An Approach for Collaborative Decision in Distributed Intrusion Detection System

Abstract

Computers have virtually changed every aspect of our life. The rapid growth in the development of computers was focused on making the computer easy to use for all. The rapid growth did not give as much importance on the security of the computer system thereby leaving system as vulnerable to attacks. As internet and its applications are increasing, complex and hybrid networks are being used for communication. So many loopholes are being explored to intrude into other systems. There are many tools and techniques available for securing networks like Firewalls, IDS etc. and until now they are used very frequently by nearly all the organizations to safeguard information and other critical data but these are not sufficient for implementing complete security because the intruders have become smarter.

Higher security being the priority of many organizations has led to the importance and promoting active research on efficient Intrusion Detection Systems. To deal with various types of attacks we need to have information of attacks from other sources as well. This can be done by sharing intrusion information with all. As hackers are becoming more intelligent we need to
have collaborative decision making system where intrusion activity is decided by knowing other’s opinion as well. We have proposed an approach to enhance the collaborative decision making by conducting polls between registered intrusion detection systems in the network. Intrusion activity for new packets and false positives is decided based on all opinions gathered from registered intrusion detection systems.

References


Index Terms

Computer Science  Security

Keywords

Distributed IDS, Anomaly detection