

Learning Program Behavior for Intrusion Detection

Abstract:

A new approach, based on the k-Nearest Neighbor (kNN) classifier, is used to classify program behavior as normal and intrusive. Short sequences of system calls have been used to characterize a program's normal behavior. However, separate databases of short system call sequences have to be built for different programs, and learning program profiles involves time-consuming training and testing processes. With the kNN classifier, the frequencies of system calls are used to describe the program behavior. Text categorization techniques are adopted to convert each program execution to a vector and calculate the similarity between two program activities. Since there is no need to generate individual program profiles, the calculation involved is largely reduced. Preliminary experiments with 1998 DARPA BSM audit data show that the kNN classifier can effectively detect intrusive attacks and achieve a very low false positive rate.