QIANG LIU

PostDoc@EPFL | BC 154, Station 14, 1015 Lausanne, Switzerland
cyruscyliu@gmail.com | https://cyruscyliu.github.io | Revision: July, 2024

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 02/2023 - Present
Research Topics: Hypervisor Fuzzing [1], Protocol Fuzzing [2]

As a PostDoc, I am leading several research projects in hypervisor fuzzing and protocol fuzzing to find new vulnerabilities, evaluate existing tools, and explore new research problems. Besides, I am collaborating with PhD/Master students and advising summer interns at EPFL. I also help my advisor onboard new members and organize informal activities like Hotpot parties and group lunches.

Institute of Cyberspace Research (ICSR), Zhejiang University, China
PhD Candidate (since 09/2020) ← PhD Student 05/2019 - 02/2023
Research Topics: Firmware Rehosting [3, 4], Hypervisor Fuzzing [5]

Lab of Internet and Security Technology (LIST), Zhejiang University, China
PhD Student (since 09/2018) ← Research Intern 07/2017 - 04/2019
Research Topics: Mobile Authentication [6, 7, 8], 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/MENTORING EXPERIENCE

Advisor, Summer@EPFL
I advise interns on researching a specific topic, training them on reviewing existing approaches, coding, writing papers, and giving presentations. 06/2024 - Present
Project 1: MagmaStateful: A Ground-Truth Fuzzing Benchmark for Stateful Protocols

Mentor, Undergraduate Final Project, Zhejiang University
I participated in the discussion, provided feedback, devised technical solutions, reviewed their papers, and managed the overall time budget for the two projects. 09/2020 - 06/2021
Project 1: Rehosting Linux Kernels for Cyber Physical Systems based on QEMU
Project 2: The Design and Implementation of Linux GPU Kernel Driver Vulnerability Detection System based on Userspace Fuzzing

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: FUZZING'24, ASE'22 AE
Reviewer: ACM CSUR'24

SOFT AND TECHNICAL SKILLS

Research	Questioning, Critical Thinking, Innovation, Experiment Design, Reading/Reviewing/Writing Research Papers/Grant, Making Slides, Giving Presentation
Coding	Assembly language, Bash, C/C++, LaTeX, LLVM IR, Java, Markdown, Python, SQL, Software Development Life Cycle, Github Workflow, Open Source, Docker
RE/Exploit	AFL++/libFuzzer, CyberChef, Git/GitHub/GitLab, Ghidra/IDA/Radare2, pwntools, QEMU, Ubuntu, Vim
Management	Experience in Laboratory Inventory Management, Reimbursement, Hiring, Training, Advising, Project Management, Meetings, Retreat, Informal Activities

PRESENTATIONS

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

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

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

PUBLICATIONS

8. Ahmad Hazimeh, Duo Xu, Qiang Liu, Yan Wang, and Mathias Payer. Tango: Extracting higher-order feedback through state inference (to appear). In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID, CCF B)*, 2024

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, CCF A)*, 2024

6. Qiang Liu, Flavio Toffalini, Yajin Zhou, and Mathias Payer. Videzzo: Dependency-aware virtual device fuzzing. In *IEEE Symposium on Security and Privacy (S&P, CCF A)*, 2023

5. 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, CCF A)*, 2023

4. 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, CCF A)*, 2021

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)*, pages 734–748, 2021

2. 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, CCF A)*, 2021

1. 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, CCF A)*, 2020