

Zhenpeng Lin

✉ zplin@u.northwestern.edu

🌐 zplin.me

🐦 Markak

Education

- 2021– current **PhD in Computer Science**, *Northwestern University*
Advisor : Xinyu Xing
- 2019–2021 **Master's Degree in Computer Science**, *Penn State University*
Advisor : Xinyu Xing
- 2018–2019 **Master Student in Computer Science**, *Wuhan University*
Advisor : Guojun Peng
- 2014–2018 **Bachelor's Degree in Computer Science**, *Xidian University*

Real-world Hacking Experience

Linux Kernel Exploiter

My research mainly focuses on understanding the exploitability of kernel bugs. Therefore, exploiting the kernel is part of my daily routine. I have found numerous 0days during my research and have demonstrated exploitation in Google Pixel (Demo, click me), Google's Container-Optimized OS (COS), and various Linux distros.

Google Bug Hunter

In 2022 and 2023, I ranked *18th* at Google Bug Hunters Leaderboard. I primarily contributed to the KCTF VRP. I was the very first to successfully exploit it, and so far, I have earned over \$200k rewards from Google.

Pwn2Own Winner

At Pwn2Own 2022, I successfully demonstrated the exploitation of the latest Ubuntu system. I leverage my kernel exploitation expertise to find and exploit the vulnerability (CVE-2022-2588).

BlackHat Speaker

I have presented my research at all of the Black Hat events, including Black Hat Asia, Black Hat EU, and Black Hat USA. One of my favorites is the DirtyCred technique, which helps develop a universal exploit against various Linux kernels across different architectures, and versions.

Kernel Defender

In addition to exploiting the kernel, I also help patch kernel vulnerabilities and develop techniques to protect the kernel. My knowledge and expertise enable me to enhance Grsecurity's AUTOSLAB and develop effective defenses such as HotBPF and CAMP (both are research works under submission).

DEFCON CTFer

I have been playing CTF since my freshman year and have won numerous prizes with team Nu1L(which is Straw Hat now). In both 2021 and 2022, we made it to the DEFCON Final and ranked *7th* in both years.

Publications

DirtyCred: Escalating Privilege in Linux Kernel

Zhenpeng Lin, Yuhang Wu, Xinyu Xing

ACM CCS 2022

GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs (CSAW 2022 Top-10 Finalist)

Zhenpeng Lin, Yueqi Chen, Dongliang Mu, Chensheng Yu, Yuhang Wu, Xinyu Xing, Kang Li

IEEE S&P 2022

An In-depth Analysis of Duplicated Linux Kernel Bug Reports

Dongliang Mu, Yuhang Wu, Yueqi Chen, **Zhenpeng Lin**, Chensheng Yu, Xinyu Xing, Gang Wang

NDSS 2022

A Systematic Study of Elastic Objects in Kernel Exploitation

Yueqi Chen, **Zhenpeng Lin**, Xinyu Xing

ACM CCS 2020

Other Publications

Cautious! A New Exploitation Method! No Pipe but as Nasty as Dirty Pipe

Zhenpeng Lin, Yuhang Wu, Xinyu Xing

Black Hat USA 2022

HotBPF - An On-demand and On-the-fly Memory Protection for the Linux Kernel

Yueqi Chen, **Zhenpeng Lin**

Linux Security Summit Europe 2022

Your Trash Kernel Bug, My Precious 0-day

Zhenpeng Lin, Yueqi Chen, Xinyu Xing, Kang Li

Black Hat Europe 2021

Finding Multiple Bug Effects for More Precise Exploitability Estimation

Zhenpeng Lin, Yueqi Chen

Linux Security Summit North America 2021

A General Approach to Bypassing Many Kernel Protections and its Mitigation.

Yueqi Chen, **Zhenpeng Lin**, Xinyu Xing

Black Hat Asia 2021

Bypassing Many Kernel Protections Using Elastic Objects.

Yueqi Chen, **Zhenpeng Lin**

Linux Security Summit Europe 2020

Work Experience

Nov.2023– **Certik**, Research Intern, Mentored by Kang Li

Current Worked on low-level security of Web 3 infrastructures (layer-1 blockchains), trustzone, and kernel security.

- May.2021– **Grsecurity**, *Research Intern, mentored by Brad Spengler & Pax Team*
July.2021 Worked on improving and evaluating AUTOSLAB – a Linux kernel heap hardening.
- May.2020– **Baidu**, *Research Intern, mentored by Kang Li*
July.2020 Worked on escalating the exploitability of Linux kernel vulnerabilities. Generated a research paper – GREBE.
- April.2019– **Arizona State University**, *Research Intern, mentored by Fish Wang*
July.2019 Worked on optimizing IR lifting to accelerate symbolic execution engine (e.g., angr)

■ Honors and Awards

- 2023 *18th* at Google Bug Hunter Leaderboard
- 2022 Android VRP rewards for CVE-2022-20409
- 2022 KCTF rewards for CVE-2022-20409
- 2022 KCTF rewards for CVE-2022-2588
- 2022 KCTF rewards for CVE-2022-29581
- 2022 CSAW Best Applied Security Paper Award TOP-10 Finalists
- 2022 *7th* at DEF CON Finals 2022
- 2022 Pwn2Own Winner
- 2021 KCTF rewards for CVE-2021-4154
- 2021 *7th* at DEF CON Finals 2021
- 2020 Black Hat USA, Student Scholarship
- 2019 *5th* at DEF CON Qualifier 2019
- 2018 *1st* at Baidu AI CTF
- 2018 *1st* at WCTF Junior
- 2018 *4th* at OCTF/TCTF
- 2017 *1st* at BCTF

■ Community Services

PC Reviewer

IEEE Workshop on Offensive Technologies, WOOT 2023
International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2023

External Reviewer

IEEE Security and Privacy, S&P 2023
ACM CCS 2022, IEEE Security and Privacy 2022
USENIX Security 2021, ACM CCS 2021, IEEE Security and Privacy 2021
USENIX Security 2020, ACM CCS 2020