A detailed description on unsupervised heterogeneous anomaly based intrusion detection framework

ABSTRACT

Observing network traffic flow for anomalies is a common method in Intrusion Detection. More effort has been taken in utilizing the data mining and machine learning algorithms to construct anomaly based intrusion detection systems, but the dependency on the learned models that were built based on earlier network behaviour still exists, which restricts those methods in detecting new or unknown intrusions. Consequently, this investigation proposes a structure to identify an extensive variety of abnormalities by analysing heterogeneous logs, without utilizing either a prepared model of system transactions or the attributes of anomalies. To accomplish this, a current segment (clustering) has been used and a few new parts (filtering, aggregating and feature analysis) have been presented. Several logs from multiple sources are used as input and this data are processed by all the modules of the framework. As each segment is instrumented for a particular undertaking towards a definitive objective, the commitment of each segment towards abnormality recognition is estimated with various execution measurements. Ultimately, the framework is able to detect a broad range of intrusions exist in the logs without using either the attack knowledge or the traffic behavioural models. The result achieved shows the direction or pathway to design anomaly detectors that can utilize raw traffic logs collected from heterogeneous sources on the network monitored and correlate the events across the logs to detect intrusions.

Keyword: Anomaly detection; Clustering; Heterogeneous logs; Filtering; Feature analysis