Weiteng Chen

Microsoft Research, Redmond

Phone: 9518233194
Email: weitengchen@microsoft.com
Gender: Male

EDUCATION

PhD. in Computer Science Sep 2017 - Sep 2022
University of California, Riverside, USA
- Overall GPA: 4.0

B.S. in Computer Science Sep 2012 - July 2016
Peking University, Beijing, P.R.China
- Overall GPA: 3.61/4

PUBLICATIONS

Weiteng Chen, and Zhiyun Qian. ”Off-path TCP exploit: how wireless routers can jeopardize your secrets.” 27th USENIX Security Symposium (USENIX Security 18).

Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, **Weiteng Chen**. ”Shadowblock: A lightweight and stealthy adblocking browser” In The World Wide Web Conference 2019.

Weiteng Chen, Xiaochen Zou, Guoren Li and Zhiyun QIan. ”KOOBE: Towards Facilitating Exploit Generation of Kernel Out-Of-Bounds Write Vulnerabilities” 29th USENIX Security Symposium (USENIX Security 20).

Weiteng Chen, Yu Wang, Zheng Zhang, Zhiyun Qian. ”SyzGen: Automated Generation of Syscall Specification of Closed-Source macOS Drivers” ACM CCS 2021.

Hang Zhang, **Weiteng Chen**, Yu Hao, Guoren Li, Yizhuo Zhai, Xiaochen Zou, Zhiyun Qian. ”Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels” ACM CCS 2021.

Xiaochen Zou, Guoren Li, **Weiteng Chen**, Hang Zhang, Zhiyun Qian. ”SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs” USENIX Security 2022.

Jian Liu, Lin Yi, **Weiteng Chen**, Chengyu Song, Zhiyun Qian, and Qiuping Yi. ”LinKRID: Vetting Imbalance Reference Counting in Linux kernel with Symbolic Execution” USENIX Security 2022.

Yizhuo Zhai, Yu Hao, Zheng Zhang, **Weiteng Chen**, Guoren Li, Zhiyun Qian, Chengyu Song, Manu Sridharan, Srikanth V. Krishnamurthy, Trent Jaeger, Paul Yu. ”Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel” In Proceedings of the Network & Distributed System Security Symposium (NDSS) 2022, San Diego, CA.

Yu Hao, Guoren Li, Xiaochen Zou, **Weiteng Chen**, Shitong Zhu, Zhiyun Qian, and Ardalan Amiri Sani. “SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers” [To appear] In Proceedings of IEEE Security and Privacy (Oakland) 2023, San Francisco, CA.

SELECTED AWARDS AND HONORS

2022 A $26,500 bug bounty from Apple Inc.
2021 Dissertation Year Program Award
2019 IRTF 2019 Applied Networking Research Prize
2018 Usenix Security’18 Student Grant
2018 CSAW’18 Applied Research Competition US-CANADA Finalist
2017 A $15,000 award at GeekPwn International Security Geek Contest 2017 Silicon Valley
2015 Merit Student
2015 May 4th scholarship (top 20%)
2014 POSCO Asia Fellowship (top 10%)

RESEARCH INTERESTS

Fuzzing, Program Analysis, Kernel Exploitation, Operating Systems, Network Security, Mobile Security, Privacy and Side Channel Attacks.

PROJECT HOMEPAGE

https://github.com/seclab-ucr
https://github.com/CvvT

WORK EXPERIENCE

Senior Researcher Microsoft Research
Oct. 2022 - Present Redmond, WA

. Confidential computing
. AI for security

Security Research Intern IBM Research
June 2022 - September 2022 Yorktown Heights, NY

Fuzzing Linux Kernel
. I developed a novel system to automate the generation of syscall specifications with respect to their dependencies and found 30+ unique bugs in the Linux kernel.

Security Software Developer Intern Facebook Inc.
June 2021 - September 2021 Menlo Park, CA

Binary-only Fuzzing
. Integrating AFL-QEMU to support binary-only fuzzing on a large fleet of remote machines
. Bug triaging and exploitability assessment via GDB scripts

Security Research Intern Didi Research America LLC.
July 2018 - September 2018 450 National Avenue, Mountain View, CA

Analyzing Linux Vulnerabilities and Exploits
. Analyze Linux vulnerabilities and exploits
. Fuzzing Linux kernel and Windows subsystem for Linux

RESEARCH EXPERIENCE

Research Assistant Security Lab, UC, Riverside
September 2017 - Present California, USA

Off-Path TCP Exploit by Leveraging a Timing Side Channel in Wireless Routers
. We reported the timing side channel inherent in all generations of Wi-Fi technology and had a teleconference with IEEE 802.11 working group. Though the vulnerability is acknowledged, we are yet to see an appropriate solution to eliminate it in the near future.
. We showed that the side channel affects macOS, Windows, and Linux by inspecting their kernel source code and conducting real-world attacks (*i.e.,* off-path TCP injection) against them.

KOOBE: Towards Facilitating Exploit Generation of Kernel Out-Of-Bounds Write Vulnerabilities
. We implemented a framework, namely KOOBE, to facilitate exploit generation of kernel OOB write vulnerabilities by combining fuzzing and symbolic execution.
. KOOBE could assess the severity of a Linux OOB write vulnerability by attempting to generate a corresponding PoC that could achieve IP hijacking demonstrating the need for an immediate fix

SyzGen: Automated Generation of Syscall Specification of Closed-Source macOS Drivers
. We developed SyzGen capable of automatically extracting both structures and constraints of

syscall arguments, as well as the dependencies between syscalls, given a specific macOS driver.
. We evaluated SyzGen against 25 drivers on macOS and found 34 bugs, 5 of which have been assigned CVE numbers so far.

Research Assistant Information Security Lab., Peking University
September 2014 - June 2017 California, USA

Unpacking Packed Android Application
. Analyzed 3 commercial packing technologies developed by Tencent, Alibaba and Baidu.
. Propose a framework to automatically unpack applications during runtime.

Research Assistant Network and Information Security Lab, Tsinghua University
July 2015 - June 2016 California, USA

Devising Challenges for AliCTF 2016
. Devise one challenge for AliCTF 2016. Several technologies were employed, including java and native code obfuscation, anti analysis, bytecode self-modification, encryption, etc.