Abstract

In this paper, we suggest a multi-dimensional approach towards intrusion detection. Network and system usage parameters like source and destination IP addresses; source and destination ports; incoming and outgoing network traffic data rate and number of CPU cycles per request are divided into multiple dimensions. Rather than analyzing raw bytes of data corresponding to the values of the network parameters, a mature function is inferred during the training phase for each dimension. This mature function takes a dimension value as an input and returns a value that represents the level of abnormality in the system usage with respect to that dimension. This mature function is referred to as Individual Anomaly Indicator. Individual Anomaly Indicators recorded for each of the dimensions are then used to generate a Global Anomaly Indicator, a function with n variables (n is the number of dimensions) that provides the Global Anomaly Factor, an indicator of anomaly in the system usage based on all the dimensions considered together. The Global Anomaly Indicator inferred during the training phase is then used to detect anomaly in the network traffic during the detection phase. Network traffic data encountered during the detection phase is fed back to the system to improve the maturity of the Individual Anomaly Indicators and hence the Global Anomaly Indicator.
References


**Index Terms**

Computer Science Security

**Keywords**

Multi-dimensional Approach Principal Component Analysis Feature Global Anomaly Indicator Individual Anomaly Indicator

Global Anomaly Factor

Individual Anomaly Factor