COLLEGE OF ENGINEERING
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

CPE498 Capstone Design Course

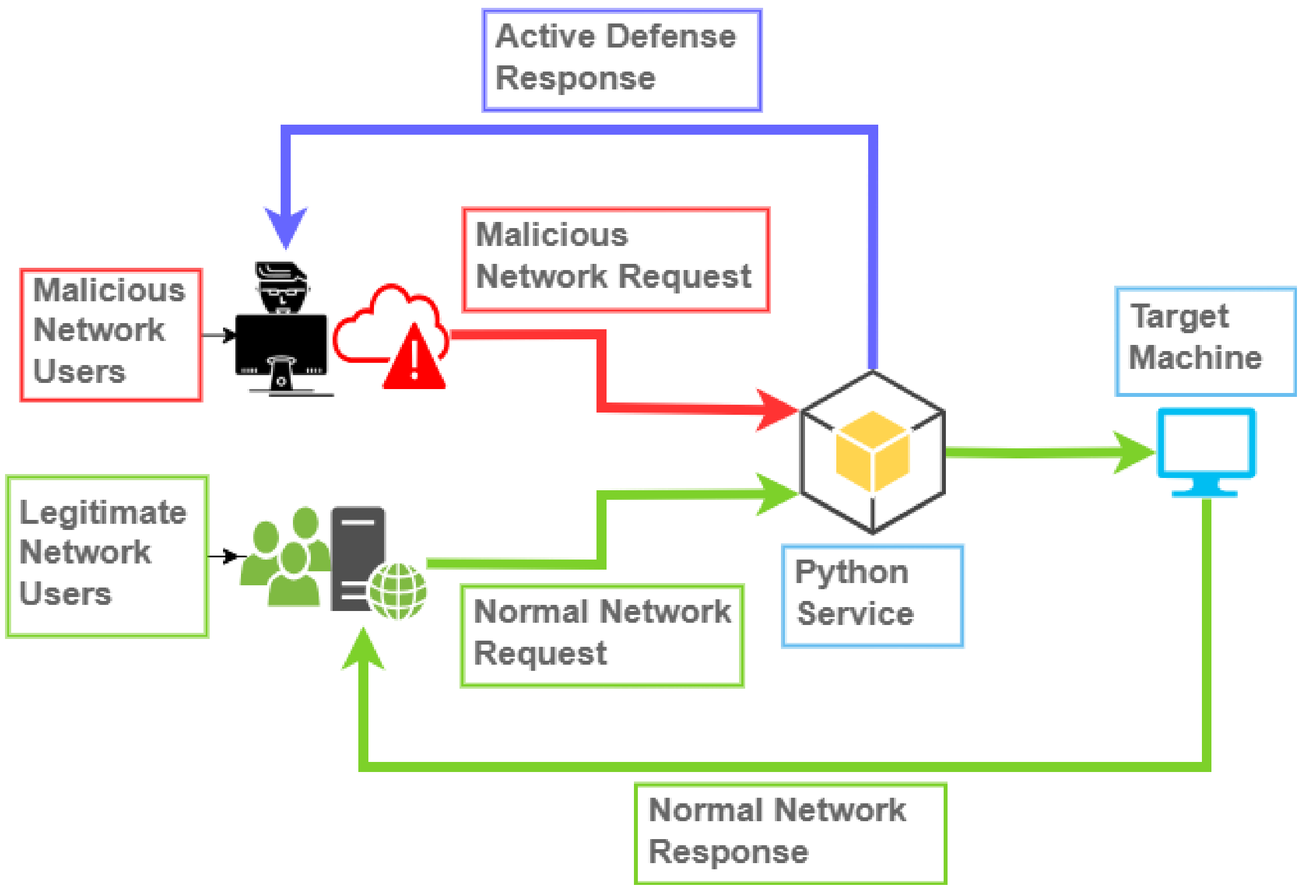
Charger Active Cybersecurity Defense Testbed Team 1

Sydney Bacon, Koby Harris, Alex Smithfield, Nicholas Whisenant

Dr. David Coe, Associate Professor, Electrical & Computer Engineering, UAH

Overview of Project

- Defensive cybersecurity tools are almost all passive; most tools seek to block incoming attacks, not disrupt their execution
- An active defense mechanism that can neutralize an attacking application is needed
- Active defense responses can be discovered through fuzz testing and replayed through a Python service



Major Results

- Developed a comprehensive fuzz testing workflow
- Proved cybersecurity attack tools can be mitigated through active defense
- Proved our fuzzing workflow can be applied to attack tools to discover active defense responses

Future Work

- Future work could include applying the workflow to an established offensive tool
- Another potential direction is the development of a comprehensive fuzz testing tool

Requirements

- Develop a fuzz testing workflow for identifying active defense mitigations against offensive cybersecurity programs
- Develop offensive cybersecurity programs capable of attacking across a network with the assistance of LLMs
- Develop a Python application capable of providing active defense by replaying identified active defense responses

Design Approach

- Our fuzzing workflow provides a framework for discovering active defense responses for a give offensive tool
- The Python application functions by accepting a connection from an attacker, retrieving and sending an active defense response to them.