

XIANG CHEN

📍 Academic Building 3664, Lifts 31/32, Clear Water Bay, Kowloon, Hong Kong

✉ xchenht@cse.ust.hk · 🏠 xchenht.student.ust.hk · 🗣 x14ngch3n · 🆔 0009-0007-0626-6888 · 🏠 Google Scholar

EDUCATION

The Hong Kong University of Science and Technology	2024/08 - now
Ph.D. student in Prism Lab, CSE, supervised by Charles Zhang.	
Shanghai Jiao Tong University	2021/09 - 2024/03
Master degree in Cyber Security, supervised by Yue Wu and Jiaping Gui.	
Thesis: C/C++ system software Static analysis techniques through the lens of Integer Overflow Detection	
Shanghai Jiao Tong University	2017/09 - 2021/06
Bachelor degree in Information Security, selected to the Zhiyuan Honor Program.	
Thesis: Vulnerability Detection and Analysis for Massive Large-scale IoT Devices	
Peking University Summer School	2019/07 - 2019/08

PUBLICATIONS

- **Xiang Chen**. 2024. IntTracer: Sanitization-aware IO2BO Vulnerability Detection across Codebases. In 2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion '24) 📄 🔗
- Tianming Zheng, Haojun Liu, Hang Xu, **Xiang Chen**, Ping Yi, Yue Wu, Few-VulD: A Few-shot learning framework for software vulnerability detection, Computers & Security, 2024 📄

SERVICES

NDSS '26 Artifact Evaluation Committee	2025/07 - 2025/12
CCS '25 Artifact Evaluation Committee	2025/06 - 2025/07
OSDI '25 Artifact Evaluation Committee	2025/04 - 2025/05
PLDI '25 Artifact Evaluation Committee	2025/03 - 2025/04
USENIX Sec '25 Artifact Evaluation Committee	2025/01 - 2025/08
China Computer Federation (CCF) Student Chapter in SJTU, Executive Committee	2022/11 - 2023/12
GeekPwn 2020 volunteer	2020/10

AWARDS

Postgraduate Scholarship (PGS)	2024/09 - now
Shanghai Jiao Tong University Outstanding Graduate (<10%)	2024/03
Rong Chang Leadership Scholarship (<1%)	2021/11 - 2023/11
DEFCON CTF 30 2nd place (played with Katzebin)	2022/08
Zhiyuan Honor Bachelor Degree (Cum Laude , <1%)	2021/06
Shanghai Outstanding Graduate (<5%)	2021/06

TEACHING EXPERIENCE

HKUST Firebird CTF Team Coach 🔗	2025/08 - now
Tutoring reverse engineering and binary exploitation CTF challenges. Organizing CTF contests.	
COMP 3021: Java Programming 🔗	2025/01 - 2025/06
Design course project: an LLM chat client that supports configurable persistence, large-scale functional, and parallel querying.	
IS308: Computer System Security (The first "John Hopcroft" Class) 🔗	2023/02 - 2023/06
Mentoring five labs in binary/web security and cryptography. Hosting a CTF-style final exam.	
NIS7021: Software and System Security 🔗	2022/10 - 2023/01
Design two labs in reverse engineering and binary hardening using LLVM.	

INDUSTRY EXPERIENCE

Hong Kong University of Science and Technology

2024/06 - 2024/08

Research assistant in the Clearblue project. My job is to upgrade the LLVM infrastructure version of the static analyzer.

NIO Inc.

2022/10 - 2023/10

Funding project “decreasing FP and FN rates in static C/C++ program analysis” from Cyber Security Academy Student Innovation Grant Program. The project focuses on using Facebook Infer’s Abstract Interpretation framework and taint analysis technique in detecting Uninitialized Value issues in Linux Kernel.

Huawei Technologies Co., Ltd.

2023/07 - 2023/09

Develop and maintain rules for customized C/C++ static analysis tools and apply them to 5G base station codebases. Research on Large Language Model-assisted program analysis on customized memory management functions.

Shanghai Qizhi Institute

2022/07 - 2022/11

G.O.S.S.I.P Research Group Internship, weekly paper reading and research on (1) automatic program repair using LLVM Instrumentation and the Daikon invariant detector and (2) automatic bug fix for use-after-move issues in C++ 11 using Clang-Tidy.

Shanghai Feysh Technology Co.,Ltd

2021/07 - 2021/09

Manually review more than 4000 analysis results of ClangStaticAnalyzer on Juliet C/C++ Test Suite. Implement four checkers for SEI CERT C Coding Standard.

OPEN-SOURCE CONTRIBUTIONS

Open Source Promotion Plan (openEuler)

2023/07 - 2023/09



Enhance LLVM InstCombine pass with a peephole optimization, which can eliminate `abs()` in ternary expressions like: `x>y? abs(x-y+1):0` and combine the original if-else-branch to linear CFG using the AArch64 `csinc` instruction.

SJTUBeamer

2021/04 - 2021/11

The Shanghai Jiao Tong University official \LaTeX beamer template with more than 600 stars.

TALKS

- **Xiang Chen**, Siqi Ma. 2023. Custom Memory Functions Demystified: A tutorial of memory corruption detection using Goshawk. In ACM ASIA Conference on Computer and Communications Security (**ASIA CCS '23**) 
- **Xiang Chen**. 2023. C/C++ static analysis with LLVM compiler infrastructure. Voice of Information Security-Young 

SKILLS

- Programming Languages: C/C++ \geq Python $>$ Java, Rust, OCaml
- Development Toolchains: VSCode, Vim, CMake, LLVM/Clang, GDB, Docker, Git
- Capture-The-Flag: IDA/Binja, Pwntools, Angr, Wireshark, Sage