Dongyu **Meng**

Ph.D. Candidate · University of California, Santa Barbara

zbshfmmm@gmail.com / dmeng@ucsb.edu | trevillie.github.io | Trevillie | trevillie

Security researcher with experience in smart contract analysis, DeFi anomaly detection, symbolic execution, and adversarial ML. I have published in major security venues and hold prior industry experience in automotive autopilot robustness and anti-spam systems. I also have teaching and mentoring experience in core security and systems courses. I organize and play CTFs with the Shellphish hacking team.

Education

University of California, Santa Barbara — *Santa Barbara, CA*
Ph.D. Computer Science - advisors: Giovanni Vigna, Chris Kruegel — *2025*
- Focus: Security | Research Interests: Smart contract analysis, anomaly detection, ML for security, adversarial ML.

ShanghaiTech University, Chinese Academy of Sciences — *Shanghai, China*
M.S. Computer Science - advisor: Hao Chen — *2018*

Tsinghua University — *Beijing, China*
B.S. Control Science and Engineering - advisor: Jun Li — *2015*

Industry Experience

Keen Security Lab, Tencent — *Shanghai, China*
Security Research Intern — *Sept. 2017 - Apr. 2018*
- Analyzed automotive autopilot firmware and evaluated model safety and stability under adversarial conditions.

Zhihu — *Beijing, China*
Data Analyst Intern — *Summer 2014*
- Developed internal data tooling and SQL pipelines to support the anti-spam team.

Projects (Selected)

HOUSTON — Anomaly Detection for Ethereum DeFi Attacks
- Built a high-throughput transaction tracing and invariant analysis pipeline capable of processing mainnet transaction stream in real time.
- Achieved 94.8% true positive accuracy with only 0.16% false positives.
- Alerts are fully explainable and generalize across diverse DeFi protocols and attack types.

DISSONANCE — Differential Analysis for Smart Contract Upgrades
- Implemented symbolic-execution–driven analysis to support safe and consistent smart contract upgrades.
- Developed a semantic comparison engine detecting behavioral drift and refactoring-induced inconsistencies across contract versions.

Teaching

CS177, Computer Security (UCSB) — *Spring 2020*
TA | Hosted discussions and CTF challenges on network security, reverse engineering, and exploitation.

Undergraduate Data Structure (ShanghaiTech) — *Fall 2015*
TA | Outstanding TA Award

Publications (Selected)

HOUSTON: Real-Time Anomaly Detection of Attacks against Ethereum DeFi Protocols
Dongyu Meng*, Fabio Gritti*, Robert McLaughlin, Nicola Ruaro, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna
Network and Distributed System Security (NDSS) Symposium, 2026

Approve Once, Regret Forever: On the Exploitation of Ethereum's Approve-TransferFrom Ecosystem
Nicola Ruaro, Fabio Gritti, Dongyu Meng, Robert McLaughlin, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna
USENIX Security Symposium (USENIX Security), 2025

A History of Greed: Practical Symbolic Execution for Ethereum Smart Contracts
Nicola Ruaro, Fabio Gritti, Robert McLaughlin, Dongyu Meng, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna
International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2025

Bullseye Polytope: Scalable Clean-Label Poisoning Attack with Improved Transferability
Hojjat Aghakhani, Dongyu Meng, Yu-xiang Wang, Christopher Kruegel, Giovanni Vigna
IEEE European Symposium on Security and Privacy (Euro S&P), 2021

Bran: Reduce Vulnerability Search Space in Large Open Source Repositories by Learning Bug Symptoms
Dongyu Meng, Michele Guerriero, Aravind Machiry, Hojjat Aghakhani, Priyanka Bose, Andrea Continella, Christopher Kruegel, Giovanni Vigna
ACM Asia Conference on Computer and Communications Security (AisaCCS), 2021

MagNet: a Two-Pronged Defense against Adversarial Examples
Dongyu Meng, Hao Chen
ACM Conference on Computer and Communications Security (CCS), 2017