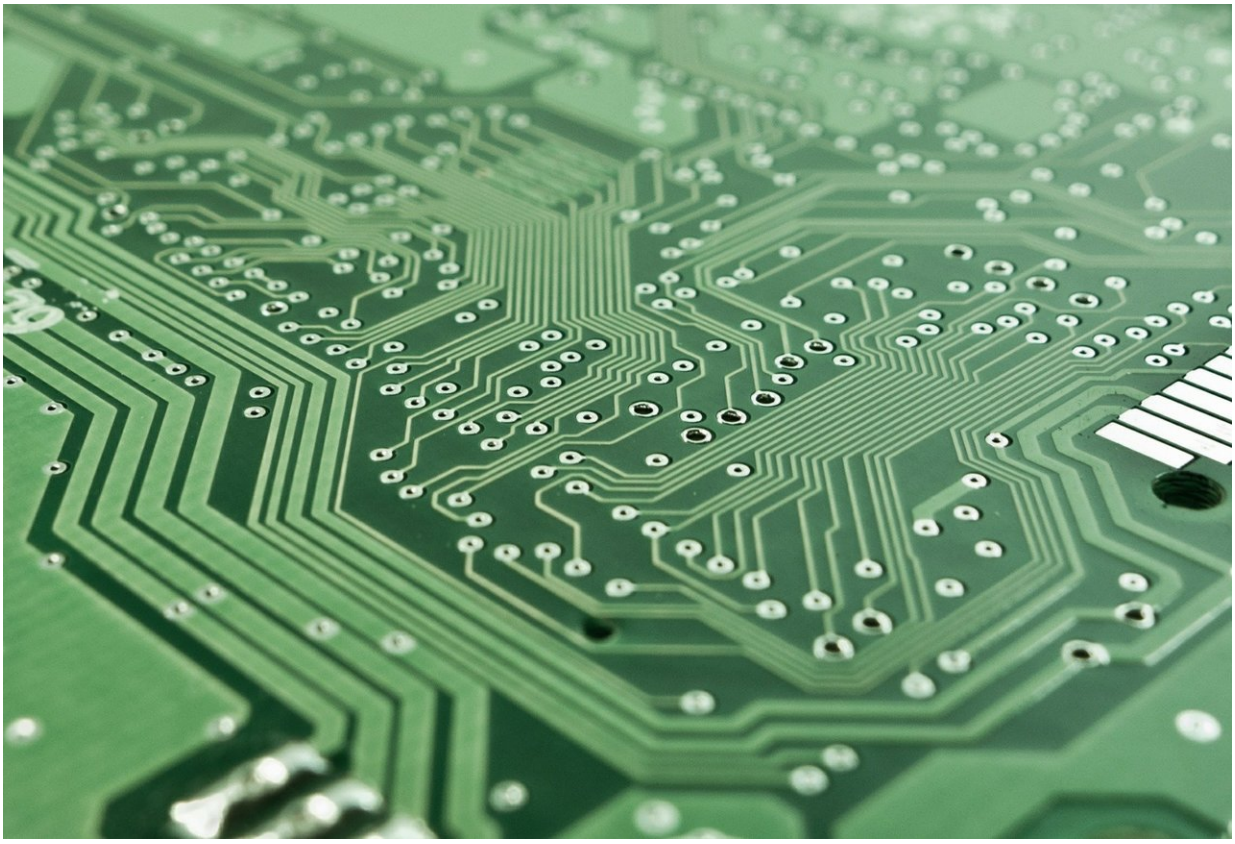
MeltdownPrime and SpectrePrime: Researchers nail exploits

February 17 2018, by Nancy Owano



Credit: CC0 Public Domain

Research from authors with affiliations that include Princeton and NVIDIA has drawn interest with their paper, "MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting

Invalidation-Based Coherence Protocols," which is on *arXiv*.

For those who would like a refresher on what are Meltdown and Spectre: These are two security flaws and they affect almost all computing devices, said Seung Lee, *The Mercury News*, last month. That was the news that caused a big stir and discomfort.

"The flaws—dubbed Meltdown and Spectre—are in chips made by Intel and other major suppliers. They can allow hackers to steal data from the memory of running apps, including password managers, browsers and emails."

The authors of the paper on *arXiv*, Caroline Trippel, Daniel Lustig, and Margaret Martonosi, discuss a tool they developed for "automatically synthesizing microarchitecture-specific programs capable of producing any user-specified hardware execution pattern of interest."

They said they show "how this tool can be used for generating small microarchitecture-specific programs which represent exploits in their most abstracted form—security litmus tests."

If you're not sure how bad this good news is, well, *The Register*'s headline may help. It began with "Hate to ruin your day, but.."

The exploits attack flaws deeply embedded within modern chip architecture, said Thomas Claburn in *The Register*.

Tom McKay in *Gizmodo*: "In short, they trick multi-core systems into leaking data stored across more than one processor memory cache."

These are, after all, design exploits. The authors figured out new ways that malware can pull sensitive information from a vulnerable computer's memory— by exploiting "Meltdown and Spectre design

blunders," Claburn said, in processors.

Claburn, summing up, wrote that they described "variants of Meltdown and Spectre exploit code that can be used to conduct side-channel timing attacks."

The exploits can be used to manipulate vulnerabilities in the way a number of varieties of modern processors handle a technique for better performance. It is called "speculative execution and extract hidden system data."

What is meant by side-channels? "Meltdown and Spectre are referred to as side-channel attacks because they exploit unanticipated side effects arising from these processor design characteristics," he wrote.

What exactly is their tool about? Claburn said the tool models chip microarchitectures to analyze specific execution patterns, such as Meltdown-Spectre-based timing attacks. The exploit techniques are dubbed MeltdownPrime and SpectrePrime.

The authors wrote, "Meltdown and Spectre represent a class of recently discovered cache timing side-channel attacks that leverage the effects of out-of-order and speculative execution on cache state." They said Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. They said Spectre "miss-trains branch predictors in modern processors in order to trick applications into accessing arbitrary locations in their memory."

McKay said "There's good news, namely that MeltdownPrime and SpectrePrime are likely resolved by the same patches that developers are releasing to resolve the original bugs."

Meanwhile, reporting on the Intel response, *Engadget* said Intel was

expanding its "bug bounty" to catch more Spectre-like security flaws. Its potential solution involved enlistments for help. "It's widening its bug bounty program to both include more researchers and offer more incentives to spot Meltdown- and Spectre-like holes," Jon Fingas said.

Intel issued a Feb. 14 news item about its Bugs Bounty Program. Rick Echevarria, vice president and general manager of Platform Security at Intel Corporation, was the author of the report on the updates that have been made to the program.

Updates to the program include: Moving from an invitation-only program to one that now is open to all security researchers. The move is to expand the pool of eligible researchers. Also, they are offering "a new program focused specifically on side channel vulnerabilities" (through December 31) and the award for disclosures under that program is up to $250,000. They are raising "bounty awards across the board, with awards of up to $100,000 for other areas."

More information: MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting Invalidation-Based Coherence Protocols, arXiv:1802.03802 [cs.CR] arxiv.org/abs/1802.03802

Abstract
The recent Meltdown and Spectre attacks highlight the importance of automated verification techniques for identifying hardware security vulnerabilities. We have developed a tool for synthesizing microarchitecture-specific programs capable of producing any user-specified hardware execution pattern of interest. Our tool takes two inputs: a formal description of (i) a microarchitecture in a domain-specific language, and (ii) a microarchitectural execution pattern of interest, e.g. a threat pattern. All programs synthesized by our tool are capable of producing the specified execution pattern on the supplied microarchitecture.

We used our tool to specify a hardware execution pattern common to Flush+Reload attacks and automatically synthesized security litmus tests representative of those that have been publicly disclosed for conducting Meltdown and Spectre attacks. We also formulated a Prime+Probe threat pattern, enabling our tool to synthesize a new variant of each—-MeltdownPrime and SpectrePrime. Both of these new exploits use Prime+Probe approaches to conduct the timing attack. They are both also novel in that they are 2-core attacks which leverage the cache line invalidation mechanism in modern cache coherence protocols. These are the first proposed Prime+Probe variants of Meltdown and Spectre. But more importantly, both Prime attacks exploit invalidation-based coherence protocols to achieve the same level of precision as a Flush+Reload attack. While mitigation techniques in software (e.g., barriers that prevent speculation) will likely be the same for our Prime variants as for original Spectre and Meltdown, we believe that hardware protection against them will be distinct. As a proof of concept, we implemented SpectrePrime as a C program and ran it on an Intel x86 processor, averaging about the same accuracy as Spectre over 100 runs—-97.9% for Spectre and 99.95% for SpectrePrime.