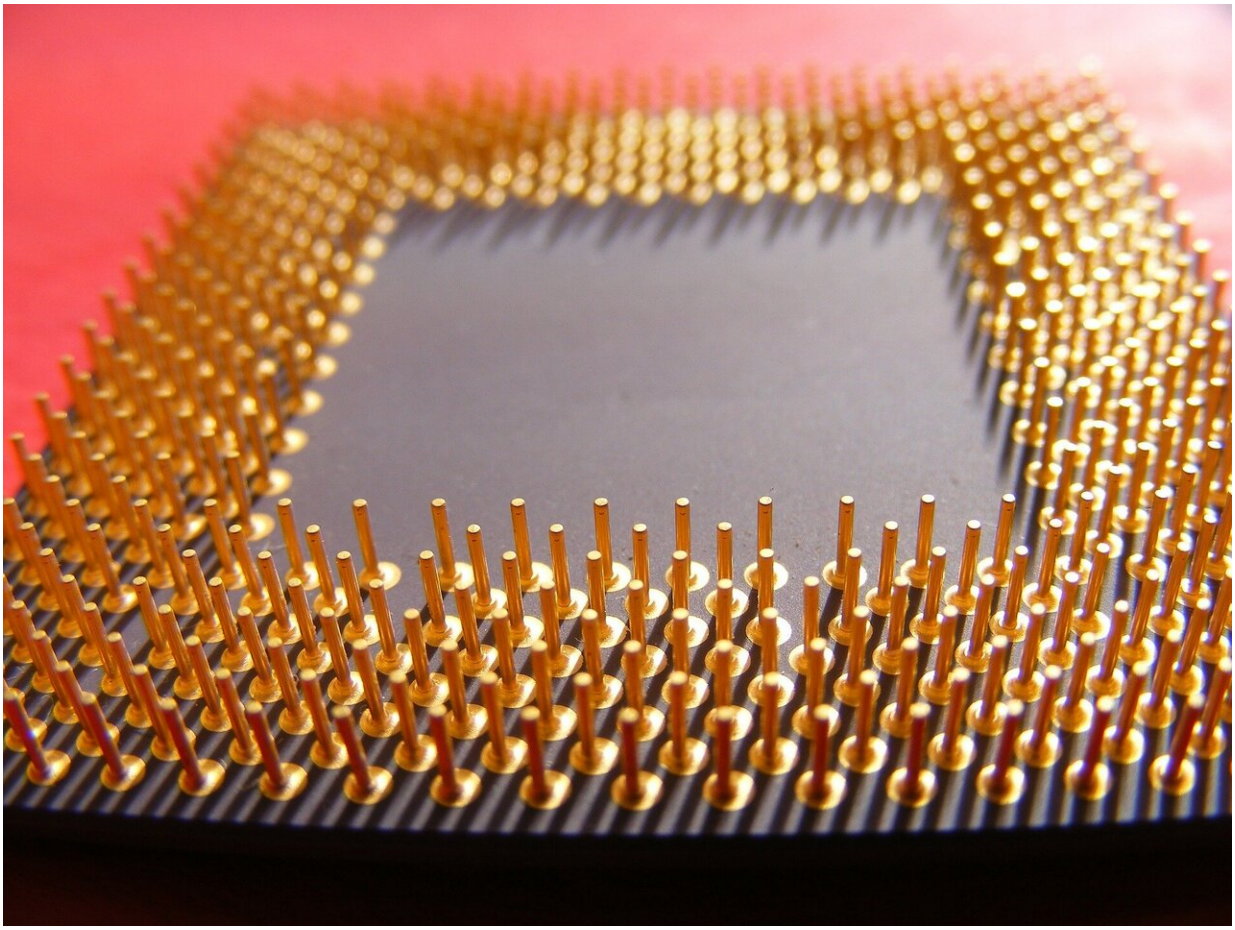
AMD processors susceptible to security vulnerabilities, data leaks

March 10 2020, by Jelani Harper



Credit: CC0 Public Domain

Graz University of Technology researchers recently revealed that AMD

CPUs dating as far back as the early 2010s are susceptible to side channel attacks. Researchers have now demonstrated that a pair of infiltration approaches—collectively termed "Take A Way"—can access AES encryption keys.

Take A Way consists of a pair of side-channel attacks called Collide+Probe and Load+Reload, and was so named because these attacks compromise the way predictor in the Level 1 cache of AMD's processing units. Designed to increase the overall effectiveness of the cache access mechanisms in this hardware, the way predictor is exploited by Take A Way to leak the content of valuable memory. Specifically, the cache way predictor is used to predict where data is housed within the processor to determine when its data is accessed.

Each side attack has a particular strength for taking advantage of the way predictor. Load+Reload is able to surreptitiously use an AMD CPU's shared memory without disrupting its cache line. Collide+Probe enables attackers to oversee access to memory without knowledge of its shared memory or physical address.

Collectively, these infiltrators can do much damage to the purported security of AMD CPUs, including exchanging data between programs in the same core, building secret channels between software pieces that shouldn't communicate, and breaking address space layout randomization (ASLR) to gain access to memory.

In fact, researchers were able to demonstrate many of these capabilities in a variety of settings, including cloud-based virtual machines and popular browsers like Firefox and Chrome.

According to the researchers, Take A Way was used to "demonstrate a covert channel with up to 588.9 kB/s, which we also use in a Spectre attack to exfiltrate secret data from the kernel. Furthermore, we present

a key-recovery attack from a vulnerable cryptographic implementation. We also show an entropy-reducing attack on ASLR of the kernel of a fully patched Linux system, the hypervisor, and our own address space from JavaScript."

The paper also explains that it should be possible to protect AMD's processors from Take A Way. These weaknesses could likely be rectified with firmware fixes, a solution that has proved useful for similar vulnerabilities in processing units for Spectre and Meltdown attacks. In most cases, updating firmware takes a toll on the performance of the hardware. Physical updates to the underlying architecture could prove helpful, as well.

The researchers also indicated that they made representatives at AMD aware of these vulnerabilities last August. However, the chip provider has yet to issue a public response or a fix for the issue.

More information: Take A Way: Exploring the Security Implications of AMD's Cache Way Predictors (PDF)