SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks

Abstract

—Application layer distributed denial of service (DDoS) attacks have become a severe threat to the security of web servers. These attacks evade most intrusion prevention systems by sending numerous benign HTTP requests. Since most of these attacks are launched abruptly and severely, a fast intrusion prevention system is desirable to detect and mitigate these attacks as soon as possible. In this paper, we propose an effective defense system, named SkyShield, which leverages the sketch data structure to quickly detect and mitigate application layer DDoS attacks. First, we propose a novel calculation of the divergence between two sketches, which alleviates the impact of network dynamics and improves the detection accuracy. Second, we utilize the abnormal sketch to facilitate the identification of malicious hosts of an ongoing attack. This improves the efficiency of SkyShield by avoiding the reverse calculation of malicious hosts. We have developed a prototype of SkyShield and carefully evaluated its effectiveness using real attack data collected froma large-scale web cluster. The experimental results show that SkyShield can quickly reduce malicious requests, while posing a limited impact on normal users.