Summary of attempt Two

Writer: Date: 25/05/2021

Fan Zhang

Tianlei Qi

First prediction attempt

LSTM (1085 test samples)

Top-10: 10.63%

Top-50: 31.91%

Top-100: 42.55%

Top-150: 53.19%

Top-200: 61.7%

Top-1% : 10.63%

Top-10%: 42.55%

Top-50%: 85.7%

Top-70%: 93.61%

RF (621 test samples)

TOP-10:9%

TOP-50:27%

TOP-100:31.8%

TOP-150:34%

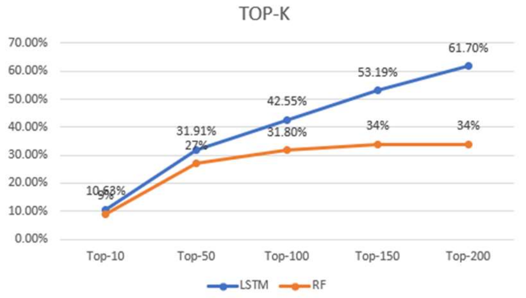
TOP-200: 34%

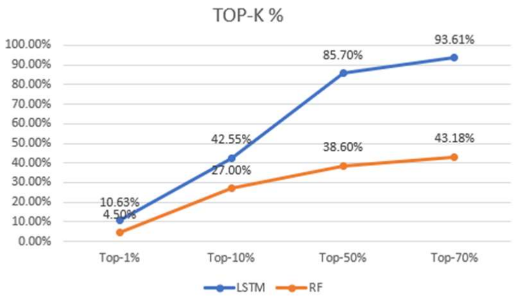
Top-1% : 4.50%

Top-10%: 27.00%

Top-50%: 38.60%

Top-70%: 43.18%





What have we fixed and improved from previous attempt?

Our last attempt of Random Forest method generated abnormal results which is significantly higher than the paper's result. After reviewing our process and compare with the paper process, we found that the utilization of source code data doesn't match the paper description. The paper described a proxy tool (Understand) for extracting the code metric. However, our approach used the extracted AST from codesenor as representations and trained with Random Forest Algorithm which explains the differences between our two attempts.

What do you think of the performance of the detection? Is it good or not good? Why?

From the result accuracy point of view, the LSTM method has a better performance compared to the RF method due to the higher Top@K values.

From the efficiency point of view, the LSTM utilized lower CPU resource and shorter execution time than the RF method.

What is your conclusion? Could you give the final conclusion about the method based on the current result?

Our second attempt has similar result compare with the paper. This can be demonstrated by our result curve has similar pattern with paper provided.

The similar results of LSTM and RF could support the credibility of the paper method. Therefore, our conclusion of current stage is that the paper has provided a valid dataset and valid vulnerability detection methods.