# Intel will equip anti-malware system directly into the CPU

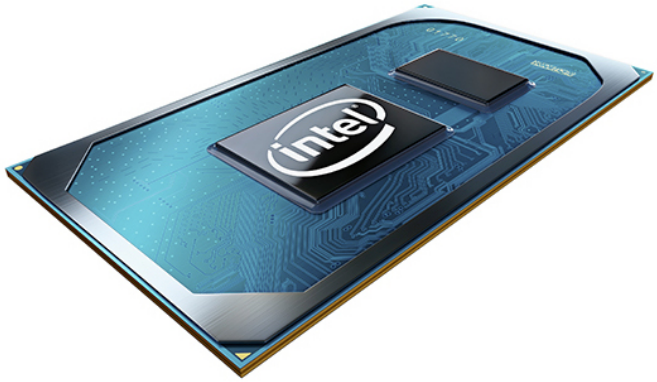
Control-Flow Enforcement technology is expected to debut with Tiger Lake microarchitecture.

Hacking is a reciprocal game in which an attacker finds a technique to infiltrate the system, the defender has to devise a countermeasure to stop that technique, and then the hacker is back. come up with a new way to bypass the system's security barrier. Yesterday, Intel announced plans to integrate a "shield" directly into its CPUs - a barrier designed to prevent software vulnerabilities that can execute malicious code on infected computers. .

Control-Flow Enforcement Technology, or CET, shows a fundamental change in the way microprocessors execute instructions from applications such as web browsers, email managers, or PDF readers. Developed by Intel and Microsoft, CET is designed to prevent a technique called "return-oriented programming" (ROP) used by hackers to bypass anti-vulnerability solutions. introduced by software developers about a decade ago. Although Intel first announced it would deploy CET in 2016, it was Monday that the company officially announced its Tiger Lake CPU microarchitecture would be the first microarchitecture equipped with this technology.

ROP is the response of those who take advantage of software vulnerabilities to security solutions such as "Executable Space Protection" and "randomize the address space layout", which has been included in Windows, macOS and Linux less than 2 decades ago. These defensive solutions are designed to significantly reduce the damage that software vulnerabilities can cause, through making changes in system memory to prevent malicious code execution. Even when successfully taking advantage of buffer overflow errors or other vulnerabilities, the exploit behavior will only cause the system or application to crash, not to interfere violently into the system.

ROP allows attackers to retake the upper hand. Instead of using malicious code written by an attacker, ROP attacks will take advantage of functions that normal applications, or routine operating system tasks, place into a known memory area. comes with the name "stack". The word "return" in the ROP implies the use of the RET instruction, which plays a central role in the code stream rearrangement.



**Very effective**

Alex Ionescu, an experienced Windows security expert and deputy technical director at security firm CrowdStrike, often says that if a typical program is like a building made of Lego blocks arranged in a particular sequence, the ROP uses the same Lego blocks but in a different sequence. Thanks to that, ROP can turn a building into a spaceship. This technique is capable of bypassing anti-malware solutions because it uses code that is in memory already licensed by the system to execute.

CET brings changes in the CPU, creating a new stack called a "control stack". This stack cannot be edited by an attacker and does not store any data. It contains the return addresses of Lego blocks that are already in the stack. Thus, even if the attacker has changed a return address in the data stack, the control stack still retains the address as it was originally. The microprocessor can detect this and prevent execution.

" *Because there is no effective software solution before ROP, CET will be very effective in detecting and preventing this type of intrusion,* " Ionescu said. " *Previously, operating systems and security solutions had to guess or infer whether ROP had occurred, or conduct forensic analysis, or detect signs / effects in phase 2 of vulnerability exploits* ".

CET not only has a defensive ability against ROP, it also provides a range of other protection solutions, some of which can prevent exploitation techniques such as "jump-oriented programming". ), "call-oriented programming" . However, blocking ROP is one of the most notable points of CET.

Intel has integrated other security functions into its CPUs, but the results are not high. For example, Intel SGX (short for Software Guard eXtension), is designed to create impenetrable protected pieces of memory for high-security functions such as generating encryption keys. Or "Coverged Security and Management Engine", briefly called "Management Engine" (ME), a subsystem inside Intel CPUs and chipsets, including a range of sensitive functions such as the Trusted Platform Module built into the firmware for chip encryption, UEFI BIOS firmware validation, and Microsoft System Guard and BitLocker.

However, the constant security flaws discovered deep within the CPU features have made them a prime target for countless attack techniques over the years. The most recent SGX vulnerability was discovered only last week!

Some argue that CET will also be easily defeated, or worse, put users at risk of being affected by attacks that cannot be performed before CET is introduced. But Joseph Fitzpatrick, a hardware hacker and researcher at SecuringHardware.com, said he was optimistic that CET would do better than that. According to him, a major difference between CET and SGX or ME is that the two previous solutions were additional security features, while CET was a feature that existed on the CPU from the beginning. ME basically adds a management layer outside the operating system. SGX adds operating modes that cannot theoretically be manipulated by a controlled code or operating system.CET simply added mechanisms to prevent normal operations - returning intact addresses removed from the stack and jumping out / into inappropriate locations in the program code - successfully implemented. . If CET fails to do so, normal activity continues. It does not allow an attacker any additional access.

Once CET integrated CPUs are on the market, this "shield" will work, but only if the processor runs an operating system that supports CET. Windows 10 version 2004 released last month already supports this feature. Intel has not yet revealed the launch time of Tiger Lake CPU. While the new protection solution could provide users with an important new tool, Ionescu and fellow researcher Yarden Shafir have found a way to bypass it. It will probably take less than a decade for CET to be defeated like previous solutions!