Matthew Cai

(561) 777-6131 · matthew.cai.official@gmail.com · github.com/nightxade

Education

University of California, Berkeley Expected May 2027
Bachelor of Science, Electrical Engineering and Computer Science GPA: 4.00/4.00

Undergrad Coursework: SICP, DSA, Machine Structures, Circuits, Computer Architecture, Computer Security, Compilers, OS, Advanced Algorithms, Databases, Machine Learning, Reinforcement Learning, Linear Algebra, Discrete Math, Calculus I/II/III, Abstract Algebra

Graduate Coursework: Computer Architecture (audit), Computer Security, Performance Optimization

Leadership: Berke1337 Cybersecurity Club, Quantum Computing at Berkeley (QCB), Eta Kappa Nu (HKN)

Experience

Meta | *(Incoming) Offensive Security Engineering Intern* June 2026 – August 2026
Meta | *Software Engineering (Network Security) Intern* May 2025 – August 2025
· Redesigned concurrency and pipelining for validation of network access control list (ACL) generation, reducing runtime by **99%**
· Devised a scalable, custom lexer to automate generating **6,000+** lines of AST grammars from Apache Thrift interfaces
· Replaced quadratic-complexity IP prefix matching with radix trees in TACACS+ validator, cutting runtime from **2.5 min to 1 sec**
· Developed CLI to enhance and debug ACL generation library capirca by leveraging real-time OLAP databases and entity graphs

MITRE | *Reverse Engineering Intern* June 2024 – August 2024
· Assessed the performance of Ghidra BSim, an open-source binary differential analysis tool, across diverse architectures and OSS
· Integrated Ghidra's Python API into a headless CLI with parallelized BSim database queries and statistical results for engineers
· Reverse engineered firmware vulnerabilities and exploited side channels in an embedded ARM device for a CTF, tied for **1st place**

Research

Graduate Computer Security Research at UC Berkeley (CS 261) | *Security Researcher [1]* February 2026 – May 2026
· Designed the *first* LLM-based decompiler for **Go source recovery**, integrating Gemini, Ghidra, GoReSym, and custom Go heuristics
· Curated *first* Go decompiler benchmark of **1.8M functions** extracted from 1600 unique binaries across **120 OSS** projects
· Introduced novel evaluation metrics: CodeBLEU, LLM-as-a-judge, and syntax validation scoring weighted by code and AST complexity

Security Group at UC Berkeley (D. Song) | *Security Researcher [2]* January 2025 – December 2025
· Engineered sandboxed LLM-agent MCP for automated PoC generation across **1,500 vulnerabilities** in **200 OSS** projects
· Discovered **15 zero-days** during benchmarking, leading to CVE-2025-7797, CVE-2025-7464, and CVE-2025-7462
· Architected framework to evaluate LLM agents on generating ROP chains for real-world binaries, e.g. GNU Coreutils

Industrial Cyber-Physical Systems (iCyPhy) at UC Berkeley | *Systems Researcher [3]* October 2025 – December 2025
· Extended the GameTime algorithm for worst-case execution time (WCET) analysis of the Lingua Franca polyglot language
· Programmed 3 FRDM-K64F microcontrollers with Zephyr RTOS to demo WCET analysis on a real embedded, distributed system

Publications

[1] ComeBack: Assessing LLM Decompilation for Go Preprint, 2026
Matthew Cai, Jonah Bedouch

[2] CyberGym: Evaluating AI Agents' Real-World Cybersecurity Capabilities at Scale ICLR Oral 2026
Zhun Wang, Tianneng Shi, Jingxuan He, Matthew Cai, Jialin Zhang, Dawn Song

[3] Formally Verified WCET Analysis of Distributed Lingua Franca Systems via GameTime Preprint, 2025
Zeynep Guzey, Anagha Ananth, Matthew Cai, Jiaquan Li, Shaokai Lin

Activities and Projects

Cybersecurity Capture the Flag | *Cryptography, Vulnerability Researcher* September 2023 – Present
· Member of **top 3** US CTF Team, *Squid Proxy Lovers*: 3rd at Google 2025, 2nd at idek 2025, 2nd at Dice Qual 2025, 5th at Lake 2025
· Skills: symmetric cryptanalysis; lattice attacks; stack/heap userspace ELF exploitation; microarchitecture exploitation

Berke1337 Cybersecurity Club | *Officer* August 2024 – Present
· Helped build custom homelab for network defense training and created custom pwn challenges for demonstrations and practice
· Organized training and recruitment for the club CTF team; taught members software exploitation, fuzzing, cryptography, etc.

Google × Flare Verifiable AI Hackathon | *3rd Place* March 2025
American Invitational Mathematics Examination | *5-time qualifier, highest score of 7* 2019 – 2024

Skills

Languages: C/C++, Python, SageMath, Go, Rust, OCaml, Lisp, Java, SQL, x86, ARM, RISC-V, Bash, Chisel, LaTeX
Tools: Git/Mercurial, Docker, Make, GDB/pwndbg, Wireshark, Ghidra/Binary Ninja/IDA, VirtualBox
Operating Systems: Windows, Linux (Kali, Debian, Ubuntu, Arch)
Research Interests: security, microarchitecture, performance, databases, distributed systems, AI safety, ML systems