Traceback Model for Identifying Sources of Distributed Attacks In Real Time

Abdulghani Ali Ahmed, Ali Safa Sadiq and Mohamad Fadli Zolkipli
Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang (UMP), Pahang, Malaysia

ABSTRACT
Locating sources of distributed attack is time-consuming; attackers are identified long after the attack is completed. This paper proposes a trackback model for identifying attackers and locating their distributed sources in real time. Attackers are identified by monitoring violations of malicious end users on their bandwidth shares predefined in the service level agreement. Then, active connections of the malicious users are investigated to locate the host machines used as distributed sources of attack traffic. Mathematical model and simulation results demonstrate that the proposed model can reduce the required time for identifying malicious users and locating host machines used as the actual sources of attack packets.

KEYWORDS: real-time trackback; distributed attack; explicit congestion notification; service level agreement; active connection

DOI: 10.1002/sec.1476