A Novel Approach to Clustering Malware Behaviour to Improve Malware Detection

Rebecca Merriman

Technical Report

RHUL–ISG–2020–6

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

My project objective is to implement clustering for operations of three different types of malware, specifically Ransomware, Backdoor and Trojan in order to evaluate the accuracy of clustering-based malware detection to then conclude using these results and results from other papers whether clustering malware behaviour improves malware detection.

To meet this aim, smaller objectives need to be met. My objectives include reviewing existing literature on Ransomware, Trojans, Backdoors and clustering and then implementing the clustering process of Ransomware, Backdoor and Trojan families from behaviour profiles (produced from static and dynamic analysis) to validation/results. The results are critically compared and the accuracy of clustering-based malware detection from my and other results is evaluated.

Ransomware, Backdoor and Trojan are all types of malware. Malware is malicious software which undermines the security of users by performing unwanted functions. The clustering of Ransomware, Backdoors and Trojans were compared because they can work alongside each other to infect a victim's system. Ransomware can be used to install Backdoors into a system and Trojans can be used to deliver Backdoors or Ransomware into a system.

In this project, the clustering process was carried out on 3 malware families (Ransomware, Trojans and Backdoor), making sure that samples in the same cluster were as similar as possible and samples in a different cluster were as dissimilar as possible. 12 experiments were run all together and the best clustering for each of the different types of malware for each of the validation metrics was evaluated. The best clustering according to all the FMS, F1, ARI and SC scores for Ransomware was the Uni-gram with the system call representation of Category and vector representation of Frequency Vector, for Backdoor it was the Di-gram with the system call representation of Full Representation and vector representation of Frequency Vector and for Trojan it was the Tri-gram with the system call representation of Category and vector representation of Frequency Vector.

The main finding was that there is a discrepancy with the accuracy of clustering-based malware and whether clustering improves malware detection. The accuracy of clustering-based malware detection is highly subjective as it depends on many factors including the type of machine learning algorithm, the features selected, the feature selection methods, the model construction methods and evaluation metrics. This is illustrated in my results where the different methods of feature selection and vector representation yielded different results (scores and best clustering methods) for the validation metrics and the accuracy was low. In contrast other papers used different methods and found that accuracy was high, providing evidence for this subjectivity and conflicting findings. Therefore, future research should be conducted to find out all the reasons that may affect the accuracy of clustering malware and discover the best methods in terms of accuracy and a good run time for clustering malware to improve malware detection. This will then help to conclude whether clustering improves malware detection or not.