Classification of UDP Traffic for DDoS Detection

Alex Bardas

Kansas State University

Abstract:

"UDP (User Datagram Protocol) traffic has recently been used in flooding-based distributed denial of service (DDoS) attacks, most notably by those launched by the Anonymous group. Despite extensive past research in the general area of DDoS detection/prevention, the industry still needs effective tools to deal with DDoS at- tacks leveraging UDP traffic. This work presents our investigation into the proportional-packet rate assumption, and the use of this criterion to classify UDP traffic with the goal of detecting malicious addresses that launch flooding-based UDP DDoS attacks. We performed our experiments on data from a large number of production networks including large corporations (edge and core), ISPs, universities, financial institutions, *etc*. In addition, we also conducted experiments on the DETER testbed as well as a testbed built in the Argus cybersecurity lab. All the experiments indicate that the proportional-packet rate assumption generally holds for benign UDP traffic and can be used as a reasonable criterion to differenti- ate DDoS and non-DDoS traffic. We designed and implemented a prototype classifier based on this assump- tion and discuss ways it can be used to effectively detect UDP-based flooding attacks."