Computer security flaws reveal faster isn't necessarily better

Researchers discover 20-year-old security bugs in CPU chips, highlighting the need for safer computers.

In the drive for better performing computers, manufacturers' traditional focus on speed has come at the expense of security. Highlighting just how vulnerable today's computers really are, two fundamental security flaws were recently discovered in computer processors. Called Meltdown and Spectre, the flaws could allow users unauthorised access to personal data stored in the most protected part of your computer system.

The two bugs were independently found by four different research groups, one of which was a team of researchers from Graz University of Technology, Austria. Supported with EU-funding for the project SOPHIA, the Graz team played a key role in the discovery of Meltdown and Spectre.

A Meltdown in the works

Both bugs allow access to unauthorised information, but they achieve this in different ways. Meltdown does this by overcoming memory isolation, which allows malicious programmes to read ordinarily non-accessible parts of a computer's memory. This is made possible by a performance feature called 'out-of-order execution'. To speed up a process, "modern processors run operations out-of-order i.e., they look ahead and schedule subsequent operations to idle execution units of the processor," the Graz team and other researchers explain in a paper posted on the Cornell University Library website.

"The root cause of Meltdown," the authors report, "is the hardware. The attack is independent of the operating system, and it does not rely on any software vulnerabilities." All Intel processors that implement out-of-order execution are affected. Fortunately, the researchers have developed software patches against Meltdown.

The Spectre in the system

Processors conducting an out-of-order execution may reach a branch where the future direction depends on instructions that have yet to be executed. To maximise performance, processors then predict the path a programme is likely to follow and prematurely execute the instructions in them. It's the vulnerability inherent in this process that makes Spectre attacks possible. Spectre allows data to be stolen from the memory of other applications running on a machine by breaking the isolation between them.

In a separate study to which the Graz researchers also contributed, the authors describe how this class of attacks works: "At a high level, Spectre attacks trick the processor into speculatively executing instructions sequences that should not have executed during correct program execution." These speculative operations result in confidential information being leaked.

Spectre poses a more serious problem for the industry, since it's harder to fix and affects not only Intel, but AMD and ARM processors, too.

Although only recently discovered, the flaws have existed since the mid-1990s. A worrying thought, since these vulnerabilities may potentially have been exploited for decades by some without anyone knowing. Stefan Mangard, lead researcher for SOPHIA, highlights the need for more secure computers in an interview posted on the European Research Council website: "In today's environment of increasing attacks on computer systems […], we need to accept security as a major design criterion. I hope the discovery of the Meltdown and Spectre flaws will trigger a new way of thinking about computer design."

SOPHIA (Securing Software against Physical Attacks) is continuing its research into ways to execute software securely and efficiently in the presence of physical attacks on all kinds of computing devices.

For more information, please see:
CORDIS project webpage

Source: Based on project information and media reports

Related information

Projects	SOPHIA - Securing Software against Physical Attacks
Programmes	H2020-EU.1.1.
Countries	Austria

Subjects

Information Processing and Information Systems

Last updated on 2018-05-04