Thesis Defense

Computer Science Master's Program

"Real-Time Network Simulations for ML/DL DDoS Detection Using Docker"

By **Luis Garcia**

Abstract:

As the integration of artificial intelligence (AI) within cybersecurity continues to grow, machine learning (ML) and deep learning (DL) models are increasingly used to detect such attacks. However, these models are rarely evaluated in real-time attack scenarios to see how subtle changes from the real networking environment can affect their predictions. To address this issue, we propose a scalable, platform-independent Docker testbed specifically designed for simulating real-time Distributed Denial of Service (DDoS) attack scenarios that allows researchers to deploy and evaluate their pre-trained, ML and DL detection models. Our framework is simple to configure and can run across Intel and ARM CPUs, as well as Windows, Linux, and macOS operating systems. The testbed was validated with our six pre-trained models in a 10-minute DDoS attack simulation, where performance metrics such as resource consumption were actively monitored across different operating systems and CPUs. This Dockerized environment offers researchers an accessible and flexible solution for testing and improving DDoS detection models in a realistic, real-time context.

Date: Wednesday, October 23rd, 2024
Time: 8:00 AM – 10:00 AM
Location: 14-232b
Zoom: https://calpoly.zoom.us/j/83826618802
Committee: Dr. Kurfess, Dr. Fang, and Dr. Sisodia