Fnu Suya

suya@virginia.edu • fsuya.org • suya • suyafnu
suyeecav • Updated on May 3, 2021

Education

- Ph.D. in Computer Science, University of Virginia — Aug 2017 – May 2022
- Ph.D. in Computer Science, Arizona State University — Aug 2015 – May 2017
- B.Eng. in Electrical Engineering, China Agricultural University — Aug 2010 – May 2014

Research Interests

Machine learning security and deep learning, with particular interests in evaluating model robustness under test time attacks (i.e., adversarial examples) and training time attacks (i.e., data poisoning and backdoor attacks).

Research Experience

- Qualcomm Technologies, Inc., Aleksei Triastcyn — May 2021 – Aug 2021
  - Poisoning Attacks on Federated Learning
- Amazon Web Services, Inc., MohamadAli Torkamani — Jan 2021 – Apr 2021
  - Robust Learning on Extremely Large Graphs
- University of Virginia, David Evans, Yuan Tian — Aug 2017 – Present
  - Machine Learning Security in Training and Inference Time
- Bosch Center for Artificial Intelligence, Anit Kumar Sahu — June 2020 – Aug 2020
  - Query Efficient Black-box Attacks
- Arizona State University, Guoliang Xue, Paolo Papotti — Aug 2015 – Jul 2017
  - Incentive Mechanism Design, Machine learning Privacy
- Tsinghua University, Bo Bai — Aug 2014 – Feb 2015
  - Energy Efficient Wireless Communication

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

- CS Graduate Research Award, University of Virginia — 2018
- CS Department Fellowship, University of Virginia — 2017
- NSF Travel Grant, GlobalSIP — 2016
- CIDSE Doctoral Fellowship, Arizona State University — 2015
- Outstanding Student Scholarship, China Agricultural University — 2011 – 2013

Service

Reviewer/Subreviewer	IJCAI 2021, ICML 2020-2021, NeurIPS 2021, IEEE S&P 2018-2021, Usenix Security 2018-2021, NDSS 2018-2021, CCS 2018-2021, Sensys 2021, ASIACCS 2019, Euro S&P 2019, AAAI 2017-2019, SIGMOD 2017, DASFAA 2017, MobiHoc 2016
Program Committee	IJCAI 2021

Skills

Programing	Python, Matlab, C, C++, LaTeX
Frameworks	TensorFlow, PyTorch, MXNet, NumPy, SciPy, Scikit-learn
Systems	Linux, OSX
Languages	Mongolian (native), Chinese, English

Publications

Google Scholar ID: OmLIG8EAAAAJ

2021 Y. Tian, **F. Suya**, F. Xu, D. Evans. "Stealthy Backdoors as Compression Artifacts". In: *arXiv preprint*. URL: https://arxiv.org/abs/2104.15129.

2020a F. Suya, J. Chi, D. Evans, Y. Tian. "Hybrid batch attacks: Finding black-box adversarial examples with limited queries". In: *29th USENIX Security Symposium (USENIX Security 2020)*. URL: https://arxiv.org/abs/1908.07000.

2020b F. Suya, S. Mahloujifar, A. Suri, D. Evans, Y. Tian. "Model-Targeted Poisoning Attacks with Provable Convergence". In: *arXiv preprint arXiv:2006.16469*. URL: https://arxiv.org/abs/2006.16469.

2020c J. Wang, M. Luo, **F. Suya**, J. Li, Z. Yang, Q. Zheng. "Scalable Attack on Graph Data by Injecting Vicious Nodes". In: *The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2020)*. URL: https://arxiv.org/abs/2004.13825.

2019 Y. Chen. "Demystifying Hidden Privacy Settings in Mobile Apps". In: *2019 IEEE Symposium on Security and Privacy (S&P 2019)*. URL: https://ieeexplore.ieee.org/abstract/document/8835388.

2018 F. Suya, D. Evans, Y. Tian. "Poster: Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers". In: *2018 IEEE Symposium on Security and Privacy (S&P 2018)*. URL: https://www.ieee-security.org/TC/SP2018/poster-abstracts/oakland2018-paper37-poster-abstract.pdf.

2017 F. Suya, Y. Tian, D. Evans, P. Papotti. "Query-limited black-box attacks to classifiers". In: *NIPS Workshop on Machine Learning and Computer Security (MLSec)*. URL: https://arxiv.org/abs/1712.08713.

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: *IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2016*. URL: https://ieeexplore.ieee.org/abstract/document/7906068.