Abstract

Streathly Denial of Service (DDS) attacks are a complicated threat to the event. Now days, there are an increasing number of DDS attacks against on-line application and Web services. Detecting application layer DDS attack is a hard task. In this, its detection scenario based on the information theory depends on metrics. It has two phases: Behavior monitoring and Detection. In the first phase, the Web user commerce behavior is access from the system log during safe cases. Depends on the observation, Entropy of requests per session and the trust score for each user is evaluated. In the second phase, the suspicious requests are identified depends on the changes in entropy and a rate limiter is identified to downgrade services to malicious attackers. A scheduler is included to planning the session based on the trust score of the user and the system workload.

References
9. Raja Azrina Raja Othman “Understanding the Various Types of Denial of Service Attack “.

Index Terms

Computer Science
Networks

Keywords

Sophisticated attacks strategy, Low-rate attacks, Intrusion detection, DDS, Application Layer & Entropy.