

Luoxi Meng

📍 San Diego, CA 92037 📞 +1 (734) 934-3212 ✉ lumeng@ucsd.edu 🌐 rosie-m.github.io

EDUCATION

University of California San Diego , San Diego, CA PhD, Computer Science & Engineering	09/2023 – 06/2028 (Expected)
University of Michigan , Ann Arbor, MI Master of Science, Computer Science & Engineering	08/2021 – 04/2023
Simon Fraser University , Burnaby, BC, Canada Bachelor of Science (with Distinction) Computing Science, Dual Degree Program with Zhejiang University	09/2019 – 08/2021
Zhejiang University , Hangzhou, China Bachelor of Engineering Computer Science and Technology, Dual Degree Program with Simon Fraser University	09/2017 – 06/2021

PEER-REVIEWED PUBLICATIONS

Stateful Least Privilege Authorization for the Cloud

Leo Cao*, Luoxi Meng*, Deian Stefan, Earlence Fernandes (*Equal contribution)
USENIX Security 2024 (Acceptance rate = 17.60%)

Perseus: Reducing Energy Bloat in Large Model Training

Jae-Won Chung, Yile Gu, Insu Jang, Luoxi Meng, Nikhil Bansal, Mosharaf Chowdhury
ACM SOSP 2024 (Acceptance rate = 17.34%)

Chasing Low-Carbon Electricity for Practical and Sustainable DNN Training

Zhenning Yang, Luoxi Meng, Jae-Won Chung, Mosharaf Chowdhury
ICLR Workshop: Tackling Climate Change with Machine Learning 2023

PREPRINTS

ceLLMate: Sandboxing Browser AI Agents

Luoxi Meng, Henry Feng, Ilia Shumailov, Earlence Fernandes
<https://arxiv.org/abs/2512.12594>

InferPriv: Evaluating Inferential Privacy Leakage in LLM Assistants

Pengrun Huang*, Yiwei Fu*, Luoxi Meng, Kamalika Chaudhuri (*Equal contribution)
<https://arxiv.org/abs/2610.34640>

INDUSTRIAL EXPERIENCE

SystemsResearch@Google (SRG)

Sunnyvale, CA

Student Researcher

06/2026 – 09/2026

- Independently scoped a new research problem: analyzed how browser agents break the web's core security boundary and pinned down its root causes.
- Designed and built an information flow control (IFC) system in Python that protects the confidentiality and integrity of user data. It is enforced as a proxy at the Chrome DevTools Protocol (CDP) boundary.
- Led the research end-to-end, from threat modeling and policy formalization to system architecture design, coordinating with a team of five collaborators across security and systems.

SpeedLine Solutions Inc.

Abbotsford, BC, Canada

Software Developer Intern

01/2021 – 04/2021

- Performed end-to-end testing on the shopping cart component; identified and fixed the inconsistency between frontend data presentation and backend data store.
- Deployed Google Tag Manager (GTM) to the company's online ordering website and created custom tags and triggers for eCommerce measurement and analytics, which cover 90% of user activities.

Morgan Stanley, Algorithmic Trading Infrastructure

Shanghai, China

Project Intern

07/2019 – 08/2019

- Designed and implemented an application that tracks real-time trading data and visualizes it in a GUI; deployed it to the internal platform to improve the efficiency of online testing and debugging.
- Presented an introduction to the new application at a global team meeting.

RESEARCH EXPERIENCE**ceLLMate: Sandboxing Browser AI Agents**

Security and Cryptography @ UC San Diego

Advised by Prof. Earlene Fernandes

05/2025 – 02/2026

- Led the design and implementation of *ceLLMate*, the first sandboxing framework that enforces least privilege for browser-use agents (BUAs).
- Addressed the semantic gap in BUAs by introducing request-level mediation and agent sitemaps for stable, complete, and context-aware policy enforcement.
- Validated *ceLLMate* in a GitLab case study using the WASP benchmark, prevented 100% of prompt injection attacks while preserving intended functionality, with 0.215% latency overhead.

Stateful Least Privilege Authorization for the Cloud

Security and Cryptography @ UC San Diego

Advised by Prof. Earlene Fernandes

09/2023 – 08/2024

- Identified the overprivilege of OAuth tokens in the cloud through real-world examples.
- Designed *StatefulAuth*, a stateful least privilege authorization framework that enables a new class of authorization policies, integrated it with OAuth 2.0, and demonstrated it with case studies on three real-world apps.

Energy-Efficient Systems for Large Model Training

SymbioticLab @ UMich

Advised by Prof. Mosharaf Chowdhury

08/2022 – 05/2023

- Extended *Zeus*, an energy optimization framework for Deep Neural Network (DNN) training, from single-GPU to single-node multi-GPU that supports efficient data parallel training.
- Won 2nd Best Overall Solution in Carbon Hack 22 by creating *Carbon-Aware Zeus*, which reduces the total carbon footprint in DNN training with almost no training time increase.
- Co-designed *Perseus*, conducted experiments and produced main evaluation figures.

Automated Formal Verification of Efficient Implementations

Distributed and Operating Systems @ UMich

Advised by Prof. Manos Kapritsos

04/2022 – 10/2022

- Co-designed *Cruiser*, an automated approach that produces high-performance, fully verified distributed system implementations.
- Implemented and formally verified three distributed protocols based on *Cruiser*.

TECHNICAL SKILLS**Programming Languages:** Python, C/C++, Java, JavaScript/TypeScript, Go, CUDA, Dafny, Shell**Libraries/Frameworks:** Pandas, NumPy, PyTorch, Matplotlib, FastAPI, Pydantic, SQLAlchemy, Node.js**Tools:** Docker, Kubernetes, Clang/LLVM, GCC