Modular framework for traffic inspection and interactive management

S. Shiva, C. Ellis, V. Datla, H. Bedi, and S. Roy

Cyber attacks have created a global threat, both in defending local and global networks. Attacks are becoming more sophisticated and possess the ability to spread to numerous vulnerable hosts in a matter of seconds. It is essential to provide tools necessary in detecting, classifying, and defending from various types of attacks. A variety of taxonomies aim at classifying vulnerabilities or attacks, but to date they have limitations in providing a defense strategy that can be used in a local application setting. This can be due to the enormous possibilities of defense strategies. Limitations exist toward providing defense strategies within an attack taxonomy. This presents an invaluable research area focused on the information a network administrator can apply when attempting to defend the network against cyber attacks.

It is towards this end that we propose a modular framework in which arbitrary elements can be introduced in order to evaluate the effectiveness and scalability for game theoretic defense measures and traditional network assessment. Further, we plan to introduce a game theoretic decision framework to provide future assessments on the feasibility of utilizing game theory as a defense tool.