Machine Learning for Computer Security

Comment: The exercises are a good preparation, the Exam was very similiar. But making small errors will decide between a good grade and just a satisfactory one.

MC-Question

check all trues

a)

- ☐ loss function compares gorund true label and predicted label
- ☐ penalties are a regularization technique used against overffitings
- ☐ cross-validation is technique for tuning hyperparameters
- ☐ unsupervised learning uses labels

b)

- ☐ two class svm is not suitable because of class imbalance
- ☐ machine learning for android malware detection features from API calls and permission
- ☐ ROC curves are not relevant for analysing perfomance
- ☐ android malware detection models generaluze well to future malware

c)

- ☐ scaling and nomalization is to assure that all features contribute equally
- ☐ to reduce dimensionality feature selection is used
- ☐ bag of words does not take the order words into account
- ☐ hashing features convert numerical into categorical values

d)

- ☐ semantic gap is the difference between attacks and benign anomalies
- ☐ center of neighborhood uses k neares neigbhours with k as regulasation parameter
- ☐ anomaly detection assumes that normal data and anomlies have the same statistical properties
- ☐ Anomaly detection can not be used for unknown attacks

Embeddings

- given E calculate using one hot vectors the embeddings
- draw these vectors
- calculate cosine similarity (equation not given) between Embeddings
- give the equation for the simplified skip gram model for p(wo, wi) in term of P, E

Classification

- dataset with points given, draw positive and negatives
- calculate the empirical risk of the dataset
- calculate the two first perceptron update steps
- how many steps does the perceptron take to converge

Clustering

- Points in a feature space given as drawing
- Perform complete linkage clustering and give the set notation for each step
- Draw the dendogram and mark the slicing point for 3 clusters
- Mark the clusters in the given plot
- Design a function D(A,B) that gives the distance between the centroids of the two clusters A,B. You can use d(a,b) as the distance between two points

Graph Algorithms

- AST Graph given (more complicated than in the exercises)
- Write the corresponding C Code (use function calls!)
- Implement the Control Flow Edges (the AST includes nested ifs and logical AND)

Performance Metrics

- Give the Equations for Precision and Recall in terms of TP, FP, TN, FN
- Why is the harmonic mean beneficial in the F1 score compared to the arithmetic mean
- Given benign and malicious points in a circular feature space: Draw the Precision Recall Curve

Adversarial Machine Learning

- Given a classification function $f(x) = (w_1 x_1)^3 + (w_2 x_2)^3 + b$, θ and points, evaluate the function
- Calculate the gradient with respect to x and the model parameters θ
- Apply a given Fast Gradient Adversarial function to calculate an x with minimum pertubation
- Apply the classification function to the pertubated x and compare it to the original f(x)