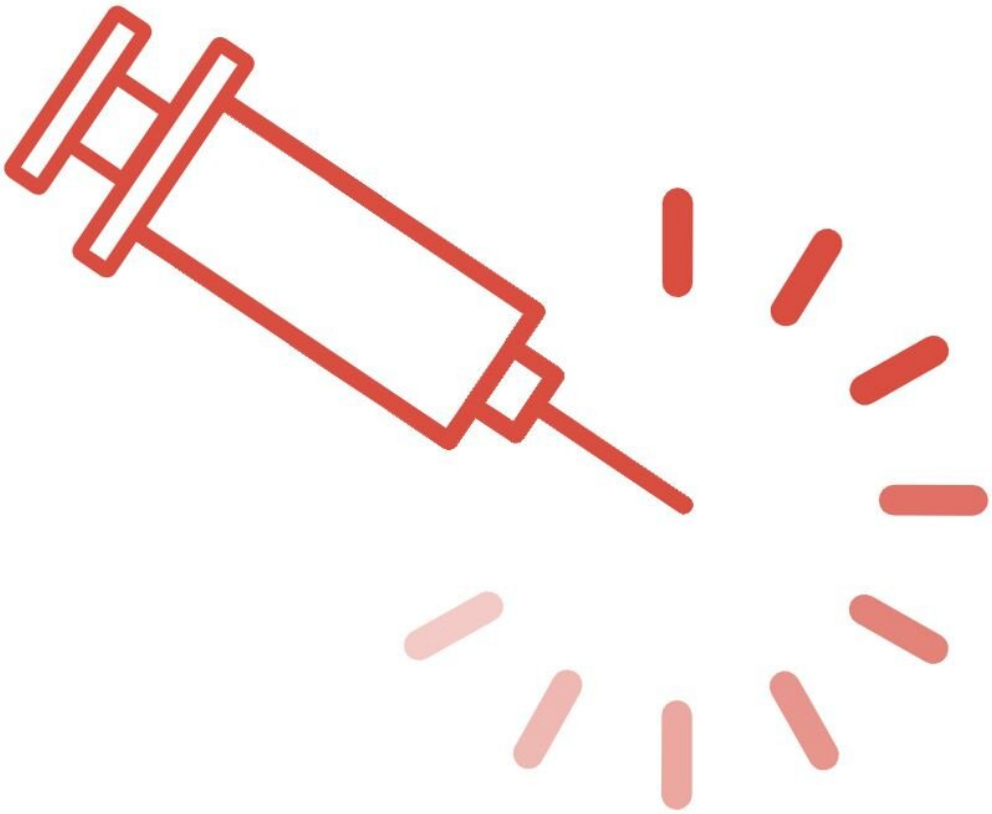
LVI: Intel processors still vulnerable to attack, study finds

March 10 2020



The Load Value Injection attack on Intel processors uses the vulnerability of SGX enclaves to smuggle or 'inject' attacker-controlled data into a software program that the victim is running on their computer. Credit: KU Leuven

Computer scientists at KU Leuven have once again exposed a security flaw in Intel processors. Jo Van Bulck, Frank Piessens, and their colleagues in Austria, the United States, and Australia gave the manufacturer one year's time to fix the problem.

In the past couple of years, Intel has had to issue quite a few patches for vulnerabilities that computer scientists at KU Leuven have helped to expose, including Plundervolt, Zombieload and Foreshadow. "All measures that Intel has taken so far to boost the security of its processors have been necessary, but they were not enough to ward off our new attack," says Jo Van Bulck from the Department of Computer Science at KU Leuven.

Like the previous attacks, the new technique—dubbed Load Value Injection—targets the 'vault' of computer systems with Intel processors: SGX enclaves.

"To a certain extent, this attack picks up where our Foreshadow attack of 2018 left off. A particularly dangerous version of this attack exploited the vulnerability of SGX enclaves so that the victim's passwords, medical information, or other sensitive information was leaked to the attacker. Load Value Injection uses that same vulnerability, but in the opposite direction: The attacker's data are smuggled—'injected'—into a software program that the victim is running on their computer. Once that is done, the attacker can take over the entire program and acquire sensitive information, such as the victim's fingerprints or passwords."

The vulnerability was already discovered on 4 April 2019. Nevertheless, the researchers and Intel agreed to keep it a secret for almost a year. Responsible disclosure embargoes are not unusual when it comes to cybersecurity, although they usually lift after a shorter period of time. "We wanted to give Intel enough time to fix the problem. In certain scenarios, the vulnerability we exposed is very dangerous and extremely

difficult to deal with, because this time, the problem did not just pertain to the hardware: The solution also had to take software into account. Therefore, hardware updates like the ones issued to resolve the previous flaws were no longer enough. This is why we agreed upon an exceptionally long embargo period with the manufacturer."

"Intel ended up taking extensive measures that force the developers of SGX enclave software to update their applications. However, Intel has notified them in time. End-users of the software have nothing to worry about: they only need to install the recommended updates."

"Our findings show, however, that the measures taken by Intel make SGX enclave software up to 2 to even 19 times slower."

What are SGX enclaves?

Computer systems are made up of different layers, making them very complex. Every layer also contains millions of lines of computer code. As this code is still written manually, the risk for errors is significant. If such an error occurs, the entire computer system is left vulnerable to attacks. You can compare it to a skyscraper: If one of the floors becomes damaged, the entire building might collapse.

Viruses exploit such errors to gain access to sensitive or personal information on the computer, from holiday pictures and passwords to business secrets. In order to protect their processors against this kind of intrusion, Intel introduced an innovative technology in 2015: Intel Software Guard eXtensions (Intel SGX). This technology creates isolated environments in the computer's memory, so-called enclaves, where data and programs can be used securely.

"If you look at a computer system as a skyscraper, the enclaves form a vault," researcher Jo Van Bulck explains. "Even when the building

collapses, the vault should still guard its secrets—including passwords or medical data."

The technology seemed watertight until August 2018, when researchers at KU Leuven discovered a breach. Their attack was dubbed Foreshadow. In 2019, the Plundervolt attack revealed another vulnerability. Intel has released updates to resolves both flaws.

The vulnerability was first exposed by Jo Van Bulck and Frank Piessens at KU Leuven. The researchers also wrote a paper about their discovery, for which they collaborated with colleagues from TU Graz (Austria), Worcester Polytechnic Institute and the University of Michigan (United States), the University of Adelaide and Data61 (Australia). In May 2020, the paper "LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection" by Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yuval Yarom, Berk Sunar, Daniel Gruss, and Frank Piessens will be presented at the IEEE Symposium on Security and Privacy.

More information: lviattack.eu/

LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection, IEEE Symposium on Security and Privacy, 2020.

Provided by KU Leuven

Citation: LVI: Intel processors still vulnerable to attack, study finds (2020, March 10) retrieved 18 April 2024 from https://techxplore.com/news/2020-03-intel-processors-vulnerable.html