Abstract

The alarming rise in the number of computer security incidents since the late 80's had inspired researchers to devise new mechanisms for detection and containment of malwares like worms and viruses. Traditional approaches like worm signatures are helpless against new age polymorphic and metamorphic worms. Design and implementation of an anomaly based detection system seems is a difficult task due to the difficulty in defining a normal model.

There have been attempts to generate vulnerability signatures for vulnerable application against and metamorphic worms attacks. It has however not been possible to generate compact vulnerability signatures that can be used for efficient filtering of exploit message packets. Protocol level vulnerability signatures has come out as a possible solution to this. However no efficient scheme for such vulnerability signature generation has far been developed.

It has been our endeavor to work towards development of a scheme for effective and fast generation of protocol level vulnerability signatures. The signature generation here requires static as well as dynamic analysis of the binary executables of the vulnerable program. For the static analysis we take the CFG of the program. As part of this work, in this project, we develop a module for merging of input independent paths and the loops so as to reduce the search space.