SYNFloodAlert: A Novel Sliding-window Algorithm for Fast Detection of SYN Flooding Attacks

(ROI # 2007-03)

Description

- SYNFloodAlert is an algorithm for fast detection of SYN flooding attacks or traffic overloading on TCP/IP based network devices. SYNFloodAlert uses function approximation to predict the number of SYN packets entering and leaving the incomplete connection queue based on a moving window. Discrepancy in the number of SYN packets entering and leaving the incomplete connection queue of a network device signals anomalies.

Advantages

- SYNFloodAlert algorithm is not susceptible to SYN flooding attacks because it is a stateless algorithm, meaning that it does not allocate memory resources for each new TCP connection on a network device.
- The algorithm can be easily installed as an application over any operating system on the network device.
- The algorithm becomes immediately operational on installation because it does not require separate offline training sessions to identify SYN flooding attacks.
- The algorithm allows automatic enhancement or relaxation of security settings through tunable parameters.

Performance Summary

- Results on seven test datasets containing SYN flooding attacks and normal background Web traffic showed that the SYNFloodAlert algorithm has 100% attack detection accuracy with a false alarm rate as low as 0.021 and with an average attack detection delay of 116 seconds.

Areas of Application

- SYNFloodAlert can be used to detect SYN flooding attacks on Web servers and routers; it can also be used to balance load on network services. It can be integrated with Intrusion Prevention Systems (IPS) to monitor network devices for SYN flooding.

Patent Status

- Two issued patents: US 8,127,357 and US 7,865,954