

# 卢弘毅

+86 156 2529 0103   ◇   [luhy2017@mail.sustech.edu.cn](mailto:luhy2017@mail.sustech.edu.cn)   ◇   <https://hongyi.lu>

## 教育背景

香港科技大学 计算机科学博士	2022 – 至今
南方科技大学 数学学士	2017 – 2021

## 工作经历

COMPASS Lab.   科研助理 ↔ 张锋巍教授 • 完成计算机系统相关的研究工作。	Nov. 2021 – 2022 南方科技大学
---	----------------------------

## 学术发表

[1] Lijian Huang\*, **Hongyi Lu\***, Shuai Wang, and Fengwei Zhang. Towards Secure BPF Kernel Extension with Hardware-enhanced Memory Isolation. In *Major Revision with TDSC*, 2026.

[2] **Hongyi Lu**, Fengwei Zhang, Zhenkai Zhang, Shuai Wang, and Yanan Guo. CuSAFE: Capturing Memory Corruption on NVIDIA GPUs. In *Submission with USENIX Security*, 2026.

[3] **Hongyi Lu\***, Yunjie Deng\*, Sukarno Mertoguno, Shuai Wang, and Fengwei Zhang. MOLE: Breaking GPU TEE with GPU-Embedded MCU. In *the Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS, CCF-A)*, 2025.

[4] **Hongyi Lu**, Zhibo Liu, Shuai Wang, and Fengwei Zhang. DTD: Comprehensive and Scalable Testing for Debuggers. In *the Proceedings of the ACM on Software Engineering (FSE, CCF-A)*, 2024.

[5] **Hongyi Lu**, Shuai Wang, Yechang Wu, Wanning He, and Fengwei Zhang. MOAT: Towards Safe BPF Kernel Extension. In *33nd USENIX Security Symposium (USENIX Security, CCF-A)*, 2024.

[6] Wanning He\*, **Hongyi Lu\***, Fengwei Zhang, and Shuai Wang. RingGuard: Guard io\_uring with eBPF. In *the Proceedings of the 1st Workshop on eBPF and Kernel Extensions (eBPF)*, pages 56–62, 2023.

[7] Haonan Li, Weijie Huang, Mingde Ren, **Hongyi Lu**, Zhenyu Ning, Heming Cui, and Fengwei Zhang. A Novel Memory Management for RISC-V Enclaves. In *the Proceedings of the 10th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP)*, 2022.

[8] **Hongyi Lu** and Fengwei Zhang. Raven: a Novel Kernel Debugging Tool on RISC-V. In *the Proceedings of the 59th ACM/IEEE Design Automation Conference (DAC, CCF-A)*, pages 1039–1044, 2022.

[9] **Hongyi Lu**, Yechang Wu, Shuqing Li, You Lin, Chaozu Zhang, and Fengwei Zhang. BADUSB-C: Revisiting BadUSB with Type-C. In *2021 IEEE Security and Privacy Workshops (WOOT)*, pages 327–338, 2021.

我合计作为第一作者/共同第一作者（以 \* 标记）发表**四篇 CCF-A 类论文**，其中两篇是安全领域的“四大”会议。另外，我还有一篇在投的安全“四大”论文与一篇正在大修的 CCF-A 类期刊论文。

## 学术服务

正式审稿人	TIFS, TDSC
外部审稿人	USENIX Security 2023, S&P 2023, PoPET 2023, CCS 2023, CCS 2022

## 项目介绍

**论文项目：**CuSAFE   [sites.google.com/view/safe-gpu](https://sites.google.com/view/safe-gpu)

我们创建了一个名为 CuSAFE 的系统。该系统支持对 CUDA 程序中的内存安全问题进行检测。

我们的评测显示 CuSAFE 在性能和准确率两方面都超越了已有的相关工具，例如 compute-sanitizer（由 NVIDIA 开发），cuCatch（PLDI’ 22，由 NVIDIA 开发）与 LMI（HPCA’ 25）

我提出了该项目并作为唯一的学生负责该项目，我独自完成了整个项目的开发。2025

**论文项目：**MOLE (CCS’ 25)   [sites.google.com/view/mole-gpu](https://sites.google.com/view/mole-gpu)

我们提出了一种针对现有 GPU 可信执行环境的新式攻击。该攻击利用了一个在 Arm GPU 中的隐藏 MCU 来破坏 GPU 可信执行环境的安全性。

该攻击攻破了多个 GPU 可信执行环境，例如 StrongBox（CCS’ 22，由蚂蚁集团开发）、CAGE（NDSS’ 24，由蚂蚁集团开发）和 MyTEE（NDSS’ 23）。

我提出了该项目并作为项目负责人，我开发了该项目的大部分代码，另一位同学邓韵杰完成了 OpenCL 用户态攻击组件与攻击测试程序的开发。2025

**论文项目：**MOAT (USENIX Security’ 24)   [sites.google.com/view/safe-bpf](https://sites.google.com/view/safe-bpf)

我们创建了一个名为 MOAT 的系统。该系统能够利用 Intel MPK/Arm StageII 等硬件特性隔离恶意 BPF 程序以阻止对它们内核的攻击

我们正在与企业合作将该项目推向生产环境，该项目提供了**117 万人民币的资助**。

我提出了该项目并作为项目负责人，我独自完成了整个项目的开发。目前与企业的合作由我负责指导，另一位同学黄沥剑负责开发。2024

**发明专利 2022 1 0436969.8**

内核空间调试方法及其装置、计算机设备、存储介质2022

《软件基础》翻译工作   [coq-zh.github.io/SF-zh](https://coq-zh.github.io/SF-zh)

我协助翻译了《软件基础》中的部分内容。《软件基础》是形式化验证领域的一本知名教科书。2022

**论文项目：**BadUSB-C (WOOT’ 21)

我们发现了针对 USB-C 设备的一种新式攻击，其利用 USB-C 的视频传输能力增强了传统 BadUSB 的攻击能力。该项目被受影响企业认定为高危漏洞，我们因此获得了**3 万元人民币的赏金**2021