QIANG LIU

PostDoc in System Security @EPFL | https://cyruscyliu.github.io
cyruscyliu@gmail.com | BC 154, Station 14, 1015 Lausanne, Switzerland | Revision: June, 2026

RESEARCH VISION

System Security: Make computer systems measurably trustworthy and difficult to compromise

- I propose the OME framework to Observe, Model, and Enforce the trustworthiness of computer systems at runtime. Grounded in dynamic analysis, OME treats trust as a measurable property of execution rather than a static design assumption.
- I currently apply it to low-level system software, such as the Linux kernel [15, 14, 8] and hypervisors [12, 10, 7], within a single machine. The OME framework can also scale to higher-level components (e.g., interpreters [9, 3], browsers [4], and AI agents) and to distributed and heterogeneous environments (e.g., xPU, remote resources, and network protocols [11]).
- Beyond dynamic analysis, I aim to take multiple complementary approaches to support the full lifecycle of system trust, such as secure programming languages such as Rust, large-scale static analysis [4], secure boot and attestation, and minimal recovery systems, from build to deployment, execution, and recovery.

Agentic AI: I also investigate design principles for AI agents for system security to automate labor-intensive workflows in learning, research, engineering, tech transfer, and community building.

EDUCATION

PhD, Cybersecurity, Zhejiang University, China 09/2018 - 09/2023
Advisors: Prof. Yajin Zhou
Research Topics: Dynamic analysis of the Linux Kernel [15, 14, 8] and hypervisors [12]
Thesis: Research on Key Technologies of Virtualization for Linux-based Peripherals

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 @ZJU)
Research Topics: Mobile authentication [13, 16, 17]
Thesis: Applying LSTM to the Implicit Continuous Authentication of Smart Phones

WORKING EXPERIENCE

PostDoc, HexHive, EPFL, Switzerland 11/2023 - Present
Advisor: Prof. Mathias Payer
Research Topics: 1) Dynamic analysis of the Linux Kernel [1] and hypervisors [10, 7], 2) Application security in web browsers [4] and programming languages [3, 9], 3) Hardening network protocols [11], 4) Building agentic workflows for security and checking the security of agentic AI

🏆 HyperPill [10] won the best paper award at USENIX Security'24
🏆 Tango [11] won the best paper award at ACM RAID'24
🏆 Magma [5] was selected as one of the finalists for the Cybersecurity Artifacts Competition and Impact Award at ACSAC'25

TEACHING/ADVISING EXPERIENCE

Co-advisor, Multi-Agent System Secuirty
Alexandre Norén Vaisse, @EPFL, MSc semester project, compartmentalization 02/2026 - 06/2026

Co-advisor, Web Browser Security
Han Zheng @EPFL, PhD research projects, Browser testing [4] 08/2024 - 08/2025
Yishun Zeng @THU/EPFL, PhD research project, Browser workload synthesis 01/2023 - 12/2023

Co-advisor, Programming Language Security
Rafaila Galanopoulou @EPFL, PhD research project, Rust Ecosystem 02/2026 - Present
Athanasios Trispiotis, @EPFL, MSc semester project, Rust Bug Detection 02/2026 - 06/2026
Yiwen Xu @EPFL, PhD research project, Rust for Kernel 10/2025 - Present
Chibin Zhang @EPFL, PhD research projects, interpreter fuzzing [9, 3] 08/2024 - 04/2026

Co-advisor, Network Protocol Security
Xuesong Bai @UCI, PhD research project, BGP fuzzing 10/2025 - Present
Philippe Dourassov @EPFL, BSc final project, BGP fuzzing 09/2024 - 01/2025

Co-advisor, Magma: A Ground-Truth Fuzzing Benchmark [5]
Vijay Soucramanien @EPFL, BSc final project, agentic benchmark update 02/2026 - 06/2026
Nadine Alfadelraad @ETHZ, MSc semester project, agentic PoC generation 10/2025 - 01/2026
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
Thaqiya Aman @PUB/EPFL, BSc summer internship, fuzzing benchmarks 06/2024 - 08/2024

Co-advisor, Hypervisor Security
Sofia Saltovskaia @EPFL, PhD research projects, pKVM 10/2025 - Present
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 [7] 01/2024 - 12/2024

Co-advisor, Linux Kernel Security
Yangxi Xiang @ZJU, PhD research project, post kernel fuzzing 10/2025 - Present
Zezhong Ren @UCAS, PhD research project, post kernel fuzzing 10/2025 - 02/2026
Wenlong Zhang@ZJU, MSc semester project, Linux kernel's incomplete fixes [6] 02/2021 - 06/2021
Kaiyuan Liu @ZJU, BSc final project, embedded firmware rehosting 09/2020 - 06/2021
Yangxi Xiang @BUPT/ZJU, BSc final project, kernel driver fuzzing [8] 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: SecDev'26, 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

Enforcing Trust at Runtime
Invited Job Talk, GBU, Dongguan, China 05/2026

The Impact of Magma: A Ground-Truth Fuzzing Benchmark
Cybersecurity Artifacts Impact Awards, ACSAC'25, online 12/2025

Enforcing Trust at Runtime
Invited Talk, SUSTech, Shenzhen, China 12/2025
Invited Talk, CUHK, Hong Kong, China 12/2025

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 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 (Co-)First-Authored* Papers

Due to the focus 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 [15] (2019–2021), ViDeZZo [12] (2021–2023), MalHype [1] (2024–-Present), and Magma2025 [2] (2025–Present).

Contributions as a Co-advisor

As a PostDoc, I play a senior role in guiding collaborations, typically contributing to two projects per year through refinement of ideas, implementation of components, evaluation, revisions of manuscript, rebuttal, and presentations. Since 2023, I have consistently co-advised the following projects (including their publication dates) at this pace: HyperPill [10] and Tango [11] (2024), Truman [7] and Reflecta [9] (2025), CrossFit [3] and Grape [4] (2026).

[1] **Qiang Liu***, Yongzheng Wu, Yier Jin, and Mathias Payer. "MalHype: Full Title is Hidden". In: *Working in Process*. 2026.

[2] **Qiang Liu***, Han Zheng, Srividya Subrammanian, Florian Hofhammer, Flavio Toffalini, and Mathias Payer. “Magma2025: Full Title is Hidden”. In: *Working in Process*. 2026.

[3] Chibin Zhang, **Qiang Liu**, and Mathias Payer. “CrossFit: Demystifying VM Callback Bugs in Interpreters”. In: *ACM International Conference on the Foundations of Software Engineering (FSE)*. 2026.

[4] Han Zheng, Flavio Toffalini, **Qiang Liu**, and Mathias Payer. “Squeezing Juicy Variant Bugs Out of Modern Browsers”. In: *USENIX WOOT Conference on Offensive Technologies (WOOT)*. 2026.

[5] Ahmad Hazimeh, Adrian Herrera, Srividya Subramanian, Thaqiya Aman, Sara Vaccino, **Qiang Liu§**, and Mathias Payer. “The Impact of Magma: A Ground-Truth Fuzzing Benchmark”. In: *Annual Computer Security Applications Conference (ACSAC): Artifact Impact Competition (IMPACT-ACSAC, **Corresponding Author**)*. 2025.

[6] **Qiang Liu***, Wenlong Zhang, Muhui Jiang, Lei Wu, and Yajin Zhou. “Characteristics, Root Causes, and Detection of Incomplete Security Bug Fixes in the Linux Kernel”. In: *arXiv preprint* (2025).

[7] 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.

[8] 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).

[9] 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.

[10] 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)*. 2024.

[11] 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, **Marked as Corresponding Author**)*. 2024.

[12] **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.

[13] 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).

[14] 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.

[15] **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, Co-first author)*. 2021.

[16] 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).

[17] 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).