

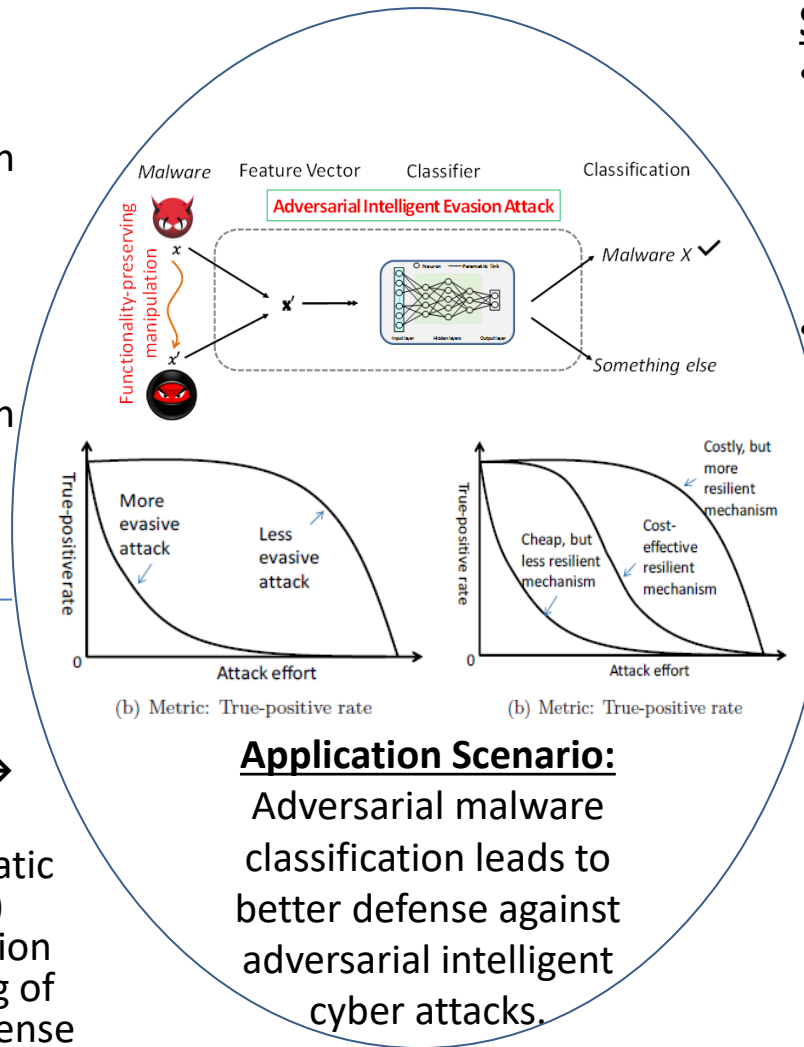
NSF SaTC: CORE: Small: Collaborative: A Framework for Enhancing the Resilience of Cyber Attack Classification and Clustering Mechanisms

Challenge:

- How to **quantify** the vulnerability and resilience of classification and clustering mechanisms against adversarial intelligent cyber evasion attacks?
- How to **enhance** the resilience of classification and clustering mechanisms against adversarial intelligent cyber evasion attacks?

Solution:

- Defense principles → Framework → Metrics → Effective Mechanisms
- Key innovations: Systematic (black-, gray-, white-box) threat model quantification → deeper understanding of the enemy → better defense



Scientific Impact:

- The project will **deepen understanding** of the vulnerability of AI/Machine Learning to adversarial intelligent cyber evasion attacks.
- The project will **invent countermeasures** to enhance resilience of AI/Machine Learning against adversarial intelligent cyber evasion attacks.

Broader Impact:

- Safer AI/Machine Learning
- Potential transition to practice
- 30+ publications (including ICSE'22, ACSAC'21 IJCAI'19, AAAI'19, WWW'19, ACSAC'18, IEEE TDSC)
- MIT Lincoln Lab AICS 2019 Adversarial Malware Classification Challenge Winner
- 10+ media reports
- 3 PhD Dissertations
- 10+ seminar/invited presentations
- 3+ courses used research materials
- 5 undergraduate and 1 HS student