YIZHUO ZHAI

900 University Ave, Riverside, CA 92521
(+1) 951 476 6303 ⋄ yizhuo dot zhai at email dot ucr dot edu

EDUCATION

Xidian University *Xian, Shaanxi Province, P.R. China (Sept 2012 - June 2016)*

BS in Software Engineering GPA: 3.82/4.0, 91/100 (ranked 1st)
University of Limerick (Study Abroad) *Ireland (Sept 2015 - June 2016)*

University of California Riverside *Riverside, CA (Sept 2016 - Present)*

PhD candidate Co-advised by Srikanth V. Krishnamurthy and Zhiyun Qian
Computer Science Overall GPA: 3.92/4.00 Expected Grad: Dec 2022

TECHNICAL STRENGTHS

Computer Languages(In order of strength): C++, C, Java, Python, Swift, Shell Script
Software & Tools LLVM, Linux, Clang, Hadoop

WORK EXPERIENCE

Research Assistant @UCR CSE Sept 2016-Current
host: Hayawardh Vijayakumar

Doing system security and static analysis.

Published/co-authored papers accepted by or submitted to top-tier venues.

Research Internship @ Baidu X-Lab Jun 2020-Sept 2020
host: Shengjian Guo

· Improve the product security and code quality.

Research Internship @ Samsung Research America Jun 2021-Sept 2021

Finding the type confusion bugs in large software.

PUBLICATIONS

UBITect: A Precise and Scalable Method to Detect Use-before-Initialization bugs in Linux Kernel
Yizhuo Zhai, *Yu Hao, Hang Zhang, Daimeng Wang, Chengyu Song, Zhiyun Qian, Mohsen Lesani, Srikanth V. Krishnamurthy, and Paul Yu In Proceedings of the 2020 ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'20)*

Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel
Hang Zhang, Weiteng Chen, Yu Hao, Guoren Li, ***Yizhuo Zhai****, Xiaochen Zou, Zhiyun Qian In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS'21)*

Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels
Yizhuo Zhai, *Yu Hao, Zheng Zhang, Weiteng Chen, Guoren Li, Zhiyun Qian, Chengyu Song, Manu Sridharan, Srikanth V. Krishnamurthy, Trent Jaeger, Paul Yu In Proceedings of the Network Distributed System Security Symposium (NDSS) 2022. (NDSS'22)*

PROJECTS

EfficientSan Dec 2021 - Present
Research Project

· Help reducing the type confusion sanitizers' overhead while keep the same security promise.

IncreLux Sept 2019 - Dec 2021
Research Project

· Incremental analysis for Linux kernel.
· We are building a framework to enable the incremental analysis across different versions of Linux kernel.

UBITECT Sept 2016 - Aug 2019
Research Project

· Created a static analysis tool detecting use-before-initialization (UBI) bugs scaling to the whole Linux kernel in LLVM IR level.
· This is a work to do inter-procedural/inter-module analysis targeting at the use of uninitialized variables.
· Successfully find 138 new UBI bugs in Linux kernel, 52 bugs are confirmed.

LLVMCookBook April 2019 - Aug 2019

· Established a llvm front end for the self-defined language in LLVMCookBook, registered new optimization passes in IR level.
· Refer, update and test the code in the book to be compatible with LLVM 7.0.0.
· Became more familiar with LLVM. While further understood how compiler front end, optimizer and back end works. (Github:`https://github.com/YizhuoZhai/LLVMCookBook`)

Router Malware Clustering Sept 2017 - Dec 2017
Data Mining Class Project

· Clustering different kinds of router malware based on their execution trace.
· Two distinguished features are: the system call times and the memory usage over time, **dynamic time wrapping** is used to deal with the second feature.
· Eight clusters are calculated via the algorithm.

CTF Style Binary Exploits Jan 2017 - Mar 2017
Security Lab

· The lab required student to understand both offensive techniques (e.g., how exploit works) and the defensive techniques (e.g., how to patch a vulnerability).
· Topics included stack overflow, heap overflow, format string, return oriented programming, etc. (Schedule:`https://www.cs.ucr.edu/~csong/seclab/17/cal.html`)
· Solved 80/100 challenges within 10 weeks.

TowelRoot Sept 2016 - Dec 2016
OS Class Project

· Fully understand CVE-2014-3153 and can utilize it to compromise an Android device.
· CVE-2014-3153 shows some flaw when using Linux data structure. The logic is hard to understand while the proof of concept (PoC) is non-trivial.
· Get the root privilege of an Android device within 1 minutes.

SELECTED VOLUNTEER WORK

UCR MESA Sept 2017 - Current

I currently work as a volunteer for the UCR MESA (https://mesa.engr.ucr.edu) events. I mainly help with the middle school and high school technique competitions.
· 6/2018 GEMS(Girls Excelling in Mathematics and Succeeding) events: Student Organizer
· 3/2018 2018 Seaperch Competition: Runner
· 2/2018 MESA Day: Judge for High School NEDC (National Engineering Design Competition)
· 11/2017 MESA Robotics Invitational: High School Judge

SELECTED CLASSES

System: Advanced OS, Program Verification, Advanced Compiler Construction, Computer Security
AI: Machine Learning, Data Mining, Artificial Intelligence, Probablistic Module of AI

NOTABLE AWARDS

09/2016 Deans Distinguished Fellowship
06/2016 Presidents Volunteer Award (Bronze)
04/2015 First Prize Scholarship by college
10/2014 National Scholarship
10/2014 Special Scholarship by college
10/2013 First Prize Scholarship by college
03/2013 Special Scholarship by college