QIANG LIU

PostDoc@EPFL | BC 154, Station 14, 1015 Lausanne, Switzerland
cyruscyliu@gmail.com | https://cyruscyliu.github.io | Revision: June, 2025

HIGHLIGHTS

- Dedicated to **system security**, including (1) developing prior-to-release vulnerability identification and post-release attack mitigation, both grounded in a deep understanding of hardware and software, and (2) building the chain of trust examined by full-chain exploit analysis, with a strong passion for exploring **AI system security**, **AI for system understanding**, and **system resilience**
- Published **papers at all four top-tier security conferences**
- HyperPill won the **best paper award** at USENIX Security'24
- Tango won the **best paper award** at ACM RAID'24
- Built a grammar-based arbitrary hypervisor fuzzing framework and found **100+ hypervisor bugs**
- Built a partial rehosting framework of Linux-based firmware
- Designed and graded the advanced operating systems lab
- **Co-advising four PhD students**; mentored two PhD students, four master's students and five bachelor's students on their thesis/semester projects
- Served on the technical program committees of USENIX Security'26, IEEE/ACM ASE'25, and USENIX Security'25; reviewed for ACM CSUR and ACM TOSEM
- Organized hotpot parties and TGIF events for my lab

EDUCATION

College of Computer Science, Zhejiang University, China
PhD, Cybersecurity 09/2018 - 09/2023
Thesis: Research on Key Technologies of Virtualization for Linux-based Peripherals
Advisors: Prof. Yajin Zhou and Prof. Mathias Payer (External Co-advisor)

School of Electrical Engineering, Beijing Institute of Technology, China
Bachelor, Electrical Engineering, Cybersecurity (since 09/2016) 09/2014 - 06/2018
GPA: 88.2, Rank: 2/30
Thesis: Applying LSTM to the Implicit Continuous Authentication of Smart Phones
Advisors: Prof. Limin Pan and Prof. Tiantian Zhu (External Co-advisor)

RESEARCH EXPERIENCE

HexHive, EPFL, Switzerland
PostDoc (since 11/2023, visiting doctoral student before) 02/2023 - Present
Working with Prof. Mathias Payer
Research Topics: Hypervisor Security [1, 4], AI System Security [8, 9], AI for System Understanding [10, 2], System Resilience

Institute of Cyberspace Research (ICSR), Zhejiang University, China
PhD Candidate (since 09/2020, PhD student before) 05/2019 - 02/2023
Research Topics: Firmware Rehosting [6, 3], Hypervisor Fuzzing [5]

Lab of Internet and Security Technology (LIST), Zhejiang University, China
PhD Student (since 09/2018, research intern before) 07/2017 - 04/2019
Research Topics: Mobile Authentication [7, 11, 12], Ransomware Detection

Information System Security and Countermeasures Experiments Center, Beijing Institute of Technology, China
Research Intern 09/2016 - 06/2017

Research Topics: Network Protocol Fuzzing with Peach

TEACHING/ADVISING EXPERIENCE

Co-advise, Interpreter Security

PhD student 4, **research projects** [8, 9], EPFL 08/2024 - Present

Co-advise, Browser Security

PhD student 3, **research project** [10], EPFL 08/2024 - Present

PhD student 2, **research project**, focusing on program synthesis, EPFL/THU 01/2023 - 12/2023

Co-advise, Understanding of Network Procotols

Bachelor's student 5, summer internship, focusing on exploitation, EPFL 07/2025 - 08/2025

Master's student 4, summer internship, focusing on visualization, EPFL 07/2025 - 08/2025

Master's student 3, master semester project, focusing on benchmarks, EPFL 02/2025 - 06/2025

Bachelor's student 4, **undergradate final project**, focusing on BGP, EPFL 09/2024 - 01/2025

Bachelor's student 3, Summer@EPFL, focusing on benchmarks, EPFL 06/2024 - 08/2024

Co-advise, Identification of Hypervisor Bugs

Master's student 2, **master thesis**, focusing on ARM64, EPFL 09/2024 - 01/2025

Master's student 1, master semester project, focusing on race conditions, EPFL 09/2024 - 01/2025

PhD student 1, **research project** [4], EPFL/THU 01/2024 - 12/2024

Bachelor's student 2, **undergradate final project**, focusing on rehosting, ZJU 09/2020 - 06/2021

Co-advise, Identification of Linux Kernel Bugs

Bachelor's student 1, **undergradate final project**, focusing on GPU driver, ZJU 09/2020 - 06/2021

Teacher Assistant, Operating System, Zhejiang University

I joined the discussion and subsequently drafted the initial version of the instructions for building an operating system from scratch for AArch64 and RISC-V. Besides, I answered questions during office hours and graded assignments. 09/2019 - 01/2020

Teacher Assistant, Information Security Labs, Zhejiang University

I graded assignments. 03/2019 - 06/2019

SERVICE EXPERIENCE

PC Members: USENIX Security'26 and 25, IEEE/ACM ASE'25, FUZZING'24, ASE'22 AE

Reviewer: ACM CSUR, ACM TOSOM

Sub-reviewer: NDSS'24, AsiaCCS'22, AsiaCCS'20, CODASPY'20, CODASPY'19

PRESENTATIONS EXPERIENCE

Towards Full-Lifecycle Security Enforcement of Hypervisors

Invited Guest Lecture, EPFL 05/2025

Towards Full-Lifecycle Security Enforcement of Systems

Invited Job Talk, NUS, Singapore 03/2025

Invited Job Talk, ShanghaiTech, Shanghai 03/2025

Tango: Extracting Higher-Order Feedback through State Inference

Efficiently Rebuilding Coverage in Hardware-Assisted Greybox Fuzzing

Replay-resistant Disk Fingerprinting via Unintentional Electromagnetic Emanations

Main Conference, ACM RAID'24, Padua 10/2024

ViDeZZo: Dependency-Aware Virtual Device Fuzzing

Invited Talk, SSLab, Georgia Tech, Online 09/2023

Main Conference and Poster Session, IEEE S&P'23, San Francisco 05/2023

FirmGuide: Boosting the Capability of Rehosting Embedded Linux Kernels through Model-Guided Kernel Execution
Main Conference, ASE'21, Melbourne, Online 11/2021
Poster Session, AsiaCCS'21, Hong Kong, Online 06/2021

EAPA: Efficient Attestation Resilient to Physical Attacks for IoT Devices Environment
Workshop, ACM CCS19@IoT-S&P, London 11/2019

References

[1] Alexander Bulekov, **Qiang Liu**, Manuel Egele, and Mathias Payer. HyperPill: Fuzzing for Hypervisor bugs by leveraging the Hardware Virtualization Interface. In *USENIX Security Symposium (Security, **Best Paper Award**)*, 2024.

[2] Ahmad Hazimeh, Duo Xu, **Qiang Liu**, Yan Wang, and Mathias Payer. Tango: Extracting Higher-Order Feedback through State Inference. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID, **Corresponding Author**, **Best Paper Award**)*, 2024.

[3] Muhui Jiang, Lin Ma, Yajin Zhou, **Qiang Liu**, Cen Zhang, Zhi Wang, Xiapu Luo, Lei Wu, and Kui Ren. ECMO: Peripheral transplantation to Rehost embedded Linux kernels. In *ACM Conference on Computer and Communications Security (CCS)*, 2021.

[4] Zheyu Ma, **Qiang Liu**, Zheming Li, Tingting Yin, Wende Tan, Chao Zhang, and Mathias Payer. Truman: Constructing device behavior models from os drivers to fuzz virtual devices. In *Network and Distributed System Security Symposium (NDSS)*, 2025.

[5] **Qiang Liu**, Flavio Toffalini, Yajin Zhou, and Mathias Payer. VIDEZZO: Dependency-aware Virtual Device Fuzzing. In *IEEE Symposium on Security and Privacy (S&P)*, 2023.

[6] **Qiang Liu**, Cen Zhang, Lin Ma, Muhui Jiang, Yajin Zhou, Lei Wu, Wenbo Shen, Xiapu Luo, Yang Liu, and Kui Ren. FIRMGUIDE: Boosting the Capability of Rehosting Embedded Linux Kernels through Model-Guided Kernel Execution. In *IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2021.

[7] Jie Ying, Tiantian Zhu, Qiang Liu, Chunlin Xiong, Zhengqiu Weng, Tieming Chen, Lei Fu, Mingqi Lv, Han Wu, Ting Want, and Yan Chen. TRAPCOG: An Anti-noise, Transferable, and Privacy-preserving Real-time Mobile User Authentication System with High Accuracy. *IEEE Transactions on Mobile Computing (TMC)*, 2023.

[8] Chibin Zhang, Gwangmu Lee, **Qiang Liu**, and Mathias Payer. Reflecta: Reflection-based scalable and semantic scripting language fuzzing. In *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2025.

[9] Chibin Zhang, **Qiang Liu**, and Payer Mathias. Crossfit: Demystifying vm callback bugs in interpreters. In *IEEE/ACM International Conference on Software Engineering (ICSE, under submission)*, 2025.

[10] Han Zheng, Flavio Toffalini, **Qiang Liu**, and Mathias Payer. Grape: Squeezing juicy variant bugs out of modern browsers. In *ACM Conference on Computer and Communications Security (CCS, under submission)*, 2025.

[11] Tiantian Zhu, Lei Fu, Qiang Liu, Zi Lin, Yan Chen, and Tieming Chen. One Cycle Attack: Fool Sensor-Based Personal Gait Authentication With Clustering. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2021.

[12] Tiantian Zhu, Zhengqiu Weng, Qijie Song, Yuan Chen, Qiang Liu, Yan Chen, Mingqi Lv, and Tieming Chen. ESPIALCOG: General, Efficient and Robust Mobile User Implicit Authentication in Noisy Environment. *IEEE Transactions on Mobile Computing (TMC)*, 2020.