Eliminating infamous security threats

June 12 2019

Credit: CC0 Public Domain

Speculative memory side-channel attacks are security vulnerabilities in computers for which no efficient solutions have been found. Existing solutions only address specific security threats without solving the underlying issue.

Speculative side-channel attacks exploit a fundamental functionality in microprocessors to expose security vulnerabilities. The first such security threats, Meltdown and Spectre, were announced last year, but many more have been discovered since. Previous security solutions have been limited and often incurred a high performance penalty.

Now, researchers from Uppsala University, NTNU, and University of Murcia have come up with a more appealing solution, which will be presented at the prestigious International Symposium on Computer Architecture (ISCA) at the end of June.

"Our solution reduces the performance and energy costs, and increases the security of the computer system, when compared to previous solutions," says Christos Sakalis, Ph.D. student at Uppsala University.

Speculation Exploited

The security vulnerability manifests when the microprocessor tries to guess (speculate) on what to do next. If the microprocessor guesses incorrectly (misspeculates), it will undo any work it has done and start anew. Speculation lies at the core of today's high-performance microprocessors and it is necessary for taking full advantage of the microprocessors' capabilities.

"In theory, any misspeculations should not leave any visible traces, but they do leave traces nonetheless," says Alexandra Jimborean from Uppsala University.

These traces are exploited by Meltdown and Spectre to retrieve information through so called side-channels. The information can be used to circumvent security checks in the microprocessor to access, e.g., passwords and encryption keys. This has proven to be an "Achilles heel for computer security." The work to find methods to prevent such

attacks has been intense, involving people and institutions all over the world. Finally, we now have an efficient solution to the problem.

Different Speculation

Christos Sakalis, Stefanos Kaxiras, Alberto Ros, Alexandra Jimborean, and Magnus Själander have been working together to come up with a new solution.

"We have developed a new method that completely hides the speculation," says Stefanos Kaxiras from the Uppsala Architecture Research Team at Uppsala University.

The proposed method delays part of the speculation and uses another form of speculation to predict the expected value. This form of speculation is completely invisible.

All this is achieved without reducing the performance of the processors more than 11 percent and with only a 7 percent energy usage increase. An earlier proposed solution reduced the performance of the processor by 46 percent and increased the energy usage by 51 percent.

"Our solution requires relatively small modifications to existing processor designs, which in combination with the low performance reduction makes our method practical to employ in future microprocessors," says Magnus Själander from NTNU's Department of Computer Science.

More information: Efficient Invisible Speculative Execution through Selective Delay and Value Prediction. The 46th Annual International Symposium on Computer Architecture (ISCA '19), doi.org/10.1145/3307650.3322216