Penghui Li

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

: +86-15810530509
: 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
Advisor: Professor Wei Meng

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

Professional Experience

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

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

Research Interests and Impacts

I am generally interested in computer security, software engineering, and program analysis. My research has found over three hundred new software bugs, resulting in urgent updates in foundational systems such as Linux kernel and GitHub. All my research works have been published at top computer security and software engineering venues.

Publication

[1] **Holistic Concolic Execution for Dynamic Web Applications via Symbolic Interpreter Analysis**
Penghui Li, Wei Meng, and Chenlin Wang
Under Review.

[2] **SDFuzz: Effective Directed Fuzzing Driven by Target States**
Penghui Li, Wei Meng, and Chao Zhang
Under Review.

[3] **Testing Graph Database Systems via Graph-Aware Metamorphic Relations**
Zeyang Zhuang, Penghui Li, Pingchuan Ma, Wei Meng, and Shuai Wang
Under Review.

[4] **DDRace: Finding Concurrency UAF Vulnerabilities in Linux Drivers with Directed Fuzzing**
Ming Yuan, Bodong Zhao, Penghui Li, Jiashuo Liang, Xinhui Han, Xiapu Luo, and Chao Zhang
In Proceedings of the 32nd USENIX Security Symposium (Security). August 2023.

[5] **Detecting Correctness, Security, and Performance Bugs in Software Systems with Automated Analysis and Testing**
Penghui Li
Ph.D. Thesis, The Chinese University of Hong Kong. July 2023.

[6] **SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration**
Changhua Luo, Wei Meng, and Penghui Li
In Proceedings of the 44th IEEE Symposium on Security and Privacy (Oakland). May 2023.

[7] **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). November 2022.

[8] **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). November 2022.
☆ ACM CCS 2022 Best Paper Honorable Mention.

[9] **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). November 2021.
☆ Top 5 Finalist of Best Software Artifact.

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

[11] **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). April 2021.

Awards and Honors

ACM CCS 2022 Best Paper Honorable Mention	Nov 2022
HKSAR Reaching Out Award	Apr 2022
IEEE/ACM ASE 2021 Top 5 Finalist of Best Software Artifact	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
UCAS Merit Student	Jul 2018
UCAS Merit Student	Jul 2017
UCAS Outstanding Individual in Research Practice	Jul 2016

Professional Services

Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)	2023

External Reviewer

IEEE Symposium on Security and Privacy (Oakland)	2023 – 2024
The Annual Computer Security Applications Conference (ACSAC)	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 Experience

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

TChecker

A precise static analysis for identifying taint-style vulnerabilities

`https://github.com/cuhk-seclab/tchecker`

SEDiff

A differential fuzzing framework for testing symbolic execution engines

`https://zenodo.org/record/6665380`

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