A survey of intrusion alert correlation and its design considerations

Abstract

In recent years, network intrusion attempts have been on the rise. Malicious attempts, including hacking, botnets, and worms are used to intrude and compromise the organization's networks affecting their confidentiality, integrity and availability of resources. In order to detect these malicious activities, intrusion detection systems (IDSs) have been widely deployed in corporate networks. IDS sends alerts to security personnel in case of anomalous activities in the network. Unfortunately, one of the IDSs' drawbacks is they produce a large number of false positives and non-relevant positives alerts that could overwhelm the security personnel. Existing efforts to address this are done via identification of the similarities and causality relationships between alerts, grouping them into different clusters and prioritizing them after conducting the assessment on them. In this paper, we present commonly used alert correlation approaches and highlight the advantages and disadvantages from various perspectives. Existing alert correlation models are critically reviewed and compared in this paper. Subsequently, we emphasize four main considerations in alert correlation design which are: attack scenario either single packet or multi-stage attack, its architecture either centralized or distributed, performance assessment on accuracy of alert detection, and its processing time and the data to be used for testing.