Main Memory Encryption (MME)

Return to Glossary

Main Memory Encryption (MME) can be utilized to protect a system against a variety of attacks. While data is typically encrypted today when stored on disk, it is stored in Dynamic Random Access Memory (DRAM) in the clear. This can leave the data vulnerable to snooping by unauthorized administrators or software or by hardware probing. New non-volatile memory technology (NVDIMM) exacerbates this problem since an NVDIMM chip can be physically removed from a system with the data intact, similar to a hard drive. Without encryption any stored information such as sensitive data, passwords, or secret keys can be easily compromised.

Source:
https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:m:mme&rev=1633726166

Last update: **2021/10/08 16:49**