A new method to protect WebAssembly against Spectre attacks

August 11 2021

Credit: Pixabay/CC0 Public Domain

Computer scientists have developed a new compiler framework, called Swivel, to protect WebAssembly, or Warm, against Spectre attacks—the class of execution attacks, which exploit the way processors predict the computations that need to happen next. The team will present its

research at the USENIX Security Symposium taking place Aug. 11 to 13, 2021.

Wasm is an instruction set that has increasingly been used to sandbox untrusted code outside the browser. But unfortunately, Spectre attacks can bypass Wasm's isolation guarantees. To prevent this, Swivel ensures that potentially malicious code can neither use Spectre attacks to break out of the Wasm sandox pr force another Wasm client or the embedding process itself to leak secret data.

Swivel does this via two different approaches: a software-only approach that can be used on existing CPUs; and a hardware-assisted approach that uses extensions available in Intel 11th-generation CPUs.

More information: Full paper: www.usenix.org/system/files/sec21fall-narayan.pdf

Provided by University of California - San Diego