World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:04, 2017

Metamorphic Computer Virus Classification Using Hidden Markov Model

Authors : Babak Bashari Rad

Abstract : A metamorphic computer virus uses different code transformation techniques to mutate its body in duplicated instances. Characteristics and function of new instances are mostly similar to their parents, but they cannot be easily detected by the majority of antivirus in market, as they depend on string signature-based detection techniques. The purpose of this research is to propose a Hidden Markov Model for classification of metamorphic viruses in executable files. In the proposed solution, portable executable files are inspected to extract the instructions opcodes needed for the examination of code. A Hidden Markov Model trained on portable executable files is employed to classify the metamorphic viruses of the same family. The proposed model is able to generate and recognize common statistical features of mutated code. The model has been evaluated by examining the model on a test data set. The performance of the model has been practically tested and evaluated based on False Positive Rate, Detection Rate and Overall Accuracy. The result showed an acceptable performance with high average of 99.7% Detection Rate.

Keywords : malware classification, computer virus classification, metamorphic virus, metamorphic malware, Hidden Markov Model
Conference Title : ICCITIA 2017 : International Conference on Computer and Information Technologies, Innovations and Applications
Conference Location : Boston, United States
Conference Dates : April 24-25, 2017