QIANG LIU

PostDoc@EPFL | BC 154, Station 14, 1015 Lausanne, Switzerland
cyruscyliu@gmail.com | https://cyruscyliu.github.io | Revision: September, 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
- Built a grammar-based arbitrary hypervisor fuzzing framework and found 100+ hypervisor bugs
- Built a full system rehosting framework of Linux-based firmware
- Published papers at all four top-tier security conferences and have won two best paper awards
- Co-advised/ing four PhD students
- Served on the technical program committees of IEEE/ACM ASE'25, and USENIX Security'25; reviewed for ACM CSUR and ACM TOSEM

EDUCATION

Bachelor, Electrical Engineering, Beijing Institute of Technology, China 09/2014 - 06/2018
GPA: 88.2, Rank: 2/30
Advisors: Prof. Limin Pan and Prof. Tiantian Zhu (External Co-advisor)
Research Topics: Mobile Authentication [8, 11, 12]
Thesis: Applying LSTM to the Implicit Continuous Authentication of Smart Phones

PhD, Cybersecurity, Zhejiang University, China 09/2018 - 09/2023
Advisors: Prof. Yajin Zhou and Prof. Mathias Payer (External Co-advisor)
Research Topics: Firmware Rehosting [10, 9], Hypervisor Security [7]
Thesis: Research on Key Technologies of Virtualization for Linux-based Peripherals

WORKING EXPERIENCE

PostDoc, HexHive, EPFL, Switzerland 11/2023 - Present
Advisor: Prof. Mathias Payer
Research Topics: Hypervisor Security [5, 1], Network Security [6], Interpreter Security [2, 3], Browser Security [4], AI System Security, AI for System Understanding, and System Resilience

🏆 HyperPill won the best paper award at USENIX Security'24
🏆 Tango won the best paper award at ACM RAID'24

TEACHING/ADVISING EXPERIENCE

Co-advisor, Browser Security
PhD student 4 @EPFL, research project [4] 08/2024 - Present
PhD student 3 @THU/EPFL, research project, focusing on program synthesis 01/2023 - 12/2023

Co-advisor, Interpreter Security
PhD student 2 @EPFL, research projects [2, 3] 08/2024 - Present

Co-advisor, MAGMA: A Ground-Truth Fuzzing Benchmark
BSc student 5 @EPFL, summer internship, focusing on exploitation 07/2025 - 08/2025
MSc student 3 @ETHZ/EPFL, MSc semester project, focusing on benchmarks 02/2025 - 06/2025
BSc student 4 @EPFL, BSc final project, focusing on BGP 09/2024 - 01/2025
BSc student 3 @EPFL, summer internship, focusing on benchmarks 06/2024 - 08/2024

Co-advisor, Rehosting and Hypervisor Security
MSc student 2 @EPFL, MSc thesis, focusing on ARM64 09/2024 - 01/2025
MSc student 1 @ETHZ/EPFL, MSc semester project, focusing on race conditions 09/2024 - 01/2025
PhD student 1 @THU/EPFL, research project [1] 01/2024 - 12/2024
BSc student 2 @ZJU, BSc final project, focusing on rehosting 09/2020 - 06/2021

Co-advisor, Operating System Security
BSc student 1 @ZJU, BSc final project, focusing on GPU drivers 09/2020 - 06/2021

Teaching 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

Teaching Assistant, Information Security Labs, Zhejiang University
I graded assignments. 03/2019 - 06/2019

SERVICE EXPERIENCE

Session Chair: AsiaCCS'25
PC Members: USENIX Security 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 Talk, UNSW, Sydney, Australia 07/2025
Invited Talk, ANU, Canberra, Australia 07/2025
Invited Talk, University of Melbourne, Melbourne, Australia 07/2025
Invited Guest Lecture, EPFL, Lausanne, Switzerland 05/2025

Towards Full-Lifecycle Security Enforcement of Systems
Invited Job Talk, NUS, Singapore, Singapore 03/2025
Invited Job Talk, ShanghaiTech, Shanghai, China 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, Italy 10/2024

ViDeZZo: Dependency-Aware Virtual Device Fuzzing
Invited Talk, Georgia Tech, Online 09/2023
Main Conference and Poster Session, IEEE S&P'23, San Francisco, USA 05/2023

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

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

REFERENCES

[1] 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.

[2] 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.

[3] Chibin Zhang, **Qiang Liu**, and Mathias Payer. “Full Name Is Hidden”. In: *Under Submission.* 2025.

[4] Han Zheng, Flavio Toffalini, **Qiang Liu**, and Mathias Payer. “Full Name Is Hidden”. In: *Under Submission.* 2025.

[5] 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.

[6] 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.

[7] **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.

[8] 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”. In: *IEEE Transactions on Mobile Computing (TMC)* (2023).

[9] 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.

[10] **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.

[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”. In: *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”. In: *IEEE Transactions on Mobile Computing (TMC)* (2020).