李鹏辉

出生年月 ：1997.04　　联系电话 ：158 1053 0509

籍　　贯 ：湖南长沙　　电子邮件 ：phli@cse.cuhk.edu.hk

学　　历 ：博士研究生　　个人主页 ：peng-hui.github.io

教育背景

香港中文大学 2019.08 – 2023.07

博士，计算机科学与工程学系，绩点：3.97/4.00

指导老师：孟玮教授

中国科学院大学 2015.09 – 2019.07

学士，计算机科学与技术学院，绩点：3.83/4.00

哥伦比亚大学 2018.01 – 2018.05

访问学生，工程学院

研究经历

清华大学 2022.02 – 2022.09

访问学生，指导老师：张超教授

中科院信息工程研究所 2018.10 – 2019.06

研究实习生，指导老师：陈恺研究员

研究兴趣与影响

主要研究方向为**系统安全、软件工程、程序分析**。

以往的研究工作已在重要系统软件中发现了超过 300 个软件缺陷和安全漏洞，推动了基础软件的更新（如 PHP 语言解释器和 Linux 内核）。**所有研究成果均发表于相关领域的顶级会议**（中国计算机学会推荐 A 类会议）。

论文发表

★ 目前已发表 7 篇 CCF-A 类长文，其中 4 篇担任第一作者。

[1] **SDFuzz: Effective Directed Fuzzing Driven by Target States**

Penghui Li, Wei Meng, and Chao Zhang

Under Review.

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

[3] **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.

[4] **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.

[5] **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.

[6] **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.

[7] **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.

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

[9] **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.

荣誉奖励

ACM CCS 最佳论文提名	2022.11
香港特别行政区政府外展体验奖	2022.04

ASE 2021 最佳软件奖	2021.11
盈科-香港电讯奖学金提名	2021.08
GitLab 漏洞赏金	2021.05
ACM WWW 学生奖学金	2021.03
GitLab 漏洞赏金	2021.01
香港中文大学博士奖学金	2019.08 – 2023.07
三好学生	2017.06
三好学生	2017.06
科研优秀个人	2016.06

专业服务

外部评审

IEEE 安全与隐私研讨会 (Oakland)	2023
ACM 计算机与通信安全会议 (CCS)	2021 – 2023
ACM 国际万维网会议 (WWW)	2020 – 2022
ACM 亚洲计算机与通信安全会议 (AsiaCCS)	2021 – 2022

教学经验

课程助教

计算机与网络安全	2021 秋季
Web 应用程序编程	2021 春季
网络安全概论	2019 秋季，2020 秋季
工程线性代数	2020 春季

学生指导

池彦廷

上海交通大学本科生 2021.08 – 2022.05

本科毕业设计 – 符号执行工具的测试

现于明尼苏达大学双城分校攻读博士学位

郑志贺

香港中文大学本科生 2018.10 – 2019.04

本科毕业项目 – PHP 程序分析

陈海谦

香港中文大学本科生 2018.10 – 2019.04

本科毕业项目 – PHP 程序分析

其它

软件开源

MdPerfFuzz

检测性能漏洞的模糊测试工具

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

LChecker

分析 PHP 隐性类型转换缺陷

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

XSym

PHP 符号执行系统

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

漏洞发现

性能漏洞

CVE-2021-22217, CVE-2021-39877 等

PHP 隐性类型转换缺陷

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 等