Ren Pang

📞 (484)747–2401 | ✉ ain-soph@live.com | ⌂ ain-soph.github.io

My research focuses on developing safe, robust and resilient machine/deep learning applications. Experienced in addressing the security concerns in image classification, AutoML, etc.

EDUCATION

Ph.D.	*Information Sciences and Technology*	Pennsylvania State University	2019–2023
B.Sc.	*Mathematics*	Nankai University	2014–2018

EXPERIENCE

Software Engineer (Intern), *Meta*   2022 Summer

Pages and Groups Integrity
Introduce new classification model for malicious page detection. It mitigates the impact of incorrect label annotation, and provides interpretable classification outputs for better user experience.

TorchVision
Provide the official TorchVision implementation of SwinTransformerV2.

PUBLICATIONS

1. 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.
2. 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.
3. 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.
4. Graph Backdoor,
   Z. Xi, **R. Pang**, S. Ji, and T. Wang,
   Proceedings of *the USENIX Security Symposium* (**USENIX**), 2021.
5. On the Security Risks of AutoML,
   R. Pang, Z. Xi, S. Ji, X. Luo, and T. Wang,
   Proceedings of *the USENIX Security Symposium* (**USENIX**), 2022.
6. 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.
7. The Dark Side of AutoML: Towards Architectural Backdoor Search,
   R. Pang, C. Li, Z. Xi, S. Ji, T. Wang,
   Arxiv Preprint, 2022.
8. Demystifying Self-supervised Trojan Attacks,
   C. Li, **R. Pang**, Z. Xi, T. Du, S. Ji, Y. Yao, T. Wang,
   Arxiv Preprint, 2022.
9. Reasoning over Multi-view Knowledge Graphs,
   Z. Xi, **R. Pang**, C. Li, T. Du, S. Ji, F. Ma, T. Wang,
   Arxiv Preprint, 2022.

OPEN-SOURCE CONTRIBUTIONS

1. **TrojanZoo**   ⚫ https://github.com/ain-soph/trojanzoo

   Offer a universal, flexible PyTorch platform to conduct security analysis of attacks and defenses on deep neural network models.

2. **TorchVision.SwinTransformerV2**   ⚫ https://github.com/pytorch/vision/pull/6246

   Provide TorchVision official implementation of SwinTransformerV2.

3. **TorchVision.AutoAugmentation**   ⚫ https://github.com/pytorch/vision/pull/6609

   Provide TorchVision official implementation of AutoAugmentation for object detection. This work is based on the next generation PyTorch APIs.

4. **Matplotlib.Text**   ⚫ https://github.com/matplotlib/matplotlib/pull/20101

   Fix Text class bug when font argument is provided without math_fontfamily.