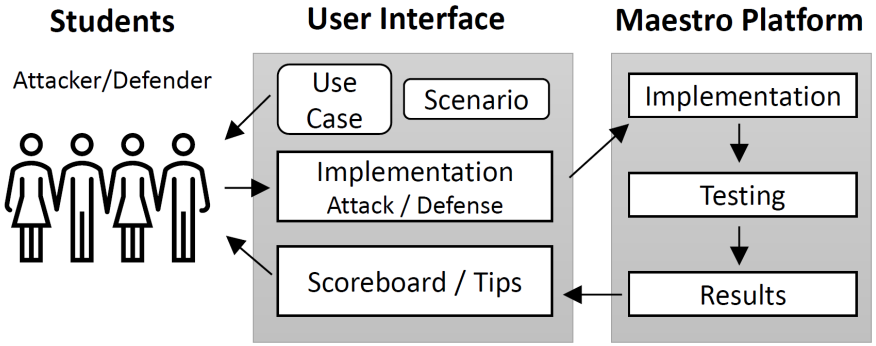
Multi-Level Attack and Defense Simulation Environment for Artificial Intelligence Education and Research

UCI University of California, Irvine

Challenge:

- Education in AI robustness falls behind
- Lacks a hands-on platform to teach how to develop robust AI system



Scientific Impact:

- Bridging the gap between the research in AI robustness and education
- A framework formalizing various AI attacks and defenses to enable new research

Solution:

- Developing Maestro, a new platform, integrating various AI attacks, defenses, and applications
- Game-based learning to let students implement methods and compete

Maestro Platform
- Multi-level access for attacks
- Multi-level defense setup
- Diverse application domains

Broader Impact and Broader Participation:

- Raise public awareness of AI robustness
- Fostering a workforce who can build robust AI
- Courses offered at UCI
- Public release of the Maestro platform

2039634, 08/01/2020 – 07/31/2022

University of California, Irvine
Zhou Li (zhou.li@uci.edu), Sergio Gago Masague (sgagomas@uci.edu), Sameer Singh (sameer@uci.edu)