ZIHOU REN

Phone: (+86)18811137173 ◇ Email: renzihou2012@163.com ◇ Profile: https://zihou.ren

EDUCATION

Tsinghua University — *Ph.D. Student, Cyberspace Security* *Sep. 2024–Jul. 2029*
Institute for Network Sciences and Cyberspace; GPA: 4.0/4.0.
Research interests: systems security, container security, and kernel performance profiling.

Tsinghua University — *B.Eng., Computer Science and Technology* *Sep. 2020–Jul. 2024*
Department of Computer Science and Technology; GPA: 3.8/4.0; top 30% of the department.
Tsinghua University Scholarship for Excellence in Science and Technology Innovation.

INTERNSHIPS

Shanghai SiOrigin Technology Co., Ltd. *Sep. 2025–May 2026*
RISC-V compiler middle-end and back-end development and performance optimization:

- Implemented the full translation pipeline from builtins to assembly for 1,000+ custom instructions.
- Designed dataflow analysis & peephole optimizations to improve cache utilization and performance.

Shanghai Zhizhenjunzhi Technology Co., Ltd. *Jun. 2023–Jul. 2023*
Researched unknown network protocol identification; built a feature extraction and classification system using clustering and deep learning (CNNs, LSTMs) for noisy, high-dimensional network traffic sequences.

RESEARCH

Network and System Reliability and Security Lab, Tsinghua University *Apr. 2023–Present*
Advisor: Associate Professor Long Wang

- **Z. Ren**, *et al.* No Touching Others' Assets: Detecting Container Escapes via CAGEGuard. *Submitted to USENIX Security.* Modeled container boundaries through asset ownership and detected escapes using eBPF; achieved a 90% detection rate with low false positives and overhead.
- **Z. Ren**, *et al.* RootSeeker: Evidence-Guided Root Cause Analysis for Container Escapes. *Submitted to Journal of Software.* Designed AI agent harness which can help Locating source-code vulnerabilities that lead to container escapes; achieved 48% function-level accuracy.
- **Z. Ren**, *et al.* REALM: Identifying Minimal Task Assets for LLM Agents. arXiv:2610.39155: Identify the minimal assets set that should be accessible to an LLM agent based on user tasks, addressing the issue of overly broad permissions in traditional containers and resisting external malicious instruction injection. On the AgentDyn dataset, using qwen3.5-flash as the base model, the attack success rate was reduced from 19% to 0.2%.
- C. Liu, **Z. Ren**, *et al.* Understanding eBPF Performance Overhead. *Submitted to EuroSys.* Systematically measured eBPF performance overhead.

Intelligent Technology and Systems Lab, Tsinghua University *Sep. 2022–Mar. 2023*
Advisor: Professor Yiqun Liu

- Studied user click models and reinforcement learning for ranking tasks.

Institute of HCI and Media Integration, Tsinghua University *Sep. 2021–Jun. 2022*
Advisor: Professor Jiangtao Wen

- X. Zhang, **Z. Ren**, *et al.* Phocus: Picking Valuable Research from a Sea of Citations. arXiv:2201.02915. Used neural networks to assess citation importance and to judge the quality of research.

SKILLS

Programming: Python, C/C++, Rust, JavaScript, HTML/CSS
Vibe Coding: Codex, Claude Code, skill authoring
Machine Learning: PyTorch
High-Performance Computing: eBPF, DPDK, perf
Tools: Git, CMake, LLVM, Docker, LaTeX
English: CET-6, 649/710

LEADERSHIP AND SERVICE

Tsinghua University Ski Team — *Captain* *Mar. 2025–Feb. 2026*
Undergraduate Compilers Course — *Teaching Assistant* *Sep. 2024–Present*
Tsinghua University Student Ski Association — *President* *Sep. 2023–Aug. 2024*