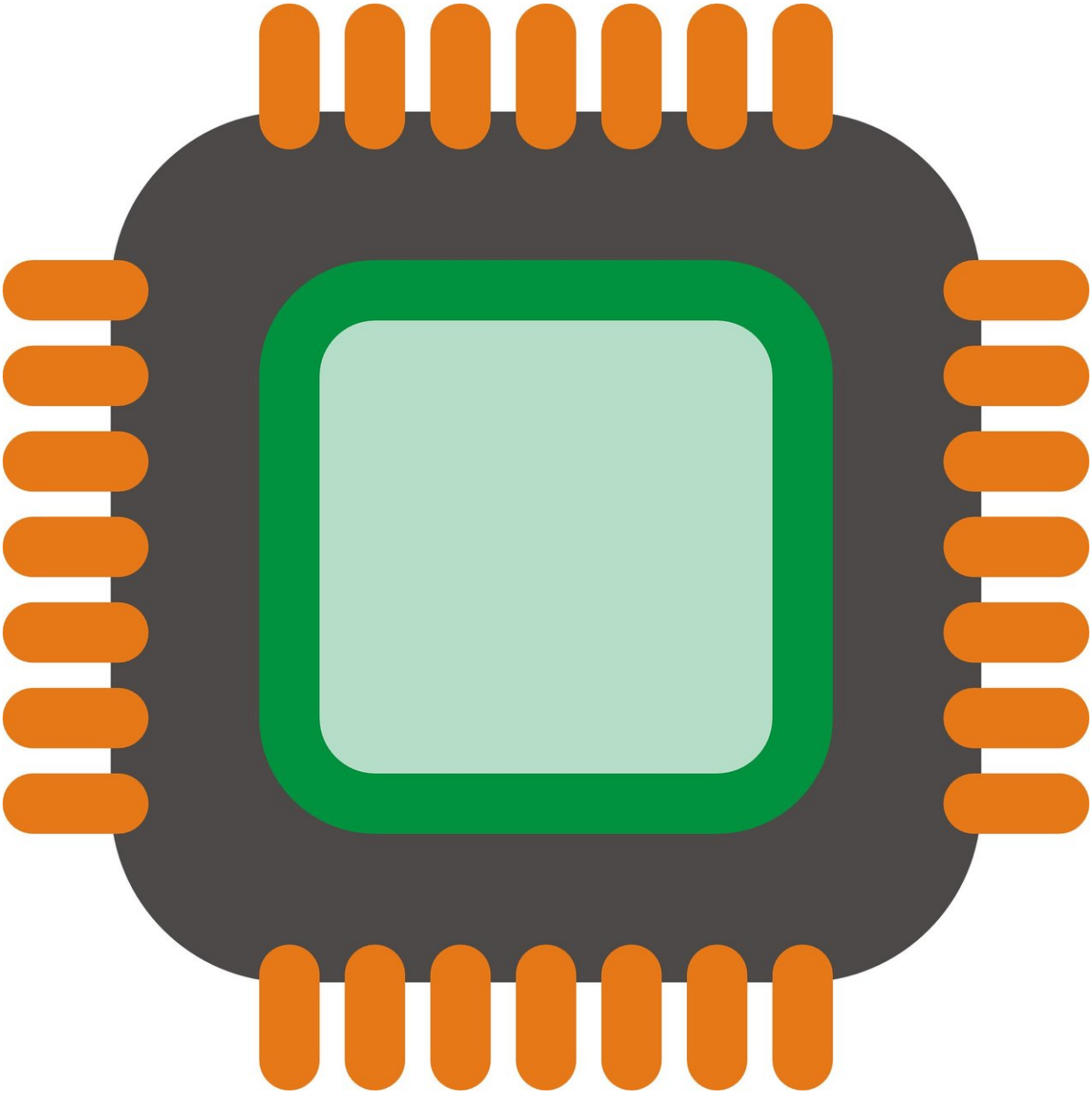
Intel receives notice of research on side-channel vulnerability

November 5 2018, by Nancy Owano



Credit: CC0 Public Domain

Intel's Hyper-Threading technology was in the news recently and it was all about the spotting of an attack vulnerability aimed at CPUs called PortSmash. It can steal decryption keys.

What is Hyper-Threading? *Tom's Hardware* offers this definition, from Scharon Harding: "Hyper-Threading is Intel's term for simultaneous multithreading (SMT). This is a process where a CPU splits each of its physical cores into virtual cores, which are known as threads... Hyper-Threading allows each core to do two things simultaneously. It increases CPU performance by improving the processor's efficiency, thereby allowing you to run multiple demanding apps at the same time or use heavily-threaded apps without the PC lagging."

BleepingComputer's Lawrence Abrams said the SMT/hyper-threading method can increase performance as the two threads will use idle CPU resources more efficiently to execute instructions faster.

Nonetheless, the vulnerability spotting took center stage this month as security watchers were referring to the exploit as the PortSmash side-channel vulnerability, or Hyper-Threading CPU vulnerability, or Hyper-Threading exploit.

Who identified the attack? *The Register* referred to "brainiacs in Cuba and Finland." The researchers are from Tampere University of Technology, Tampere, and Technical University of Havana.

Thomas Claburn in *The Register* said that if the spied-upon process is performing some kind of cryptography, it is possible for the PortSmash process sharing the same CPU core to extract secret information, such as

a decryption key, from its victim program.

TechSpot called PortSmash "a dangerous side-channel vulnerability." Kellep Charles, in *Security Boulevard*, explained what is meant by side-channel technique. Charles said it is used for "leaking encrypted data from a computer's memory or CPU, that will also record and analyze discrepancies in operation times, power consumption, electromagnetic leaks, or even sound to gain additional info that may help break encryption algorithms and recovering the CPU's processed data."

Tech-watching sites reported on an advisory about this exploitation of simultaneous multi-threading; reports also said an official research paper will be released later.

The advisory is titled "CVE-2018-5407: new side-channel vulnerability on SMT/Hyper-Threading architectures" from Billy Brumley.

Claburn wrote that the fix which Brumley suggested was to disable SMT/Hyper-Threading in the processor chip's BIOS. OpenBSD already disables Intel's hyper-threading for security reasons.

Dan Goodin in *Ars Technica* said the attack was carried out on servers running Intel Skylake and Kaby Lake chips and Ubuntu.

This *BleepingComputer* portion is what Nicola Tuveri, a member of the research team, shared, over how another member of the team, Billy-Bob Brumley, explained the attack to his daughter:

"You have a bag of jelly beans. I have a bag of jelly beans. We're pouring them into the same funnel. I can't see you or your jelly beans. But the rate at which I can pour my jelly beans depends on the rate you're pouring your jelly beans. If your rate depends on a secret, I can learn that secret by timing how fast my jelly beans are going into the

funnel."

As for disclosure, they informed Intel. They published a proof of concept.

A number of sites reporting on the team's findings also carried a statement from Intel:

"This issue is not reliant on speculative execution, and is therefore unrelated to Spectre, Meltdown or L1 Terminal Fault. We expect that it is not unique to Intel platforms. Research on side-channel analysis methods often focuses on manipulating and measuring the characteristics, such as timing, of shared hardware resources. Software or software libraries can be protected against such issues by employing side channel safe development practices."

Moving on, OpenSSL developers have released an update that makes PortSmash infeasible, wrote Goodin.

"PortSmash is tracked in the CVE vulnerability tracking system with the CVE-2018-5407 identifier. The OpenSSL project also released version 1.1.1 that prevents a PortSmash attack from recovering OpenSSL data," said Catalin Cimpanu in *ZDNet*.

"Fixes for this attack have already been added to OpenSSL 1.1.1 and for those who need an older version, patches are available for versions >= 1.1.0i," Abrams said.