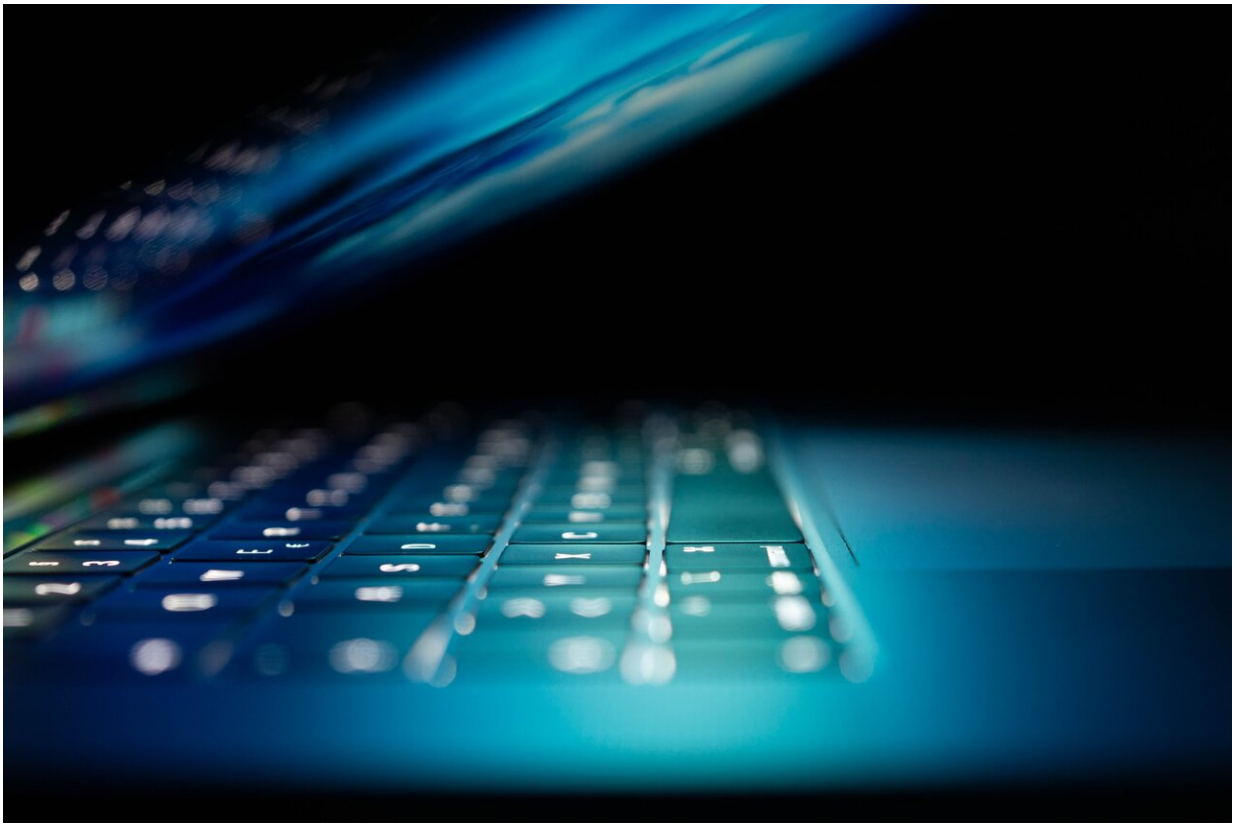
New technique offers faster security for non-volatile memory tech

April 5 2022, by Matt Shipman



Credit: Unsplash/CC0 Public Domain

Researchers have developed a technique that leverages hardware and software to improve file system security for next-generation memory technologies called non-volatile memories (NVMs). The new encryption

technique also permits faster performance than existing software security technologies.

"NVMs are an emerging technology that allows rapid access to the data, and retains data even when a system crashes or loses power," says Amro Awad, senior author of a paper on the work and an assistant professor of electrical and computer engineering at North Carolina State University. "However, the features that give NVMs these attractive characteristics also make it difficult to encrypt files on NVM devices—which raises security concerns. We've developed a way to secure files on NVM devices without sacrificing the speed that makes NVMs attractive."

"Our technique allows for file-level encryption in fast NVM memories, while cutting the related execution time significantly," says Kazi Abu Zubair, first author of the paper and a Ph.D. student at NC State.

Traditionally, computers use two types of data storage. Dynamic random access memory (DRAM) allows quick access to stored data, but will lose that data if the system crashes. Long-term storage technologies, such as hard drives, are good at retaining data even if a system loses power—but store the data in a way that makes it slower to access.

NVMs combine the best features of both technologies. However, securing files on NVM devices can be challenging.

Existing methods for file system encryption use software, which is not particularly fast. Historically, this wasn't a problem because the technologies for accessing file data from long-term storage devices weren't particularly fast either.

"But now that NVMs are allowing faster access to file data, the software approach to file encryption has become a problem, because it slows down overall operations," Abu Zubair says.

"To address this challenge, we've developed a novel architecture that incorporates some elements of the encryption and decryption process into hardware, which is faster than software. As a result, processes that allow users to store and retrieve file data securely are significantly faster."

In simulations, the researchers found that using their novel encryption architecture to secure files in NVMs slowed down operations by 3.8%, when running workloads that were representative of real-world applications. When using software approaches to provide security for the same workloads, operations slowed by about 200%.

"If this was implemented in commercial processors, it would significantly improve performance for secure file operation in large data centers and cloud systems," Abu Zubair says.

"While this work addresses file encryption, we think it is important to assess other security functions—such as auditing and run-time ransomware detection—in the context of direct access file systems," says Awad. "And addressing those security functions using traditional software approaches can also slow system performance. We're optimistic that our hybrid hardware/software approach may be able to improve performance for those functions as well—that's an area we're exploring."

The paper will be presented April 5 at the 28th IEEE International Symposium on High-Performance Computer Architecture (HPCA-22).

More information: "Filesystem Encryption or Direct-Access for NVM Filesystems? Let's Have Both!" Presented: April 5, 2022, The 28th IEEE International Symposium on High-Performance Computer Architecture (HPCA-22). Conference: hpca-conf.org/2022/

Provided by North Carolina State University