

Yihui (Kyle) ZENG

<https://kylebot.net/>

+1 805-710-0402 | zengyhkyle@gmail.com | @kylebot

EDUCATION

Arizona State University

Ph.D. student, Major in Computer Science

Aug 2019 – present

The Chinese University of Hong Kong

B.S., Major in Mathematics, Minor in Computer Science

Aug 2013 – Jun 2018

PUBLICATIONS

- Playing for K(H)eaps: Understanding and Improving Linux Kernel Exploit Reliability
*Kyle Zeng**, Yueqi Chen*, Haehyun Cho, Xinyu Xing, Adam Doupe, Yan Shoshitaishvili, Tiffany Bao
Proceedings of the USENIX Security Symposium (USENIX), August 2022.
** Indicates equal contribution*
- Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs
Jayakrishna Menon Vadayath, Moritz Eckert, Kyle Zeng, Nicolaas Weideman, Gokulkrishna Praveen Menon, Yanick Fratantonio, Davide Balzarotti, Adam Doupe, Tiffany Bao, Ruoyu Wang, Christophe Hauser, Yan Shoshitaishvili
Proceedings of the USENIX Security Symposium (USENIX), August 2022.
- SyML: Guiding Symbolic Execution Toward Vulnerable States Through Pattern Learning
Nicola Ruaro, Lukas Dresel, Kyle Zeng, Tiffany Bao, Mario Polino, Andrea Continella, Stefano Zanero, Christopher Kruegel, Giovanni Vigna
Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses (RAID), October 2021.
- Favocado: Fuzzing the Binding Code of JavaScript Engines Using Semantically Correct Test Cases
Sung Ta Dinh, Haehyun Cho, Kyle Martin, Adam Oest, Kyle Zeng, Alexandros Kapravelos, Gail-Joon Ahn, Tiffany Bao, Ruoyu Wang, Adam Doupe, Yan Shoshitaishvili
Proceedings of the Network and Distributed System Security Symposium (NDSS), February 2021.
- Not All Coverage Measurements Are Equal: Fuzzing by Coverage Accounting for Input Prioritization
Yanhao Wang, Xiangkun Jia, Yuwei Liu, Kyle Zeng, Tiffany Bao, Dinghao Wu, Purui Su
Proceedings of the Network and Distributed System Security Symposium (NDSS), February 2020.

WORK EXPERIENCE

Arizona State University, US

Research Assistant

Sep 2019 – present

- Researched Linux kernel security, symbolic execution, and fuzzing automatic vulnerability discovery technique
- Enhanced the popular symbolic execution engine angr by improving its tracer component, enabling it to automatically generate exploits for 78 real-world embedded devices using 16 different vulnerabilities

University of California, Santa Barbara, US

Staff Research Associate

Sep 2018 – Feb 2019

- Researched path triage problem in symbolic execution for automatic vulnerability discovery. Applied symbolic execution, machine learning, graph theory, and crash analysis in this project

- Contributed to multiple popular open-source projects, including but not limited to: angr, rex, archr, and shellphish-qemu

HORNORS & AWARDS

- SCAI Doctoral Fellowship, Arizona State University, 2022
- Engineering Graduate Fellowship, Arizona State University, 2020
- Cybersecurity Fellowship, Arizona State University, 2019
- 1978 Mathematics Alumnus Li Sze-lim Scholarship, the Chinese University of Hong Kong, 2016
- Scholarship for Outstanding Student, the Chinese University of Hong Kong, 2014-2016
- Dean's Honors List, the Chinese University of Hong Kong, 2014-2015
- Matriculation Scholarship for Academic Excellence, the Chinese University of Hong Kong, 2013
- Ching-ling Soong Zhiyuan Scholarship, Ching-ling Soong Zhiyuan Foundation, 2013

SECURITY EXPERIENCE

TyphoonPWN 2022, KR

May 2022 – Jun 2022

Participant

- Winner of Linux Privilege Escalation category by successfully performing local privilege escalation on Ubuntu 22.04 operating system using a 0-day vulnerability
- Discovered a novel exploitation technique that improves the exploit reliability to 100%
- Reported the bug used in the competition and obtained a CVE ID: CVE-2022-2585

Google kCTF VRP, US

Dec 2021 – present

Participant

- Performed local privilege escalation on Google Kubernetes Engine successfully for four times. Exploited the Linux kernel with one 1-day vulnerability and three 0-day vulnerabilities
- Applied cross-cache attack in the Linux kernel and devised three previously unknown exploitation techniques to complete the exploitations. Two novel techniques are confirmed by Google
- Submissions: CVE-2021-4154 (\$5,1337), CVE-2022-29581 (\$71,337), CVE-2022-1786 (\$91,337), CVE-2022-2585 (reported)

Shellphish CTF Team, US

Sep 2018 – present

Team Member

- Maintain the popular open-source project how2heap. Devised the house-of-botcake glibc heap exploitation technique
- 3rd place in CSAW'21 CTF (US-Canada region) in 2021
- Entered DEF CON CTF final competition from 2019 to 2022, ranked 10th, 7th, 14th, and 13th, respectively
- Experienced in Pwn and Reverse CTF categories. Expert in Linux kernel, Chromium browser, and JavascriptCore engine exploitation

PwC's HackaDay Cybersecurity Competition, HK

Team Leader

Apr 2017 – Jun 2018

- 1st place in this competition in both 2017 and 2018
- Performed penetration testing. Reverse engineering, return-oriented programming, SQL-injection, and more skills were applied to achieve remote code execution on competition computers

FOUND VULNERABILITIES

ntfs-3g

- CVE-2021-39251, CVE-2021-39252, CVE-2021-39253, CVE-2021-39254, CVE-2021-39255, CVE-2021-39256, CVE-2021-39257, CVE-2021-39258, CVE-2021-39259, CVE-2021-39260, CVE-2021-39261, CVE-2021-39262, and CVE-2021-39263

Linux Kernel

- CVE-2022-29581, CVE-2022-1786, CVE-2022-2585

SKILLS

Computer Skills: Python, C/C++, Javascript, assembly language, PHP, SQL, MATLAB, LaTeX