Abstract: Recently, there has been a rapid growth in cloud computing due to their ability to offer computing and storage on demand, its elasticity, and significant reduction in operational costs. However, cloud security is a grand obstacle for full deployment and utilization of cloud services. In this paper, we address the security of the DNS protocol that is widely used to translate the cloud domain names to correct IP addresses. The DNS protocol is prone to attacks like cache poisoning attacks and DNS hijacking attacks that can lead to compromising user's cloud accounts and stored information. We present an anomaly based Intrusion Detection System (IDS) for the DNS protocol (DNS-IDS) that models the normal operations of the DNS protocol and accurately detects any abnormal behavior or exploitation of the protocol. The DNS-IDS system operates in two phases, the training phase and the operational phase. In the training phase, we model the normal behavior of the DNS protocol as a finite state machine and we derive the normal temporal statistics of how normal DNS traffic transition within that state machine and store them in a database. To bound the normal event space, we also apply few known DNS attacks (e.g. Cache poisoning) and store the temporal statistics of the abnormal DNS traffic transition in a separate database. Then we develop an anomaly metric for the DNS protocol that is a function of the temporal statistics for both the normal and abnormal transitions of the DNS by applying classification algorithms like the Bagging algorithm. During the operational phase, the anomaly metric is used to detect DNS attacks (both known and novel attacks). We have evaluated our approach against a wide range of DNS attacks (DNS hijacking, Kaminsky attack, amplification attack, Birthday attack, DNS Rebinding attack). Our results show attack detection rate of 97% with very low false positive alarm rate (0.01397%), and round 3% false negatives.

Bio:.