Zhenpeng Lin

✉ zplin@u.northwestern.edu · https://zplin.me

Education

Northwestern University 2022 – Present
Ph.D student advised by Xinyu Xing
Penn State University 2019 – 2022
Ph.D student advised by Xinyu Xing
Wuhan University 2018 – 2019
Master student advised by Guojun Peng
Xidian University 2014 – 2018
B.E. in Cyberspace Security

Research Interests

Binary Analysis, Reverse Engineering, and Vulnerability & Exploitation

Publications

DirtyCred: Escalating Privilege in Linux Kernel
Zhenpeng Lin, *Yuhang Wu, Xinyu Xing*
ACM CCS 2022
GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs
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

Talks

Cautious! A New Exploitation Method! No Pipe but as Nasty as Dirty Pipe
Zhenpeng Lin, *Yuhang Wu, Xinyu Xing*
Black Hat USA 2022

Your Trash Kernel Bug, My Precious 0-day.
Zhenpeng Lin, *Yueqi Chen, Xinyu Xing, Kang Li*
Black Hat Europe 2021

Finding Multiple Bug Effectis 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

Experiences

Grsecurity May. 2021 – July. 2021

Research Intern, worked with Brad Spengler & Pax Team

Worked on improving and evaluating a Linux kernel heap hardening.

Baidu X-Lab May. 2020 – July. 2020

Research Intern, worked with Kang Li

Worked on escalating the exploitability of Linux kernel vulnerabilities.

Arizona State University Apr. 2019 – July. 2019

Summer Intern, worked with Ruoyu (Fish) Wang

Focused on optimizing IR lifting to accelerate symbolic execution engine (e.g., angr).

Automatic Exploit Generation System July. 2017 - Sep. 2018

independent researcher

Won 3rd place in RHG 2017 and 1st place in Baidu AI CTF 2018.

Chaitin Tech Inc. Sep. 2017 – Jan. 2018

Security Researcher

Worked on vulnerability discovery and exploitation, found critical vulnerabilities causing remote code execution (RCE) and local privilege escalation (LPE) in HUAWEI's products: CVE-2017-8187, CVE-2017-8188, CVE-2017-8190, CVE-2017-8191, CVE-2017-17223, CVE-2017-17221, CVE-2017-17222.

Honors and Awards

7th at DEF CON Finals 2022	2022
Pwn2Own Winner	2022
LSS North America, Student Travel Grant Award	2021
Black Hat USA, Student Scholarship	2021
7th at DEF CON Finals 2021	2021
Black Hat USA, Student Scholarship	2020
5th at DEF CON Qualifier 2019	2019
1st at Baidu AI CTF	2018
1st atWCTF Junior	2018
4th at 0CTF/TCTF	2018
1st at BCTF	2017

Community Services

External reviewer

IEEE Security and Privacy 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