

Songyang Peng

Website ✉ s_peng@ucsb.edu 🌐 alexps9 📄 LinkedIn 🎓 Scholar

Work on machine learning systems, agentic AI, and AI system security.



Education

University of California, Santa Barbara, CA, United States

Sept.2026–Present

Ph.D. in Computer Science, Advisor: [Wenbo Guo](#)

Fudan University, Shanghai, China

Sept.2023–June.2026

M.S. in Computer Science, Advisors: [Jiarun Dai](#), [Yuan Zhang](#)

Tianjin University, Tianjin, China

Sept.2019–June.2023

B.S. in Computer Science ([Qiushi Class](#)), Advisor: [Yu Mei](#)

Internship Experience

ByteDance Ark

Apr.2025–Oct.2025

LLM Inference Engineer Intern, Mentor: [Meng Wang](#)

- LLM serving: contributed to xLLM, ByteDance's internal LLM serving engine.
- Agent infrastructure: contributed to [verl](#) [🌐 23,931 ⭐].

Tencent IEG

Dec.2024–Mar.2025

AI Research Intern, Game & Engine Intelligence

- Selected for the Game-Engine Computer Graphics Practice Elite Talent Program.

Preprint

* indicates equal contribution

- Jiaqi Luo*, **Songyang Peng***, Jiarun Dai, Zhile Chen, Zhuoxiang Shen, Geng Hong, Xudong Pan, Yuan Zhang, Min Yang, *AgentGuard: An Attribute-Based Access Control Framework for Tool-Use LLM-Based Agent*. Preprint.
- **Songyang Peng**, Ruoyu Fang, Xinfeng Yuan, Haidong Zheng, Zesong Yang, Ruijie Wang, Hongze Mi, Yilan Guo, Linxiao Zhou, *Amour: A Latent Dynamical System for Controllable and Stateful Social Interaction in LLMs*, **KDD 2026 Workshop on SciSoc Agents & LLMs (Oral)**. Manuscript under review.
- Yuzhou Nie, Weifang Zhang, Zach Xu, **Songyang Peng**, Yuheng Tang, Minzhou Pan, Bo Li, Dawn Song, Ce Zhang, Wenbo Guo, *HiMA: Efficient Hybrid Model Serving for Agentic Systems*, **ICML 2026 Workshop on Agents in the Wild**.

Publications

- **Songyang Peng**, Jiarun Dai, Yanghao Lv, Jiaqi Luo, Zongan Huang, Yuan Zhang, Min Yang, *BHUNTER: Generating Blind-Spot Driving Scenarios for Robustness Testing of Perception Systems*, **ACM TOSEM, 2026**.
- Zongan Huang, Jiarun Dai, Jiaqi Luo, Qifan Xiao, **Songyang Peng**, Xudong Pan, Yuan Zhang, Min Yang, *Facilitating Logical Flaw Detection for Autonomous Driving Systems through LLM-Empowered Oracle Generation*, **IEEE TIFS, 2026**.
- Hongze Mi, Yibo Feng, WenJie Lu, Song Cao, Jinyuan Li, Yanming Li, Xuelin Zhang, Haotian Luo, **Songyang Peng**, He Cui, Tengfei Tian, Jun Fang, Hua Chai, Naiqiang Tan, *Darwinian Memory: A Training-Free Self-Regulating Memory System for GUI Agent Evolution*, **ICML 2026**.
- Jiaqi Luo, Jiarun Dai, Fengyu Liu, **Songyang Peng**, Youkun Shi, Tong Bu, Geng Hong, Xudong Pan, Yuan Zhang, *Autonomy Comes with Costs: Detecting Denial-of-Service Vulnerabilities Caused by Resource Abusing in LLM-based Agents*, **USENIX Security 2026**.
- Tong Bu, Jiarun Dai, Jiaqi Luo, **Songyang Peng**, Zongan Huang, Min Yang, *APSFUZZ: Simulation-Based Fuzzing Testing for Automated Parking Systems*, **USENIX VehicleSec 2025**.

Open Source Contributions

- **AgentGuard** [🌐 150 ⭐]: Co-first author of an attribute-based access-control framework for tool-use LLM agents. [Website](#).
- **BHUNTER** [🌐 21 ⭐]: Open-sourced the artifact for blind-spot driving-scenario generation. [Project](#).
- **Mooncake** [🌐 6,834 ⭐]: Hardened the shared-memory transport backing-file and mapping lifecycle ([PR #3145](#),

merged).

Awards

Outstanding Graduate, Tianjin University	2023
Mathematical Contest in Modeling (MCM), Honorable Mention	2021
1st Prize, China Collegiate Intelligent Robot Innovation Competition	2020

Professional Service

Reviewer, ACL	2027
Workshop Reviewer, Agents in the Wild (ICML)	May 2026

Skills

Proficient: Python, C/C++, PyTorch, LLM serving ([SGLang](#), [vLLM](#)), Git/Linux
Familiar: [FlashInfer](#), LaTeX