MACHINE LEARNING PROJECT

Vasisht Duddu::2015137
Shubham Khanna::2015179
Anubhav Jain::2015129

MACHINE LEARNING IN CYBERSECURITY

PROBLEM STATEMENT

With the advancement of technology, security of systems and detection of attacks are crucial. As part of the semester course project, we would like to use machine learning techniques to implement a cybersecurity tool comprising:

->Virus and Malware Detection (Classification)
  Classify PE32 executables as malware/not malware
->Network Anomaly Detection (Classification)
  Detect attacks on networks using datset containing trafic logs and connections

LEARNING ALGORTIHMS

->Naive Bayes
->Decision Trees
->Logistic Regression
(We will choose the most optimal algorithm among the above mentioned)
->SVM
->Random Forest (Will use ensemble approaches)

TRAINING APPROACHES

We would like to try both Stochastic Gradient Descent and Batch Gradient Descent.

MODEL SELECTION AND PARAMTER TUNING

We would try various models(linear, nonlinear and Gaussian) and use cross validation to choose the optimal values.

DATASET AND CODE

All the code and Datsets will be available at:
->https://github.com/vduddu/MachineLearning/tree/master/MLSec