Liu Qiang, Ph.D. Candidate

Revision: April 2023

cyruscyliu@gmail.com @qiangliu717
BC 160, Station 14, CH-1015 Lausanne, Switzerland
https://cyruscyliu.github.io/

Affiliation

2023.02 – now **HexHive, École Polytechnique Fédérale de Lausanne, Switzerland**
Visiting doctoral student
Research topics: Operating system security and hypervisor security

2019.05 – now **Institute of Cyberspace Research (ICSR), Zhejiang University, China**
Ph.D. student, Ph.D. candidate (2020.09)
Research topics: Dynamic analysis on OS kernels [2, 3].).

2021.08 – 2022.03 **HexHive, École Polytechnique Fédérale de Lausanne, Switzerland**
Visiting doctoral student
Research topics: Dynamic analysis on hypervisors.

2017.07 – 2019.04 **Lab of Internet and Security Technology (LIST), Zhejiang University, China**
Research intern and Ph.D. student (2018.09)
Research topics: Mobile authentication [4, 5] 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

2019.05 – now **Ph.D. Student, Ph.D. Candidate (2020.09), Computer Science**
College of Computer Science, Zhejiang University, China
Supervisor: Yajin Zhou (Zhejiang University)

2018.09 – 2019.05 **Ph.D. Student, Computer Science**
College of Computer Science, Zhejiang University, China
Supervisor: Yan Chen (Northwestern 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

2022 ASE'22 Artifact Evaluation

Service (continued)

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.

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

Honors and Awards

Winter 2018 First place of ANU's CECS International Summer School Project:
`https://cecs.anu.edu.au/news/smart-cities-focus-inaugural-cecs-international-summer-school`

2016-2017 University-level outstanding Scholarship
Diwen Scholarship

2015-2016 University-level outstanding Scholarship (twice)
National Scholarship for Encouragement

2014-2015 University-level outstanding students
University-level outstanding Scholarship (twice)
National Scholarship for Encouragement

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

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

Research Publications

Conference Proceedings

1 Liu, Q., Toffalini, F., Zhou, Y., & Payer, M. (2023). Videzzo: Dependency-aware virtual device fuzzing. In *IEEE Symposium on Security and Privacy (S&P, CCF A)*.

2. Jiang, M., Ma, L., Zhou, Y., Liu, Q., Zhang, C., Wang, Z., … Ren, K. (2021). Ecmo: Peripheral transplantation to rehost embedded linux kernels. In *ACM SIGSAC Conference on Computer and Communications Security (CCS, CCF A)*.

3. 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. In *IEEE/ACM International Conference on Automated Software Engineering (ASE, CCF A)*.

Journal Articles

1. Ying, J., Zhu, T., Liu, Q., Xiong, C., Weng, Z., Chen, T., … Chen, Y. (2023). 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)*.

2. 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 (TIFS, CCF A)*. doi:10.1109/TIFS.2020.3016819

3. 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 (TMC, CCF A)*. doi:10.1109/TMC.2020.3012491