Changhua Luo

Address:
LG103B, Chow Yei Ching Building
The University of Hong Kong
HKSAR, China

Contact:
✉: chluo@cse.cuhk.edu.hk
☎: +86-15071423979
https://chluo1997.github.io/

Education

The Chinese University of Hong Kong Aug 2020 – Jun 2024
Doctor of Philosophy, Computer Science and Engineering
Advisor: Professor Wei Meng

Wuhan University Sept 2015 – Jul 2019
Bachelor of Engineering, Information Security

Professional Experience

Tenure-track Assistent Professor
Wuhan University Jan 2025 – now

Postdoctoral Researcher
The University of Hong Kong Jul 2024 – Jan 2025
Advisor: Professor Chenxiong Qian

Visiting Scholar
Tsinghua University Jun 2023 – Sept 2023
Host: Professor Chao Zhang

Research Assistant
The Chinese University of Hong Kong Feb 2020 – Jul 2020
Advisor: Professor Wei Meng

Research Interests and Impacts

My research interests primarily include program analysis, software security, and web security. Recently, I mainly worked on developing techniques for automatically detecting, exploiting, and patching vulnerabilities in software (C/C++ and Web applications). My works have discovered and fixed numerous critical vulnerabilities in widely used software systems like Objdump, Poppler, and Redis.

Publication

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

[2] **Augmenting PoC Exploit Generation for Node.js Applications using Test Suites**
Changhua Luo, Penghui Li, Wei Meng, and Chao Zhang
Minor revision for CCS 2024.

[3] **IDFuzz: Intelligent Directed Grey-box Fuzzing**
Yiyang Chen, Wenyu Zhu, Changhua Luo, Chao Zhang, Wang Long, and Bingkai Su
Under review.

[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] **Strengthening Supply Chain Security with Fine-grained Safe Patch Identification**
Changhua Luo, Wei Meng, and Shuai Wang
In Proceedings of the 46th International Conference on Software Engineering (ICSE). April 2024.

[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] **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, 20/971=2.06%.

[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 31st Web Conference (WWW). April 2021.

Awards and Honors

ACM CCS 2022 Best Paper Honorable Mention	Nov 2022
CUHK Postgraduate Student Scholarship	Aug 2020 – Jul 2024
Championship in Information Security Triathlon, Central China Division	June 2017
Second Prize in the National College Student Mathematics Competition	2016
Merit Student in Wuhan University	2015 – 2018

Professional Services

External Reviewer

IEEE Symposium on Security and Privacy (Oakland)	2023 – 2024

The ACM Conference on Computer and Communications Security (CCS)	2021 – 2024
The Web Conference (WWW)	2020 – 2022, 2024
The ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2021 – 2022

Teaching Experience

Teaching Assistant

Introduction to Cyber Security	Spring 2022, Spring 2023
Computer and Network Security	Fall 2021
Computer Principles and Java Programming	Spring 2021
Introduction to Computing Using Java	Fall 2020

Invited Talks

Enhancing Application Security: Vulnerability Detection, Validation, and Patching

Huawei HK; Xidian University; Wuhan University; Sun Yat-sen University

Strengthening Supply Chain Security with Fine-grained Safe Patch Identification

ICSE '24

SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration

Oakland '23

TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications

CCS '22

Miscellaneous

Open-Source Software

SelectFuzz

An efficient directed fuzzer using selective path exploration

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

TChecker

A precise static analysis tool for detecting taint style vulnerabilities in PHP applications

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

SPatch

A tool that helps update outdated third-party code in C/C++ software.

`https://github.com/cmd12981/SPatch`

Selected Vulnerability Findings

Injection Vulnerabilities on Web Applications

CVE-2022-35212, CVE-2022-35213

Vulnerabilities Caused by Incomplete Patches

CVE-2022-37768, CVE-2022-37769, CVE-2022-37770, CVE-2022-37047, CVE-2022-37048, CVE-2022-37049, CVE-2022-38349, CVE-2022-38350, CVE-2022-38351, CVE-2022-38352