Speculative Execution Attacks and Hardware Defenses

Ruby B. Lee
Princeton University, Princeton, NJ, USA
rblee@princeton.edu

ABSTRACT

Speculative execution attacks like Spectre and Meltdown exploit hardware performance optimization features to illegally access a secret and then leak the secret to an unauthorized recipient. Many variants of speculative execution attacks (also called transient execution attacks) have been proposed in the last few years, and new ones are constantly being discovered. While software mitigations for some attacks have been proposed, they often cause very significant performance degradation. Hardware solutions are also being proposed actively by the research community, especially as these are attacks on hardware microarchitecture. In this talk, we identify the critical steps in a speculative attack, and the root cause of successful attacks. We define the concept of "security dependencies", which should be implemented to prevent data leaks and other security breaches. We propose a taxonomy of defense strategies and show how proposed hardware defenses fall under each defense strategy. We discuss security-performance tradeoffs, which can decrease the performance overhead while still preventing security breaches. We suggest design principles for future security-aware microarchitecture.

CCS Concepts: Security and privacy~Security in hardware

Keywords: Speculative Execution Attacks; Hardware Defenses

BIOGRAPHY

Ruby B. Lee is the Forest G. Hamrick Professor in Engineering and Professor of Electrical and Computer Engineering at Princeton University, and the Director of PALMS (Princeton Architecture Lab for Multimedia and Security). Her current research lies at the intersection of Cyber Security, Computer Architecture and Deep Learning. She designs fundamental security features into computer systems, from smartphones to clouds, including secure processors and secure caches that are resilient to cache side-channel attacks. She uses deep learning to improve security, including detecting anomalous behavior in power-grid systems, cloud computing and smartphones. She also works at improving the security of deep learning systems. Prof. Lee is a Fellow of the ACM and IEEE, member of the American Academy of Arts and Sciences, and has over 130 U.S. and international patents and numerous publications. She has served on National committees that have improved cybersecurity research in the U.S.

Prior to Princeton, Lee was chief architect at Hewlett Packard, responsible at different times for processor architecture, multimedia architecture and security architecture. She was a founding architect of the PA-RISC architecture used world-wide in HP's business, technical and control computer families for decades, and architect of the first multimedia instructions in commercial microprocessors that facilitated ubiquitous multimedia. Her work in security has been the forerunner of industry hardware security offerings. Lee has a B.A. (distinction) from Cornell University, where she was a College Scholar, and a PhD in E.E. (minor in C.S.) from Stanford University.

ASHES '21, November 19, 2021, Virtual Event, Republic of Korea.

ACM ISBN 978-1-4503-8662-3/21/11.
https://doi.org/10.1145/3474376.3487404