TechXplore

New CPU security loophole: Analysis of energy consumption allows data theft

August 2 2023

Andreas Kogler from the Institute of Applied Information Processing and Communications at Graz University of Technology. Credit: Lunghammer–TU Graz

Researchers at TU Graz and the Helmholtz Center for Information

Security have discovered a novel security gap in all common main processors (CPUs) of computers that can hardly be mitigated. CPUs are designed to run multiple applications simultaneously. This is beneficial for efficiency, but poses a security risk.

Researchers at TU Graz and the Helmholtz Center for Information Security have found a novel method that allows attackers to read data from the memory of CPUs by analyzing the processor's energy consumption. They call this method of attack "Collide+Power."

In a Collide+Power attack, the attackers store a data package on a segment of the CPU. In a second step, malicious code causes the attacker's own data to be overwritten ("collide") with the data the attackers are targeting. This overwriting consumes power—the more the two data packages differ from each other, the more power is consumed. The entire process is then repeated thousands of times, each time with minimally different attacker data packages to be overwritten. Finally, the targeted data package can be derived from the slightly different power consumptions that occur each time during this process.

Although the power consumption of CPUs cannot be read without administrator rights, attackers can bypass this security barrier: In addition to increased power consumption, overwriting the data packets also leads to delays in the computing processes on the attacked processor. These delays can be used to determine the power consumption and, in turn, the target data.

"All computers with modern CPUs are affected by this security weakness," says Andreas Kogler from the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology. "And this security risk is very difficult to fix."

However, a Collide+Power attack is currently still extremely timeconsuming: Due to the countless overwrite operations, the data theft requires at least 16 hours per bit, in other scenarios even up to a year. However, future leaps in technological development could significantly reduce the time required, making Collide+Power attacks an everyday security risk.

In principle, the issue of so-called power side channels has been known for a long time and is one of the research topics of Stefan Mangard, who leads the IAIK at the TU Graz and has co-authored the Collide+Power study. However, the research group of Daniel Gruss at IAIK only recently discovered that power measurements on modern computers do not require expensive measurement hardware and physical access, but can be done directly from software.

The major chip manufacturers have been informed about the Collide+Power risk in advance and have adjusted their guidelines accordingly. For the general public, the researchers have set up a website describing the security gap in detail: collidepower.com

More information: Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels. www.usenix.org/conference/usen … /presentation/kogler

Provided by Graz University of Technology

Citation: New CPU security loophole: Analysis of energy consumption allows data theft (2023, August 2) retrieved 9 May 2024 from https://techxplore.com/news/2023-08-cpu-loophole-analysis-energy-consumption.html