Tingwei Zhang

✉ tingwei@cs.cornell.edu   Tingwei-Zhang   https://ztingwei.com/

Education

2023 – *2028*	🔖	**Ph.D. Computer Science, Cornell University** Advisor: Vitaly Shmatikov Research Interests: the security and privacy aspects of machine learning
2020 – 2023	🔖	**B.A. in Computer Science with Minor in Statistics, University of Virginia (UVA)** Graduated with *Highest Distinction* in Distinguished Majors Program in computer science. Worked with Prof. David Evans and Prof. Yuan Tian on security of machine learning projects at Security Research Group at UVA.

Publications and Manuscripts

Google Scholar ID: YVJJz9cAAAAJ

Conference Proceedings

1. S. Fnu, A. Suri, **T. W. Zhang**, J. T. Hong, Y. Tian, and D. Evans, “SoK: Pitfalls in Evaluating Black-Box Attacks,” in *Proceedings of the IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2024)*, Toronto, Canada, 2024. URL: https://arxiv.org/abs/2310.17534.

Teaching

Spring 2024	🔖	Cornell Tech CS5450: Networked and Distributed Systems, Head TA
Fall 2023	🔖	Cornell University CS2110: Object-Oriented Programming and Data Structures, TA
Fall 2022	🔖	UVA CS4774: Machine Learning, TA
Spring 2022	🔖	UVA CS4102: Algorithms, TA

Honors & Awards

2021 & 2022	🔖	**Dean’s List of Distinguished Students**, College of Arts & Sciences, UVA
2018	🔖	**Honorable Nomination**, 21st ANNUAL HiMCM

Skills

Programing	🔖	Python, PyTorch, TensorFlow, Java, C/C++, Methmetics, R
Languages	🔖	Mandarin (native), and English
Interests	🔖	Basketball, Movies, Erhu - Chinese two-stringed fiddle, and Traveling

Last updated Jan. 1, 2024