PURDUE INNOVATES | Office of Technology Commercialization

Context Annotation of Permissions in SafeBet

Context-aware speculative execution scheme blocks Spectre/Meltdown with minimal performance loss.

The computer hardware security vulnerabilities Spectre and Meltdown leave devices using Intel, AMD, or ARM processors susceptible to exploitation of private user data. While experts have been aware of these exploits since 2018, prior solutions require significant sacrifices in hardware complexity and processor performance. Researchers at Purdue University have developed SafeBet, a microprocessor hardware scheme to prevent Spectre- and Meltdown-style security vulnerabilities with minimal impact to performance. This is an extension of technology 2021-THOT-69479 -- "SpecuGuard: A Computer System for Secure Speculative Execution." In simulated attacks, SafeBet was able to completely deny access to secret information as compared to prior methods which allow an attacker access to the information but prevent transmission of it. One feature of the technology is context annotation of the source address, which allows SafeBet to prevent repeated access to the same information from different, potentially malicious sources. This technology has applications in the design of high-performance, general-purpose microprocessors to prevent vulnerability to Spectre- or Meltdown-style attacks.

Advantages

-Resistant to Spectre and Meltdown attacks

-Minimal impact to processor performance

Applications

-Microprocessor design

-Cybersecurity

Technology Validation:

Technology ID

2023-VIJA-69938

Category

Agriculture, Nutrition, & AgTech/Ag Robotics & Automation

Semiconductors/IC Design & EDA Tools

Further information

Parag Vasekar

psvasekar@prf.org

View online page

This technology has been validated through computer simulations against Spectre attacks. SafeBet manages to maintain security while operating only 6% slower than the unsafe baseline hardware. Alternative approaches resulted in slowdowns of 83% compared to the unsafe baseline.

TRL: 4

Intellectual Property:

Provisional-Patent, 2022-12-07, United States

PCT-Patent, 2023-12-07, WO

NATL-Patent, 2025-06-03, United States

Keywords: chip design, Chips, Computer Technology, Cybercrime, Electrical Engineering, hacking, microprocessor, Privacy, Security, vulnerability