Abstract

Now-a-days to increase the computation efficiency distributed systems are used in which the computing resources are shared among several systems. Such openness of distributed system leads to increase in potential attacks on the hardware and software by exploration of system vulnerability. This paper presents implementation of Intrusion Detection System (IDS) to model the behavior of users using Hidden Markov Model (HMM). This model attempts to detect intrusive attack efficiently. The IDS is an identification system which can be characterized by probabilities of false acceptance and false rejection. False acceptance means that the IDS allow intruders to continue their activity. False rejection means that the IDS stops the activity of a legitimate user. IDS can be developed by adoption of an appropriate mathematical model that allows us to generate user profiles efficiently and facilitates an effective and accurate decision-making process for intrusion detection. Due to the nondeterministic nature of user behavior, the decision about intrusive or nonintrusive behavior must take into account all evidence for and against the claim. So the probabilistic approach is to be implemented to model user profile to detect attack.

References
- Nong Ye, Xiangyang Li, Qiang chen, Sayed Masum Emran and Ming ming Xu "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data." IEEE Transaction Systems, mans and cybernetics

Index Terms

Computer Science
Security
Keywords
   Intrusion detection System  Anomaly detection technique  Hidden Markov Model
KDD Cup 1999 data set