SEADer: A Social Engineering Attack Detection method based on Natural Language Processing and Artificial Neural Networks

August 2019

Decision Tree: 0.918

Random Forest: 0.917

Multi-Layer Perceptron: 0.925

Dataset “*SEADER”*

After the pre-processing of the dialogues (steps 1 – 11), the classification dataset has

the following 4 labels: (1) Intent, (2) Spelling, (3) Link and (4) attack or no attack.

The SymSpellpy library (a Python port of SymSpell) was used for spelling, the Web of Trust (WOT) Application Programming Interface (API) was used to check any links and finally the SciKit library for the MLP classifier.

compound dataset is based on the 147 entries plus 600 entries from customer support-based tweets from Twitter, none of which are classified as attacks.

* Compound dataset results a higher accuracy.