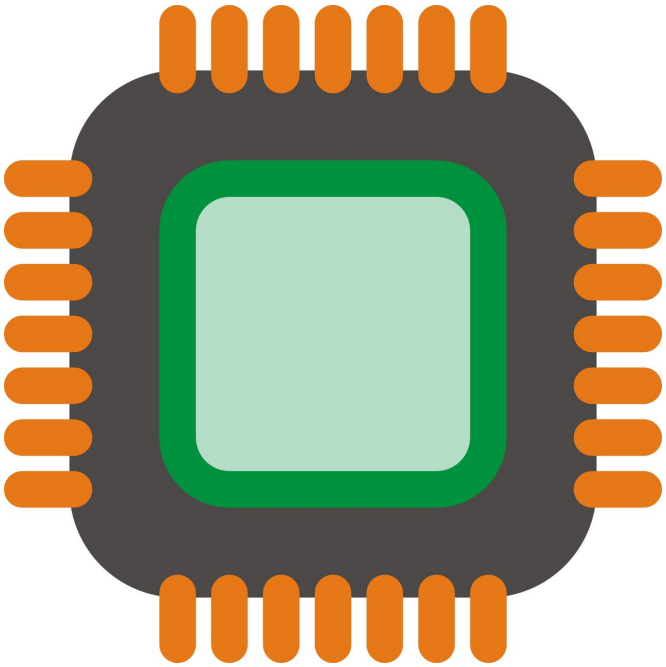
# Intel processor vulnerability could put millions of PCs at risk

14 August 2018



Credit: CC0 Public Domain

A newly discovered processor vulnerability could potentially put secure information at risk in any Intel-based PC manufactured since 2008. It could affect users who rely on a digital lockbox feature known as Intel Software Guard Extensions, or SGX, as well as those who utilize common cloud-based services, a new report says.

Researchers at the University of Michigan, the Belgian research group imec-Distrinet, Technion Israel Institute of Technology, the University of Adelaide and Data61 identified the SGX security hole, called Foreshadow, in January and informed Intel. That led Intel to discover its broader potential in the cloud. This second variant, Foreshadow-NG, targets Intel-based virtualization environments that cloud computing providers like Amazon and Microsoft use to create thousands of virtual PCs on a single large server.

Intel has released software and microcode updates to protect against both varieties of attack. Cloud providers will need to install the updates to guard their machines. On an individual level, the owners of every SGX-capable Intel PC manufactured since 2016 will need an update to protect their SGX. Some of these updates will be installed automatically while others will need to be installed manually, depending on how a machine is configured.

To be demonstrated Aug. 16 at the Usenix Security Symposium in Baltimore, the flaw is similar to Spectre and Meltdown, the hardware-based attacks that shook the computer security world in early 2018. Researchers were able to break several security features that are present in most Intel-based machines.

"SGX, virtualization environments and other similar technologies are changing the world by enabling us to use computing resources in new ways, and to put very sensitive data on the cloud—medical records, cryptocurrency, biometric information like fingerprints," said Ofir Weisse, graduate student research assistant in computer science and engineering at U-M and an author on the paper presented at Usenix. "Those are important goals, but vulnerabilities like this show how important it is to proceed carefully."

**The attacks and their targets**

The Software Guard Extensions feature that the Foreshadow demonstration attack targets is not widely used today. Used by just a handful of cloud providers and a few hundred thousand customers, it's lying dormant on the vast majority of computers equipped with it, and those machines are not vulnerable at this time. That said, the researchers caution that the threat will grow with the use of the product.

"As long as users install the update, they'll be fine.

And in fact, the vast majority of PC owners don't use SGX, so it's not likely to become a major problem right now," said Thomas Wenisch, a U-M computer science and engineering associate professor and an author on the paper. "The real danger lies in the future, if SGX becomes more popular and there are still large numbers of machines that haven't been updated. That's why this update is so important."

SGX creates a digital lockbox called an "secure enclave" in a machine, keeping the data and applications inside isolated from the rest of the machine. Even if a security vulnerability compromises the entire machine, the data protected by SGX is supposed to remain inaccessible to everyone but the owner of the data.

The main application of SGX is to enable the processing and storage of sensitive information, like proprietary business information or health data, at remote third-party data centers where not even data center employees should be able to access the protected data. SGX can also be used for controlling the distribution of copyrighted digital content, for example allowing a movie to be viewed only on specific machines.

Foreshadow breaks SGX's lockbox, enabling an attacker to read and modify the data inside. While this is not the first attack to target SGX, it is the most damaging thus far.

"Previous work could get some of the data some of the time. Foreshadow gets most of the data most of the time," said Daniel Genkin, a U-M assistant professor of computer science and engineering and an author on the paper. "In addition to reading the data, Foreshadow also extracts what's called an attestation key. That key enables attackers to masquerade as a secure machine and trick people into sending secret data to it."

The second variant, Foreshadow-NG, breaks the digital wall that keeps individual cloud customers' virtual PCs isolated from one another on large servers. This could enable a malicious virtual machine running in the cloud to read data belonging to other virtual machines. The virtualization code is present in every Intel-based computer manufactured since 2008.

"Foreshadow-NG could break the fundamental security properties that many cloud-based services take for granted," said Baris Kasikci, a U-M assistant professor of computer science and engineering and an author on the paper.

**How the attacks work**

Both variants of the vulnerability gain access to the victim machine using what's known as a side channel attack. These attacks infer information about a system's inner workings by observing patterns in seemingly innocuous information—how long it takes the processor to access the machine's memory, for example. This can be used to gain access to the inner workings of the machine.

The attack then confuses the system's processor by exploiting a feature called speculative execution. Used in all modern CPUs, speculative execution speeds processing by enabling the processor to essentially guess what it will be asked to do next and plan accordingly.

The attack feeds in false information that leads speculative execution into a series of wrong guesses. Like a driver following a faulty GPS, the processor becomes hopelessly lost. This confusion is then exploited to cause the victim machine to leak sensitive information. In some cases, it can even alter information on the victim machine.

While these vulnerabilities were caught before causing major damage, they expose the fragility of secure enclaves and virtualization technologies says Ofir Weisse, the graduate student research assistant involved in the work. He believes that the key to keeping technologies secure lies in making designs open and accessible to researchers so that they can identify and repair vulnerabilities quickly.

Foreshadow is detailed in a paper titled "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution."

**More information:** More information about Foreshadow is available at ForeshadowAttack.com.

Provided by University of Michigan