WENJIE QIU

736 Eastgate Ave. • St. Louis 63130, MO

+1-3142035508 • qiuwenjie@wustl.edu • floatingsong.com

EDUCATION

Washington University in St. Louis (WUSTL) St. Louis, United States
Candidate for M.S. in Computer Science Aug. 2018 – Present
Central China Normal University (CCNU) Wuhan, China
B.S. in Electronic and Information Engineering Sept. 2014 – June 2018

TECHNICAL SKILLS

- Programming Languages: C, C++, Python, MATLAB, SQL, Bash
- Misc: Docker, Android, OpenCV, STM32, Cadence

WORK EXPERIENCE

Research Intern
S3 Lab, Stevens Institute of Technology June 2019 – Aug. 2019
- Built a docker-based micro service backend for Automatic Verification of Temporal Alignment.
- Summarized the disassembling algorithms and workflow of Radare2 – a reverse-engineering framework.

ACADEMIC EXPERIENCE

Research on program behaviors in trusted execution environment
Research Assistant, Computer Security & Privacy Laboratory, WUSTL Oct. 2019 – Present
- Built OpenCV inside SCONE – a secure Linux container with SGX.
- Evaluated performance overhead of different OpenCV modules executing inside SCONE versus outside world.

Research on post-fuzzing analysis of Linux kernel
Research Assistant, Computer Security & Privacy Laboratory, WUSTL Mar. 2019 – May 2019
- Summarized the reference counting mechanism in Linux kernel.
- Summarized the pattern of use-after-free vulnerabilities caused by reference counting mismatch in Linux kernel.
- Proposed a detection heuristic of potential use-after-free vulnerabilities in Linux kernel.

Research on emulation of and fuzzing on embedded operating systems
Research Assistant, Computer Security & Privacy Laboratory, WUSTL Jan. 2019 – May 2019
- Analyzing market share of embedded operating system, especially focusing on Linux-like embedded OS.
- Partially emulated FreeRTOS on STM32 platform via QEMU.

Designing and implementing a machine learning assisted fuzzer based on AFL
Course Project, Software Security Mar. 2019 - May 2019
- Proposed a heuristic of distance measurement of fuzzing traces generated by testcases in AFL.
- Applied K-means clustering algorithm on fuzzing traces generated by testcases in AFL.
- Designed and implemented a task-division mechanism which several fuzzing instances can be created, and each one is responsible for one type of testcases determined by clustering algorithm.

PUBLICATION

- Exploiting Exception Handling for Binary Disassemling (preparing for ISSTA 2020)

HONORS & AWARDS

- Awarded “Three Good Student”, CCNU. (Top 10%) 2016
- Awarded “Boya” Scholarship, CCNU. (The prime academic scholarship in CCNU, top 5%) 2016

REFERENCE:

Prof. Ning Zhang (WUSTL), Prof. Jun Xu, Prof. Eric Koskinen (Stevens Institute of Technology)