Tremendous efforts have been taken over many years to secure the network against attacks; still attackers are successful with painful frequency. Experienced attackers try to disable the Intrusion Detection System (IDS) before launching attack. Therefore there should be some mechanism in IDS for uninterrupted detection of intrusion even though failure in IDS has occurred due to attacks. This paper presents the design and implementation of Novel Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tables. Proposed architecture is immune to both, failure of IDS components and compromised IDS components. This architecture is capable of restricting the effect of network attacks like DoS, DDoS and Probing to a subset of network. Experimental results prove the usefulness and efficiency of this architecture.
Reference

- Xiaohong Qu, Zhijie Liu, Xiaoyao Xie, “Research on Distributed Intrusion Detection System Based on Protocol Analysis”, IEEE 2009

Index Terms

Computer Science  Network Security
Key words

Firewall
Intrusion-Tolerance
DoS attack
NIDS
Distributed IDS