Distributed defense scheme for managing DNS reflection attack in network communication systems

ABSTRACT

Domain Name System (DNS) is based on client-server architecture and employed User Packet Diagram (UDP) protocol to transport requests and responses. Due to UDP supports unreliable connection, malicious users are able to fabricate spoofed DNS requests very easily. Such DNS problems in turn affect numerous other network services and critical in resource utilization. Delay in deploying secure DNS motivates the need for local networks to protect DNS infrastructure. DNS reflection attack for example takes advantage of the DNS response message and results substantially larger than DNS query messages. In this work, we propose a distributed defense scheme in DNS infrastructure to prevent from reflection attack. Our defense scheme aims to prevent spoofed addresses from getting any responses by applying a classification-based packet filtering strategy. Specifically, our local DNS server regularly checked DNS requests in its database in order to differentiate between legitimate and illegitimate requests. We invent validation phase in our filtering strategy by getting confirmation before the request stored in local side server. The key idea behind this is to ensure the local DNS database is merely stored legitimate requests and prevent the fake DNS request transferred to users. Our analysis and the corresponding experimental results show that the proposed scheme offers an effective defense solution while implicitly improving network communication traffic

Keyword: DNS reflection attack; Defense scheme; Communication traffic