TechAndComputer (May 18, 2011) Security concerns are one of the key obstacles to the adoption of new non-volatile main memory (NVMM) technology in next-generation computers, which would improve computer start times and boost memory capacity. But now researchers from North Carolina State University have developed new encryption hardware for use with NVMM to protect personal information and other data.

NVMM technologies, such as phase-change memory, hold great promise to replace conventional dynamic random access memory (DRAM) in the main memory of computers. NVMM would allow computers to start instantly, and can fit more memory into the same amount of space used by existing technologies. However, NVMM poses a security risk.

Conventional DRAM main memory does not store data once the computer is turned off. That means, for example, that it doesn't store your credit card number and password after an online shopping spree. NVMM, on the other hand, retains all user data in main memory even years after the computer is turned off. This feature could give criminals access to your personal information or other data if your laptop or smart phone were stolen. And, because the data in the NVMM is stored in main memory, it cannot be encrypted using software. Software cannot manage main memory functions, because software itself operates in main memory.

NC State researchers have developed a solution using a hardware encryption system called i-NVMM.

"We could use hardware to encrypt everything," explains Dr. Yan Solihin, associate professor of electrical and computer engineering at NC State and co-author of a paper describing i-NVMM, "but then the system would run very slowly -- because it would constantly be encrypting and decrypting data.

"Instead, we developed an algorithm to detect data that is likely not needed by the processor. This allows us to keep 78 percent of main memory encrypted during typical operation, and only slows the system's performance by 3.7 percent."

The i-NVMM tool has two additional benefits as well. First, its algorithm also detects idleness.

That means any data not currently in use -- such as your credit card number -- is automatically encrypted. This makes i-NVMM even more secure than DRAM. Second, while 78 percent of the main memory is encrypted when the computer is in use, the remaining 22 percent is encrypted when the computer is powered down.

"Basically, unless someone accesses your computer while you're using it, all of your data is protected," Solihin says.

i-NVMM relies on a self-contained encryption engine that is incorporated into a computer's memory module -- and does not require changes to the computer's processors. That means it can be used with different processors and different systems.

"We're now seeking industry partners who are interested in this technology," Solihin says.

The paper, "i-NVMM: A Secure Non-Volatile Main Memory System with Incremental Encryption," will be presented June 6 at the International Symposium on Computer Architecture (ISCA) in San Jose, Calif. The paper was co-authored by Dr. Siddhartha Chhabra, a former Ph.D. student at NC State. The research was supported, in part, by the National Science Foundation.

Email or share this story:

Story Source:

The above story is reprinted (with editorial adaptations by Tech*andComputer.com* staff) from materials provided by
North Carolina State University
.

Note: If no author is given, the source is cited instead.