Optimizing Decision Tree in Malware Classification System by using Genetic Algorithm

Mohd Najwadi Yusoff and Aman Jantan
School of Computer Science,
Universiti Sains Malaysia,
Penang, Malaysia.
{najwadi,aman}@cs.usm.my

ABSTRACT
Malware classification is a vital component and works together with malware identification to prepare the right and effective malware antidote. Current techniques in malware classification do not give a good classification result while dealing with new as well as unique types of malware. In general, these kinds of malware are highly specialized and very difficult to classify. Therefore, this paper proposed the usage of Genetic Algorithm (GA) as an approach to optimize Decision Tree (DT) in malware classification. GA is chosen because unique types of malware are basically functioning like crossover and permutation operations in GA. New classifier is developed by combining GA with DT that we called as Anti-Malware System (AMS) Classifier. Experimental results obtained from AMS Classifier and DT are compared and visualized in tables and graphs. AMS Classifier shows an accuracy increase from 4.5% to 6.5% from DT Classifier. Outcome from this paper is a new Anti-Malware Classification System (AMCS) consists of AMS Classifier and new malware classes that we named as Class Target Operation (CTO). Malware is classified by using CTO which are mainly based on malware target and its operation behavior.

KEYWORDS
Malware classification, Genetic Algorithm, optimization, unique malware