



薛子涵

电话: 15281016407

邮箱: xuezihan@iie.ac.cn

github: fems2991



教育背景

2019.09 - 2024.07(计划)	博士	中科院信工所信息安全国家重点实验室	计算机系统结构	导师 宋威
2014.09 - 2017.07	硕士	西南交通大学信息科学与技术学院(保送)	集成电路工程	导师 陈向东
2010.09 - 2014.07	本科	西南交通大学信息科学与技术学院	电子科学与技术	

工作经历

2017.08 - 2019.08 工程师 北京通号基础院芯片室 多功能车辆总线芯片, 功能安全芯片

科研经历

2019.09 - 至今 针对缓存侧信道攻击的处理器防御技术研究

缓存侧信道攻击广泛应用于信息泄露和隐蔽信道, 其中驱逐集的构造作为缓存侧信道攻击的关键步骤, 成为了攻防双方的研究热点。为了阻止攻击者构造出驱逐集以此从根源上挫败缓存侧信道攻击, 本研究提出了缓存随机化方案, 周期性或在检测到攻击时打乱地址-缓存组索引之间的映射关系。在该研究项目中, 我独立部署并测试了缓存随机化方案。

- **调研:** 分析驱逐集构造算法(GE、CT、PPP)特点探索高效的检测方法, 分析现有防御方案(缓存随机化、缓存分区)优劣。
- **模型:** 搭建缓存模型(C/C++编程), 利用该模型评估检测器的有效性; 测试缓存随机化对缓存性能(MPKI)的影响。
- **设计:** 单周期的哈希算法以降低访问延时, 多步迁移方案以降低重映射代价, 重映射状态机, 攻击检测器。
- **部署:** 将随机化缓存方案部署在开源处理器 rocketchip 上(chisel/verilog 编程)以 75Mhz 的频率在 FPGA 上运行 Linux。
- **测试:** 在开启检测器状态下现有驱逐集构造算法全部无法工作; 对 SPEC CPU 2006 每个 case 运行 100G 指令并统计平均性能(CPI)开销, 结果表明随机化缓存对性能(CPI)影响小于 1%。
- **成果:** 首个能抵御缓存侧信道攻击的双核处理器(<https://github.com/comparch-security/chipyard-random-llc>)。TC(CCF-A)[1]、RAID(CCF-B)[2]、S&P(CCF-A)[3]。

2019.09 - 至今 标签缓存结构研究并用以抵御控制流劫持

控制流(CFI)完整性检查是一种有效抵御控制流劫持的防御方法, 通常该方法需要在函数跳转前插入安全检查代码, 这种软件插桩的方法严重损害了程序的执行效率。标签缓存将这种低效的软件插桩方式替换成了高效的硬件方式, 以此降低 CFI 检查的性能开销。在该研究项目中, 我对标签缓存进行了优化, 部署性能监测模块, 对标签缓存性能进行测试和评估。

- **调研:** 研究控制流劫持手段(ROP/COP/JOP)和相关防御措施; 研究现有标签缓存优化技术。
- **设计:** 层次化标签表、动态搜索顺序、并行化标签访问、统一的标签内存结构、避免额外写、避免空访问。
- **成果:** 带有标签缓存的 RISC-V 处理器、TC(CCF-A)[5](已投)

获得奖励

- 2023 年中国科学院大学三好学生
- 2015 年硕士研究生国家奖学金
- 2013 年飞思卡尔智能车竞赛四川省一等奖
- 2012 年电子设计竞赛四川省一等奖

发表文章

- [1]Wei Song, Zihan Xue, Jinchi Han, Zhenzhen Li, Peng Liu. Randomizing Set-Associative Caches Against Conflict-Based Cache Side-Channel Attacks. IEEE Transactions on Computers(TC), 2024. (CCF-A).
- [2]Zihan Xue, Jinchi Han, and Wei Song. CTPP: A fast and stealth algorithm for searching eviction sets on Intel processors. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, Hongkong, China, October 2023. (CCF-B).
- [3]Wei Song, Boya Li, Zihan Xue, Zhenzhen Li, Wenhao Wang, and Peng Liu. Randomized last level caches are still vulnerable to cache side channel attacks! But we can fix it. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, Online, pp. 955–969, May 2021. (CCF-A).
- [4]薛子涵, 解达, 宋威. 基于 RISC-V 的新型硬件性能计数器. 计算机系统应用, November 2021, 30(11): 3–10.
- [5] Wei Song, Da Xie, Zihan Xue, Peng Liu. A Parallel Tag Cache for Hardware Managed Tagged Memory in Multicore Processors. IEEE Transactions on Computers(TC).(CCF-A).(已投)