Abstract

Proliferation of heterogeneous network systems and increasing usage of Internet makes network security issue to be more and more important. Intrusion detection systems (IDS) are increasingly a key part of system defense, often operating under a high level of privilege to achieve their purposes. In accordance with the increasing importance of intrusion detection systems (IDS), users justifiably demand the trustworthiness of the IDS. However, IDS
themselves are prone to various attacks and it becomes the natural primary target of hostile attacks with the aim of disabling the detection feature and allowing an attacker to operate without being detected. This paper suggests that intrusion detection system (IDS) must be fault tolerant; otherwise, the intruder may first subvert the IDS then attack the target system at will. Making an IDS fault tolerant [2] is a challenging task. The aim of this research paper is to enhance the fault tolerance of IDS using AES and DES based heartbeat events. Brute Force attack has been simulated and the effectiveness of encrypted heartbeat event based fault tolerance for Intrusion Detection System is evaluated.

Reference

2000.

Index Terms

Computer Science Wireless
Key words

Intrusion Detection System
Heartbeat Message
Fault tolerance
Integrity Checking
AES
DES