Penghui Li

https://peng-hui.github.io · phli@cse.cuhk.edu.hk · +852-65535797

Research Interest

Software security; software engineering; program analysis.

Education

The Chinese University of Hong Kong 2019.08 – 2023.07

- Ph.D. in Computer Science and Engineering, GPA: 3.97/4

University of Chinese Academy of Sciences 2015.09 – 2019.07

- B.E. in Computer Science and Technology, GPA: 3.83/4

Publications

★ My research aims to understand and detect software bugs with automated and scalable approaches. My work has found hundreds of new bugs in foundational system software, *e.g.,* PHP interpreter and Linux kernel. Research outcome has been published in top software security and engineering venues such as ESEC/FSE, ASE, CCS, WWW, and has received recognition with awards from academia and industry.

[1] DDRace: Finding Concurrency UAF Vulnerabilities with Directed Fuzzing
Ming Yuan, Bodong Zhao, Penghui Li, Jiashuo Liang, Xinhui Han, Xiapu Luo, and Chao Zhang
In Submission to The 32nd USENIX Security Symposium (Security). Anaheim, CA, August 2023.

[2] SDFuzz: Practical Directed Fuzzing with Context-Sensitive Target State Feedback
Penghui Li, Wei Meng, and Chao Zhang
In Submission to The 45th International Conference on Software Engineering (ICSE). Melbourne, Australia, May 2023.

[3] SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration
Changhua Luo, Wei Meng, and Penghui Li
In Submission to The 44th IEEE Symposium on Security and Privacy (Oakland). San Francisco, CA, May 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). Singapore, November 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). Los Angeles, CA, November 2022.

[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). Melbourne, Australia, November 2021.

[7] LChecker: Detecting Loose Comparison Bugs in PHP
Penghui Li and Wei Meng
In Proceedings of The Web Conference (WWW). Ljubljana, Slovenia, April 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). Ljubljana, Slovenia, April 2021.

Selected Awards

- Reaching Out Award, HKSAR 2022.04
- Top 5 Finalist of Software Artifact Award in ASE 2021.11
- PCCW-HKT Scholarship Nomination 2021.08
- The Web Conference 2021 Student Scholarship 2021.03
- Postgraduate Scholarship 2019.08 – 2023.07
- Merit Student 2017/2018
- Outstanding Individual in Research Practice 2016.07

Professional Services

External Reviewer

- IEEE Symposium on Security and Privacy 2023
- The ACM Conference on Computer and Communications Security (CCS) 2021/2022
- The Web Conference (WWW) 2020/2021/2022
- The ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2021/2022

Teaching Assistant

- Introduction to Database Systems 2021F
- Building Web Applications 2021S
- Introduction to Cyber Security 2019F/2020F
- Linear Algebra for Engineers 2020S

Student Research Mentor

- Yanting Chi
  Final-year undergraduate student from SJTU
  Bachelor degree thesis on symbolic execution 2021.08 – 2022.05
  Next position: Ph.D. student at University of Minnesota, Twin Cities
- ChiHo Cheng
  Final-year undergraduate student from CUHK
  Final-year project on PHP code analysis 2018.10 – 2019.04
- HoiHim Chan
  Final-year undergraduate student from CUHK
  Final-year project on PHP code analysis 2018.10 – 2019.04

Miscellaneous

Open-Source Software

- MdPerfFuzz: an extensible language-based fuzzer for performance bugs. 2021.10
  `https://github.com/cuhk-seclab/MdPerfFuzz`
  ★ Top 5 Finalist of Software Artifact Award in ASE 2021
- XSym: a cross-language symbolic execution engine for PHP. 2021.08
  `https://github.com/cuhk-seclab/XSym`
- LChecker: a static detector for PHP loose comparison bugs. 2021.05
  `https://github.com/cuhk-seclab/LChecker`

Acknowledged Bugs

- 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.*