CMSC451 - CS24-327 Machine Learning for 5G Security Analysis Project Proposal

Current State

1. Completing a detailed scheduled plan for the entirety of the project, including milestones, due dates, and specific individual tasks.
2. Researching python libraries (tensor flow, pytorch, and scikit learn), understanding more about vulnerabilities within systems, types of security attacks, and attack graphs.

Problem Statement

1. Wireless networks are becoming both increasingly critical to modern life and increasingly complex and difficult to secure. Applying ML to the analysis of cyber attack graphs, a common way to represent the steps for completing a cyber attack, represents a promising path for supporting the security of modern wireless networks.

Business and Functional Requirements

1. Data for constructing ML models for security analysis
2. Code to produce and train ML models
3. Test and evaluation data comparing ML model performance

Any constraints

1. None at this time

Propose a solution(s) approach (deliverables)

1. Data for constructing ML models for security analysis: This involves collecting and preparing relevant data related to cyber attack graphs and 5G network security vulnerabilities.
2. Code to produce and train ML models: You will need to develop code that can preprocess the collected data, build ML models, and train them using appropriate algorithms and techniques.
3. Test and evaluation data comparing ML model performance: To evaluate the effectiveness of the ML models, you will need to gather test data and compare the performance of the models in terms of identifying likely attack paths, predicting new links in the attack graph, or combining multiple graphs.

Resources - hardware, services, skills, etc:

1. Python, TensorFlow, Torch, and scikit learn
2. Possibly AWS server

3. https://arxiv.org/abs/2108.03514 (article given from sponsor about security of a similar network)
4. https://arxiv.org/pdf/2108.03514.pdf (pdf version)
5. NIST Framework (detailing potential attacks and security risks)

Stakeholders

1. Idaho National Laboratory