任自厚

电话: (+86)18811137173 ◇ 邮箱: renzihou2012@163.com ◇ 主页: https://zihou.ren

教育

清华大学 直博生（网络空间安全） *2024.9 - 2029.7*

网络科学与网络空间研究院，学分绩 4.0/4.0，研究方向为系统安全、容器安全、系统内核性能测绘。

清华大学 工学学士（计算机科学与技术） *2020.9 - 2024.7*

计算机科学与技术系，学分绩 3.8/4.0，系排名前 30%。获得清华大学科技创新优秀奖学金。

实习

上海紫荆芯界智能科技有限公司 *2025.9 - 2026.5*

参与 RISCV 编译器中后端开发与性能优化：

- 实现扩展指令集（自定义指令数量 1000+）从 builtin 到汇编指令的完整翻译链路；
- 设计并实现基于硬件特性的数据流分析算法和多个窥孔优化算法，提高缓存利用率和计算性能。

上海直真君智科技有限公司 *2023.6 - 2023.7*

研究未知网络协议识别算法：针对高维、高噪声的网络流量序列数据，设计并实现基于聚类算法和深度学习模型（CNN、LSTM）的特征提取与分类系统。

科研

清华大学 网络与系统可靠性与安全实验室 王龙 副教授 *2023.4 至今*

- **Z. Ren**, *et al.* No Touching Others' Assets: Detecting Container Escapes via CAGEGuard（USENIX Security 在投，**CCF-A**）：基于资产所有权的容器边界建模与基于 eBPF 的容器逃逸检测，检测成功率 90%，低假阳性，低开销;
- **任自厚**, *et al.* RootSeeker: 面向容器逃逸的证据引导根因分析（《软件学报》在投，**CCF-中文 A**）：通过自纠错设计与面向智能体的日志、代码检索引擎编写，引导智能体分析容器逃逸日志、定位源码中的漏洞，端到端函数准确率 48%；
- **Z. Ren**, *et al.* REALM: Identifying Minimal Task Assets for LLM Agents (arXiv:2610.39155)：基于用户任务确定 LLM Agent 可访问的最小资产集合，解决传统容器等授权过宽的问题，抵抗外部恶意指令注入。在 AgentDyn 数据集上使用 qwen3.5-flash 作为基座模型，将攻击成功率从 19% 降低至 0.2%。
- C. Liu, **Z. Ren**, *et al.* Understanding eBPF Performance Overhead（EuroSys 在投，**CCF-A**）：系统性 eBPF 性能开销测量；

清华大学 智能技术与系统实验室 刘奕群 教授 *2022.9 - 2023.3*

- 研究用户点击模型、强化学习在排名任务中的应用。

清华大学 人机交互与媒体集成研究所 温江涛 教授 *2021.9 - 2022.6*

- X. Zhang, **Z. Ren**, *et al.* Phocus: Picking Valuable Research from a Sea of Citations (arXiv:2201.02915)：借助神经网络评价论文中不同引用的重要性，构建更好的论文评价体系。

技能

编程语言 Python, C/C++, Rust, Javascript, HTML/CSS

Vibe Coding Codex, Claude Code, Skills 编写

机器学习 PyTorch

其他工具 Git, CMake, LLVM, Docker, LaTeX

高性能计算 eBPF, DPDK, perf

英语水平 大学英语六级 649/710

社工

清华大学滑雪队 队长 *2025.3 - 2026.2*

本科生课程《编译原理》 助教 *2024.9 至今*

清华大学学生滑雪协会 会长 *2023.9 - 2024.8*