

# XIANG CHEN

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

✉ x14ngch3n@gmail.com / xchenht@cse.ust.hk · 🌐 xchenht.student.ust.hk · 📞 x14ngch3n · 📄 0009-0007-0626-6888

## EDUCATION

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

## INDUSTRY EXPERIENCE

<b>Hong Kong University of Science and Technology</b> Research assistant in the <a href="#">Clearblue</a> project. My job is to port the analysis framework to modern LLVM infrastructures.	2024/06 - 2024/08
<b>NIO Inc.</b> 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 <a href="#">Facebook Infer</a> ’s Abstract Interpretation framework and taint analysis technique in detecting Uninitialized Value issues in Linux Kernel.	2022/10 - 2023/10
<b>Huawei Technologies Co., Ltd.</b> Develop and maintain rules for enterprise-domestic 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.	2023/07 - 2023/09
<b>Shanghai Qizhi Institute</b> <a href="#">G.O.S.S.I.P</a> Research Internship, doing weekly paper reading and research on (1) automatic program repair using <a href="#">LLVM Pass</a> and <a href="#">Daikon invariant detector</a> and (2) automatic bug fix for use-after-move issues in C++ 11 using <a href="#">Clang-Tidy</a> .	2022/07 - 2022/11
<b>Shanghai Feysh Technology Co.,Ltd</b> Manually review more than 4000 analysis results of <a href="#">ClangStaticAnalyzer</a> performed on Juliet C/C++ Test Suite. Implement four ClangStaticAnalyzer checkers for <a href="#">SEI CERT C Coding Standard</a> .	2021/07 - 2021/09

## TEACHING EXPERIENCE

<b>IS308: Computer System Security (The 1st “John Hopcroft” Class)</b> Provide mentorship on five labs in binary/web security and cryptography. Host a Jeopardy-style final exam.	2023/02 - 2023/06
<b>NIS7021: Software and System Security</b> 🌐 Design two labs in reverse engineering, and dynamic instrumentation.	2022/10 - 2023/01

## OPEN-SOURCE CONTRIBUTIONS



<b>Open Source Promotion Plan (openEuler)</b> 🌐 📄 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.	2023/07 - 2023/09
<b>SJTUBeamer</b> 🌐 Shanghai Jiao Tong University official L <sup>A</sup> T <sub>E</sub> X beamer template, gained more than 500 stars.	2021/04 - 2021/11

## 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 📄

## TALKS

---

- **Xiang Chen**, Siqu 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 

## AWARDS

---

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

## SERVICES

---

Executive Committee Member of China Computer Federation (CCF) <u>Student Chapter</u> in SJTU	2022/11 - 2023/12
GeekPwn volunteer	2019/10

## SKILLS

---

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