White Paper

Information Technology
Cybersecurity

Intel® Hardware Shield – Intel® Total Memory Encryption

Intel Business Client Platform Security Marketing

Introduction

This document covers security features in Intel® Hardware Shield on the Intel vPro® platform as they pertain to helping to protect system memory. It covers both software and hardware security capabilities. Specifically, this document provides in-depth information on Intel® Total Memory Encryption (Intel® TME).

Intel® Hardware Shield Overview

The Intel vPro platform delivers hardware-enhanced security features that help protect all layers in the computing stack. Intel Hardware Shield, exclusive to the Intel vPro platform, helps reduce the attack surface of the system by locking down system critical resources to help prevent malicious code injection from compromising the OS, helping to ensure the OS runs on legitimate hardware, and delivering hardware to OS security reporting to enable the OS to enforce a more comprehensive security policy. In addition, Intel Hardware Shield offers advanced threat protection features that can perform active memory scanning to help improve the detection of advanced threats while reducing false positives and minimizing performance impact.

Intel Hardware Shield comes ready out of the box with every Intel vPro platform. Intel Hardware Shield has three main components. The components are: advanced threat protections, application and data protections and below-the-OS security.

Advanced Threat Protections:

This security feature is hardware-powered and provides AI-enabled threat detection with minimal performance degradation for the user. Advanced Threat Detection features provide proactive scanning for hard to detect threats, like ransomware and cryptomining.

Application and Data Protections:

This is hardware-powered virtualization-based security for applications and the operating system. It eliminates an entire class of attacks that evade current software solutions. In addition to eliminating attacks, this set of features also provides performance enhancements. One of the technologies in this group is Intel TME.

Below-the-OS Security:

Intel Hardware Shield can lock down memory in the BIOS against firmware attacks and enforces a secure boot at the hardware level. These below-the-OS security features are set-up by the PC manufacturer, so IT departments and users can take advantage of them right out of the box.

Intel's Vision of Hardware-based Security

Intel's vision of security architecture is based on the idea that workloads expand and threat models evolve. Three significant security challenges emerge as computing decentralizes from cloud to edge:

1. Lack of physical security—edge installations lack security guards and hardened walls found at traditional data centers.
2. Workloads are distributed more than ever—rather than monolithic workloads, each solution may include numerous microservices running on numerous devices, and security is only as strong as the weakest link.
3. Different architecture types are everywhere—spatial, vector, matrix, and scalar architectures all proliferate at the edge, with GPUs, XPUs and AI accelerators in cameras, sensors and other smart, connected devices. They all need solid security architecture.

For these reasons, Intel architectures start with foundational security. Intel has a proud history of delivering innovative security technologies—from Intel® OS Guard to Intel® BIOS Guard to Intel® Boot Guard to Intel® Trusted Execution Technology (Intel® TXT) and more—to make sure that the platform comes up correctly and is running what is expected.

Intel has delivered security engines that have been used more than a billion times worldwide. Intel hardware-based cryptography is one example. The first microcode accelerating the original Advanced Encryption Standard (AES) in Intel® Core™ processors improved performance by an order of magnitude —that enabled HTTPS everywhere, helping to secure e-commerce, worldwide.

That Intel innovation also enabled hard drive encryption, and the next logical thing to address is main memory. Intel TME was introduced with the 11th Gen Intel® Core™ vPro® mobile processor to shut down an entire attack class—one where an attacker steals a system, crashes it, and then reads the contents out of memory. Such attacks on an 11th Gen Intel Core vPro mobile processor-based system yield only garbage: cypher-text, nothing that attackers can use.

Filesystem encryption is now a standard practice in many enterprises, protecting user data when it is at rest. On the other hand, data stored in main memory is kept in the clear, as are exchanges between memory chips and the processors. Memory attacks clearly represent a significant exposure with the potential to scale quickly through an enterprise network. Physical memory hacking has been used both by common cybercriminals, as well as nation-state backed hacking specialists. Hackers are crafting memory attacks designed to help them gain footholds, move laterally, and achieve persistence deep inside well-defended enterprise networks.

Enterprise businesses need integrated software and hardware solutions to protect system memory. That is where Intel Hardware Shield comes in, delivering hardware-based security capabilities to help protect every layer of the compute stack.

The security improvements extend to helping to prevent a bad actor from taking over the computer memory on the way to a data breach.

What is Intel Total Memory Encryption?

Intel TME encrypts a computer's entire memory with a single transient key. All memory data passing to and from the CPU is encrypted. This includes memory data such as customer credentials, encryption keys, and other IP or personal information. Intel TME was developed to provide greater protection for system memory against hardware attacks, such as removing and reading the dual in-line memory module (DIMM) after spraying it with liquid gases (cold boot attack) or installing purpose-built attack hardware. Intel TME also helps protect against memory bus probing or relocation/splicing attacks.

Intel TME is enabled in the very early stages of the boot process, and once configured and locked, will encrypt all the data on external memory buses of a CPU using the National Institute of Standards and Technology (NIST) standard AES-XTS algorithm with 128-bit keys. The encryption key used for memory encryption is generated using a hardened random number generator in the CPU and never exposed to software. This allows existing software to run unmodified while better protecting memory. A new platform key is generated by the processor on every boot.

Data in memory and on the external memory buses is encrypted and is only in plain text while inside the CPU, similar to storage encryption on hard disks or SSDs. There are some scenarios where it would be advantageous to not encrypt a portion of memory, so Intel TME allows the BIOS to specify a physical address range to remain unencrypted. IT Admins can enable/disable the usage of Intel TME in the BIOS settings.

The AES-XTS mode, typically used for block-based storage devices, takes the physical address of the data into account when encrypting each cacheline block. This ensures that the effective key is different for each cacheline. Moving encrypted content across physical address results in garbage on read, mitigating block-relocation attacks.

Malware running in the OS is not mitigated by Intel TME. Intel TME is intended to provide protection from certain physical attacks. Intel TME also cannot protect against remotely acquired malware that gets into memory.

How Intel Total Memory Encryption Works

Figure 1 (page 3) shows an implementation of Intel TME on a client computer.

The Intel TME capability to encrypt memory is intended to provide protections of AES-XTS to the external memory buses and DIMMs. The AES-XTS encryption engine is in the direct data path to external memory buses and, therefore, all the memory data entering and/or leaving the CPU on memory buses is encrypted using AES-XTS.

A Key for Intel TME is generated at every boot time. If the system is resuming from a standby, Intel TME can restore the key from storage. Additional details are available in the Intel TME specification.

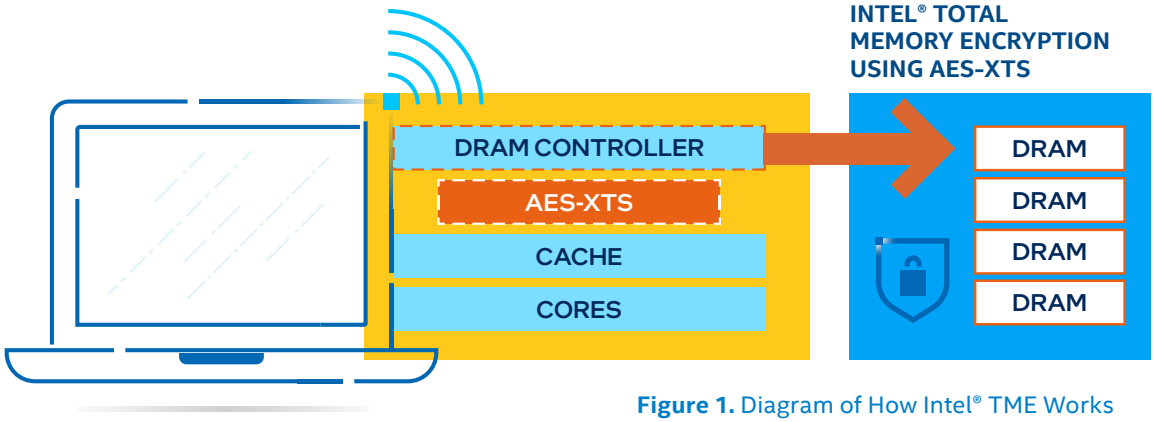

Figure 1. Diagram of How Intel® TME Works

Performance

Intel TME adds a layer of protection against cold boot attacks, and the overall performance impact of Intel TME is relatively small.

Intel Total Encryption Memory Summary

Memory attacks have quietly emerged as a powerful and versatile new class of hacking techniques to subvert conventional IT security systems. Memory without proper encryption, can be vulnerable to physical attacks. Once in the memory, hackers can read all that the computer is doing, steal sensitive data, passwords or encryption keys, install spyware or modify the system to allow backdoors for other malware. Malicious software in memory can even render the end-user computer completely inoperable.

Intel TME is effective against hardware or physical attacks on system memory, such as a cold boot attack. With Intel TME, IT managers now have a protection mechanism similar to protecting data in hard disk drives or SSDs via encryption. In today's mobile world, laptops can be lost or stolen. While Intel TME cannot find the laptop, the memory in the system is better protected.

Using Intel TME encrypts a computer's entire memory. The encryption key is produced by a random number generator inside the CPU. Data in memory and on the external memory buses is encrypted and has greater protection against some types of hardware attacks. IT managers should be proactive in preventing attacks. Being vigilant about building a defense in depth security strategy with Intel TME provides an additional layer of protection for the IT professionals.

Intel Hardware Shield, a component of the Intel vPro platform is designed to improve the security of the computer. The Intel Hardware Shield technologies, when used with a minimum access policy, help to harden computing platforms. Intel TME enhances the Intel Hardware Shield capabilities on the 11th Gen Intel Core vPro mobile platforms to help reduce security risks.

Additional Resources

Intel vPro® Platform
Intel.com/vPro

Intel.com/HardwareShield

Intel Total Memory Encryption Specification

Intel vPro Expert Center

Intel vPro Platform Support
Intel.com/support

[1] The first microcode accelerating the original Advanced Encryption Standard (AES) in Intel® Core™ processors improved performance by an order of magnitude—see https://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

0521/MZ/DCC/PDF