

Yue Gao

DOCTORAL STUDENT · COMPUTER SCIENCE

Department of Computer Sciences, University of Wisconsin–Madison, 1210 W. Dayton St., Madison, WI 53706

+1 (608) 733-8789 | gy@cs.wisc.edu | pages.cs.wisc.edu/~gy | [Lodour](#) | [ygao234](#) | [Google Scholar](#)

Education

University of Wisconsin–Madison

Ph.D. in Computer Science

- Advisor: [Kassem Fawaz](#)

Madison, WI

Jan. 2020 – Present

University of Wisconsin–Madison

M.S. in Computer Science

- Advisor: [Kassem Fawaz](#)

Madison, WI

Sep. 2018 – Dec. 2020

Shanghai University

B.Eng. in Computer Science and Technology

- Major GPA: 3.99/4.00 (ranked 1/292)
- Advisor: [Xiaodong Yue](#)
- Thesis: A Deep Neural Network based Image Compression Method

Shanghai, China

Sep. 2014 – Jul. 2018

Research Experience

University of Wisconsin–Madison

Research Assistant at [Wi-Pi](#) and [MadS&P](#)

- Advisor: [Kassem Fawaz](#)
- Research Area: Trustworthy Machine Learning, Security and Privacy.

Madison, WI

Nov. 2018 – Present

Microsoft Research Redmond

Research Internship

- Mentors: [Jay Stokes](#) and [Emre Kiciman](#)
- Develop defenses and auditing frameworks for textual backdoor attacks on language models.

Redmond, WA

Jun. 2021 – Sep. 2021

TuCodec Inc.

Research and Development Internship

- Improve the efficiency of deep learning based image compression algorithms (1 min → 5 secs).
- Winner of the 1st CVPR [Workshop and Challenge on Learned Image Compression](#).
- Develop deep learning systems on mainstream operating systems (Windows, macOS, Linux).

Shanghai, China

Jan. 2018 – Jul. 2018

Publications

CONFERENCE PAPERS

The Interplay Between Vulnerabilities in Machine Learning Systems [PDF] [Code]

[Yue Gao](#), [Ilia Shumailov](#), [Kassem Fawaz](#).

ICML (Oral, 2%)

May 2022

Experimental Security Analysis of the App Model in Business Collaboration Platforms

[Yunang Chen](#)^{*}, [Yue Gao](#)^{*}, [Nick Ceccio](#), [Rahul Chatterjee](#), [Kassem Fawaz](#), [Earlence Fernandes](#).

USENIX Security

May 2022

WORKSHOP PAPERS

Variational Autoencoder for Low Bit-rate Image Compression [PDF]

[Lei Zhou](#)^{*}, [Chunlei Cai](#)^{*}, [Yue Gao](#), [Sanbao Su](#), [Junmin Wu](#).

CVPR Workshop

Jul. 2018

PREPRINTS

On the Limitations of Stochastic Pre-processing Defenses [PDF]

[Yue Gao](#), [Ilia Shumailov](#), [Kassem Fawaz](#), [Nicolas Papernot](#).

arXiv

May 2022

Analyzing Accuracy Loss in Randomized Smoothing Defenses [PDF]

[Yue Gao](#), [Harrison Rosenberg](#), [Kassem Fawaz](#), [Justin Hsu](#), [Somesh Jha](#).

arXiv

Mar. 2020

Selected Projects

Trustworthy Machine Learning Systems under Multiple Threats

Madison, WI

Mentor: [Kassem Fawaz](#)

Sep. 2020 – Jan. 2021

- Explore a broader attack vector in real-world machine learning systems.
- Propose an attack framework breaking ALL but one prior defenses.
- Demonstrate new amplified threats on trustworthy machine learning.

Defenses against Machine Learning Attacks (Competitive)

Madison, WI

Mentor: [Kassem Fawaz](#), [Somesh Jha](#)

Mar. 2019 – Present

- Improve adversarial robustness with physical constraints.
- Defend against patch attacks in multimodal scenarios ([so2sat](#) classification, [carla](#) object detection).

Online Business Collaboration Platforms

Madison, WI

Mentor: [Rahul Chatterjee](#), [Kassem Fawaz](#), [Earlence Fernandes](#)

Mar. 2021 – Dec. 2021

- Analyze the permission model of third-party apps in black-box collaboration platforms (e.g., Slack, MS Teams).
- Exploit OAuth-based designs to bypass access control and affect user privacy.

Professional Activities

2022	Reviewer , NeurIPS (5) and ICML (4)
2021 – 2022	External Reviewer , USENIX Security Symposium
2021 – 2022	External Reviewer , IEEE Symposium on Security and Privacy
2019	External Reviewer , ACM Conference on Computer and Communications Security
2016 – 2017	Team Leader , Collegiate ICPC Team at Shanghai University

Selected Honors & Awards

2017	China National Scholarship
2017	The China Computer Federation Elite Collegiate Award
2015	Bronze Prize , ACM ICPC Asia East-Continent Final Contest
2016	Shanghai City Scholarship
2015	Bronze Prize , ACM ICPC Asia Shanghai Regional Contest

Technical Skills

Python	Research (2018 – present), system optimization (2018), backend development (2016 – 2017).
PyTorch	Research (2019 – present), distributed training (2020 – 2022).
Docker	Research (2018 – 2022), computing cluster (2017 – 2018).
C / C++	Kernel development (2019), system optimization (2018), programming contest (2014 – 2018).
TensorFlow	Service deployment (2018).
Java EE	Backend development (2016).