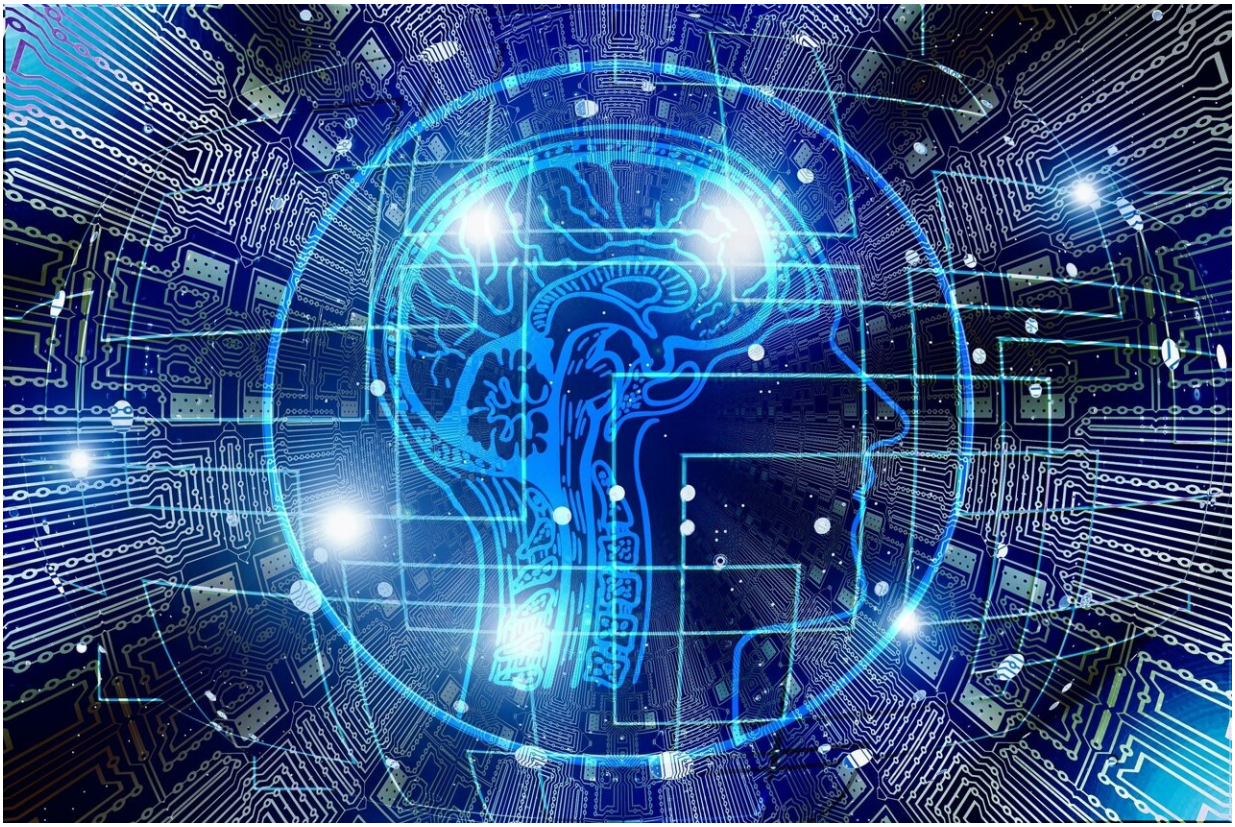
Is a security feature on the way that makes computing faster?

March 23 2022



Credit: Pixabay/CC0 Public Domain

Multiple programs running concurrently on a device rely on data stored in the device's memory hardware, but sensitive information might not be shared among all the programs, exposing the device to a "memory timing

side-channel attack."

When attempting to access memory hardware, response delays are noted and exploited to retrieve sensitive information like passwords or cryptographic keys. The current solution of restricting memory hardware to a single program slows computation.

U.S. National Science Foundation grantee researchers based at the Massachusetts Institute of Technology developed an approach that allows memory hardware to be shared without compromising security from memory timing side-channel attacks, and increases computation speed by 12% compared to state-of the art solutions. The research is published in *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*.

"Nowadays, it is very common to share a computer with others, especially if you do computation in the cloud or even on your own mobile device," said senior author Mengjia Yan. "Through these shared resources, an attacker can seek out even very fine-grained information."

There are several ways a malicious program can target shared memory to access sensitive information. The team focused on a solution to foil contention attacks—when the malicious program tries to access memory hardware at the same time as another program.

"The attacker is poking at the memory controller, the library door, to say, 'is it busy now?'" said co-author Joel Emer. "If they get blocked because the library door is opening already—because the victim program is already using the memory controller—they are going to get delayed."

The researchers developed a scheme that uses a graph structure, known as a directed acyclic graph, or DAG, to process requests and submit the

requests to the memory controller on a fixed schedule. The structure allows memory hardware to be shared among programs securely. The team named the security scheme DAGguise.

DAGguise could be modified to defend against different side-channel attacks that target shared computing resources like on-chip networks.

More information: Peter W. Deutsch et al, DAGguise: mitigating memory timing side channels, *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (2022). DOI: 10.1145/3503222.3507747

Provided by National Science Foundation