June Lim

jl2658@cam.ac.uk • +65 90893031 • LinkedIn • Blog

Education

University of Cambridge — Cambridge, UK
Computer Science, BA (Hons), St Catharine's College — Oct 2026 – Jun 2029 (expected)

National University of Singapore — Singapore
Non-Graduating Programme, two semesters each of Computer Science and Mathematics — 2021 – 2023
CS2106 Operating Systems (A-), CS2100 Computer Organisation (A-), MA2002 Calculus (A+), MA2001 Linear Algebra I (A)

NUS High School of Math and Science — Singapore
Honours in Computer Science and Mathematics, Majors in Physics and Chemistry (GPA 5.0/5.0) — 2018 – 2023
Best in Subject: English Language (2020 – 2023), Art (2019 – 2020); Outstanding Contribution (Service) Award, 2022

Experience

Ensign Infosecurity — Singapore
Malware & Vulnerability Research Intern — May 2026 – Aug 2026

- Led end-to-end vulnerability research on an embedded wireless platform: firmware extraction and decryption, firmware and proprietary protocol reverse engineering, and Qiling-based emulation to reproduce vulnerabilities.
- Emulated a trusted execution environment (TEE) under QEMU and exploited it to break the cryptographic root of trust of a commercial device.
- Researched commercial packers (unpacking, virtual machine and tamper-detection evasion, devirtualisation), contributing to the firm's malware analysis workflows. Further details are withheld under a non-disclosure agreement.

Alliance DAO — Remote
Blockchain Intern — May 2024 – Dec 2024

- Wrote technical due diligence on 19 protocols, including DePIN and DeAI projects (e.g. Akash, io.net, Ritual, Nillion): reverse engineered vague designs from on-chain contracts and assessed trust assumptions and token incentives.
- Executed a testnet Sybil attack on Crynux's GPU network, in which unverifiable VRAM claims captured high-value tasks and earned payouts without inference, at the cost of staked tokens only; found the documented QoS logic to be largely unimplemented.
- Analysed hardware-rooted trust in decentralised compute (TEE attestation on SGX, SEV and TrustZone; GPU TEE limitations) and published the analysis publicly.

ODA Capital — Singapore
Blockchain Intern — Oct 2023 – Dec 2023

- Designed S&P-style growth and value crypto indices from bespoke multi-chain on-chain data (Ethereum L2s, Solana), plus a regime-switching strategy rotating between them on volatility and open interest signals.
- Backtested the strategy and analysed inter-bucket correlations; stress-tested it with a stationary block bootstrap (Politis–Romano) on stationarity-tested returns (NumPy, Pandas, `arch`).
- Handed the project over to the team for continued development after the internship.

Research

National University of Singapore — *Silver Award, Singapore Science and Engineering Fair 2023*
Interpreting and Evading Visualization-Based Deep Learning Malware Classifiers — 2022 – 2023

- Designed a black-box, label-only evasion attack that injects opaque predicates and bogus control flow via a patched Obfuscator-LLVM: 100% evasion of detected samples that compiled (122/187), under 0.5% mean file-size increase and about four queries on average, with behaviour verified in Cuckoo Sandbox.
- Mapped CNN attention (GradCAM, contour analysis) back to PE sections and validated it by decompiling the flagged regions in Ghidra, showing that the model keys on padding and headers rather than malicious code; benchmarked six existing attacks and concluded that visualisation-based classifiers are neither interpretable nor robust.

Singapore Institute of Technology — Singapore
A Novel Feature Vector for AI-Assisted Windows Malware Detection *(co-authored)* — 2022 – 2023

- Co-designed an order-independent, fixed-size (27,090-dimension) feature vector from Cuckoo Sandbox API traces, encoding API names, arguments and return values with signed feature hashing, hierarchical path and URL decomposition, and log-scaled numerics; focused on interpreting and shaping the vector's components.
- Contributed to a detector reaching 97.4% accuracy and a 2.95% false negative rate (five-fold cross-validation, 14,860 samples), against 96.3–96.4% and 3.7–4.9% for two published baselines.
- Published at IEEE DASC 2023 (as Justin Lim), *doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361451*

Awards and Competitions

Mandiant FLARE-On 12 — 10th Place among Singapore finishers (2025)
DSTA CDDC Brainhack CTF — 1st Place, four consecutive years (2022 – 2025); 4,500+ student participants
NUS Greyhats GreyCTF; Singapore Govtech AI CTF — 1st Place, two consecutive years (2024 – 2025)
NUS Hack&Roll Hackathon — Overall Top 9 in 2024, 2025 and 2026; 2026 project: ESP32 badge using ESP-NOW and BLE for proximity-based interest matching
SCS Splash Awards — Overall Winner (2022) for a microplastics movement prediction model (GRU on HYCOM ocean data)

Leadership and Organising

Centre for Nurturing Computing Excellence (CENCE) Singapore
ICO Team Leader and Trainer; NCO Secretary and Trainer Nov 2025 – Jul 2026

- Led Team Singapore (four students, selected through the National Cybersecurity Olympiad, NCO) at the International Cybersecurity Olympiad (ICO) 2026 in Tunisia, a 20-country field, achieving one gold, two silver and one bronze medal; delivered three months of training (reverse engineering, forensics and web3, with further trainers for binary exploitation, web and cryptography) and managed logistics, strategy and challenge review on site.
- Coordinated the challenge setters, the core team and external communications as NCO Secretary and Scientific Committee member for a two-round national competition (73 finalists); authored the reverse engineering syllabus, vetted the committee's syllabus input and prepared technical guides.
- Set challenges including simplified firmware reverse engineering and a VEH-based virtual machine simulating an anticheat; taught the reverse engineering and binary exploitation sessions (Ghidra, gdb, pwntools) within a month-long national training workshop run with other trainers.

BlahajCTF Singapore
Head of Training, Head of Challenge Setting; Advisor 2023 – Present

- Set challenges in 2023, then oversaw challenge setting in 2024 – 2025 for Singapore's largest pre-university Capture the Flag (CTF) competition (1,000+ participants across 70 schools): led 16 setters on 70+ challenges, with responsibility for quality control, difficulty grading, playtesting and infrastructure, and wrote much of the reverse engineering, binary exploitation and forensics content.
- Planned and ran the first on-site five-day workshop (50 students, seven trainers); wrote and presented the introductory Linux and reverse engineering materials and vetted all other trainers' content.
- Contributed, in an advisory role in 2026, to securing partnerships with the Cyber Security Agency of Singapore, forming the four-week Intermediate Youth Cyber Exploration Programme (I.YCEP; primary trainer for malware analysis and reverse engineering), and with NUS, under which BlahajCTF will run NCO training; continue to write reverse engineering materials.

Singapore Armed Forces, HQ 9th Singapore Division Singapore
Security, Intelligence and Public Affairs Apr 2024 – Apr 2026

- Led the division's event coverage and public affairs team (up to 14 personnel across photo, video and social media), attaining the rank of Corporal First Class.
- Ran coverage of the ASEAN Armies Rifle Meet 2025 (all ASEAN member states, 420+ shooters) and the ASEAN Chiefs of Army Multilateral Meeting 2025: managed the events' social media presence, planned manpower and coverage schedules with senior commanders, and produced photo and video content; photographs appeared in press releases and official state media, and the work earned letters of appreciation.

Skills & Interests

Languages: C/C++, Python, Verilog, Assembly (x86-64, ARM, MIPS), Solidity, SQL, Java, C#, Mandarin Chinese
Skills: Reverse Engineering (x86-64, ARM, firmware), Binary Exploitation, Embedded Systems, PCB Design (KiCad), FPGA Development, Symbolic Execution and Constraint Solving, Smart Contract Analysis, Time-Series Analysis and Backtesting
Tools and Libraries: Ghidra, x64dbg, gdb, QEMU, Qiling Framework, angr, Z3, KiCad, Foundry, SageMath, NumPy, Pandas, `arch`, PyTorch; some experience with IDA and Triton DBA
Hardware Projects

- Designed custom STM32 and ESP32 boards in KiCad, with Arduino-compatible bootloaders, for stage prop lighting control; multiple units have been in use for about five years.
- Implemented cryptographic and hashing algorithms in Verilog on the GreyCTF 2025 FPGA badge (Lattice ECP5) and solved all of its challenges, including Verilog reverse engineering and race-condition exploitation; currently learning Hardcaml.

Interests: Hardware Hacking (UART, SPI flash), Formal Methods, Music Production, Photography, Video Editing