LU HONGYI

+86 156 2529 0103 ◇ luhy2017@mail.sustech.edu.cn ◇ https://hongyi.lu

Education

HKUST **2022 – Present**
Ph.D. Computer Science

SUSTech **2017 – 2021**
B.Sc. Mathematics

Working Experience

COMPASS Lab. *Research Assistant* **Nov. 2021 – 2022**
↪ Prof. Zhang Fengwei *Southern University of Science and Technology*

- Conducted research in computer systems.

Publications

[1] Lijian Huang*, **Hongyi Lu***, Shuai Wang, and Fengwei Zhang. Towards Secure BPF Kernel Extension with Hardware-enhanced Memory Isolation. In *IEEE Transactions on Dependable and Secure Computing (**TDSC, CCF-A**)*, 2026.

[2] **Hongyi Lu**, Fengwei Zhang, Zhenkai Zhang, Shuai Wang, and Yanan Guo. CuSafe: Capturing Memory Corruption on NVIDIA GPUs. In *35nd USENIX Security Symposium (**USENIX Security, CCF-A**)*, 2026.

[3] **Hongyi Lu**. Hardware-assisted Memory Isolation. In *the Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (**CCS, PhD Symposium**)*, 2025.

[4] **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.

[5] **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.

[6] **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.

[7] 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.

[8] 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.

[9] **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.

[10] **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.

Academic Service

Official Reviewer TIFS, TDSC

Ext. Reviewer USENIX Security 2023, S&P 2023, PoPET 2023, CCS 2023, CCS 2022

Grant & Awards

CCS Student Grant $1750 **2025**

USENIX Security Student Grant $625 **2024**

Projects

Note: Descriptions in *Contribution* are confirmed by my collaborators.

CuSafe

We built a system named CuSafe. It detects memory safety vulnerabilities in CUDA programs.

Our evaluation shows that CuSafe beats existing tools such as compute-sanitizer (**NVIDIA**), cuCatch (PLDI '22, **NVIDIA**), and LMI (HPCA' 25) in both performance and accuracy; CuSafe also supports the LLMs such as LLaMA2 and LLaMA3. CuSafe is approx. 13× faster than the compute-sanitizer, which is the official tool provided by **NVIDIA**.

Contribution: I proposed this project and worked as the sole student; I completed the whole project myself. **2025**

Mole (CCS' 25) sites.google.com/view/mole-gpu

We proposed a new attack against existing GPU TEEs; it leverages an under-documented MCU in Arm Mali GPUs to break the security of GPU TEEs. **Arm** have acknowledged our findings and enhanced their supply-chain security.

It breaks multiple GPU TEEs, such as StrongBox (CCS' 22, **Ant Group**), CAGE (NDSS' 25, **Ant Group**) and MyTEE (NDSS' 23).

Contribution: I proposed this project and worked as the leader with another student Yunjie Deng. I am responsible for reverse engineering and modifying core GPU MCU firmware, while Yunjie Deng analyzed the GPU programs and tested the attack prototype. **2025**

Moat (USENIX Security' 24) sites.google.com/view/safe-bpf

We build a system named Moat. It isolates BPF programs using hardware features like Intel MPK/Arm Stage-II.

We have worked with a company to put it into production for **1,170,000 Yuan**.

Contribution: I proposed this project and worked as the leader; I completed the whole project myself. Collaborations with the company is supervised by me and developed by another student Lijian Huang. **2024**

Patent ZL 2022 1 0436969.8

Kernel Space Debug Method, Device and Storage Medium **2022**

Translation of Software Foundation coq-zh.github.io/SF-zh

I helped translate the Software Foundation, a famous textbook about formal verification. **2022**

BadUSB-C (WOOT' 21)

We uncovered a novel attack vector against USB-C devices. It enhances the power of BadUSB attacks with the video capability of USB-C. We received **30,000 Yuan** bounty award from the affected vendor. **2021**