Elisa Tsai (Wentao Cai)

Department of Computer Science, 2260 Hayward Street, Ann Arbor, MI, 48105, USA
Email: eltsai@umich.edu Homepage: eltsai.github.io

INTERESTS

Web security; machine learning for security; machine learning efficiency.

My research focuses on building pragmatic, GenAI-powered systems for web security. I also design algorithms for data efficiency and inference efficiency for vision and large language models.

EDUCATION

University of Michigan, Ann Arbor 2020 - present
Ph.D. Candidate, Computer Science
Advisor: Prof. Atul Prakash

Univeristy of Science and Technology of China (USTC) 2020
B.S., Computer Science and Technology

WORK EXPERIENCE

Google Summer of Code - Honeynet RiotPot June. 2023 - Aug. 2023
Software Engineer
I contributed to Riotpot, an IoT honeypot under the Honeynet project, implementing multiple protocol emulation to increase the honeypot's relevance to real-world attacks.

PUBLICATIONS

1. Label-Free Coreset Selection with Proxy Training Dynamics
   Haizhong Zheng (co-lead), Elisa Tsai (co-lead), Yifu Lu, Jiachen Sun, Brian R. Bartoldson, Bhavya Kailkhura, Atul Prakash
   *To appear, **ICLR (The International Conference on Learning Representations) 2025***
2. Harmful Terms and Where to Find Them: Measuring and Modeling Unfavorable Financial Terms and Conditions in Shopping Websites at Scale
   Elisa Tsai, Neal Mangaokar, Boyuan Zheng, Haizhong Zheng, Atul Prakash
   *To appear, **WWW (The Web Conference) 2025** (Oral)*
3. Modeling and Detecting Internet Censorship Events
   Elisa Tsai, Ram Sundara Raman, Atul Prakash, Roya Ensafi
   NDSS (Network and Distributed System Security Symposium) 2024
4. CERTainty: Detecting DNS Manipulation at Scale using TLS Certificates
   Elisa Tsai, Deepak Kumar, Ram Sundara Raman, Gavin Li, Yael Eiger, Roya Ensafi
   PETS (Privacy Enhancing Technologies Symposium) 2023
5. DOLMA: Securing Speculation with the Principle of Transient Non-Observability
   Kevin Loughlin, Ian Neal, Jiacheng Ma, Elisa Tsai, Ofir Weisse, Satish Narayanasamy, Baris Kasikci
   USENIX Security 2021
6. Terms of Deception: Exposing Obscured Financial Obligations in Online Agreements with Deep Learning
   Elisa Tsai, Anoop Singhal, Atul Prakash
   DLSP (Deep Learning Security and Privacy Workshop) 2024

7. Detecting Social Engineering Scams While Preserving User Privacy in the Digital Era (Proposal Position Paper)
   Atul Prakash, Shivani Kumar, Elisa Tsai
   ConPro (Workshop on Technology and Consumer Protection) 2024

GRANT PROPOSALS

I actively contributed to the proposal design, proposal writing, and presentation for the following grants:

Data Efficiency of LLMs Fine-tuning with RLHF Cisco, 2023
$150*K per year* PI: Atul Prakash

Intelligent Assistants for Detecting Social Engineering Scams OpenAI, 2023
$100*K* PI: Atul Prakash

TEACHING

EECS 588 Computer & Network Security , **Grad Student Instructor** *Winter 2024, UMich*

EECS 281 Data Structures and Algorithms , **Grad Student Instructor** *Fall 2023, UMich*

EECS 598 Secure and Trustworthy ML , **Grad Student Instructor** *Winter 2023, UMich*

SERVICE

- SECRIT (SECurity Reading Is Terrific) Reading Group Host 2021 – 2024
- CSEG (CSE Graduate Students) Outreach Chair 2022 – 2023
- CSEG (CSE Graduate Students) Social Co-Chair 2022 – 2023