Penghui Li

Researcher
Zhongguancun Laboratory

✉: lipenghui315@gmail.com
🏠: https://peng-hui.github.io

Research Interests

I am broadly interested in **security and privacy**. My research aims to automatically and efficiently detect security threats, and safeguard services and users from attacks. I have found **over three hundred new vulnerabilities**, resulting in urgent updates in foundational systems such as Linux kernel and GitHub.

Education

The Chinese University of Hong Kong Aug. 2019 – July 2023
Doctor of Philosophy, Computer Science and Engineering
Advisor: Professor Wei Meng
GPA: 3.97/4

University of Chinese Academy of Sciences Aug. 2015 – July 2019
Bachelor of Engineering, Computer Science and Technology
GPA: 3.87/4

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

Publication

Summary: First-author × 7, S&P/Security/CCS × 6, FSE/ASE × 2, WWW × 2, VLDB × 1

[1] **FuzzCache: Optimizing Web Application Fuzzing with Software-Based Data Cache**
Penghui Li and Mingxue Zhang
In Proceedings of the 31st ACM Conference on Computer and Communications Security (CCS). Oct. 2024.

[2] **SDFuzz: Target States Driven Directed Fuzzing**
Penghui Li, Wei Meng, and Chao Zhang
In Proceedings of the 33rd USENIX Security Symposium (Security). Aug. 2024.

[3] **Testing Graph Database Systems via Graph-Aware Metamorphic Relations**
Zeyang Zhuang, Penghui Li, Pingchuan Ma, Wei Meng, and Shuai Wang
In Proceedings of the 50th International Conference on Very Large Data Bases (VLDB). Aug. 2024.

[4] **Holistic Concolic Execution for Dynamic Web Applications via Symbolic Interpreter Analysis**
Penghui Li, Wei Meng, Mingxue Zhang, Chenlin Wang, and Changhua Luo
In Proceedings of the 45th IEEE Symposium on Security and Privacy (Oakland). May 2024.

[5] **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). Aug. 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). Nov. 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). Nov. 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). Nov. 2021.
☆ Best Software Artifact Nomination.

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

Under Review

[12] **Augmenting PoC Exploit Generation for Node.js Applications Using Test Suites**
Changhua Luo, Penghui Li, Wei Meng, and Chao Zhang
Under Review. 2024.

[13] **Predator: Efficient Dynamic Validation for Web Application Vulnerabilities**
Chenlin Wang, Wei Meng, Changhua Luo, and Penghui Li
Under Review. 2024.

Theses

[14] **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.

[15] **Detecting CPU Exhaustion Denial-of-Service Vulnerabilities in Web Applications**
Penghui Li
B.Eng. Thesis, University of Chinese Academy of Sciences. June 2019.

Research Experience

Zhongguancun Laboratory Sep. 2023 – Present
Researcher

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

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

Awards and Honors

ACM CCS 2022 Best Paper Honorable Mention	Nov. 2022
HKSAR Reaching Out Award	Apr. 2022
IEEE/ACM ASE 2021 Best Software Artifact Normination	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 – July 2023
UCAS Merit Student	July 2018
UCAS Merit Student	July 2017
UCAS Outstanding Individual in Research Practice	July 2016

Professional Services

Program Committee Member

European Conference on Computer Systems (EuroSys), Shadow PC	2024
Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)	2024
USENIX Security (Security), Artifact Evaluation Committee	2024
The ACM Conference on Computer and Communications Security (CCS), Artifact Evaluation Committee	2023

Reviewer

ACM Transactions on Software Engineering and Methodology (TOSEM)
IEEE Transactions on Dependable and Secure Computing (TDSC)

External Reviewer

ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)	2024
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

Grant Experience

Project Title: Detecting Memory-Safety Vulnerabilities in Multilingual Software

- No. 14209323, General Research Fund from Hong Kong Research Grants Council, 2023
- Principal investigator: Prof. Wei Meng
- Awarded amount: 1,352,729 HKD
- My role: planned the project and wrote the initial proposal draft under the guidance of the PI

Teaching and Mentoring

Teaching Assistantship

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

Research Mentorship

Chenlin Wang — Aug. 2023 – Dec. 2023

- Ph.D. student at CUHK
- My role: worked as a collaborator and provided high-level suggestions for his PHP fuzzing project

Changhua Luo — Nov. 2019 – July 2022

- Ph.D. student at CUHK
- My role: mentored the award-winning static analysis project [8]

Yanting Chi Oct. 2021 – May 2022

- Undergraduate student from SJTU
- My role: guided his bachelor's 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
- My role: guided the final-year project on PHP static analysis, especially taint analysis

Hoihim Chan Oct. 2018 – Apr. 2019

- Undergraduate student from CUHK
- My role: guided the final-year project on PHP static analysis, especially taint analysis

Open-Source Contributions

TChecker: a static analysis tool with precise inter-procedural support 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

Access Control Vulnerabilities

- 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