Yet another New security flaw with Intel processors

BY TIM SANDLE TECHNOLOGY LISTEN | PRINT

Saarburg - A new security flaw has been detected by German researchers in relation to Intel. This comes on the back of earlier concerns from January and March 2018. The flaw means that passwords can potentially be stolen.

For several decades, malicious software has been able to abstract data from the inner workings of operating systems and hardware. Although significant research resources have been spent on assuring software security, vulnerabilities remain.

Earlier in 2018, research indicated a security flaw with Intel processors. Since the resolution of this, technologists working at the CISPA Helmholtz

Centre (Saarbrücken, Germany) have identified a new security gap. As EE News reports, researchers described the new flaw enables an "inverse spectre attack".

READ MORE: Ford introduces 'exosuits' into 15 factories

With the earlier issues, in January 2918, computer firms needed to fix the Meltdown and Spectre flaws that, under a given set of conditions, would allow attackers to steal data. Later on, a new concern was raised in relation to a new bug called Spectre Next Generation. Spectre NG is similar to the previously patched flaws, allowing third parties to extract sensitive information such as passwords stored in memory.

Now a new threat has arisen. According to Giorgi Maisuradze and Professor Dr. Christian Rossow a ret2spec (return-to-speculation) vulnerability with the chips allows for would-be attackers to read data without authorization.

According to Professor Rossow: “The security gap is caused by CPUs predicting a so-called return address for runtime optimization.”

The implications of this are: “If an attacker can manipulate this prediction, he gains control over speculatively executed program code. It can read out data via side channels that should actually be protected from access.

This means, in essence, that malicious web pages could interpret the memory of the web browser in order to access and copy critical data. Such data would include stored passwords.

ICYMI: Canada challenges women to lead the Cleantech future

This is not a new vulnerability, because all Intel processors manufactured over the past ten years are potentially affected by the vulnerabilities. While

the research has focused on Intel, it stands that similar attack mechanisms will probably exist for ARM and AMD processors.

The new vulnerability will be presented to the ACM Conference on Computer and Communications Security, which takes place in Toronto in October. In the meantime a white paper has been issued, titled “ret2spec: Speculative Execution Using Return Stack Buffers.”

More about intel, chips, processors, cybersecurity