

# 谢厚龙

手机：(+86) 19121220286 · 邮箱：pxhl@qq.com

性别：男 · 籍贯：江苏 · 年龄：25 岁



## 教育背景

华东师范大学 (985), 软件工程学院, 研究生硕士 2022.09 - 2026.06  
中国矿业大学 (211), 计算机科学与技术学院, 本科, 保研 2018.09 - 2022.06

## 项目经历

基于大模型增强的网络协议模糊测试技术研究, 科研项目 2025.08 - 2026.02

- **情况**: 网络协议是现代信息系统的基础设施, 传统基于变异的模糊测试普遍受到初始种子质量低和随机字节变异破坏语法的限制, 难以有效探索协议状态空间并触发潜在漏洞。
- **任务**: 作为项目负责人, 确定改进方向并制定技术路线, 研发一款能够提升种子质量和变异策略效率的模糊测试工具, 借助大模型能力提高网络协议漏洞挖掘成效。
- **行动**: 以 DeepWiki 协议实现信息为核心构建“清洗—语义原子化—文档树分块—向量化检索”的协议知识库, 提出语义感知分块算法以减轻大模型幻觉和版本偏差; 设计基于知识库的种子丰富智能体, 使用“检索—生成—校验” ReAct 闭环生成并验证高质量交互序列, 弥补缺失消息类型并扩大状态空间; 聚合字段约束构建可解析的细粒度语法模板, 通过少样本提示与自一致性检查抑制模板漂移, 自动映射约束类型到保持和破坏两类变异策略, 引入自适应调度在约束驱动和随机变异间权衡; 最终实现并开源大模型增强的模糊测试工具 XPGFuzz。
- **结果**: 在 ProFuzzBench 平台全面对比 AFLNet 和 ChatAFL 等工具, XPGFuzz 相比 AFLNet 在状态覆盖、状态迁移覆盖、分支覆盖和行覆盖上平均提升 25.43%、54.37%、13.38% 和 12.26%, 相比 ChatAFL 同指标平均提升 15.49%、32.39%、14.25% 和 12.36%, 并发现对比工具未能挖掘的独有漏洞, 显著提升了网络协议安全测试的覆盖度与深度。

## 实习经历

上海英特尔公司固件自动化测试开发, Client 内存初始化组 2023.12 - 2024.06

- **情况**: 所在组负责 PC 内存初始化模块, 为固件自动化测试平台提供支撑。原有串口监听与日志分发软件在重启后需重新启服, 无法满足多机、多读者实时采集 BIOS 串口日志的需求, 影响测试效率与流水线稳定性。
- **任务**: 用 Python 从零开发可替代的串口监听与日志分发服务 (serial-listener), 支持多客户端并发读、单客户端写, 常驻运行、无需随测试重启; 纳入组内测试仓库, 支撑多台测试机部署与 CI/CD 集成。
- **行动**: 设计 C/S 架构: 服务端多线程 HTTP 处理读/写请求, 为每个客户端维护独立读指针、按区间返回增量日志, 串口数据以字节流落盘避免编码问题; 封装 Server/Client 类, 通过端口占用检测与后台常驻避免多实例; 实现自动检测可用串口及按偏移拉取等接口, 便于测试脚本与 CI 调用。
- **行动**: 多机部署中处理端口占用、时序与代理策略 (如内网代理配置); 用 PyInstaller 打包 exe 并规范虚拟环境与最小依赖, 便于在无 Python 环境的测试机上分发; 参与 GitHub Actions CI 与 self-hosted runner 的配置与调试 (代理与 PowerShell 环境变量排查)。
- **结果**: 替代方案通过组内验证并合入主仓, 在多台测试机 (含海外环境) 上大规模部署; 无需重启即可支持多客户端实时读、单客户端写, 稳定支撑固件自动化测试流水线; 期间熟悉 UEFI/BIOS 与串口调试、CI/CD 与内网部署实践。

## 专业技能

- **编程语言**: 精通 Python。熟悉 C、C++、Java 等编程语言。
- **提示词工程**: 深度 AI 用户。目前 AI token 费用每月超过 20 美元。
- **AI 工具**: 熟练使用 Dify、Coze、Linkai 等 AI 智能体开发平台。
- **AI 编程工具**: 熟练使用 Cursor、Claude code 进行 vibe coding。
- **开源**: 热衷开源, 熟练使用 Git 进行版本控制。开源网站: <https://github.com/08183080>。
- **个人网站**: 2026 年, 空闲时运用 Cursor 编程, 搭建了个人网站: <https://www.aixpg.one/>。
- **其他**: 熟练使用 Linux, Docker, Latex, Github, Vercel, 爬虫, Langchain, ChatAFL 等工具。