should depend on TCB components versions. In this case, CEKs extracted using firmware issues are no longer valid after the firmware has been updated. With SEV-SNP, a similar model has been adopted by AMD in the form of the VCEK.

The VCEK is derived from a secrets that depend on TCB component versions. However, as we have shown in this work, this dependency still allows an attacker to extract valid VCEKs for all possible TCB versions. Although the VCEK is bound to firmware versions, it does *not* depend on the *functionality* of the respective firmware component. The dependency between the firmware version, represented by a field in a component’s header, and the its functionality is only implicit. Components, including their firmware version field in the header, are signed by the ARK. A valid signature links the component to its firmware version in the signed header.

To increase the security properties of the VCEK key derivation, we propose to include a hash – instead of the firmware version – of the respective TCB component in the secrets, similar to the DICE model proposed by the Trusted Computing Group [23]. Including

the hash binds a secret to the component’s functionality. Using a key-derivation function, the ROM bootloader binds the *sec_255* secret to the hash of the PSP OS, see Section 6.3.

In this model, if an attacker could get code execution on the AMD-SP, the secrets that could be extracted are useless as they depend on the attacker’s payload.

While this model presents a security improvement compared to the current version of the derivation model, it also has practical drawbacks: any *functional* update of a component, i.e., a non-security-related change, still results in a new VCEK. In addition to this, this model prevents TCB rollback of endorsement keys as currently supported by SEV-SNP. Without knowing the specific requirements of the AMD-SP’s firmware components, it is impossible to fully evaluate the applicability of the proposed model. Nevertheless, from a pure security perspective, we believe including the hash within the intermediate secrets provides a strengthened security model.

8 CONCLUSION

The attacks presented in this paper highlight SEV’s insufficient protection against physical attacks. Despite its crucial role for SEV’s security properties, the AMD-SP can be tricked into executing attacker-controlled code. The hardware setup to mount the presented glitching attack is cheap and readily available. Building on this setup, we presented how an adversary with physical access to the target host can implant a custom SEV firmware that decrypts a VM’s memory using SEV’s debug API calls.

Furthermore, we showed that the glitching attack enables the extraction of endorsement keys. The endorsement keys play a central role in the remote attestation mechanism of SEV and can be used to mount remote attacks. Even an attacker without physical access to the target host can use extracted endorsement keys to attack SEV-protected VMs. By faking attestation reports, an attacker can pose as a valid target for VM migration to gain access to a VM’s data.

Our analysis revealed that the TCB versioning scheme introduced with SEV-SNP does not protect against the presented attacks. Based on our results, we conclude that SEV cannot adequately protect confidential data in cloud environments from insider attackers, such as rogue administrators. The presented attacks do not rely on firmware issues and can not be easily mitigated. Hence, we proposed mitigations for future AMD Epyc CPUs. Nevertheless, to the best of our knowledge, all currently available CPUs that support SEV are susceptible to the presented attacks.

REFERENCES

- [1] Advanced Micro Devices, Inc. 2018. *Understanding Power Management and Processor Performance Determinism*. Retrieved 2021-04-06 from <https://www.amd.com/system/files/documents/understanding-power-management.pdf>
- [2] Advanced Micro Devices, Inc. 2020. *AMD Secure Encrypted Virtualization API Version 0.24*. Retrieved 2021-03-26 from https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf
- [3] Advanced Micro Devices, Inc. 2020. *AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More*. Retrieved 2021-04-07 from <https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf>
- [4] Advanced Micro Devices, Inc. 2021. *AMD CEK Certificate Server*. Retrieved 2021-04-16 from <https://kdsintf.amd.com/cek/>
- [5] Advanced Micro Devices, Inc. 2021. *AMD Milan Root Key*. Retrieved 2021-04-16 from https://developer.amd.com/wp-content/resources/ask_ark_milan.cert

- [6] Advanced Micro Devices, Inc. 2021. *AMD VCEK Certificate Server*. Retrieved 2021-04-16 from <https://kdsintf.amd.com/vcek/>
- [7] Advanced Micro Devices, Inc. 2021. *SEV firmware for ROME*. Retrieved 2021-04-16 from https://developer.amd.com/wordpress/media/2013/12/amd_sev_fam17h_model3xh_0_24b0A.tar.gz
- [8] Advanced Micro Devices, Inc. 2021. *SEV Secure Nested Paging - Firmware ABI Specification Revision 0.9*. Retrieved 2021-05-03 from <https://www.amd.com/system/files/TechDocs/56860.pdf>
- [9] National Institute of Standards and Technology. 2013. *Digital Signature Standard (DSS)*. <https://doi.org/10.6028/NIST.FIPS.186-4>
- [10] Tamas Ban. 2020. *Arm Ltd.: Trusted Firmware M*. Retrieved 2021-04-25 from https://www.trustedfirmware.org/docs/TF-M_fault_injection_mitigation.pdf
- [11] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. 2006. The Sorcerer's Apprentice Guide to Fault Attacks. *Proc. IEEE* 94, 2 (Feb. 2006), 370–382. <https://doi.org/10.1109/JPROC.2005.862424>
- [12] Jeremy Boone. 2020. There's A Hole In Your SoC: Glitching The MediaTek BootROM. <https://research.nccgroup.com/2020/10/15/theres-a-hole-in-your-soc-glitching-the-mediatek-bootrom/>
- [13] Daniel R. L. Brown. 2010. *SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0*. <https://www.secg.org/sec2-v2.pdf>
- [14] Robert Bühren, Alexander Eichner, and Christian Werling. 2019. *Uncover, Understand, Own - Regaining Control Over Your AMD CPU*. Retrieved 2021-01-14 from https://media.ccc.de/v/36c3-10942-uncover_understand_own_-_regaining_control_over_your_amd_cpu
- [15] Robert Bühren, Christian Werling, and Jean-Pierre Seifert. 2019. Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (London, United Kingdom) (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 1087–1099. <https://doi.org/10.1145/3319535.3354216>
- [16] Lily Chen. 2009. *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*. <https://doi.org/10.6028/NIST.SP.800-108>
- [17] Zitai Chen, Georgios Vasilakis, Kit Murdock, Edward Dean, David Oswald, and Flavio D. Garcia. 2021. VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Vancouver, B.C. <https://www.usenix.org/conference/usenixsecurity21/presentation/chen-zitai>
- [18] The MITRE Corporation. 2019. *CVE-2019-9836*. Retrieved 2021-04-19 from <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9836>
- [19] A. Djellid-Ouar, G. Cathebras, and F. Bancel. 2006. Supply Voltage Glitches Effects on CMOS Circuits. In *International Conference on Design and Test of Integrated Systems in Nanoscale Technology, 2006. DTIS 2006*. IEEE, Tunis, Tunisia, 257–261. <https://doi.org/10.1109/DTIS.2006.1708651>
- [20] Zhao-Hui Du, Zhiwei Ying, Zhenke Ma, Yufei Mai, Phoebe Wang, Jesse Liu, and Jesse Fang. 2017. Secure Encrypted Virtualization is Unsecure. (2017). arXiv:1712.05090
- [21] Andreas Galauner. 2018. *Glitching the Switch*. Retrieved 2021-03-15 from <https://media.ccc.de/v/c4.openchaos.2018.06.glitching-the-switch>
- [22] Gianluca Pacchiola. 2021. *Gipi/Low-Level: Hardware | Glitching*. Retrieved 2021-04-14 from <https://github.com/gipi/low-level/blob/master/docs/security/hardware.md#glitching>
- [23] Trusted Computing Group. 2021. *TCG Trusted Platform Architecture Hardware Requirements for a Device Identifier Composition Engine*. Retrieved 2021-05-04 from https://www.trustedcomputinggroup.org/wp-content/uploads/Device-Identifier-Composition-Engine-Rev69_Public-Review.pdf
- [24] Felicitas Hetzelt and Robert Bühren. 2017. Security Analysis of Encrypted Virtual Machines. In *Proceedings of the 13th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (Xi'an, China) (VEE '17)*. ACM, New York, NY, USA, 129–142. <https://doi.org/10.1145/3050748.3050763>
- [25] Andrea Höller, Armin Krieg, Tobias Rauter, Johannes Iber, and Christian Kreiner. 2015. QEMU-Based Fault Injection for a System-Level Analysis of Software Countermeasures Against Fault Attacks. In *2015 Euromicro Conference on Digital System Design*. 530–533. <https://doi.org/10.1109/DSD.2015.79>
- [26] International Rectifier. 2015. *IR35201 8+0/7+1/6+2 Dual Output Digital Multi-Phase Controller*. Retrieved 2021-04-19 from https://www.infineon.com/dgdl/Infineon-IR35201MTRPBF-DS-v01_00-EN.pdf?fileId=5546d462576f347501579c95d19772b5
- [27] International Rectifier. 2016. *IR35204 3+1 Dual Output Digital Multi-Phase Controller*. Retrieved 2021-04-19 from https://www.infineon.com/dgdl/Infineon-IR35204MTRPBF-DS-v01_00-EN.pdf?fileId=5546d462576f347501579c95e21172b9
- [28] David Kaplan. 2017. *Protecting VM Register State with SEV-ES*. Retrieved 2021-04-07 from <https://www.amd.com/system/files/TechDocs/Protecting%20VM%20Register%20State%20with%20SEV-ES.pdf>
- [29] David Kaplan, Jeremy Powell, and Tom Woller. 2016. *AMD Memory Encryption*. Retrieved 2021-04-07 from https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf
- [30] Zijo Kenjar, Tommaso Frassetto, David Gens, Michael Franz, and Ahmad-Reza Sadeghi. 2020. VOLTpwn: Attacking X86 Processor Integrity from Software. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 1445–1461.
- [31] Roger Lai. 2013. *AMD Security and Server innovation*. Retrieved 2021-03-26 from https://uefi.org/sites/default/files/resources/UEFI_PlugFest_AMD_Security_and_Server_innovation_AMD_March_2013.pdf
- [32] Thomas Lendacky and Gary Hook. 2021. *CCP Linux kernel driver*. Retrieved 2021-05-04 from <https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/tree/drivers/crypto/ccp/>
- [33] Mengyuan Li, Yinqian Zhang, Zhiqiang Lin, and Yan Solihin. 2019. Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 1257–1272. <https://www.usenix.org/conference/usenixsecurity19/presentation/li-mengyuan>
- [34] Yifan Lu. 2019. Injecting Software Vulnerabilities with Voltage Glitching. (Feb. 2019). arXiv:1903.08102 [cs]
- [35] Akash Malhotra. 2020. *Full-stack, Multilayered Security Features for a Changing World*. Retrieved 2021-03-26 from <https://www.amd.com/system/files/documents/ryzen-pro-article-multilayered-security-features.pdf>
- [36] Mathias Morbitzer, Manuel Huber, and Julian Horsch. 2019. Extracting Secrets from Encrypted Virtual Machines. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19)*. Association for Computing Machinery, New York, NY, USA, 221–230. <https://doi.org/10.1145/3292006.3300022>
- [37] Mathias Morbitzer, Manuel Huber, Julian Horsch, and Sascha Wessel. 2018. SEVered: Subverting AMD's Virtual Machine Encryption. In *Proceedings of the 11th European Workshop on Systems Security (Porto, Portugal) (EuroSec'18)*. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3193111.3193112>
- [38] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, F. Piessens, and D. Gruss. 2020. Plundervolt: How a Little Bit of Undervolting Can Create a Lot of Trouble. *IEEE Security Privacy* 18, 5 (Sept. 2020), 28–37. <https://doi.org/10.1109/MSEC.2020.2990495>
- [39] Colin O'Flynn. 2016. Fault Injection Using Crowbars on Embedded Systems. *IACR Cryptol. ePrint Arch.* (2016). <https://eprint.iacr.org/2016/810>
- [40] PJRC. 2021. *Teensy® 4.0 Development Board*. Retrieved 2021-04-01 from <https://www.pjrc.com/store/teensy40.html>
- [41] P. Qiu, D. Wang, Y. Lyu, R. Tian, C. Wang, and G. Qu. 2020. VoltJockey: A New Dynamic Voltage Scaling Based Fault Injection Attack on Intel SGX. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2020), 1–1. <https://doi.org/10.1109/TCAD.2020.3024853>
- [42] Martin Radev and Mathias Morbitzer. 2020. Exploiting Interfaces of Secure Encrypted Virtual Machines. (Oct. 2020). arXiv:2010.07094 [cs]
- [43] Kedar Rajpathak and Tejaswi Raja. 2020. *Cross-Domain Voltage Glitch Detection Circuit for Enhancing Chip Security*. Retrieved 2021-03-11 from <https://patents.google.com/patent/US20200285780A1/en>
- [44] Renesas Electronics Corporation. 2020. *ISL62776 Multiphase PWM Regulator for AMD CPUs Using SVI2*. Retrieved 2021-04-19 from <https://www.renesas.com/us/en/document/dst/isl62776-datasheet>
- [45] Richtek Technology Corporation. 2019. *Dual-Output PWM Controller for AMD SVI2 CPU Power Supply*. Retrieved 2021-04-19 from https://www.richtek.com/assets/product_file/RT3667BT/DS3667BT-00.pdf
- [46] Horst Schirmeier, Martin Hoffmann, Christian Dietrich, Michael Lenz, Daniel Lohmann, and Olaf Spinczyk. 2015. FAIL*: An Open and Versatile Fault-Injection Framework for the Assessment of Software-Implemented Hardware Fault Tolerance. In *2015 11th European Dependable Computing Conference (EDCC)*. IEEE, Paris, France, 245–255. <https://doi.org/10.1109/EDCC.2015.28>
- [47] Texas Instruments. 2016. *SN74LVC07A Hex Buffer and Driver with Open-Drain Outputs*. Retrieved 2021-04-19 from <https://www.ti.com/lit/ds/symlink/sn74lvc07a.pdf>
- [48] N. Timmers, A. Spruyt, and M. Witteman. 2016. Controlling PC on ARM Using Fault Injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. 25–35. <https://doi.org/10.1109/FDTC.2016.18>
- [49] Thomas Troughkine, Guillaume Bouffard, and Jessy Clédière. 2020. Fault Injection Characterization on Modern CPUs. In *Information Security Theory and Practice (Lecture Notes in Computer Science)*. Springer International Publishing, Cham, 123–138. https://doi.org/10.1007/978-3-030-41702-4_8
- [50] Thomas Troughkine, Sébanjila Kevin Bukasa, Mathieu Escouteloup, Ronan Lashermes, and Guillaume Bouffard. 2021. Electromagnetic Fault Injection against a Complex CPU, toward New Micro-Architectural Fault Models. *Journal of Cryptographic Engineering* (March 2021). <https://doi.org/10.1007/s13389-021-00259-6>
- [51] Jan Werner, Joshua Mason, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. 2019. The SEVerEst Of Them All: Inference Attacks Against Secure Virtual Enclaves. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19)*. Association for Computing Machinery, New York, NY, USA, 73–85. <https://doi.org/10.1145/3321705.3329820>
- [52] WikiChip. 2020. *Socket AM4 - Packages - AMD*. Retrieved 2021-04-01 from https://en.wikichip.org/wiki/amd/packages/socket_am4#Pin_Map
- [53] WikiChip. 2020. *Socket SP3 - Packages - AMD*. Retrieved 2021-04-01 from https://en.wikichip.org/wiki/amd/packages/socket_sp3#Pin_Map

- [54] Luca Wilke, Jan Wichelmann, Mathias Morbitzer, and Thomas Eisenbarth. 2020. SEVurity: No Security Without Integrity – Breaking Integrity-Free Memory Encryption with Minimal Assumptions. *2020 IEEE Symposium on Security and Privacy (SP)* (May 2020), 1483–1496. <https://doi.org/10.1109/SP40000.2020.00080>
- [55] Marc Witteman. 2018. *Riscure: Secure Application Programming in the Presence of Side Channel Attacks*. Retrieved 2021-04-18 from https://www.riscure.com/uploads/2018/11/201708_Riscure_Whitepaper_Side_Channel_Patterns.pdf