Public Review for

Practical Challenge-Response for DNS

R. Al-Dalky, M. Rabinovich, M. Allman

DNS attacks are becoming an increasingly difficult challenge for authoritative DNS servers. Establishing the legibility and authenticity of a request via challenge-response is a step forward in dealing with the flood of requests from an increasingly diverse catalogue of services and devices. Successful deployment of the proposed approach can help in preventing DNS amplification attacks, where attackers spoof DNS queries from a victim which in turn receives the flood of (large) query answers. The proposed approach requires certain deviations from the standard practices on the Internet today, while enabling dealing with more complicated attack scenarios in the presence of DNS resolver pools.

While the reviewers and the authors highlighted the deployment challenges of the proposed approach in presence of DNSSEC, reflection attacks, or CNAME breaking at zone APEXes, the contributions of the paper in the measurement domain, and the proposed strategy, were deemed of great interest to the network measurement and security community as a potentially scalable and practical step forward in dealing with DNS attacks.

Public review written by
Hamed Haddadi
Imperial College