Abstract

Cyber security has always been a challenge. The advances in networks, operating systems, and personal computers go head to head with increasing complexities of cyber attacks. Therefore, methods of assessing cyber security are crucial in order to operate networks in high levels of confidentiality, integrity and availability.

The frameworks developed to assess cyber security give an indication of the security level. Therefore it can suggest improvement to network designs. The frameworks depend on attacker modeling techniques such as stochastic Markov Chains, Petri Nets, Attack Graphs, Bayesian Networks, and Attack Trees. These models map the actual attacks process into comprehensive models. Although, these techniques successfully mapped the attack process but they could not correctly model the attack behavior. This gap was filled by Game theory analysis which can model the attacker behavior in terms strategy of selecting between attacks.

Game theory models the interaction between the attackers, and the defender of a network. The attacker objective is to maximize his rewards. The defender, however, aim to minimize this reward. The game payoff, reward and cost, values can either be generic or relate to the network under consideration. They can be operational measure like bandwidth, performance measures like down time, or resources spent in deploying the attacks.

A DNS server is analyzed using a stochastic Markov Chain model with cache poison attack as a source of failure. The attacker behavior is analyzed using a dynamic zero-sum game. Two of the performance metrics were studied which gave an indication of the security level. These are Mean Time to Failure and Mean Time to First Failure.

Software was developed to solve the model analysis. Furthermore, an improvement to the model is proposed where payoff values of the game were assigned utilizing attack and restoration rates on the DNS instead of the generic values presented in the original model. The results showed that cost to reward ratio are dominating factor in deciding the outcomes of the game model.