Liu Qiang, Ph.D. Candidate

Revision: October 2021

cyruscyliu@gmail.com @qiangliu717
ICSR, Yuquan Campus, 38 Zheda Road, Hangzhou, China, 310027

Affiliation

2021.08 – 2022.01 **HexHive group, École Polytechnique Fédérale de Lausanne, Switzerland**
Visiting doctoral student

2019.05 – now **Institute of Cyberspace Research (ICSR), Zhejiang University, China**
Ph.D. student, Ph.D. Candidate (2020.09)
Research topics: Security analysis on low-level software and systems (embedded Linux kernel, hypervisors like QEMU, etc.).

2017.07 – 2019.04 **Internet and Security Technology (LIST) Lab, Zhejiang University, China**
Research intern and Ph.D. student
Research topics: Mobile authentication [3, 4] and ransomware detection.

2016.09 – 2017.06 **Information System Security and Countermeasures Experiments Center, Beijing Institute of Technology, China**
Research intern
Research topics: Network protocol fuzzing with Peach.

Education

2018.09 – now **Ph.D. Student, Ph.D. Candidate (2020.09), Computer Science**
College of Computer Science, Zhejiang University, China
Advisor: Yajin Zhou (Zhejiang University)

2014.09 – 2018.06 **Bachelor, Electrical Engineering**
School of Electrical Engineering, Beijing Institute of Technology, China
Thesis title: *Applying LSTM to the implicit continuous authentication of smart phones.*
Thesis statement: *Through implicit continuous authentication system based on the smart phone motion sensor, it is possible to solve the problems of ease of use and security in user authentication. With the LSTM model and parameters tuning, the final FAR reached 6.352% and the FRR reached 6.232%. This result shows that the implicit continuous authentication has considerable accuracy, providing support for the introduction of implicit continuous authentication into existing smartphones.*
Advisor: Yan Chen (Northwestern University)
Co-advisors: Limin Pan and Senlin Luo (Beijing Institute of Technology)
Tutor: Tiantian Zhu (Zhejiang University of Technology)

Service

2020.09 – 2021.06 **Mentor, Undergraduate Final Project, Zhejiang University**
Instructor: Yajin Zhou
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
I joined the discussion, gave feedback, came up with technical solutions, reviewed their papers and controlled the overall time budget of the two projects.

Service (continued)

2019.09 – 2020.01 **Teacher Assistant, Operating System, Zhejiang University**
Instructor: Yajin Zhou
I joined the discussion and then wrote the first version of instructions to build an operation system for AArch64 and RISCV from scratch.

2019.03 – 2019.06 **Teacher Assistant, Information Security Labs, Zhejiang University**
Instructor: Yajin Zhou

Talk

2021.06 **Poster, AsiaCCS 2021, Hong Kong, China**
FirmGuide: Boosting the Capability of Rehosting Embedded Linux Kernels through Model-Guided Kernel Execution

2019.11 **Presenter, CCS19@IoT-S&P'19, London, UK**
EAPA: Efficient Attestation Resilient to Physical Attacks for IoT Devices Environment

Technical Focus

Coding	Python, C/C++, Java, LaTeX, Docker, Bash, Vim
Security	Fuzzing, Symbolic execution, Static analysis with LLVM pass
Languages	English/Chinese speaking and writing
CTF	Reverse engineering, PWN, Firmware analysis

Research Publications

Conference Proceedings

1. Jiang, M., Ma, L., Zhou, Y., Liu, Q., Zhang, C., Wang, Z., … Ren, K. (2021). Ecmo: Peripheral transplantation to rehost embedded linux kernels.
2. Liu, Q., Zhang, C., Ma, L., Jiang, M., Zhou, Y., Wu, L., … Ren, K. (2021). Firmguide: Boosting the capability of rehosting embedded linux kernels through model-guided kernel execution.

Journal Articles

1. Zhu, T., Fu, L., Liu, Q., Lin, Z., Chen, Y., & Chen, T. (2021). One cycle attack: Fool sensor-based personal gait authentication with clustering. *IEEE Transactions on Information Forensics and Security*, *16*, 553–568. doi:10.1109/TIFS.2020.3016819
2. Zhu, T., Weng, Z., Song, Q., Chen, Y., Liu, Q., Chen, Y., … Chen, T. (2020). Espialcog: General, efficient and robust mobile user implicit authentication in noisy environment. *IEEE Transactions on Mobile Computing*, 1–1. doi:10.1109/TMC.2020.3012491