A CREDIBLE COST-SENSITIVE INTRUSION RESPONSE SYSTEM

Abstract

With the growth of modern systems and infrastructures, the rate of intrusion has being on the increase. Intrusion response system plays a paramount role in counter measuring against any detected intrusion or cyber-attacks by the intrusion detection system. The problem of intrusion response system is that when the responses are deployed against a detected intrusion, they often alter the state of the system negatively, affecting resources and leading to damage. Intrusion response system needs to maximize security goal while minimizing costs. Defining an accurate measurement of these cost factors and ensuring consistent assessment across various computing environments are common challenges in using a cost-sensitive approach. In this work, an adaptive and cost sensitive intrusion response system (ACOS_IRS) was design in order to correct these problems. The architecture of ACOS_IRS was divided into two major phases namely: intrusion detection system and intrusion response engine. The intrusion response engine phase comprises of the five sub-components: alert filter/correlation module, response manager, database, cost sensitivity evaluation module, adaptability and response deployment module. Once an intrusion has been detected, intrusion detection system raises alert and then passes the attack specific parameters to the Alert Filter and correlation module. In the alert filter/correlation module, the dimension of these alerts is then reduced using principal component analysis algorithm so as to ultimately reduce the number of feature used for classification. Neural network machine learning algorithm was used to build a classifier that automatically distinguishes true and false positives alert. The cost metric for assessing cost of responses deployed was based on three factors: the cost of damage caused by the intrusion, the cost of automatic response to an intrusion and the operational cost. This approach provides consistent basis for response assessment across different systems and environment while allowing the response cost to adapt to system environment. The adaptability of the response is based on the effectiveness of the previous response action and feedback received. Java 1.1.8 will be used for implementation and a Knowledge Discovery in Database (KDD) benchmark dataset will also be used for evaluation. The experiments will be conducted by simulating the network attacks and testing the response behaviors. The initial result shows efficient response systems which can responds quickly enough to thwart active attacks in real time.