Research on Side-Channel Attack in RISC-V

Ben Chen

Dept of Computer Science and Engineering, SUSTech

September 8, 2024

With Great Power Come Great Side Channels[1]

Motivation: Noise and false positive in time measurement is fatal to side channel

- Improve statistical analysis on timing result with bounded type-1 error
- Propose new decision rule based on boostrap to obtain a reasonable accept and reject hypothesis H_0, and implement a evaluation tool called RTLF
- Compared with Mona, dudect, tlsfuzzer and t-test, shows a higher accuracy

ZenHammer[2]

Motivation: RowHammer attack on Intel $\rightarrow$ attack on AMD chips

- Reverse engineer the address mapping function of DRAM
- Design a access pattern to bypass the TRR, and activate the throughput optimization to make attack effective
- Evaluated on AMD Zen 2 and Zen 3 with multiple DDR4 and DDR5 memory to smash the page table, secrets and priviledge escalation

BunnyHop[3]

Exploit the instruction prefetcher on Intel

- Exploit the interaction between branch predictor and instruction prefetcher to enhance the speculative attack
- Propose a variant of Flush+Reload and Prime+Probe attack
- Show an attack on the KASLR with BunnyHop-Reload attack to extract kernel space address

PrefetchX[4]

Exploit the XPT prefetcher on Intel

- XPT prefetch L2 directly from memory with prediction of L3 cache miss, XPT is shared cross-core and works without shared cache and memory
- Propose a new attack primitive: PREFETCHX-Evict and PREFETCHX-Flush
- Experiemtn shows an extraction of RSA private key and monitor of user keyboard behaviour, and works in visualized envrionment(AWS EC2)

L1 I$ Attack on Xiangshan

https://www.bilibili.com/video/BV1mhH5eeEyZ/?share_source=copy_web&vd_source=cff89ae5ccad158ff4e1081ad1a85564&t=10621

WhisperFuzz[5]

Motivation: fuzzing software $\rightarrow$ fuzzing hardware

- Using white-box fuzzing to locate possible timing vulnerability in RTL source code
- Combined with static analysis, can cover the archtectural temporal diagram and states transformation to indicate possible timing difference
- Evaluated on BOOM, Rocket Core, CVA6, 8 critical out of 12 found

SpecLFB[6]

Defense against the Speculative Side-Channel attack

- Propose a new component called Line-Fill Buffer to store the cache line before the instruction retired
- Design ROB unsafe mask to track status of instruction to narrow the protection range
- Evaluated on SonicBOOM(RISC-V) and tested on FPGA and Gem5

ClepsydraCache[7]

Defense cache side-channel attack with TTL and address randomization

- Mechanism to create dynamic TTL and monitor cache's Time-To-Live and evict when expired
- Use address randomization to make eviction set construction hard
- Prevent Prime+Probe, Flush+Reload with low overhead

Possible Direction

- Attack on the cross-core L2 cache prefetch
- Multi-core attack on the RVWMO model
- Defense against (speculative) cache side-channel

References I

[1] Martin Dunsche et al. "With Great Power Come Great Side Channels: Statistical Timing Side-Channel Analyses with Bounded Type-1 Errors". In: *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 6687–6704. ISBN: 978-1-939133-44-1. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/dunsche.

[2] Patrick Jattke et al. "ZenHammer: Rowhammer Attacks on AMD Zen-based Platforms". In: *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 1615–1633. ISBN: 978-1-939133-44-1. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/jattke.

References II

[3] Zhiyuan Zhang et al. "BunnyHop: Exploiting the Instruction Prefetcher". In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 7321–7337. ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/zhang-zhiyuan-bunnyhop.

[4] Yun Chen et al. "PREFETCHX: Cross-Core Cache-Agnostic Prefetcher-based Side-Channel Attacks". In: *2024 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. 2024, pp. 395–408. DOI: 10.1109/HPCA57654.2024.00037.

[5] Pallavi Borkar et al. "WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors". In: *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 5377–5394. ISBN: 978-1-939133-44-1. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/borkar.

References III

[6] Xiaoyu Cheng et al. "SpecLFB: Eliminating Cache Side Channels in Speculative Executions". In: *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 631–646. ISBN: 978-1-939133-44-1. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/cheng-xiaoyu.

[7] Jan Philipp Thoma et al. "ClepsydraCache – Preventing Cache Attacks with Time-Based Evictions". In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 1991–2008. ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/thoma.