Researchers discover new security flaws in Intel processors

May 15 2019

Following the discoveries of Meltdown and Spectre, Michael Schwarz, Daniel Gruss and Moritz Lipp (from left) have uncovered two serious new security flaws in computer processors. Credit: Lunghammer – TU Graz

ZombieLoad and Store-to-Leak Forwarding are two new exploits that have just been announced by TU Graz security researchers Daniel Gruss, Moritz Lipp, Michael Schwarz and an international team.

The three computer scientists, along with TU Graz Professor Stefan

Mangard, were part of the team that discovered the serious security flaws Meltdown and Spectre last year.

ZombieLoad

ZombieLoad uses a similar approach to Meltdown. In order to enable faster processing, computer systems prepare several tasks in parallel before discarding the ones that are either not needed or for which the necessary permissions have not been given. Due to the way processors are designed, they always have to pass on data, even if it is not correct.

The check for permission only happens once sensitive processing steps, which depend on assumptions made by the computer system, have already been prepared. "In the split second between the command and the check, using this new form of attack, we can see the pre-loaded data from other programs," explains Gruss. In other words, the researchers can read what the computer is currently processing.

The KAISER patch developed by a team at TU Graz provided a simple solution for Meltdown, which affected the speed of a computer. Coming up with a solution for ZombieLoad attacks could be more difficult, says Gruss. "Every CPU has multiple cores, and each of these cores is also split in two. This means several programs can run simultaneously. We think that one of these two parts of each core has to be disabled." That would mean a 50 percent drop in performance. Or in clouds, which are also vulnerable to this method of attack, 50 percent fewer potential users on the same hardware.

All processors manufactured by Intel between 2012 and the beginning of 2018 are affected.

Store-to-leak forwarding

Store-to-leak forwarding also reads pre-loaded data by exploiting the efficient way in which computer processors function. "The computer assumes that I want to use the data which I have just written to the processor again right away. So it keeps it in the buffer for faster access," explains Gruss. This functionality can also be used to determine the architecture of the computer processor and find the exact location where the operating system is running. "If I know exactly where the processor is running the operating system, then I can launch targeted attacks against flaws in the operating system."

New updates urgently required

The researchers immediately reported their discoveries to Intel, which has been working on a solution ever since. "Computer users should install all new updates without delay to ensure that their systems are protected," recommends Gruss.

More information: More information about Zombieload: zombieload.com/zombieload.pdf

More information about Store-to-Leak Forwarding: cpu.fail/store-to-leak.pdf

Provided by Graz University of Technology

Citation: Researchers discover new security flaws in Intel processors (2019, May 15) retrieved 25 April 2024 from https://phys.org/news/2019-05-flaws-intel-processors.html