Effective amplification mitigation and spoofing detection during DNS flooding attacks on internet

ABSTRACT

Recent flooding attacks using Domain Name System (DNS) is used by cybercriminals to launch hundreds of gigabytes of attack traffic to paralyze their victims. The lack of security features in DNS protocol and adding security layers to this protocol is subject of further studying. In this reserach, we proposed a distributed mechanism to counter DNS reflection based attacks with high detection accuracy and little overhead on network channels. We suggested Distributed Defense Scheme (DDS) to provide authenticity to DNS transactions (i.e. request and response) through authentication message exchange. Then our classification filtering plays an important role in distinguishing between real bogus DNS requests and discarding the fake requests. Our analysis shows how DDS can remarkably reduce amplification factor for attack traffic without affecting normal traffic flow.

Keyword: DNS security; DNS reflection/ amplification attacks; DNS authentication; Authentication message; Classification filtering