Yihui (Kyle) ZENG

https://kylebot.net/

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

EDUCATION

Arizona State University

Ph.D. student, Major in Computer Science — Aug 2019 – Present

Advisors: Tiffany Bao, Yan Shoshitaishvili, Ruoyu (Fish) Wang, and Adam Doupé

The Chinese University of Hong Kong

B.S., Major in Mathematics, Minor in Computer Science — Aug 2013 – Jun 2018

Advisor: Wing Cheong Lau

PUBLICATIONS

- RetSpill: Igniting User-Controlled Data to Burn Away Linux Kernel Protections
  Kyle Zeng, *Zhenpeng Lin, Kangjie Lu, Xinyu Xing, Ruoyu Wang, Adam Doupé, Yan Shoshitaishvili, Tiffany Bao*
  Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2023.
- Greenhouse: Single-Service Rehosting of Linux-Based Firmware Binaries in User-Space Emulation
  Hui Jun Tay, ***Kyle Zeng****, Jayakrishna Menon Vadayath, Arvind S Raj, Audrey Dutcher, Tejesh Reddy, Wil Gibbs, Zion Leonahenahe Basque, Fangzhou Dong, Adam Doupé, Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang*
  Proceedings of the USENIX Security Symposium (USENIX), August 2023.
- Playing for K(H)eaps: Understanding and Improving Linux Kernel Exploit Reliability
  Kyle Zeng*, *Yueqi Chen*, Haehyun Cho, Xinyu Xing, Adam Doupé, 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 Doupé, 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.
- An Empirical Study on Mobile Payment Credential Leaks and Their Exploits
  Shangcheng Shi, Xianbo Wang, ***Kyle Zeng****, Ronghai Yang, Wing Cheong Lau*
  Proceedings of the 17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm'21), September 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 Doupé, 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

Apple Inc, US

Red Team Kernel & System Intern May 2023 – Aug 2023

- Investigated the security of the user space allocator, libmalloc, on macOS and found multiple critical design flaws
- Explore potential exploitation techniques to bypass the latest security defense kalloc_type deployed in XNU, the macOS kernel

Arizona State University, US

Research Assistant Sep 2019 – Present

- Researched Linux kernel security, symbolic execution, and the 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
- Published five peer-reviewed conference papers in the cyber security field

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, shellphish-qemu, and how2heap
- Advised by Giovanni Vigna and Christopher Kruegel

HORNORS & AWARDS

- Google PhD Fellowship, 2023
- 3rd place, Google Bug Hunters Leaderboard, 2023
- SCAI Doctoral Fellowship, Arizona State University, 2023
- 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

Pwn2Own Vancouver 2024, CA Feb 2024 – Mar 2024

Participant

- Winner of Pwn2Own in Ubuntu Desktop Privilege Escalation category ($20,000)
- Found, analyzed, and exploited one 0-day vulnerability (CVE not yet assigned) in the Linux kernel

Pwn2Own Toronto 2023, CA Sep 2023 – Oct 2023

Captain

- Led SEFCOM T0 team to analyze and find one 0-day vulnerabilities in Wyze Cam v3 camera
- Partially won Surveillance Systems category at Pwn2Own Toronto 2023 ($3,750)
- Reported the bug used at the competition to the vendor and waiting for CVE assignment

Pwn2Own Vancouver 2023, CA Feb 2023 – Mar 2023

Participant

- Winner of Pwn2Own in Ubuntu Desktop Privilege Escalation category ($30,000)
- Found, analyzed, and exploited one vulnerability (CVE-2023-1829) in the Linux kernel
- Designed a generic technique for exploitation double-free vulnerabilities in the Linux kernel

Pwn2Own Toronto 2022, CA Nov 2022 – Dec 2022

Captain

- Led ASU SEFCOM team to analyze and find three 0-day vulnerabilities in Synology NAS DS920+ network attached storage device
- Independently wrote a sophisticated heap-based 3-bug exploit chain by applying various heap-based exploitation techniques such as House-of-Spirit and Heap Fengshui
- Partially won NAS category at Pwn2Own Toronto 2022 ($10,000)
- One of the bugs used in our chain got labelled with CVE-2022-45188

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 ($70,000)
- 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 four 0-day vulnerabilities
- Applied cross-cache attack in the Linux kernel and devised four previously unknown exploitation techniques to complete the exploitations. All four novel techniques are confirmed by Google
- Awarded the first full bounty in kCTF's history ($91,337) for the CVE-2022-1786 submission
- Submissions: CVE-2021-4154, CVE-2022-29581, CVE-2022-1786, CVE-2022-2585, CVE-2023-1829

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 in 2021 and 3rd place in CSAW'22 CTF in 2022 (US-Canada region)
- 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, CVE-2022-4378, CVE-2023-0394, CVE-2023-23454, CVE-2023-42752, CVE-2023-42753, CVE-2023-42754, CVE-2023-42755, CVE-2023-42756

SKILLS

Computer Skills: Python, C/C++, Javascript, assembly language (x86_64, i386, aarch64, arm, mips), PHP, SQL, LaTeX