Fnu Suya

suya@umd.edu • fsuya.org • suya • suyafnu
suyeecav • Updated on November 30, 2023

Professional Appointments

MC2 Postdoctoral Fellow, *University of Maryland, College Park* Oct 2023 – present

Education

Ph.D. in Computer Science, *University of Virginia* 2017 – 2023
Thesis: *On the Limits of Data Poisoning Attacks*
Advisor: Yuan Tian (UCLA), David Evans

M.Sc. in Computer Science, *University of Virginia* 2017 – 2022
Advisor: Yuan Tian (UCLA), David Evans

Ph.D. in Computer Science, *Arizona State University* 2015 – 2017
Advisor: Paolo Papotti (EURECOM), discontinued due to advisor relocation

B.Eng. in Electrical Engineering (Honors), *China Agricultural University* 2010 – 2014

Research Interests

Trustworthy Machine Learning, Machine Learning for Security

Internship Experience

Research Intern, *Qualcomm*, San Diego (with Aleksei Triastcyn on robust FL) 2021
Research Intern, *Amazon AWS*, New York City (with MohamadAli Torkamani on GNNs) 2021
Research Intern, *Bosch AI Center*, Pittsburgh (with Anit Kumar Sahu on black-box attacks) 2020
Research Intern, *Tsinghua University*, China (with Bo Bai on wireless communication) 2014-2015

Conference and Journal Papers

Google Scholar ID: OmLIG8EAAAAJ

2023a F. Suya, A. Suri, T. Zhang, S. Hong, Y. Tian, D. Evans. "SoK: Pitfalls in Evaluating Black-Box Attacks". In: *arXiv preprint arXiv:2310.17534*.

2023b F. Suya, X. Zhang, Y. Tian, D. Evans. "What Distributions are Robust to Indiscriminate Poisoning Attacks for Linear Learners?" In: *NeurIPS 2023*.

2023c Y. Tian, **F. Suya**, A. Suri, F. Xu, D. Evans. "Manipulating Transfer Learning for Property Inference". In: *CVPR 2023*.

2022 Y. Tian, **F. Suya**, F. Xu, D. Evans. "Stealthy Backdoors as Compression Artifacts". In: *IEEE TIFS*.

2021 F. Suya, S. Mahloujifar, A. Suri, D. Evans, Y. Tian. "Model-Targeted Poisoning Attacks with Provable Convergence". In: *ICML 2021*.

2020a F. Suya, J. Chi, D. Evans, Y. Tian. "Hybrid Batch attacks: Finding Black-box Adversarial Examples with Limited Queries". In: *USENIX Security 2020*.

2020b J. Wang, M. Luo, **F. Suya**, J. Li, Z. Yang, Q. Zheng. "Scalable Attack on Graph Data by Injecting Vicious Nodes". In: *ECML-PKDD 2020*.

2019 Y. Chen, M. Zha, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, **F. Suya**, Y. Tian, K. Chen, X. Wang, W. Zou. "Demystifying Hidden Privacy Settings in Mobile Apps". In: *IEEE S&P (Oakland) 2019*.

2016 F. Suya, Y. Shi, B. Bai, W. Chen, J. Zhang, K. B. Letaief, S. Zhou. "Optimal Stochastic Power Control with Compressive CSI Acquisition for Cloud-RAN". In: *GlobalSIP 2016*.

Workshop Papers and Posters

2023a A. Kinfe, C. Jung, K. Lin, M. Clyburn, **F. Suya**. "HackWrt: Network Traffic-Based Eavesdropping of Handwriting". In: *CPS-IoT Week 2023*.

2023b F. Suya, X. Zhang, Y. Tian, D. Evans. "When Can Linear Learners be Robust to Indiscriminate Poisoning Attacks?" In: *ICML AdvML-Frontiers Workshop 2023*.

2022 E. Rose, **F. Suya**, D. Evans. "Poisoning Attacks and Subpopulation Susceptibility". In: *VISxAI workshop 2022 (Best Paper Award)*.

2018 F. Suya, D. Evans, Y. Tian. "Poster: Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers". In: *IEEE S&P (Oakland) 2018*.

2017 F. Suya, Y. Tian, D. Evans, P. Papotti. "Query-limited Black-box Attacks to Classifiers". In: *N(eur)IPS MLSec Workshop 2017 (Spotlight Presentation)*.

Talks and Presentations

1. What Distributions are Robust to Indiscriminate Poisoning Attacks for Linear Learners?
NeurIPS, New Orleans, LA Dec, 2023
2. When Can Linear Learners be Robust to Indiscriminate Poisoning Attacks?
ICML Workshop on AdvML-Frontiers, Online Jul, 2023
3. Model-Targeted Poisoning Attacks with Provable Convergence
ICML, Online Jul, 2021
4. Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries
Usenix Security, Online Aug, 2020
5. Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers
IEEE S&P (Oakland), San Francisco, CA May, 2018
6. Query-limited Black-box Attacks to Classifiers
N(eur)IPS workshop on MLSec, Long Beach, CA Dec, 2017
7. Optimal Stochastic Power Control with Compressive CSI Acquisition for Cloud-RAN
GlobalSIP, Washington DC Dec, 2016

Mentoring Experience

- Yulong Tian (Visiting PhD student at UVa, PhD student at NJU, China)
- Tingwei Zhang (Undergraduate student at UVa, now a PhD student at Cornell CS)
- Evan Rose (Undergraduate student at UVa, now a PhD student at Northeastern CS)
- Scott Hong (Undergraduate student at UVa, now a MS student at Columbia)
- Sangsu Kwag (PhD Student at UMD)
- Shayan Shabihi (PhD Student at UMD)

Teaching Experience

- Learning Theory (UVA CS 6501-005), TA S2019
- Cryptography (UVA CS 6501-009), TA S2019
- Game Theory (ASU CSE 556), TA F2016
- Introduction to C++ Programming (ASU CSE 100), TA F2015 – S2016
- Introduction to Programming Languages (ASU CSE 240), TA F2015 – S2016

Honors & Awards

- MC2 Postdoctoral Fellowship: awarded annually to one individual by the Maryland Cybersecurity Center (MC2) 2023

- Outstanding/Top Reviewer: ICLR 2022, NeurIPS 2022, 2023
- CS Graduate Research Award, University of Virginia 2018
- CS Department Fellowship, University of Virginia 2017
- NSF Travel Grant 2016
- CIDSE Doctoral Fellowship, Arizona State University 2015
- Outstanding Student Scholarship, China Agricultural University 2011 – 2013

Service

PC/Reviewer	IEEE EuroS&P, IEEE S&P, ICML, NeurIPS, ICLR, ICCV, CVPR, AISTATS, IJCAI
Journal Reviewer	Artificial Intelligence, TMLR
Sub-Reviewer	IEEE EuroS&P, IEEE S&P, Usenix Security, NDSS, CCS, Sensys, ASIACCS, AAAI, SIGMOD

Skills

Programing	Python, PyTorch, TensorFlow, Matlab, C, C++
Languages	Mongolian (native), Mandarin, English