Cross-Platform Mobile Architecture Feature Comparison Research Addendum

Intel Corporation

IOActive, Inc.
701 5th Avenue, Suite 7250
Seattle, WA 98104

Toll free: (866) 760-0222
Office: (206) 784-4313
Fax: (206) 784-4367

Intel-commissioned study. Published May 2021.

Management Summary

In this Intel-commissioned document, IOActive, Inc. (IOActive) presents a comparison of the security features provided and publicly documented by Intel® Corporation (Intel) in the 11th Gen Intel® Core™ vPro® mobile processors with AMD's Ryzen 5000 Pro mobile processor series based on public documentation from AMD.

Our comparison is based on a set of objectives bundled into the categories: "***Below the OS***", "***Platform Update***", "***Trusted Execution***", "***Advanced Threat Protection (ATP)***", and "***Crypto Extension***".

Intel vs AMD

In the category ***Below the OS***, the subject AMD platform has no corresponding technology to Intel® System Security Report but does offer analogous capabilities to other Intel technologies.

For ***Platform Update****,* the subject AMD platform does not offer comparable capabilities to Intel BIOS Guard or Firmware Update Restart.

Based on our research, 11th Gen Intel® Core™ vPro® mobile processors and the subject AMD architecture have equivalent capabilities in the ***Trusted Execution*** category.

From our comparative analysis, we observe that the subject AMD platform does not offer comparable capabilities to Intel® Threat Detection Technology (Intel® TDT) in the ***ATP*** category. *We consider Intel TDT an impactful platform differentiator in this comparison*.

In the category ***Crypto Extension***, the subject AMD platform has no corresponding technology to Intel's AVX512-variant of AES.

The composites of the security technologies discussed in this document offer a compounded value that is greater than the sum of the parts.

Our research team ran a series of tests for Intel TDT, based on install and executable instructions provided by the Intel TDT team. The tests aimed to detect a curated selection of samples of cryptominers and known ransomware in various environments and on different platforms.

The test results show a detection rate of 100% for ransomware and 100% for cryptominers by Intel TDT. Also, to better mimic threats that are increasingly obfuscating in virtual machines (VMs), we ran comparisons to popular anti-virus (AV) software that are not enabled for CPU-based threat detection. In these cases, Intel TDT was able to detect 75% of obfuscated cryptominers, compared to 0% by AV software, AV software has a lack of visibility into these types attacks due to its typical deployment in the host OS. Note: Intel TDT is not a standalone AV or EDR package, it is intended to integrate into these solutions to augment and improve threat detection efficacy.

Technical Summary

IOActive's analysis is based on publicly available documents from both Intel and AMD describing particular security technologies for the subject mobile PC-targeted architectures. We developed a security feature model and used it to compare the two subject platforms as described in the Model and Comparison subsection.

Model and Comparison

Our approach for a comparison of features across vendor platforms started with the formulation of a security model. Our model consists of a carefully selected list of security objectives, bundled into categories. The objectives define goals and properties that provide security benefits to the customer. The categories relate to different execution stages of the CPU.

The following paragraphs define the categories and their objectives. They also list technologies or building blocks which can be used to achieve the objectives. Finally, a comparison of the corresponding technologies implemented by Intel and AMD is provided.

The model we present here is not exhaustive. It is missing a complete inventory of use-cases and would benefit from a thorough threat-model of the security features. IOActive adapted an organizational structure of objectives provided by Intel to create this model.

Each compared feature is presented as fulfilling, fulfilling with qualifications, or not fulfilling the associated objective.

Below the OS (Platform Integrity)

With the beginning of the boot sequence, the CPU must evaluate its hardware and firmware environment and ensure transition only to a verified bootloader. This integrity validation mitigates the risk of instruction tampering or interception by an adversary as well as providing a trustworthy baseline for the remainder of boot and operation.

In particular, the objectives include:

- Identify unauthorized changes to hardware and firmware
- Prevent malicious code injection in BIOS/UEFI memory
- Ensure OS and virtual environments are running directly on platform hardware (assuming no malicious code injection)
- Enforce OEM/IHV's provided policy and report on it

The main building blocks to achieve these objectives include:

- Secure Boot
  - Root of trust/Chain of trust
  - Enforcement
- Measured Boot

- Secure storage
- Static root of trust measurement
- Dynamic root of trust measurement
- Attestation

Table 1. Below the OS solutions

Intel Solution	AMD Solution
Intel® Boot Guard	AMD Secure Boot
Intel® Trusted Execution Technology	AMD SKINIT + Secure Loader
Intel® Runtime BIOS Resilience	AMD SMM Supervisor[1]
Intel® System Security Report	No equivalent feature
Intel® System Resources Defense	AMD SMM Supervisor[1]

Platform Update

This category is about mechanisms for trustworthy firmware updates. Each of these protections addresses the risk of replacement of some or all of the platform-defining software and firmware with malicious components.

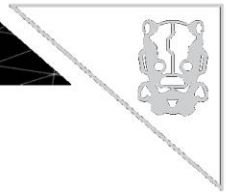
- Objectives
  - Update firmware code with integrity check
  - Downgrade protection
  - Focus on BIOS for most recent and secure updates
- Building Blocks
  - Provide new environment so OEMs can perform more flexible and modular updates securely
  - Utilizes UEFI capsule architecture for driving better firmware updates

Table 2. Platform Update solutions

Intel Solution	AMD Solution
Intel® Firmware Guard	No equivalent feature[2]
Intel® BIOS Guard	No equivalent feature[2]

[1] As of publication, only a brief high-level description of this feature was available. The authors are provisionally accepting the assertions in this description.

[2] https://www.amd.com/system/files/documents/guardmi-infographic.pdf equates AMD secure boot to both of these Intel features, but this is not substantiated by the public documentation such as https://www.amd.com/system/files/TechDocs/40332.pdf



Trusted Execution/Application and OS Protection

In this category we list objectives for protection and prevention mechanisms to ensure a trustworthy runtime environment. Building on the integrity measures above, these elements enhance the stability and safety of the platform's operation.

- Objectives
  - Prevent memory corruption and tampering attacks
  - Protect sensitive data from unauthorized access
  - Protect data and virtualized containers with hardware-enforced isolation and encryption
  - Improve performance of virtualized security workloads
- Building Blocks/Hypervisor Support
  - Virtualization instructions
    - VM extensions
    - Nested virtualization
  - Virtual I/O
  - Virtual interrupts
  - Memory protection/encryption
  - Hardware-based encryption and random number generation

Table 3. Trusted Execution solutions

Intel Solution	AMD Solution
Intel® Virtualization Extensions (VT-x)	AMD-V
Intel® Virtualization Technology for Directed I/O (VT-d)	AMD-Vi
APIC Virtualization	Advanced Virtual Interrupt Controller (AVIC)
Mode Based Execution Control	AMD-V with GMET
Intel® Control-flow Enforcement Technology (Shadow Stack and Indirect Branch Tracking)	Shadow Stack Only
Intel® Total Memory Encryption	AMD SEV/SME[3]

[3] Multiple VMs can only share *unencrypted* memory (accessible to their common hypervisor). See https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf, page 4

Advanced Threat Protection

The objectives in this category do not protect or prevent attacks but allow to detect them.

- Objectives
  - Increase security and performance via offload to GPU dedicated security workloads
  - Leverage hardware telemetry to help detect advanced threats such as ransomware and cryptomining attacks
- Building Blocks
  - Reference code components
  - Detectors

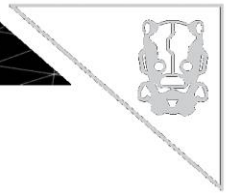
Table 4. ATP solutions

Intel Solution	AMD Solution
Intel® TDT- Security Offload to iGPU (e.g. Memory Scanning)	No equivalent feature
Intel TDT - Advanced Platform Telemetry	No equivalent feature

Crypto Extension

This category lists objectives for hardware support for crypto primitives with specific properties.

- Objectives
  - Provide hardware implementations for certified crypto primitives
  - Avoid side channels in the implementation of crypto primitives
  - Allow crypto operations without storing key where it can get lost
  - High speed and throughput
- Building Blocks
  - Good source of randomness (rdrand)
  - Side-channel free efficient crypto primitives
  - Secure key storage (TPM, PKEY)
  - Parallelizable implementation of primitives
  - Hardware-assisted AES encryption
  - Hardware-assisted AES decryption
  - Hardware-assisted AES inverse mix column transformation
  - Hardware-assisted AES created round keys with key expansion schedule
  - Cryptographically secure enhanced non-deterministic random bit generator



- Cryptographically secure deterministic random bit generator

Table 5. Crypto Extension solutions

Intel Solution	AMD Solution
Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)	AMD AES-NI[4]
Intel® Secure Key	AMD RNRAND
Key Locker	No equivalent feature

[4] AMD does not appear to have a corresponding technology to Intel's AVX512-variant of AES