Xiaoyu Cao

CONTACT

- **Email**: xiaoyu.cao@duke.edu
- **Phone**: Hidden

127 North Building
Duke University
Durham, NC 27708

EDUCATION

- **Duke University** **Aug. 2019 – Present**
  PhD., Computer Engineering
  Advisor: Neil Zhenqiang Gong
- **Iowa State University (ISU)** **Aug. 2016 – Aug. 2019**
  PhD., Computer Engineering
  Advisor: Neil Zhenqiang Gong
- **University of Science and Technology of China (USTC)** **Sep. 2012 – Jul. 2016**
  B.E., Electronic Engineering

RESEARCH INTERESTS

- Trustworthy AI

HONORS AND AWARDS

- IBM Fellowship in ECE of Iowa State University **2016 – 2017**
- Outstanding Undergraduate Scholarship at USTC **2012 – 2014**
- *The Most Creative Award* in Robot Design Competition *RoboGame* at USTC **2013**

PUBLICATIONS

1. Jia, Jinyuan, Xiaoyu Cao, Binghui Wang, and Neil Zhenqiang Gong. "Certified Robustness for Top-k Predictions against Adversarial Perturbations via Randomized Smoothing." in *International Conference on Learning Representations (ICLR)*, 2020.

2. Fang, Minghong, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong. "Local model poisoning attacks to Byzantine-robust federated learning." In *USENIX Security*, 2020.

3. Xiaoyu Cao, Neil Zhenqiang Gong. "Mitigating Evasion Attacks to Deep Neural Networks via Region-based Classification". In *Annual Computer Security Applications Conference (ACSAC)*, 2017.

4. Neil Zhenqiang Gong, Altay Ozen, Yu Wu, Xiaoyu Cao, Richard Shin, Dawn Song, Hongxia Jin, Xuan Bao. "PIANO: Proximity-based User Authentication on Voice-Powered Internet-of-Things Devices". In *International Conference on Distributed Computing Systems (ICDCS)*, short paper, 2017.

TEACHING EXPERIENCE

- Teaching Assistant for CprE 308 - Operating Systems **Fall 2016 & Spring 2017**

SKILLS

- Python, Tensorflow, PyTorch, C/C++, JAVA