Paper Reading Notes

Jerry

Junyi Yang[1]

PhD. Student at the Institute of Computing Technology, Chinese Academy of Sciences
Website
LinkedIn
Github

yangjunyi22s@ict.ac.cn

[1] *Jerryy959*

Contents

PART

I

介绍

Section 1

大纲

这份笔记主要记录自己阅读的 paper，与对应的总结。分类原则是按照类别进行划分，主要包括体系结构与大模型。

PART

II

文章

Section 2

计算机体系结构

Subsection 2.1

SpecLFB: Eliminating Cache Side Channels in Speculative Executions[1]

> *Cache side-channel attacks based on speculative executions are powerful and difficult to mitigate. Existing hardware defense schemes often require additional hardware data structures, data movement operations and/or complex logical computations, resulting in excessive overhead of both processor performance and hardware resources. To this end, this paper proposes SpecLFB, which utilizes the microarchitecture component, Line-Fill-Buffer, integrated with a proposed mechanism for load security check to prevent the establishment of cache side channels in speculative executions. To ensure the correctness and immediacy of load security check, a structure called ROB unsafe mask is designed for SpecLFB to track instruction state. To further reduce processor performance overhead, SpecLFB narrows down the protection scope of unsafe speculative loads and determines the time at which they can be deprotected as early as possible. SpecLFB has been implemented in the open-source RISC-V core, Sonic- BOOM, as well as in Gem5. For the enhanced SonicBOOM, its register-transfer-level (RTL) code is generated, and an FPGA hardware prototype burned with the core and running a Linux-kernel-based operating system is developed. Based on the evaluations in terms of security guarantee, performance overhead, and hardware resource overhead through RTL simulation, FPGA prototype experiment, and Gem5 simulation, it shows that SpecLFB effectively defends against attacks. It leads to a hardware resource overhead of only 0.6% and the performance overhead of only 1.85% and 3.20% in the FPGA prototype experiment and Gem5 simulation, respectively.*

Remark **翻译：** 缓存侧信道攻击[1]基于推测执行非常强大且难以缓解。现有的硬件防御方案通常需要额外的硬件数据结构、数据移动操作和/或复杂的逻辑计算，导致处理器性能和硬件资源的过度开销。为此，本文提出了 *SpecLFB*，它利用微架构组件，即行填充缓冲区

[1] 利用 *Cache* 信息获取信息，见常见的侧信道攻击方法

（*Line-Fill-Buffer*），并集成了用于加载安全检查的提出机制，以防止在推测执行中建立缓存侧信道。为确保加载安全检查的正确性和即时性，为 *SpecLFB* 设计了一种称为 *ROB* 不安全掩码的结构，用于跟踪指令状态。为了进一步减少处理器性能开销，*SpecLFB* 缩小了不安全推测加载的保护范围，并尽可能早地确定它们可以解除保护的时间。*SpecLFB* 已在开源 *RISC-V* 核心 *Sonic-BOOM* 以及 *Gem5* 中实现。对于增强的 *SonicBOOM*，生成了其寄存器传输级（*RTL*）代码，并开发了一个烧录了核心并运行基于 *Linux* 内核操作系统的 *FPGA* 硬件原型。基于通过 *RTL* 模拟、*FPGA* 原型实验和 *Gem5* 模拟在安全保证、性能开销和硬件资源开销方面的评估，它表明 *SpecLFB* 有效地防御了攻击。在 *FPGA* 原型实验和 *Gem5* 模拟中，它导致硬件资源开销仅为 *0.6%*，性能开销分别为 *1.85%* 和 *3.20%*。

Section 3

人工智能与大模型

References

[1] Xiaoyu Cheng, Fei Tong, Hongyu Wang, Zhe Zhou, Fang Jiang, and Yuxing Mao. SpecLFB: Eliminating cache side channels in speculative executions. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 631–646, Philadelphia, PA, August 2024. USENIX Association.