Yihui (Kyle) ZENG

+1 805-710-0402 | zengyhkyle@gmail.com | @ky1ebot

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

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

WORK EXPERIENCE

Arizona State University, US

Research Assistant — Sep 2019 – present

- Research on the *fuzzing* automatic vulnerability discovery technique, symbolic execution, and Linux kernel security
- 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
- Published several academic papers on top security conferences

University of California, Santa Barbara, US

Staff Research Associate — Sep 2018 – Feb 2019

- Researched on path triage problem in symbolic execution for automatic vulnerability discovery. Applied symbolic execution, machine learning, graph theory, and crash analysis in this project. This work was published on RAID 2021
- Contributed to multiple popular open-source projects, including but not limited to: *angr*, *rex*, *archr*, and *shellphish-qemu*

HORNORS & AWARDS

- SCAI Doctoral Fellowship in 2022
- Engineering Graduate Fellowship in 2020

- Cybersecurity Fellowship in 2019
- 1978 Mathematics Alumnus Li Sze-lim Scholarship 2016-2017
- Scholarship for Outstanding Student in 2014, 2015, and 2016
- Dean's Honors List 2014-2015
- Matriculation Scholarship for Academic Excellence in 2013
- Ching-ling Soong Zhiyuan Scholarship in 2013

ACTIVITIES

Google kCTF, US Dec 2021 – present

Participant

- Performed local privilege escalation on Google Kubernetes Engine successfully twice. Exploited the Linux kernel with a 1-day vulnerability and a 0-day vulnerability, respectively
- Applied cross-cache attack in the Linux kernel and devised multiple previously unknown exploitation techniques to complete the exploitation
- Awarded 60k-100k bug bounty (in process)

Shellphish CTF Team, US Sep 2018 – present

Team Member

- Maintain the popular open-source project *how2heap*. Deviced *house-of-botcake* glibc heap exploitation technique
- 3rd place in CSAW'21 CTF (US-Canada region) in 2021
- Entered DEF CON CTF final competition in 2019, 2020, and 2021
- 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

SKILLS

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