

Yun Chen

Google Scholar

+65 91576198 | yun.chen@u.nus.edu | [linkedin.com/in/yun-chen-274006208](https://www.linkedin.com/in/yun-chen-274006208)

Education

National University of Singapore

PhD in Computer Science

- GPA: 4.25/5

Singapore

2020 - Current

Beijing Institute of Technology

MPhil in Cybersecurity

- GPA: 86/100

Beijing, China

2017 - 2020

Henan University

BEng in Computer Science

- GPA: 86/100

Kaifeng, China

2013 - 2017

Research Interests

Computer Architecture, Hardware and Embedded System Security, Side-Channel Attack, Trusted Computing

Research Experience

National University of Singapore

Ph.D. Candidate (advised by Prof. Trevor E. Carlson)

Singapore

2020 - Current

- New CPU microarchitecture against physical side-channel attacks.** Develop an out-of-order processor capable of securely reordering instructions to mitigate power side-channel attacks while minimizing performance overhead and optimizing power efficiency.
- Novel microarchitectural side-channel attack on x86 via IP-stride prefetcher.** Reverse-engineer the Intel IP-stride prefetcher and present a novel side-channel attack capable of leaking control flow by mis-training the hardware IP-stride prefetcher. ***Approved by Intel.**
- Novel microarchitectural side-channel attack on x86 via XPT prefetcher.** Reverse-engineer the Intel eXtended Prediction Table (XPT) prefetcher and present a novel side-channel attack capable of leaking the victim's page activities by selectively resetting the XPT prefetcher's status. ***Approved by Intel.**
- Novel transient attack on x86 via Loop Stream Detector (LSD).** Reverse-engineer the Intel LSD and present a novel transient attack primitive by LSD. ***Approved by Intel.**
- Automatic side-/covert-channel leakage detection on ARM TrustZone.** Design a comprehensive and automatic side-channel vulnerability analysis tool on ARM TrustZone. Build a new cross-world and cross-core covert-channel attack via the analysis tool.
- Side-channel-resilient TEE.** A smart trusted firmware-driven isolation mechanism that can isolate PMUs and caches between the trusted zone and the untrusted zone with negligible performance overhead.
- Out-of-order commit processor (side project).** Develop an out-of-order processor that can out-of-order commit instructions without modifying the compiler or operating system, hence improving the processor's IPC.

Work Experience

AMD

Research Intern (managed by Prof. Nachiket Kapre (PMTS in AMD))

Singapore

May 2022 - February 2023

- CGRA Verification.** Build an automatic verification toolkit for verifying the functionalities and correctness of hardware.
- Customize the AMD-Xilinx Nanotube compiler.** Develop and extend the Nanotube compiler for the programmable RDMA SmartNIC project.
- Programmable RDMA SmartNIC using CGRA.** Build RDMA packetization and de-packetization eBPF code via nanotube compiler to accelerate the RDMA throughput and make it programmable. ***Internal Patent Application Award.**

Publications

CONFERENCE PAPERS

GadgetSpinner: A New Loop Stream Detector-Based Transient Execution Primitive

Yun Chen, Ali Hajiabadi, Trevor E Carlson

International Symposium on High-Performance Computer Architecture (HPCA), 2024

PrefetchX: Cross-Core Cache-Agnostic Prefetcher-Based Side-Channel Attacks

Yun Chen, Ali Hajiabadi, Lingfeng Pei, Trevor E Carlson

International Symposium on High-Performance Computer Architecture (HPCA), 2024

Prime+Reset: Introducing A Novel Cross-World Covert-Channel Through Comprehensive Security Analysis on ARM TrustZone

Yun Chen, Arash Pashrashid, Yongzheng Wu, Trevor E Carlson

AfterImage: Leaking Control Flow Data and Tracking Load Operations via the Hardware Prefetcher

Yun Chen, Lingfeng Pei, Trevor E. Carlson

International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2023

Optimal Attack Path Generation Based on Supervised Kohonen Neural Network

Yun Chen, Kun Lv, Changzhen Hu

International Conference on Network and System Security (NSS), 2017

JOURNAL PAPERS

Dynamic defense strategy against advanced persistent threat under heterogeneous networks

Kun Lv, **Yun Chen (corresponding author)**, Changzhen Hu

Information Fusion (IF = 17.6) 49 (2019) pp. 216–226. 2019

DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks

Yun Chen, Hui Xie, Kun Lv, Shengjun Wei, Changzhen Hu

Information Sciences (IF = 8.2) 501 (2019) pp. 100–117. 2019

A dynamic hidden forwarding path planning method based on improved Q-learning in SDN environments

Yun Chen, Kun Lv, Changzhen Hu

Security and Communication Networks (IF = 1.98) 2018 (2018). 2018

UNDER REVIEW

PARADISE: Mitigating Power Attacks through Fine-Grained Instruction Reordering

Yun Chen, Ali Hajiabadi, Romain Poussier, Yaswanth Tavva, Andreas Diavastos, Shivam Bhasin, Trevor E Carlson

Under Review, 2021

Teaching and Mentoring Experience

2024 **CS2100 Computer Organization 2024 Spring, Teaching Assistant**, National University of Singapore

Singapore

2023 **Teaching Workshop, Participant**, National University of Singapore

Singapore

2023 **Chun Yu Lam, Research Mentor**, National University of Singapore

Singapore

Skills

Programming C, Chisel, Python, SystemVerilog

Miscellaneous Reverse-Engineering, Linux, Shell (Bash), AWS EC2, $\text{\LaTeX}$ (Overleaf), Git, Chipyard, FireSim, Commercial CAD tools (Synopsys DC, PrimePower, etc.)

Awards and Honors

2023 **ASPLOS Travel Grant**, ASPLOS 2023

Canada

2023 **Incentive Award**, National University of Singapore

Singapore

2022 **AMD Internal Patent Application Award**, Advanced Micro Devices Inc.

Singapore

2022-2023 **Research Achievement Award**, National University of Singapore

Singapore

2020-2024 **NUS Research Scholarship**, National University of Singapore

Singapore

2017-2019 **Academic Scholarship**, Beijing Institute of Technology

China

2013-2017 **Henan University Scholarship**, Henan University

China