

Secure Speculative Execution

SpecuGuard speculative execution blocks Spectre/Meltdown attacks with low false positives and no CPU performance penalty.

Researchers at Purdue University have developed a hardware table and control logic for modern central processing units (CPU), a system known as SpecuGuard. The secure speculative execution system addresses Spectre and Meltdown vulnerabilities without altering CPU performance, unlike traditional systems. Spectre attacks are used for reading forbidden data by exploiting microprocessor hardware and can induce misspeculated paths, causing unintended side channels through the CPU's microarchitecture where data can be leaked. In either Spectre or Meltdown attacks, entire kernels or browser memories can be read. To plug these channels is difficult and sometimes infeasible and load and control-flow transfer techniques for data cleanup are typically unsafe. However, SpecuGuard allows for delays and recognition of user-checked code prior to committing data transfers. SpecuGuard employs speculative access control tables (SACT) to track load-instruction pairs and evaluate every possible speculative access for improved safety. In addition, SpecuGuard can avoid intrusive changes to clock-critical issue queue circuitry. In testing, SpecuGuard's false positive rate was found to be low while tagging and mapping data even during dynamic memory allocation.

Technology Validation: A low rate of false positives was achieved with SpecuGuard.

Publication:

"Secure Automatic Bound Checking: Prevention is Simpler Than Cure."
CGO 2020: Proceedings of the 18th ACM/IEEE International Symposium on Code Generation and Optimization. DOI: 10.1145/3368826.3377921

Advantages:

-Prevents Cyber Attacks

-Low False Positive Rate

Technology ID

2021-THOT-69479

Category

Agriculture, Nutrition, &

AgTech/Ag Robotics &

Automation

Energy & Power Systems/Grid

Modernization & Smart Grids

Further information

Parag Vasekar

psvasekar@prf.org

View online page



-Enables More Accurate and Safer Speculative Access Determination

Applications:

-Central Processing Unit Hardware

-Cybersecurity

TRL: 3

Intellectual Property:

Provisional-Patent, 2021-05-06, United States

Provisional-Patent, 2021-08-13, United States

Provisional-Patent, 2021-09-23, United States

Utility Patent, 2022-05-05, United States

DIV-Patent, 2024-05-25, United States

Keywords: Circuits, Computer Engineering, Computer Hardware, Computer Security, cyber-physical systems, Cybersecurity, Data Processing, Memory, Security, Computer Technology