White Paper

Cybersecurity
Information Technology

Runtime Encryption of Memory With Intel® Total Memory Encryption - Multi-Key

Hormuzd Khosravi
Sr. Principal Engineer
Intel Corporation

Introduction

Most cyberattacks occur at the application and data level, and those attacks are getting more sophisticated. The security perimeter erodes as cyberthreats evolve and become more complex. For IT professionals, balancing user experience against security priorities can be daunting. That's especially true today, as home and business PC uses converge with more people working remotely than ever before. That means IT must provide high-performance devices and enhanced support for employee productivity while also taking proactive measures to improve security by protecting valuable assets and data. Cybercriminals regularly gain access to valuable data by hacking poorly secured applications. Common security failures include "code injection" attacks, in which attackers insert malicious code that can tamper with data, or even destroy it. Wherever confidential data is stored, it must be protected against unauthorized access, whether through physical device theft or from malicious applications. The 12th gen Intel vPro® processors include security capabilities to isolate and help protect login credentials, sensitive data, and business-critical applications in secure virtual machines. In addition, 12th gen Intel vPro processors include advanced hardware-based encryption technologies to help protect data in flight, at rest, and in applications.

Today, it is well understood that data at rest in local and/or network-attached storage needs to be protected using strong encryption protocols, and this has been a universal practice in the cloud and enterprise. Similarly, data in transit is commonly encrypted using SSL/TLS/HTTPS protocols. However, when the same data is being processed by the CPU, it is in the memory and is not protected using cryptography. Memory contains high-value assets such as storage encryption keys, session keys for communication protocols, personally identifiable information and credentials, and more. Therefore, it is critical that data in memory has comparable protection to data at rest in storage devices. It is not sufficient to encrypt memory content but encrypting content on the memory bus is equally important. The encryption has to be general purpose, flexible, supported in hardware with very limited impact on applications/workloads, and not a heavy lift for the OS/hypervisor enabling.

In this paper, we describe a new memory encryption technology that Intel introduced on the 12th gen Intel vPro® processor codenamed 'Alder Lake', Intel® Total Memory Encryption - Multi-Key (Intel® TME-MK). This technology is addressing the data protection needs by encrypting memory content at runtime using NIST standard AES-XTS algorithms. Virtualized and containerized environments need more granular, page-level memory encryption. Intel TME-MK

Table of Contents

enhances Intel® Total Memory Encryption (Intel® TME) for page-granular memory encryption through support for multiple encryption keys. This paper first provides a technical overview of the technology and then describes the usages for Intel vPro customers.

Description

As described above, Intel is introducing Intel TME-MK to help address runtime data protection needs for all platform memory via the ability to encrypt the memory during execution and in use.

Intel TME and Intel TME-MK Technical Overview

Intel TME has the capability to encrypt the entire physical memory of a system with a single encryption key, addressing concerns with cold boot and physical attacks on the memory subsystem. This capability is enabled in the very early stages of the boot process by the BIOS and once configured and locked, will encrypt all the data on external memory buses of a SOC using the NIST standard AES- XTS algorithm with 256-bit keys. The encryption key used for TME uses a hardware random number generator implemented in Intel SOC and the keys are not accessible by software or using external interfaces to Intel SOC. Intel TME capability does not require OS or system software enabling.

Intel TME-MK enables the use of multiple encryption keys, allowing the selection of the encryption key per page using the processor page tables. Encryption keys are programmed into the memory controller. Intel TME-MK inherits many of the mitigations against hardware attacks from Intel TME. Intel TME-MK does not mitigate vulnerable or malicious operating systems or virtual machine managers (VMM). Intel TME-MK offers additional mitigations when compared to Intel TME (Kernel Mapping Attacks, Freed Data Leak Attacks, Cross Domain Replay Attacks, etc.) Intel TME and Intel TME-MK use the AES encryption algorithm in the AES-XTS mode. This mode typically is used for block- based storage devices and takes the physical address of the data into account when encrypting each block. This ensures that the effective key is different for each block of memory. Moving encrypted content across physical addresses results in garbage data upon read, significantly mitigating block-relocation attacks.

The Intel TME-MK capability maintains a key table, not visible to software, which stores the key and encryption type information associated with each KeyID. Each KeyID may be configured in four different ways:

1) Encryption using software specified key
2) Encryption using hardware-generated key
3) Encrypt using default platform Intel TME Key
4) Does not encrypt at all (memory will be plain text)

The OS/Hypervisor can assign the proper KeyID in the upper physical address bits contained in the paging-structure entries. The hypervisor would have ultimate control over these KeyIDs or domains via the Extended Page Tables (EPT) paging structures.

For a native/bare-metal OS, the IA32e page tables will be used to determine the proper key domain.

For direct physical mappings (e.g., VMX pointers, CR3 with no EPT), the behavior is the same and the software can choose the proper KeyID by using the upper physical address bits in these addresses.

Page Granular Encryption

Intel TME-MK supports page granular encryption. As an example, in figure 1, we show one hypervisor/VMM and two VMs. By default, the hypervisor uses KeyID 0 (same as Intel TME). VM1 uses KeyID1 for its own private pages and VM2 is using KeyID 2 for its own private pages. In addition, VM1 can always use KeyID 0 (Intel TME KeyID) for any page and is also opting to use KeyID 3 for shared memory between itself and VM2. The KeyID is included in the upper bits of the physical address field (in this example, KeyID 2 is shown).

The remainder of the bits in the physical address field is used to address bits in the memory. Figure 1 shows one possible page assignment along with KeyID for illustration purposes. Although in this case, the hypervisor has full freedom to be able to use any KeyID with any pages for itself or any of its

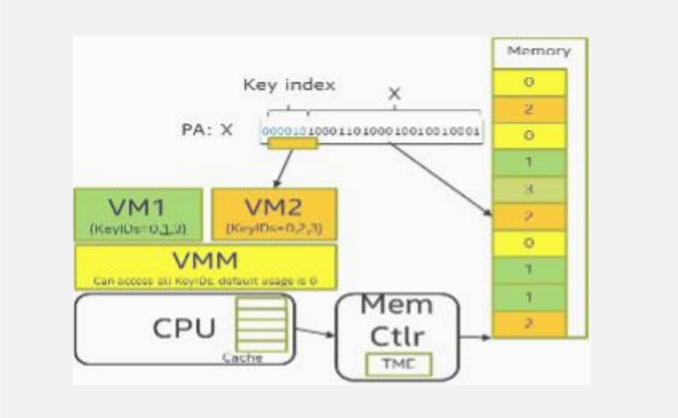

Figure 1 – Intel TME-MK is enabled in Windows/Hyper-V and is deployed as part of Windows11 22H2 on 12th Gen Intel vPro processors.

Usages

The primary usage for Intel TME-MK is around providing protections for encrypted VMs; these can be software containers hosted in Windows. One such example of separate Hyper-V managed memory encryption keys per VM would be useful for scenarios like Privileged Access Workstations. More information on Privileged Access Workstations is available.

Please refer to Microsoft Total Memory Encryption Multi-Key (Intel TME-MK) on Windows 11 22H2 blog

Conclusion

Intel builds-in security from the ground up, for powerful defense in today's threat environment. Together, Intel hardware and Windows 11 software meet the modern threats of today's hybrid work environments by delivering hardware-based isolation, end-to-end encryption, and advanced malware protection. With Windows 11 on 12th Gen Intel vPro PCs, customers get business-class productivity and intuitive new experiences without compromising security. For more information on the complete list of hardware technologies that Windows 11 security builds upon, please refer to our Windows 11 Security on Intel Hardware whitepaper.

For More Information:

Intel Virtualization Technologies whitepaper
Microsoft 11 Security Book
Intel.com/vPro

Acknowledgments

Venky Venkateswaran, Intel Corporation
Jennifer Larson, Intel Corporation
Michael Zeuthen, Intel Corporation

Notices & Disclaimers

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.