New Spectre cyberthreat evades patches

July 27 2018, by Holly Ober

Credit: CC0 Public Domain

"Spectre" was a prescient name for the processor vulnerability that takes advantage of speculative execution. Since its initial discovery in January, 2018, at least three variants of the attack have been found.

Now, a group of computer scientists in the Bourns College of Engineering at UC Riverside that has been involved in some of these discoveries has unveiled a potentially unstoppable version called

SpectreRSB.

SpectreRSB appears immune to known defenses against other Spectre variants including Retpoline and Intel's microcode patches under some attack scenarios.

All modern computer processors use a process known as speculative execution to complete operations with greater speed. The processor predicts what the next step will be and executes that step when the information to determine that step is not available.

It works similarly to assembly lines in factories. In programs, most instructions are executed one by one, making the pipeline operation simple. However, some instructions challenge the pipeline: we do not know where the next instruction is coming from until the pipeline finishes executing the previous instruction.

It's as if a Jeep is ready to roll off the assembly line and the workers have to wait until it is completely assembled before they discover what the next car to assemble will be, causing the pipeline to stop working.

To get around these delays, when the computer has finished an operation but doesn't have instructions what to do next, speculation avoids stalling the pipeline. If the processor predicts correctly, it keeps the pipeline busy doing useful work. If incorrect, it dumps the data and restarts the computation. The pipeline would have been idle anyway, and no performance is lost.

Another way to think of it is as a guest who asks you to bring them a soda. You open the fridge and see several kinds. Rather than wait for instructions from your guest, you predict they will want cola. If you're right, you've saved effort. If wrong, you go back to the fridge and get the right one.

Speculative execution, combined with related techniques such as out-of-order processing, result in several-fold increase in processor performance.

During speculation, the processor may momentarily access regions of its memory that are usually securely segregated from all the computer hardware. Computer designers thought this to be safe, since any such access would be discarded, leaving no exposure. But the speculatively accessed data leaves a trail that can be used to expose this data.

When the first Spectre variant was discovered earlier in 2018, Google developed a patch called Retpoline that secures regions where speculative decisions are made, known as branch predictors. Intel also created patches that prevent, or give programmers tools to prevent, some variants of the attacks.

The new variant reported by the UC Riverside group exploits the return stack buffer, which stores addresses the processor will need to return to after it has finished an operation.

SpectreRSB works by inserting the wrong return address, or deleting addresses, in the return stack buffer. By controlling the return addresses, an attacker can also control the speculation addresses, pointing them to secret information.

The patches available to date protect speculation only on the branch predictors. Because SpectreRSB enters through the return stack buffer instead of the branch predictors, the available patches might not be able stop it.

The paper recommends that all processors incorporate a patch known as RSB refilling, which inserts a dummy address into the stack buffer to thwart the attack. Intel's Core i7 processors starting from Skylake, called

Skylake+, incorporate RSB refilling but older models and different processor lines, such as Intel's Xeon which are the primary platform used on Intel-based cloud computing systems and servers, do not, and remain vulnerable to SpectreRSB.

Spectre-class attacks require sophisticated attackers who already have access to run on the victim machine. The patches protect against this vulnerability.

The paper's authors are doctoral students Esmaiel Mohammadian Koruyeh and Khaled Khasawneh, along with Chengyu Song and Nael Abu-Ghazaleh, who are both professors of computer science and engineering. Their paper, "Spectre Returns! Speculation Attacks using the Return Stack Buffer," is available at arxiv.org and will appear in the Usenix Security workshop on offensive technologies in August 2018.

In 2016, Abu-Ghazaleh and collaborators Dmitry Ponomarev from Binghamton University, Dmitry Evtyushkin from College of William and Mary, and Ryan Riley from Carnegie Mellon University characterized the vulnerabilities of the branch predictor which are at the core of Spectre variant 2. Earlier in 2018 the group identified branchscope, an attack that enables attackers to control a different component of the branch predictor. To counter these threats Abu-Ghazaleh, Ponomarev, Evtyushkin, and Chengyu Song developed SafeSpec, a design approach for future processors to eliminate speculation vulnerabilities.

More information: Spectre Returns! Speculation Attacks using the Return Stack Buffer: arxiv.org/pdf/1807.07940.pdf

Provided by University of California - Riverside