ABSTRACT

Anomaly detection systems based on various soft-computing techniques like Genetic algorithms, Neural networks and Fuzzy logic exist in the literature. However, they are not as successful as misuse detection systems due to various parameters like detection time, accuracy, implementation delay, etc. Hence a Genetic-aided fuzzy-based anomaly detection system is proposed in this thesis. Such an anomaly detector shows better accuracy at a relatively lesser detection time. A similar study came in handy by modeling the detection of attacks by a misuse detection system using colored petrinets thus experimenting on commercially available misuse detectors like Snort and Bro.

When all the above systems were designed and aimed to operate at the Network layer, a need for an intrusion detection system that operates at the application layer arises as these network layer detectors do not aim at detecting protocol specific attacks. The need for such a system at the application layer is more relevant as they are exposed to maximum abstraction, and the state-of-art solutions are incapable of detecting misuses in these layers. This thesis explores the prospects of having a misuse detection system that operates on the application layer protocols like HTTP, FTP, etc. It is well known that all misuse detection systems work on the concept of storing signatures that represent an attack pattern or misuse, which are later matched inline using trivial pattern matching algorithms with the incoming network stream for detection. However, the forms of attacks that are detected are restricted to those that have a syntactic match with the signatures only in the network layer.
It was understood that attacks at application layer are not trivial to be matched syntactically for detection, but needs a contextual way of understanding them, thus leading to a study of the need of semantics at application layer. A semantic anomaly detection system was designed using statistical distances and a semantic misuse detector that operates on HTTP was implemented. These paved way for design of a generic application layer semantic rule language. The design proposed in this thesis uses protocol analysis to define contextual constraints on these signatures based on the semantics of the attacks, thereby increasing the intelligence of such a system by detecting more misuses at a different layer of study. Such a system when appended with the existing network security infrastructure detects different classes of attacks that appear at the application layer which could never have been detected, thereby considerably increasing the detection rate. Protocol analysis provides means to reconstruct the protocol context of communication session from an ongoing network stream or trace, which when employed with a misuse detection system considerably reduces the false positives and false negatives.