Yuxuan Sun

South Kensington, London | (044) 07729-462072 | sunyxedu@gmail.com

RESEARCH INTERESTS

I am broadly interested in Artificial Intelligence for Security, computer security and Competitive Game AI. My current research focuses on automated vulnerability discovery through static analysis and efficient fuzzing, and on designing deep reinforcement learning agents for competitive strategy games.

EDUCATION

Imperial College London   2024-2027
*BEng in Computing (expected **First Class Honor**, 84.01/70)*

AWARDS

*USACO (USA Computing Olympiad) Platinum (Highest Division) **Rank 32 in the World** (2023 US OPEN CONTEST)*
*Imperial College London Arm/C Group Project Awards 24/25 **Best Overall Project***
*Codeforces Username: sunyx, **Title: Master, Rating: 2216***
*Binary Prediction of Poisonous Mushrooms (Kaggle) **Rank 95/2422***

EXPERIENCE

Intern Teammate   **r3kapig**   2025.12 – Present
- Competed in LA CTF 2026 with R3kapig; placed 5th/955 teams.
- Member of R3kapig, ranked #1 overall on CTFtime in 2025.

Researcher, *Shenzhen*, Guangdong   **Tencent Xuanwu Lab**   2025.5 - Present
- Designed and implemented a **high-recall, cost-efficient semantic code retrieval framework** for this automated vulnerability detection system at **Tencent Xuanwu Lab**. Discovered a critical vulnerability (CVE-2025-57801) using this system; with this framework, three additional critical vulnerabilities and 20+ lower-severity were identified.
- Our experiments show that across multi-language repositories, even at 25% lower cost than embedding-only baselines, it attains about 1.5× higher recall (about 90% vs. about 60%). It also outperforms industrial AI coding assistants (Cursor, Claude Code) in function-level code search tasks by over **30× in recall** and excels the SOTA LocAgent tool by over **6x**.
- Accepted by **Black Hat Asia 2026 Call for Tools**; awarded £3,250 in funding from Imperial College London.
- Available on Github and NVD Database.

Research Assistant, *Shanghai*   **Shanghai Jiao Tong University**   2025.7 - Present
- Designed a novel **multi-target direct fuzzing** method that can significantly speed up target coverage in the **G.O.S.S.I.P** (Group of Software Security in Progress), under the supervision of Prof. Juanru Li and Dr. Yunlong Lyu. Currently designing an LLM-assisted Static Analysis Tool.
- Reviewed a **TrustCom** conference paper in the field of **AI Security**. Evaluated its contribution and methodological rigor and provided detailed feedback.

Research Assistant, *London*, UK   **Imperial College London**   2025.1 – 2025.7
- Constructed **Reinforcement Learning Based Fuzzing algorithm** using Contextual Combinatorial Volatile Multi-Armed Bandit with Adaptive Discretization in the **Security and Machine Learning Lab** under the mentorship of Prof. Sergio and Dr. Myles.

Researcher, *Shenzhen*, Guangdong   **Tencent**   2023.6 - 2024.1

- Researched **cryptographic accumulators** in the Tencent Aspiring Explorers in Science program under Prof. Yu Yu and Prof. Yuncong Hu (SJTU). Developed a novel **transparency system** integrating Chunking and Prefix Merkle Tree. Authored a research paper titled [Advanced Transparency System](#), which was cited by **Intel Labs**.

Others

- Participated in the **cryptography summer camp** hosted by Shanghai Qi Zhi Institute and Shanghai Jiao Tong University in 2024.7.
- Mentored Chinese National Olympiad in Informatics **Gold medalists** in the Tencent TSpark Program on **automated offensive security** research, where we developed an agent that automatically exploited known CVEs for penetration testing in 2025.8.

PROJECTS

AlphaGen

- Developed a bot for *generals.io* that collects and preprocesses game data, trains via **Imitation Learning**, and refines with **Offline Policy Improvement** in **Reinforcement Learning**; implemented in a parameter-efficient manner using Tiny Recursive Model. Currently collaborating with MIT student Steven Chen.

Emulator and Assembler

- Developed **B-Arm Assembler (BAS)**, a full-featured ARM assembler, and **B-Emulator (BEMU)**, a C-based high-performance emulator with UART, timer, and HVS support. Led algorithm design, including **priority queue integration**, **prefix tree integration** and **RL-based cache replacement policy** for adaptive TLB optimization, etc. Awarded **Best Overall Project** at Imperial College London.

Image super-resolution

- Implemented **Super-Revolution Generative Adversarial Network** for a 4x image super-resolution task, generating high-resolution images from low-resolution inputs. Utilized two loss functions: **content loss and adversarial loss**. Applied MSE loss in both image pixel and feature spaces for content loss, and integrated adversarial loss to enhance image realism.

Additional Projects

- Explored various projects spanning **traditional ML** and **NLP** (e.g., translator, legal QA system, image captioning) and applied AI systems. Full portfolio available on [GitHub](#).

SKILLS AND INTERESTS

Classic Machine Learning Models: Proficient in regression models, Bayesian learning, decision trees and pruning, KNN, ensemble learning, and support vector machines.

Deep Learning Models: Experienced with multi-layer perceptron, convolutional neural networks, recurrent neural networks, transformers, and deep generative models.

Computer Vision: Skilled in using MMDetection and Vision Transformer.

Natural Language Processing: Proficient in identifying and applying models from Hugging Face for various applications.

Programming: Proficient in **Python** for machine learning and **C++** for algorithms. Skilled in **Git-based version control**.

Interests: Scientific Research, Piano (Level 10, CMA Piano Grading Examination), Badminton (High School Varsity Team), Go (5-Dan), and strategy games (Ultimate Champion in Clash Royale, top-20 in generals.io)