Name: Dhruva Kapadia
MIS: 111903142

ASSIGNMENT 1

The following research papers are based on 3 trends in cybersecurity:

1. Zero Trust Architecture
2. Intrusion Detection
3. Phishing attacks

1. Building A Zero Trust Architecture Using Kubernetes

Paper : https://ieeexplore.ieee.org/document/9418203
Authors: Daniel D'Silva; Dayanand D. Ambawade
Conference: 2021 6th International Conference for Convergence in Technology
Year : 2021

Summary:

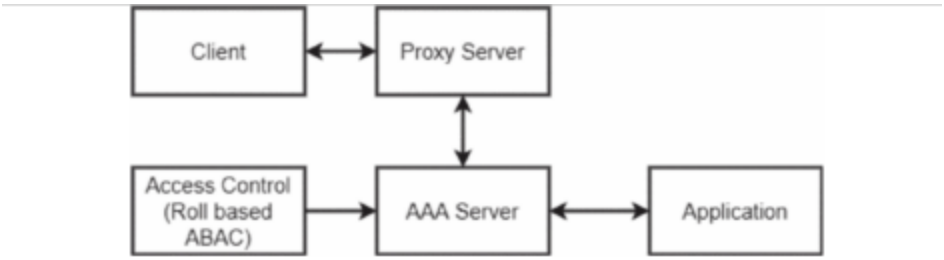
This paper proposes a zero trust model for cloud computing environments and states the advantages of using a Zero Trust Architecture for protecting any organizational data . It concludes three important properties of the Zero trust network based on literature survey of many authors which are secure access irrespective of location, access control policies and traffic logging. It shows the response of the proposed model to different types of attacks like Infiltration, Phishing, Probe attack etc.

Zero Trust: Zero trust is a cybersecurity strategy where security policies are not applied based on assumed trust instead devices and applications are periodically verified.

Zero Trust Architecture(ZTA): It comprises user and application authentication and device authentication. It keeps checking the user authenticity, monitors the user's devices, and checks for any location change initiated by the user device.

Kubernetes: Kubernetes is software that manages many server computers and runs a large number of programs across those computers. On Kubernetes, all programs run in containers so that they can be isolated from each other, and be easy to develop and deploy.

Proposed Architecture:



a. Client - Any device having a web browser

b. Proxy server - The proxy server is responsible for passing the request from the client to the Kubernetes cluster

c. AAA(Authentication, Authorization,Application) Server: It acts as the only mediator between the proxy server and the application. It contains Kubernetes software (acts as the master node)

d. Access control : AAA as well as Application server both contain this block. It assigns role based authority to clients

e. Application server: Slave nodes connected to the AAA Server.

Working:

1. Client requests a particular web page
2. The proxy server keeps track of the client page who has requested the page and forwards the Kubernetes cluster request.
3. Within the Kubernetes cluster, the Ingress accepts the request and forwards it to the Keycloak service.
4. Keycloak then validates the user through basic authentication such as ID and Password and verifies the machine's authenticity through X.509 certificates.
5. Once the user is verified, it informs Kubernetes to redirect the request to the application.
6. During this time, the Kubernetes cluster keeps track of the certificates and continually checks their authenticity.

KeyCloak - Identity and Access Management tool. The applications using KeyCloak need not deal with login forms, authenticating users and storing users.

Kubernetes Ingress - It is an API object that provides routing rules to manage external users' access to the services in a Kubernetes cluster

Outcomes:

1. The proposed model was implemented and tested against different attacks.
2. The requirement of Zero trust network over traditional RBAC(Role Based Access Control) was justified.
3. The difficulties of establishing a ZTA in existing systems were pointed out

Limitations:

Different ways of migrating to the proposed ZTA (deployment strategies) were not highlighted

2. Detecting phishing websites using machine learning technique

Paper :
https://www.researchgate.net/publication/355263255_Detecting_phishing_websites_using_machine_learning_technique
Authors: Ashit Kumar Dutta
Journal : PLOS ONE Anti-Phishing Technique
Year : 2021

Summary:

The paper proposes a novel method based on neural networks and natural language processing to detect malicious URLs and alert users. It explains the types of phishing attacks namely Technical Subterfuge and Social Engineering in brief. It mentions the three types of approaches for phishing detection which are Machine Learning, Proactive Phishing URL detection and Phishing based black and white list. Dataset used comprises Normal(Benign) dataset and Phishing Dataset. For Benign websites AlexRank is used whereas for Phishing PhishTank is used. The paper also compares various methodologies used for phishing detection till date and points out the limitations in those approaches. It also compares the results of the proposed method with different classification algorithms like Random Forest, MLP(Multi-Layer Perceptron), Decision Trees etc.]

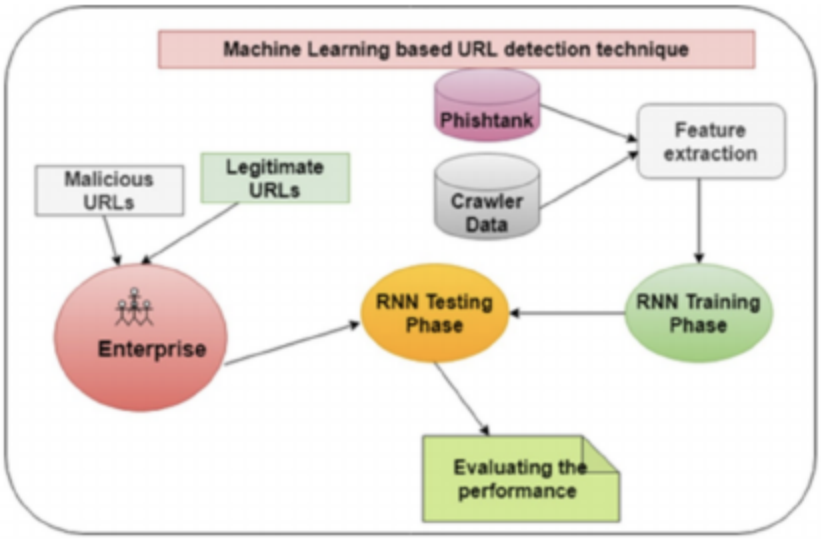
Phishing Attacks: Phishing is a cyber attack that uses email for sending malicious links or attachments. The email recipient unaware of the malicious content sent downloads the attachment or clicks on a link.

Social Engineering Attacks: In cybersecurity, Social engineering is a technique that relies on human error to gain unauthorized access to private information or systems. Eg. Malicious links sent through mails, SMS etc.

Technical Subterfuge: The attacker gains access to a system/organization by using a tool. Eg. DNS poisoning

AlexaRank: A website which contains a set of URLs with their ranking assigned

Proposed Architecture:



Working:

1. Data Collection:
    a. Develop a crawler from AlexaRank website
    b. Phishtank and Crawler are used to collect Malicious and Benign URLs .
    c. Remove Invalid URLs and count the total number of URLs
2. Data Preprocessing:
    a. For each URL, the following category of variables is selected:
        i. Address based - eg. length of url, IP address
        ii. Domain based - eg. DNS record, age of domain
        iii. HTML and Javascript based - eg. Iframe , website forwarding
    b. Total 17 features are selected and each URL is converted into a vector
3. Training:
    a. The url vectors are passed through RNN(Recurrent Neural Networks) to learn the properties of benign and malicious urls.
    b. Different sets of parameters such as epochs, learning_rate etc are passed and parameters yielding best results are selected.
4. Testing: F1-Score and Accuracy are used for evaluation purposes.

Outcomes:

1. The proposed model was compared with other existing url detectors and was found better in terms of accuracy and F1-Score.

Limitations:

1. The paper does not include literature review related to black and white list method of phishing detection.
2. It does not compare the proposed approach with other possible deep learning models like CNN etc.

3. Detecting Cybersecurity attacks across different network features and learners

Paper:
https://www.researchgate.net/publication/349546005_Detecting_cybersecurity_attacks_across_different_network_features_and_learners
Authors: Joffrey Leevy, John Hancock
Journal: Journal of Big Data
Year : 2021

Summary:

The paper proposes a novel ensemble approach for feature selection for intrusion detection systems. It uses CIC-IDS-2018 dataset for training and testing purposes. It shows the significance of the Destination Port feature for intrusion detection. It evaluates the performance of different classifiers like CatBoost , LighBGM, Decision Trees and Random Forests.

Decision Trees: It is like a tree with nodes or leaves representing class labels and branches representing observations.

Random Forests: It is an ensemble of multiple decision trees.

CatBoost: It uses Ordered Boosting, which imposes an order on the samples that CatBoost uses to fit constituent decision trees.

LightBGM: It uses Gradient-based One-Side Sampling and Exclusive Feature Bundling to handle large numbers of data instances and features. One-Side Sampling ignores a substantial portion of data instances with small gradients, while Exclusive Feature Bundling groups mutually exclusive features to reduce variable count.

Proposed Architecture:

1. Data cleaning:
    a. Timestamp column was dropped as the model should not be biased towards attack time.
    b. Protocol field was dropped as it was redundant
    c. Day 4 had a few additional columns Flow ID, Src IP, Src Port, and Dst IP which were dropped.
    d. Fields like Fwd_Header_Length, Flow_Duration, and Flow_IAT_Min had negative values in some instances. Such rows were removed
    e. Bwd_PSH_Flags, Bwd_URG_Flags, Fwd_Avg_Bytes_Bulk Fwd_Avg_Packets_Bulk, Fwd_Avg_Bulk_Rate , Bwd_Avg_Bytes_Bulk , Bwd_Avg_Packets_Bulk , Bwd_Avg_Bulk_Rate all these fields had same

value in every instance and hence they were dropped

f. Instances containing NaN, Infinity or -Infinity values were dropped

g. After data cleaning, a total of 66 features were left

2. Feature selection:

For feature selection, ensemble learning techniques were used which included supervised techniques like Random Forest, LightGBM, CatBoost, XGBoost and filter based techniques like Mutual Information, Gain Ratio and Chi-Squared.

a. The dataset was passed through all of the above 7 techniques.

b. Each technique selected 20 features except CatBoost which had selected only 14 features.

c. After obtaining the 7 rankings, feature selection techniques are used to select features that appear in k out of 7 rankings, where k has the value 4, 5, 6, or 7

d. After the above step 4 groups of features were obtained.

3. Training:

a. 11 datasets were created. First 4 were created by using the 4 groups obtained from feature selection excluding destination port, next 4 were created by using these same groups but destination port included, next dataset included all 66 features , second last dataset contained all features except destination port and the last one included only destination port as a feature.

b. Each dataset was passed as an input to 7 classifiers namely DT, RF, Naive Bayes , Logistic Regression, CatBoost, XGBoost, and LightGBM.

4. Testing: F1-Score metrics was used for evaluating all techniques

F1-Score: harmonic mean of precision and recall, is equal to 2 · Precision · Recall/(Precision + Recall)

Outcomes:

1. The paper concludes that LightBGM performs the best on the CIC-IDS-2018 dataset.
2. Destination_Port is a significant factor in the performance of models for identifying attacks is proved by evaluating the performances of 11 datasets

Limitations:

1. The paper does not mention the platform used for testing so many combinations of the dataset.
2. It does not comment about the importance of GPUs and distributed computing for training a dataset which is 6.83 GB large in size.