ML for 5G Security Analysis

Megan Sorochin, Even Pham, James McGlone, Miles Fagan

Tensor Flow

-Create Machine Learning models

-Help implement Best Practices for data automation, model tracking, performance monitoring, and model retraining

-Used to load and deploy data

PyTorch

- Deep Learning tensor library for Python

- Two main features
  - Tensor computation with strong GPU acceleration support
  - Automatic Differentiation for creating and training deep neural networks

SciKit Learn

– Machine Learning Library in Python

— Algorithm Examples —

-Support Vector Machines

-Decision Trees

-Random Forests

-Neural Networks

– Data preprocessing, model evaluation, and model deployment

NIST

National Institute of Standards and Technology

- Cybersecurity framework for using best practices to organize and improve cybersecurity of programs.

- NIST has outlined a 5G security framework with a growing list of security categories and capabilities

-Organized by reference names 5GSC1-5GSC8:

Subscriber Privacy 5GSC-1

API Security 5GSC-5

Radio Network Security 5GSC-2

Network Slicing Security 5GSC-6

Authentication Enhancements 5GSC-3

Application Security 5GSC-7

Interworking & Roaming Security 5GSC-4

Internet Security Protocol Recommended Practice 5GSC-8

Vulnerabilities

- 5G networks in particular introduce a large amount of security vulnerabilities that can be exploited by attackers

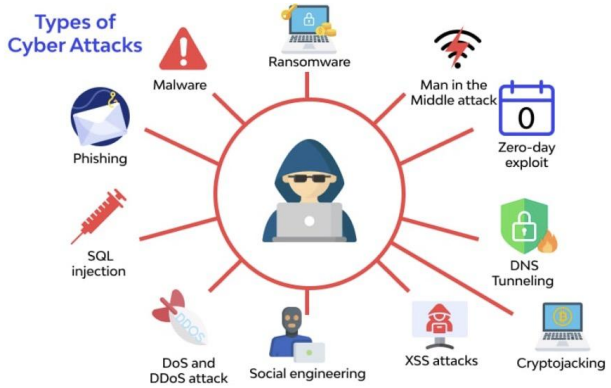
- Issues in the networks architecture can cause issues with unauthorized access or eavesdropping

- Weaknesses can be from underlying software-defined infrastructure

- Attack vectors such as network slicing vulnerabilities and threats to the Internet of Things (IoT) devices connected to 5G networks add to the complexity of safeguarding these systems

Types of Attacks

1. **Denial-of-service (DoS) attacks**
2. Distributed denial-of-service (DDoS) attacks
3. Hijacking and signaling storms
4. Resource theft
5. **Configuration attacks**
6. **Man-in-the-middle attacks**
7. Eavesdropping
8. Data exfiltration
9. Malware deployment



Attack Graphs

- Can be used to construct multi-stage attack paths where each path represents a chain of exploits that could be leveraged by an attacker to penetrate network
- Used to understand where vulnerabilities exist and how to protect important assets
- In order to find vulnerabilities, “ethical hackers” infiltrate businesses networks and create attack graphs to help uncover ways they could be attacked
- Automated attack graphing has recently become a trend as “hand done” attack graphs can include errors

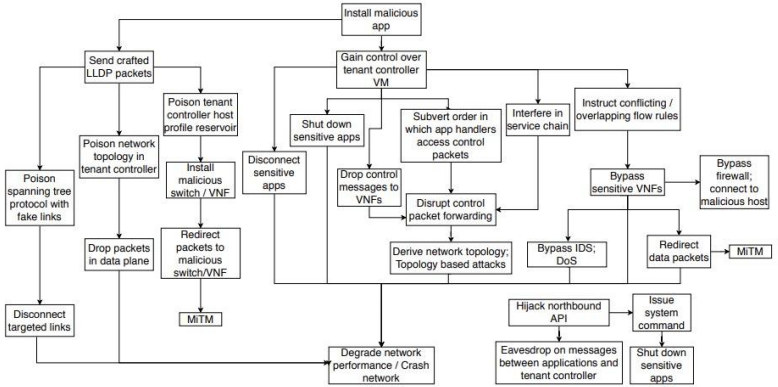


Fig. 5: Aggregated attack graph of SDN control plane vulnerabilities

Attack graph from https://arxiv.org/pdf/2108.03514.pdf

Machine Learning Implementation

Steps:

1. Selecting Programming Language
    a. May influence APIs and libraries used
2. Selecting Algorithm
    a. Important to be specific about class, type of algorithm, and specific implementations
3. Selecting Problem
    a. Finding a set of problems in which you can test/ validate the algorithm created
4. Research Algorithm
    a. Learn about the algorithm you chose from others to find other uses and potential roadblocks
5. Unit Tests
    a. Write tests for each function and know what to expect as a result from each function

Machine Learning Algorithms

- Where artificial intelligence conducts task to be able to predict output values given the input data

- These algorithms are different ways of predicting output based on the given data set

- Linear regression
- Logistic regression
- Decision tree
- SVM algorithm
- Naive Bayes algorithm
- KNN algorithm
- K-means
- Random forest algorithm
- Dimensionality reduction algorithms
- Gradient boosting algorithm and AdaBoosting algorithm