Ruiyi Zhang

ruiyi.zhang@cispa.de · zhangruiyi.me/ ·

Research Interests

My research focuses on CPU and systems security, including software-induced CPU faults, side-channel attacks, and the security of trusted execution environments (TEE).

Education

04/2021 – present **CISPA Helmholtz Center for Information Security**
Ph.D. in Computer Science
Supervisor: Michael Schwarz

09/2015 – 06/2019 **University of Electronic Science and Technology of China**
B.E. in Software Engineering (Computer Security)

Employment

04/2021 – present **CISPA Helmholtz Center for Information Security**
Ph.D. Student with Michael Schwarz

08/2024 – 11/2024 **Google Research**
Research Intern with Adria Gascon, Daniel Moghimi

07/2018 – 03/2021 **PeckShield Inc.**
Security Researcher with Lei Wu, Xuxian Jiang

Conference Publications

Note: Conferences such as IEEE S&P, USENIX Security, CCS, NDSS, and ASPLOS are ranked at the highest level (A*).
Google Scholar: https://scholar.google.com/citations?user=jqaD56sAAAAJ

[C1] **Ruiyi Zhang**, Tristan Hornetz, Daniel Weber, Fabian Thomas, Michael Schwarz, *Title Under Embargo.*
USENIX Security Symposium (USENIX Security '2026).

[C2] **Ruiyi Zhang**, Albert Cheu, Adria Gascon, Daniel Moghimi, Phillipp Schoppmann, Michael Schwarz, Octavian Suciu, *SNPeek: A Side-Channel Analysis Framework for Privacy Applications on Confidential Virtual Machines* [pdf].
Network and Distributed System Security (NDSS '2026)

[C3] Fabian Thomas, Eric García Arribas, Lorenz Hetterich, Daniel Weber, Lukas Gerlach, **Ruiyi Zhang**, Michael Schwarz, *Automatic Discovery of User-exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs* [pdf].
ACM Conference on Computer and Communications Security (CCS '2025)

[C4] **Ruiyi Zhang**, Tristan Hornetz, Lukas Gerlach, Michael Schwarz, *Taming the Linux Memory Allocator for Rapid Prototyping* [pdf].
Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA '2025)

[C5] Lorenz Hetterich, Fabian Thomas, Lukas Gerlach, **Ruiyi Zhang**, Nils Bernsdorf, Eduard Ebert, Michael Schwarz, *ShadowLoad: Injecting State into Hardware Prefetchers* [pdf].

Architectural Support for Programming Languages and Operating Systems (ASPLOS '2025).

[C6] **Ruiyi Zhang**, Lukas Gerlach, Daniel Weber, Lorenz Hetterich, Youheng Lü, Andreas Kogler, Michael Schwarz, *CacheWarp: Software-based Fault Injection using Selective State Reset* [pdf].
USENIX Security Symposium (USENIX Security '2024).

[C7] **Ruiyi Zhang**, Daniel Weber, Taehyun Kim, Michael Schwarz, *(M)WAIT for It: Bridging the Gap between Microarchitectural and Architectural Side Channels* [pdf].
USENIX Security Symposium (USENIX Security '2023).

[C8] Lukas Gerlach, Daniel Weber, **Ruiyi Zhang**, Michael Schwarz, *A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs* [pdf].
IEEE Symposium on Security and Privacy (IEEE S&P '2023)

[C9] Daniel Weber, Lukas Gerlach, Fabian Thomas, **Ruiyi Zhang**, Michael Schwarz, *Indirect Meltdown: Building Novel Side-Channel Attacks from Transient-Execution Attacks* [pdf].
European Symposium on Research in Computer Security (ESORICS '2023)

[C10] Daniel Weber, Lukas Gerlach, Fabian Thomas, **Ruiyi Zhang**, Michael Schwarz, *Reviving Meltdown 3a* [pdf].
European Symposium on Research in Computer Security (ESORICS '2023)

Before PhD

** denotes equal contributions*

[C11] Ningyu He*, **Ruiyi Zhang***, Haoyu Wang, Lei Wu, Xiapu Luo, Yao Guo, Ting Yu, Xuxian Jiang, *EOSAFE: Security Analysis of EOSIO Smart Contracts* [pdf].
USENIX Security Symposium (USENIX Security '2021)

Honors and Awards

2025 **Cybersecurity Award for Best Hardware and Physics Paper**, SpringerOpen

2024 **Distinguished Artifact Reviewer**, USENIX Security Symposium

2023-2025 **Acknowledged in AMD Security Bulletin (CVE-2023-20592, Two under embargo)**

Teaching

2025 Summer **Foundation of Cybersecurity (Undergraduate Course) - CISPA**
Role: Guest Lecturer

2023 Winter **Side Channel Attacks and Defenses (Graduate Course) - CISPA**
Role: Teaching Assistant

Service

- **Search Committee** — CISPA Summer Research Internship Program, 2026
- **Reviewer** — IEEE Transactions on Information Forensics and Security (TIFS), 2025
- **Sub-Reviewer** — USENIX Security Symposium 2023/2024/2025/2026,
  ACM CCS 2024, NDSS Symposium 2025/2026,
  ESORICS 2023, DIMVA 2024

- **Artifact Evaluation Committee** — USENIX Security Symposium, 2023/2024.

Selected Media Coverage

08/2024 Tom's Hardware. *GhostWrite vulnerability exploits architectural bug in RISC-V CPU to gain root access* [link]

08/2024 The Register. *Faulty instructions in Alibaba's T-Head C910 RISC-V CPUs blow away all security* [link]

11/2023 BleepingComputer. *New CacheWarp AMD CPU attack lets hackers gain root in Linux VMs* [link]

11/2023 The Hacker News. *CacheWarp Attack: New Vulnerability in AMD SEV Exposes Encrypted VMs* [link]

11/2023 DarkReading. *CacheWarp' AMD VM Bug Opens the Door to Privilege Escalation* [link]

Invited Talks

05/2025 AICrypt Workshop (Co-located with EUROCRYPT 2025)
Side-Channel Privacy Attacks in Confidential VMs

08/2024 Black Hat USA, Briefings
Arbitrary Data Manipulation and Leakage with CPU Zero-Day Bugs on RISC-V

11/2022 Black Hat Middle East and Africa, Briefings
Bridging the Gap between Microarchitectural and Architectural Side Channels