Jiyong Yu

Email : jiyongy2@illinois.edu
Mobile : +1-734-846-1707
Website: jiyongyu.github.io

Education

- **University of Illinois at Urbana-Champaign** Champaign, IL
  Ph.D. in Computer Science (Advisor: Prof. Chris Fletcher) *Aug 2017 - present (expected graduation date: Aug 2023)*
- **University of Michigan** Ann Arbor, MI
  Bachelor of Science in Computer Engineering *Sep 2015 - May 2017*
- **Shanghai Jiao Tong University** Shanghai, China
  Bachelor of Science in Electrical and Computer Engineering *Sep 2013 - Aug 2017*

Work Experience

- **University of Illinois at Urbana-Champaign** Champaign, IL
  Research Assistant *Aug 2017 - present*
  - Design hardware-based defenses for micro-architectural side-channel attacks with provable security
  - Reverse-engineer recent Intel and Apple processors (such as Apple M1) and develop new side-channel attacks
  - Build secure system infrastructures using existing hardware-based security mechanisms (such as Intel SGX)
- **Intel Labs** Hillsboro, OR
  Graduate Technical Intern *May 2021 - Aug 2021*
  - Designed, implemented and evaluated new hardware-based Spectre V1 attack mitigation for future Intel processors
  - The hardware mitigation was directly inspired by my previous publication named "Speculative Taint Tracking"
- **Microsoft Research** Redmond, WA
  Research Intern *May 2020 - Aug 2020*
  - Built an anti-piracy framework for protecting unmodified proprietary software applications using Intel SGX
  - The internship project was later published in SEED 2022
- **Intel Labs** Hillsboro, OR
  Graduate Research Intern *May 2019 - Aug 2019*
  - Analyzed existing speculative side-channel attacks and defenses
  - Modeled and evaluated multiple speculative side-channel defense approaches using a production CPU simulator
  - Identified a new type of speculative side-channel attack and patented the defense mechanism for the attack

Ongoing Projects

- **High-accuracy Timer-less Cache Side-Channel Attacks on Apple M1 (lead author)**
  - Identify new hardware primitives for enabling timer-less micro-architectural side-channel attacks
  - Reverse-engineer Apple M1 cache set index mapping and replacement policy, for high-accuracy cache side-channel attacks
  - Evaluate attacks using standard cryptographic libraries and JavaScript infrastructure
- **Exploiting BTBs on Modern Intel Processors for Byte-level Control-flow Inference (lead author)**
  - Reverse-engineer detail functionality of Branch Target Buffers (BTB) on recent Intel processors.
  - Identify previous-ignored BTB mechanism which enables byte-level control-flow inference.
  - Demonstrate the identified vulnerability can cause both program data and code leakage, under different threat models.

Peer-reviewed Publication

- **Pagoda: Towards Binary Code Privacy Protection with SGX-based Execute-Only Memory; Jiyong Yu**, Xinyang Ge, Christopher W. Fletcher, Trent Jaeger, Weidong Cui. 2nd IEEE International Symposium on Secure and Private Execution Environment Design (**SEED**), 2022

- **Speculative Privacy Tracking (SPT): Leaking Information From Speculative Execution Without Compromising Privacy;** Rutvik Choudhary, **Jiyong Yu**, Christopher W. Fletcher, Adam Morrison. 54th IEEE/ACM International Symposium on Microarchitecture (**MICRO**), 2021

- **Speculative Interference Attacks: Breaking Invisible Speculation Schemes;** Mohammad Behnia, Prateek Sahu, Riccardo Paccagnella, **Jiyong Yu**, Zirui Zhao, Xiang Zou, Thomas Unterluggauer, Josep Torrellas, Carlos Rozas, Adam Morrison, Frank Mckeen, Fangfei Liu, Ron Gabor, Christopher W. Fletcher, Abhishek Basak, Alaa Alameldee. 26th International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**), 2021

- **Speculative Taint Tracking (STT): A Comprehensive Protection for Speculatively-Accessed Data; Jiyong Yu**, Mengjia Yan, Artem Khyzha, Adam Morrison, Josep Torrellas, Christopher W. Fletcher, **Communications of the ACM, Research Highlight**, 2021

- **Exposing cache timing side-channel leaks through out-of-order symbolic execution;** Shengjian Guo, Yueqi Chen, **Jiyong Yu**, Meng Wu, Zhiqiang Zuo, Peng Li, Yueqiang Cheng, and Huibo Wang Object-Oriented Programming, Systems, Languages, and Applications (**OOPSLA**), 2020

- **Speculation Invariance (InvarSpec): Faster Safe Execution Through Program Analysis;** Zirui Zhao, Houxiang Ji, Mengjia Yan, **Jiyong Yu**, Christopher W. Fletcher, Adam Morrison, Darko Marinov, Josep Torrellas. 53rd IEEE/ACM International Symposium on Microarchitecture (**MICRO**), 2020

- **Speculative Data-Oblivious Execution: Efficient Elimination of Speculative Covert Channels; Jiyong Yu**, Namrata Mantri, Josep Torrellas, Adam Morrison, Christopher W. Fletcher, 47th International Symposium on Computer Architecture (**ISCA**), 2020 [**Intel Hardware Security Academic Award, 1st Place**]

- **Creating Foundations for Secure Microarchitectures with Data-Oblivious ISA Extensions; Jiyong Yu**, Lucas Hsiung, Mohamad El Hajj, Christopher W. Fletcher. IEEE Micro Top Picks, 2020

- **Speculative Taint Tracking: A Comprehensive Protection for Speculatively Accessed Data; Jiyong Yu**, Mengjia Yan, Artem Khyzha, Adam Morrison, Josep Torrellas, Christopher W. Fletcher. IEEE Micro Top Picks, 2020

- **Speculative Taint Tracking: A Comprehensive Protection for Speculatively Accessed Data; Jiyong Yu**, Mengjia Yan, Artem Khyzha, Adam Morrison, Josep Torrellas, Christopher W. Fletcher. 52nd ACM/IEEE International Symposium on Microarchitecture (**MICRO**), 2019 [**Best Paper Award**]

- **Data Oblivious ISA Extensions for Side Channel-Resistant and High Performance Computing; Jiyong Yu**, Lucas Hsiung, Mohamad El Hajj, Christopher W. Fletcher. 26th Network and Distributed System Security Symposium (**NDSS**), 2019 [**Distinguished Paper Award Honorable Mentions**] [**CSAW 2019 Finalist**]

- **UCNN: Exploiting Computational Reuse in Deep Neural Networks via Weight Repetition;** Kartik Hegde, **Jiyong Yu**, Rohit Agrawal, Mengjia Yan, Michael Pellauer, Christopher W. Fletcher. 45th International Symposium on Computer Architecture (**ISCA**), 2018

Honors and Awards

- Best Paper Award: MICRO'19

- Distinguished Paper Award Honorable Mentions: NDSS'19

- Intel Hardware Security Academic Award, 1st place, 2021

- CSAW'19 Applied Research Finalists

- CACM Highlight

- 2x IEEE MICRO Top Picks

- Microsoft Research PhD Fellowship, 2020-2022

- W.J. Poppelbaum Scholarship, 2021

Patents

APPARATUS AND METHOD FOR NON-SPECULATIVE RESOURCE DEALLOCATION
Inventors: Fangfei Liu, Carlos Rozas, Thomas Unterluggauer, Francis Mckeen, Alaa Alameldeen, Abhishek Basak, Xiang Zou, Ron Gabor, **Jiyong Yu**
Applicant: Intel Corporation, Santa Clara, CA, US
Application No. 16/728815

Programming Languages

C/C++, Python, x86/ARM Assembly, BASH scirpting, Verilog