Total Memory Encryption (TME)

Return to Glossary

Total Memory Encryption (TME) is the capability to encrypt the entirety of physical memory of a system. This capability is typically enabled in the very early stages of the boot process with a small change to Basic Input/Output System (BIOS) and once configured and locked, will encrypt all the data on external memory buses of an System-on-a-Chip (SoC) using the NIST: SP 800-34E AES-XTS algorithm with 128-bit keys or 256-bit keys depending on the algorithm availability and selection. The encryption key used for TME uses a hardware random number generator implemented in the Intel SoC, and the keys are not accessible by software or using external interfaces to the Intel SoC. TME capability is intended to provide protections of AES-XTS to external memory buses and DIMMs. The architecture is flexible and will support additional memory protection schemes in the future. This capability, when enabled, is intended to support (unmodified) existing system and application software. Overall performance impact of this capability is likely to be relatively small and is highly dependent on workload. [1)]

Source:
https://software.intel.com/content/dam/develop/external/us/en/documents-tps/multi-key-total-memory-encryption-spec.pdf

1)
Intel Architecture Memory Encryption Technologies: Specification, version 1.3, Intel Corporation, April 2021, Accessed: 8 October 2021, https://software.intel.com/content/dam/develop/external/us/en/documents-tps/multi-key-total-memory-encryption-spec.pdf