Abstract

In this we present an efficient solution for eliminating false positives in intrusion detection systems using a parallelized version of Genetic Algorithm. Genetic algorithm uses selection, mutation and crossover operations eliminating most of the false positives in a reasonable time. Almost all existing versions are sequential without exploiting the capabilities of newer multiprocessors or distributed systems. By parallelizing genetic operations in the context of intrusion detection systems we reduce the total complexities. This parallelized approach gives better solution than sequential one by taking advantage of the parallel architecture. We propose the use of cache oblivious technique in our algorithm to provide efficient memory transfers. The complexity of this algorithm is $O((N/B) \log M/B N^{1/3} + N^{1/3})$ which is very much lesser when compared to other sorting algorithms.

Reference

Transactions on Information and System Security (TISSEC) 3(3), 186-205.


http://www.infoworld.com/cgi-bin/displayTC.pl?/980504sb3-ibm.htm.


Index Terms

Computer Science
Architectures
Processor

Key words
Cache Oblivious

Clustering

Genetic algorithm

False Positive

Funnel Sort