Ren Pang

Resume

Education

2019–present **PhD Informatics**, *College of Information Sciences and Technology*, Pennsylvania State University, (Advisor: Ting Wang).

2018–2019 (transferred) **PhD Computer Science**, *Department of Computer Science and Engineering*, Lehigh University, (Advisor: Ting Wang).

2014–2018 **BSc. Mathematics**, *Department of Mathematics*, Nankai University.

Research Interests

Deep Learning Security; Adversarial Robustness; Trojan Backdoor

Publications

ACM CCS'20 **A Tale of Evil Twins: Adversarial Inputs versus Poisoned Models**.
Ren Pang, Hua Shen, Xinyang Zhang, Shouling Ji, Yevgeniy Vorobeychik, Xiapu Luo, Alex Liu, Ting Wang
ACM SAC Conference on Computer and Communications (CCS)

ACM KDD'20 **AdvMind: Inferring Adversary Intent of Black-Box Attacks**.
Ren Pang, Xinyang Zhang, Shouling Ji, Xiapu Luo, Ting Wang
ACM International Conference on Knowledge Discovery and Data Mining (KDD)

AAAI'21 **i-Algebra: Towards Interactive Interpretability of Neural Nets**.
Xinyang Zhang, **Ren Pang**, Shouling Ji, Fenglong Ma, Ting Wang
AAAI Conference on Artificial Intelligence

USENIX Security '21 **Graph Backdoor**.
Zhaohan Xi, **Ren Pang**, Shouling Ji, Ting Wang
USENIX Security Symposium

Preprint **TROJANZOO: Everything you ever wanted to know about neural backdoors (but were afraid to ask)**.
Ren Pang, Zheng Zhang, Xiangshan Gao, Zhaohan Xi, Shouling Ji, Cheng Peng, Ting Wang

180 Candleford Heights – State College, PA
(484) 222 3321 • ain-soph@live.com

Research Experiences

2018 **Adversarial Vulnerabilities in Neural Networks**.
My work explores the mutual reinforcement effects between two attack vectors in deep learning: adversarial inputs and poisoned models, and designs a unified framework to control the trade-offs.

2019 **Detection of Black-box Adversarial Attacks**.
The project develops a novel estimation model to infer the adversary intent of black-box adversarial attacks.

2020 **Backdoors in Neural Networks**.
We construct a universal platform (trojanzoo) that contains state-of-the-art works on backdoor attacks and defenses, evaluate the performance of different methods under the same metric, and explore the underlying mechanism of backdoors in neural networks.

GitHub

I'm currently maintaining the trojanzoo repo, which is a generic platform to conduct deep learning security research (codes of all projects contained):
`https://github.com/ain-soph/trojanzoo`

Teaching Experience

2018 Fall **Teaching Assistant**, *CSE 017: Structured Programming and Data Structures*, Lehigh University (Instructor: Jeff Heflin).

Technical Skills

Language Python; Java; C++; MatLab; Bash; LaTeX
Package pytorch; matplotlib; sphinx
Tools GitHub; Travis CI; Github Action; Docker