Literature Survey

- An effective method to detect stepping-stone intrusion (SSI) is to estimate the length of a connection chain. This type of detection method is referred to as a network-based detection approach. Existing network-based SSI detection methods are either ineffective in the context of the Internet because of the presence of outliers in the packet round-trip times (RTTs) or inefficient, as many packets must be captured and processed. Because of the high fluctuation caused by the intermediate routers on the Internet

  In the paper "Matching TCP/IP Packets to Detect Stepping-Stone Intrusion" by Jianhua Yang, and Shou-Hsuan Stephen Huang author suggest using the technique of matching the TCP/IP Protocols using a Step-Function method, to detect network attackers from using a long connection chain to hide their identities when they launch attacks. The objective of the method is to estimate the length of a connection chain based on the changes in packet round trip times. The key point to compute the round-trip time of a connection chain is to match a Send and its corresponding Echo packet.

  In detection of stepping stone intrusion using TCP/IP packet matching algorithm here we estimate the length of downstream TCP/IP packet to find stepping stone intrusion using SDC and SWAM algorithms. Where the disadvantages of SDC are overcome by SWAM algorithm. This new algorithm SWAM uses slide window format. The proposed approach algorithm can detect stepping-stone intrusion and resist intruders' time-jittering and chaff perturbation manipulation to some extent.

  In the research paper "Mining Network Traffic with the k-Means Clustering Algorithm for Stepping-Stone Intrusion Detection" by Lixin Wang, Jianhua Yang, Xiaohua Xu, and Peng-Jun author suggest using k-means clustering algorithm which can accurately determine the length of a connection chain without requiring a large number of TCP packets being captured and processed, so it is more efficient. This algorithm is also easier to implement than all existing approaches for stepping-stone intrusion detection. The effectiveness, correctness, and efficiency of our proposed detection algorithm are verified through well-designed network experiments

  In the research "Modelling and Detecting Stepping-Stone Intrusion" by Yong Zhong Zhang, Jianhua Yang, Chumming Ye the author the propose the idea applying signal processing technology to stepping-stone intrusion detection. Here the author presents 4 model to detect intrusion they are mainly Sequence Model, Pair Model, RTT model, Pair Model.

In the research paper “Modelling Stepping Stone Attacks with Constraints in Cyber Infrastructure” the author models and analyses scenarios wherein an attacker employs multiple strategies to choose stepping stones. The problem is modelled as an Adjacency Quadratic Shortest Path using dynamic vulnerability graphs with multi-agent dynamic system approach. Using this approach, the shortest stepping stone attack with maximum node degree and the shortest stepping stone attack with maximum impact are modelled and analysed.