IOActive®

Research-fueled Security Services

Cross-Platform Security Feature Comparison Research

Management and Technical Summary

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 December 2020.

Management Summary

In this document IOActive presents

A. A comparison of security features provided by Intel in the vPro CPU model Tiger Lake and AMD's Ryzen 4000 series, and highlights from current academic research where applicable

B. Test results of selected tests cases for Intel's TDT technology.

IOActive has compared security related technologies from both Intel and AMD using vPro Tiger Lake (Intel) and Ryzen 4000-series (AMD) CPUs. Our comparison is based on a set of objectives bundled into the categories "Below the OS", "Platform Update", "Trusted Execution", "Advanced Threat Protection" and "Crypto Extension".

From our research we conclude that AMD offers no technologies in the categories "Advanced Threat Protection" (ATP) and "Platform Update". Intel offers "*BIOS Guard"* and Firmware Update Restart and "*Control-Flow Enforcement Technology"* and "*Threat Detection Technology"* for ATP. In the category "Below the OS", AMD has no corresponding technology to Intel's "*System Security Report*". In the category "Crypto Extension", AMD has no corresponding technology to Intel's AVX512 variant of AES. Based on our research, Intel and AMD have equivalent capabilities in the "*Trusted Execution"* category*.*

The following technologies are the most impactful platform differentiators for security:

1. Control-Flow Enforcement Technology (CET)

2. Threat Detection Technology (TDT)

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

Our research team ran a series of tests for *Threat Detection Technology*, based on install and executable instructions provided by Intel's 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 crypto-miners by TDT. Also, to better mimic threats that are increasingly obfuscating in virtual machines, we ran comparisons to popular anti-virus software that are not enabled for CPU-based threat detection. In these cases, TDT was able to detect 75% of obfuscated cryptominers compared to 0% by anti-virus software that has a lack of visibility into these types attacks due to AV software's 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

The report sections “*Intel Technologies”* and “*AMD Technologies”* quote from publicly available documents of both vendors and list particular security technologies. The section “*Detailed Features Comparison”* explains the commonalities and differences of the corresponding technologies from both vendors. We developed a security feature model and used it to compare the two subject platforms as described in the “*Model and Comparison*” subsection.

“*Intel Threat Detection Technology Tests*” contains a detailed description of the setup for the tests for TDT, the particular samples of ransomware and cryptominers that were used as test cases for the various tests, and the test results.

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. Our choice of objectives in this model has been negotiated with Intel.

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 boot loader. 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
- Solutions

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

Platform Update

This category is about mechanisms for trustworthy firmware updates.

- Objectives
    - Update of Firmware code with integrity check
    - Downgrade protection
    - Modern updates with focus on BIOS update for most up to date 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
- Solutions

Intel Solution	AMD Solution
Firmware Update Restart	No equivalent feature
Intel BIOS Guard	No equivalent feature

Trusted Execution/Application and OS Protection

In this category we list objectives for protection and prevention mechanisms to ensure a trustworthy runtime environment.

- 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
    - Virtual machine extensions
    - Nested Virtualization
  - Virtual I/O
  - Virtual interrupts
  - Memory protection / encryption
  - Hardware-based encryption and random number generation
- 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	AMD Advanced Virtual Interrupt Controller (AVIC)
Mode Based Execution Control	AMD-V with GMET
Control-flow Enforcement Technology	Not implemented in Ryzen 4000
Intel Total Memory Encryption	AMD SEV/SME

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 crypto mining attacks
- Building Blocks
  - Reference code components
  - Detectors
- Solutions

Intel Solution	AMD Solution
Threat Detection Technology – Advanced Memory Scanning	No equivalent feature
Threat Detection Technology - 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
  - Provide good source of randomness (rdrand)
  - Side-channel free efficient crypto primitives
  - Secure key storage (TPM, PKEY)
  - Provide parallelizable implementation of primitives
  - Hardware Assist AES encryption
  - Hardware Assist AES decryption
  - Hardware Assist AES Inverse Mix Column Transformation
  - Hardware Assist AES Create round keys with key expansion schedule
  - Cryptographically Secure Enhanced Non-Deterministic Random Bit Generator
  - Cryptographically Secure Deterministic Random Bit Generator
- Solutions

Intel Solution	**AMD Solution**
Intel Advanced Encryption	AMD AES-NI
Intel Secure Key	AMD RNRAND
Key Locker	No equivalent feature