

# XIANG CHEN

800 Dongchuan RD. Minhang District, Shanghai, China

✉ [cascades@sjtu.edu.cn](mailto:cascades@sjtu.edu.cn) · 🌐 [xiangchen.xyz](http://xiangchen.xyz) · 🔄 [cascades-sjtu](https://github.com/cascades-sjtu) · in [cascades](#) · ID 0009-0007-0626-6888

## EDUCATION

<b>Shanghai Jiao Tong University</b>	2021/09 - now
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	
<b>Shanghai Jiao Tong University</b>	2017/09 - 2021/06
Bachelor degree in Information Security, <a href="#">Zhiyuan Honor Program</a>	
Thesis: Vulnerability Detection and Analysis for Massive Large-scale IoT Devices	
<b>Peking University Summer School</b>	2019/07 - 2019/08

## INDUSTRY EXPERIENCE

<b>NIO Inc.</b>	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 <a href="#">Facebook Infer</a> ’s Abstract Interpretation framework and taint analysis technique in detecting Uninitialized Value issues in Linux Kernel.	
<b>Huawei Technologies Co., Ltd.</b>	2023/07 - 2023/09
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.	
<b>Shanghai Qizhi Institute</b>	2022/07 - 2022/11
<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> .	
<b>Shanghai Feysh Technology Co.,Ltd</b>	2021/07 - 2021/09
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> .	


## TEACHING EXPERIENCE

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



## OPEN-SOURCE CONTRIBUTIONS

<b>Open Source Promotion Plan (openEuler)</b> 🔄 🌐	2023/07 - 2023/09
Enhance LLVM InstCombine pass with a peephole optimization, which can eliminate <code>abs()</code> in ternary expressions like: <code>x&gt;y? abs(x-y+1):0</code> and combine the original if-else-branch to linear CFG using the AArch64 <code>csinc</code> instruction.	
<b>SJTUBeamer</b> 🔄	2021/04 - 2021/11
Shanghai Jiao Tong University official L <sup>A</sup> T <sub>E</sub> X beamer template, gained more than 500 stars.	

## 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)  

## 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](#) 

## 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) <a href="#">Student Chapter</a> in SJTU	2022/11 - 2023/12
GeekPwn volunteer	2019/10

## SKILLS

---

- Programming Languages: C/C++  $\geq$  Python > Rust > OCaml
- Develop Environment: Debian, VSCode, Vim, GDB/LLDB
- Capture-The-Flag: Binary Ninja, Angr, Pwntools, Wireshark, Sage