

# Penghui Li

Ph.D. candidate  
Department of Computer Science and Engineering  
The Chinese University of Hong Kong

☎: +852-65535797  
✉: phli@cse.cuhk.edu.hk  
🏠: <https://peng-hui.github.io>

## EDUCATION

Ph.D. Computer Science and Engineering, The Chinese University of Hong Kong, 2019–2023  
B.E. Computer Science and Technology, University of Chinese Academy of Sciences, 2015–2019

## RESEARCH AREAS

Software security and testing: scalable static analysis, holistic symbolic execution, and fuzz testing  
Software engineering and assessment: empirical and statistic analysis of bugs and patches

## RESEARCH EXPERIENCE

2019.08–2023.07

The Chinese University of Hong Kong  
Research Assistant  
Advisor: Professor. Wei Meng

2022.02–2022.09

Tsinghua University  
Visiting Student  
Host: Professor. Chao Zhang

2018.10–2019.06

Institute of Information Engineering, Chinese Academy of Sciences  
Research Intern  
Host: Professor. Kai Chen

## PUBLICATIONS

I have published 5 papers in top-tier software security and engineering venues such as ESEC/FSE, ASE, CCS, WWW. My work has found hundreds of new bugs in foundational system software, *e.g.*, PHP interpreter and Linux kernel, and has received recognition with awards from academia and industry.

- 2023 DDRace: Finding Concurrency UAF Vulnerabilities with Directed Fuzzing  
Ming Yuan, Bodong Zhao, Penghui Li, Jiashuo Liang, Xinhui Han, Xiapu Luo, Chao Zhang  
In Submission to the 32nd USENIX Security Symposium (Security), 2023 (Accept  
Conditional on Major Revision)
- 2023 SDFuzz: Practical Directed Fuzzing with Context-Sensitive Target State Feedback  
Penghui Li, Wei Meng, Chao Zhang  
In Submission to the 45th International Conference on Software Engineering (ICSE), 2023

- 2023 SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration  
Changhua Luo, Wei Meng, Penghui Li  
Conditionally Accepted to the 44th IEEE Symposium on Security and Privacy (Oakland), 2023
- 2022 SEDiff: Scope-Aware Differential Fuzzing to Test Internal Function Models in Symbolic Execution  
Penghui Li, Wei Meng, Kangjie Lu  
In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), 2022
- 2022 TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications  
Changhua Luo, Penghui Li, Wei Meng  
In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS), 2022  
**Best Paper Honorable Mention Award**
- 2021 Understanding and Detecting Performance Bugs in Markdown Compilers  
Penghui Li, Yinxi Liu, Wei Meng  
In Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2021
- 2021 LChecker: Detecting Loose Comparison Bugs in PHP  
Penghui Li, Wei Meng  
In Proceedings of the Web Conference (WWW), 2021
- 2021 On the Feasibility of Automated Built-in Function Modeling for PHP Symbolic Execution  
Penghui Li, Wei Meng, Kangjie Lu, Changhua Luo  
In Proceedings of the Web Conference (WWW), 2021

## AWARDS AND HONORS

- 2022 Best Paper Honorable Mention Award, CCS 2022
- 2022 Reaching Out Award, HKSAR
- 2021 Top 5 Finalist of Software Artifact Award
- 2021 PCCW-HKT Scholarship Nomination
- 2021 The Web Conference Student Scholarship
- 2021 GitLab Bug Bounty
- 2019 CUHK Postgraduate Student Scholarship
- 2018 Merit Student
- 2017 Merit Student
- 2016 Outstanding Individual in Research Practice

## PROFESSIONAL SERVICES

### External Reviewer

2023	IEEE Symposium on Security and Privacy
2021–2022	The ACM Conference on Computer and Communications Security
2020–2022	The Web Conference
2021–2022	The ACM Asia Conference on Computer and Communications Security

### Teaching Assistant

2021 Fall	Introduction to Database Systems
2021 Spring	Building Web Applications
2020 Fall	Introduction to Cyber Security
2020 Spring	Linear Algebra for Engineers
2019 Fall	Introduction to Cyber Security

### Student Research Mentor

2021.10–2022.05	Yanting Chi, undergraduate student from SJTU Bachelor degree thesis on symbolic execution Next position: Ph.D. student at University of Minnesota, Twin Cities
2018.10–2019.04	ChiHo Cheng, undergraduate student from CUHK Final-year project on PHP static analysis
2018.10–2019.04	HoiHim Chan, undergraduate student from CUHK Final-year project on PHP static analysis

## MISCELLANEOUS

### Open-Source Software

2021	MdPerfFuzz: an extensible language-compiler fuzzer for performance bugs <a href="https://github.com/cuhk-seclab/MdPerfFuzz">https://github.com/cuhk-seclab/MdPerfFuzz</a> Top 5 Finalist of Software Artifact Award in ASE 2021
2021	XSym: a holistic cross-language symbolic execution engine for PHP-based web applications <a href="https://github.com/cuhk-seclab/XSym">https://github.com/cuhk-seclab/XSym</a>
2021	LChecker: a static detector for PHP loose comparison bugs <a href="https://github.com/cuhk-seclab/LChecker">https://github.com/cuhk-seclab/LChecker</a>

### Selected Bug Findings

CPU-exhaustion denial-of-service vulnerabilities  
CVE-2021-22217, CVE-2021-39877, *etc.*

Loose comparison bugs  
CVE-2020-23352, CVE-2020-23353, CVE-2020-23355, CVE-2020-23356, CVE-2020-23357,  
CVE-2020-23358, CVE-2020-23359, CVE-2020-23360, CVE-2020-23361, *etc.*

## REFERENCES

### **Wei Meng**

Assistant Professor  
Department of Computer Science and Engineering  
The Chinese University of Hong Kong  
Room 109, Ho Sin-Hang Engineering Building, Shatin  
New Territories, Hong Kong  
✉: wei@cse.cuhk.edu.hk

### **Kangjie Lu**

Assistant Professor  
Department of Computer Science and Engineering  
University of Minnesota  
5-217 Keller Hall, 200 Union Street SE  
Minneapolis, MN 55455  
✉: kjlu@umn.edu

### **Chao Zhang**

Associate Professor  
Institute for Network Sciences and Cyberspace  
Tsinghua University  
3-209 FIT Building, Haidian District  
Beijing, China 100084  
✉: chaoz@tsinghua.edu.cn