Zhenxiao Qi

Address: WCH Room 465 BCOE, Riverside, CA, 92507 Tel: +1 9514219319

E-mail: zqi020@ucr.edu Homepage: https://enlighten5.github.io GitHub: https://github.com/enlighten5

Education Background

✧ **University of California, Riverside (UCR)** *08/2018-Present*

- Degree expected: Ph.D.
- Major: Computer Science

✧ **University of California, Riverside (UCR)** *07/2017-06/2018*

- Exchange student
- Major: Computer Science

✧ **Xidian University (XDU)** *07/2014-06/2017*

- Degree: Bachelor of Engineering
- Major: Information Security

Research Experience

LogicMEM: A Logic Inference Approach to Automate Profile Generation for Binary-only Memory Forensics *04/2020-present*

Supervisor: Prof. Heng Yin

- This is an ongoing project collaborated with Google Cloud Team. In this work, we proposed a logic inference-based approach to reconstruct kernel objects for binary-only memory forensics. The evaluation results show that LogicMEM produces no false positive and false negative when generating a profile and enables memory forensics for memory dumps collected from production environments, where traditional approaches fail to generate profiles.

SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets *07/2019-12/2020*

Supervisor: Prof. Heng Yin

- This paper was accepted to NDSS'21. In this work, we proposed a novel Spectre V1 gadget detection approach by enabling dynamic taint analysis on speculative execution paths. The evaluation results show that SpecTaint improves the detection precision and recall by large margins with reasonable efficiency, and it detects new Spectre V1 gadgets from real-world applications such as Brotli and deep learning framework Caffee.

QEMU Virtualization (KVM)/Emulation (TCG) Mode Switch *04/2018-06/2018*

Supervisor: Prof. Heng Yin

- In this project, we developed a novel on-the-fly mode switching functionality for QEMU, which enables QEMU to perform instrumentation in TCG mode on demand while running in native speed KVM mode. This functionality is achieved by adding a new thread in QEMU workflow, inside which we alter between KVM and TCG modes when receiving user command, and carefully synchronize CPU states between two modes. We evaluated our implementation on common-used operating systems, such as Windows, Debian, Ubuntu, etc.

Upgrade of DECAF *06/2018-09/2018*

Supervisor: Prof. Heng Yin

- This project aims at porting DECAF from QEMU 1.0 to QEMU 2.10. DECAF (short for Dynamic Executable Code Analysis Framework) is a binary analysis platform based on QEMU. Following

the implementation of DECAF, we port the functionalities of DECAF (e.g., VMI, Taint analysis, etc.) to QEMU 2.10. Most of the works are done while some issues relating to memory mapped IO remain.

Publications:

- [**NDSS'21**] **Zhenxiao Qi**, Qian Feng, Yueqiang Cheng, Mengjia Yan, Peng Li, Heng Yin, and Tao Wei, SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets, to appear in the Network and Distributed System Security Symposium, February 2021.
- [**RAID'19**] Ali Davanian, **Zhenxiao Qi**, Yu Qu, and Heng Yin, DECAF++: Elastic Whole-System Dynamic Taint Analysis, in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses, September 2019.

Professional Services:

Reviewer: Cybersecurity

Sub-reviewer: USENIX Security'21, DIMVA'19

Artifact Evaluation:

- ACSAC'18 TIFF: Using Input Type Inference To Improve Fuzzing
- ACSAC'19 Speculator: A Tool to Analyze Speculative Execution Attacks and Mitigations

Graduate-level CS courses taken in UCR

- **ADVANCED OPERATING SYSTEMS; ADVANCED COMPUTER ARCHITECTURE; ADVANCED COMPILER DESIGN;**
- SEMINAR IN COMPUTER SCIENCE; ARTIFICIAL INTELLIGENCE; **COMPUTER SECURITY;** ALGORITHM TECHNIQUES IN COMPUTATIONAL BIOLOGY; DATA MINING TECHNIQUES;

Teaching Experience:

- CS202 Advanced Operating Systems: Fall '19 / Winter '20
- CS100 Software Construction: Spring '20 / Winter '21
- CS153 Design of Operating Systems: Fall '20

Honors and Awards

- Outstanding Teaching Assistance in CSE Department 2019-2020
- Dean's Distinguished Fellowship, UC, Riverside 2018
- Outstanding Student Scholarship, Xidian University 2014-2017

Programming Skills:

Programming Language:

- Fluent in **C**, **Python**, **LaTeX.**
- Other language: assembly language, MATLAB, **Java, C++.**

Operating Systems:

- **Linux**, Windows, XV6.

Tools and Platforms:

- AFL, Angr.
- QEMU, DECAF.
- TensorFlow, Caffee.
- Hadoop, Spark.