QIANG LIU

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

NAMES OF 3 REFERENCES

Assistant Professor, Dr. Yajin Zhou <yajin@vm-kernel.org> Zhejiang University
Associate Professor, Dr. Mathias Payer <mathias.payer@nebelwelt.net> EPFL
Associate Professor, Dr. Manuel Egele <megele@bu.edu> Boston University

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 [10, 13, 14]
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 [12, 11], Hypervisor Security [9]
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 [7, 2], Network Security [8], Interpreter Security [4, 5], Browser Security [6], AI System Security [1], 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
Han Zheng @EPFL, PhD research projects, Browser testing [6] 08/2024 - Present
Yishun Zeng @THU/EPFL, PhD research project, Browser workload synthesis 01/2023 - 12/2023

Co-advisor, Interpreter Security
Chibin Zhang @EPFL, PhD research projects, interpreter fuzzing [4, 5] 08/2024 - Present

Co-advisor, MAGMA: A Ground-Truth Fuzzing Benchmark
Nadine Alfadelraad, MSc semester project, agentic PoC generation 10/2025 - Present
Sara Vaccino @EPFL, BSc summer internship, PoC generation 07/2025 - 08/2025
Srividya Subramanian @ETHZ/EPFL, MSc semester project, fuzzing benchmarks 02/2025 - 06/2025
Philippe Dourassov @EPFL, BSc final project, BGP fuzzing 09/2024 - 01/2025
Thaqiya Aman @PUB/EPFL, BSc summer internship, fuzzing benchmarks 06/2024 - 08/2024

Co-advisor, Hypervisor Security
Sydney Hauke @EPFL, MSc thesis, ARM64 hypervisor fuzzing 09/2024 - 01/2025
Christoph Wech @ETHZ/EPFL, MSc semester project, hypervisor race conditions 09/2024 - 01/2025
Zheyu Ma @THU/EPFL, PhD research project, virtual device models [2] 01/2024 - 12/2024

Co-advisor, Kernel Security
Yangxi Xiang @ZJU, PhD research project, post kernel fuzzing 10/2025 - Present
Zezhong Ren @ZGCLab/THU, PhD research project, post kernel fuzzing 10/2025 - Present
Kaiyuan Liu @ZJU, BSc final project, embedded firmware rehosting 09/2020 - 06/2021
Yangxi Xiang @BUPT/ZJU, BSc final project, kernel driver fuzzing [3] 09/2020 - 06/2021

Teaching Assistant, Operating System, ZJU
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. Additionally, I answered questions during office hours and graded assignments. 09/2019 - 01/2020

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

SERVICE EXPERIENCE

PC Members: FUZZING'26, USENIX Security 25, IEEE/ACM ASE'25, FUZZING'24, ASE'22 AE
Reviewer: IEEE TIFS, ACM CSUR, ACM TOSOM
Sub-reviewer: NDSS'24, AsiaCCS'22, AsiaCCS'20, CODASPY'20, CODASPY'19
Session Chair: AsiaCCS'25

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

PUBLICATIONS

Contributions of First-Authored and Corresponding-Authored Papers

Because my research focuses on low-level system security, each project requires a long development cycle to move from idea to a publishable prototype at a top-tier venue. Typically, it takes around two years to fully realize a research idea, implement and evaluate it, and go through the peer-review process. Since 2019, I have consistently led major projects at this pace: FirmGuide [12] (2019 – 2021), ViDeZZo [9] (2021 – 2023), Tango [8] (2023 – 2024), and MalHype [1] (2024 – present).

Contributions as a Co-advisor

In addition, I typically contribute to two collaborative projects per year, where I refine ideas, implement some components, co-write and revise papers, revise rebuttals, and revise presentation slides. As a postdoc, I play the senior role in guiding these collaborations. Since 2023, I have consistently co-advise the following projects at this pace: HyperPill [7] (2023 - 2024), Truman [2] and Reflecta [4] (2024 - 2025), CrossFit [5] and Grape [6] (2024 - Present).

[1] **Qiang Liu**, Yongzheng Wu, Yier Jin, and Mathias Payer. "Full Name Is Hidden". In: *Working In Process.* 2026.

[2] 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.

[3] Yangxi Xiang, Feng Wang, Yuan Chen, **Qiang Liu**, Haoyu Wang, Jiashui Wang, Lei Wu, Chaoyuan Chen, and Yajin Zhou. "Minoris: Practical Out-of-Emulator Kernel Module Fuzzing". In: *IEEE Transactions on Dependable and Secure Computing (TDSC)* (2025).

[4] 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.

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

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

[7] 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.

[8] 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.

[9] **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.

[10] 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).

[11] 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.

[12] **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.

[13] 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).

[14] 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).