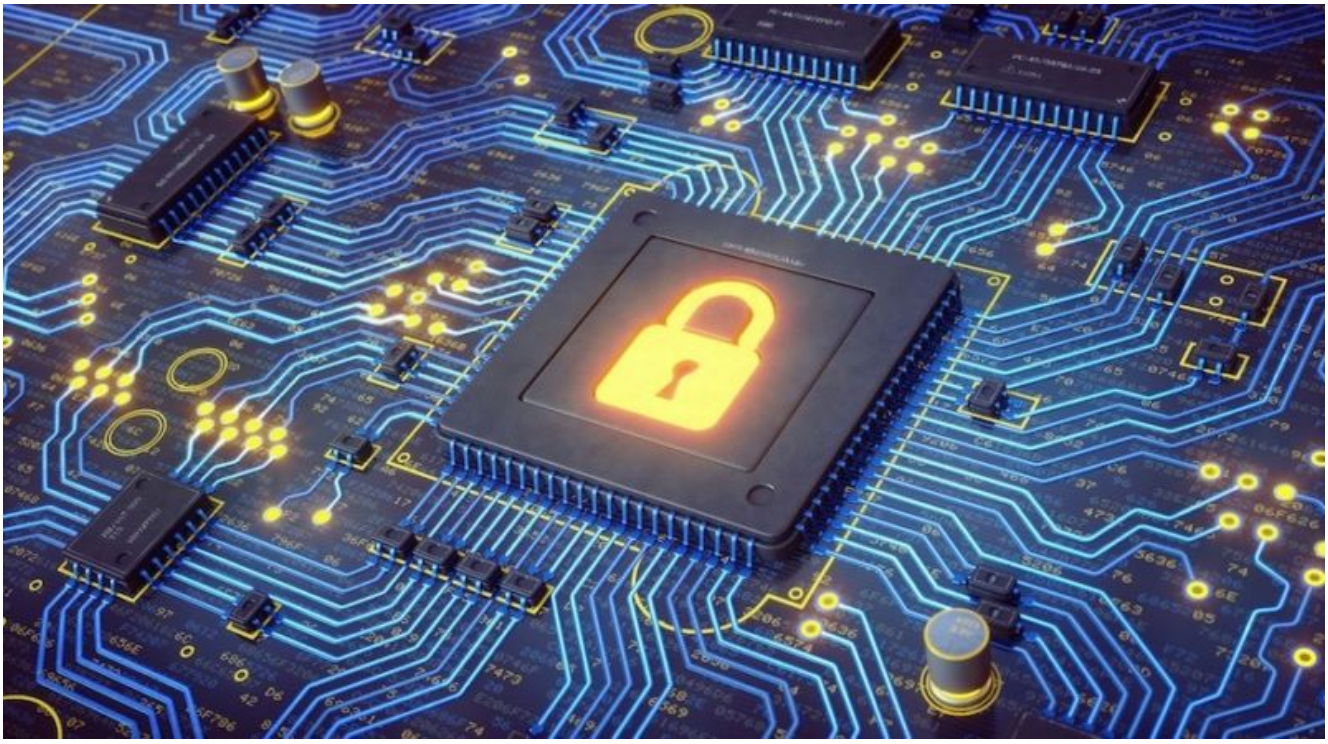
Intel’s SGX coughs up crypto keys when scientists tweak CPU voltage



reader comments

48 with 44 posters participating

Share this story

To counter the growing sophistication of computer attacks, Intel and other chipmakers have built digital vaults into CPUs to segregate sensitive computations and secrets from the main engine computers use. Now, scientists have devised an attack that causes the Software Guard Extensions—Intel’s implementation of this secure CPU environment—to divulge cryptographic keys and induce potentially dangerous memory errors.

Plundervault, as the attack has been dubbed, starts with the assumption that an attacker is able to run privileged software

on a targeted computer. While that's a lofty prerequisite, it's precisely the scenario Intel's SGX feature is designed to protect against. The chipmaker bills SGX as a private region that uses hardware-based memory encryption to isolate sensitive computations and data from malicious processes that run with high privilege levels. Intel goes as far as saying that "Only Intel SGX offers such a granular level of control and protection."

But it turns out that subtle fluctuations in voltage powering the main CPU can corrupt the normal functioning inside the SGX. By subtly increasing or decreasing the current delivered to a CPU—operations known as "overvolting" and "undervolting"—a team of scientists has figured out how to induce SGX faults that leak cryptographic keys, break integrity assurances, and potentially induce memory errors that could be used in other types of attacks. While the exploit requires the execution of privileged code, it doesn't rely on physical access, raising the possibility of remote attacks.

Surgical strikes

The breakthrough leading to these attacks was the scientists' ability to use previous research into the undocumented model-specific register inside the x86 instruction set to abuse the dynamic voltage scaling interface that controls the amount of voltage used by a CPU. Also noteworthy is surgically controlling the voltage in a way that introduces specific types of attacks.

In a paper published on Tuesday, the scientists wrote:

> *In this paper, we present Plundervolt, a novel attack against Intel SGX to reliably corrupt enclave computations by abusing privileged dynamic-voltage-scaling interfaces. Our work builds on reverse engineering efforts that revealed which ModelSpecific Registers (MSRs) are used to control the*

> *dynamic voltage scaling from software [64, 57, 49]. The respective MSRs exist on all Intel Core processors. Using this interface to very briefly decrease the CPU voltage during a computation in a victim SGX enclave, we show that a privileged adversary is able to inject faults into protected enclave computations. Crucially, since the faults happen within the processor package, i.e., before the results are committed to memory, Intel SGX's memory integrity protection fails to defend against our attacks. To the best of our knowledge, we are the first to practically showcase an attack that directly breaches SGX's integrity guarantees. In summary, our main contributions are:*
>
> *1) We present Plundervolt, a novel software-based fault attack on Intel Core x86 processors. For the first time, we bypass Intel SGX's integrity guarantees by directly injecting faults within the processor package.*
>
> *2) We demonstrate the effectiveness of our attacks by injecting faults into Intel's RSA-CRT and AES-NI implementations running in an SGX enclave, and we reconstruct full cryptographic keys with negligible computational efforts.*
>
> *3) We explore the use of Plundervolt to induce memory safety errors into bug-free enclave code. Through various case studies, we show how in-enclave pointers can be redirected into untrusted memory and how Plundervolt may cause heap overflows in widespread SGX runtimes.*
>
> *4) Finally, we discuss countermeasures and why fully mitigating Plundervolt may be challenging in practice.*

The researchers privately reported the vulnerability to Intel ahead of Tuesday's publication. In response, Intel has released a microcode and BIOS updates that mitigate attacks by locking voltage to the default settings. Readers using Intel Core processors from Skylake onward and some platforms based

on Xeon E should install INTEL-SA-00289 once it becomes available from respective computer makers. The vulnerability is tracked as CVE-2019-11157.

https://arstechnica.com/?p=1631159