陈力恒

方向：隐私计算（TEE&MPC）、模糊测试

团队：清华 Vul337　　**手机：**15381969076

导师：张超老师　　**邮箱：**791960492@qq.com

教育及经历

2014-2018　　北京交通大学 本科　　信息安全及金融学（双学位）

- 排名：计算机 6/300+，信安 2/23。

2018-2021　　中国科学院大学（软件所） 硕士　　计算机软件与理论

- 研究内容：围绕 CPU 及 TEE 的侧信道攻防。

2021-至今　　清华大学（网研院 Vul337）&中国科学院大学（信工所） 博士　　网络空间安全

- *2021-2023* 深入分析 SGX 模型特点并构建多维结构化高效的 SGX 应用模糊测试框架 EnclaveFuzz，被 NDSS 2024 接收（BIG4, CCF-A，一作），已开源（https://github.com/vul337/EnclaveFuzz）。
- *2022-2023* 参与研究模糊测试中利用优化过的数据控制流图改进种子调度策略，被 TOSEM 2024 接收（CCF-A，二作），已开源（https://github.com/vul337/Graphuzz）。
- *2023-至今* 负责蚂蚁隐语的安全及功能性测试工作（校企合作），结合了人工审计和自动化测试等方法，已发现若干设计问题及代码实现问题。正开展第二年期工作，旨在正式发布隐语。同时依托项目开展 MPC 框架差分测试及 Fuzzing Roadblocks 绕过等研究点。
- *2023-至今* 北京互娱首席科学家，负责广告投放平台（带 DMP 的 DSP）的设计，重点在提供隐私计算能力和数据合作方构建更强的用户画像。

自我评价

目前的研究方向为机密计算、隐私计算、模糊测试和静态程序分析。隐私计算方面，感兴趣于利用硬件能力保护数据隐私助力创造数据价值，以及在 AI 模型的交付部署过程中保护其安全。机密计算方面，感兴趣于 TEE 的应用以及针对 CPU 和 TEE 的侧信道攻击和防御。未来也希望利用 AI 基于软件基因重构软件生态，并设计下一代的硬件设施。

技能及其它

语言方面：对 C++（300k+开发量）/Python 较为熟练，对 OCaml/Rust 有一定基础。

架构方面：对 Linux 用户态程序/编译器较为熟练，对 CPU/Kernel 及其驱动/虚拟机有一定经验。

GitHub：https://github.com/LeoneChen Blog：https://blog.csdn.net/clh14281055