Memorandum Of Understanding

Xitore, Inc.

Vol. 1 , Issue 4

SECURITIZATION OF MEMORY MODULES AGAINST MALICIOUS ACTS

STANDARD MODULE

- Historically Memory modules are used to provide one or more array of Volatile Memories (i.e. DRAM, SRAM, etc.) to directly connected into host Central Processing Unit(s) (CPUs) via host memory controller.
- When Application launched from one or more storage devices (i.e. HDD, SDD, etc.) the active portion of executable file (i.e. .exe) and any associated libraries (i.e. DLL), along with any logging, database, or other part of the application that needs to reside active for the entire duration of execution of the application will load into host main memory.
- What happens if someone yank this module and less than few second plug it into a near by live system?
- Can an intruder get access to your AES Key, Decompression algorithm, Network Security tables residing in your memory module.
- If so how can one protect this?

XITORE SECURITY

- Another Xitore innovation is that it has developed technology that can prevent security breaches through physically removing a plugged-in and powered memory DIMM module and then accessing the contents in other nearby systems. This patented Xitore innovation recognizes when a DIMM is maliciously removed as an intrusion by an unaccepted act such as de-populating a fully powered and working module while the system is up and running, and prevents the data from being accessed elsewhere.
- Hence protecting your most vulnerable sensitive Corporate or Government data & security means by an intruder.

Disclaimer:

Xitore, Inc. is not a member of either JEDEC or SNIA organizations since its inception in 2014. The company is a technology licensing company with a comprehensive patent portfolio in Persistent and Storage Class Memory space. For more information visit our website at: Xitore IP Licensing