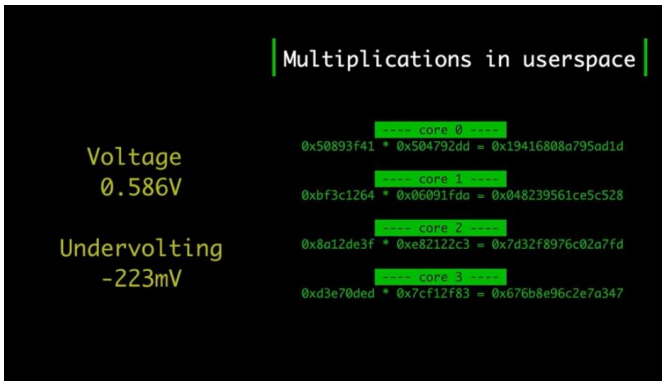
Research shows how Plundervolt could mess with Intel CPUs

13 December 2019, by Nancy Cohen



Undervolting can bring trouble Intel would not care to endure at all. Fortunately, the latest research warning signals have won Intel's attention and they are addressing the situation.

Cutting to the chase: Plundervolt. "Modern processors are being pushed to perform faster than ever before—and with this comes increases in heat and power consumption," said a team of researchers on their own Plundervolt website page, with the subhead "How a little bit of undervolting can cause a lot of problems."

Plundervolt is the name of a type of attack they explored.

Many chip manufacturers allow frequency and voltage to be adjusted as and when needed, they continued, but more than that "they offer the user the opportunity to modify the frequency and voltage through privileged software interfaces. With Plundervolt we showed that these software interfaces can be exploited to undermine the system's security."

In the conclusion section of their research paper, the group stated that "our work provides further evidence that the enclaved execution promise of outsourcing sensitive computations to untrusted remote platforms creates new and unexpected attack surfaces that continue to be relevant and need to be studied further."

They said that "With Plundervolt we showed that these software interfaces can be exploited to undermine the system's security." Plundervolt specifically targets Intel Software Guard eXtensions (SGX).

"We were able to corrupt the integrity of Intel SGX on Intel Core processors by controling the voltage when executing enclave computations." (Intel SGX is a set of security-related instruction codes built into Intel CPUs.)

Who is this team? The answer is not just one security business but a research team across borders: Kit Murdock, David Oswald, Flavio D Garcia (The University of Birmingham); Jo Van Bulck, Frank Piessens (imec-DistriNet, KU Leuven); and Daniel Gruss (Graz University of Technology).

Before that, Navjivan Pal, in his final year project at the University of Birmingham under Oswald's supervision, had looked at the potential of using undervolting for faulting (non-SGX) computations.

Catalin Cimpanu in *ZDNet* reported what Oswald at the University of Birmingham had told *ZDNet*. "The undervolting induces bit flips in CPU instructions itself, such as multiplications or AES rounds (AES-NI)."

No, even Intel SGX's memory encryption/authentication technology cannot protect against Plundervolt, said the investigators.

In addition to extraction of cryptographic keys, Plundervolt, they found, can cause "memory safety misbehaviour in certain scenarios." Out-of-bounds

accesses may arise when an attacker faults multiplications emitted by the compiler for array element indices or pointer arithmetic, they said. "Plundervolt can break the processor's integrity guarantees, even for securely written code."

The Plundervolt site carried a list of questions and answers, and one of the questions was, "Should I now throw away my CPU or stop using SGX altogether?" Their answer was, "No, definitely not. If you are not using SGX, no actions are required. If you are using SGX, it suffices to apply the microcode update provided by Intel to mitigate Plundervolt."

Plundervolt was first reported in June 7. The team found that "Intel responded quickly after we started the responsible disclosure process." Since then, Intel discussed the issue with them and kept them informed of their timeline.

The CVE is CVE-2019-11157.

Intel released its security advisory, first on Dec. 10 and then, at the time of this writing, with an update on Dec. 11," Intel Processors Voltage Settings Modification Advisory,"INTEL-SA-00289.

Regarding Dec. 10, elsewhere on Intel, Jerry Bryant, director of security communication in the Intel Platform Assurance and Security group, had this to say in a "Technology at Intel" blog of Dec. 10:

"When SGX is enabled on a system, a privileged user may be able to mount an attack through the control of CPU voltage settings with the potential to impact the confidentiality and integrity of software assets. Intel has worked with system vendors to develop a microcode update that mitigates the issue by locking voltage to the default settings."

Damage thus far? Bryant reported that "We are not aware of any of these issues being used in the wild."

Paul Lilly in Hot Hardware: "Fortunately, this can't be leveraged remotely, meaning an attacker couldn't lure a user to a compromised website and then carry out the attack. Plundervolt runs from an app on an infected PC with root or admin privileges, and does not even work in virtualized environments. So even though it is a High level security flaw, the chances of this impacting a user is pretty small."

Bryant reiterated the advice that "we recommend installing security updates as soon as possible." He said "Your computer manufacturer is the best source to obtain most updates from." He offered a link for the list of computer manufacturer support sites.

You can read the details of their work in their paper, "Plundervolt: Software-based Fault Injection Attacks against Intel SGX."

"We present Plundervolt," said the authors and they described it as a software-based fault attack on Intel Core x86 processors.

Here is what Intel stated as recommendations in its security advisory: Intel recommends that users of the processors they listed on their advisory page update to the latest BIOS version provided by the system manufacturer that addresses these issues. Also, "An SGX TCB key recovery is planned for later in Q1 2020, this document will be updated with technical details in due course."

More information: www.plundervolt.com/ www.plundervolt.com/doc/plundervolt.pdf