Practical Challenge-Response for DNS

Rami Al-Dalky
Case Western Reserve University
rxa271@case.edu

Michael Rabinovich
Case Western Reserve University
michael.rabinovich@case.edu

Mark Allman
ICSI
mallman@icir.org

ABSTRACT

Authoritative DNS nameservers are vulnerable to being used in denial of service attacks whereby an attacker sends DNS queries while masquerading as a victim—hence coaxing the DNS server to send the responses to the victim. Reflecting off innocent DNS servers both hides the attackers identity and often amplifies the attackers traffic by turning small DNS requests sent to the nameserver into large DNS answers sent to the victim. In this poster we discuss a practical challenge-response technique that establishes a requester's identity before sending a full answer. Unlike previous schemes, our work deals with so-called "resolver pools"—or groups of DNS resolvers that work together to lookup records in the DNS. In these cases a challenge transmitted to a resolver N1 may be dealt with by a different resolver N2, thus leaving an authoritative DNS server wondering whether N2 is another resolver in the pool or a victim. We propose a technique called "challenge chains" to establish identity in the face of resolver pools. We show that the cost of our scheme in terms of added delay is small. This work appears in [1].

[1] Rami Al-Dalky, Michael Rabinovich, Mark Allman. Practical Challenge-Response for DNS. ACM Computer Communication Review, 48(3), July 2018.

CCS CONCEPTS

• **Networks** → **Network protocol design**; **Naming and addressing**;

KEYWORDS

DNS; measurement; security; performance.

ACM Reference Format:
Rami Al-Dalky, Michael Rabinovich, and Mark Allman. 2018. Practical Challenge-Response for DNS. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3232755.3232765

ANRW '18, July 16, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232765