Zhenxiao Qi

Address: WCH Room 465 BCOE, Riverside, CA, 92507 Tel: +1 9514219319 E-mail: zqi020@ucr.edu

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

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

Supervisor: Dr. Heng Yin, Associate Prof.

- The project aims at on-the-fly switching between QEMU KVM virtualization and TCG emulation, which enables QEMU to perform instrumentation in TCG mode on demand while running in native speed at other times We achieve the aforementioned functionality by adding a new thread in QEMU workflow, inside which we alter between KVM and TCG modes when receiving user command. The most essential part is to synchronize the CPU state between switches. We verified its functionality on common-used operating systems, such as Windows, Debian, Ubuntu, etc.

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

Supervisor: Dr. Heng Yin, Associate Prof.

- 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. It is based on QEMU 1.0, which is slower than the newly released QEMU 2.10. We determine to take advantage of the improvements from QEMU 2.10 and port the functionalities of DECAF(VMI, Taint analysis, etc.) to QEMU 2.10. Following the convention of DECAF, we instrument the TCG translation phase and rewrite the code which is not compatible with QEMU 2.10. Most of the works are done while some issues relating to memory mapped IO remaining.

Spectre Vulnerabilities Detection via System-wide Emulation *07/2019-present*

Supervisor: Dr. Heng Yin, Associate Prof.

- This is project aims at capturing spectre and meltdown vulnerability through taint tracking and transient execution modeling on DECAF. To simulate the transient execution, we perform dynamic binary instrumentation and memory restore mechanism on top of QEMU. Moreover, we take advantages of the taint tracking functionality of DECAF for vulnerability identification.

Academic Achievements:

Publication:

- [RAID'19] Ali Davanian, **Zhenxiao Qi**, Yu Qu, and Heng Yin, DECAF++: Elastic Whole-System Dynamic Taint Analysis, to appear in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses, September 2019

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;

Honors and Awards

- Dean's Distinguished Fellowship, UC, Riverside *2018*
- Outstanding Student Scholarship, Xidian University 2014-2017

Computer Skills

Programming Language:

- Fluent in **C**, **Python**
- Other language: assembly language, Matlab, **Java, C++**

Operating System: Linux, Windows, XV6

Tools and Platforms:

- AFL, Angr
- Qemu, DECAF
- TensorFlow, Caffee
- Hadoop, Spark