Zirui Neil Zhao

☎ +1 217-898-0181 | ✉ ziruiz6@illinois.edu | 🌐 neilzhao.me | github.com/zzrcxb

Research Interests

Computer Architecture, Hardware and Software Security, Cloud Computing, Program Analysis

Education

University of Illinois Urbana-Champaign (UIUC) Aug. 2018 – May 2024 (*expected*)
Ph.D. Candidate in Computer Science. Thesis Advisor: Prof. Josep Torrellas
Thesis: "You Share, You Leak, Practical Side-Channel Attacks and Defenses in Modern Clouds"

University of Science and Technology of China (USTC) Aug. 2014 – June 2018
Bachelor of Science in Applied Physics. School of the Gifted Young. Yan Jici Talent Students Program
Thesis: "ParaRail: Simplified Programming Interface for Large-Scale FPGA Clusters". Advisor: Yongqiang Xiong

Peer-Reviewed Publications

12. **Perspective: Secure Operating System Speculation Views**
Tae Hoon Kim, David Rudo, Kaiyang Zhao, Zirui Neil Zhao, and Dimitrios Skarlatos
*51st International Symposium on Computer Architecture (**ISCA 2024**), Buenos Aires, Argentina, June 29–July 3, 2024*

11. **Last-Level Cache Side-Channel Attacks Are Feasible in the Modern Public Cloud**
Zirui Neil Zhao, Adam Morrison, Christopher W. Fletcher, and Josep Torrellas
*29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2024**), Volume 2, La Jolla, CA, USA, April 27–May 1, 2024*

10. **Everywhere All at Once: Co-Location Attacks on Public Cloud FaaS**
Zirui Neil Zhao, Adam Morrison, Christopher W. Fletcher, and Josep Torrellas
*29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2024**), Volume 1, La Jolla, CA, USA, April 27–May 1, 2024*

9. **Untangle: A Principled Framework to Design Low-Leakage, High-Performance Dynamic Partitioning Schemes**
Zirui Neil Zhao, Adam Morrison, Christopher W. Fletcher, and Josep Torrellas
*28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2023**), Volume 3, Vancouver, BC, Canada, March 25–29, 2023, pages 771–788.*
🏆 **IEEE Micro Top Picks 2024 Honorable Mention**

8. **Declassiflow: A Static Analysis for Modeling Non-Speculative Knowledge to Relax Speculative Execution Security Measures**
Rutvik Choudhary, Alan Wang, Zirui Neil Zhao, Adam Morrison, and Christopher W. Fletcher
*2023 ACM SIGSAC Conference on Computer and Communications Security (**CCS 2023**), Copenhagen, Denmark, November 26–30, 2023*

7. **Binoculars: Contention-Based Side-Channel Attacks Exploiting the Page Walker**
Zirui Neil Zhao, Adam Morrison, Christopher W. Fletcher, and Josep Torrellas
*31st USENIX Security Symposium (**USENIX Security 2022**), Boston, MA, USA, August 10–12, 2022, pages 699–716*

6. **Pinned Loads: Taming Speculative Loads in Secure Processors**
Zirui Neil Zhao, Houxiang Ji, Adam Morrison, Darko Marinov, and Josep Torrellas
*27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2022**), Lausanne, Switzerland, February 28–March 4, 2022, pages 314–328*

5. **Jamais Vu: Thwarting Microarchitectural Replay Attacks**
Dimitrios Skarlatos[*], Zirui Neil Zhao[*], Riccardo Paccagnella, Christopher W. Fletcher, and Josep Torrellas
*26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2021**), Virtual Event, April 19–23, 2021, pages 1061–1076.*
[*]Authors contributed equally to this work

4. **Speculative Interference Attacks: Breaking Invisible Speculation Schemes**
Mohammad Behnia, Prateek Sahu, Riccardo Paccagnella, Jiyong Yu, Zirui Neil Zhao, Xiang Zou, Thomas Unterluggauer, Josep Torrellas, Carlos V. Rozas, Adam Morrison, Frank McKeen, Fangfei Liu, Ron Gabor, Christopher W. Fletcher, Abhishek Basak, and Alaa R. Alameldeen
*26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS 2021**), Virtual Event, April 19–23, 2021, pages 1046–1060*

3. **PaCon: A Symbolic Analysis Approach for Tactic-Oriented Clustering of Programming Submissions**
Yingjie Fu, Jonathan Osei-Owusu, Angello Astorga, Zirui Neil Zhao, Wei Zhang, and Tao Xie
*2021 ACM SIGPLAN International Symposium on SPLASH-E (**SPLASH-E 2021**), Chicago, IL, USA. October 20, 2021, pages 32–42*

2. **Speculation Invariance (InvarSpec): Faster Safe Execution Through Program Analysis**
Zirui Neil Zhao, Houxiang Ji, Mengjia Yan, Jiyong Yu, Christopher W. Fletcher, Adam Morrison, Darko Marinov, and Josep Torrellas
*53rd Annual IEEE/ACM International Symposium on Microarchitecture (**MICRO 2020**), Virtual Event, October 17–21, 2020, pages 1138–1152*

1. **Benchmarking the Capability of Symbolic Execution Tools with Logic Bombs**
Hui Xu, Zirui Neil Zhao, Yangfan Zhou, and Michael R. Lyu
IEEE Transactions on Dependable and Secure Computing, 17 (6), 2020, pages 1243–1256

Industrial Research Experience

Intel Labs – Research Intern May 2021 – Aug. 2021
Manager: Carlos V. Rozas; Mentor: Fangfei Liu
Project: Cost-Effective Spectre Mitigations

- Designed a program analysis pass to improve the performance of Intel's Spectre v1 mitigation
- Studied the residual speculative attack surface of Intel Cryptographic Capability Computing (C^3)
- Technology transfer of my prior work

Intel Labs – Research Intern Aug. 2020 – Nov. 2020
Manager: Carlos V. Rozas; Mentor: Fangfei Liu
Project: Secure Processor Design

- Applied my prior work, *InvarSpec*, on Intel's secure processor design to improve its performance
- Published "Speculative Interference Attacks: Breaking Invisible Speculation Schemes"
- Technology transfer of my prior work

Lyft – Research Intern June 2020 – July 2020

Manager: Ryan Cox; Mentors: Tony Allen, Tianyin Xu (UIUC)

Project: Non-Stop Regression Detection

- Designed a statistical approach to monitor service regressions and bad deployments at Lyft
- Deployed live, monitoring hundreds of critical services at Lyft

Microsoft Research Asia – Research Intern Dec. 2017 – June 2018

Manager: Yongqiang Xiong; Mentor: Guo Chen

Project: Simplified Programming Interface for Large-Scale FPGA Clusters

- Designed an FPGA programming interface that disaggregates a large monolithic FPGA program into several small components that independently run on separate FPGAs

Invited Talks

Everywhere All at Once: Co-Location Attacks on Public Cloud FaaS

- *Intel 2nd Annual Resilient Architectures and Robust Electronics (RARE) Workshop, Oct. 2023*

Untangle: A Principled Framework to Design Low-Leakage, High-Performance Dynamic Partitioning Schemes

- *Semiconductor Research Corporation (SRC) TECHCON, Sept. 2023*
- *Semiconductor Research Corporation (SRC) Hardware Security Annual Review, June 2023*
- *Intel IPAS Tech Sharing, Apr. 2023*
- *28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Mar. 2023*

Binoculars: Contention-Based Side-Channel Attacks Exploiting the Page Walker

- *31st USENIX Security Symposium, Aug. 2022*
- *Security and Privacy Research at Illinois (SPRAI) Seminar, Mar. 2022*

Towards Understanding Spectre-PHT in Memory-Safe Languages

- *6th Workshop on Principles of Secure Compilation (PriSC), co-located with the 49th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL), Jan. 2022*

Pinned Loads: Taming Speculative Loads in Secure Processors

- *Semiconductor Research Corporation (SRC) Hardware Security Annual Review, June 2022*
- *27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Mar. 2022*
- *Intel Labs Webinar, Nov. 2021*

Jamais Vu: Thwarting Microarchitectural Replay Attacks

- *Semiconductor Research Corporation (SRC) Hardware Security Annual Review, June 2021*
- *26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Apr. 2021*
- *Intel Labs Webinar, Feb. 2021*

Speculation Invariance (InvarSpec): Faster Safe Execution Through Program Analysis

- *53rd IEEE/ACM International Symposium on Microarchitecture (MICRO), Oct. 2020*
- *Intel Side Channel Academic Program (SCAP) Workshop, Sept. 2020*

Awards & Honors

- Selected for the PhD Forum at MICRO 2023 Nov. 2023
- W. J. Poppelbaum Memorial Award for Architecture Design Creativity, CS@UIUC Mar. 2023
- Chinese National Software Application Conference Prototype Contest, 3rd Prize Dec. 2018
- International Genetically Engineered Machine Competition, Gold Medal Nov. 2016
- Outstanding Freshman Scholarship Sept. 2015
- Special Freshman Scholarship Sept. 2014

Teaching Experience

Parallel Computer Architecture (UIUC) Teaching Assistant
Instructor: Prof. Josep Torrellas *2023 Spring Semester*

- Gave three lectures on cache coherence and prefetching
- Designed and graded homeworks

C Language Programming II (USTC) Teaching Assistant
Instructor: Prof. Jianhui Ma *2017 Spring Semester*

- Gave one lecture on socket programming
- Mentored students during lab sessions

Electromagnetism B (USTC) Teaching Assistant
Instructor: Prof. Chunkai Xu *2016 Fall Semester*

- Graded homeworks

Mentoring Experience

- Dingyuan Cao, Ph.D. Student at UIUC, with Prof. Josep Torrellas
- David Rudo, Undergraduate Student at CMU, with Prof. Dimitrios Skarlatos
- Tae Hoon Kim, Undergraduate Student at CMU, with Prof. Dimitrios Skarlatos
- Alan Wang, Undergraduate Student at UIUC, with Prof. Christopher W. Fletcher
- Rutvik Choudhary, Ph.D. Student at UIUC, with Prof. Christopher W. Fletcher
- Yingjie Fu, Ph.D. Student at PKU, with Prof. Tao Xie
- Jonathan Osei-Owusu, MSc Student at UIUC, with Prof. Tao Xie
- Guangyao Xu, Undergraduate Intern at UIUC, with Prof. Tao Xie
- Kaiyuan Zhang, MSc Intern at UIUC, with Prof. Tao Xie
- Adelson Aguasvivas, Undergraduate Intern at UIUC, with Prof. Tao Xie

Grant Writing Experience

- Meta Security Research Request for Proposals, Amount $100,000
  Proposal: A Secure Speculative Execution Abstraction Across the OS and Hardware
  PI: Dimitrios Skarlatos, 2022
- Intel Resilient Architectures and Robust Electronics, Amount $255,000
  Proposal: Using Flexible Hardware Isolation for a Secure High-Performance Uncore
  PIs: Josep Torrellas, Tianyin Xu, 2021

Academic Community Service

• Welcomed Prospective Undergraduate Students During Campus Visits (UIUC)	2022, 2023
• 28th International Symposium on Model Checking of Software (SPIN) Web Chair	2022
• Automated Software Engineering (ASE) Co-Reviewer	2020, 2021
• Conference on Computer and Communications Security (CCS) Co-Reviewer	2019
• International Conference on Software Engineering (ICSE) Co-Reviewer	2019