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

The Chinese University of Hong Kong Aug 2019 – Jul 2023
Doctor of Philosophy, Computer Science and Engineering

University of Chinese Academy of Sciences Aug 2015 – Jul 2019
Bachelor of Engineering, Computer Science and Technology

Columbia University Jan 2018 – May 2018
Visiting Student, Computer Science and Engineering

Research Experience

The Chinese University of Hong Kong Aug 2019 – Jul 2023
Graduate Student
Advisor: Professor Wei Meng

Tsinghua University Feb 2022 – Sep 2022
Visiting Student
Host: Professor Chao Zhang

Institute of Information Engineering, Chinese Academy of Sciences Oct 2018 – Jun 2019
Research Intern
Host: Professor Kai Chen

Research Interests

Computer security, software engineering, program analysis

Publication

My research so far has found hundreds of new bugs, and has resulted in urgent updates in foundational systems such as Linux kernel and GitHub. Research outcome has been published in top security and software engineering venues, and has received recognition with awards from academia and industry.

[1] **SDFuzz: Practical Directed Fuzzing with Context-Sensitive Target State Feedback**
Penghui Li, Wei Meng, and Chao Zhang
In Submission to The International Conference on Software Engineering (ICSE). 2023.

[2] **SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration**
Changhua Luo, Wei Meng, and Penghui Li
In Conditional Accept to The IEEE Symposium on Security and Privacy (Oakland). 2023.

[3] **DDRace: Finding Concurrency UAF Vulnerabilities with Directed Fuzzing**
Ming Yuan, Bodong Zhao, Penghui Li, Jiashuo Liang, Xinhui Han, Xiapu Luo, and Chao Zhang
In Conditional Accept to The USENIX Security Symposium (Security). 2023.

[4] **SEDiff: Scope-Aware Differential Fuzzing to Test Internal Function Models in Symbolic Execution**
Penghui Li, Wei Meng, and Kangjie Lu
In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE). 2022.

[5] **TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications**
Changhua Luo, Penghui Li, and Wei Meng
In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS). 2022.
☆ ACM CCS 2022 Best Paper Honorable Mention Award.

[6] **Understanding and Detecting Performance Bugs in Markdown Compilers**
Penghui Li, Yinxi Liu, and Wei Meng
In Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE). 2021.
☆ Top 5 Finalist of Best Software Artifact Award.

[7] **LChecker: Detecting Loose Comparison Bugs in PHP**
Penghui Li and Wei Meng
In Proceedings of the Web Conference (WWW). 2021.

[8] **On the Feasibility of Automated Built-in Function Modeling for PHP Symbolic Execution**
Penghui Li, Wei Meng, Kangjie Lu, and Changhua Luo
In Proceedings of the Web Conference (WWW). 2021.

Awards and Honors

ACM CCS 2022 Best Paper Honorable Mention Award	Nov 2022
HKSAR Reaching Out Award	Apr 2022
IEEE/ACM ASE 2021 Top 5 Finalist of Best Software Artifact Award	Nov 2021
PCCW-HKT Scholarship Nomination	Aug 2021
GitLab Bug Bounty	May 2021
The Web Conference Student Scholarship	Mar 2021
GitLab Bug Bounty	Jan 2021
CUHK Postgraduate Student Scholarship	Aug 2019 – Jul 2023
Merit Student	Jul 2018
Merit Student	Jul 2017
Outstanding Individual in Research Practice	Jul 2016

Professional Services

External Reviewer

IEEE Symposium on Security and Privacy (Oakland)	2023
The ACM Conference on Computer and Communications Security (CCS)	2021 – 2022
The Web Conference (WWW)	2020 – 2022
The ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2021 – 2022

Teaching Assistant

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

Student Research Mentor

Yanting Chi Oct 2021 – May 2022
Undergraduate student from SJTU
Bachelor degree thesis on symbolic execution
Next position: Ph.D. student at University of Minnesota, Twin Cities

Chiho Cheng Oct 2018 – Apr 2019
Undergraduate student from CUHK
Final-year project on PHP static analysis

Hoihim Chan Oct 2018 – Apr 2019
Undergraduate student from CUHK
Final-year project on PHP static analysis

Miscellaneous

Open-Source Software

MdPerfFuzz
An extensible performance bug fuzzer for language compilers
`https://github.com/cuhk-seclab/MdPerfFuzz`

XSym
A holistic cross-language symbolic execution engine for PHP-based web applications
`https://github.com/cuhk-seclab/XSym`

LChecker
A static detector for PHP loose comparison bugs
`https://github.com/cuhk-seclab/LChecker`

Selected Vulnerability Findings

CPU-exhaustion DoS vulnerabilities
CVE-2021-22217, CVE-2021-39877

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

References

Wei Meng
Assistant Professor
Department of Computer Science and Engineering
The Chinese University of Hong Kong
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

Updated in Dec 2022