REN PANG

College of Information Sciences and Technology, the Pennsylvania State University
Email: rbp5354@psu.edu *Tel*: (484) 747-2401 *Web*: `https://ain-soph.github.io`

A. Research Interests

Deep Learning Security: Adversarial Robustness; Neural Backdoors

AutoML: Neural Architecture Search; Auto Augment

Others: Lifelong Learning; Dataset Condensation

B. Education Background

Ph.D., Information Sciences and Technology, Pennsylvania State University	2019–present
Ph.D., Computer Science and Engineering, Lehigh University (transferred)	2018–2019
BSc., Mathematics, Nankai University	2014-2018

C. Publications

1. TrojanZoo: Towards Unified, Holistic, and Practical Evaluation of Neural Backdoors,
R. Pang, Z. Zhang, X. Gao, Z. Xi, S. Ji, P. Cheng, and T. Wang,
Proceedings of *the IEEE European Symposium on Security and Privacy* (EuroS&P), 2022.

2. On the Security Risks of AutoML,
R. Pang, Z. Xi, S. Ji, X. Luo, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2022.

3. Graph Backdoor,
Z. Xi, **R. Pang**, S. Ji, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2021.

4. i-Algebra: Towards Interactive Interpretability of Deep Neural Networks,
X. Zhang, **R. Pang**, S. Ji, F. Ma, and T. Wang,
Proceedings of *the AAAI Conference on Artificial Intelligence* (AAAI), 2021.

5. AdvMind: Inferring Adversary Intent of Black-Box Attacks,
R. Pang, X. Zhang, S. Ji, X. Luo, and T. Wang,
Proceedings of *the ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD), 2020.

6. A Tale of Evil Twins: Adversarial Inputs versus Poisoned Models,
R. Pang, H. Shen, X. Zhang, S. Ji, Y. Vorobeychik, X. Luo, A. Liu, and T. Wang,
Proceedings of *the ACM Conference on Computer and Communications Security* (CCS), 2020.

D. Open-Sourced Projects

Owner

AlpsPlot
`https://github.com/ain-soph/alpsplot`

TrojanZoo: Towards Unified, Holistic, and Practical Evaluation of Neural Backdoors
`https://github.com/ain-soph/trojanzoo`

TrojanZoo Sphinx Theme
`https://github.com/ain-soph/trojanzoo_sphinx_theme`

Contributor

matplotlib; pytorch_sphinx_theme; sphinxcontrib-katex; torchvision

E. Teaching Assistant Experiences

CYBER 497: Machine Learning Security (Penn State), 2020 Spring

CSE 017: Structured Programming and Data Structures (Lehigh), 2018 Fall

F. Technical Skills

Language

Python; Java; C++; MatLab; Bash; LaTeX; HTML; JavaScript

Package

pytorch; matplotlib; sphinx; jinja; pytest

Tools

Auto CI; Docker; GitHub Actions