Performance Analysis of Swelling Elastomer Seals in Petroleum Applications

Haifaa AL Hassani

Abstract

Wireless Local Area Networks (WLANs) are vulnerable to various types of attacks, such as intercepting sensitive information transmitted between two wireless devices, violating the privacy of legitimate users, and preventing access to network resources. Encryption, authentication, and Medium Access Control (MAC) address filtering are the basic ways to secure and protect WLANs. Each of these mechanisms has weaknesses and susceptible to various attacks targeting confidentiality, integrity and authenticity. Honeypots are trap networks used to seduce attackers to break in and it permits network administrators to study and analyze attackers’ motives and techniques. Wireless honeypots were recently introduced to benefit from honeypot’s objectives in the wireless world. This project investigates the effectiveness of using wireless honeypots in detecting specific WLAN attacks. To conduct the investigation, two wireless honeypot systems have been implemented. The first one uses fake access point and the other one uses a real access point. Nagios is an open source tool that has been used as monitoring and alerting tool on both implemented wireless honeypots.

Several experiments were conducted in the course of this investigation. Some attacks were successfully discovered by the help of Wireless honeypot, some other attacks went undetected. Attacks such as ping flood and MAC address spoofing were successfully detected. Unfortunately, detection of some other attacks wasn't achieved because of some limitations in the tools used in the experiments. The investigation concludes that attacks on WLANs can be detected in specific situations when wireless honeypot is implemented using compatible tools with more advanced features.