# Ting Wang

Computer Science Department, Stony Brook University
*Email*: inbox.ting@gmail.com *Tel*: (814) 699-2557 *Web*: `https://alps-lab.github.io/`

## *A. Research Interests*

I conduct research at the interface of security, privacy, and machine learning. My current work focuses on building safe and trustworthy artificial intelligence (AI) technologies.

## *B. Professional Positions*

| | |
|---|---|
| Stony Brook University<br>*Associate Professor, Empire Innovation Scholar*<br>Computer Science Department | 2023–present |
| The Pennsylvania State University<br>*Assistant Professor* (2019–2022), *Associate Professor* (2022–2023)<br>College of Information Sciences and Technology | 2019–2023 |
| Meta<br>*Research Scientist* | 2021–2022 |
| Lehigh University<br>*Assistant Professor*<br>Department of Computer Science and Engineering | 2015–2019 |
| IBM Thomas J. Watson Research Center<br>*Research Staff Member and Security Analytic Lead* | 2011–2015 |

## *C. Education Background*

| | |
|---|---|
| Ph.D., Computer Science, Georgia Institute of Technology | 2011 |
| M.Sc., Computer Science, The University of British Columbia | 2006 |
| B.E. (*Cum Laude*), Computer Science and Technology, Zhejiang University | 2004 |

## *D. Selected Honors and Awards*

| | |
|---|---|
| ACM CHI Best Paper Honorable Mention | 2023 |
| ACM SIGSOFT Distinguished Paper Award | 2022 |
| Faculty Research Excellence Award (Penn State) | 2021 |
| Dean's Circle of Teaching Excellence Award (Penn State) | 2020 |
| Rossin Assistant Professorship (Lehigh) | 2019 |
| NSF CAREER Award | 2019 |
| ACM/IEEE ESEM Best Paper Runner-up Award | 2019 |
| ACM AISec Best Paper Award | 2018 |
| IEEE CNS Best Paper Award | 2017 |
| ACM CoNEXT Best Paper Runner-up Award | 2010 |

## *E. Selected Publications*

(∗ student/scholar under my supervision)

1. On the Difficulty of Defending Contrastive Learning against Backdoor Attacks,
C. Li,* R. Pang,*, B. Cao, Z. Xi,* J. Chen, S. Ji, T. Wang,
Proceedings of *USENIX Security Symposium* (USENIX), 2024

2. Improving the Robustness of Transformer-based Large Language Models with Dynamic Attention,
L. Shen, Y. Pu, S. Ji, C. Li, X. Zhang, C. Ge, T. Wang,
Proceedings of *Network and Distributed System Security Symposium* (NDSS), 2024

3. Model Extraction Attacks Revisited,
J. Liang,*, R. Pang,* C. Li,*, T. Wang,
Proceedings of *ACM ASIA Conference on Computer and Communications Security* (ASIACCS), 2024

4. Generative AI in the Wild: Prospects, Challenges, and Strategies,
Y. Sun, E. Jang, F. Ma, Ting Wang,
Proceedings of *ACM CHI Conference on Human Factors in Computing Systems* (CHI), 2024

5. ReMasker: Imputing Tabular Data with Masked Autoencoding,
T. Du,* L. Melis, T. Wang,
Proceedings of *International Conference on Learning Representations* (ICLR), 2024

6. Backdoor Contrastive Learning via Bi-level Trigger Optimization,
W. Sun, X. Zhang, H. Lu, Y. Chen, T. Wang, J. Chen, L. Lin,
Proceedings of *International Conference on Learning Representations* (ICLR), 2024

7. Defending Pre-trained Language Models as Few-shot Learners against Backdoor Attacks,
Z. Xi,* T. Du,* C. Li,* R. Pang,* S. Ji, J. Chen, F. Ma, and T. Wang,
Proceedings of *the Annual Conference on Neural Information Processing Systems* (NeurIPS), 2023

8. IMPRESS: Evaluating the Resilience of Imperceptible Perturbations Against Unauthorized Data Usage in Diffusion-Based Generative AI
B. Cao, C. Li,* T. Wang, J. Jia, B. Li, and J. Chen,
Proceedings of *the Annual Conference on Neural Information Processing Systems* (NeurIPS), 2023

9. UniT: A Unified Look at Certified Robust Training against Text Adversarial Perturbation,
M. Ye,* Z. Yin,* T. Zhang, T. Du,* J. Chen, T. Wang, and F. Ma,
Proceedings of *the Annual Conference on Neural Information Processing Systems* (NeurIPS), 2023

10. VLATTACK: Multimodal Adversarial Attacks on Vision-Language Tasks via Pre-trained Models,
Z. Yin,* M. Ye,* T. Zhang, T. Du,* J. Zhu, H. Liu, J. Chen, T. Wang, and F. Ma,
Proceedings of *the Annual Conference on Neural Information Processing Systems* (NeurIPS), 2023

11. An Embarrassingly Simple Backdoor Attack on Self-supervised Learning,
C. Li,* R. Pang,* Z. Xi,* T. Du,* S. Ji, Y. Yao, and T. Wang,
Proceedings of *the International Conference on Computer Vision* (ICCV), 2023

12. The Dark Side of AutoML: Towards Architectural Backdoor Search,
R. Pang,* C. Li,* Z. Xi,* S. Ji, and T. Wang,
Proceedings of *the International Conference on Learning Representation* (ICLR), 2023

13. AutoML in the Wild: Obstacles, Workarounds, and Expectations,
Y. Sun,* Q. Song, X. Gui, F. Ma, and T. Wang,
Proceedings of *the ACM CHI Conference on Human Factors in Computing Systems* (CHI), 2023

14. On the Security Risks of Knowledge Graph Reasoning,
Z. Xi,* T. Du,* C. Li,* R. Pang,* S. Ji, X. Luo, X. Xiao, F. Ma, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2023

15. FreeEagle: Detecting Complex Neural Trojans in Data-Free Cases,
C. Fu, X. Zhang, S. Ji, T. Wang, P. Lin, Y. Feng, and J. Yin,

Proceedings of *the USENIX Security Symposium* (SECURITY), 2023

16. AIRS: Explanation for Deep Reinforcement Learning based Security Applications,
J. Yu, W. Guo, Q. Qin, G. Wang, T. Wang, and X. Xing,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2023

17. PAT: Geometry-Aware Hard-Label Black-Box Adversarial Attacks on Text,
M. Ye,* J. Chen, C. Miao, H. Liu, T. Wang, and F. Ma
Proceedings of *the ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD), 2023

18. Certified Edge Unlearning for Graph Neural Networks,
K. Wu, J. Shen, Y. Ning, T. Wang, and W. Wang
Proceedings of *the ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD), 2023

19. 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.

20. Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era,
C. Li,* L. Wang, S. Ji, X. Zhang, Z. Xi,* S. Guo, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2022.

21. Label Inference Attacks Against Vertical Federated Learning,
C. Fu, X. Zhang, S. Ji, J. Chen, J. Wu, S. Guo, J. Zhou, A. Liu, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2022.

22. "Is Your Explanation Stable?": A Robustness Evaluation Framework for Feature Attribution,
Y. Gan, Y. Mao, X. Zhang, S. Ji, Y. Pu, M. Han, J. Yin, and T. Wang,
Proceedings of *the ACM Conference on Computer and Communications Security* (CCS), 2022

23. Transfer Attacks Revisited: A Large-Scale Empirical Study in Real Computer Vision Settings,
Y. Mao, C. Fu, S. Wang, S. Ji, X. Zhang, Z. Liu, J. Zhou, A. Liu, R. Beyah, and T. Wang
Proceedings of *the IEEE Symposium on Security and Privacy* (Oakland), 2022

24. An Invisible Black-box Backdoor Attack through Frequency Domain,
T. Wang, Y. Yao, F. Xu, S. An, H. Tong, and T. Wang,
Proceedings of *the European Conference on Computer Vision* (ECCV), 2022

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

26. Towards Fair and Robust Classifiers,
H. Sun, K. Wu, T. Wang, and W. Wang,
Proceedings of *the IEEE European Symposium on Security and Privacy* (EuroS&P), 2022

27. LeapAttack: Hard-Label Adversarial Attack on Text via Gradient-Based Optimization,
M. Ye,* J. Chen, C. Miao, T. Wang, and F. Ma,
Proceedings of *the ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD), 2022

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

29. Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations,
P. Jing, Q. Tang, Y. Du, L. Xue, X. Luo, T. Wang, S. Nie, and S. Wu,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2021.

30. UNIFUZZ: A Holistic and Pragmatic Metrics-Driven Platform for Evaluating Fuzzers,
Y. Li, S. Ji, Y. Chen, S. Liang, W. Lee, Y. Chen, C. Lyu, C. Wu, R. Beyah, P. Cheng, K. Lu, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2021.

31. Cert-RNN: Towards Certifying the Robustness of Recurrent Neural Networks,
T. Du,* S. Ji, L. Shen, Y. Zhang, J. Li, J. Shi, C. Fang, J. Yin, R. Beyah, T. Wang,
Proceedings of *the ACM Conference on Computer and Communications Security* (CCS), 2021.

32. Trojaning Language Models for Fun and Profit,
X. Zhang,* Z. Zhang,* S. Ji, and T. Wang,
Proceedings of *the IEEE European Symposium on Security and Privacy* (EuroS&P), 2021.

33. 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.

34. 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.

35. 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.

36. Text Captcha Is Dead? A Large Scale Deployment and Empirical Study,
C. Shi, S. Ji, Q. Liu, C. Liu, Y. Chen, Y. He, Z. Liu, R. Beyah, and T. Wang,
Proceedings of *the ACM Conference on Computer and Communications Security* (CCS), 2020.

37. Interpretable Deep Learning under Fire,
X. Zhang,* N. Wang,* H. Shen,* S. Ji, X. Luo, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2020.

38. TextShield: Robust Text Classification Based on Multimodal Embedding and Neural Machine Translation,
J. Li, T. Du, S. Ji, R. Zhang, Q. Lu, M. Yang, and T. Wang,
Proceedings of *the USENIX Security Symposium* (SECURITY), 2020.

39. SirenAttack: Generating Adversarial Audio for End-to-End Acoustic Systems,
T. Du,* S. Ji, J. Li, Q. Gu, T. Wang, and R. Beyah,
Proceedings of *the ACM ASIA Conference on Computer and Communications Security* (ASIACCS), 2020.

40. DeepSec: A Uniform Platform for Security Analysis of Deep Learning Models,
X. Ling, S. Ji, J. Zou, J. Wang, C. Wu, B. Li, and T. Wang,
Proceedings of *the IEEE Symposium on Security and Privacy* (Oakland), 2019.

41. TextBugger: Generating Adversarial Text Against Real-world Applications,
J. Li, S. Ji, T. Du, B. Li, and T. Wang,
Proceedings of *the Network and Distributed System Security Symposium* (NDSS), 2019.

42. Model-Reuse Attacks on Deep Learning Systems,
Y. Ji,* X. Zhang,* S. Ji, X. Luo, and T. Wang,
Proceedings of *the ACM Conference on Computer and Communications Security* (CCS), 2018.

43. Integration of Static and Dynamic Code Stylometry Analysis for Programmer De-anonymization,
N. Wang,* S. Ji, and T. Wang,
Proceedings of *the ACM Workshop on Artificial Intelligence and Security* (AISec), 2018.

44. Towards Evaluating the Security of Image CAPTCHA in The Wild,
B. Zhao, H. Weng, S. Ji, J. Chen, T. Wang, Q. He, and R. Beyah,
Proceedings of *the ACM Workshop on Artificial Intelligence and Security* (AISec), 2018.

45. Quantifying Graph Anonymity, Utility, and De-anonymity,
S. Ji, T. Du, Z. Hong, T. Wang, and R. Beyah,
Proceedings of *the IEEE International Conference on Computer Communications* (INFOCOM), 2018.

46. Backdoor Attacks against Learning Systems,
Y. Ji,* X. Zhang,* and T. Wang,
Proceedings of *the IEEE Conference on Communications and Network Security* (CNS), 2017.

47. Private, yet Practical, Multiparty Deep Learning,
X. Zhang,* S. Ji, H. Wang, and T. Wang,
Proceedings of *the IEEE International Conference on Distributed Computing Systems* (ICDCS), 2017.

48. BotMeter: Charting DGA-Bot Landscapes in Large Networks,
T. Wang, X. Hu, J. Jang, S. Ji, M. Stoecklin, and T. Taylor,
Proceedings of *the IEEE International Conference on Distributed Computing Systems* (ICDCS), 2016.

49. Characterizing and Detecting Malicious Web Infrastructures through Server Visibility Analysis,
J. Zhang,* X. Hu, J. Jang, T. Wang, G. Gu, and M. Stoecklin,
Proceedings of *the IEEE International Conference on Computer Communications* (INFOCOM), 2016.

50. PARS: A Uniform and Open-source Password Analysis and Research System,
S. Ji, S. Yang, T. Wang, C. Liu, W. Lee, and R. Beyah,
Proceedings of *the Annual Computer Security Applications Conference* (ACSAC), 2015.

## *F. Funding and Grants*

1. PI, SaTC:CORE:Small: Understanding and Mitigating the Security Risks of AutoML, $500,000 (Personal Portion: 50%), National Science Foundation, 2022 – 2025.
2. PI at Penn State, CCF:PPoSS:LARGE: Principles and Infrastructure of Extreme-Scale Edge Learning for Computational Screening and Surveillance for Health Care, $4,993,564 (Personal Portion: 25%), National Science Foundation, 2021 – 2026.
3. Sole PI, CAREER: Trustworthy Machine Learning from Untrusted Models, $509,895 (Personal Portion: 100%), National Science Foundation, 2019 – 2024.
4. Sole PI, III:CORE:Small: Usable Interpretability, $495,592 (Personal Portion: 100%), National Science Foundation, 2019 – 2022.
5. PI at Penn State, HORUS: Hardened Orchestrated Response for Uncertain Settings, (Personal Portion: $355,183), Defense Advanced Research Projects Agency, 2019 – 2022, with Josyula Rao (PI, IBM Research).
6. Sole PI, SaTC:CORE:Small: Towards Attack-Agnostic Defenses against Adversarial Inputs in Learning Systems, $498,315 (Personal Portion: 100%), National Science Foundation, 2017 – 2022.
7. Sole PI, CRII:SaTC: Re-Envisioning Contextual Services and Mobile Privacy in the Era of Deep Learning, $168,683 (Personal Portion: 100%), National Science Foundation, 2016 – 2019.

## *G. Professional Services*

Journal Editorship – Associate Editor of ACM Transactions on Intelligent Systems and Technology (2023–present); Associate Editor of Journal of Computer Security (2019–present); Guest Editor of Frontiers in Big Data (2021–2022)

Program Committee – ACM Conference on Computer and Communications Security (CCS) (2020–2024); USENIX Security Symposium (SECURITY) (2021–2024); Annual Conference on Neural Information Processing Systems (NeurIPS) (2023–2024); International Conference on Machine Learning (ICML) (2023–2024); International Conference on Learning Representations (ICLR) (2023–2024); ACM Conference on Management of Data (SIGMOD) (2022–2024); ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) (2016–2024); ACM International Conference on Information and Knowledge Management (CIKM) (2017–2024)

Journal Review – Nature Scientific Reports; ACM Transactions on Database Systems; ACM Transactions on the Web; IEEE Transactions on Big Data; IEEE Transactions on Network and Service Management; IEEE Transactions on Knowledge and Data Engineering; Data Mining and Knowledge Discovery; IEEE/ACM Transactions on Networking; The International Journal on Very Large Data Bases; IEEE Transactions on Parallel and Distributed Systems; IEEE Internet Computing.

Grant Review – National Science Foundation (2012, 2014, 2017–2019, 2021–2024)