Short review on metamorphic malware detection in Hidden Markov Models

ABSTRACT

Metamorphic malware is well known for evading signature-based detection. To cope up with numerous malware which can emerge easily by using open source malware generator, efficient detection in terms of accuracy and runtime performance shall be considered during analysis. Detection strategies such as data mining combine with machine learning have been used by researchers for heuristically detecting malware. In this paper, we present Hidden Markov Model as an efficient metamorphic malware detection tool by exploring the common obfuscation techniques used in malware while reviewing and comparing the different studies that adopt HMM as a detection tool.

Keyword: Metamorphic; Malware; Hidden markov models; Obfuscation; Heuristics