Luyi Li

9500 Gilman Dr, La Jolla, CA 92092
Email: lul014@ucsd.edu / owenliluyi@gmail.com • Home Page • Google Scholar

OVERVIEW

I am a third-year PhD student in the Computer Science and Engineering department at University of California, San Diego (UCSD), advised by Professor Dean Tullsen. My research interests primarily lie in the field of computer architecture and microarchitecture security. I have worked on several research projects about **exploring modern microarchitecture vulnerability** and **designing hardware exploit mitigations**.

EDUCATION

University of California, San Diego, La Jolla, CA, USA — Sep 2022 – Jul 2027 (Expected)

- Ph.D. in Computer Science and Engineering
- **Advisor:** Prof. Dean Tullsen
- **Research Interest:** Microarchitecture Security (Branch Predictor Vulnerability, CXL Vulnerability)
- **Honors & Prizes:** JSOE Fellowship (2022-2023)

University of California, San Diego, La Jolla, CA, USA — Sep 2022 – Jun 2024

- M.S. in Computer Science and Engineering

Nanjing University, Nanjing, Jiangsu, China — Sep 2018 – Jul 2022

- B.E. in Electrical Engineering (VLSI Design)
- **Advisor:** Prof. Zhongfeng Wang, Prof. Lang Feng, Prof. Jun Lin
- **Honors & Prizes:** People Scholarship (2019 & 2020), Jinxiao Scholarship (2021)

PUBLICATIONS

PUBLISHED / ACCEPTED

[1] **Luyi Li**[*], Hosein Yavarzadeh[*], Dean Tullsen, "Indirector: High-Precision Branch Target Injection Attacks Exploiting the Indirect Branch Predictor".
In *USENIX Security Symposium* (***USENIX Security***), 2024 [**Distinguished Paper Award**] [[*]Co-first Author] [Acceptance Rate: 18.32%]

[2] **Luyi Li**, Jiayi Huang, Lang Feng, and Zhongfeng Wang, "PREFENDER: A Prefetching Defender against Cache Side Channel Attacks as A Pretender (Extended Version)".
In *IEEE Transactions on Computers* (***TC***), 2024

[3] **Luyi Li**, Jiayi Huang, Lang Feng, and Zhongfeng Wang, "PREFENDER: A Prefetching Defender against Cache Side Channel Attacks as A Pretender".
In *Design, Automation and Test in Europe* (***DATE***), 2022 [**Best Paper Candidate**] [Acceptance Rate: 25.00%]

[4] Lang Feng[*], Jiayi Huang[*], **Luyi Li**, Haochen Zhang, and Zhongfeng Wang, "RVDFI: A RISC-V Architecture with Security Enforcement by High Performance Complete Data-Flow Integrity".
In *IEEE Transactions on Computers* (***TC***), 2021 [[*]Co-first Author]

[5] **Luyi Li**, Jun Lin, and Zhongfeng Wang, "PipeBSW: A Two-Stage Pipeline Structure for Banded Smith-Waterman Algorithm on FPGA".
In *IEEE Computer Society Annual Symposium on VLSI* (***ISVLSI***), 2021 [**Best Paper Candidate**]

SELECTED PROJECTS

High-Precision Target Injection Attacks via Indirect Branch Predictor — Apr 2023 – Feb 2024

Published in *USENIX Security* 2024

- **Overview:** This paper introduces novel high-precision Branch Target Injection (BTI) attacks, leveraging the intricate structures of the Indirect Branch Predictor (IBP) and the Branch Target Buffer (BTB) in high-end Intel CPUs. It presents, for the first time, a comprehensive picture of the IBP and the BTB within the most recent Intel processors, revealing their size, structure, and the precise functions governing index and tag hashing. Additionally, this study reveals new details into the inner workings of Intel's hardware defenses, such as IBPB, IBRS, and STIBP, including previously unknown holes in their coverage. Leveraging insights from reverse engineering efforts, this research develops highly precise Branch Target Injection (BTI) attacks to breach security boundaries across diverse scenarios, including cross-process and cross-privilege scenarios and uses the IBP and the BTB to break Address Space Layout Randomization (ASLR).

Secure Data Prefetcher Design against Cache Side Channel Attacks Mar 2021 – Mar 2022

Published in *DATE* 2022 and *IEEE Transactions on Computers*

- **Overview:** Cache side channel attacks are increasingly alarming in modern processors due to the recent emergence of Spectre and Meltdown attacks. A typical attack performs intentional cache access and manipulates cache states to leak secrets by observing the victim's cache access patterns. Different countermeasures have been proposed to defend against both general and transient execution based attacks. Despite their effectiveness, they mostly trade some level of performance for security, or have restricted security scope. In this paper, we seek an approach to enforcing security while maintaining performance. We leverage the insight that attackers need to access cache in order to manipulate and observe cache state changes for information leakage. Specifically, we propose *PREFENDER*, a secure prefetcher that learns and predicts attack-related accesses for prefetching the cachelines to simultaneously help security and performance. Our results show that *PREFENDER* is effective against several cache side channel attacks while maintaining or even improving performance for SPEC CPU 2006 and 2017 benchmarks.

Hardware Implementation of Data-Flow Integrity on RISC-V CPU Nov 2020 – May 2021

Published in *IEEE Transactions on Computers*

- **Overview:** With the rapid revolution of open-source hardware, RISC-V architecture has been prevalent in both academic research and industrial developments. Due to the increasing threats of information leakage, it is imperative to provide a secure RISC-V ecosystem to defend against malicious software exploits. Toward this goal, data-flow integrity (DFI) is employed as a strict security policy for enforcing the legitimacy of each data access, thereby filtering out most of the attack exploits. However, due to the intensive computations needed by DFI, there are only limited proposals successfully implementing partial DFI with low performance overhead. Moreover, all the previous studies failed to enforce the complete DFI policy in a real hardware platform, while trading off security strength for performance efficiency. To provide RISC-V architecture with high security enforcement and low performance overhead, we leverage the open-source Rocket Chip and propose RvDfi , the first complete DFI implementation based on RISC-V architecture with only 17.8% performance overhead on average and 3.9% in minimum, incurring much less performance loss compared to the 166.3% overhead caused by previous complete DFI implementation.

SKILLS

Programming Language: C/C++, Assembly, Python, Verilog/System Verilog, Chisel

Computer Architecture Tool: Gem5, RISC-V Toolchain

English Proficiency: TOEFL 105 (R28 L28 S22 W27), GRE 323 (V155 Q168) + AW3.5