AMD RYZEN™ PRO 5000 SERIES MOBILE PROCESSORS MAKING DEFENSES COUNT: DESIGNING FOR SUBSTANTIAL DEPTH

By: Akash Malhotra
Product Security and Strategy Group

As risks accelerate in volume and variety, AMD continues to believe that meaningful protection for today's PCs requires a carefully layered approach that relies on best-in-class security controls and capabilities embedded directly into hardware, software, and firmware. This is especially true for a more mobile, "new normal."

AMD works closely with operating systems (OS) and original equipment manufacturers (OEMs) to provide hardware security features that complement and strengthen their own security design.

This paper highlights AMD Ryzen™ PRO 5000 series mobile processors' security features and the part they play in a multilayered approach to device security.

EVERYTHING BUILT WITH SECURITY IN MIND

AMD "Zen"-based core architectures provide a strong security foundation. AMD's security architecture helps to reduce exposure of attacks, can reduce downtime, may require fewer patches, and can help to improve the total cost of ownership.

AN INTEGRATED HARDWARE ROOT OF TRUST

AMD keeps improving its silicon architecture with each generation, helping to improve effectiveness against future cyberattacks.

INTEGRATED SECURITY FEATURES, FROM FIRMWARE TO OS

Once the initial firmware and OEM BIOS are authenticated, control passes to the OS through a secure-boot process that continues the chain of trust using Root of Trust, anchored in the hardware.

BETTER MEMORY PROTECTION: AMD MEMORY GUARD

AMD Ryzen™ PRO series mobile processors were the first commercial processors on the market to provide technology that helps protect user data by encrypting the complete system memory contents as a standard feature.

THE AMD RYZEN™ PRO 5000 SERIES MOBILE PROCESSORS' SECURITY ARCHITECTURE

We'll now look at some of the key processor-level features the AMD Ryzen™ PRO 5000 series mobile processors bring to the product—and more importantly, the end-user experience.

AMD SECURE PROCESSOR (ASP)

The AMD Secure Processor is dedicated hardware available in each system-on-a-chip (SoC), designed to anchor a hardware root of trust. It will also help boot and initialize the SoC through a secure boot flow and establish an isolated Trusted Execution Environment. Even though it is part of the silicon, it is considered isolated, as the host SoC cannot access its memory. The ASP is foundational to platform security, with the following components:

Cryptographic Co-processor (CCP): A dedicated crypto block which provides cryptographic functionality for key generation and key management. Since cryptographic operations are implemented in hardware, it provides a performance benefit that is critical for time-sensitive operations.

Boot ROM: A read-only memory which holds the on-chip boot ROM firmware

Static Random-Access Memory (SRAM): RAM with deep sleep power mode support

Memory Management Unit (MMU): ASP MMU manages access to boot ROM and SRAM

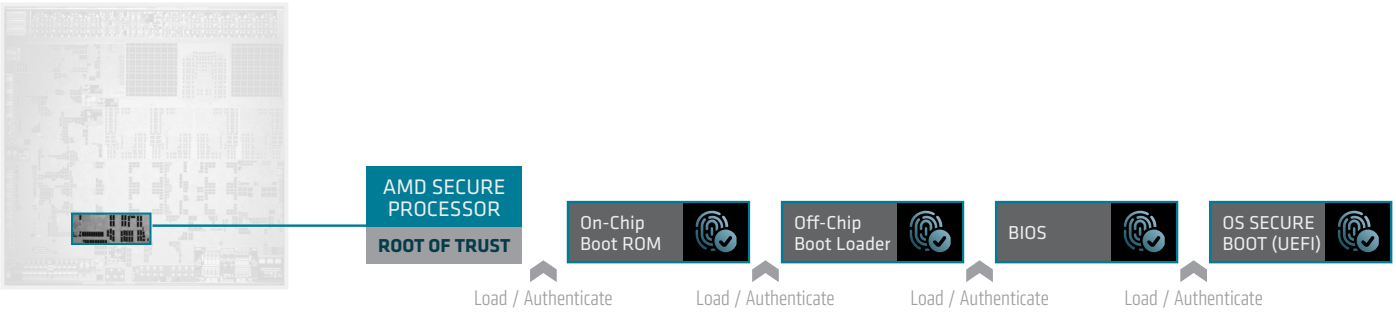
AMD PLATFORM SECURE BOOT (PSB)

AMD Platform Secure Boot (PSB) provides a hardware root of trust (RoT) to authenticate the initial firmware including BIOS during boot process of the device. When a system powers on, ASP executes the ASP boot ROM code, which then authenticates various ASP boot loader code before initializing silicon and system memory.

Once system memory is initialized, ASP boot loader code verifies the OEM BIOS code, authenticating other firmware components before the OS is booted.

PSB enforces platform integrity by providing stronger protection from rogue or malicious firmware, automatically denying them access upon detection. AMD PSB helps provide seamless and secure transition from low-level firmware to OS.

AMD Platform Secure Boot *Figure 1*



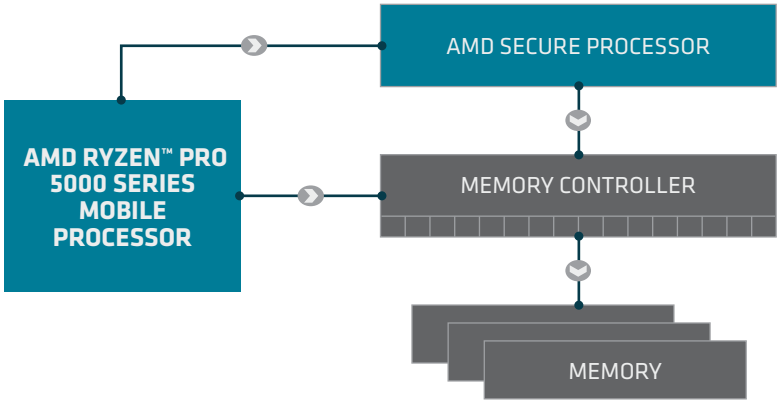
AMD MEMORY GUARD

AMD Memory Guard is a full memory encryption technology that offers a simple yet compelling security solution to help protect customer data, especially when physical attacks on the system are a concern. With AMD Memory Guard, all DRAM contents are encrypted utilizing a random key, which helps provide protection against physical cold boot, DRAM interface snooping, and similar types of attacks.

For systems with NVDIMM, AMD Memory Guard also helps provide protection against an attacker removing a memory module and attempting to extract its contents, implemented via dedicated hardware in the on-die memory controllers.

- Each controller includes a high-performance Advanced Encryption Standard (AES) engine that encrypts data when it is written to DRAM, and decrypts it when read.
- A 128-bit key is generated by an on-die NIST SP 800-90 compliant hardware random number generator in a mode which utilizes an additional physical-address-based tweak to help protect against cipher-text block move attacks.
- The encryption key used by the AES engine with AMD Memory Guard is randomly generated on each system reset and is not visible to any software running on the CPU cores. This key is managed entirely by the AMD Secure Processor (ASP).

AMD Memory Guard *Figure 2*



AMD SHADOW STACK

Attackers are busy trying to find innovative ways to break into systems while remaining undetected longer, and Return-on-Programming (ROP) is increasingly popular. ROP is a sophisticated class of software attacks where attackers don't inject their own malicious code into a process, but instead try to gain control of the system by exploiting weakness in the legitimate code.

HOW DOES THIS WORK?

In computer programming, a "routine" performs a particular set of operations. When a software program executes, it calls a routine. When that routine finishes its job, it returns to the main program using the return address. This process is called "jump and return."

In ROP attacks, attackers modify the jump routine return address. So instead of going back to the main program, it jumps around to different routines, stitching together routine sub-codes to create malicious code which can now harm the system. Most importantly, this type of attacks goes undetected, as it looks like legitimate code.

AMD Ryzen™ PRO 5000 series mobile processors help mitigate ROP attacks by providing software access to special registers in the CPU where a copy of the return address can be stored.

Applications can utilize a parallel stack, known as the "shadow stack," to help mitigate software attacks that attempt to modify the control flow. Utilizing special hardware, the shadow stack is used to store a copy of return addresses, which is checked against the normal program stack on return operations.

If the content differs, an exception is generated which can help prevent malicious code from gaining control of the system. In this way, shadow stack hardware can help mitigate some of the most common and exploitable types of software bugs.

AMD Shadow Stack adds robustness against ROP attacks; because a copy of the return address is in the hardware, it is very difficult for malicious code to tamper with.

Microsoft Hardware Enforced Stack Protection is supported on AMD Ryzen™ PRO 5000 series mobile processors using AMD Shadow Stack.

MICROSOFT SECURED-CORE PC

Microsoft Secured-Core PC helps protect your device from firmware vulnerabilities, shields the operating system from attacks, and can prevent unauthorized access to devices and data through advanced access controls and authentication systems.

Secured-Core PC is enabled on AMD platforms using various security technologies and services:

- AMD-V™ with GMET
- AMD Secure Init and Jump with Attestation (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- AMD System Management Mode (SMM) Supervisor
- Direct Memory Access (DMA) Protection

AMD-V WITH GMET

AMD-V is a set of hardware extensions that enable virtualization on AMD platforms. Guest Mode Execute Trap (GMET) is a silicon performance acceleration feature which enables the hypervisor to efficiently handle code integrity checks and help protect against malware.

SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

The SKINIT instruction helps create a "root of trust" starting with an initially untrusted operating mode. SKINIT reinitializes the processor to establish a secure execution environment for a software component called the secure loader (SL) and starts execution of the SL to help prevent tampering. SKINIT extends the hardware-based root of trust to the secure loader.

AMD SECURE LOADER (SL)

The AMD Secure Loader is responsible for validating the platform configuration by interrogating the hardware and requesting configuration information from the DRTM service provided by AMD Secure Processor.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

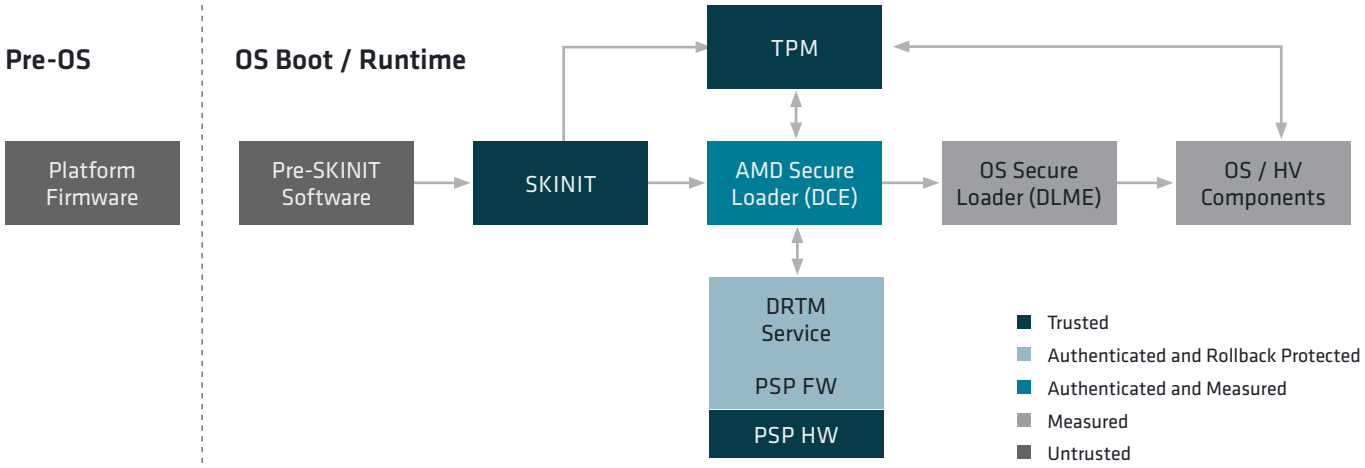
AMD DRTM block is made up of SKINIT CPU instruction, ASP, and the SL. This block is responsible for creating and maintaining a chain of trust between firmware. AMD DRTM works on the concept that the firmware and boot loader can load freely with the assumption that they are unprotected code and knowing that shortly after launch the system will transition into a trusted state with the hardware forcing low-level firmware down a well-known and measured code path.

DRTM block measures and authenticates the bootloader and also gathers and stores the following system information in a protected manner for further use by the OS, including verification and attestation.

- Physical memory map
- PCI configuration space location
- Local APIC configuration
- I/O APIC configuration
- IOMMU configuration / TMR configuration
- Power management configuration

DRTM Flow

Figure 3



At any point after the system has booted into OS, the operating system can request AMD service block to remeasure and attest the values before executing further operations. Thus the OS can help protect integrity of the system from boot to run time.

SHARED HARDWARE CONFIDENCE

This means that the firmware component is authenticated and measured by the ASP block on AMD silicon, and the measurement is stored in a protected manner for further use by the OS, including verification and attestation.

AMD SMM SUPERVISOR

SMM is a special-purpose CPU mode in x86 microcontrollers that handles power management, hardware configuration, thermal monitoring, and anything else the Device Manufacturer deems useful.

Whenever one of these system operations is requested, an interrupt (SMI) is invoked at runtime, executing SMM code installed by the BIOS. SMM code executes in the highest privilege level and is invisible to the OS, making it an attractive target for malicious activity that can be potentially used to access hypervisor memory and change the hypervisor.

The SMI handler is typically provided by a developer different than the operating system and has access to OS/hypervisor memory and resources. This means exploitable vulnerabilities in SMM code lead to a compromise of Windows OS/HV and Virtualization Based Security (VBS).

To help isolate SMM, AMD introduces a security module called AMD SMM Supervisor that executes immediately before control is transferred to the SMI handler, after an SMI has occurred. AMD SMM Supervisor resides in AMD DRTM service block, and is used to:

- Block SMM from being able to modify hypervisor or OS memory, except for a small communication buffer between the two
- Prevent SMM from introducing new SMM code at run time
- Block SMM from accessing DMA, I/O, or registers that can compromise hypervisor or OS.

DMA PROTECTION

AMD platforms support direct memory access (DMA) protection in pre-boot and OS environments via AMD secure technologies like Input Output Memory Management Unit (IOMMU) with DMA remapping technology.

- DMA protection helps safeguard against a possible attack on the platform firmware where adversaries can use connected devices to perform DMA attacks.
- DMA provides devices' direct access to physical memory address space for improved performance. But this also makes it easier for malicious software to inject malware into the system, which can go undetected by the OS.

To help prevent such attacks, AMD has designed a security architecture to help manage and control device DMA access via Input Output Memory Management Unit (IOMMU) at the pre-OS firmware level.

DMA security architecture hands over responsibility of system memory protection settings from the firmware level to the OS after the OS boot loader has been established in memory. The DMA protection using IOMMU is applied on each boot, until the OS takes control of the IOMMU itself.

PLATFORM UPDATE

AMD Ryzen™ PRO 5000 series mobile processors not only provides improved security defenses against attackers trying to gain access to the system in real-time, they also provide a robust update mechanism. This enables organizations to seamlessly update platforms to patch vulnerabilities created by hardware or software bugs.

AMD works closely with OEMs to provide secure platform update architecture built around strong integrity which is compliant with industry-standard best practice guidelines and is integrated into OEM's platform update solution. AMD Ryzen™ PRO 5000 series mobile processors has a feature called "Firmware Anti-Rollback (FAR)" that enables hardware-based policy to block downgrade of AMD ASP firmware.

AMD Ryzen™ 5000 series mobile processors also provide a secure recovery framework called "A/B Recovery," which can be integrated into an OEM solution to enable recovery in the event of catastrophic failure.

CRYPTO ACCELERATOR

In today's world, cryptographic operations are important to help protect data and communications. While cryptographic operations are important, they are also very compute intensive. AMD's idea to help reduce cost associated with cryptographic algorithm computation is to provide new instructions in silicon which are optimized.

"Zen 3" architecture has added support for vectorized AES encryption for 256-bit (vAES256) which can be used by applications and complex workloads to take advantage of the benefits associated with it.

SUMMARY

AMD believes that modern security solutions can be achieved through layered defenses. Combining hardware-based security features and associated software protections helps protect against current and future cyberattacks including sophisticated low-level firmware attacks. With each generation of core and products, AMD will continue to innovate and push boundaries of security in hardware, and offer more comprehensive security solutions to customers.

AMD PRO Security Features and Benefits *Figure 4*

SECURITY FEATURE	BENEFIT	AMD PRO SECURITY
Memory Encryption	Encrypts memory to help prevent a physical attacker from reading sensitive data in memory. Helps mitigate cold boot attacks.	AMD Memory Guard
Secure Boot	Boot protection that helps prevent unauthorized software and malware from taking over critical system functions.	AMD Platform Secure Boot
Windows 10 Security	Microsoft security feature set which helps mitigate threats.	Supported
Virtualization-Based Security	Uses hardware virtualization features to create and isolate a region of memory from the normal operating system.	AMD-V
Firmware TPM	A firmware version instead of real hardware which provides authenticity to the platform and helps monitor for signs of security breaches.	AMD Firmware TPM
Random Number Generator	A hardware-based random number generator for cryptographic protocols. Provides cryptographic capabilities.	AMD RDRAND
AES-NI	Helps accelerate encryption protocols and protect network traffic (internet and email content) and personal data.	AMD AES

AMD PRO Security Features and Benefits, continued

SECURITY FEATURE	BENEFIT	AMD PRO SECURITY
Microsoft Secured-Core PC	Enables you to boot securely; helps protect device from firmware vulnerabilities, shield the operating system from attacks, and prevent unauthorized access to devices and data, with advanced access controls and authentication systems.	Secured-Core PC Compatible
Control Flow Attack Protection	Helps protect against control-flow attacks by checking the normal program stack against a hardware-stored copy and enabling Microsoft Hardware Enforced Stack Protection as part of a comprehensive set of AMD security features to help secure PCs.	AMD Shadow Stack
Guest Mode Execute Trap	A silicon performance acceleration feature which enables hypervisor to efficiently handle code integrity checks and helps protect against malware.	AMD GMET
System Management Mode Supervisor	A security module which helps isolate System Management Mode.	SMM Supervisor
Secure Init and Jump with Attestation	An instruction which helps create a "root of trust" starting from an initially untrusted operating mode.	AMD SKINIT
Direct Memory Attack Protection	Helps protect a system from malicious software trying to inject malware through devices which have direct access to physical memory address and can go undetected by the OS.	DMA Protection
Dynamic Run Time Measurement	Helps with integrity of the platform by transitioning low-level firmware from un-trusted to trusted state.	AMD DRTM

DISCLAIMER

"Zen" is a code name for AMD architecture, and is not a product name. GD-122

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. GD-18.

© 2021 AMD, the AMD arrow logo, EPYC, Radeon, Ryzen, and combinations thereof are trademarks of Advanced Micro Devices, Inc.

AMD