Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation

Submitted by Sergey Bratus on Fri, 03/13/2020 - 12:41pm. Contributors:
Ira JenkinsPrashant AnantharamanRebecca ShapiroJ Peter BradySergey BratusSean Smith

Spectre attacks have drawn much attention since their announce-ment. Speculative execution creates so-called transient instructions, those whose results are ephemeral and not committed architec-turally. However, various side-channels exist to extract these tran-sient results from the microarchitecture, e.g., caches. Spectre Variant 1, the so-called Bounds Check Bypass, was the first such attack to be demonstrated. Leveraging transient read instructions and cache-timing effects, the adversary can read secret data. In this work, we explore the ability of intraprocess memory iso-lation to mitigate Spectre Variant 1 attacks. We demonstrate this using Executable and Linkable Format-based access control (ELFbac) which is a technique for achieving intraprocess memory isolation at the application binary interface (ABI) level.

Additionally, we consider Memory Protection Keys (MPKs), a recent extension to In-tel processors, that partition virtual pages into security domains. Using the original Spectre proof-of-concept (POC) code, we show how ELFbac and MPKs can be used to thwart Spectre Variant 1 by constructing explicit policies to allow and disallow the exploit. We compare our techniques against the commonly suggested miti-gation using serialized instructions, e.g., lfence. Additionally, we consider other Spectre variants based on transient execution that intraprocess memory isolation would naturally mitigate.

Prashant Anantharaman is a Ph.D. student at Dartmouth College who works on Language-Theoretic Security. He works on securing various Industrial IoT and Power Grid protocols by building secure parsers for them and has recently begun exploring various binary file and protocol formats.

Ira Jenkins | Prashant Anantharaman | Rebecca Shapiro | J Peter Brady | Sergey Bratus | Sean Smith

Other available formats:

Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation
Switch to normal viewerSwitch to experimental viewer

Paper Session 3